Дисклеймер.

Автор не несет ответственности за любой ущерб, причиненный Вам при использовании данного документа. Автор напоминает, что данный документ может содержать ошибки и опечатки, недостоверную и/или непроверенную информацию. Если Вы желаете помочь в развитии проекта или сообщить об ошибке/опечатке/неточности:

GitHub проекта

Автор в ВК

Внимание: данный документ не поддерживается и поддерживаться не будет! Сообщения об ошибках НЕ рассматриваются, пулл реквесты НЕ принимаются! Если Вы хотите поддерживать этот документ - форкните проект на Github. Благодарю за понимание.

В данном документе используются следующие обозначения: $*$ — бинарная операция на множестве, $\cdot$ — бинарная операция умножения на множестве. Данная хрень сделана для облегчения набора текста и понимания исходного кода. Просьба понять, простить и не путатся.

Алгебра и теория чисел

$X \backslash Y = \{x \in X(\text{Элементы множества}); x \notin Y \text{ (условие вхождения)}\}$

card X - мощность множества.

$|x|$ — количество элементов множества.

"Графиком функции Γ из X в Y" (где X и Y - множества) называется подмножество $\Gamma \leq X \times Y$, такое, что $\forall x \in X \ \exists! \ y \in Y : (x, y) \in \Gamma$

Функция - тройка, состоящая из (X, Y, Γ), где (X, Y) - множества, а Γ - график.

$X \times Y = \{(x, y) | (x \in X, y \in Y)\}$ — Декартово произведение.

Вместо f = (X, Y, Γ) будем писать: $f : X \to Y$, где f(x) = y для (x, y) ∈ Γ.

$f : R \to R_0$ — общий вид для функций, например, $f(x) = x^2$;

Образ функции f: $Imf = \{f(x) | x \in X\} = \{y \in Y | \exists x \in X : f(x) = y\} \leq Y$

$f : X \to Y$, где X называется domain, а Y — codomain.

Иногда образ функции обозначают $f'(x)$

$2Z \neq Z + Z$ (потому что $2Z$ — множество четных чисел, а $Z + Z$ — сумма любых двух целых чисел).

$Z^2 = N_0^2$;

$N = \{1, 2, ...\}$;

$N_0 = \{0, 1, 2, ...\}$;

$Z = \pm N_0$;

$Q\frac{Z}{N}$;

R, C, H - примеры множеств чисел.

$f : X \to Y,\ x \in X,\ y \in Y$;

$f^{-1}(y) = \{x \in X | f(x) = y\}$ — прообраз y или слой над y.

$Y' \subset Y \Rightarrow f^{-1}(y') = \{x \in X | f(x) \in Y'\}$;

$X' \subset X \Rightarrow f^{-1}(x') = \{f(x) | x \in X\}$;

$f|'_x : X' \to Y$.

$\Gamma_f|'_x = \Gamma \cap (X' \times Y)$

$Y' \subset Y$ — любое подмножество.

f — сюръективна, если $Im\ f = Y \Leftrightarrow \forall y \in$

$Y \exists x \in X : f(x) = y$ (если $f(x) = y$ имеет хотя бы одно решение).

$f : R \to R_{\geq 0}$ — «подмаска» для $f(x) = x^2$.

$\forall C \in [f(a); f(b)] \exists c \in [a, b]$, тогда $f(c) = C$.

$2^{\sqrt{2}} = 2^{\lim\limits_{n\to\infty} a_n} =? \lim\limits_{n\to\infty} 2^{a_n}$

$f : Z \times Z \to Z$;
$f(x, y) = 4x + 9y$;
$f(-2, 1) = 1$;
$f(-2k, k) = k$ — доказательство сюръективности функции $f(x, y) = 4x + 9y$.

f — инъективна, если $\forall y \in Y \ |f^{-1}(y)| \leq 1 \Leftrightarrow (f(x_1) = f(x_2) \Rightarrow x_1 = x_2) \Leftrightarrow \forall y \in Y$ уравнение $f(x) = y$ имеет меньше или одно решение.

f — биективна, если сюръективна и инъективна одновременно, т.е. $f(x) = y$ имеет ровно 1 решение при любом y.

Если $f : X \to Y$ — биекция, то $\exists f^{-1} : Y \to X : f^{-1}(f(x)) = x$ и $f(f^{-1}(y)) = y$

$\sin x$ — не биекция, ибо:

$\arcsin(\sin(x)) \neq x$;
$\sin(\arcsin(x)) = x$;

Нахождение обратной функции:
$f(x) = e^{x^3}$ решить $e^{x^3} = y \Leftrightarrow x^3 = lny \Leftrightarrow x = \sqrt[3]{ln(y)} \Leftrightarrow g(y) = \sqrt[3]{ln(y)}$.

Конец первой лекции.

$x = \sqcup_{i \in I} X_i$ (I — множество индексов).
$x = \cup_{i \in I} X_i$ и $X_i \cap X_j = \varnothing \ \forall i \neq j$;
$f : X \to Y$;
$x = \sqcup_{y \in Y} \ f^{-1}(y)$
$n - const; n \in N$;
f — ничего не понятно
$f(k) = k\%n$ (остаток от деления).

Отношением на множестве X называется произвольное подмножество $R \leq X \times X$ (где $x \in X, \ y \in Y$)
Вместо (x, y) пишут xRy, где R — бинарная операция.

Например, отношение $\geq$ на R (множество вещественных чисел).

Свойства отношений:

1) Рефлексивность: xRx, $\forall x \in X$. ($\geq$ - рефлексивно, а $>$ — нет (т.е. в этом отношении есть прямая $y = x$));

2) Симметричность: $xRy \Leftrightarrow yRx$ $\forall (x, y) \in X$. (Т.е. картинка симметрична относительно прямой $y = x$);

3) Антисимметричность: $\{xRy,\ yRx\} \Rightarrow x = y$;

4) Транзитивность: $\{xRy, yRz\} \Rightarrow xRz$;

— важнейшее.

Наиболее часто встречающиеся виды отношений:

Отношение эквивалентности — отношение, обладающее свойствами рефлексивности, симметричности и транзитивности.

Отношение частичного порядка — отношение, обладающее свойствами рефлексивности, антисимметичности и транзитивности.

Пример: отношение делимости (вставить

символ делимости) на N_0 (с оговоркой, что 0 (символ делимость) 0 (ноль делится на ноль))

На $Z(n \in N)$:
$a \sim_n b \Leftrightarrow (a-b) \vdots n$
$\{(a-b) \vdots n, (b-c) \vdots n\} \Rightarrow (a-c) \vdots n$ (доказательство транзитивности.)

$a \sim_n b$ можно записывать как $a \equiv b (mod\, n)$. Читается как «a сравнимо с b по модулю n», где модуль — то, на что мы делим.

«$\sim$» — отношение эквивалентности на множестве X, $x \in X$

$\bar{x} = y \in X | y \sim x$ — класс эквивалентности.

Теорема
$\bar{x} \cap \bar{z} = \varnothing$ или $\bar{x} = \bar{z}$ — *Возможно, "не равно"?*
Доказательство:

Пусть $y = (\bar{x} \cap \bar{z})$, т.е. $(y \sim x, y \sim z) \Rightarrow x \sim z$;

$\forall t \in \bar{X} : t \sim x \sim z \Rightarrow t \sim z \Rightarrow t \in \bar{Z}$, т.е. $\bar{x} \leq \bar{z}$. Аналогично $\bar{z} \leq \bar{x}$.

$X = \sqcup_{x \in X'} \bar{x}$, где X' — некое подмножество X.

X' — множество представителей классов эквивалентности.

$(a - b) \vdots n$

$a = a_1 n + a_2$

$b = b_1 n + b_2$, где $a_2,\ b_2$ — остатки от деления на n

$(a - b) \vdots n \Leftrightarrow (a_2 - b_2) \vdots n\ (a_2 = b_2)$.

Класс эквивалентности по $mod(n)$ (класс сравнения по $mod(n)$) — множество всех чисел $k + nZ$, где k — остаток от деления $(k = 0, ..., n - 1)$.

n-арная операция на множестве X – это функция из $\{X \times ... \times X\}(n \text{ раз }) \to X$.

У нас будут нулярные, унарные и бинарные операции.

$\sum_{n=1}^{0} a_n = 0$, т.е. $\varnothing \times X = \varnothing$;
$\prod_{n=1}^{0} a_n = 1$, т.е. $\{*\} \times X = \{(*, x)(x \in X)\}$

Нулярная операция — функция от одноточечного множества $\{*\} \to X$ (Элемент множества X).

G — множество, $*$ — бинарная операция (абстрактная).

$G, *$ — группа, если:

1) $a * (b * c) = (a * b) * c \; \forall a, b, c \in G$;

2) $\exists e$ нейтральный элемент $\in G$, $e * a = a * e = a \; \forall a \in G$;

3) $\forall a \in G \; \exists a' \in G : a * a' = e$

$(G, *)$, удовлетворяющее аксиоме (1) называется полугруппой, а $(G, *)$, удовлетворяющее аксиомам (1) и (2) — моноидом.

4) $a * b = b * a \; \forall a, b \in G$

Если $(G, *)$ удовлетворяет аксиомам (1), (2), (3), (4), то группа называется коммута-

тивной (абелевой).

R — множество, «$+$» «$\cdot$» — бинарные операции на R.

R — кольцо, если:
1) $a + (b + c) = (a + b) + c$;
2) $\exists 0 \in R : a + 0 = a$;
3) $\forall a \ \exists(-a) : a + (-a) = 0$;
4) $a + b = b + a$;
5) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
6) $a \cdot (b+c) = a \cdot b + a \cdot c$, $(b+c) \cdot a = b \cdot a + c \cdot a$;
—
7) $\exists 1 \in R : 1 \cdot a = a \cdot 1 = a$ (кольцо с единицей);
8) $a \cdot b = b \cdot a$ (коммутативное кольцо);
9) $\forall a \neq 0 \ \exists a^{-1} : a \cdot a^{-1} = 1$;
10) $0 \neq 1$;
Множество $((R, +, \cdot))$, удовлетворяющее всем 10 аксиомам называется полем.

Конец второй лекции.

Z — кольцо целых чисел.

F[x] — кольцо многочленов из поля F.

$0 \cdot a = 0$ ($\forall$ кольца).

X — группа или кольцо.

$Y \subseteq X$.

Определение:

Y называется подгруппой или подкольцом, если оно является группой или кольцом относительно операций, заданных в X.

Предположение: $Y \subseteq X$

Y является подгруппой (подкольцом) X тогда и только тогда, когда оно замкнуто относительно операций:

Для группы:

-Групповая операция и взятие обратного по сложению.

Для кольца:

-Сложение, умножение и взятие обратного по сложению

Пример:
$X = Z$.
$Y = nZ = \{n \cdot k | k \in Z\}$.
$I^2 = \{r^2 | r \in I\} = \{\sum r_i, p_i | r_i, p_i \in I\}$ — *отвлечение*

$R[x]$, $R[x^2]$ — подкольцо (многочлены от x^2).
$xR[x]$ — подкольцо.
$Z + xR[x]$ — подкольцо с единицей.

Прямое произведение:
X, Y — группы (кольца).
$X \times Y = \{(x, y) | x \in X, y \in Y\}$.
$(a, b) *_{x,y} (a *_x c, b *_y d)$.

Если X и Y «аддитивные» структуры (то есть их можно складывать), то вместо $X \times Y$ пишут $X \oplus Y$ (прямая сумма).

R — поле вещественных чисел.

$R \oplus R$ $(1,0)(0,1) = (0,0)$

Прямая сумма колец — не самая хорошая операция, т.к. вызывает гадости:

Гадость 1: Произведение двух ненулевых элементов равно нулю.

Определение: $a \neq 0$ — левый делитель нуля, если $\exists b \neq 0 : ab = 0$.

Кольца без делителей нуля — области целостности.

Гадость 2: $(1,0)^2 = (1,0)$

Определение: если $e = e^2$, то e — идемпотент.

X, Y — группы либо кольца.

