Линейная алгебра КТ 2025 М3136

created by fyddan

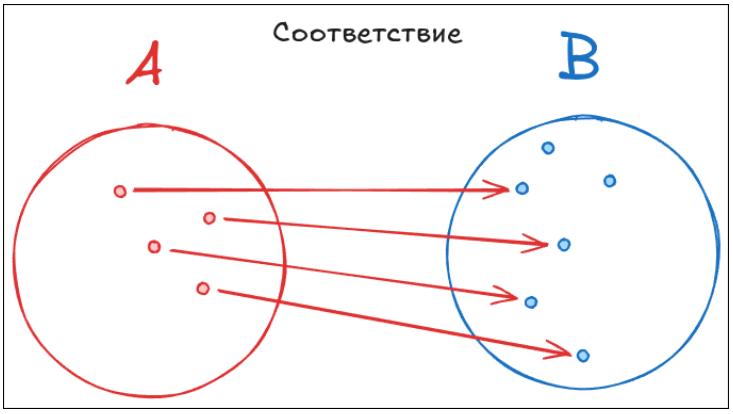
также спасибо Ерину Алексею за определения и Давыденко Тарасу за билеты по тензорам и внешним степеням

Содержание

1 Соответствия, композиции соответствий, ассоциативность композиции.

1.1 Соответствия

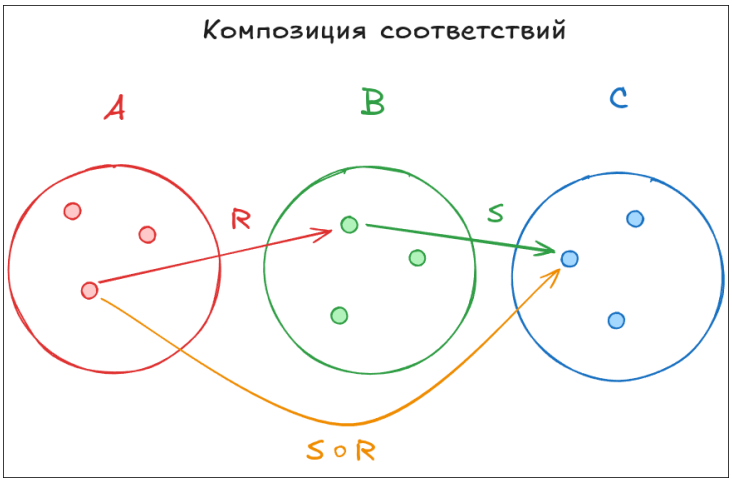
Определение: соответствием из A в B называют подмножество $R \subset A \times B$, такое что $\forall\ a \in A\ \exists\ b\ \ \in B : (a, b) \in R$, разница с отношением в том, что тут мы требуем, чтобы каждый элемент из первого множества имел хотя бы один парный элемент из второго множества.



1.2 Композиция соответствий

Определение: Пусть R - соответствие из A в B, S - соответствие из B в C, тогда композиция $S \circ R$ это такое соответствие из A в C:

$$S \circ R = \{(a, c) \in A \times C \mid \exists b \in B : (a, b) \in R,\ \ (b, c) \in S\}$$



1.3 Ассоциативность композиции

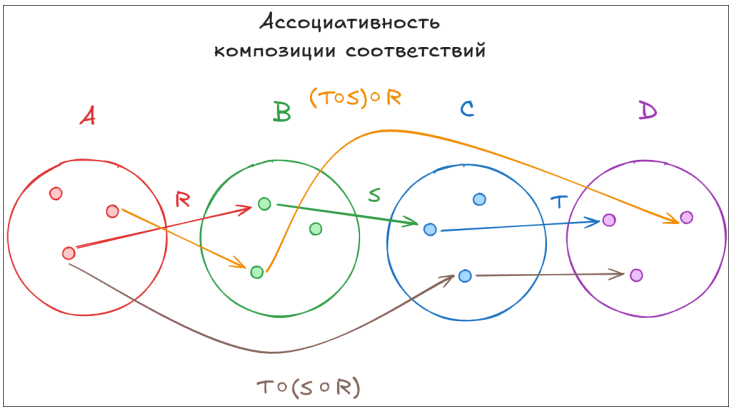
Композиция обладает свойством ассоциативности, докажем это: пусть у нас есть соответствие R из A в B, S из B в C, T из C в D, тогда сделаем предположение что

$(T \circ S) \circ R$ равносильно $T \circ (S \circ R)$, покажем что это одно и то же:

$(T \circ S) \circ R = \{(a,d) \in A \times D : \exists b \in B : (a,b) \in R, (b,d) \in T \circ S\} = \{(a,d) \in A \times D : \exists b \in B, \exists c \in C : (a,b) \in R, (b,c) \in S, (c,d) \in T\}$

$T \circ (S \circ R) = \{(a,d) \in A \times D : \exists c \in C : (a,c) \in S \circ R, (c,d) \in T\} = \{(a,d) \in A \times D : \exists b \in B, \exists c \in C : (a,b) \in R, (b,c) \in S, (c,d) \in T\}$

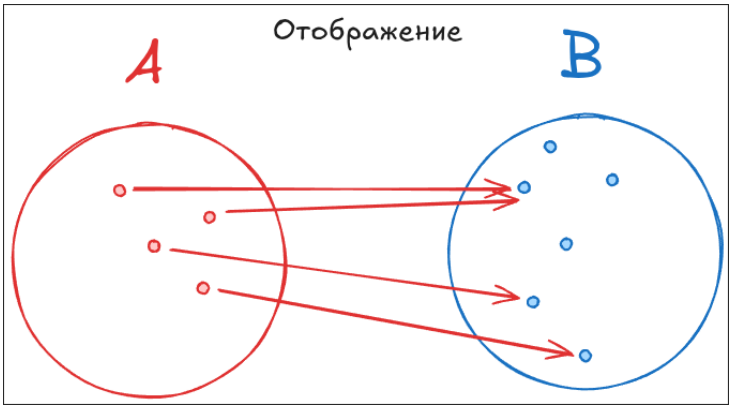
Заметим что правила задания множества полностью совпадают, следовательно это равные множества, что и требовалось доказать.



2 Отображение множеств как частный случай соответствия. Инъекция и сюръекция. Обратимость отображения слева и справа. Совпадение левого и правого обратных.

2.1 Отображения

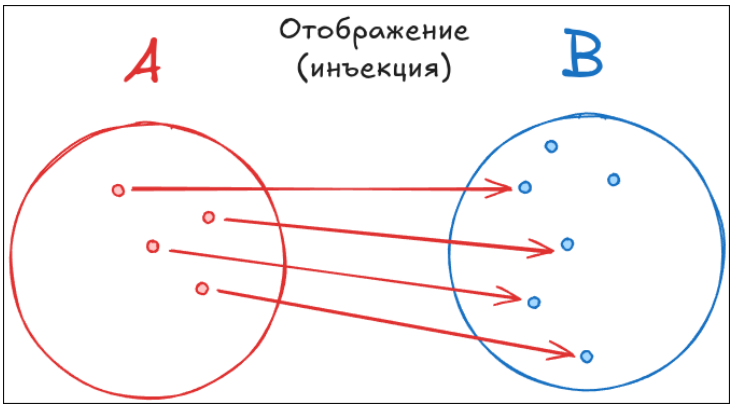
Определение: назовем отображением соответствие $f \subset A \times B$ такое что: $\forall a \in A \; \exists! \; b \in B : (a,b) \in f$



2.2 Инъекция

Определение: инъекция это такое отображение для которого выполняется:

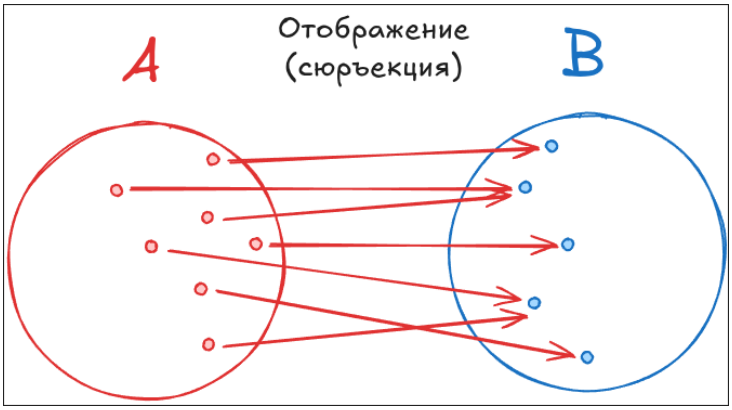
$$f(a) = f(b) \iff a = b$$



2.3 Сюръекция

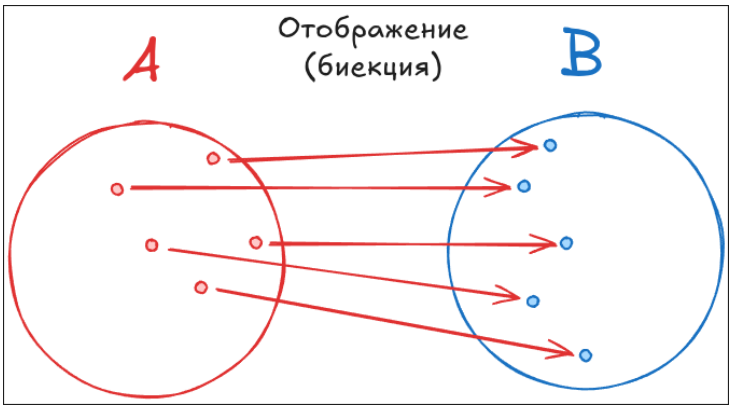
Определение: сюръекция это такое отображение для которого выполняется:

$$\forall b \in B \; \exists a \in A : f(a) = b$$



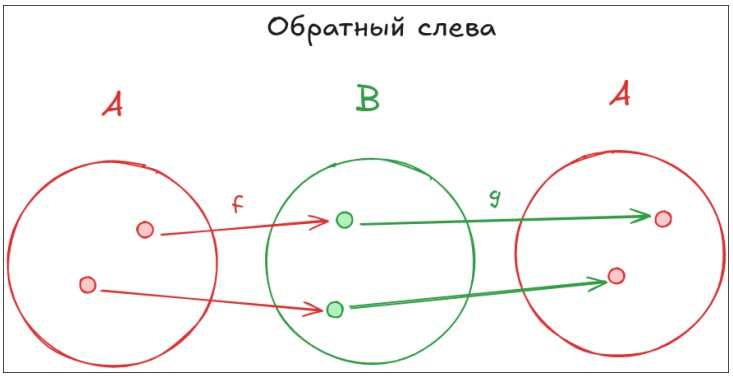
2.4 Биекция

Определение: биекция это отображение, которое и инъективно и сюръективно, то есть можно составить взаимно однозначное соответствие.



2.5 Обратное отображение слева

Определение: Пусть у нас есть отображение $f : A \to B$, тогда отображение $g : B \to A$ называется обратным слева, если $g \circ f = idA$, то есть элемент из A возвращается в себя же. Интересно что f обязано быть инъективным, так как иначе при $a_1 \neq a_2, f(a_1) = f(a_2)$ случится противоречие, так как $g(f(a_1)) = g(f(a_2)) \implies a_1 = a_2$. Обратный слева также называют idA, так как он всегда возвращает свое же значение.

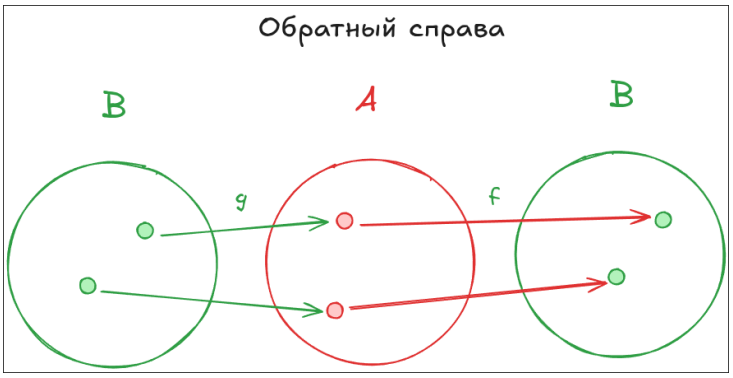


2.6 Обратное отображение справа

Определение: Пусть у нас есть отображение $f : A \to B$, тогда отображение $g : B \to A$ называется обратным справа, если $f \circ g = idB$, то есть элемент из B возвращается в себя же. f обязано быть сюръективным, то есть содержать прообразы для каждого $b \in B$, иначе мы не сможем для любого элемента из B совершить путь через A обратно в себя. Обратный справа также называют idB.

2.7 Совпадение обратного правого и обратного левого

Из определений обратного правого и левого следует, что $f : A \to B$ одновременно инъективно и сюръективно, следовательно это биекция, тогда $g : B \to A$ это просто обратное отображение, которое можно также обозначить как f^{-1}.



3 Определение бинарной операции, моноида, группы. Единственность нейтрального и обратного элемента. Примеры моноидов и групп.

3.1 Бинарная операция

Определение: Бинарной операцией $\cdot$ на множестве M называется отображение из $M \times M \to M$. Например умножение на $\mathbb{N}$ это бинарная операция, а вот на $\mathbb{N} \cup \{-1\}$ уже нет, так как при умножении числа на -1 мы выйдем за пределы исходного множества.

3.2 Полугруппа

Определение: Полугруппой $(M, \cdot)$ называется такая алгебраическая структура, в которой соблюдается ассоциативность, то есть: $m_1 \cdot (m_2 \cdot m_3) = (m_1 \cdot m_2) \cdot m_3$, пример - $(\mathbb{N}, \cdot)$. У нас соблюдается ассоциативность.

3.3 Моноид

Определение: моноидом называется полугруппа, в которую добавили нейтральный элемент e, для которого выполняется: $e \cdot m = m = m \cdot e$, если также добавляется коммутативность, то есть $m_1 \cdot m_2 = m_2 \cdot m_1$, тогда мы называем это коммутативным (абелевым) моноидом. Пример: $(\mathbb{N} \cup \{0\}, +)$

3.4 Единственность нейтрального элемента

Утверждение: нейтральный элемент единственный, если он существует.
Доказательство: пусть у нас все таки есть e_1 и e_2, оба нейтральные элементы, тогда $e_1 = e_2$:

$$e_1 = e_1 \cdot e_2 = e_2$$

что и требовалось доказать.

3.5 Группа

Определение: группой называют моноид, в котором $\forall m \in M \; \exists m^{-1} : m \cdot m^{-1} = e$. То есть для каждого элемента найдется обратный, который при проведении операции с таковым вернет нейтральный элемент. Пример: $(\mathbb{Q} \setminus \{0\}, \cdot)$ или $(\mathbb{Z}, +)$.

3.6 Единственность обратного элемента

Утверждение: обратный элемент единственный, если он существует.
Доказательство: пусть у нас есть обратные к g элементы h_1 и h_2, тогда $h_1 = h_2$:

$$h_1 = h_1 \cdot (g \cdot h_2) = (h_1 \cdot g) \cdot h_2 = h_2$$

что и требовалось доказать.

4 Определение кольца. Закон нуля. Умножение на -1. Коммутативность и ассоциативность. Примеры колец.

4.1 Кольцо

Определение: кольцом называется множество M с определенными двумя бинарными операциями, например: $\cdot, +$. Так, что $(M, +)$ - абелева группа, а $(M, \cdot)$ - полугруппа. А также операции связаны законом дистрибутивности: $\forall a, b, c \in M \ a \cdot (b + c) = a \cdot b + a \cdot c, (a + b) \cdot c = a \cdot c + b \cdot c$.

4.2 Ассоциативное кольцо

Определение: ассоциативным кольцом называется то, у которого вторая операция также ассоциативна.

4.3 Кольцо с единицей

Определение: кольцом с единицей называется то, у которого для второй операции определен нейтральный элемент.

4.4 Коммутативное кольцо

Определение: коммутативным кольцом называется то, у которого вторая операция коммутативна.

4.5 Примеры:

- $(\mathbb{Z}, +, \cdot)$ - коммутативное ассоциативное с единицей
- $(3\mathbb{Z}, +, \cdot)$ - коммутативное ассоциативное

5 Делимость в коммутативном кольце. Делители нуля. Область целостности. Ассоциированные элементы. Критерий ассоциированности в области целостности. Сокращение в области целостности.

5.1 Делимость

Определение: $a|b, a, b \in R$ означает $\exists c \in R\ b = a \cdot c$.

5.2 Делители нуля

Определение: $r \neq 0 \in R$ - делитель нуля, если $\exists s \neq 0 \in R : r \cdot s = 0$

5.3 Область целостности

Определение: кольцо R называется областью целостности, если в нем нет делителей нуля.

5.4 Ассоциированные элементы

Определение: $a, b \neq 0 \in R$ называют ассоциированными ($a \sim b$), если $a|b$ и $b|a$.
Утверждение: Пусть R - область целостности, $a, b \in R$ и $a \sim b$, тогда $\exists u \in R^\times : a = u \cdot b$.
Доказательство:

$$a \sim b \implies \begin{cases} a|b \\ b|a \end{cases} \implies \begin{cases} \exists c \in R : b = a \cdot c \\ \exists d \in R : a = b \cdot d \end{cases} \implies$$
$$\implies b = b \cdot c \cdot d \implies b(1 - c \cdot d) = 0 \implies$$
$$\implies c \cdot d = 1 \implies c, d \in R^\times \implies u = d$$

5.5 Сокращение в области целостности

Утверждение: R - область целостности и $a \neq 0$, тогда $(a \cdot b = a \cdot c) \implies (b = c)$
Доказательство: $a \cdot (b - c) = 0 \implies b - c = 0 \iff b = c$

6 Алгоритм Евклида в евклидовой области. Существование НОД в евклидовой области. Теорема о линейном представлении НОД в евклидовой области.

6.1 Евклидова область

Определение: область целостности R, в которой существует функция нормы $N : R \setminus \{0\} \to \mathbb{N}$ такая что: $N(a \cdot b) \geq N(a)$ и $\forall a, b \in R\ \exists c, r \in R, b \neq 0 : a = b \cdot c + r : N(r) < N(b)$, или $r = 0$.

6.2 НОД

Определение: R - коммутативное кольцо с единицей, $a, b \in R$, $gcd(a,b) = d \in R$: 1) $d|a, d|b$ 2) $\forall c \in R : c|a, c|b\ c|d$.
Свойство: если $gcd(a,b)$ существует, то единственный с точностью до ассоциированного. Если $gcd(a,b) = d = d'$, то $d|d'$ и $d'|d$, а если R - область целостности, то $d = d' \cdot u, u \in R^\times$
Доказательство: $d|a, d|b, d'|a, d'|b \implies d'|d$, аналогично для d

6.3 Алгоритм Евклида

Теорема: R - евклидово кольцо $a, b \in R$ и они одновременно не ноль, тогда:

$$1)\exists gcd(a,b) = d \in R\ 2)\exists x, y \in R : d = ax + by$$

Доказательство: 1 случай: $a = 0$ или $b = 0$, тогда $gcd(0,b) = b$ или $gcd(a,0) = a$, так как $a = gcd(a,0) = a \cdot 1 + 0 \cdot 1$ и аналогично для b
2 случай: $a, b \neq 0$
$a = q_0 b + r_0 \wedge N(r_0) < N(b)$
$b = q_1 r_0 + r_1 \wedge N(r_1) < N(r_0)$
$r_0 = q_2 r_1 + r_2 \wedge N(r_2) < N(r_1)$
$\dots$
$r_{n-1} = q_{n-1} r_n + r_{n+1} \wedge N(r_{n+1}) < N(r_n)$
на каком то шаге станет:
$r_n = q_n r_{n+1} \implies r_{n+2} = 0$
Утверждение: $r_{n+1} = gcd(a,b)$
Доказательство:

1. Первое условие НОД
   $r_{n+1}|a \wedge r_{n+1}|b$: $r_{n+1}|r_n \implies r_{n+1}|r_{n-1} \implies \cdots \implies r_{n+1}|b \implies r_{n+1}|a$
2. Существует линейная комбинация с r_{n+1}
   $r_0 = a - q_0 b$
   $r_1 = b - q_1 r_0 = b - q_1(a - q_0 b) = b - q_1 a + q_0 q_1 b = -q_1 a + b(1 + q_0 q_1 b)$, пусть коэффициент a это S_1, а коэффициент с b это T_1.
   $r_2 = S_2 a + T_2 b$
   $\dots$
   $r_{n+1} = S_{n+1} a + T_{n+1} b$
3. Также нам нужно доказать второе условие НОД
   $\forall c \in R : c|a, c|b \implies c|S_{n+1} a \wedge c|T_{n+1} b \implies c|r_{n+1} \implies gcd(a,b) = r_{n+1}$

7 Евклидова область является областью главных идеалов.

7.1 Область главных идеалов

Определение: область целостности R - область главных идеалов, если для любого идеала $I \subseteq R$ существует такой элемент $x \in I : (x) = I$

7.2 Идеал

Определение:

$$I - \text{идеал } M \iff \begin{cases} I \subseteq M, I \neq \varnothing \\ \forall a, b \in I \ a + b \in I \\ \forall m \in M \ m \cdot i \in I \end{cases}$$

7.3 Главный идеал

Определение:

$$(x) - \text{главный идеал } M \iff (x) = \{xm : m \in M\}$$

Утверждение: любое евклидовое кольцо R - область главных идеалов.
Доказательство: Пусть I - идеал в R, $I \neq \{0\}$, $S = \{N(x) : x \in I\} \implies \exists N(d)$ - наименьшая норма. Можно утверждать, что $(d) = I$:

1. левое включение: $d \in I \implies rd \in I \implies (d) \subset I$
2. правое включение: Пусть $x \in I$, разделим x на d с остатком: $x = dq \cdot r$, нам нужно, чтобы $r = 0$. У нас допустима ситуация, что $N(r) < N(d)$, но такая ситуация на самом деле невозможна, так как $r = x - dq \implies r \in I$, но $N(d)$ - наименьшая норма для элементов из I, поэтому r может быть только нулем, тогда $I \subset (d)$

8 В области главных идеалов каждая возрастающая цепочка идеалов стабилизируется.

8.1 Теорема

Пусть R - область главных идеалов, также у нас есть цепочка вложенных идеалов: $I_1 \subset I_2 \subset I_3 \ldots$, тогда $\exists N \in \mathbb{N} : I_N = I_{N+1} = I_{N+2} \ldots$, то есть цепочка стабилизируется. Такое явление еще называют Нетеровым кольцом.
Доказательство: Так как R - ОГИ, каждый $I_k = (i_k)$, то есть каждый идеал главный. Допустим у нас есть $I_\infty = \bigcup\limits_{k=1} I_k$, теперь покажем, что I_∞ это тоже идеал:

1. Замкнутость по сложению
   Пусть $a, b \in I_\infty$, тогда $\exists n_1, n_2 \in \mathbb{N} : a \in I_{n_1}, b \in I_{n_2}$, тогда не умаляя общности: $a, b \in I_{n_2} \implies a + b \in I_{n_2} \in I_\infty$
2. Замкнутость по умножению на элемент из кольца
   Пусть $a \in I_\infty$ и $r \in R$, тогда $\exists n \in \mathbb{N} : a \in I_n$, так как I_n - идеал: $ar \in I_n \in I_\infty$

Так как I_∞ - идеал и он лежит в R, $\exists x \in I_\infty : (x) = I_\infty$, тогда $\exists N : x \in I_N$, но мы можем сказать, что $I_N = I_\infty$, тут не очевидно только левое включение: $\forall y \in I_\infty \implies y = sx, s \in R, x \in I_N \implies sx = y \in I_N \implies I_N = I_\infty$, тогда начиная с N: $I_N = I_{N+1} = I_{N+2} \ldots$

9 В области главных идеалов необратимый элемент раскладывается в произведение неприводимых.

9.1 Неприводимый элемент

Определение: $r \in R \setminus R^\times$ - неприводимый, если из разложения $r = st$ следует, что хотя бы один из элементов обратимый, то есть $s \in R^\times \vee t \in R^\times$

9.2 Теорема

Утверждение: R - ОГИ, $r \in R \setminus R^\times$, тогда существует разложение r в произведение неприводимых единственное с точностью до перестановки множителей и ассоциированности.
Доказательство: Пусть у нас есть множество $S = \{(x) : x-$ не раскладывается в произведение неприводимых, $x \neq 0, x \in R \setminus R^\times\}$, мы предположим, что оно не пусто, по доказательству конечности цепочки вложенных идеалов мы можем взять максимальный элемент (z), тогда мы можем сказать, что z не может быть неприводимым, так как тогда оно будет иметь разложение на неприводимые $z = z$, что противоречит нашему множеству S. Тогда из этого следует, что z - приводимый, тогда он имеет разложение $z = st, s, t \in R \setminus R^\times$, но тогда z делится на s или t, а это то же самое, что $(z) \subset (s)$ или $(z) \subset (t)$, но (z) - минимальный по включению идеал в $S \implies (s), (t) \notin S$, тогда по определению множества S s и t имеют разложение на неприводимые: $s = q_1 \cdot q_2 \dots q_n$, $t = p_1 \cdot p_2 \dots p_n$, но тогда $z = (q_1 \cdot q_2 \dots q_n) \cdot (p_1 \cdot p_2 \dots p_n)$, следовательно z имеет разложение на неприводимые, получаем противоречие, следовательно $S = \varnothing$, тогда любой элемент в Области главных идеалов имеет разложение на неприводимые.

10 Основная теорема арифметики в области главных идеалов.

10.1 Простой элемент

Определение: элемент $r \in R \setminus R^\times$ называется простым, если из того, что $r|ab \implies r|a \vee r|b$

10.2 Лемма

Утверждение: R - ОГИ, r - неприводим, тогда r - простой.
Доказательство: Пусть $r|ab$, рассмотрим все возможные линейные комбинации (r, a), тогда $\exists d \in R : (d) = (r, a) \implies d|r, d|a$, $r \in (r, a) \implies r \in (d) \implies \exists s \in R : r = sd \implies$ 1) $d \in R^\times$ 2) $r \sim d$.

1. Если $d \in R^\times \implies (d) = R \implies d = 1$, получается что наша линейная комбинация это $1 = xr + ya$, мы можем домножить все на b, тогда $b = xrb + yab$, тогда $r|xrb, r|ab \implies r|b$

2. Если $r \sim d$, то по определению ассоциированности $r|d$, а $d|a \implies r|a$

То есть для любого случая r - простой

10.3 Единственность разложения на неприводимые

Пусть $r = p_1 \cdot p_2 \dots p_n = q_1 \cdot q_2 \dots q_n$ все элементы неприводимы, а значит простые. Рассмотрим p_1: $p_1|(p_1 \cdot p_2 \dots p_n), p_1|(q_1 \cdot q_2 \dots q_m)$. $m = n$, иначе бы какие то элементы были единицами, чтобы не нарушить равенство, тогда бы нарушилось условие, что все элементы неприводимы. Затем находим среди элементов q_i такой, что $p_1 \sim q_i$, меняем местами q_i и q_1, после всех подобных перестановок получим $p_1 \sim q_1, p_2 \sim q_2, \dots, p_n \sim q_n$.

11 Фактор-кольцо, корректность операций. Кольцо классов вычетов. Обратимые элементы в $\mathbb{Z}/n\mathbb{Z}$.

11.1 Отношение эквивалентности

Определение: $\sim$ - отношение эквивалентности на множестве M, если $\sim \subset M \times M$, в котором для пары (a, b) выполняется заданное условие $a \sim b$, а также отношение обладает: 1) рефлексивность, 2) симметричность, 3) транзитивность.

11.2 Фактор-кольцо

Определение: R - кольцо, I - идеал на этом кольце, тогда R/I это фактор по отношению эквивалентности такому, что $a \sim b \iff a - b \in I$, то есть элементы различаются на элемент из идеала. Тогда R/I это множество из классов эквивалентности $[x] = \{y \in R : x \sim y\}$

11.3 Корректность операций

Докажем, что $[a] + [b] = [a + b] = [a' + b'], a \sim a', b \sim b'$: Нам нужно доказать что $a + b \sim a' + b'$. $(a + b) - (a' + b') = (a - a') + (b - b') \in I$
Докажем что $[ab] = [a'b']$: $ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + b'(a - a') \in I$

11.4 Кольцо классов вычетов

Определение: Кольцо классов вычетов это кольцо $\mathbb{Z}$ факторизованное по главному идеалу (n). Оно содержит классы эквивалентности, в которых $a \sim b \implies a = b \mod n$. То есть классы эквивалентности содержат элементы, которые дают одинаковый остаток при делении на n.

11.5 Обратимые элементы в $\mathbb{Z}/n\mathbb{Z}$.

Обратимыми в Z/nZ являются такие $x : gcd(x, n) = 1$, это очень легко доказывается, мы можем представить линейную комбинацию для нод: $xk + yn = 1 \mod n \implies xk = 1 \mod n \implies k$ - обратимый элемент для x. То есть в $\mathbb{Z}/p\mathbb{Z}$ все ненулевые элементы обратимы, соответственно это уже не просто кольцо, а поле

12 Гомоморфизм колец. Проекция на фактор - гомоморфизм. Ядро гомоморфизма - идеал. Образ гомоморфизма - подкольцо.

12.1 Гомоморфизм колец

Определение: отображение $f : R \to S$ - гомоморфизм если:

1. $f(r_1 + r_2) = f(r_1) + f(r_2)$
2. $f(r_1 \cdot r_2) = f(r_1) \cdot f(r_2)$
3. $f(1_R) = 1_S$, требование единицы не является обязательным, если кольца без единицы.

12.2 Проекция на фактор кольца

Утверждение: Если I - идеал кольца R, то $\pi : R \to R/I$ - гомоморфизм.
Доказательство: $\pi(a)$ просто отправляет a в его класс эквивалентности $[a]$.

1. $\pi(a + b) = [a + b] = [a] + [b] = \pi(a) + \pi(b)$
2. $\pi(ab) = [ab] = [a] \cdot [b] = \pi(a) \cdot \pi(b)$
3. $\pi(1) = [1] = 1_{R/I}$

12.3 Ядро гомоморфизма

Определение: для гомоморфизма $f : R \to S$ ядро $\ker f = \{r \in R : f(r) = 0\}$, то есть в ядре лежат все элементы R, которые превратятся в ноль.
Утверждение: $\ker f$ - идеал в кольце R.
Доказательство:

1. $ker f \neq \varnothing$, т.к всегда в ядре находится ноль.
2. пусть $a, b \in \ker f$, тогда $f(a) = f(b) = 0 \implies f(a + b) = f(a) + f(b) = 0 + 0 = 0 \in \ker f$
3. пусть $a \in \ker f$, $b \in R$, тогда $f(ra) = f(r) \cdot f(a) = f(r) \cdot 0 = 0 \in \ker f$

Все три условия для того что ядро - идеал доказаны.

12.4 Образ гомоморфизма

Определение: образ гомоморфизма $f : R \to S$ - $Im\ f\{s \in S : \exists r \in R : f(r) = s\}$
Утверждение: такой образ - подкольцо S.
Доказательство:

1. $f(0_R) = f(0_R + 0_R) = f(0_R) + f(0_R) \implies f(0_R) = 0_S$
2. Пусть $x, y \in Im\ f \implies \exists a, b \in R : x = f(a), y = f(b)$, тогда $x - y = f(a) - f(b) = f(a - b) \in Im\ f$ - замкнуто по вычитанию, значит есть для каждого обратный элемент по сложению

3. $xy = f(a) \cdot f(b) = f(ab) \in Im\ f$ - замкнуто по умножению

Следовательно $Im\ f$ - подкольцо S.

13 Критерий инъективности гомоморфизма колец через определение ядра. Гомоморфизм является изоморфизмом тттк он биекция.

13.1 Критерий инъективности

Утверждение: $f : R \to S$ - гомоморфизм, тогда f - инъекция $\iff \ker f = \{0\}$
Доказательство:

1. достаточность:
   Пусть $\exists a \in \ker f : f(a) = 0$, но $f(0) = 0$, тогда по инъективности f $a = 0$

2. необходимость:
   Пусть $a, b \in R$ и $f(a) = f(b) \implies f(a) - f(b) = 0 \implies f(a - b) = 0 \implies$
   $\implies a - b \in \ker f \implies a - b = 0 \implies a = b \implies f-$ инъекция

13.2 Изоморфизм

Определение: Кольца R и S называют изоморфными если для гомоморфизма $f : R \to S$, существует гомоморфизм $g : S \to R$, такой что у f есть обратный слева $g \circ f = id_R$ и обратный справа $f \circ g = id_S$.

13.3 Гомоморфизм являтся изоморфизмом

Утверждение: если гомоморфизм $f : R \to S$ - изоморфизм $\iff$ f - биекция.
Доказательство:

1. достаточность:
   если f - изоморфизм, то по определению существует $g : S \to R$ такой, что $g \circ f = id_R \implies f$ - инъекция и $f \circ g = id_S \implies f$ - сюръекция, тогда f - биекция.

2. необходимость:
   если f - биекция, то существует обратное отображение f^{-1}, нам надо доказать, что это гомоморфизм (наличие обратного левого и правого исходит из биективности f). Возьмем любые y_1, y_2 такие что $x_1 = f^{-1}(y_1), x_2 = f^{-1}(y_2)$:

   (a) сложение:
   нам нужно доказать, что $f^{-1}(y_1+y_2) = f^{-1}(y_1)+f^{-1}(y_2)$. $y_1+y_2 = f(x_1+x_2)$.
   $f^{-1}(y_1 + y_2) = f^{-1}(f(x_1 + x_2)) = x_1 + x_2 = f^{-1}(y_1) + f^{-1}(y_2)$

   (b) умножение:
   нам нужно доказать, что $f^{-1}(y_1 \cdot y_2) = f^{-1}(y_1) \cdot f^{-1}(y_2)$. $y_1 \cdot y_2 = f(x_1 \cdot x_2)$.
   $f^{-1}(y_1 \cdot y_2) = f^{-1}(f(x_1 \cdot x_2)) = x_1 \cdot x_2 = f^{-1}(y_1) \cdot f^{-1}(y_2)$

Выходит, что f^{-1} - гомоморфизм, тогда f - изоморфизм.

14 Лемма о пропуске гомоморфизма через факторкольцо. Теорема об изоморфизме.