$\varphi : X \to Y$

Определение: φ — гомоморфизм, если $\varphi(a *_x b) = \varphi(a) *_y \varphi(b)$ $\forall$ бинарной операции $*$.

Предположение:

Группы:

$\varphi(e_x) = e_y$;

$\varphi(a^{-1}) = \varphi(a)^{-1}$.

Кольца:
$\varphi(0) = 0$;
$\varphi(-a) = -\varphi(a)$
Для колец с единицей необязательно $\varphi(1) = 1$.

$\varphi, \chi : R \to R \oplus R$
$\varphi(r) = (r, r)$ — группа.
$\chi(r) = (r, 0)$
Доказательство:
$\varphi(e) = \varphi(e, e) = \varphi(e) \cdot \varphi(e)$
$\varphi(e)\varphi(e^{-1}) = \varphi(e) \cdot (\varphi(e)\varphi(e)^{-1} \Rightarrow e_y = \varphi(e_x)$.

$X = (Z; +)$;
$Y = (R; \cdot) = (R \setminus \{0\}, \cdot)$;
$\varphi : X \to Y$;
$\varphi(n) = (-1)^n$;
$\varphi(m + n) = (-1)^{m+n}$ (1)
$\varphi(m) \cdot \varphi(n) = (-1)^m \cdot (-1)^n$ (2)
Если (1) и (2) равны, то это — гомоморфизм.

Мономорфизм — инъективный гомоморфизм;

Эпиморфизм — сюръективный гомоморфизм;

Изоморфизм — биективный гомоморфизм;

Эндоморфизм — гомоморфизм в себя ($X \to X$);

Автоморфизм — изоморфизм в себя.

Образ гомоморфизма = образ функции.

$Im\varphi = \{\varphi(x) | x \in X\} \subseteq Y$;

$\varphi : X \to Y$;

Ядро (Kernel)

$\ker \varphi = \{x \in X | \varphi(x) = e_y$ (для группы) $, \varphi(x) = 0$ (для кольца) $\}$.

Для:

$\{\varphi : X \to Y; \varphi(n) = (-1)^n\} \Rightarrow \ker \varphi = 2Z$

Решение:

$\varphi(n) = 1 \Leftrightarrow (-1)^n = 1 \Leftrightarrow n$ —четное.

Ядро всегда содержит нейтральный элемент.

$\varphi(e) = x$; $x \cdot x = \varphi(e) \cdot \varphi(e) = \varphi(e + e) = \varphi(e) = x$. Если $x^2 = x$, то, применив умножение на обратный элемент, получим $x^2 =$

$x \Rightarrow x^{-1}x^2 = x^{-1}x \Rightarrow x = e.$

Определение: Подгруппа H в группе G называется нормальной (инвариантной), если $\forall h \in H$ и $g \in G : g^{-1}hg \in H$ для коммутативных групп все подгруппы нормальные.

$\{1\}$ — всегда нормальная группа.

G — всегда нормальная группа.

Определение:

$I \subseteq R$ называется двусторонним идеалом, если $\forall x, y \in I,\ \forall r \in R : (x + y, -x \in I), (rx \in I, xr \in I)$

Пример:

Если R — коммутативное кольцо, rR — идеал для кольца $\mathbb{Z}$ идеал $n\mathbb{Z}$

Рассмотрим кольцо $\mathbb{Z}$ и его идеал (ядро) $n\mathbb{Z}$, где $n = 5$. В кольцо у нас входят числа $-7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7$. В ядро входят числа $-10, -5, 0, 5, 10$. Для того, чтобы каждый элемент ядра отображался в нейтральный элемент кольца (0), мы должны взять элемент ядра и умножить его

на обратный элемент ядра: $-5 \cdot 5 = 0$.

$xF[x]$ — идеал в кольце многочленов.
$X \subseteq Y$ — подмножество.
$X \leq Y$ —подгруппа, полукольцо.
$X \trianglelefteq Y$ — нормальная подгруппа, двусторонний идеал.

Предположение:
$\ker \varphi$ — нормальная подгруппа или двусторонний идеал, если $\forall g \in G : gH = Hg \Leftrightarrow H = g^{-1}Hg \Leftrightarrow \forall h \in H : g^{-1}hg \in H$. Это означает, что $gh_1 = h_2g$ в некоторых группах (Это НЕ КОММУТАТИВНОСТЬ!!!) *(Thank you, Даша)*
$g^{-1}Hg \subseteq H$
$gHg^{-1} \subseteq H$
$H \subseteq g^{-1}Hg$
где $g \cdot H = \{gh | h \in H\}$

$\trianglelefteq$ — является нормальной подгруппой.

Конец третьей лекции.

Перестановки

S_3 — перестановки на множестве $\{1, 2, 3\}$

Запись перестановки в циклическом виде (циклической форме):

σ — перестановка, функция из множества (1, 2, 3) в себя

$\sigma = (i_1, ...i_k)$ означает, что

$\sigma(i_1) = i_2, \sigma(i_2) = i_3, \sigma(i_{k-1}) = i_k, \sigma(i_k) = i_1$;

$(1\ 2\ 3)^2$

$\sigma = (1\ 2\ 3)$

$\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 1$

$\sigma^2(1) = \sigma(\sigma(1)) = \sigma(2) = 3$. (единица перешла в тройку)

$\sigma^2 = (1\ 3\ 2)$.

1 2 3 4 5 6 |

2 4 5 1 6 3 |= (1 2 4) (3 5 6) — независимый цикл

Упражнение (на доп. баллы):

$\sigma = (i_1, ...i_k), \tau \in S_n$.

Вычислить (записать в циклической форме) $\tau^{-1}\sigma\tau$.

Пример не нормальной подгруппы:

Возьмем $\sigma = (1\ 2)$ — транспозиция,

$H = e, \sigma < S_3$, e — нейтральный элемент.

сопрягаем элемент сигма:

$\tau = (1\ 3) = (3\ 1) = \tau^{-1}$

$\tau^{-1}\sigma\tau = (1\ 3)(1\ 2)(1\ 3) = (1)(2\ 3) \notin H$ (один осталось на месте, два перешло в один, один перешло в три, значит, два перешло в три)

$\tau\sigma\tau\ (1) = \tau\sigma(3) = \tau(3) = 1$

$\tau H = \{\tau, \tau\sigma\} = \{(1\ 3), (1\ 2\ 3)\}.$

$H\tau = \{\tau, \sigma\tau\} = \{(1\ 3), (1\ 3\ 2)\}.$

Как видно, левый смежный класс не совпадает с правым смежным классом, то есть не является нормальной подгруппой.

$\{e, (1\ 2\ 3), (1\ 3\ 2)\} \trianglelefteq S_3$

Цикл длины 3 в кубе дает единицу.

$\varphi : G \to F$

$H = \ker\varphi = \{g \in G | \varphi(g) = e\} = \varphi^{-1}(e)$, e — нейтральный элемент.

Лемма:

$\ker\varphi$ — нормальная подгруппа.

Доказательство:

$\forall h_1, h_2 \in H : h_1 \cdot h_2 \in H,\ h_1^{-1} \in H$

$\forall g \in G : g^{-1}hg \in H$ — нужно доказать.

Дано: $\varphi(h_1) = \varphi(h_2) = e$

Доказать:

$\varphi(h_1, h_2) = e$

$\varphi(h_1^{-1}) = e$

$\varphi(g^{-1}h, g) = e$

Докво:

1)$\varphi(h_1 \cdot h_2) = \varphi(h_1) \cdot \varphi(h_2) = e \cdot e = e$

2)$\varphi(h^{-1}) = \varphi(h)^{-1} = \varphi(h) \cdot \varphi(h)^{-1} = e$

3) $\varphi(g^{-1}h_1 \cdot g) = \varphi(g^{-1}) \cdot \varphi(h_1) \cdot \varphi(g) = e$ (т.к. $\varphi(g^{-1})$ и $\varphi(g)$ уничтожаются (их произведение равно e)).

Это доказательство непосредственной проверки.

R — кольцо,

$I \subseteq R$, то I — идеал в R

Примером идеала в множестве целых чисел является множество чисел, делящихся на фиксированное число.

I — идеал в R, если I — аддитивная подгруппа (подгруппа к операции сложения) и $\forall r \in R, s \in I$ $rs, sr \in I$. (кольцо с идеалом чаще всего коммутативно).

Лемма: $\varphi : R \to A$ — гомоморфизм колец, тогда $\ker \varphi$ — двусторонний идеал в R.

Доказательство — непосредственная проверка.

В случае гомоморфизма колец ядро — прообраз нуля ($\ker \varphi = \varphi^{-1}(0)$)

Отвлечение (почему идеал)

$a + b\sqrt{d}, a, b \in Z$, где d — фиксированное целое.

$xR + yR$ — тоже идеал, но не соответствует числу. x, y — идеальные числа.

К этому мы вернемся довольно скоро (зловещий смех).

Предложения: $\varphi : G \to F$ — гомоморфизм групп.

$\varphi(g) = f \in F$

тогда $\varphi^{-1}(f) = g \cdot \ker \varphi$

Доказательство:

$\varphi(g \ker \varphi) = \varphi(g) \cdot \varphi(\ker \varphi) = \varphi(g) = f$.

$g_1 : \varphi(g_1) = f = \varphi(g) \Rightarrow \varphi(g^{-1}g_1) = e \Rightarrow g^{-1}g_1 \in \ker \Rightarrow g_1 \in g \cdot \ker \varphi$.

Теорема Лагранжа.

Лемма: $H \trianglelefteq G$ — группа

$\forall g_1, g_2 \in G$, g_1H равномощно g_2H.

Доказательство:

$\varphi : H \to g_1H$, $\varphi(h) = g_1h, h \in H$ — биекция.

$\varphi^{-1}(x) = g_1^{-1}x$.

Количество элементов в группе — порядок группы.

Лемма: $H \leq G, g_1, g_2 \in G$
$g_1H \cap g_2H = \varnothing$ или $g_1H = g_2H$
Доказательство:
$g \in g_1H \cap g_2H$,
$g = g_1h_1 = g_2h_2$ для $h_1, h_2 \in H$, тогда
$g_1 = g_2h_2h_1^{-1}$
$\forall h \in H : g_1h = g_2(h_2h_1^{-1}h) \in g_2H \Rightarrow g_1H \subseteq g_2H$

Теорема Лагранжа:
Порядок подгруппы является делителем порядка группы.
$H \leq G$
$|G| = |H| \cdot |G : H|$, где $|G : H|$ — количество смежных классов.

Конец четвертой лекции.

Доказательство т. Лагранжа: $H \leq G$, $|G| < \infty$
$H_1 = H, H_2, ...H_m$ — левые смежные классы по H.
$G = \sqcup_{i=1}^{m} H_i \Rightarrow |G| = \sum\limits_{i=1}^{m} |H_i| = \sum\limits_{i=1}^{m} |H| = m \cdot |H|$,

а $m = |G : H| = |G/H| = |H\backslash G|$ — количество смежных классов.

$\sqcup$ — дизъюнктное (непересекающееся) объединение.

Класс смежности: зафиксировали элемент группы и умножаем его на все элементы подгруппы (Запись: gH, где g — элемент группы, H — подгруппа.)

В каждом классе смежности содержится столько же элементов, сколько содержится в подгруппе.

Одна из важнейших конструкций в алгебре:

Теорема: $H \trianglelefteq G$, H — нормальная подгруппа, G группа.

Тогда существует сюръективный гомоморфизм (эпиморфизм) $\varphi : G \twoheadrightarrow F$, такой что $\ker \varphi = H$. Если $\varphi' : G \twoheadrightarrow F$ — гомоморфизм с ядром H, то существует единственный изоморфизм, $\Theta : F \to F'$, такой что $\varphi' = \Theta \circ \varphi$

Диаграмма (ориентированный граф, вершины помечены математическими объектами, а стрелки - отображениями этих объектов) называется коммутативной, если для любых вершин A, B и любых двух путей из A в B композиции отображений по каждому из них равны.