14.1 Лемма

Утверждение: $f : R \to S$ - гомоморфизм, I - идеал R, тогда $\exists \overline{f} : R/I \to S$ - гомоморфизм, такой, что $\overline{f} \circ \pi = f \iff I \subset \ker f$.
Доказательство:

1. достаточность:
   $\forall a \in I \ f(a) = \overline{f}(\pi(a)) = \overline{f}(0) = 0 \implies a \in \ker f$

2. необходимость:
   Пусть $[r] \in R/I$, тогда $\overline{f}([r]) = f(r), r \in [r]$. Но нам необходимо доказать корректность: Пусть $r, r' \in [r]$, $f(r') = \overline{f}([r]) = f(r)$? Это действительно так: $f(r) - f(r') = f(r - r') \in I$ и равно нулю, по предположению, что $I \subset \ker f$.
   Почему $\overline{f}$ - гомоморфизм:

   - $\overline{f}([1]) = f(1) = 1$
   - $\overline{f}([a] + [b]) = \overline{f}([a + b]) = f(a + b) = f(a) + f(b) = \overline{f}([a]) + \overline{f}([b])$
   - $\overline{f}([a] \cdot [b]) = \overline{f}([a \cdot b]) = f(a \cdot b) = f(a) \cdot f(b) = \overline{f}([a]) \cdot \overline{f}([b])$

Также покажем коммутативность: Пусть $r \in R$, $\overline{f}(\pi(r)) = \overline{f}([r]) = f(r)$

14.2 Первая теорема об изоморфизме

Утверждение: $f : R \to S$ - гомоморфизм, тогда $R/\ker f \xrightarrow{\cong} Im\ f$
Доказательство: существует гомоморфизм $R \to Im\ f$, тогда, чтобы построить $R/\ker f \to Im\ f$ необходимо и достаточно по лемме, чтобы $\ker f \subset \ker f$, что всегда правда. Обозначим этот гомоморфизм $\overline{f}$, теперь нам надо доказать, что он биективен:

1. инъекция:
   $\ker f = \{[r] \in R/\ker f : \overline{f}([r]) = 0\} = \{[r] : f(r) = 0\} = \{0\}$, тогда это инъекция

2. Сюръекция:
   Пусть $s \in Im\ f$, тогда существует $r \in R : f(r) = s$, тогда $\overline{f}([r]) = f(r) = s$, получается сюръекция.

$\overline{f}$ - биекция, а значит и изоморфизм.

15 Китайская теорема об остатках в $\mathbb{Z}$.

Утверждение: $gcd(m, n) = 1$, тогда $\sigma : \mathbb{Z}/mn\mathbb{Z} \xrightarrow{\cong} (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$
Доказательство: $\sigma(k) = (k \mod n, k \mod m)$ Покажем, что σ - гомоморфизм:

1. Сложение: $\sigma(k+k') = ([k+k']_n, [k+k']_m) = ([k]_n+[k']_n, [k]_m+[k']_m) = ([k]_n, [k]_m)+([k']_n, [k']_m) = \sigma(k) + \sigma(k')$

2. Умножение: Умножение: $\sigma(k \cdot k') = ([k \cdot k']_n, [k \cdot k']_m) = ([k]_n \cdot [k']_n, [k]_m \cdot [k']_m) = ([k]_n, [k]_m) \cdot ([k']_n, [k']_m) = \sigma(k) \cdot \sigma(k')$

3. Сохраняет единицу: $\sigma([1]_{mn}) = ([1]_{mn} \mod n, [1]_{mn} \mod m) = ([1]_n, [1]_m)$

Определим $\ker \sigma = \{k \in \mathbb{Z}/nm\mathbb{Z} : k = 0 \mod n \wedge k = 0 \mod m\}$, пусть у нас $k \in \ker \sigma$, тогда k делится на m и n, тогда $k = 0 \mod nm \implies \sigma$ - инъекция. Так как у нас одинаковое количество элементов в $\mathbb{Z}/nm\mathbb{Z}$ и $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ и σ - инъекция, каждый элемент слева получает уникальный справа, при этом каждый слева имеет связь, получается левое полностью покрывает правое, тогда это сюръекция и биекция соответственно. Если σ - биекция, то мы уже ранее доказывали, что σ - изоморфизм.

16 Количество элементов в произведении колец. Обратимые элементы в произведении колец. Мультипликативность функции Эйлера.

16.1 Произведение колец

Определение: R, S - кольца, тогда $R \times S = \{(r, s) : r \in R, s \in S\}$ с операциями:

1. сложение: $(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$

2. умножение: $(r_1, s_1) \cdot (r_2, s_2) = (r_1 r_2, s_1 s_2)$

Докажем, что это кольцо:

1. Ассоциативность сложения:
$(r_1, s_1) + ((r_2, s_2) + (r_3, s_3)) = (r_1, s_1) + (r_2 + r_3, s_2 + s_3) = (r_1 + r_2 + r_3, s_1 + s_2 + s_3) = (r_1 + r_2, s_1 + s_2) + (r_3 + s_3) = ((r_1, s_1) + (r_2, s_2)) + (r_3, s_3)$

2. Существование нейтрального элемента:
$(r_1, s_1) + (0_R, 0_S) = (r_1, s_1) \implies (0_R, 0_S)$ - нейтральный элемент по сложению.

3. Существование обратных по сложению:
$\forall r \in R, s \in S, -r, -s$ - обратные по сложению, тогда $(r, s) + (-r, -s) = (0_R, 0_S)$.

4. Ассоциативность умножения:
$((r_1, s_1) \cdot (r_2, s_2)) \cdot (r_3, s_3) = (r_1 \cdot r_2 \cdot r_3, s_1 \cdot s_2 \cdot s_3) = (r_1, s_1) \cdot ((r_2, s_2) \cdot (r_3, s_3))$

5. Дистрибутивность:
$(r_1, s_1) \cdot ((r_2, s_2) + (r_3, s_3)) = (r_1, s_1) \cdot (r_2 + r_3, s_2 + s_3) = (r_1 r_2 + r_1 r_3, s_1 s_2 + s_1 s_3) = (r_1 r_2, s_1 s_2) + (r_1 r_3, s_1 s_3) = (r_1, s_1) \cdot (r_2, s_2) + (r_1, s_1) \cdot (r_3, s_3)$

Доказали все аксиомы кольца, значит это кольцо.

16.2 Количество элементов в произведении колец

Утверждение: R, S - конечные кольца, тогда $|R \times S| = |R| \cdot |S|$
Доказательство: допустим зафиксируем $r \in R$, тогда пар (r, s_i) будет $|S|$, и всего таких возможных пар с разными r будет $|R| \cdot |S|$.

16.3 Обратимые элементы в произведении колец

Утверждение: R, S - кольца, тогда $(R \times S)^\times = R^\times \times S^\times$
Доказательство:

1. правое включение:
   $(r, s) \in R^\times \times S^\times \implies (r, s)^{-1} = (r^{-1}, s^{-1})$

2. левое включение:
   $(r, s) \in (R \times S)^\times \implies (t, u) \in R \times S : (r, s) \cdot (t, u) = (1, 1) \implies (rt, su) = (1, 1) \implies r, s$ - обратимы.

16.4 Функция эйлера

Определение: $\varphi : \mathbb{N} \to \mathbb{N}$, $\varphi(n) = |\{k : 1 \leq k \leq n, gcd(k, n) = 1\}$, такая функция считает сколько взаимно простых элементов с n, которые меньше n.

16.5 Мультипликативность функции Эйлера

Утверждение: Пусть $gcd(m, n) = 1$, тогда $\varphi(mn) = \varphi(m) \cdot \varphi(n)$
Доказательство: так как в кольце вычетов $\mathbb{Z}/n\mathbb{Z}$ элемент k обратим только когда $gcd(k, n) = 1$, мы можем сказать, что $|(\mathbb{Z}/n\mathbb{Z})^\times| \cong \varphi(n)$. Теперь мы можем сказать, что $\varphi(mn) = |(\mathbb{Z}/mn\mathbb{Z})^\times| \overset{\text{КТО}}{=} |(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^\times| = |(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times| = |(\mathbb{Z}/m\mathbb{Z})^\times| \cdot |(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(m) \cdot \varphi(n)$

17 Вычисление функции Эйлера. Теорема Эйлера.

17.1 Вычисление функции Эйлера

$\varphi(n) = \varphi(\prod p_i^k) = \prod \varphi(p_i^k)$, теперь нам надо понять как быстро считать $\varphi(p^k)$: $\varphi(p) = p - 1$ $\varphi(p^2) = p^2 - \frac{p^2}{p}$, здесь такая логика, всего у нас элементов p^2, мы можем мысленно разделить их на p блоков по p элементов так, что у нас в каждом блоке только последний будет делиться на p, например тут это $p, 2p \dots p^k$, их будет столько же, сколько у нас блоков, а их $\frac{p^2}{p}$. В общем случае это $\varphi(p^k) = p^k - \frac{p^k}{p} = p^k - p^{k-1} = p^{k-1} \cdot (p - 1)$.

17.2 Теорема Эйлера

Утверждение: если $gcd(a, n) = 1$, то $a^{\varphi(n)} = 1 \mod n$
Доказательство: пусть у нас есть множество взаимно простых с n $\{r_1, r_2, \dots r_{\varphi(n)}\}$, все эти числа обратимы в $\mathbb{Z}/n\mathbb{Z}$, домножим каждый такой элемент на a, скажем, что у нас количество элементов осталось прежним, так как если $ar_i = ar_j$, то мы можем сократить на a, потому что оно обратимо по модулю n, тогда $r_i = r_j \implies i = j$. $r_1 \cdot r_2 \cdot \dots \cdot r_{\varphi(n)} = ar_1 \cdot ar_2 \cdot \dots \cdot ar_{\varphi(n)} \mod n \implies r_1 \cdot r_2 \cdot \dots \cdot r_{\varphi(n)} = a^{\varphi(n)} \cdot (r_1 \cdot r_2 \cdot \dots \cdot r_{\varphi(n)}) \mod n$, Так как у нас произведение элементов r состоит из обратимых элементов мы можем сократить на него, тогда $a^{\varphi(n)} = 1 \mod n$.

18 Построение кольца многочленов над полем, деление с остатком. Деление на двучлен. Теорема Безу. Следствие о количестве различных корней многочлена.

18.1 Кольцо многочленов

Определение: $R[x] = \{(r_1, r_2, \dots, r_n, 0, 0 \dots) : r_i \in R \wedge \exists n\}$ - кольцо многочленов. $(r_1, r_2, \dots, r_n, 0, 0, \dots)$ - финитная последовательность, пусть $e_i \in R[x] = (0, 0, 0, \dots, 1, 0, \dots)$, где единица стоит на i-том месте. Тогда $r \cdot e_i = (0, 0, 0, \dots, r, 0, \dots)$, $e_i \cdot e_j = e_{i+j}$. Также мы можем сложить две такие последовательности: $a, b \in R[x]$, $m > n$, $(a_0, a_1, \dots, a_n, 0, \dots) + (b_0, b_1, \dots, b_m, \dots) = (a_0 + b_0, a_1 + b_1, \dots, a_n + b_n, \dots, b_m, 0, \dots)$. Тогда мы также можем разложить нашу последовательность: $(r_0, r_1, \dots, r_n, 0, \dots) = (r_0, 0, \dots) + (0, r_1, 0, \dots) + (0, 0, \dots, r_n, 0, \dots)$, что то же самое, что и $r_0 \cdot e_0 + r_1 \cdot e_1 + \dots + \dots + r_n \cdot e_n$. Обозначим e_0 как 1, e_1 как x, $e_k = e_1 \cdot e_1 \cdot e_1 \cdot \dots \cdot e_1 = x^k$. Тогда мы можем сказать, что $R[x] = \{r_0 + r_1 x + \dots + r_n x^n : r_i \in R \wedge \exists n\}$.

18.2 Поле

Определение: кольцо R называется полем, если $\forall r \neq 0 \in R$ существует $r^{-1} : r \cdot r^{-1} = 1$

18.3 Кольцо многочленов над полем

Утверждение: $(k[x])^\times = k^\times = k \setminus \{0\}$
Доказательство: $\deg p(x)$ - номер последнего ненулевого элемента последовательности $p(x) \in k[x]$ пусть также $\exists q(x) \in k[x] : p(x) \cdot q(x) = 1 = 1 + 0x + 0x^2 \dots$ $(p_0 + p_1 x + \dots + p_n x^n) \cdot (q_0 + q_1 x + \dots + q_m x^m) = \dots + p_n q_m x^{n+m} = 1$ У нас два варианта: либо $p_n q_m = 0$, но они оба не ноль по условию, а делителей нуля не существует в поле k. Тогда $n + m = 0$, в таком случае $n = m = 0$, тогда $p(x) = p_0 \in k$ и $q(x) = q_0 \in k$.

Утверждение: $k[x]$ - область целостности
Доказательство: $p(x), q(x) \in k[x], p(x) \neq 0, q(x) \neq 0$, $\deg(pq) = deg(p) + deg(q)$. $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x)) = 0 \implies \deg(p(x)) = \deg(q(x)) = 0$ $p_0 \cdot q_0 = 0$, но в k нет делителей нуля - противоречие.

Утверждение: $k[x]$ - евклидова область.
Доказательство: $k[x]$ - область целостности из прошлого доказательства. Теперь нам надо доказать существование функции N. $N(p) = \deg p$ $\forall p \in k[x], p \neq 0$, проверим свойства нормы:

1. $N(p(x)q(x)) \geq N(p(x))$, равенство только когда $q(x)$ - обратим
2. Покажем, что $\forall f(x), g(x) \in k[x], g(x) \neq 0$ $\exists! q(x), r(x) \in k[x]$, так что: $f(x) = g(x) \cdot q(x) + r(x)$: либо $r(x) = 0$, либо $N(r(x)) < N(g(x))$ или $\deg r < \deg g$

Рассмотрим два случая деления многочленов с остатком:
1 случай:
$\deg f < \deg g$, то $q(x) = 0, r(x) = f(x)$, тогда $f(x) = 0 \cdot g(x) + f(x)$, пример: $x = 0 \cdot x^2 + x$
2 случай:

Пусть $\deg f(x) \geq g(x)$, $f(x) = a_n x^n + \cdots + a_0, g(x) = b_m x^m + \cdots + b_0, n \geq m$.
тогда: $f_1(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x), \deg f_1(x) < n$
$f_2(x) = f_1(x) - ?g(x)$, если подставить $f_1(x)$, то $f_2(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x) - ?x^? g(x)$, можно выносить $g(x)$ за скобки
...
$f_k(x) = f(x) - (?)g(x)$ до тех пор, пока $\deg f_k < \deg g$, тогда $f_k(x) = 0 \cdot g(x) + f_k(x)$
Получается: $f(x) = (?)g(x) + f_k(x)$, тогда у нас два варианта: $f_k = 0$ либо $\deg f_k < \deg g$
Также докажем единственность такого деления:
Пусть существуют $q_1, q_2, r_1, r_2 \in k[x] : f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$
$g(q_1 - q_2) = r_2 - r_1$, Пусть $r_2 - r_1 \neq 0, r_1 \neq 0, \deg r_1 > \deg r_2$, тогда $\deg((q_1 - q_2)g) = \deg(q_1 - q_2) + \deg g > \deg(r_1) \geq (r_2 - r_1)$, но у нас $\deg((q_1 - q_2)g) = \deg(r_1 - r_2)$, получаем противоречие. Тогда $r_1 - r_2 = 0 \implies r_1 = r_2$. Получается, что $(q_1 - q_2) = 0 \implies q_1 = q_2$.

18.4 Деление на двучлен

Пусть мы хотим разделить $f(x)$ на $g(x) = (x - a)$ $f(x) = q(x)(x - a) + r(x)$, стоит заметить, что в данном случае $r(x)$ это просто $r \in k$, так как либо он ноль, либо его степень меньше 1, а значит это тоже константа.

18.5 Теорема Безу

Теорема: при делении $f(x)$ на $g(x) = x - a$ $r(x) = f(a)$
Доказательство: $f(x) = q(x)(x - a) + r(x)$, $f(a) = q(x) \cdot 0 + r(x) \implies f(a) = r(x)$

18.6 Первое следствие:

$\exists \alpha : f(\alpha) = 0$, тогда $f(x) = q(x)(x - \alpha)$, то есть $f(x)$ делится на $(x - \alpha)$

18.7 Второе следствие:

Утверждение: Пусть $\deg f = n$, тогда количество различных корней $f(x) \leq n$.
Доказательство: Пусть $a_1, a_2, \ldots a_n$ - корни $f(x)$, тогда $f(x) = g(x)(x - a_1)$, подставим a_2: $f(a_2) = g(a_2)(a_2 - a_1) = 0 \implies g(a_2) = 0$, тогда по первому следствию $g(x)$ можно дальше разложить так, чтобы $f(x) = g(x)(x - a_1)(x - a_2)$. таким образом мы можем разложить все корни так, что deg такого разложения будет равен количеству корней + степени оставшегося $g(x)$, что меньше чем исходный n, так как у нас при разложении всегда уменьшается степень $g(x)$.

19 Теорема о формальном и функциональном равенстве многочленов. Антипример для конечного поля.

19.1 Характеристика

Определение: Пусть R - кольцо, Характеристика R ($char\ R$) - это наименьшее натуральное n, такое что сумма n единиц равняется нулю. Если такого n не существует, то $char\ R = 0$. Из этого следует, что R - бесконечно.

19.2 Формальное и функциональное равенство многочленов

Определение: $f(x), g(x) \in k[x]$. Они равны формально, если просто равны в кольце многочленов. И равны функционально, если $\forall c \in k\ f(c) = g(c)$.
Теорема: из функционального равенства следует формальное, если $char\ k = 0$
Доказательство: Возьмем $h(x) = f(x) - g(x) \in k[x]$, если у нас не формально равны, то $h \neq 0$, тогда допустим $\deg h = n$. Но тогда h имеет бесконечное количество различных корней, хотя по следствию из теоремы безу он имеет только не больше n различных корней - противоречие, значит $f(x) = g(x)$
Антипример: если мы берем конечное поле, например $\mathbb{Z}/p\mathbb{Z}$, то в случае например многочленов $f(x) = x^p$ и $g(x) = x$ у нас они совпадают функционально, так как по малой теореме ферма $a^{p-1} = 1 \mod p \implies a^p = a \mod p$, но при этом формально они отличаются.

20 Сумма, произведение и пересечение идеалов. Проверка. Связь произведения и пересечения в общем случае и в случае взаимно простых (комаксимальных) идеалов.

20.1 Сумма идеалов

Определение: R - кольцо, I, J - идеалы в R, тогда $I + J = \{i + j : i \in I, j \in J\}$
Утверждение: $I + J$ - идеал.
Доказательство:

1. $(i_1 + j_1) + (i_2 + j_2) = (i_1 + i_2) + (j_1 + j_2) \in I + J$
2. $r \in R$, $r(i_1 + j_1) = ri_1 + rj_1 \in I + J$

Пример: в $\mathbb{Z}$ сложим $12\mathbb{Z} + 18\mathbb{Z} = \{18m + 12n\}_{n,m\in\mathbb{Z}} = 6\mathbb{Z}$ ($gcd(12, 18)$) так работает для всех целых чисел

20.2 Пересечение Идеалов

Определение: $I \cap J$ - пересечение идеалов
Утверждение: $I \cap J$ - идеал
Доказательство: пусть $a, b \in I \cap J$

1. $a+b \in I, a+b \in J \implies a+b \in I \cap J$
2. $r \in R$, $ra \in I, ra \in J \implies ra \in I \cap J$

Пример: $R = \mathbb{Z}$, $I = 12\mathbb{Z}, J = 18\mathbb{Z}$, тогда $I \cap J = 36\mathbb{Z}$ или же Нок(12, 18)

20.3 Умножение идеалов

Определение: $I \cdot J = \{\sum\limits_{k=1} i_k j_k : i_k \in I, j_k \in J\}$
Утверждение: $I \cdot J$ - идеал
Доказательство:

1. $\sum\limits_k i_k j_k + \sum\limits_s i'_s j'_s \in I \cdot J$
2. $r \in R$ $r\sum\limits_k i_k j_k = \sum\limits_k (ri_k) \cdot j_k \in I \cdot J$

Пример: $I \cdot J = \{\sum\limits_k 12a_k \cdot 18b_k\} = \{216\sum\limits_k a_k b_k\} = 216\mathbb{Z}$

20.4 Взаимная простота идеалов

Определение: I, J - взаимнопросты, если $I + J = R \iff 1 \in I + J$

20.5 Связь умножения и пересечения

Лемма: 1)$I \cdot J \subset I \cap J$ и если I, J - взаимно просты, то 2)$I \cap J = I \cdot J$
Доказательство:

1. Пусть $\sum\limits_k i_k j_k \in I \cdot J$, тогда $i_k j_k \in I \implies \sum\limits_k i_k j_k \in I$, аналогично для J, тогда сумма лежит в пересечении $I \cap J$
2. Пусть $a \in I \cap J$, так как I, J - взаимно просты, $\exists i \in I, j \in J : 1 = j + i \implies a = ai + aj$, тогда пусть $a \in J$ для i и $a \in I$ для j, тогда a - сумма элементов $i_k j_k$, а значит она лежит в $I \cdot J$

21 Китайская теорема об остатках для колец.

21.1 Теорема:

I, J - взаимно простые идеалы в кольце R, тогда $R/I \cdot J \cong R/I \times R/J$
Доказательство: $\varphi : R \to R/I \times R/J$ - гомоморфизм
$r \mapsto ([r]_I, [r]_J)$
$Im\ \varphi$: Докажем, что φ - сюръекция.
т.к I, J - взаимно простые, $1 \in I + J$ или $\exists i \in I, j \in J : 1 = i + j$
$\varphi(i) = ([i]_I, [i]_J) = (0, [1-j]_J) = (0, 1)$
$\varphi(j) = ([1-i]_I, [j]_J) = (1, 0)$
Пусть $([r]_I, [r]_J) = \varphi(rj + si) \implies Im\ \varphi = R/I \times R/J$
$\ker\varphi$: $r \in \ker\varphi$, $\varphi(r) = ([r]_I, [r]_j) = (0, 0) \iff r \in I \wedge r \in J \iff r \in I \cap J$, но так как I, J - взаимно просты $I \cap J = I \cdot J$

Получается $\ker\varphi = I \cdot J$.
Тогда по теореме об изоморфизме:
$\varphi : R/\ker\varphi \xrightarrow{\cong} Im\ \varphi$, что то же самое, что $\varphi : R/I \cdot J \xrightarrow{\cong} R/I \times R/J$, что и требовалось доказать.

21.2 Более общая формулировка

Теорема: Пусть R - кольцо с идеалами $I_1, I_2, \ldots, I_n$, все попарно взаимно просты, тогда $R/I_1 \cdot \cdots \cdot I_n \cong R/I_1 \times \cdots \times R/I_n$
Доказательство: Берем просто пару идеалов $I = I_1$ и $J = I_2 \cdot \cdots \cdot I_n$, доказываем как для двух идеалов. Но нужно показать, что I, J - взаимно простые. Сделаем линейные комбинации для I_1 и каждого другого идеала, затем перемножим их, тогда получится $1 = (i_1 + y_2)(i_2 + y_3)\ldots(i_{n-1} + y_n) = y_2 y_3 \ldots y_n +$ какой то элемент из идеала I, тут y_i - элемент I_i идеала. Тогда мы составили линейную комбинацию для I и J.

22 Формула Тейлора для многочлена. Критерий кратности корня.

22.1 Формула Тейлора для многочлена

$f(x) \in k[x], f(x) = a_0 + a_1 x + \cdots + a_n x^n$, $x = y + c, y = x - c$, $f(x) = a_0 + a_1(y + c) + a_2(y + c)^2 + \cdots + a_n(y + c)^n$. Пусть такой $f(x) = b_0 + b_1 y + \cdots + b_n y^n$, тогда $f(x) = b_0 + b_1(x - c) + b_2(x - c)^2 + \cdots + b_n(x - c)^n$
Определение: $f'(x)$ - производная многочлена $f(x) \in k[x]$, если для $f(x) = a_0 + a_1 x + \ldots a_n x^n$, $f'(x) = a_1 + 2a_2 x + 3a_3 x^2 + \cdots + n a_n x^{n-1}$
Утверждение: $b_m = \frac{f^{(m)}(c)}{m!}$, если $char\ k = 0$
Доказательство: $f(x) = b_0 + b_1(x - c) + \cdots + b_m(x - c)^m + \cdots + b_n(x - c)^n$, если мы возьмем производную m раз, то все члены до $(x - c)^m$ занулятся, а $f^{(m)}(x) = m! \cdot b_m + ?(x - c)$, тогда при подстановке $f^{(m)}(c) = m! \cdot b_m \implies b_m = \frac{f^{(m)}(c)}{m!}$

22.2 Критерий кратности корня

Определение: $p(x) \neq 0 \in k[z]$, элемент $\alpha \in k$ называется корнем кратности $m \neq 1$, если $p(x) = (x - \alpha)^m \cdot g(x)$, где $g(\alpha) \neq 0$
Определение: корень α называют кратным, если α кратности ≥ 2
Утверждение: α - кратный корень $p(x) \iff p(\alpha) = 0$ и $p'(\alpha) = 0$
Доказательство:

1. Достаточность: α - кратный корень $p(x) \implies p(x) = (x - \alpha)^2 \cdot h(x)$
   $p(\alpha) = 0$
   $p'(x) = 2(x - \alpha) \cdot h(x) + (x - \alpha)^2 \cdot h'(x) \implies p'(\alpha) = 0$

2. Необходимость: $p(\alpha) = 0, p'(\alpha) = 0$
   По теореме Безу: $p(x) = (x - \alpha)s(x)$, $p'(x) = s(x) + (x - \alpha) \cdot s'(x)$, но так как $p'(\alpha) = 0 \implies s(\alpha) = 0$, тогда снова по теореме безу: $s(x) = (x - \alpha) \cdot h(x)$, тогда $p(x) = (x - \alpha)^2 \cdot h(x) \implies \alpha$ - корень кратности ≥ 2.

Утверждение: $p(x) \neq 0 \in k[x]$, α - корень кратности $m \iff f(\alpha) = 0, f'(\alpha) = 0, \ldots f^{(m-1)}(\alpha) = 0$ и $f^{(m)}(\alpha) \neq 0$

23 Количество корней с кратностями не больше степени многочлена.

Теорема: $p(x) \neq 0 \in k[x], \alpha_1, \ldots, \alpha_n$ - различные корни кратности $l_1, \ldots, l_n$ соответственно. Тогда $p(x) = (x-\alpha_1)^{l_1} \cdot (x-\alpha_2)^{l_2} \cdot \cdots \cdot (x-\alpha_n)^{l_n} \cdot g(x), g(\alpha) \neq 0$
Доказательство: Так как $k[x]$ - евклидова область, это ОГИ, значит работает разложение на неприводимые, пусть $p(x) = u_1(x) \cdot \cdots \cdot u_n(x)$ - разложение на неприводимые. Пусть $\alpha_1, \ldots, \alpha_n$ - наши корни кратности $l_1, \ldots, l_n$ соответственно, тогда каждый двучлен вида $(x-\alpha_i)$ забирает ровно l_i элементов u_i. Тогда наш многочлен выглядит так: $p(x) = (x-\alpha_1)^{l_1} \cdot \ldots (x-\alpha_n)^{l_n} \cdot h(x)$, где $h(\alpha_i) \neq 0 \forall i$.
Следствие: $l_1 + l_2 + \cdots + l_n \leq \deg p(x)$

24 Интерполяционная формула Лагранжа, единственность.

24.1 Интерполяционная формула Лагранжа

Если мы хотим, чтобы наша кривая проходила через определенные точки $y_0, y_1, \ldots, y_n \in k$, то мы можем построить многочлен $f(x) \in k[x] : \deg f \leq n, f(x_i) = y_i$. $f(x) = \sum\limits_{i=0}^{n} y_i l_i(x)$, где $l_i(x_j) \in k[x]$ - такой многочлен, который равен одному если $i = j$, то есть в этой точке мы должны подняться на y_i вверх, иначе этот многочлен дает 0. $l_i(x) = \frac{(x-x_0)(x-x_1)\ldots(x-x_{i-1})(x-x_{i+1})\ldots(x-x_n)}{(x_i-x_0)(x_i-x_1)\ldots(x_i-x_{i-1})(x_i-x_{i+1})\ldots(x_i-x_n)}$, тогда $f(x_j) = \sum\limits_{i=0}^{n} y_i \cdot l_i(x_j) = y_j$

24.2 Единственность

Пусть $h(x) = f(x) - g(x)$, где $f(x), g(x)$ - решают задачу интерполяции, тогда $h(x)$ будет иметь $n+1$ корень при условии $\deg h \leq n$, что противоречит теореме безу, значит $h(x) = 0 \implies f(x) = g(x)$.

25 Критерий максимальности идеала. Критерий простоты идеала.

25.1 Критерий простоты идеала

Теорема: $I \lhd R$ - простой $\iff$ R/I - область целостности
Доказательство:

1. Достаточность:
   $[a] \cdot [b] = 0$ в $R/I \implies [a \cdot b] = 0 \implies ab \in I \implies \left[\begin{array}{l} a \in I \\ b \in I \end{array}\right.$
   Получается, если $ab = 0$, то либо $a = 0$, либо $b = 0 \implies R/I$ - область целостности

2. Необходимость:
   $ab \in I \implies [ab] = [a][b] = 0 \implies \left[\begin{array}{l} [a] = 0 \\ [b] = 0 \end{array}\right. \implies \left[\begin{array}{l} a \in I \\ b \in I \end{array}\right.$

25.2 Критерий максимальности идеала

Теорема: $I \lhd R$ - максимален $\iff$ R/I - поле
Доказательство:

1. Достаточность:
   Пусть $[a] \in R/I$ и $[a] \neq 0$, мы хотим найти $[a]^{-1}$. $[a] \neq 0 \implies a \notin I$, введем идеал $J = I + (a), I \subsetneqq J \implies J = R \implies 1 \in J \implies 1 \in I + (a) \implies 1 = i + ra \implies [1] = [ra] = [r][a] \implies [r] = [a]^{-1} \implies R/I$ - поле

2. Необходимость:
   $I \subsetneqq J$, мы хотим показать, что $R = J$. Пусть $x \in J \setminus I \implies [x] \neq 0$. Введем $y : [x][y] = 1 \implies [xy] = 1 \implies [xy - 1] = 0 \implies xy - 1 = i \in I \implies 1 = xy - i$, где $xy \in J, i \in J \implies 1 \in J \implies J = R$

26 Квадратичные вычеты и невычеты. Символ Лежандра. Формула для символа Лежандра. Мультипликативность. Подсчет $\left(\frac{-1}{p}\right)$.

26.1 Квадратичные вычеты и невычеты

Пусть мы хотим определить имеет ли уравнение $x^2 = a$ в поле $\mathbb{Z}/p\mathbb{Z}, a \neq 0, p \notin 2\mathbb{Z}$. Если такой x существует, то $x^{p-1} = 1$ по малой теореме Ферма.
$1 = x^{p-1} = (x^2)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}}$
$(\mathbb{Z}/p\mathbb{Z})^\times = (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$ является циклической группой по умножению:
$\exists \gamma \in (\mathbb{Z}/p\mathbb{Z}) : \forall b \in (\mathbb{Z}/p\mathbb{Z})^\times \exists k \in \mathbb{N} \cup \{0\} : b = \gamma^k$
$\gamma^{p-1} = 1$ и $\gamma^m \neq 1 \forall m \in [1, p-2]$
Пусть $a^{\frac{p-1}{2}} = 1$ и $\exists k : a = \gamma^k$, $a^{\frac{p-1}{2}} = 1 = \gamma^{k\frac{p-1}{2}} \implies \frac{p-1}{2}k \vdots p-1 \iff \frac{k}{2} \in \mathbb{Z} \iff k \in 2\mathbb{Z}$. Пусть $k = 2n$, тогда если $x = \gamma^n$, то $x^2 = \gamma^{2n} = \gamma^k = a$
$a^{\frac{p-1}{2}}$ - решение $x^2 = 1$, т.к мы находимся в поле, то у этого уравнения не больше двух решений по теореме безу, оба решения мы знаем: $x = 1, x = -1$
Утверждение: уравнение $x^2 = a$, где $a \neq 0$ имеет решения в $\mathbb{Z}/p\mathbb{Z} \iff a^{\frac{p-1}{2}} = 1$, иначе $a^{\frac{p-1}{2}} = -1$

26.2 Символ Лежандра. Формула для символа Лежандра. Мультипликативность

Определение: символом Лежандра $\left(\frac{a}{p}\right)$ называется функция $(\mathbb{Z}/p\mathbb{Z})^\times \to \{1, -1\}$:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, x^2 = a \text{ имеет решения} \\ -1, x^2 = a \text{ не имеет решений} \end{cases}$$

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$$

Свойства:

1. $\left(\frac{a^2}{p}\right) = 1$
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ - мультипликативность

26.3 Подсчет $\left(\frac{-1}{p}\right)$

$x^2 = -1 \mod p$,

- если имеет решение, то $(-1)^{\frac{p-1}{2}} = 1 \iff \frac{p-1}{2} \in 2\mathbb{Z} \iff p-1 \in 4\mathbb{Z} \iff p = 1 \mod 4$
- если не имеет решения, то $(-1)^{\frac{p-1}{2}} = -1 \iff \frac{p-1}{2} \notin 2\mathbb{Z} \iff \frac{p-1}{2} = 2m+1, m \in Z \iff p-1 = 4m+2 \iff p = 4m+3 \mod p \iff p = 3 \mod p$

$$\left(\frac{-1}{p}\right) - \begin{cases} 1, p = 1 \mod 4 \\ -1, p = 3 \mod 4 \end{cases}$$

27 Формула Гаусса для символа Лежандра (с доказательством). Вычисление $\left(\frac{2}{p}\right)$

27.1 Лемма:

$a \in (\mathbb{Z}/p\mathbb{Z})\,, p \notin 2\mathbb{Z}$. Рассмотрим $\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\}$ по модулю $p = \{r_1, r_2, \ldots, r_{p-1}\}, 1 < r_i < p-1$. Назовем такое множество S, пусть $L = |\{x \in S : x > \frac{p}{2}\}|$, тогда $\left(\frac{a}{p}\right) = (-1)^L$

Доказательство: $S = \{u_1, \ldots, u_L\} \cup \{v_{L+1}, \ldots, v_{\frac{p-1}{2}}\}$, где $\frac{p}{2} < u_i < p-1$ и $v_j < \frac{p}{2}$

Перемножим все элементы в S:

$\prod\limits_{s \in S} s \underset{p}{\equiv} a \cdot 2a \cdot 3a \cdot \cdots \cdot \frac{p-1}{2}a \underset{p}{\equiv} \left(\frac{p-1}{2}\right)! a^{\frac{p-1}{2}}$

Рассмотрим $\{p-u_1, p-u_2, \ldots, p-u_L\}, 1 \le p-u_i < \frac{p}{2}$

Лемма: все элементы $\{p-u, \ldots, p-u_L\} \cup \{v_{L+1}, \ldots, v_{\frac{p-1}{2}}\}$ попарно различны

Доказательство:

- 1 случай: $p-u_i = p-u_j \implies u_i = u_j \implies k_i a = k_j a \implies k_i = k_j \implies$ противоречие
- 2 случай: $v_i = v_j$ аналогично первому случаю
- 3 случай: $p-u_i = v_j \implies u_i + v_j \underset{p}{\equiv} 0 \implies k_i a + k_j a \underset{p}{\equiv} 0 \implies k_i + k_j \underset{p}{\equiv} 0$ но $k_i \in \left[1; \frac{p-1}{2}\right] \implies k_i + k_j \in [2, p-1]$

В $\{p-u_i, \ldots, p-u_L\} \cup \{v_{L+1}, \ldots, v_{\frac{p-1}{2}}\}$ все элементы $\in \left[1; \frac{p-1}{2}\right]$

Их $\frac{p-1}{2}$ штук и они все различны по нашей лемме, тогда они просто равны $\{1, 2, \ldots, \frac{p-1}{2}\}$

$$\prod_{r \in \{1, \ldots, \frac{p-1}{2}\}} r = \left(\tfrac{p-1}{2}\right)! = \prod_{i=1}^{L}(p-u_i) \prod_{j=L+1}^{\frac{p-1}{2}} v_j = (-1)^L \prod_{i=1}^{L} u_i \prod_{j=L+1}^{\frac{p-1}{2}} v_j = (-1)^L \prod_{s \in S} s = \left(\tfrac{p-1}{2}\right) a^{\frac{p-1}{2}} (-1)^L$$

$\left(\frac{p-1}{2}\right)! (-1)^L = \left(\frac{p-1}{2}\right)! a^{\frac{p-1}{2}}$, так как $\left(\frac{p-1}{2}\right)! \neq 0 \mod p$ на них можно сократить:

$$a^{\frac{p}{2}} = (-1)^L \implies \left(\frac{a}{p}\right) = (-1)^L$$

27.2 Вычисление $\left(\frac{2}{p}\right)$

$\{2, 4, 6, \ldots, p-1\} = S$
$L = \frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor$
$\left(\frac{2}{p}\right) = (-1)^L$
Пусть $p = 1 \mod 8 \iff p = 1 + 8t$
$L = 4t - 2t \in 2\mathbb{Z}$
Пусть $p = 3 \mod 8 \iff p = 3 + 8t$
$L = 1 + 4t - 2t \notin 2\mathbb{Z}$
Пусть $p = 5 \mod 8 \iff p = 5 + 8t$
$L = 2 + 4t - 2t - 1 \notin 2\mathbb{Z}$
Пусть $p = 7 \mod 8 \iff p = 7 + 8t$
$L = 3 + 4t - 1 - 2t \in 2\mathbb{Z}$
Можно подобрать функцию, которая ведет себя таким же образом: $\frac{p^2-1}{8}$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

28 Квадратичный закон взаимности*.