Лемма: $\varphi : G \to F$, $H = \ker \varphi$

$\varphi(g) = f$, $\varphi^{-1}(f) = gH = Hg$.

Конструкция для доказательства существования:

$F = \{gH | g \in G\}$;

$\varphi(g) = gH$

$gH \cdot g_1H = gg_1H$

$h_1h_2 \in H : gh \cdot g_1h_1 = gg_1g_1^{-1}hgh_1$, здесь $g_1^{-1}hg \in H$, $gh \cdot g_1h_1 \in gg_1H$

Следовательно,

$gH \cdot g_1H = g(Hg_1)H = g(g_1H)H = gg_1(H \cdot H) = gg_1H$

("Почему он использует магию вне Хогвартса?" (с) Виталя)

$G/H = \{gH | g \in G\}$, $G/H = H/G$ — так как H — нормальная подгруппа.

$\rho_H : G \to G/H$ по $modH$.

Следствие (теорема о гомоморфизме):

$\varphi : G \to G'$

$G \twoheadrightarrow G/H$ и $G \twoheadrightarrow Im\varphi$, $G/H \sim Im\varphi$.

Образ φ изоморфен фактормножеству по $\ker\varphi$.

$Im\varphi \cong G/\ker\varphi$, т.ч. $\varphi' = \Theta \circ \varphi$.

R — кольцо, I — двусторонний идеал. Теперь все то же самое делаем для колец.

R/I — факторкольцо, т.е. $R/I = \{r + I | r \in R\}$

$(r+I)(r_1+I) := rr_1 + I$

$t, t_1 \in I : (r+t)(r_1+t_1) = rr_1 + rt_1 + tr_1 + tt_1, \in rr_1 + I$, где $rt_1, tr_1, tt_1 \in I$

$\varphi : R \to A$ — гомоморфизм колец.

$Im\varphi \cong R/ker\varphi$ — теорема о гомоморфизме колец.

(Вместо слова «группа» — «кольцо», вместо «нормальной подгруппы» — «двусторонний идеал». Все остальное та же дичь).

Пример:

$Z_n = \{0, ..., n-1\},\ +modn,\ -modn$

В Z_5 $3+4=2$, $3 \cdot 4 = 2$

$\varphi : Z \to Z_n$

$\varphi(x) = x \cdot modn$

$(x+y)modn = (xmodn + ymodn)modn$

Найдем ядро:

$\varphi(x) = xmodn = 0 \Leftrightarrow x \vdots n \Leftrightarrow x \in \ker\varphi$

$Z/nZ \cong Z_n$ — факторкольцо, где $Z/nZ = \{0 + nZ, 1+nZ, ..., n-1+nZ\}$, Z_n — множество элементов, делящихся на n.

Пример:

$Z/5Z$ $\{0, 1, 2, 3, 4\}$ — множество представителей смежных классов.

$3 + 4 = 7 \in 2 + 5Z$.

Кольцо многочленов:
$R[x]$, $I = \{p | p(0) = 0\} = xR[x]$
$R[x]/xR[x]$ — факторкольцо.
$\alpha_0 + \alpha_1 x + ... + \alpha_n x^n$.
Строим гомоморфизм $\varphi : R[x] \to R$;
$\varphi(p) = p(0)$
Получаем, что
$R[x]/xR[x] = R$

$\to$ — тупо стрелка.
$\twoheadrightarrow$ — сюръекция.
$\rightarrowtail$ — инъекция.
$\tilde{\to}$ — биекция.
$\hookrightarrow$ — вложение подмножества в множество.
$\mapsto$ — «отображается в» ($f : X \to Y$ отображает $x \mapsto f(x)$)

Конец пятой лекции.

Алгоритм деления с остатком:
в $\mathbb{Z} : \forall a, b \; \exists c, r : a = bc + r, |r| < |b|$;
В кольце многочленов, где $F[x]$ — поле:
$F[x] : \forall a, b \neq 0 \; \exists c, r : a = bc + r, \; \deg r < \deg b, \; a, b$

— многочлены, deg — степень многочлена.

Рассмотрим произвольное Евклидово кольцо:

Будем считать, что у нас задано: пусть кольцо R — коммутативная область целостности с единицей.

Область целостности — это кольцо, в котором можно сокращать на элементы. В области целостности $\forall r \neq 0\ ra = rb \Leftrightarrow a = b$. Доказательство: $r(a-b) = 0 \Leftrightarrow a - b = 0$.

Замечание:

Два элемента кольца называются ассоциированными, если a делится на b и наоборот: $a, b \in R$, a ассоциировано с b если $a \in bR$, и $b \in aR$ или, что то же самое, $aR = bR$ ($aR,\ bR$ — идеалы).

Если $aR = bR$, R — область целостности (при $a \neq 0$), то:

$a = bx,\ b = ay,\ \Rightarrow a = ayx \Leftrightarrow yx = 1$. ($x, y$ — обратимые элементы).

А при $a = 0$:

$bR = \{0\} \Rightarrow b = 0 \Rightarrow a = b \cdot 1$.

Пусть $f : R \to \mathbb{N}_0 \cup \{-\infty\}$, такая, что:

1) $f(0) < f(r)\ \forall r \in R \setminus \{0\}$

2) $\forall a, b \in R\ \exists c, r \in R :\ f(r) < f(b)$ и $a = bc + r$.

Если такая функция существует, то R называется евклидовым кольцом, ну а f называется евклидовой

нормой.

Определение: Главный идеал кольца — идеал, порожденный одним элементом, то есть идеал вида aR. R называется кольцом главных идеалов, если любой идеал является главным.

Теорема: Любое евклидово кольцо является кольцом главных идеалов.

Доказательство: $I \trianglelefteq R$ (произвольный идеал). Пусть a — ненулевой элемент идеала I, такой, что $f(a) \leq f(b)\ \forall b \in I \setminus \{0\}$

Возьмем произвольный элемент $d \in I \setminus \{0\}$. Тогда по условию евк. кольца, $\exists c, r \in R : d = ac + r,\ f(r) < f(a)$.

Но $r = d - ac$ (a лежит в идеале, соответственно, ac также лежит в идеале, d лежит в идеале, ну, значит, r тоже лежит в идеале)

Если $r \neq 0$, то $f(r) < f(a) \leq f(r)$ — противоречие. ($r = 0$, то есть $d = ac \in aR$).

Из всего предыдущего мы получили, что:

$I \subseteq aR,\ a \in R \Rightarrow aR \subseteq I \Rightarrow I = aR$.

Основная теорема арифметики.

Определение: Элемент $p \in R$ называется непри-

водимым, если p необратим и если выполнено следующее условие: $p = ab$ влечёт p ассоциировано с a или с b ($p = ab$ влечёт a или b — обратимо).

Определение: Идеал I — простой, если выполнено следующее условие: $ab \in I \Rightarrow a \in I$ или $b \in I$.

Идеал $2 \cdot 3 \in 6\mathbb{Z}$ не является простым, т.к. $2, 3 \notin 6Z$.

$\{0\}$ — простой идеал любой области целостности.

$17\mathbb{Z}$ — простой в $\mathbb{Z}$.

Определение: Элемент кольца $p \in R$ называется простым, если идеал pR — простой.

Возьмем $R = \mathbb{Z}$ (кольцо целых чисел). Идеалы типа $17\mathbb{Z}$ будут являться простыми, т.к. 17 делится только на самого себя и единицу, а $17 \in 17\mathbb{Z}$. Следовательно, элементы простого идеала в кольце целых чисел являются простыми числами!

Плохое кольцо:

$\mathbb{Z}(\sqrt{5}) = \{a + b\sqrt{5} | a, b \in \mathbb{Z}\}$.

$(3 + \sqrt{5})(3 - \sqrt{5}) = 4 = 2 \cdot 2 \in 2R$ («двойка — неразложимый элемент этого кольца. я верю в это!»)

Произведение двух элементов, не лежащих в $2R$ лежит в $2R$, значит, $2R$ — не простой идеал. (2 — неприводимый элемент кольца).

(Пояснение: $(3 + \sqrt{5})$ и $(3 - \sqrt{5})$ не лежат в $2R$, а их произведение 4 лежит в $2R$, следовательно, $2R$ — не простой идеал, т.к. 4 можно разложить как $(3 +$

$\sqrt{5})(3-\sqrt{5}))$

$a+b\sqrt{5}(a-b\sqrt{5})c=(a^2-5b^2)c=2$ («плохой пример. надо было взять $\sqrt{-5}$. Но я ничего доказывать не буду»). — неясно, нужно или нет.

Лемма: Если R — кольцо главных идеалов, то любой неприводимый элемент является простым (простой неприводим всегда). Обратное верно всегда.

Доказательство:

Надо доказать: если произведение $ab \in xR$, то либо $a \in xR$, либо $b \in xR$.

От противного: пусть $a \notin xR$, либо $b \notin xR$.

Тогда: $aR + xR = a'R$, так как $\forall$ идеал главный.

$x \in a'R$, т.е. $x = a'x'$. Одно из них должно быть обратимо. Либо обратимо a', и тогда $a'R = R$. Либо $x'R$ обратимо, то $a'R = xR$, тогда $a \in a'R = xR$ — противоречие. Следовательно, что $aR + xR = a'R = R$.

Аналогично $bR + xR = R$.

Кольцо, в котором нельзя разложить число на простые множители (WHAT?)

$R = \mathbb{Z}[x_n : n \in \mathbb{N}]/(x_n - x_{n+1}^2)_{n\in\mathbb{N}}$

В новом кольце R нет элементов

$\bar{x_n}$ — смежный класс x_n

В кольце очевидно выполнено равенство:

$\bar{x_1} = \bar{x_2}^2 = \bar{x_3}^4 = ... = \bar{x_n}^{2^{n-1}}$

Конец шестой лекции.

Теорема арифметики (основная).

Пусть R — область главных идеалов, то есть каждый идеал порожден одним элементом. Тогда $\forall r \in R \; \exists$ неприводимые элементы $p_1, ..., p_m \in R$ и $\varepsilon \in R^*$: $r = \varepsilon p_1, ..., p_m$.

При этом: $\varepsilon p_1, ..., p_m = \delta q_1 \cdot ... \cdot g_n$, $\varepsilon, \delta \in R^*$, а p_i, q_i неприводимы, то $m = n$ и $\exists \sigma \in S_n : p_i$ ассоциировано с $q_{\sigma(i)} \forall i = 1, ..., n$.

Лемма:

R — область целостности, p и q — ассоциированы, $\Leftrightarrow p = qx$ для некоторого $x \in R^*$

Доказательство:

p и q ассоциированы, если $p \vdots q$ и $q \vdots p$, то есть $pR = qR$.

$p = qx, q = py \Rightarrow p = pxy \Leftrightarrow p(1 - xy) = 0,$

следовательно, R — область целостности, $p \neq 0 \Rightarrow 1 - xy = 0$.

Лемма 1: R — область главных идеалов, тогда $\forall r \in R \; \exists$ неприводимые элементы $p_1, ..., p_m \in R$ и $\varepsilon \in R^* : r = \varepsilon p_1, ..., p_m$. (Пример: $4 = 1 \cdot 2 \cdot 2 = (-1) \cdot (-2) \cdot 2$)

Возьмем идеал, порожденный R и максимальный идеал.

Определение: идеал M называется максимальным, если он максимальный из идеалов $\neq R$, т.е. $\forall M' \supsetneqq M : M' = R$.

Лемма 2: Любой максимальный идеал является простым идеалом.

Доказательство леммы 2: $a, b \in R$, такие, что $ab \in M$ (M — максимальный идеал). Предположим, что $a \notin M$.

Посмотрим на идеал $M \supsetneqq M + aR \Rightarrow$т.к. M — максимальный идеал, то $M + aR = R$.

$M \supseteq bM + baR = bR \ni b$.

$n\mathbb{Z}$, если n необратимо и $n = mk$, то $m\mathbb{Z} \geq n\mathbb{Z}$. Если идеал порожден простым числом, то он не содержится ни в каком другом идеале.