Формулировка:

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot \left(\frac{p}{q}\right), p \neq q$$

29 Теорема Гаусса. Теорема о мультипликативной группе поля.

29.1 Теорема Гаусса

Теорема:

$$n = \sum_{d|n, d \geq 1} \varphi(d), \forall n \geq 1$$

Доказательство:
$S = \{1, \ldots, n\} = \bigcup\limits_{d|n, d\geq 1} S_d$
$S_d = \{k \in S : \gcd(k, n) = d\}$, $S_d \cap S_{d'} \neq \varnothing \implies d = d'$
$|S_d| = |\left\{k \in S : \gcd\left(\frac{k}{d}, \frac{n}{d}\right) = 1\right\} = \varphi\left(\frac{n}{d}\right)$
$n = |S| = \sum\limits_{d|n, d\geq 1} |S_d| = \sum\limits_{d|n, d\geq 1} \varphi\left(\frac{n}{d}\right) = \sum\limits_{d|n, d\geq 1} \varphi(d)$

29.2 Теорема о мультипликативной группе поля

Теорема: пусть F - конечное поле, тогда $F^\times = F \setminus \{0\}$ - циклическая группа, то есть $\exists a \in F^\times : \forall g \in F^\times \exists k \in \mathbb{N} : g = a^k$
Доказательство: $G = F^\times, \psi(d) =$ количество элементов G порядка d

$$g \in G \text{ имеет порядок } d, \text{ если } g^d = 1, \text{ но } g^k \neq 1 \forall k \in [1; d-1]$$

Пусть мы нашли $h \in G$ порядка d, рассмотрим $\langle h \rangle = \{1, h, h^2, h^3, \ldots, h^{d-1}\}$ - сколько тут элементов порядка d?

$$h^k \in \langle h \rangle \text{ имеет порядок } d \iff \left(h^k\right)^m \text{ закрасит всю группу}$$

Когда $\left(h^k\right)^m = h$? $h^{km} = h^1 \iff km = 1 \mod d \iff \gcd(k, d) = 1$ Получается в $\langle h \rangle$ ровно $\varphi(d)$ элементов, которые имеют порядок d. Если мы находим хотя бы один элемент порядка d, то автоматически находим таких $\varphi(d)$ штук.
Любой элемент $\langle h \rangle$ удовлетворяет уравнению $x^d = 1$. Так как мы существуем в поле, у этого уравнения $\leq d$ различных решений, значит $\langle h \rangle$ - все решения $x^d = 1$.
Пусть t - элемент порядка d, тогда t решает $x^d = 1 \implies t \in \langle h \rangle$

$$\psi(d) = \left[\begin{array}{l} 0, \text{ если не нашли} \\ \varphi(d), \text{ иначе} \end{array}\right. \implies \psi(d) \leq \varphi(d)$$

$n = \sum\limits_{d|n} \psi(d) \leq \sum\limits_{d|n} \varphi(d) = n \implies \psi(d) = \varphi(d) \, \forall d|n$
Для $d = n \psi(n) = \varphi(n) \geq 1 \implies$ нашли хотя бы 1 элемент порядка n
Лемма: G - конечная группа, $|G| = n$, $\alpha \in G$, тогда $ord\ \alpha | n$
Доказательство: $C = \langle \alpha \rangle$, $|C| = ord\ \alpha$, $G = \bigcup\limits_{g \in G} gC$, это действительно равенство, т.к $\forall g \in G g \in gC$.

$$gC \cap g'C = \left[\begin{array}{l} \varnothing \\ gC = g'C \end{array}\right.$$

Пусть $z \in gC \cap g'C$
$z = gc_1 = g'c_2 \implies g = g'c_2c_1^{-1}$
Пусть $h \in gC \implies h = gc = g'c_2c_1^{-1}c \in g'C \implies gC \subset g'C$, аналогично можно доказать в обратную сторону, тогда $gC = g'C$
$n = |G| = |C \sqcup g_1C \sqcup g_2C \sqcup \cdots \sqcup g_kC| = |C| + |g_1C| + \cdots + |g_kC| = ord\ \alpha + ord\ \alpha + \cdots + ord\ \alpha = (k+1)\, ord\ \alpha \implies ord\ \alpha | n$

30 Критерий максимальности для идеалов в k[x]. Построение поля комплексных чисел. Алгебраическая запись.

30.1 Критерий максимальности для идеалов в k[x]

$k[x]$ - ОГИ
Утверждение: идеал (f) - максимален $\iff$ f - неприводим
Доказательство:

1. Достаточность:
   Пусть $f = g \cdot h$ и $\deg g \geq 1, \deg h \geq 1$, $(f) \nsubseteqq (g)$, так как $g \in (g)$ и $g \notin (f)$, но $(g) \notin R \implies (f)$ - не максимален, противоречие, следовательно f - неприводим.

2. Необходимость:
   Пусть $(f) \nsubseteqq J$, J - главный идеал $\implies J = (g)$

$$(f) \nsubseteqq (g) \implies g | f \implies \left[\begin{array}{l} g \equiv const \neq 0 \implies (g)\, k[x] \\ g \sim f \implies (f) = (g), \text{ но по условию не равны} \end{array}\right.$$

30.2 Построение поля комплексных чисел. Алгебраическая запись.

Возьмем кольцо многочленов и факторизуем его по неприводимому x^2+1, таким образом получается новое поле комплексных чисел, это действительно поле, так как идеал максимален.

$$R[x]/\left(x^2+1\right)=\mathbb{C}$$

$$\mathbb{C}=\{a+bx : a,b\in\mathbb{R}\}$$

И если заменить x на i то получим алгебраическую запись: $a+bi$

31 Классификация автоморфизмов $\mathbb{C}$ над $\mathbb{R}$, модуль комплексного числа. Его мультипликативность. Оценка суммы.

31.1 Классификация автоморфизмов $\mathbb{C}$ над $\mathbb{R}$

Определение: автоморфизмом $\mathbb{C}$ над $\mathbb{R}$ называется изоморфизм

$$\sigma:\mathbb{C}\to\mathbb{C}:\forall r\in\mathbb{R}\sigma(r)=r$$

Утверждение: существует два автоморфизма $\mathbb{C}$ над $\mathbb{R}$: $id,-$, $Gal(\mathbb{C}/\mathbb{R})\cong\mathbb{Z}/2\mathbb{Z}$
Доказательство: Пусть σ - автоморфизм $\mathbb{C}$ над $\mathbb{R}$
$\sigma(a+ib)=\sigma(a)+\sigma(i)\sigma(b)=a+\sigma(i)b$
$\sigma(i)^2=\sigma(i^2)=\sigma(-1)=-1$

$$\text{так как } \sigma(i) \text{ - решение } x^2=-1\sigma(i)=\left[\begin{array}{l} i \implies id \\ -i \end{array}\right.$$

$$\text{сопряжение } \overline{a+ib}:\sigma(a+ib)=a-ib$$

Свойство: $z\in\mathbb{C},\overline{z}=z \iff z\in\mathbb{R}$

31.2 Модуль комплексного числа. Его мультипликативность. Оценка суммы

Хотим построить отображение $\mathbb{C}\to\mathbb{R}$ $\frac{z+\overline{z}}{2}-\operatorname{Re}z$, вещественная часть
$\frac{z-\overline{z}}{2i}-\operatorname{Im}z$, мнимая часть
$\overline{z\cdot\overline{z}}=z\cdot\overline{z} \implies z\cdot\overline{z}\in\mathbb{R}$ $z\cdot\overline{z}=(a+ib)(a-ib)=a^2+b^2\geq 0$ $|z|=\sqrt{z\cdot\overline{z}}$
Свойства модуля:

1. $|z_1\cdot z_2|=\sqrt{z_1z_2\overline{z_1z_2}}=\sqrt{z_1\overline{z_1}}\cdot\sqrt{z_2\overline{z_2}}=|z_1|\cdot|z_2|$
2. $|z_1+z_2|\leq|z_1|+|z_2|$ - неравенство треугольника для векторов (a,b) и (c,d), если $z_1=a+ib, z_2=c+id$

32 Основная теорема алгебры*.

Теорема:

$$p(z) \in \mathbb{C}[z], \deg p \geq 1 \implies \exists z_0 \in \mathbb{C} : p(z_0) = 0$$

Следствие:

$$p \in \mathbb{C}[z], \deg p = n \implies p \text{ имеет ровно } n \text{ корней}$$

33 Эквивалентность трех определений базиса конечномерного векторного пространства.

Определение: $B \subset V$. Говорят, что B - базис, если B порождающее и линейно независимое.
Теорема: Следующие условия равносильны

1. B - базис
2. B - максимальное по включению линейно независимое множество
3. B - минимальное по включению порождающее множество

Доказательство:

- $1 \implies 2$
  Пусть B - базис, $v \in V$, тогда $v = \sum\limits_{i=1}^{n} \alpha_i e_i, e_i \in B$.
  Тогда $B \cup \{v\}$ - линейно зависимое $\implies$ B - максимальное по включению линейно независимое.

- $2 \implies 1$
  Нам надо показать, что B - порождающее.
  Пусть $v \in V \setminus B$, тогда $B \cup \{v\}$ -линейно зависимое $\implies \sum\limits_{i=1}^{n} \alpha_i e_i + \beta v = 0, e_i \in B$
  $\beta \neq 0$ так как B - линейно независимое, тогда $v = -\sum\limits_{i=1}^{n} \frac{\alpha_i}{\beta} e_i$

- $1 \implies 3$
  Пусть B - базис. Предположим, что $B \setminus \{e\}$ все еще порождающее. Тогда $e = \sum\limits_{i=1}^{n} \alpha_i e_i, e_i \in B \setminus \{e\}$, но B должно быть линейно независимым.

- $3 \implies 1$
  Покажем, что B - линейно независимое. Пусть $\sum\limits_{i=1}^{n} \alpha_i e_i = 0$, где $\exists \alpha_k \neq 0$, тогда

  $$e_k = -\sum_{i=1, i \neq k}^{n} \frac{\alpha_i}{\alpha_k} e_i$$

  Тогда $B \setminus \{e_k\}$ все еще порождающее.

34 Дополнение линейно независимого множества до базиса.

Пусть V - векторное пространство, S - линейное независимое множество, тогда $\exists B$ - базис, такой что $S \subset B$.
Доказательство: $A = \{$подмножества в V, которые содержат S и линейно независимые$\}$, $A \neq \varnothing$, т.к $S \in A$, A - частично упорядоченное множество по $\leq$: $x \leq x' \leq \ldots$
Рассмотрим произвольную цепочку C множества A: $x \leq x' \leq x'' \leq \ldots$, назовем $A_c = \bigcup\limits_{x \in C} X$, почему $A_c \in A$?

1. $\subseteq S$
2. пусть $\{e_1, \ldots, e_k\} \subset A_c$, тогда $\exists X \in C : \{e_1, \ldots, e_n\} \subset X$, но X - линейно независимое, тогда A_c тоже линейно независимое, тогда $A_c \in A$

Заметим, что $\forall X \in C X \subseteq A_c$
Лемма Цорна: если в частично упорядоченном множестве для любой цепочки есть верхняя граница, то существует максимальный элемент
По лемме Цорна существует $B \subset A_c$ - максимальный элемент, тогда $S \subseteq B$ и B максимальное по включению линейно независимое множество, которое содержит S, тогда оно вообще максимальное по включению линейно независимое, а значит является базисом

35 Лемма Стейница (лемма о подмене).

Лемма: V - векторное пространство. Пусть $S = \{w_1, \ldots, w_m\}$ - порождающее множество V, $L = \{v_1, \ldots, v_n\}$ - линейно независимое множество V.
Тогда:

1. $n \leq m$
2. после перенумерования S множество $\{v_1, v_2, \ldots, v_n, w_{n+1}, \ldots, w_m\}$ все еще порождающее.

Доказательство: по индукции по n
База: При $n = 0$ верно (ничего не меняем)
Переход: пусть для $n-1$ векторов уже знаем.
Перенумеруем S и заменим $n-1$ элементов, получим $S' = \{v_1, \ldots, v_{n-1}, w_n, w_{n+1}, \ldots, w_m\}$
Так как S' - порождающее множество, v_n можно выразить из его элементов.

$$v_n = \sum_{i=1}^{n-1} \alpha_i v_i + \sum_{i=n}^{m} \beta_i w_i$$

Мы хотим выразить w_n, чтобы заменить его на v_n

- 1 случай: $\beta_i = 0 \implies \sum\limits_{i=1}^{n-1} \alpha_i v_i - v_n = 0$, но это невозможно из-за того, что L - линейно независимое множество

- 2 случай: $\exists \beta_i \neq 0$, перенумеруем S' так, чтобы $\beta_n \neq 0$, тогда

$$w_n = \frac{v_n}{\beta_n} - \sum_{i=1}^{n-1} \frac{\alpha_i}{\beta_n} v_i - \sum_{i=n+1}^{m} \frac{\beta_i}{\beta_n} w_i$$

Рассмотрим множество $S'' = \{v_1, \ldots, v_{n-1}, w_{n+1}, \ldots, w_m\}$
Замечание: если $S' = \{v_1, \ldots, v_{n-1}\}$, то $v_n = \sum\limits_{i=1}^{n-1} \alpha_i v_i$, но L - линейно независимое.
Утверждаем, что S'' - порождающее. Так как S' - порождающее, $v \in V$

$$v = \sum_{i=1}^{n-1} \alpha_i v_i + \gamma_n w_n + \sum_{i=n+1}^{m} \gamma_i w_i$$

Теперь мы можем подставить вместо w_n наше выражение из второго случая, таким образом любой вектор выражается из элементов множества $S'' \implies S''$ - порождающее

36 Корректность размерности: любые два базиса конечномерного векторного пространства имеют одинаковую мощность.

Определение: пусть для векторного пространства V существует конечный базис B, тогда назовем $\dim V = |B|$ - размерность V
Утверждение: Определение размерности корректно
Доказательство: B, B' - базисы V и B - конечный
B - порождающий и B' линейно независимый $\implies$ $\forall$ конечного подмножества B' линейно независимо, пусть $S \subset B'$ - конечное подмножество, тогда $|S| \leq |B| \forall S \subset B'$
Тогда $|B'| \leq |B|$, теперь скажем, что B - линейно независимый и B' - порождающий, тогда $|B| \leq |B'| \implies |B| = |B'|$

37 Формула Грассмана. Антипример. Критерий прямой суммы.

37.1 Формула Грассмана

Теорема: если $V = U + W$, где все конечномерны, то

$$\dim(U + W) = \dim U + \dim W - \dim(U \cap W)$$

Доказательство: пусть $\{e_1, \ldots, e_k\}$ - базис $U \cap W$, т.к $U \cap W \subset U$, базис $U \cap W$ можно расширить до базиса U - $\{e_1, \ldots, e_k, u_1, \ldots, u_m\}$. Аналогично для W - $\{e_1, \ldots, e_k, w_1, \ldots, w_n\}$, тогда $\{e_1, \ldots, e_k, u_1, \ldots, u_m, w_1, \ldots, w_n\}$ - базис $U + W$

- порождаемость: пусть $u + w \in U + W, u = \sum \alpha_i e_i + \sum \beta_i u_i, w = \sum \mu_i e_i + \sum \gamma_i w_i \implies u + w = \sum (\mu_i + \alpha_i) e_i + \sum \beta_i u_i + \sum \gamma_i w_i$

- линейная независимость: пусть

$$\sum \alpha_i e_i + \sum \beta_i u_i + \sum \gamma_i w_i = 0\,(*)$$

$$\sum \beta_i u_i = -\sum \alpha_i e_i - \sum \gamma_i w_i$$

$\sum \beta_i u_i \in U, -\sum \alpha_i e_i - \sum \gamma_i w_i \implies \sum \beta_i u_i \in U \cap W \implies \sum \beta_i u_i = \sum s_i e_i \implies$
$\sum \beta_i u_i - \sum s_i e_i = 0 \implies \beta_i = 0 \forall i = 1 \dots n$
$(*) \sum \alpha_i e_i + \sum \gamma_i w_i = 0 \implies \alpha_i = 0 \forall i = 1 \dots k, \gamma_i = 0 \forall i = 1 \dots n$

$$\dim(U+W) = k+n+m = (k+n)+(k+m)-k = \dim W + \dim U - \dim U \cap W$$

37.2 Антипример

Допустим у нас есть пространства в $\mathbb{R}^3$:
$U_1 = \langle x, y \rangle, U_2 = \langle x+z \rangle, U_3 = \langle z \rangle$,

$$\dim(U_1+U_2+U_3) = 3 \neq 2+1+1-0-0-0+0 = 4$$

37.3 Критерий прямой суммы

Определение: сумма векторных подпространств называется прямой, если $U \cap W = 0$

$$U \oplus W$$

Утверждение: сумма $V+W$ - прямая $\iff \forall v \in U+W \exists! u \in U \exists! w \in W : v = u+w$
Доказательство:

- Достаточность:
  $v = u_1 + w_1 = u_2 + w_2 \implies u_1 - u_2 \in U = w_1 - w_2 \in W, U \cap W = 0 \implies u_1 = u_2, w_1 = w_2$
- Необходимость:
  $v \in U \cap W, v = v+0 = 0+v$, где сначала $v \in U$, затем $v \in W$, тогда по единственности разложения $v = 0$

38 Теорема о размернорсти ядра и образа.

Теорема: $\mathcal{L} : V \to W$ - линейное отображение, тогда $\dim V = \dim \ker \mathcal{L} + \dim Im\ \mathcal{L}$
Доказательство: пусть $e_1, \dots, e_k$ - базис $\ker \mathcal{L}$ - линейно независимое в $V \implies$ мы можем расширить до $e_1, \dots e_k, e_{k+1}, \dots, e_n$ - базиса пространства V.
Покажем, что $\mathcal{L}(e_{k+1}), \dots, \mathcal{L}(e_n)$ - базис $Im\ \mathcal{L}$

- Порождаемость:
  пусть $w \in Im\ \mathcal{L} \implies \exists v \in V : w = \mathcal{L}(v)$, разложим v по базису V:
  $v = \sum\limits_{i=1}^{k} \alpha_i e_i + \sum\limits_{i=k+1}^{n} \alpha_i e_i$
  $w = \mathcal{L}(v) = \mathcal{L}\left(\sum\limits_{i=1}^{k} \alpha_i e_i + \sum\limits_{i=k+1}^{n} \alpha_i e_i\right) = \sum\limits_{i=1}^{k} \alpha_i \mathcal{L}(e_i) + \sum\limits_{i=k+1}^{n} \alpha_i \mathcal{L}(e_i) = \sum\limits_{i=k+1}^{n} \alpha_i \mathcal{L}(e_i)$,
  так как $e_1, \dots, e_k \in \ker \mathcal{L} \implies \mathcal{L}(e_i) = 0\ \forall i = 1, \dots, k$

- Линейная независимость:
  Пусть $\sum\limits_{i=k+1}^{n} \beta_i \mathcal{L}(e_i) = 0 = \mathcal{L}\left(\sum\limits_{i=k+1}^{n} \beta_i e_i\right) \implies \sum\limits_{i=k+1}^{n} \beta_i e_i \in \ker \mathcal{L}$, тогда распишем эту сумму по базису ядра: $\sum\limits_{i=k+1}^{n} \beta_i e_i = \sum\limits_{i=1}^{k} \gamma_i e_i \implies \sum\limits_{i=k+1}^{n} \beta_i e_i - \sum\limits_{i=1}^{k} \gamma_i e_i = 0 \implies \beta_i = 0 \ \forall i = k+1, \ldots, n, \gamma_i = 0 \ \forall i = 1, \ldots, k$, так как это базис V

$$\dim V = n = k + (n-k) = \dim \ker \mathcal{L} + \dim Im\ \mathcal{L}$$

39 Матрица линейного отображения. Изоморфизм $Hom(k^n, k^m) \cong M_{m\times n}(k)$. Матрица композиции операторов.

39.1 Матрица линейного отображения.

Определение: $\mathcal{L} : V \to W$ - линейное отображение, $e = (e_1, \ldots, e_n)$ - базис V, $f = (f_1, \ldots, f_m)$ - базис W

$[\mathcal{L}]_{e,f}$ - матрица линейного отображения $\mathcal{L}$ в базисах e и f

Нам достаточно определить только как отображение действует на базисных векторах: $\mathcal{L}(e_i)$ - какой то вектор в W, значит мы можем выразить его в базисе W
$\mathcal{L}e_1 = a_{11}f_1 + a_{21}f_2 + a_{31}f_3 + \cdots + a_{m1}f_m$
$\mathcal{L}e_2 = a_{12}f_1 + a_{22}f_2 + a_{32}f_3 + \cdots + a_{m2}f_m$
$\vdots$
$\mathcal{L}e_j = a_{1j}f_1 + a_{2j}f_2 + a_{3j}f_3 + \cdots + a_{mj}f_m$

$$[\mathcal{L}]_{e,f} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

39.2 Изоморфизм $Hom(k^n, k^m) \cong M_{m\times n}(k)$.

Введем такое отображение $\pi : Hom(k^n, k^m) \to M_{m\times n}(k)$. Так как $k^n \cong V, \dim V = n$ и $k^m \cong W, \dim W = m$, будем использовать векторные пространства V и W. Нам нужно доказать, что π - биекция и линейное отображение. Пусть $e_1, \ldots, e_n$ - базис V, $f_1, \ldots, f_m$ - базис W. Возьмем линейное отображение $\mathcal{L} \in Hom(V, W)$. Подействуем им на базис V и выразим результат через базис W: $\mathcal{L}e_j = \sum\limits_{i=1}^{m} a_{ij} f_i$. Наше отображение $\pi(\mathcal{L}) = (a_{ij}) \in M_{m\times n}$. Покажем, что π - линейное отображение:

1. $\mathcal{L} \in Hom(V, W), \mathcal{T} \in Hom(V, W)$
   Определим $\pi(\mathcal{L} + \mathcal{T}) = \pi(\mathcal{L}) + \pi(\mathcal{T})$ как просто поэлементное суммирование элементов двух матриц.

2. $\mathcal{L} \in Hom(V, W), \gamma \in k$
   Определим $\pi(\gamma\mathcal{L}) = \gamma\pi(\mathcal{L})$ как умножение каждого элемента матрицы на элемент из поля.

Теперь нам надо доказать биекцию.

- Инъекция
  пусть $\mathcal{L} \in \ker \pi$, тогда $\pi(\mathcal{L}) = 0$, тогда $\mathcal{L}e_i = 0 \ \forall i = 1, \ldots, n$, тогда $\mathcal{L}v = 0 \ \forall v \in V \implies \ker \pi = 0 \implies \pi$ - инъекция

- Сюръекция

  Возьмем любую матрицу A из $M_{m\times n}$. Пусть у нас есть $\mathcal{L}(e_j) = \sum\limits_{i=1}^{m} a_{ij} f_i$. По свойству базиса если мы можем отправить базис в область значений, то существует единственное такое линейное отображение. Тогда $\pi(\mathcal{L}) = A$

39.3 Матрица композиции операторов.

Мы можем определить эту операцию только когда $V = W$ в $Hom(V, W)$ Пусть у нас есть две матрицы:

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

$$B_{n\times k} = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1k} \\ b_{21} & b_{22} & \cdots & b_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nk} \end{pmatrix}$$

композиция в данном случае аналогична умножению матриц, когда мы берем строку из A и поэлементно умножаем на столбец из B, то есть наш элемент в AB задается следующим образом:

$$ab_{ik} = \sum_{j=1}^{n} a_{ij} b_{jk}$$

Новая матрица имеет размер $m \times k$

40 Замена базиса (в области определения и области значения). Канонический вид матрицы линейного отображения.

40.1 Замена базиса

$\mathcal{L} : V \to W$, e - базис V размерности n, f - базис W. Тогда построим матрицу

$$[\mathcal{L}]_{e,f} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{m1} & \alpha_{m2} & \cdots & \alpha_{mn} \end{pmatrix}$$

Теперь мы хотим например заменить базис e на базис r. Запишем матрицу перехода T_1, в которой i строка - разложение r_i базисного вектора по базисным векторам e.

$$T_1 = \begin{pmatrix} \gamma_{11} & \gamma_{12} & \cdots & \gamma_{1n} \\ \gamma_{21} & \gamma_{22} & \cdots & \gamma_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \gamma_{n1} & \gamma_{n2} & \cdots & \gamma_{nn} \end{pmatrix}$$

$$[\mathcal{L}]_{e,f} T_1 = [L]_{r,f}$$

Аналогично хотим заменить базис f на базис s

$$T_2 = \begin{pmatrix} \beta_{11} & \beta_{12} & \cdots & \beta_{1m} \\ \beta_{21} & \beta_{22} & \cdots & \beta_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{m1} & \beta_{m2} & \cdots & \beta_{mm} \end{pmatrix}$$

$$T_2 [\mathcal{L}]_{e,f} = [\mathcal{L}]_{e,s}$$

40.2 Канонический вид матрицы линейного отображения.

Теорема: $\mathcal{L} : V \to W$ - линейное отображение, Тогда $\exists$ базис $e_1, \ldots, e_n$ пространства V и базис $f_1, \ldots, f_m$ пространства W, такое что:

$$[\mathcal{L}]_{e,f} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & \ddots & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

Доказательство: пусть $e_{k+1}, \ldots, e_n$ - базис $\ker \mathcal{L}$ дополним этот базис до базиса V. $\mathcal{L}(e_1), \ldots, \mathcal{L}(e_k)$ - базис $Im\ \mathcal{L} = f_1, \ldots, f_k$, достроим до базиса W.
Теперь попытаемся построить матрицу:
$\mathcal{L}e_1 = 1f_1 + 0f_2 + \ldots$
$\mathcal{L}e_2 = 0f_1 + 1f_2 + 0f_3 + \ldots$
$\vdots$
$\mathcal{L}e_k = 0f_1 + 0f_2 + \cdots + 1f_k$
Дальше мы будем обращаться к базисным векторам из ядра, следовательно везде будут нули.

41 Универсальное свойство базиса.

V - векторное пространство, $e_1, \ldots, e_n$ - базис V, пусть $\mathcal{L} \in Hom(V, W)$.

$$\mathcal{L}(v) = \mathcal{L}\left(\sum_{i=1}^{n} \alpha_i e_i\right) = \sum_{i=1}^{n} \alpha_i L(e_i)$$

Утверждение: $\forall f(e_1, \ldots, e_n) \to W \ \exists!$ линейное отображение $\mathcal{L} : V \to W : \mathcal{L}(e_i) = f(e_i)$

Доказательство: $\mathcal{L}(v) = \mathcal{L}\left(\sum\limits_{i=1}^{n} \alpha_i e_i\right)$. Определим $\mathcal{L}(v)$ как $\sum\limits_{i=1}^{n} \alpha_i f(e_i)$, теперь покажем, что это линейное отображение.

1. $\mathcal{L}(v + \widetilde{v}) = \mathcal{L}\left(\sum\limits_{i=1}^{n} \alpha_i e_i + \sum\limits_{i=1}^{n} \widetilde{\alpha}_i e_i\right) = \mathcal{L}\left(\sum\limits_{i=1}^{n} (\alpha_i + \widetilde{\alpha}_i) e_i\right) = \sum\limits_{i=1}^{n} (\alpha_i + \widetilde{\alpha}_i) f(e_i) = \sum\limits_{i=1}^{n} \alpha_i f(e_i) + \sum\limits_{i=1}^{n} \widetilde{\alpha}_i f(e_i) = \mathcal{L}(v) + \mathcal{L}(\widetilde{v})$

2. $\mathcal{L}(\beta v) = \mathcal{L}\left(\beta \sum\limits_{i=1}^{n} \alpha_i e_i\right) = \mathcal{L}\left(\sum\limits_{i=1}^{n} \beta \alpha_i e_i\right) = \sum\limits_{i=1}^{n} \beta \alpha_i f(e_i) = \beta \sum\limits_{i=1}^{n} \alpha_i f(e_i) = \beta \mathcal{L}(v)$

Также покажем единственность такого отображения: пусть $\mathcal{L}$ и $\mathcal{T}$:
$\mathcal{L}(e_i) = f(i) \forall i = 1 \ldots n, \mathcal{T}(e_i) = f(i) \forall i = 1 \ldots n$

$$(\mathcal{L} - \mathcal{T})(v) = (\mathcal{L} - \mathcal{T}) \left(\sum_{i=1}^{n} \alpha_i e_i\right) = \sum_{i=1}^{n} \alpha_i f(e_i) - \sum_{i=1}^{n} \alpha_i f(e_i) = 0 \ \forall v \in V$$

42 Двойственный базис. Изоморфизм V и V^* для конечномерного V. Канонический изоморфизм V и V^{**} для конечномерного V.

42.1 Двойственный базис. Изоморфизм V и V^* для конечномерного V.

Определение: V - векторное пространство, $V^* = Hom(V, k)$ - пространство линейных функционалов или двойственное пространство.
Пусть $e_1, \ldots, e_n$ - базис V, тогда определим набор векторов $e_1^*, \ldots, e_n^* \in V^*$ следующим образом:

$$e_i^*(e_j) = \delta_{ij} = \begin{cases} 1, i = j \\ 0, i \neq j \end{cases}$$

Утверждение: $e_1^*, \ldots, e_n^* = e^*$ - базис V^*
Доказательство:

- порождаемость:
  Пусть $\varphi \in V^*$, мы хотим получить равенство $\varphi = \sum\limits_{i=1}^{n} \beta_i e_i^*$. Посмотрим как ведет себя выражение с обеих сторон на базисном векторе e_j: $\varphi(e_j) = \beta_j e_j^*(e_j) = \beta_j$, тогда можно утверждать, что $\varphi = \sum\limits_{i=1}^{n} \varphi(e_i) e_i^*$. Это просто два линейных функционала, они равны, если равны на всех базисных векторах. $\varphi(e_i) = \beta_i = \varphi(e_i) e_i^*(e_i) = \varphi(e_i)$

- линейная независимость:
  Пусть $\sum\limits_{i=1}^{n} \gamma_i e_i^* = 0$, подставим базисный вектор e_j: $\gamma_j e_j^*(e_j) = \gamma_j = 0 \ \forall j = 1, \ldots, n$

Из этого следует, что $V \cong V^*$

42.2 Канонический изоморфизм V и V^{**} для конечномерного V.

Теорема: пространства V и $(V^*)^*$ канонически изоморфны.

Доказательство: $V^{**} = Hom\left(Hom\left(V,k\right),k\right) \overset{!}{\cong} V$ - мы хотим построить такой изоморфизм.
Построим $\zeta : V \to V^{**}$ следующим образом: $v \mapsto (\varphi \in V^* \mapsto \varphi(v))$. Утверждаем, что ζ - изоморфизм. Так как у нас $\dim V = \dim V^* = \dim V^{**}$, нам достаточно просто доказать, что ζ - инъекция. Пусть $v \in \ker\zeta$, тогда отображение $(\varphi \mapsto \varphi(v))$ - нулевое. Покажем, что $v = 0$. В пространстве V^* существует линейный функционал $v^* : v^*(v) = 1$, если $v \neq 0$. Действительно, если $v \neq 0$, то мы можем построить базис $v, e_2, \ldots, e_n$ и двойственный базис $v^*, e_2^*, \ldots, e_n^*$. Значит $v^*(v) \neq 0$, противоречие. Тогда $\ker\zeta = 0 \implies \zeta$ - инъекция, а значит и биекция.
Также нам надо показать, что ζ - линейное отображение.
$\zeta(v_1 + v_2) = \varphi(v_1 + v_2) = \varphi(v_1) + \varphi(v_2) = \zeta(v_1) + \zeta(v_2), v_1, v2 \in V, \varphi \in V^*$
$\zeta(\gamma v) = \varphi(\gamma v) = \gamma\varphi(v) = \gamma\zeta(v), v \in V, \gamma \in k$
Тогда ζ - биекция и линейное отображение, а следовательно - изоморфизм, причем канонический, так как мы не определяли базис.

43 Лемма о размерности аннулятора.

Определение: Пусть $W \subset V$ - подпространство, тогда $AnnW = \{\varphi \in V^* : \varphi(w) = 0\ \forall w \in W\}$
Лемма: $W \subset V$, тогда $\dim W + \dim\ AnnW = \dim V$
Доказательство: пусть $e_1, \ldots, e_k$ - базис W, достроим его до $e_1, \ldots, e_k, e_{k+1}, \ldots, e_n$ - базиса V. Покажем, что $e_{k+1}^*, \ldots, e_n^*$ - базис $AnnW$. Линейная независимость вытекает из того, что изначально эти векторы были линейно независимыми в базисе V^*, а мы просто взяли подмножество.