Если $p\mathbb{Z} \subseteq q\mathbb{Z} \Rightarrow p = g - k \Rightarrow g = \pm 1 \Rightarrow g\mathbb{Z} =$

$\mathbb{Z}$ или $k = \pm 1 \Rightarrow g\mathbb{Z} = p\mathbb{Z}$.

В кольце главных идеалов любой ненулевой простой идеал максимален.

$R = \mathbb{R}[x, y]$, то идеалом будет $xR \subsetneqq xR + yR$.

Лемма 3: $\forall$ идеал $I + R$ содержится в некотором максимальном идеале.

(Лемма Цорна) Примите без доказательства.

Доказательство леммы 1:

Напоминаем: мы хотим разложить кольцо в неприводимых элементов.

$rR \subseteq M$, если r — собственный $\Leftrightarrow$ r необратим.

M — простой, $M = p_1 R$, следовательно, p_1 — простой (неприводимый) элемент.

$r = p_1 r_1$; если r_1 обратим, то всё доказано (сведется к $r = \varepsilon p_1$), иначе аналогично: $r_1 = p_2 r_2$, где p_2 неприводим. Продолжим процесс. Дойдем до $r_k = p_{k+1} r_{k+1}$ и так далее. Если процесс оборвется на каком-то шаге k, то все будет доказано.

Обратим внимание, что $r = p_1 r_1 = p_1 p_2 r_2 = ... = p_1 p_2 ... p_k r_k$.

Если $r_k \in R^*$ для некоторых $k \in \mathbb{N}$, то все доказано.

Сейчас докажем, что такой процесс обязательно

прервется. Предположим обратное: ни один $r_k \notin R^*$

$rR \subseteq r_1R \subseteq r_2R \subseteq ... \subseteq r_kR \subseteq ....$

Возьмем объединение этой цепочки: $I = \cap_{k=1}^{\infty} r_kR$ — идеал (простое упражнение)

$I = qR \Rightarrow q \in r_jR$ для некоторого $j \in \mathbb{N}$

$qR \subseteq r_jR$

$r_jR \subseteq I = qR$, следовательно,

$qR = r_jR = r_{j+1}R = r_{j+2}R = ...$

Получили, что $r_j = r_{j+1}p_{j+1}$

Из двух предыдущих равенств следует, что $p_{j+1} \in R^*$.

Противоречие.

Определение: R — нёторово кольцо, если возрастающая цепочка идеалов обрывается: $I_1 \subseteq I_2 \subseteq ... \subseteq ...I_k \subseteq ...$, то $\exists j : I_j = I_n \ \forall n > j$

Лемма (упражнение (на бб)): R — нёторово, $\Leftrightarrow \forall$ идеала $I \ \exists r_1, r_2, ...r_k \in I$, таких что $I = \sum_{i=1}^{k} r_iR$

Вопрос: Верно ли, что в любом нёторовом кольце имеет место быть разложение на неприводимые множители?

Лемма 4 R — область целостности и $\forall$ неприводимый элемент является простым. (В частности, это

выполнено, если R — область главных идеалов.)

Тогда имеет место единственность разложения на неприводимые: $\varepsilon p_1 \cdot ... \cdot p_m = \delta q_1, ...q_n$, где $\varepsilon, \delta \in R^*$, p_m, q_n — неприводимые, то $\exists \sigma \in \delta_n : P_k$ ассоциированос $q_{\sigma(k)} \forall k$.

Доказательство: индукция по $min(m, n)$

(считаем, что $m < n$)

Произведение элементов обратимо, если обратимы все элементы. Если произведение обратимо ($ab \cdot c = 1$, ab — обратимо).

$m = 0$, то $\delta q_1 \cdot ... \cdot q_n \in R^* \Rightarrow n = 0$.

$m > 0$, тогда $deltaq_1 \cdot ... \cdot q_n \in pR$ — простой. (собственный идеал не может содержать обратимых элементов).

Таким образом, $q_k \in p_1 R$. $q_k = p_1 r \notin R^*$, отсюда $r \in R^*$, значит, p_1 ассоциировано с q, $\varepsilon p_2 \cdot ... \cdot p_m = \delta q_1 \cdot ... \cdot q_{k-1} \cdot q_{k+1} \cdot ... \cdot q_n$.

По индукционному предположению $m - 1 = n - 1$ и

$\exists \tau : \{2, ..., m\} \to \{1, ..., k-1, k+1, ...n\}$

такое что p_i ассоциировано с $q_{\tau(i)}$

$m = n$, $\sigma(i) = \tau(i)$ при всех $i \neq 1$, $\sigma(1) = k$.

Китайская теорема об остатках

Теорема: $I_1, ..., I_k$ — идеалы кольца R, где R (здесь и далее) — коммутативное кольцо с единицей.

Предполагается, что каждая пара идеалов взаимно простая: $I_j + I_l = R \ \forall j \neq l = 1, ..., k$.

Теорема говорит о том, что $R/(I_1 \cdot ... \cdot I_k) = \oplus_{j=1}^{k} R/I_j$. $\oplus_{j=1}^{k} R/I_j$ — набор остатков от деления на $r_1, ..., r_k$.

Если

$x \equiv 1 \mod 3$

$x \equiv 2 \mod 5$

$x \equiv ? \mod 15$, где $15 = 3 \cdot 5$

Лемма: Если $I_1, ..., I_k$ — попарно взаимно простые, то $I_1 \cdot ... \cdot I_k = I_1 \cap ... \cap I_k$.

Доказательство: Достаточно доказать для $k = 2$ и дальше применить индукционный переход:

$I_1 + I_2 = R$. Заметим, что произведение идеалов всегда содержатся в пересечении. $I_1 \cdot I_2 \subseteq I_1 \cap I_2$.

$x \in I_1 \cap I_2$. $\exists a_1 \in I_1, a_2 \in I_2 : a_1 + a_2 = 1$.

$x = x \cdot 1 = x(a_1 + a_2) = xa_1 + xa_2$, где $x \in I_2, \ a_1 \in I_1, \ x \in I_1, \ a_2 \in I_2$.

Далее перейдем по индукции с использованием следующей леммы:

Лемма Если I_1 взаимно прост с каждым из $I_2, ..., I_k$, то он взаимно прост с их произведением.

Доказательство:

Пусть $k = 3$, $I_1 + I_2 = R$, $I_1 + I_3 = R$. Отсюда $R = I_1 + I_2 \cdot R = I_1 + I_2 \cdot (I_1 + I_3) = I_1 + I_2 I_1 + I_2 I_3 \subseteq I_1 + I_2 \cdot I_3 \subseteq R$.

Дальше индукция по k.

Напомним, что мы хотим доказать, что $R/(I_1 \cdot ... \cdot I_k) \cong \oplus_{j=1}^{k} R/I_j$

Очевидным образом строим гомоморфизм: $\varphi : R \to \oplus R/I_j$

$\varphi(x) = \{r+I_1, ..., r+I_j\}$, где каждый $r+I_1 \in R/I_j$ — гомоморфизм (это легко проверить (использовать, что сумма смежных классов — смежный класс суммы))

$\varphi(x) = 0 \Leftrightarrow r \in I_j \ \forall j \ r \in I_1 \cap ... \cap I_k = I_1 \cdot ... \cdot I_k$ по лемме.

т.е $\ker \varphi = I_1 \cdot ... \cdot I_k$

Пусть $(r_1 + I_1, ..., r_k + I_k) \in \oplus R/I_j$ где $r_i \in R$.

$m : I_m + \prod\limits_{j \neq m} I_j = R$

$b_m + c_m = 1$, где $b_m \in I_m, c_m \in \prod\limits_{j \neq m} I_j = \cap_{i \neq m} I_j$

Положим $x = \sum\limits_{m=1}^{k} r_m c_m$

$\varphi(x) = \sum\limits_{m=1}^{k} \varphi(r_m c_m)$.

$\varphi(r_m c_m) = (..., ..., ...)$

$c_m \in I_j \forall j \neq m \Rightarrow r_m c_m \in I_j$

$\varphi(r_m c_m) = (0, ..., 0, r_m, 0, ..., 0)$

$c_m = 1 - b_m \in 1 + I_m$

$c_m r_m \in r_m + I_m$.

Таким образом, $\varphi(x) = (r_1, ..., r_n, ..., r_k)$.

То есть наше отображение сюръективно, поэтому

по теореме о гомоморфизме мы получаем, что образ изоморфен факторкольцу.

Повторим:
$\varphi : R \twoheadrightarrow A$, то $A \cong R/\ker\varphi$.

Примерчики:
Для целых чисел.
$R = \mathbb{Z}$
$a_1, ..., a_k$ — попарно взаимно простые числа.
тогда $a_1R, ...a_kR$ — попарно взаимно простые.
Почему? Потому что $a_iR + a_jR = pR$. Если a_i взаимно просто с a_j, то $p = 1$, следовательно, R — кольцо.
$\gcd(a_i, a_j) = p$ — «» –?
Китайская теорема об остатках говорит нам о том, что (время закончилось) если если известен смежный класс, то это то же самое, что известен остаток от деления.
$x \equiv r_1 \mod a_1$
...
$x \equiv r_k \mod a_k$
$x = \equiv \sum_{m=1}^{k} r_m c_m \mod a_i \cdot ... \cdot a_k$
$a_m + a_1 \cdot ... \cdot a_{m-1} \cdot a_{m+1} \cdot ... \cdot a_k R = R$, где $a_m \ni b_m$, $a_1 \cdot ... \cdot a_{m-1} \cdot a_{m+1} \cdot ... \cdot a_k R \ni c_m$
$a_m y + d_m z = 1$

Конец седьмой лекции.

$\forall a : \gcd(an) = 1 \Leftarrow a^{\varphi'(n)} \equiv 1 \; mod \; n$

Поэкспериментируем:

Фактически, мы находим $\mathbb{Z}_n \cong \mathbb{Z}/nZ$

$n = 3 \;\; \pm 1^2 = 1$

$n = 4 \;\; \pm 1^2 = 1$

$n = 5 \; 2, 4, 8, 16 \equiv 1, 2^4 \equiv 1$

$3, 4, 2, 6 \equiv 1 \Rightarrow 3^4 \equiv 1$

Определение:

$\varphi(n)$ — количество чисел от $(0, ..., n-1)$, взаимно простых с n.

Эти числа хороши тем, что обратимы по $mod \; n$.

Если $\gcd(a, n) = a$, то наименьший идеал, который их содержит: $a\mathbb{Z} + n\mathbb{Z} = b\mathbb{Z}$. Предположим, что есть идеал, который $b\mathbb{Z} \subseteq c\mathbb{Z}$, то это означает, что

$$\begin{cases} a \vdots b \\ n \vdots b \end{cases} \quad \forall c : \begin{cases} a \vdots c \\ n \vdots c \end{cases} \Rightarrow b \vdots c.$$

То есть $b = \gcd(a, n)$

Определение: $a, b \in R$, R — коммутативное с единицей, $\gcd(a, b)$ — это такой общий делитель a, b, который делится на все остальные общие делители.

Другими словами, если $a \in cR,\ b \in cR \Rightarrow \gcd(a,b) \in cR$, кроме того, $a, b \in \gcd(a,b)R$.

Предупреждение: gcd существует не в любом кольце. В кольце главных идеалов наибольший общий делитель существует всегда.

НОД соответствует наименьшему главному идеалу (чем больше делитель, тем меньше идеал).

Еще раз то же самое, но опять другими словами: $d = \gcd(a,b) \Leftrightarrow dR$ — наименьший главный идеал, содержащий a и b.

НОД — не число! НОД — идеал.

Теорема: Если R —кольцо главных идеалов, то $\forall a, b \in R\ \exists x, y \in R:\ ax + by = \gcd(a,b)$.

Доказательство:

$aR+bR = \{au+bv | u, v \in R\}$ — наименьший идеал, содержащий a, b. А, так как R — кольцо главных идеалов, то этот идеал — главный: $\exists d : aR+bR = dR$.

dR — наименьший главный идеал, содержащий a, b, т.е. $d = \gcd(a,b)$. Т.к. $d \in aR+bR$, то $\exists x, y \in R : d = ax + by$.