Порождаемость: пусть $\varphi \in AnnW \implies \varphi = \sum\limits_{i=1}^{k} \beta_i e_i^* + \sum\limits_{i=k+1}^{n} \beta_i e_i^*$. Но так как $e_1, \ldots, e_k$ - базис W, на нем φ будет равна нулю, следовательно $\varphi = \sum\limits_{i=k+1}^{n} \beta_i e_i^*$, тогда это базис, чего мы и хотели.

44 Сопряженное отображение. Матрица сопряженного отображения.

44.1 Сопряженный оператор.

Определение: пусть $\mathcal{L} : V \to U$ - линейное отображение, тогда определим $\mathcal{L}^* : U^* \to V^*$ следующим образом: пусть $\varphi \in U^*, \mathcal{L}^*(\varphi) = \varphi \circ \mathcal{L} \in V^*$ - сопряженное или двойственноеу к $\mathcal{L}$

44.2 Матрица сопряженного оператора.

$[\mathcal{L}^*]_{f^*,e^*} = [\mathcal{L}]_{e,f}^T$, если $A = (a_{ij})$ - матрица размера $m \times n$, тогда $A^T = (a_{ji})$ - матрица размера $n \times m$, то есть мы берем просто матрицу, переворачиваем ее и отзеркаливаем.

45 Аннулятор образа равен ядру сопряженного.

Утверждение: $Ann\left(Im\mathcal{L}\right) = \ker \mathcal{L}^*, \mathcal{L} : V \to U$
Упражнение: $W \subset V, AnnW \subset V^*$:
Пусть $\varphi \in V^* : \varphi\left(v\right) = 0\ \forall v \in V$, среди этих элементов также есть те, которые лежат в W, тогда получается, что $\varphi \in AnnW$.
Теперь пусть $\varphi_1, \varphi_2 \in AnnW$
$\left(\varphi_1 + \varphi_2\right)\left(w\right) = \varphi_1\left(w\right) + \varphi_2\left(w\right) = 0$
$\left(\gamma\varphi\right)\left(w\right) = \gamma\varphi\left(w\right) = 0$
Доказательство: $\varphi \in Ann\left(Im\mathcal{L}\right) \iff \varphi\left(u\right) = 0\ \forall u \in Im\mathcal{L} \iff \varphi\left(\mathcal{L}\left(v\right)\right) = 0\ \forall v \in V \iff \mathcal{L}^*\left(\varphi\right)\left(v\right) = 0\ \forall v \in V \iff \mathcal{L}^*\left(\varphi\right) = 0 \iff \varphi \in \ker \mathcal{L}^*$

46 Ранг оператора. Равенство строчного и столбцового рангов оператора. Теорема Кронекера–Капелли.

46.1 Ранг оператора.

Определение (через матрицы): пусть $\mathcal{L} : \underset{e}{V} \to \underset{f}{W}$. Тогда строчный ранг $\left[\mathcal{L}\right]_{e,f}$ - максимальное количество линейно независимых строк этой матрицы. Столбцовый ранг $\left[\mathcal{L}\right]_{e,f}$ - максимальное количество линейно независимых столбцов этой матрицы.
Определение: $\mathcal{L} : \underset{e}{V} \to \underset{f}{W}$. Строчный ранг - $\dim Im\mathcal{L}^*$, столбцовый ранг - $\dim Im\mathcal{L}$

46.2 Равенство строчного и столбцового рангов оператора.

Теорема: $\dim Im\mathcal{L} = \dim Im\mathcal{L}^*$ - столбцовый ранг равен строчному рангу
Доказательство: Пусть $m = \dim U^*$. $\dim Im\mathcal{L}^* = \dim U^* - \dim \ker \mathcal{L}^* = m - \dim Ann\left(Im\mathcal{L}\right) = m - \left(m - \dim Im\mathcal{L}\right) = \dim Im\mathcal{L}$
Тогда $rank\mathcal{L}$ - любой из этих рангов

46.3 Теорема Кронекера-Капелли.

Теорема: решение $\mathcal{L}x = b$ существует $\iff rank\left[\mathcal{L}\right] = rank\left(\left[\mathcal{L}\right]|\, b\right)$
Доказательство: пусть $\mathcal{L} : V \to U, b \in U$. Хотим найти $x \in V : \mathcal{L}x = b$
Решение существует если $b \in Im\mathcal{L} \iff b \in \langle \mathcal{L}e_1, \ldots, \mathcal{L}e_n \rangle$ где эти вектора базисные в $V \iff$ Максимальное количество линейно независимых в $\{\mathcal{L}e_1, \ldots, \mathcal{L}e_n\}$ равно максимальному количеству линейно независимых элементов в $\{\mathcal{L}e_1, \ldots, \mathcal{L}e_n, b\} \iff rank\left[\mathcal{L}\right] = rank\left(\left[\mathcal{L}\right]|b\right)$

47 Тензорное произведение, существование и единственность. Тензорная алгебра.

Определение:
отображение $\varphi : V \times W \to U$ называют билинейным когда оно линейно по обоим аргументам по отдельности, то есть: пусть для каждого $v \in V$ определено $f_v : W \to U$ такое что $\forall w \in W : f_v(w) = \varphi(v, w)$ и для каждого $w \in W$ определено $g_w : V \to U$ такое что $\forall v \in V : g_w(v) = \varphi(v, w)$ тогда если $\forall v \in V : f_v \in Hom(W, U)$ и

$\forall w \in W : g_w \in Hom(V, U)$ то φ билинейное отображение

Определение:

тензорным произведением пространств V и W называют такую пару (T, τ) где T это векторное пространство, τ это билинейное отображение из V, W в T что для каждого билинейного отображения φ из V, W в любое пространство U выполняется:
$\exists! \widetilde{\varphi} \in Hom(T, U) : \forall (v, w) \in V \times W : \widetilde{\varphi}(\tau(v, w)) = \varphi(v, w)$ то есть $\exists! \widetilde{\varphi} : \widetilde{\varphi} \circ \tau = \varphi$ такое пространство T с естественным τ обозначается $V \otimes W$

Доказательство:

докажем, что такое пространство единственно с точностью до изоморфизма, пусть таким свойством относительно V, W обладают два пространства (T, τ) и $(\widetilde{T}, \widetilde{\tau})$, докажем что $T \cong \widetilde{T}$. По определению, для $\widetilde{\tau} : V \times W \to \widetilde{T}$ существует единственное $\psi : T \to \widetilde{T}$ такое что $\psi \circ \tau = \widetilde{\tau}$ и в другую сторону для $\tau : V \times W \to \widetilde{T}$ существует единственное $\widetilde{\psi} : \widetilde{T} \to T$ такое что $\widetilde{\psi} \circ \widetilde{\tau} = \tau$ то есть $\psi \circ \tau = \widetilde{\tau}$ $\widetilde{\psi} \circ \widetilde{\tau} = \tau$ Значит $\widetilde{\psi} \circ \psi \circ \tau = \widetilde{\psi} \circ \widetilde{\tau} = \tau$, заметим, что для $\widetilde{\psi} \circ \psi$ подходит id_T, но так как мы определяли $\psi, \widetilde{\psi}$ как единственные подходящие, то $\widetilde{\psi} \circ \psi$ и будет только id_T
аналогично будет $\psi \circ \widetilde{\psi} = id_{\widetilde{T}}$, а так как $\psi, \widetilde{\psi}$ друг другу обратны слева и справа, значит это взаимнообратные биекции, а так как это были линейные отображения между T и $\widetilde{T}$, то мы и нашли изоморфизм
существование такого $V \otimes W$ докажем конструктивно
пусть $e_1, e_2, ..., e_n$ это базис V пусть $f_1, f_2, ..., f_m$ это базис W тогда составим для всех $i = 1, 2, ..., n$ и $j = 1, 2, ..., m$ пары из элементов базисов, и обозначим их новыми буквами $\tau(e_i, f_j) = e_i \otimes f_j$, распишем значения в общем виде
пусть $v = \sum\limits_{i=1}^{n} \alpha_i e_i$ и $w = \sum\limits_{j=1}^{m} \beta_j f_j$, тогда $\tau(v, w) = \tau\left(\sum\limits_{i=1}^{n} \alpha_i e_i, \sum\limits_{j=1}^{m} \beta_j f_j\right) = \sum\limits_{i=1}^{n} \sum\limits_{j=1}^{m} \alpha_i \beta_j (e_i \otimes f_j)$
заметим, что теперь можем по любому билинейному $\varphi : V \times W \to U$ построить линейное $\widetilde{\varphi} : V \otimes W \to U$, определив его таким образом: $\widetilde{\varphi}(e_i \otimes f_j) = \varphi(e_i, f_j)$ и, так как имеем совпадение результатов на базисе и однозначное определение $\widetilde{\varphi}$ от φ, то получаем, что наше $V \otimes W$ соответствует определению.
заметим, что как векторное пространство, $V \otimes W \cong k^{n \cdot m}$ где k это поле, над которым определены V, W, определим тензорное произведение последовательности пространств $V_1, V_2, ..., V_n$ где $n > 2$ по цепному правилу:

$$\bigotimes_{i=1}^{n} V_i = V_1 \otimes \left(\bigotimes_{i=1}^{n-1} V_{i+1}\right)$$

так, определим тензорную степень пространства: $V^{\otimes n} = \bigotimes\limits_{i=1}^{n} V$ если $n > 0$ $V^{\otimes 0} = k$ где k это поле, над которым задано V, если $n = 0$
определим прямую (внешнюю) сумму последовательности пространств пронумерованной целыми неотрицательными числами как конечные (финитные) последовательности элементов пространств из последовательности, то есть последовательности, где первый элемент принадлежит первому пространству, второй второму, и так далее, но с некоторого момента, элементы становятся стабильно нулями а именно

$$\bigoplus_{n=0}^{\infty} V_n = \{s \in \times_{n=0}^{\infty} V_n : \exists n \in \mathbb{Z}_+ \ \forall m \in \mathbb{Z}_+ \ (m > n) \Rightarrow (s_m = 0)\}$$

тогда тензорной алгеброй называют такое пространство

$$TV = \bigoplus_{n=0}^{\infty} V^{\otimes n}$$

в котором определено не коммутативное, дистрибутивное относительно сложения умножение, для $v, w \in TV$ обозначается $v \otimes w$, пусть $e_1, e_2, ..., e_n$ это базис V тогда зададим базис в TV , это будет

$$\bigcup_{k=0}^{\infty} \left\{ \bigoplus_{j=1}^{k} e_{i_j} : i \in (\mathbb{Z} \cap [1; n])^k \right\}$$

где как и в тензорном произведении двух пространств, такие элементы будут считаться отдельными буквами то есть элементы базиса это конечные последовательности индексов элементов базиса изначального V , например:
при $i = ()$ получим произведение пустой последовательности векторов
при $i = (2)$ получим e_2
при $i = (1, 2, 3)$ получим $e_1 \otimes e_2 \otimes e_3$
а произведение двух элементов $v, w \in TV$ в общем случае будет таким: сначала разложим элементы по введённому базису, а после этого переберём все элементы $\alpha \cdot e_{i_1} \otimes e_{i_2} \otimes \cdots \otimes e_{i_k}$в разложении v и элементы $\beta \cdot e_{j_1} \otimes e_{j_2} \otimes \cdots \otimes e_{j_l}$, тогда к произведению прибавится $\alpha \cdot \beta \cdot e_{i_1} \otimes e_{i_2} \otimes \cdots \otimes e_{i_k} \otimes e_{j_1} \otimes e_{j_2} \otimes \cdots \otimes e_{j_l}$, то есть v, w раскладываются по базису, перебираются все пары произведений элементов базиса V, находится коэффициент при одном в v и другом в w соответственно, и результат это сумма по всем парам элементов базиса TV произведения коэффициентов при них в v и w соответственно, на их конкатенацию (склеивание строк) например:
$(e_1 + e_1 \otimes e_2) \otimes (3 \cdot e_2 \otimes e_1 + 2 \cdot e_1 \otimes e_1)$ раскладываем по дистрибутивности, получаем:
$e_1 \otimes (3 \cdot e_2 \otimes e_1) + e_1 \otimes (2 \cdot e_1 \otimes e_1) + e_1 \otimes e_2 \otimes (3 \cdot e_2 \otimes e_1) + e_1 \otimes e_2 \otimes (2 \cdot e_1 \otimes e_1)$ упростим выражение, приведём подобные слагаемые, вынесем константы:

$$3 \cdot e_1 \otimes e_2 \otimes e_1 + 2 \cdot e_1 \otimes e_1 \otimes e_1 + 3 \cdot e_1 \otimes e_2 \otimes e_2 \otimes e_1 + 2 \cdot e_1 \otimes e_2 \otimes e_1 \otimes e_1$$

48 Внешняя степень, построение. Внешняя алгебра.

в алгебре TV определим такой двусторонний идеал:

$$I = \langle v \otimes v : \ v \in V \rangle$$

то есть идеал, натянутый на произведение двух одинаковых векторов подряд. если записать как множество, то получится

$$I = \{w_1 \otimes v \otimes v \otimes w_2 : v \in V, \ w_1, w_2 \in TV\}.$$

тогда внешней алгеброй над V назовём TV/I, обозначается $\wedge V$. в такой алгебре умножение обозначается $\wedge$, и станет антикоммутативным, то есть

$$\forall a, b \in \wedge V : \ a \wedge b = -(b \wedge a).$$

так как

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

а значит

$$a \wedge b + b \wedge a = 0.$$

k-й внешней степенью V будем называть пространство $V^{\otimes k}$ спроецированное на $\wedge V$, обозначается $\wedge^k V$, то есть пространство произведений последовательностей из k векторов из V.

49 Базис внешней степени. Подсчет размерности внешней степени.

мы уже знаем, что

$$V^{\otimes k} = \left\{ \bigoplus_{j=1}^{k} e_{i_j} : \ i \in (\mathbb{Z} \cap [1; n])^k \right\},$$

где $e_1, e_2, ..., e_n$ это базис V.

тогда если факторизовать $V^{\otimes k}$ по I то уже знаем, что получатся все те же произведения, но без порядка множителей, ведь из одного порядка можно перейти в другой, если домножить на -1 и переставить два соседних элемента по антикоммутативности внешнего произведения.

тогда чтобы построить базис, надо выбрать по представителю из всех классов эквивалентности последовательностей из k элементов из n элементов базиса V, где нет повторяющихся, и где две последовательности считаются эквивалентными, если они совпадут при перестановке элементов. количество таких элементов это по определению C_n^k.

тогда чтобы построить пример базиса, например упорядочим все последовательности определённым образом: например индексы элементов e_i будут неубывающими, но так как мы выкинули все последовательности с повторяющимися элементами, то i станут строго возрастать. тогда базисом можно выбрать такое множество:

$$\left\{ \bigwedge_{j=1}^{k} e_{i_j} : i \in (\mathbb{Z} \cap [1; n])^k, \ \forall j \in \mathbb{Z} \cap [1; k-1] : i_j < i_{j+1} \right\}.$$

50 Индуцированные гомоморфизмы на тензорной и внешней алгебрах. Определитель. Мультипликативность определителя.

пусть дано линейное отображение $\mathcal{L} : \ V \mapsto W$, тогда определим k-ю тензорную степень отображения $\mathcal{L}$ как:

$$\mathcal{L}^{\otimes k} : \ V^{\otimes k} \mapsto W^{\otimes k}$$

такое что

$$\forall i \in (\mathbb{Z} \cap [1; n])^k : \ \mathcal{L}^{\otimes k} \left(\bigotimes_{j=1}^{k} e_{i_j} \right) = \bigotimes_{j=1}^{k} \mathcal{L}(e_{i_j}).$$

на остальные вектора из $V^{\otimes k}$ значения продолжатся по линейности.

аналогично k-я внешняя степень отображения $\mathcal{L}$ это:

$$\mathcal{L}^{\wedge k} : \ V^{\wedge k} \mapsto W^{\wedge k}$$

такое что

$$\forall i \in (\mathbb{Z} \cap [1; n])^k : \ \mathcal{L}^{\wedge k} \left(\bigwedge_{j=1}^{k} e_{i_j} \right) = \bigwedge_{j=1}^{k} \mathcal{L}(e_{i_j}).$$

на остальные вектора из $V^{\wedge k}$ значения продолжатся по линейности.

пусть дан оператор $\mathcal{L} : \ V \mapsto V$, где V это векторное пространство размерности n. тогда определителем оператора $\mathcal{L}$ называют $\mathcal{L}^{\wedge n}$.

заметим, что это константа, так как $\dim V^{\wedge n} = C_n^n = 1$, то есть определитель принимает одномерный вектор вида $\alpha \bigwedge_{i=1}^{n} e_i$ и возвращает $\beta\alpha \bigwedge_{i=1}^{n} e_i$, то есть по сути эта константа β и определяет определитель, обозначается $\det \mathcal{L}$.

докажем мультипликативность определителя, а именно: пусть дано пространство V, тогда

$$\forall \mathcal{L}, \mathcal{T} \in \mathrm{End}(V) : \ \det(\mathcal{L} \circ \mathcal{T}) = \det(\mathcal{L}) \cdot \det(\mathcal{T}).$$

для этого просто раскроем внешнюю степень, то есть докажем, что

$$(\mathcal{L} \circ \mathcal{T})^{\wedge n} = \mathcal{L}^{\wedge n} \circ \mathcal{T}^{\wedge n}.$$

раскроем внешние произведения из определений, и покажем, что это одна и та же запись:

$$\mathcal{T}^{\wedge n} \left(\bigwedge_{i=1}^{n} e_i \right) = \bigwedge_{i=1}^{n} \mathcal{T}(e_i),$$

$$\mathcal{L}^{\wedge n} \left(\bigwedge_{i=1}^{n} \mathcal{T}(e_i) \right) = \bigwedge_{i=1}^{n} \mathcal{L}(\mathcal{T}(e_i)) = (\mathcal{L} \circ \mathcal{T})^{\wedge n} \left(\bigwedge_{i=1}^{n} e_i \right).$$

51 Изоморфизм $V \cong \left(\wedge^{n-1} V\right)^*$

изоморфность доказывается тривиально: пусть $\dim V = n$, тогда $\dim \wedge^{n-1} V = \dim \left(\wedge^{n-1} V\right)^* = C_n^{n-1} = n$.