Посмотрим на кольцо $\mathbb{Z}/n\mathbb{Z}$. Что означает обратимость элемента в этом кольце?

Договоримся про обозначения в этом кольце. $\mathbb{Z}/n\mathbb{Z} \cong$

$\mathbb{Z}_n = \{0, 1, ..., n-1\}$.

В $\mathbb{Z}_7 : 3 \cdot 4 = 5$, что аналогично $(3 + 7\mathbb{Z})(4 + 7\mathbb{Z}) = 12 + 7\mathbb{Z} = 5 + 7\mathbb{Z}$.

В кольце R с 1:

$1, 1{+}1, 1{+}1{+}1, ...$ может оказаться, что $1{+}1{+}1 = 0$, т.е. это кольцо по модулю 3.

Поэтому пишем «Работаем в R»: после этого целые числа обозначают элементы кольца R: n — это $\underbrace{1 + ... + 1}_{n \text{ раз}}$

$a \in (\mathbb{Z}/n\mathbb{Z})$. Мы хотим понять, обратимо ли оно.

$\exists a' : a \cdot a' = 1$ в $\mathbb{Z}/n\mathbb{Z}$ $(aa' \equiv 1 \mod n)$

$\exists x : a \cdot a' = 1 + nx$ в целых числах.

$aa' - nx = 1$ имеет решение тогда и только тогда, когда $\gcd(a, n) = 1$.

Тогда $(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}_n)^* = \{a | \gcd(a, n) = 1\}$, где $0 \leq a \leq n - 1$.

Поэтому функция эйлера есть ни что иное, как порядок группы: $\varphi = |\mathbb{Z}_n^*|$

$< a >= \{1, a, a^2, ...a^{m-1}\}$

Определение: $a \in G$ — группа.

$ord\, a = | < a > |$ (количество элементов в $\{1, a, a^2, ...a^{m-1}\}$) = наименьшее m, т.к. $a^m = 1$ (порядок элемента)

Лемма: $a^k = 1 \Leftrightarrow k{:}ord\ a$.

Доказательство: $k = ord\ a \cdot l \Rightarrow a^k = (a^{ord\ a})^l = 1^l = 1$.

В обратную сторону: пусть $k = ord\ a \cdot l + r,\ 0 \leq$

$r < ord\ a$

$a^k = a^{(}ord\ a)^l \cdot a^r = a^r$.

Если $r \neq 0$, то $a^r = 1$ противоречит минимальности $ord\ a$. Таким образом, $r = 0$.

$\{1, a, a^2, ...a^{m-1}\} \cong \mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$.

Следствие теоремы Лагранжа:

G — конечная группа, $a \in G$.

$|G|$:$ord\ a$.

Следствие (**Теорема** Эйлера):

$a^{\varphi(n)} \equiv 1 \mod n$. (Если $\gcd(a, n) = 1$)

Доказательство:

$|\mathbb{Z}_n^*| = \varphi(x)$:$ord\ a$. Отсюда, по лемме, $a^{\varphi(n)} = 1$ в $\mathbb{Z}_\ltimes^*$

Вычислим, чему равно $\varphi(n)$.

Если $n = \{q_1, ..., q_m\}$, то q_i попарно взаимно просты. Значит, и идеалы, порожденные ими, попарно взаимно просты. А значит,

$\mathbb{Z}/q_1\mathbb{Z} \cdot ... \cdot q_m\mathbb{Z} \cong \oplus_{i=1}^m \mathbb{Z}/q_i\mathbb{Z}$.

$(a_1, ..., a_m)(a'_1, ..., a'_n) = (1, ..., 1) \Leftrightarrow a_i \in \mathbb{Z}/q_1\mathbb{Z}\ \forall i$.

Следовательно, $(\mathbb{Z}/q_1 \cdot ...q_m\mathbb{Z})^* = \times_{i=1}^m (\mathbb{Z}/q_1\mathbb{Z})^*$

$\varphi(q_1, ..., q_m) = \varphi(q_1) \cdot ... \cdot \varphi(q_m)$;

$q_i = p_i^{k_i}, p_i$ — различные простые.

Конец восьмой лекции.

Теорема: $a^{\varphi(n)} \equiv 1 \mod n \, \forall a, n$, таких, что $\gcd(a, n) = 1$.

Теорема:

1) $\varphi(ab) = \varphi(a)\varphi(b)$, если $\gcd(a, b) = 1$

2) $n = \prod_{i=1}^{m} p_i^{k_i}$, где p_i — различные простые, то

$\varphi(n) = \prod_{i=1}^{m} \varphi(p_i^{k_1})$ — по нему работаем при индукционном переходе.

3) $\varphi(p^k) = p^k - p^{k-1}$ (p — простые)

Доказательство:

1) Пусть $\gcd(a, b) = 1$. Тогда $aR + bR = R$, и тогда по китайской теореме об остатках $R/abR \cong R/aR \oplus R/bR$. Отсюда $(R/abR)^* \cong (R/aR)^* \times (R/bR)$ (в случае мультипликативных групп используется значок прямого произведения). Следовательно $\varphi(ab) = \varphi(a) \cdot \varphi(b)$, где $\varphi(ab) = |(R/abR)^*|$.

2) Индукция по m:

$m = 1$ — левая и правая часть совпадают.

$m > 0$: $a = \prod_{i=1}^{m-1} p_i^{k_i}, b = p_m^{k_m}, n = ab$.

$\gcd(a, b) = 1$, По пункту 1: $\varphi(n) = \varphi(a) \cdot \varphi(b)$.

По индукционному предположению $\varphi(a) = \prod_{i=1}^{m-1} \varphi(p_i^{k_i})$

3) $\gcd(m, p^k) \neq 1 \Leftrightarrow m \vdots p$.

Таких чисел от 1 до p^k в p раз меньше, чем p^k, т.е. p^{k-1}. Это числа не взаимно просты. Тогда взаимно простых чисел $p^k - p^{k-1}$, т.е.

$\varphi(p^k)$(взаимно простые с p^k) = p^k(всего)$-p^{k-1}$(не взаимно прость

Например, $\varphi(60) = \varphi(2^2 \cdot 3 \cdot 5) = \varphi(2^2)\varphi(3)\varphi(5) = (2^2 - 2) \cdot (3 - 1) \cdot (5 - 1) = 2 \cdot 2 \cdot 4 = 16$

Следование: $\varphi(n) = n \cdot \prod_{i=1}^{m} \frac{p_i - 1}{p_i}$, где $p_1, ...p_m$ — все простые делители n.

$\varphi(72) = 72 \cdot \frac{1}{2} \cdot \frac{2}{3} = 24$.

Сравнимость по модулю n — это равенство в $\mathbb{Z}/n\mathbb{Z}$

$a + I$ — смежный класс по I. Или класс вычетов по модулю I. Иногда, если I — простой идеал, то говорят по модулю элемента, которым данный идеал образован.

Доказательство следующей за этим теоремы:

$\mathbb{Z}/n\mathbb{Z} \cong \oplus_{i=1}^{m} \mathbb{Z}/p_i^{k_i}$.

$n = \prod_{i=1}^{m} p_i^{k_i} p_i$ — различные простые.

Примарное число — степень простого числа.

$(\mathbb{Z})^* = \times_{i=1}^{m} (\mathbb{Z}/p_i^{k_i}\mathbb{Z})^*$

Усиленная теорема Лагранжа:

$\times_{i=1}^{m} G_i$, G_i — произвольная группа.

$(x_1, ..., x_m) \in \times_{i=1}^{m} G_i, x_i \in G_i$. Пусть $d_i = ord x_i$

$(x_1, ..., x_m)^l = (x_1^l, ..., x_m^l) = (e_{G_1}, ..., e_{G_m}) \Rightarrow x_i^l = e_{G_i} \forall i \Rightarrow l \vdots d_i$.

Таким образом, $ord(x_1, ..., x_m) = lcm(d_1, ..., d_m)$ (lcm — наименьшее общее кратное).

Таким образом: если $(x_1, ..., x_m) \in \times_{i=1}^{m} (\mathbb{Z}/p_i^{k_i}\mathbb{Z})^*$, то

$(x_1, ..., x_m)^l = (1, ..., 1)$ при $l = lcm(\varphi(p_1^{k_1}), ..., \varphi(p_m^{k_m}))$

Обозначим: $\varphi'(p_1^{k_1}, ...p_m^{k_m}) = lcm(\varphi(p_1^{k_1}), ..., \varphi(p_m^{k_m}))$

Теорема (Теорема Кармайкла): $a^{\varphi'(n)} \equiv 1 \mod n$, если $(a, n) = 1$.

$\varphi(60) = 16$ (выше)

$\varphi'(60) = lcm(\varphi(2^2)\varphi(3), \varphi(5)) = 4$

$7^4 = (49)^2 \equiv (-11)^2 = 121 \equiv 1 \mod 60$.

Определение: Экспонента (показатель) группы G — наименьшее натуральное число l, такое что $g^l = e \ \forall g \in G$. (если не существует, то экспонента равна бесконечности) (НОК всех порядков группы). Другими словами, l — НОК порядка $g \in G$.

Определение: Функция Кармайкла — экспонента группы $(\mathbb{Z}/n\mathbb{Z}^*)$. (обозначается $\lambda(n)$)

Теорема Кармайкла (без доказательства):

$\lambda(n) = \varphi'(n)$, если $n \not\vdots 8$

$\lambda(n) = \frac{1}{2}\varphi'(n)$, если $n \vdots 8$

Доказательство — упражнение.

$(\mathbb{Z}/2^k\mathbb{Z})^* \cong C_2 \times C_{2^{k-2}} \ \forall k \geq 3$, где C — цикличе-

ская группа.

F — поле. $F[t]$ — кольцо многочленов над полем F.

$(F[t] = \{a_0 + ... + a_n t^n | a_i \in F, a_n \neq 0 \text{ при } n \neq 0\}$ (где t — просто символ, не переменная!)

$(a_1, ..., a_n) \cdot (b_0, ..., b_n) = (c_0, ..., c_{n+m}), C_k = \sum_{i=0}^{k} a_i b_{k-i}$.

С многочленом $p(t) = a_0 + ... + a_n t^n$ связана полиномиальная функция $f_p : F \to F$.

$f_p(x) = a_0 + ... + a_n x^n \ \forall x \in F$.

Если $F = F_2 = \mathbb{Z}/2\mathbb{Z}$, то многочлены t и t^2 не равны, но соответствующие полиномиальные функции равны. (F_2 — поле из двух элементов).

$\deg(a_0 + ... + a_n t^n) := n$ при этом $a_n \neq 0$.

$\deg(0) = -\infty$;

$\deg(pq) = \deg p + \deg q$;

$\deg(p + q) \leq \deg p$.

Теорема (о делении с остатком):

deg является евклидовой нормой на $F[x]$, а само $F[x]$ — евклидово кольцо.

Доказательство:

1) $\deg 0 < \deg p \ \forall p \neq 0$

2) $p, q \neq 0 \in F[t]$

$X = \{p - qf || f \in F[t]\}$.

Пусть $p - qf$ — многочлен наименьшей возможной степени из X.

Если $r > \deg q$:

$q = a_m t^m + ...$

$r = b_{m+k} t^{m+k} + ...$

$r - qt^k \frac{b_{m+k}}{a_m} < \deg r$, но $r - qt^k \frac{bm+k}{a_m} \in X$

Противоречие показывает, что $\deg r < \deg q \Rightarrow p = qf + r,\ \deg r < \deg q$.

(мы доказали, что $F[x]$ является евклидовым кольцом)

Конец девятой лекции.

Теорема Безу:

$p \in F[t], \alpha \in F$. α — корень(?). Тогда остаток от деления $p(t)$ на $t - \alpha$ равен $p(\alpha)$.

Следствие: $p(t) \vdots (t - \alpha) \Leftrightarrow p(\alpha) = 0$.

Доказательство:

$p(t) = (t - \alpha)q(t) + r(t)$, где $\deg r < 1$. Следовательно, $r \in F$.

$p(\alpha) = (\alpha - \alpha)q(\alpha) + r = r$.

Следствие: Ненулевой многочлен не может иметь больше корней, чем степень (количество корней мно-

гочлена не превосходит его степени).

Доказательство: Пусть $\deg p = d$. Индукция по d.

При $d = 0$ многочлен является ненулевой константой и корней не имеет.

При $d > 0$ по теореме Безу: $p(t) = (t - \alpha)q(t)$.

β — корень, если $p \Leftrightarrow \beta = \alpha$ или $q(\beta) = 0$. При этом $\deg q = d - 1$.

Количество корней $p \leq$ (количество корней q)$+1 \leq (d-1)+1 = d$.

Интерполяционная формула Лагранжа:

Задача: найти многочлен $p \in F[t]$ наименьшей степени, такой, что $p(t_0) = y_0, ..., p(t_n) = y_n$, где $t_i, y_i \in F,\ t_i \neq t_j$ при $i \neq j$.

$p(t_i) = y_i$, по теореме Безу $\Leftrightarrow p(t) \equiv y_i \mod (t - t_i)$.

Отсюда очевидно, что $(t - t_i)$ и $(t - t_j)$ взаимно простые при $i \neq j$.

По КТО $F[t]/(\prod_{i=0}^{n}(t - t_j)) \cong \oplus_{i=0}^{n} F[t]/(t - t_i)$

Посмотрим, что такое $F[t]/(t - t_i)$. Это само поле F, (число (хотя не факт, может, это крокодил)). $F[t]/(t - t_i) \cong F$.

Докажем: $\varphi : F[t] \to F$ — эпиморфизм ($\forall \alpha \in F\ \varphi(\alpha) = \alpha$).

$\varphi(p) = p(t_i)$.

$\ker\varphi = \{p|\varphi(p) = 0\} = \{p|p(t_i) = 0\} = \{p|p\vdots(t - t_i)\} = (t - t_i)F[t]$.

$F[t]/(\prod_{i=0}^{n}(t - t_j)) \cong \oplus_{i=0}^{n} F$.

$p + \prod_{i=0}^{n}(t - t_i)F[t] \mapsto (p(t_0), ..., p(t_n))$ (так как это биекция, то в любой элемент $(y_0, ..., y_n)$ соответствует чему-либо из кольца $F[t]/(\prod_{i=0}^{n})$).

Теорема: $\forall y_0, ..., y_n \in F$, $\underbrace{t_0, ..., t_n}_{\text{различных}} \in F$ $\exists!$ многочлен p степени $\leq n : p(t_i) = y_i \ \forall i = 0, ..., n$.

При этом $p(t) = \sum_{i=0}^{n} y_i \frac{w_i(t)}{w_i(t_i)}$, где $w_i(t) = \prod_{j \neq i}(t - t_j)$.

Доказательство:

$w_i(t_k) = 0 \ \forall i \neq k$

$p(t_k) = y_i \frac{w_k(t_k)}{w_k(t_k)} = y_k$.

Алгебраические расширения полей

$p \in F[t]$, p — неприводим, тогда идеал $pF[t]$ является простым идеалом, а в кольце главных идеалов любой ненулевой простой идеал максимальный, следовательно, $pF[t]$ — максимальный. Факторкольцо по идеалу, порожденному p: $F \subseteq F[t]/(p)$ — поле.

Упражнение (на бб): Пусть $L = F[t]/(p)$ (p неприводим) $\supseteq F$. 1) Доказать, что p имеет корень в поле

L. 2) $\forall$ поля $k \supseteq F$, в котором многочлен имеет корень, $\exists$ мономорфизм, $L \to K$ тождественный на F.

Кратность корня и производная многочлена.

$\alpha \in F,\ p$ — многочлен.

Определение: α имеет разность k в ненулевом многочлене p, если $p(t) = (t - \alpha)^k g(t)$, где $g(\alpha) \neq 0$.

Определение: если $p = a_n t^n + ... + a_1 t + a_0$, то его производная $p' = a_n n t^{n-1} + ... + a_1$.

Пример:

$\mathbb{Z}/2\mathbb{Z}$: $(t^2 + 1)' = 2t = 0$

Свойства производной:

1) Линейность: $(p + q)' = p' + q';\ (\alpha p)' = \alpha \cdot p'$.

2) $(pq)' = p'q + pq'$.

3) Производная сложной функции: $(p \circ q)' = (p' \circ q) \cdot q'$.

(без доказательства).

Теорема Пусть α — корень многочлена p кратности k. (Если кратность равна нулю, то α не корень, $k = 1$, α — простой корень, $k > 1$, α — кратный корень (экстремум либо перегиб). Кратный корень означает, что производная в этой точке равна ну-

лю). Тогда кратностьα в многочлене p' не меньше, чем $k-1$. А если $k \neq 0$ в поле F, то кратность равна ровно $k-1$.

Доказательство:

$p = (t-\alpha)^k g(t)$. Дифференцируем это используя правила 2 и 3: $p'(t) = k(t-\alpha)^{k-1}g(t) + (t-\alpha)^k g'(t) = (t-\alpha)^{k-1}(kg(t) + (t-\alpha)g'(t))$. Подсчитаем значение $(kg(t) + (t-\alpha)g'(t)$ в точке α:

$kg(\alpha) + (\alpha - \alpha)g'(\alpha) = kg(\alpha) \neq 0$ при $k \neq 0$.

Конец десятой лекции

Теорема о рациональных корнях многочлена (без доказательства):

Если у нас есть многочлен $p(x) = a_n x^n + ... + a_0$, $a_k \in \mathbb{Z}$

Если $\frac{c}{d}$ — корень p $(c, d \in \mathbb{Z}, \gcd(c,d) = 1)$, то $a_0 \vdots c, a_n \vdots d$.

Комплексные числа

Посмотрим на кольцо многочленов $\mathbb{R}[x]$. Возьмем

многочлен x^2+1. Этот многочлен неприводим. Мы хотим взять факторкольцо.

Определение: Поле $\mathbb{C}$ по $\mathbb{R}[x]/(x^2+1)$ называется полем комплексных чисел.

Теорема Основная теорема алгебры (пока без доказательства):

Любой многочлен из $\mathbb{C}[t]$, степени ≥ 1 (ненулевой) имеет хотя бы один комплексный корень. (будет доказано как следствие теоремы Лиувилля).

Пусть $\rho : \mathbb{R}[x] \to \mathbb{R}/(x^2+1)$

$i = \rho(x)$.

$i^2+1 = \rho(x)^2+1 = \rho(x^2+1) = 0+(x^2+1)\mathbb{R}[x] = 0$ (0 факторкольца). Отсюда $i^2 = -1$.

$f+(x^2+1)\mathbb{R}[x] = (ax+b)+(x^2+1)\mathbb{R}[x] = b+ai$, где $(ax+b)$ — остаток от деления f на x^2+1.

Таким образом, $\mathbb{C} = \{a+bi | a,b \in \mathbb{R}\}$, при этом

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

2) $(a+bi)(c+di) = ac+adi+bci+bdi^2 = (ac-bd)+(ad+bc)i$.

Найдем обратный элемент:

$$\frac{1}{a+bi} = \frac{a-bi}{(a+bi)(a-bi)} = \frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i \quad (1)$$

$z = x + iy$, то x — вещественная часть ($Re\ z$), y — мнимая часть ($Im\ z$) (мнимой частью называется ВЕЩЕСТВЕННОЕ ЧИСЛО y, но ни в коем случае не iy!!!), $x - iy = \bar{z}$ — комплексно сопряженное к z.

$|a + bi| = \sqrt{a^2 + b^2}$ или $|z| = \sqrt{z \cdot \bar{z}}$.

$\varphi \in \mathbb{R}/2\pi\mathbb{Z}$, то есть $\varphi = \{\varphi_0 + 2\pi k | k \in \mathbb{Z}\} = \varphi_0 + 2\pi\mathbb{Z} \in \mathbb{R}/2\pi\mathbb{Z}$.

$$\begin{cases} a = r\cos\varphi \\ b = r\sin\varphi \end{cases}$$

Значит, наше число можно записать в виде $w = \underbrace{a + bi}_{\text{алгебраическая форма}} = r\cos\varphi + ir\sin\varphi = \underbrace{r(\cos\varphi + i\sin\varphi)}_{\text{тригонометрическая форма}}$.

φ — $Arg\ w$.

$$\varphi = \begin{cases} \arctan\frac{b}{a}, a > 0 \\ \pi + \arctan\frac{b}{a}, a < 0 \\ \pm\frac{\pi}{2}, a = 0 \end{cases}$$

Сложение и умножение в тригонометрической форме:

$w = |w|(\cos\varphi + i\sin\varphi)$.

$z = |z|(\cos\alpha + i\sin\alpha)$.

$wz = |w| \cdot |z|(\cos\varphi\cos\alpha - \sin\varphi\sin\alpha + i(\cos\varphi\sin\alpha + \sin\varphi\cos\alpha)) = |w||z| = (\cos(\alpha + \varphi) + i\sin(\alpha + \varphi))$ — формула Муавра.

Возведение в степень:

$w^w = |w|^w(\cos n\varphi + i \sin n\varphi)$.

$|wz| = |w| \cdot |z| \Rightarrow (a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$.

$\mathbb{R}^*_{>0} \times \mathbb{R}/2\pi\mathbb{Z} \cong \mathbb{C}^*$

$(r, \varphi) \mapsto r(\cos \varphi + i \sin \varphi)$.

$z \mapsto (|z|, Arg\ z)$

$\ln : \mathbb{R}^*_{>0} \to \mathbb{R}(+)$ — изомоморфизм.

Теорема: $\mathbb{C}^* \cong \mathbb{R} \times \mathbb{R}/2\pi\mathbb{Z} \cong \mathbb{R} \times \mathbb{R}/\mathbb{Z} \cong \mathbb{C}/2\pi i\mathbb{Z}$.

Определение: Если $x \in \mathbb{R}$, то $e^i x = \cos x + i \sin x$.

Ряд Тейлора для экспоненты:

$e^t = \sum\limits_{k=0}^{\infty} \frac{t^k}{k!} = 1 + t + \frac{t^2}{2} + \frac{t^3}{6} + ...$

Общая форма: $f(t) = \sum\limits_{k=0}^{\infty} \frac{f'^k(0)}{k!} t^k$.

$\cos t = \sum\limits_{m=0}^{\infty} (-1)^m \frac{t^{2m}}{(2m)!}$

$\sin t = \sum\limits_{m=0}^{\infty} (-1)^j \frac{t^{2j+1}}{(2j+1)!}$

Подставить в ряд Тейлора для экспоненты e^{ix} и убедиться, что слагаемые будут косинусами и синусами.

Конец одиннадцатой лекции.

$\mathbb{C}^* \cong \mathbb{R} \times \mathbb{R}/2\pi\mathbb{Z} \cong \mathbb{C}/2\pi i\mathbb{Z}$ — Данный изоморфизм называется Логарифм (с большой буквы): $Ln : \mathbb{C}^* \to \mathbb{C}/2\pi i\mathbb{Z}$. Ну а $Ln(z) = \ln|z| + iArgz$

$(a, b + 2\pi\mathbb{Z}) \leftrightarrow a + \underbrace{bi + 2\pi i\mathbb{Z}}_{i(b+2\pi\mathbb{Z})}$

Доказательство (предыдущей теоремы):

$z = |z|e^{iArgz} = |z|\cos(Argz) + i\sin(Argz)$ (Экспонента на мнимой оси периодична). Отсюда

$z = |z|e^{iArgz} \mapsto^f (\ln|z|, Argz)$. Обратное отображение:

$(r, \varphi + 2\pi\mathbb{Z}) \mapsto e^r e^{i\varphi}$.

Посмотрим на функцию f:

$f(zw) = (\ln|z\cdot w|, Arg(z\cdot w)) = (\ln|z|+\ln|w|, Arg\ z+ Argw) = (\ln|z|, Arg\ z)+(\ln|w|, Arg\ w) = f(z)+f(w)$.