но важен определённый изоморфизм:

пусть V определено над полем k, тогда формой объёма называют $\omega : \ V^{\wedge n} \mapsto k$, это $\omega \in (V^{\wedge n})^*$ такое что:

$$\omega \left(\bigwedge_{i=1}^{n} e_i \right) = 1.$$

заметим, что такое ω просто равно константе при произведении последовательности всех векторов из базиса.

определим $F : V \mapsto (V^{\wedge n-1})^*$ такое что

$$\forall v \in V : \ \forall u \in V^{\wedge n-1} : \ F_v(u) = \omega(v \wedge u).$$

заметим, что F линейно, так как выполняется дистрибутивность при раскрытии $\wedge$.

и F изоморфизм, так как биекция, потому что инъективный гомоморфизм в конечномерном пространстве.

52 Критерий обратимости оператора в терминах определителя. Построение обратного оператора с помощью изоморфизма $V \cong \left(\wedge^{n-1} V\right)^*$.

определим $\mathcal{L}^\vee : \ V \mapsto V$ единственным образом таким способом:

$$\forall v \in V : \ \forall u \in V^{\wedge n-1} : \ \omega(v \wedge \mathcal{L}^{\wedge n-1}(u)) = \omega(\mathcal{L}^\vee(v) \wedge u).$$

докажем, что $(\det \mathcal{L} \neq 0) \Leftrightarrow (\exists \mathcal{L}^{-1})$.

справа налево:

с одной стороны

$$\det(\mathcal{L} \circ \mathcal{L}^{-1}) = \det(\mathrm{id}_V) = 1,$$

с другой стороны

$$\det(\mathcal{L} \circ \mathcal{L}^{-1}) = \det(\mathcal{L}) \cdot \det(\mathcal{L}^{-1}).$$

тогда получается, что

$$1 = \det(\mathcal{L}) \cdot \det(\mathcal{L}^{-1}),$$

так что $\det \mathcal{L}$ не могло быть нулём.

слева направо:

построим

$$\mathcal{L}^{-1} = \frac{1}{\det \mathcal{L}} \cdot \mathcal{L}^\vee.$$

конструктивно показали, что $\exists \mathcal{L}^{-1}$.

53 Модуль над кольцом; определение конечнопорожденного и свободного модуля. Построение копредставления для конечно-порожденного модуля.

54 Нормальная форма Смита для матриц над областью главных идеалов.

55 Теорема о структуре конечно-порожденного модуля над ОГИ.

56 Структура конечно-порожденных абелевых групп.

57 Теорема Гамильтона–Кэли.

58 Существование и единственность жордановой нормальной формы над алгебраически замкнутым полем.

59 Определения

Соответсвие Между множетсвами A и B, подмножество $R \subset A \times B$.

Отображение множеств Соответвие f из A в B, в котором выполняется $\forall a \in A : \exists! b \in B : (a, b) \in f$ (элемент из A соответсвует ровно одному элементу из B).

Инъекция Отображение f из A в B, для которого выполняется $\forall a, a' \in A : f(a) = f(a') \implies a = a'$ (все элементы из A отображаются в различные значения).

Сюръекция Отображение f из A в B, для которого выполняется $\forall b \in B : \exists a \in A : f(a) = b$ (для каждого значения в B есть соответствующее значение в A).

Обратимость отображения слева и справа Отношение g является обратным слева к f, если $g \circ f = \mathrm{id}_A$. Справа – если $f \circ g = \mathrm{id}_B$.

Бинарная операция На множестве X, отображение $X \times X \to X$.

Моноид Множество M с бинарной операцией $\cdot$, для которых выполняется:

Ассоциативность $\forall a, b, c \in M : a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

Существование нейтрального элемента $\exists e \in M : \forall m \in M : e \cdot m = m \cdot e = e$.

Группа Моноид, в котором дополнительно существует обратный элемент: $\forall m \in M \setminus \{e\} : \exists m^{-1} \in M : m \cdot m^{-1} = e$.

Абелева группа Группа, в которой операция коммутативна ($a \cdot b = b \cdot a$).

Кольцо Множество R с операциями $(\cdot, +)$, такое что:

- $(R, +)$ – комутативная (абелева) группа
- Выполняется дистрибутивность умножения:

$$\forall a, b, c \in R : \begin{cases} a \cdot (b + c) = a \cdot b + a \cdot c \\ (a + b) \cdot c = a \cdot c + b \cdot c \end{cases}$$

Подкольцо Подмножество S кольца R, в котором результаты операций тоже лежат в подмножестве.

$$\begin{cases} S \subset R \\ \forall s_1, s_2 \in S : s_1 + s_2 \in S \\ \forall s_1, s_2 \in S : s_1 \cdot s_2 \in S \end{cases}$$

Идеал Непустое подмножество кольца, для которого выполняется:

- $\forall a, b \in I : a + b \in I$
- $\forall a \in I : \forall r \in R : r \cdot a \in I$

Делитель нуля Ненулевой элемент кольца $r \in R \setminus \{0\}$, такой что $\exists s \in R : s \neq 0 \wedge r \cdot s = 0$.

Область целостности Кольцо, в котором нет делителей нуля.

Ассоциированные элементы Элементы кольца $a \neq 0$, $b \neq 0$, такие что $a \mid b$ и $b \mid a$.

Евклидова область Область целостности в котором сущесвует функция нормы $N : R \setminus \{0\} \to \mathbb{N}_0$, такая что:

- $N(a \cdot b) \geq N(a)$ (и $N(a \cdot b) = N(a)$ если $b \in R^\times$)
- Можно делить с остатком, уменьшая норму: $\forall a, b \neq 0 \in R : \exists q, r \in R : a = q \cdot b + r \wedge (N(r) < N(b) \vee r = 0)$.

Наибольший общий делитель Для двух элементов кольца $a, b \in R$, максимальный по норме элемент $g \in R$, такой что $g \mid a$, $g \mid b$.

Область главных идеалов Область целостности, в которой каждый идеал главный (т.е. имеет вид $(i) = \{r \cdot i : r \in R\}$).

Неприводимый элемент Элемент $r \in R$, для которого из равенства $r = s \cdot t$ следует, что $s \in R^\times$ или $t \in R^\times$ (нельзя разбить на необратимые элементы).

Фактор-кольцо Кольцо R/I, в котором $a = b \iff (a - b) \in I$.

Гомоморфизм колец Отображение $\varphi : R \to S$, которое сохраняет структуру кольца:

- $\varphi(a) + \varphi(b) = \varphi(a + b)$
- $\varphi(a) \cdot \varphi(b) = \varphi(a \cdot b)$
- $\varphi(1_R) = 1_S$ для колец с единицей

Ядро гомоморфизма Все элементы, которые отправляются в ноль:
$\operatorname{Ker} \varphi = \{r : r \in R, \varphi(r) = 0\}$.

Образ гомоморфизма Множество значений гомоморфизма:
$\operatorname{Im} \varphi = \{\varphi(r) : r \in R\} = \{s \in S : \exists r \in R, \varphi(r) = s\}$.

Произведение колец Кольцо пар из элементов других колец с покомпонентными операциями:

- $R \times S = \{(r, s) : r \in R, s \in S\}$
- $(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$
- $(r_1, s_1) \cdot (r_2, s_2) = (r_1 \cdot r_2, s_1 \cdot s_2)$

Функция эйлера Функция $\varphi : \mathbb{N} - > \mathbb{N}$, и $\varphi(n)$ равно количеству натуральных чисел $\leq n$, которые взаимно просты с n.
$\varphi(n) = |\{x : 1 \geq x \leq n \wedge \gcd(x, n) = 1\}|$.

Кольцо многочленов над полем Кольцо $K[x]$, которое содержит последовательности коэффициентов $(k_0, k_1, \dots, k_n, 0, \dots)$, каждая из которых соответствует выражению $k_0 + k_1 x + k_2 x^2 + \dots + k_n x^n$.

Корень многочлена Элемент поля $x \in K[x]$ когда $P(x) = 0$ (очев?).

Формальное равенсто многочленов Многочлен $P(x) = p_0 + p_1 x + p_2 x^2 + \dots$ формально равен $Q(x) = q_0 + q_1 x + q_2 x^2 + \dots$ если $p_0 = q_0, p_1 = q_1, \dots$ $(\forall i : p_i = q_i)$.

Фукнциональное равенство многочленов Многочлен $P \in K[x]$ функционально равен $Q \in K[x]$ если $\forall x \in K : P(x) = Q(x)$.

Сумма, произведение, пересечение идеалов

Сумма $I + J = \{i + j : i \in I, j \in J\}$

Произведение $IJ = \{\sum_k i_k j_k : i_k \in I, j_k \in J\}$

Пересечение $I \cap J = \{x : x \in I \wedge x \in J\}$

Взаимно простые (комаксимальные) идеалы Идеалы I и J кольца R, такие что $I + J = R \iff 1 \in I + J$.

Формула Тейлора Тут нужна просто формула m-ой производной?

Кратность корня многочлена Корень α многочлена P имеет кратность m если $P = (x - \alpha)^m \cdot G$, где $G \neq 0$.

Итерполяционный многочлен Лагранжа Способ построить многочлен, проходящий через множество точек $\{(x_0, y_0), \dots (x_n, y_n)\}$.

$$f(x) = \sum_{i=0}^{n} y_i L_i(x)$$
$$L_i(x) = \frac{(x - x_0) \cdots (x - x_{i-1})(x - x_{i+1}) \cdots (x - x_n)}{(x_i - x_0) \cdots (x_i - x_{i-1})(x_i - x_{i+1}) \cdots (x_i - x_n)} = \frac{\prod_{j \neq i} x - x_j}{\prod_{j \neq i} x_n - x_j}$$

Максимальный идеал Идеал $I \triangleleft R$, $I \neq R$, когда для некоторого J: $I \subset J \implies (J = I) \vee (J = R)$.

Простой идеал Идеал $I \triangleleft R$, $I \neq R$, в котором $ab \in I \implies (a \in I) \vee (b \in I)$.

Квадратичный вычет Число $x \in \mathbb{Z}_p$, такое что $\exists y \in \mathbb{Z}_p : y^2 = x$ (x является квадратом некоторого числа по модулю p).

Символ Лежандра Фукнция $\left(\frac{a}{p}\right)$, которая показывает, является ли a квадратичным вычетом по модулю p.

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & a \text{ – кв. вычет mod } p \\ -1, & \text{иначе} \end{cases}$$

Поле комплексных чисел Поле $\mathbb{C} = \mathbb{R}[i]/(i^2 + 1)$ – дополнение действительных чисел, в котором $i^2 = -1$.

Комплексное сопряжение Для числа $x = a + bi \in \mathbb{C}$: $\bar{x} = a - bi$.

Модуль комплекного числа Для $x = a + bi$, $|x| = \sqrt{a^2 + b^2} = \sqrt{x\bar{x}}$, расстояние от 0 на комплекной плоскости.

Векторное пространство Множество V поверх K с операциями $+ : V \times V \to V$ и $\cdot : K \times V \to V$, где дополнительно:

- $(V, +)$ – абелева группа

- $(\alpha + \beta)v = \alpha v + \beta v$
- $\alpha(v_1 + v_2) = \alpha v_1 + \alpha v_2$
- $(\alpha\beta)v = \alpha(\beta v)$
- $1 \cdot v = v$

Линейная независимость Векторы v_1 и v_2 линейно независимы, если не существует таких a и b, что $av_1 + bv_2 = \vec{0}$.

Базис векторного пространства Три эквивалентных определения:

- Линейно независимое порождающее множество
- Максимальное по включению множество независимых векторов
- Минимальное по включение порождающее множество

Размерность векторного пространства $\dim V := |B|$, где B – базис пространства V.

Линейное отображение Фукнция (гомоморфизм) $\mathcal{L} : V \to W$, такая что

- $\mathcal{L}(v_1 + v_2) = \mathcal{L}(v_1) + \mathcal{L}(v_2)$
- $\mathcal{L}(\alpha \cdot v) = \alpha\mathcal{L}(v)$

Ядро линейного отображения Вектора, которые отправляются в $\vec{0}$:
$\operatorname{Ker} \mathcal{L} = \{v : v \in V, \mathcal{L}(v) = \vec{0}\}$

Образ линейного отображения Все достижимые вектора после отображения:
$\operatorname{Im} \mathcal{L} = \{u : \exists v \in V, \mathcal{L}(v) = u\} = \{\mathcal{L}(v) : v \in V\}$

Матрица линейного отображения Если $e = (e_1, e_2, \ldots, e_n)$ – базис V, $f = (f_1, \ldots, f_m)$ – базис W, то матрица линейного отображения $\mathcal{L}$ – таблица вида:

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix}$$

Преобразование задаётся как:

$$\begin{aligned} \mathcal{L}e_1 &= a_{1,1}f_1 + \cdots + a_{m,1}f_m \\ \mathcal{L}e_2 &= a_{1,2}f_1 + \cdots + a_{m,2}f_m \\ &\vdots \\ \mathcal{L}e_n &= a_{1,n}f_1 + \cdots + a_{m,n}f_m \end{aligned}$$

Двойственное пространство Пространство линейных функционалов – функций, преобразующих векторы в скаляры при этом сохраняя линейность:

- $\forall \varphi \in V^*, v, w \in V : \varphi(v) + \varphi(w) = \varphi(v + w)$
- $\forall \varphi \in V^*, v \in V, k \in K : k\varphi(v) = \varphi(kv)$

Можно их считать гомоморфизмами из V в K.

Двойственный базис Координатные функции для базиса V ($e = (e_1, e_2, \ldots, e_n)$):

$$e_i^*(e_j) = \delta_i^j = \begin{cases} 1, i = j \\ 0, i \neq j \end{cases}$$

Аннулятор множества Множество линейных функционалов, которые обнуляют все векторы в подпространстве $W \subset V$: $\text{Ann } W = \{\varphi \in V^* : \forall \omega \in W \ \varphi(\omega) = 0\}$

Сопряжённый оператор Оператор над двойственными векторами, который соответствует применению линейного оператора к пространству перед применением линейного функционала:
$\mathcal{L}^*(\varphi)(v) = \varphi(\mathcal{L}(v)) \implies \mathcal{L}^*(\varphi) = \varphi \circ \mathcal{L}$

Переход: $V \xrightarrow{\mathcal{L}} U \xrightarrow{\varphi} K$.

Ранг оператора Равные понятия ранга:

Строчный $\text{rk}_r(\mathcal{L}) = \dim(\text{Im } \mathcal{L}^*)$

Столбцовый $\text{rk}_l(\mathcal{L}) = \dim(\text{Im } \mathcal{L})$

Тензорное произведение

Тензорная алгебра

Внешнаяя степень

Внешнаяя алгебра

Определитель

Модуль Над кольцом R, абелева группа M с отображением $\cdot : R \times M \to M$ и

- $\forall r_1, r_2 \in R, m \in M : (r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$
- $\forall r \in R, m_1, m_2 \in M : r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$
- $\forall r_1, r_2 \in R, m \in M : r_1 \cdot (r_2 \cdot m) = (r_1 \cdot r_2) \dot{m}$
- $\forall m \in M : 1 \cdot m = m$

Свободный модуль Модуль, для которого $\exists n : M \cong R^n$.

Конечнопорожденный модуль Все элементы модуля являются линейными комбинациями конечного порождающего множества:
$\exists m_1, \ldots, m_n \in M : \forall x \in M : \exists r_1, \ldots, r_n \in R : x = r_1 \cdot m_1 + \cdots + r_n \cdot m_n$

Нормальная форма Смита Если R – ОГИ и A – матрица, то существуют обратимые матрицы U и V, такие что

$$UAV = \begin{pmatrix} \alpha_1 & 0 & 0 & \ldots & 0 & \ldots & 0 \\ 0 & \alpha_2 & 0 & & & & \\ 0 & 0 & \ddots & & \vdots & & \vdots \\ \vdots & & & \alpha_t & & & \\ 0 & & \ldots & & 0 & \ldots & 0 \\ \vdots & & & & \vdots & & \vdots \\ 0 & & \ldots & & 0 & \ldots & 0 \end{pmatrix}$$

Нильпотентный оператор Оператор, если применить который n раз подряд, он станет отправлять всё в $\vec{0}$.

Жорданова клетка Компонент нормальной формы, матрица вида:

$$\begin{pmatrix} \lambda & & & \dots & & 0 \\ 1 & \lambda & & & & \\ 0 & 1 & \lambda & & & \vdots \\ 0 & 0 & 1 & \lambda & & \\ \vdots & \vdots & & \ddots & \ddots & 0 \\ 0 & 0 & \dots & 0 & 1 & \lambda \end{pmatrix}$$

Жорданова нормальная форма Способ записи матрицы оператора в диагональном виде в определенном базисе:

$$\begin{pmatrix} J(\lambda_1) & & \dots & & 0 \\ & J(\lambda_2) & & & \\ \vdots & & J(\lambda_3) & & \vdots \\ & & & \ddots & \\ 0 & & \dots & & J(\lambda_m) \end{pmatrix}$$

Где $J(\lambda_i)$ – жорданова клетка.