Логарифм от комплексных:

$\ln z = \ln|z| + i\ arg\ z$, где $arg\ z \in (-\pi, pi] \cap Arg\ z$.

Пример: $\ln(-1) = i\pi$

"Одно удовольствие" решать уравнения $z^n = w$ (уравнения круга).

Для того, чтобы решать это уравнение, нужно за-

писать числа z и w в показательной форме: $z = re^{i\varphi},\ w = \rho e^{i\alpha}$

$r^n e^{in\varphi} = \rho e^{i\alpha}$

Приводим к системе: $\begin{cases} r^n = \rho \\ n\varphi = \alpha + r\pi k, k \in \mathbb{Z} \end{cases}$

Отсюда:

$z = \sqrt[n]{\rho} e^{i\frac{\alpha+2\pi k}{n}}$.

Если $k' = k + mn$ в $2\mathbb{Z}$

$e^{i\frac{\alpha+2\pi k'}{n}} = e^{i\frac{\alpha+2\pi k}{n}+2\pi m} = e^{i\frac{\alpha+2\pi k}{n}}$

На картинке корни располагаются в вершинах вписанного в окружность радиусом $\sqrt[n]{\rho}$ n-угольника.

Решения этого уравнения называются корнями n-ной степени из w. При этом пишут, что $\sqrt[n]{w} = \{z|z^n = w\}$ (это множество всех таких корней).

К примеру, $\sqrt[n]{1} = \{z|z^n = 1\} = \{e^{i\frac{\alpha+2\pi k}{n}}|k = 0, ..., n-1\} = \{\varepsilon^k|k = 0, ..., n-1,\ \varepsilon = e^{i\frac{2\pi}{n}}\}$ — циклическая подгруппа в $\mathbb{C}^*$.

Определение: ω называется первообразным корнем n-ой степени из единицы, если $ord\,\omega = n$ в группе $\mathbb{C}^*$.

В комплексных числах все корни выглядят как ε^k. ε^k — первообразный корень степени $n \Leftrightarrow \gcd(n, k) = 1$.

Теорема (основная теорема алгебры)

Любой многочлен из $\mathbb{C}[t]$, степени ≥ 1 (ненулевой) имеет хотя бы один комплексный корень.

Определение: Поле F называется алгебраически замкнутым, если любой многочлен из $F[x]$ ненулевой степени имеет корень в F.

Теорема Любое поле вкладывается в алгебраически замкнутое: $\forall$ поля $K \exists$алгебраически замкнутое поле $\bar{K}$ и моном $\bar{K}$.

Лемма Комплексное сопряжение - автоморфизм $\mathbb{C}$.

Доказательство: $\mathbb{C} \to \mathbb{C}$ — биекция ($\bar{\bar{z}} = z$, $a \pm bc = a - bc$).

$z \mapsto \bar{z}$.

$(z + w) = \bar{z} + \bar{w}$ — тривиально.

$(a + bi)(c + di) = (ac - bd) + (ad + bc)i$. А теперь перемножение сопряженных: $(a - bi)(c - di) = (ac - bd) - (ad + bc)i$, следовательно, операции сохраняются. И биекция. Какие-то вопросы?

Следствие:

1)$w + \bar{w}, w \cdot \bar{w} \in \mathbb{R}$;

2)$w \in \mathbb{R} \Rightarrow w = \bar{w}$;

3) Если $w \notin \mathbb{R}$, $(w + z)$ и $(wz) \in \mathbb{R}$, то $z = \bar{w}$;

4) $p \in \mathbb{R}[t]$, $w \in \mathbb{C}$. Тогда $p(\bar{x}) = p(\bar{w})$.

5) Если $p \in \mathbb{R}[t]$, $p(w) = 0$, то $p(\bar{w}) = 0$.

6) Если $w \in \mathbb{C}$ — корень многочлена $p \in \mathbb{R}[t]$, то

$p \vdots (t-w)(t-\bar{w}) = t^2 - (w+\bar{w})t + w\bar{w} \in \mathbb{R}[t]$.

Теорема Любой многочлен из $\mathbb{R}[t]$ степени большей двух приводим в $\mathbb{R}[t]$.

Доказательство: Пусть $p \in \mathbb{R}[t] \subset \mathbb{C}[t]$, $\deg p \geq 3$. Применим основную теорему алгебры и скажем, что: по основной теореме алгебры существует $w \in \mathbb{C}$ комплексный корень p.

Если $w \in \mathbb{R}$, то по теореме Безу $p \vdots t - w$.

Если нет, то $p \vdots t^2 - (w + \bar{w}t + w\bar{w})$. В любом случае, $p = f \cdot g$, $\deg g \geq 1$.

Доказано.

Следствие: любой многочлен в $\mathbb{R}[t]$ раскладывается на множители, степени не выше двух.

Конец двенадцатой лекции.

Линейная алгебра. Векторные пространства

Определение: F — поле, $(V, +)$ — абелева группа. V называется векторным пространством над полем F, если задана (внешняя) операция умножения $F \times V \to V$, удовлетворяющая свойствам:

(Не забываем аксиомы абелевой группы)

1) $\forall \alpha, \beta \in F, u, v \in V : \quad (\alpha\beta) \cdot v = \alpha(\beta \cdot v)$ — ассоциативность.

2) $(\alpha+\beta)v = v(\alpha) + v(\beta)$ и $\alpha(u+v) = \alpha u + \alpha v$.

3) $1 \cdot v = v$. (ненулевой элемент поля, умноженный на элемент пространства не дает нуля).

Плохой пример:

F — поле, $V \neq \{0\}$ — абелева группа. Положим, $\alpha v = 0 \; \forall \alpha \in F, v \in V$. Но эту штуку мы не хотим называть векторным пространством. Именно для этого предназначена аксиоме №3. Это удовлетворяет аксиомам 1, 2, но не является векторным пространством.

Терминология:

Элементы поля F будут обычно называться числами, вне зависимости от того, бегемоты они или крокодилы, и обозначаться будут греческими буквами.

Элементы абелевой группы V называются векторами, хотя могут и не иметь отношения к векторам, и обозначаются маленькими латинскими буквами.

Примеры векторных пространств:

0) $\{0\} = V$, умножение задается $\alpha \cdot 0 = 0$, $\forall \alpha \in F$;

1) $V = F$

n) $F^n = \left\{ \begin{pmatrix} \alpha_1 \\ ... \\ \alpha_n \end{pmatrix} | \alpha_i \in F \right\}$, $\begin{pmatrix} \alpha_1 \\ ... \\ \alpha_n \end{pmatrix} + \begin{pmatrix} \beta_1 \\ ... \\ \beta_n \end{pmatrix} = \begin{pmatrix} \alpha_1 + \beta_1 \\ ... \\ \alpha_n + \beta_n \end{pmatrix}$

$$\gamma \cdot \begin{pmatrix} \beta_1 \\ ... \\ \beta_n \end{pmatrix} = \begin{pmatrix} \gamma\beta_1 \\ ... \\ \gamma\beta_n \end{pmatrix}$$

F) X — множество, V — векторное пространство. $Func(X, V)$ — множество всех функций из X в V. Это множество также является векторным пространством. Если у нас есть функции $f, g : X \to V$, то $(f + g)x = f(x) + g(x)$ и $(\alpha f)(x) = \alpha f(x)$ $\alpha \in X$.

П (поле)) $F \subseteq K$ (поля). Тогда K можно рассматривать как векторное пространство над F.

B) Множество векторов на плоскости или в n-мерном пространстве является векторным пространством над полем вещественных чисел.

G) $(G, +)$ — абелева группа, предположим, что для некоторого простого p сумма p штук элементов группы равна нулю: $p \cdot g = 0$, $\forall g \in G$. Тогда G — векторное пространство над $\mathbb{Z}/p\mathbb{Z}$ с операцией $n \cdot v = \underbrace{v + v + v + v}_{n}$ $\forall n \in \mathbb{Z}/p\mathbb{Z}$, $\forall v \in G$, (так как $pv = 0$, то это определение не зависит от выбора представителя класса $n + p\mathbb{Z}$) (берем простое, чтобы эта штука была полем).

M) $F[t]$ — векторное пространство над F относительно обычных операций. $F \subseteq R$, где F — поле, R — кольцо. Тогда еще и R — векторное пространство над F.

Свойства (V — векторное пространство над F):
1) $0 \cdot v = 0_v$;
2) $\alpha \cdot 0_v = 0_v$;
3) $(-1) \cdot v = -v$;
4) $(-\alpha)v = \alpha \cdot (-v) = -(\alpha v)$;
И еще дофига

Определение: $U \subseteq V$. U называется подпространством в V, если оно само по себе является пространством относительно операций, заданных в V.

Обозначение $U \leq V$ означает «U является подпространством V».

Лемма: $U \subseteq V$. U подпространство, если $\forall \alpha \in F, u_1, u_2 \in U$, то $u_1 + u_2 \in U$, $\alpha u_1 \in U$.

Доказать самостоятельно

Определение: если $S \subseteq V$. Подпространство, порожденное S — это наименьшее подпространство, содержащее S (обозначение $< S >_F$ — подпространство, порожденное S (также называется линейной оболочкой) (буква F обычно не ставится)).

Лемма (следствие из предыдущей леммы):

1) Пересечение подпространств является подпространством.

2) Сумма подпространств является подпростран-

ством: U, W — подпространства в V, тогда $U + W = \{u + w | u \in U, w \in W\} \leq V$.

Лемма: $< S >= \{\alpha_1 s_1 + ... + \alpha_n s_n | n \in \mathbb{N}, \alpha_i \in F, s_i \in S\}$.

Доказательство: $s_i \in S \subseteq < S > \Rightarrow \alpha_i s_i \in < S > \Rightarrow \sum_{i=1}^{n} \alpha_i s_i \in < S >$.

Обратно: достаточно доказать, что правая часть является подпространством: сложить или умножить два таких выражения и получить такое же выражение.

Определение: Выражение $\alpha_1 s_1 + ... + \alpha_n s_n$ называется линейной комбинацией элементов $s_1, ..., s_n \in V$ с коэффициентами $\alpha_1, ..., \alpha_n \in F$

Запись может быть сокращена как $\sum_{i=1}^{n} \alpha_i s_i$.

Обозначения: $\alpha \in F, v \in V$, положим по определению $v\alpha = \alpha v$.

Обозначим $u = (u_1, ..., u_n)$, где $u_1, ..., u_n \in V$.

$a = \begin{pmatrix} a_1 \\ ... \\ a_n \end{pmatrix}$, где $a_1, ..., a_n \in F$.

Тогда $u \cdot a = \sum_{i=1}^{n} u_i a_i$

Определение: $u = (u_1, ..., u_n)$ — кортеж векторов. u — линейно независимый, если $\forall a \in F^n \setminus \{0\}$ (столбец нулей) $ua \neq 0$, и линейно зависимый. Если $\exists a \in F^n \setminus \{0\}$, такое, что $ua = 0$, то u зависимое, а равенство $ua = 0$ называется линейной зависимостью между $u_1, ..., u_n$.

Множество $\{u_1, ..., u_n\}$ линейно независимое, (здесь $u_i \neq u_j$ при $i \neq j$) если $(u_1, ..., u_n)$ линейно независимы.

Теорема: Множество называется линейно независимым, если его любое конечное подмножество линейно независимо.

$S \subseteq V$.

S — линейно независимо, если любое конечное подмножество линейно независимо.

S — система образующих (пространства V) если $< S >= V$

Конец тринадцатой лекции.

Определение: Базис — это линейно независимая система образующих.

Если $S \subseteq V$ — векторное пространство, $\sum\limits_{s \in S} \alpha_s \cdot s$, где $\alpha_s = 0$ кроме конечного числа.

Теорема (несколько эквивалентных определений базиса).

Пусть V — векторное пространство, $s \subseteq V$, драма разворачивается над полем F. Следующие условия эквивалентны:

1) S — базис по определению.

2) S — максимальная (по включению) линейно независимая система.

3) S — минимальная (по включению) система образующих.

4) $\forall v \in V \ \exists \alpha_s \in F$ (по $s \in S$, все $\alpha_s = 0$ кроме конечного числа). $v = \sum\limits_{s \in S} \alpha_s s$.

Доказательство:

(1) $\Rightarrow$ (2)

Пусть $v \in V$. По определению базиса, S — система образующих. Поэтому элемент $v = \sum\limits_{i=1}^{n} \alpha_i s_i$ при некотором $\alpha_i \in F$, $s_i \in S$. Тогда $v - \sum\limits_{i=1}^{n} \alpha_i s_i = 0$ — нетривиальная линейная комбинация элементов $S \cup \{v\}$ равна нулю $\Rightarrow$ $S \cup \{v\}$ линейно зависимая, $\Rightarrow$ S — максимальная линейно независимая.

(2) $\Rightarrow$ (1)

$v \in V \setminus S$. Так как S — максимальная, то $S \cup \{v\}$ линейно зависимая, следовательно, $\exists \alpha v + \sum\limits_{i=1}^{n} \alpha_i s_i = 0$ при $\alpha_j, \alpha_i \in F,\ s \in S$, (при этом α не все нули). Получается, что $\alpha_i = 0$, противоречие. Если же $\alpha \neq 0$, то $v = \sum\limits_{i=1}^{n} \frac{\alpha_i}{\alpha} s_i \in < S >$.

Остальное доказать самостоятельно.

Теорема: В любом векторном пространстве существует базис. Точнее, пусть $X \subseteq Y \subseteq V$, где V — векторное пространство, X — линейно независимый, а Y — система образующих. Тогда $\exists$ базис B: $X \subseteq B \subseteq Y$.

Без доказательства.

Данное утверждение очевидно для конечномерных пространств, но не очевидно для бесконечномерных пространств. Невозможно выбрать несчетный базис.

Возьмем вектор. Он линейно независим. Если это не все пространство, возьмем вектор, не лежащий в его линейной оболочке, образуем множество этими векторами. Получим плоскость. Если это не все пространство, возьмем еще один вектор, не лежащий в данной плоскости и так далее.

Определение: Пространство называется конечномерным, если в нем существует конечный базис.

Соглашение: Если V — конечномерное, то базисом будет называться упорядоченный набор векторов, обладающий свойствами базиса.

Два неколлинеарных вектора на плоскости образуют базис.

Определение: Если $f = (f_1, ..., f_n)$ — базис, а $v \in V$, такой, что $v = \sum\limits_{i=1}^{n} f_i \alpha_i$, то $v_f = \begin{pmatrix} \alpha_1, \\ ... \\ \alpha_n \end{pmatrix}$ называется столбцом координат v в базисе f.

Определение столбца координат: $v = fv_f, u = fu_f, v+u = f(v_f + u_f)$.

$\alpha v = v\alpha = (fv_f)\alpha = f(v_f\alpha)$.

Следовательно, $(v+u)_f = v_f + u_f$, $(\alpha v)_f = v_f\alpha$.

Любое конечномерное пространство не отличимо от пространства столбцов.

Матрицы.

Пусть U, V — векторные пространства, $L : U \to V$ — линейное отображение, если $\forall u_1, u_2 \in U, \alpha \in F$, $L(u_1 + u_2) = L(u_1) + L(u_2)$, $L(\alpha u_1) = \alpha L(u_1)$

Биективное линейное отображение называется изоморфизмом.

Лемма: Если L — изоморфизм, то обратная к ней L^{-1} — тоже изоморфизм.

Пусть $L : U \to V$ — линейное отображение, $f = (f_1, ..., f_n)$ — базис пространства U, $g = (g_1, ..., g_m)$ — базис пространства V. Возьмем $u \in U$: $u = \sum\limits_{i=1}^{n} f_i\alpha_i$, $\begin{pmatrix} \alpha_1 \\ ... \\ \alpha_n \end{pmatrix}$

Предложение $L(u) = L(\sum\limits_{i=1}^{n} f_i, \alpha_i) = \sum\limits_{i=1}^{n} L(f_i\alpha_i) = \sum\limits_{i=1}^{n} L(f_i)\alpha_i$. Положим, $L(f_i) = \sum\limits_{j=1}^{m} g_i\gamma_{ji}$

Получили прямоугольную табличку, которая называется матрицей:

$L_{f,g} = \begin{pmatrix} \gamma_{11} & ... & \gamma_{1n} \\ ... & & \\ \gamma_{m1} & ... & \gamma_{mn} \end{pmatrix}$ — матрица отображения L в базисах f, g.

$L(u) \in V$

$L(u)_g = \sum\limits_{i=1}^{n} L(f_i)_g\alpha$, что запишем как $L_{f,g}u_f$

$\begin{pmatrix} L(f_1)_g & ... & L(f_n)_g \end{pmatrix}$ что эквивалентно ранее записанной матрице.

И эту штуку мы умножаем на вектор:

$$\begin{pmatrix} L(f_1)_g & \dots & L(f_n)_g \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \dots \\ \alpha_n \end{pmatrix}$$

Определение:

$$L_{f,g} = \begin{pmatrix} \gamma_{11} & \dots & \gamma_{1n} \\ \dots & & \\ \gamma_{m1} & \dots & \gamma_{mn} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \dots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} \sum\limits_{i=1}^{n} \gamma_{1i}\alpha_i \\ \dots \\ \sum\limits_{i=1}^{n} \gamma_{mi}\alpha_i \end{pmatrix}$$

Определение:
$L : U \to V$, f — базис U, g — базис V
$L_{f,g} = (L(f_1)_g, ..., L(f_n)_g)$
Вытекает из предложения ранее: $L(u)_g = L_{f,g}(u_f)$

Конец четырнадцатой лекции.

$L : U \to V$
$N : V \to W$.
$(f_1, ..., f_k) = f$ — базис U,
$(g_1, ..., g_n) = g$ — базис V,
$(h_1, ..., h_n) = h$ — базис W.
Берем композицию $N \circ L$:
У нас есть
$L_{f,g} = n \times k$,

$N_{g,h} = m \times n$,

$(L \circ N)_{f,h} = N_{g,h} \cdot L_{f,g} = m \times k$.

Определение: A — матрица $m \times n$, B — матрица $n \times k$, тогда произведением матриц A и B называется матрица $C = A \cdot B$ размера ... с элементами $c_{i,j} = \sum\limits_{l=1}^{n} a_{i,l} \cdot b_{l,j} = a_{i*} b_{*j}$.

Теорема $(N \circ L)_{f,h} = N_{g,h} \cdot L_{f,g}$.

Доказательство:

$(N \circ L)(x)_h = N(L(x))_h = N_{g,h} \cdot L(x)_g = N_{g,h} \cdot (L_{f,g} \cdot x_f) = (N_{g,h} \cdot L_{f,g})(x_f)$ — мы хотим доказать последнее равенство.

$N_{g,h} = A = (a_{ij})_{1 \le j, j \le n}$

$L_{f,g} = B = (b_{ij})_{i,j=1}^{n}$.

$x_f = \begin{pmatrix} \alpha_1 \\ ... \\ \alpha_k \end{pmatrix}$

Левая часть:

$A \cdot (Bx_f) = A \cdot y,\ y_j = b_{j*} x_f = \sum\limits_{r=1}^{k} b_{jr} \alpha_r$

y — столбец той же высоты, сколько строчек в матрице N

$(Ay)_p = a_{p*} y = \sum\limits_{s=q}^{n} a_{ps} y_s = \sum\limits_{s=1}^{n} \sum\limits_{r=1}^{k} a_{ps} b_{sr} \alpha_r$.

Правая часть:

$((AB)x_f)_p = (Cx_f)_p = C_{p*} x_f = \sum\limits_{r=1}^{k} c_{pr} \alpha_r = \sum\limits_{r=1}^{k} \sum\limits_{l=1}^{n} a_{pl} b_{lr} \alpha_r$

(буква p взялась потому, что считаем p-ый эле-

мент).

Единственность матричного оператора.

$\forall x \in U : L(x)_g = L_{f,g} x_f = D x_f$; если $x = f \cdot a$, то $x_f = a$.

Пусть $x_f = \begin{pmatrix} 0 \\ 0 \\ ... \\ 0 \\ 1 \\ 0 \\ ... \\ 0 \end{pmatrix}$, где единица стоит на i месте.

Тогда $D x_f = d_{xi} = \begin{pmatrix} d_{1i} \\ ... \\ d_{ni} \end{pmatrix}$

Таким образом, i-тый столбец $L_{f,g}$ совпадает с i-тым столбцом D $\forall i$.

Лемма о замене:

S — базис векторного пространства V (все комментарии даны для трехмерного школьного пространства)

$u \in S$, $v \in V$, $v \notin < S \setminus \{u\} >$. (выкидываем один из трех некомпланарных векторов)

Тогда $S \setminus \{u\} \cup \{v\}$ — базис. (заменяем этот вектор на другой, не равный ему)

Доказательство:

Так как S — базис, то

$v = \sum\limits_{s \in S} \alpha_s s = \alpha_u u + \sum\limits_{s \in S \setminus \{u\}} \alpha_s \cdot s$

Так как $v \notin < S \setminus \{u\} >$, то $\alpha_u \neq 0$.

$u = \frac{1}{\alpha_u} v + \sum\limits_{s \in S \setminus \{u\}} (-\frac{\alpha_s}{\alpha_u}) s \ni < T >$

Обозначим $T = S \setminus \{u\} \cup \{v\}$

$S \subseteq < T > \Rightarrow \underbrace{< S > \subseteq < T >}_{= V} \subseteq V$

Отсюда T — система образующих.

$\sum\limits_{t \in T} \beta_t t = 0$ (почти все $\beta_t = 0$).

$\sum\limits_{t \in T} \beta_t t = \beta_v v + \sum\limits_{t \in S \setminus \{u\}} \beta_t t = \beta_v \alpha_u u + \beta_v \sum\limits_{t \in S \setminus \{u\}} \alpha_s s + \sum\limits_{t \in S \setminus \{u\}} \beta_t t$ — линейная комбинация векторов.

Так как S линейно независима, то все коэффициенты равны нулю, в частности, $\beta_v \alpha_u = 0 \Rightarrow \beta_v = 0 \Rightarrow \sum\limits_{t \in S \setminus \{u\}} \beta_t t = 0 \Rightarrow \beta_t = 0 \ \forall t \in T$.

Таким образом, T линейно независима $\Rightarrow T$ — базис.

Теорема: Любые 2 базиса данного пространства равномощны.

Доказательство (только для конечномерных про-

странств):

V — векторное пространство, $f = (f_1, ..., f_n)$ — базис.

Пусть s — базис (необязательно конечный).

По индукции:

Рассмотрим пространство $< f_2, ..., f_n >$ (выкинули f_1). Если бы это пространство было равно всему пространству, то это означало бы, что f_1 принадлежало бы линейной оболочке: $f_1 \in < f_2, ..., f_n > \Rightarrow f_1 = \sum_{i=2}^{n} f_i \alpha_i$, что противоречит линейной независимости.

Если бы $S \subseteq < f_2, ..., s_n >$, то $V =< S > \subseteq < f_2, ..., f_n >$, а это не так по только что доказанному.

Значит, $\exists s_1 \in S : s_1 \notin < f_2, ..., f_n >$, тогда по лемме о замене мы можем сказать, что $(s_1, f_2, ..., f_n)$ — базис.

Аналогично, $< s_1, f_3, ..., f_n > \neq V \Rightarrow \exists s_2 \in S : s_2 \notin < s_1, f_3, ..., f_n >$, по лемме $(s_1, s_2, f_3, ..., f_n)$. Продолжая процесс, найдём $s_1, ..., s_n \in S$, такие, что они образуют базис (заместив все элементы из f). Значит, $(s_1, ..., s_n) = s$ — линейно независимый набор, $S \supseteq \{s_1, ..., s_n\}$, $\{s_1, ..., s_n\}$ — максимальный линейно независимый набор, следовательно, $S = \{s_1, ..., s_n\}$.

Определение: $\dim V$ — размерность пространства V — мощность базиса.