Экзамен по алгебре

Швецова Анна по конспектам от Саютина Дмитрия

15 января 2017 г.

Содержание

1. Билет 1

1.1. Определения и основные понятия

***Определение* 1.1.** Множество R с операциями $+, \cdot$ на нём называется кольцом, если:

1. $(R, +)$ — абелева группа.
2. $\forall x,\ y,\ z \in R$: $\begin{matrix}(x+y)z = xz + yz \\ x(y+z) = xy + xz\end{matrix}$ (дистрибутивность)

***Определение* 1.2.** Кольцо называется ассоциативным, если $*$ — ассоциативна $(x(yz) = (xy)z)$.

***Определение* 1.3.** Кольцо называется коммутативным, если $*$ — коммутативна $(xy = yx)$.

***Определение* 1.4.** Кольцо называется кольцом с единицей, если $\exists 1 \colon x \cdot 1 = 1 \cdot x = x\ \forall x \in R$.

***Определение* 1.5.** Ассоциативное кольцо с единицей, причём $1 \neq 0$, в котором всякий ненулевой элемент обратим [по умножению] называется телом.

***Определение* 1.6.** Коммутативное тело называется полем.

Пример.
$2\mathbb{Z}$ —коммутативное, ассоциативное кольцо без 1
$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}/n\mathbb{Z}$
$R[x]$ — кольцо многочленов с коэффициентами из R
$R[[x]] = \{\sum\limits_{i=0}^{\infty} a_i x^i \mid a_i \in R\}$ — кольцо формальных степенных рядов.

1.2. Свойства колец

Лемма. Пусть R - кольцо (ассоциативное), $r \in R$, тогда:

1. r * 0 = 0 * r = 0
2. Если R - кольцо с единицей, то $(-1) * r = -r$, где $(-x)$ означает обратный элемент по сложению.
3. Если $|R| \neq 1$, то $0 \neq 1$.

Доказательство.

1. - $r + 0 = r = 0 + r$.
   - $r(r+0) = r^2$
   - $r^2 + r * 0 = r^2$
   - $r * 0 = 0$.
   - Аналогично доказывается правое равенство.
2. Пользуемся дистрибутивностью кольца:
   $r * 0 = 0 \Rightarrow r(-1+1) = 0 \Rightarrow .\ (-1)r + 1 * r = 0 \Rightarrow (-1)r + r = 0 \Rightarrow (-1) * r = (-r)$

3. Пусть $0 = 1$. Тогда $\forall r \in R\colon r = 1 * r = 0 * r = 0 \implies R = \{0\} \implies |R| = 1$. □

***Определение* 1.7.** Пусть R — коммутативное кольцо. Элемент $r \in R\backslash\{0\}$ называется делителем нуля, если $\exists s \in R \setminus \{0\}\colon rs = 0$.

***Определение* 1.8.** Пусть R — коммутативное кольцо. Элемент $r \in R \setminus \{0\}$ называется нильпотентным, если $\exists n \in \mathbb{N}\colon r^n = 0$

Замечание 1. В $\mathbb{Z}/n\mathbb{Z}$ есть делители нуля $\iff$ n – составное.

- Если $n = ml$ $(m, l \geqslant 2)$, то и m и l - делители нуля.
- Если есть делители нуля, то $\exists m, l \geqslant 2,\ ml \vdots n$, что невозможно.

Так что в качестве примера можно привести какое-нибудь составное число и его делитель.

Замечание 2. В $\mathbb{Z}/n\mathbb{Z}$ нильпотенты $\iff$ n делится на какой-то квадрат.

TODO: Нужно больше примеров

***Определение* 1.9.** Коммутативное ассоциативное кольцо с 1 без делителей нуля называется областью целостности (целостным кольцом).

1.3. Гомоморфизм колец

***Определение* 1.10.** $f\colon A \to B$ называется гомоморфизмом колец, если:

- A, B — кольца.
- $\forall a,\ b \in A\colon f(a + b) = f(a) + f(b)$.
- $\forall a,\ b \in A\colon f(ab) = f(a)f(b)$.

***Определение* 1.11.** $\operatorname{Ker} f = f^{-1}(0) = \{x \in A \mid f(x) = 0\}$

***Определение* 1.12.** $\operatorname{Im} f = \{f(x) \mid x \in A\}$.

Замечание. Если $f\colon A \to B$ — гомоморфизм колец, то:

1. $f(0_A) = 0_B$
2. $f(-r) = -f(r)$
3. Если $f(a) = b$, то $f^{-1}(b) = a + \operatorname{Ker} f$
4. f — инъективна $\iff$ $\operatorname{Ker} f = \{0\}$

Доказательство.

1. $f(0_A) = f(0_A * 0_A) = f(0_A) * f(0_A) \Rightarrow f(0_A) = 0_B$
2. $0_B = f(0_A) = f(-r + r) = f(-r) + f(r) \Rightarrow f(-r) = -f(r)$
3. Если $f(a) = b$, то $f^{-1}(b) = a + \operatorname{Ker} f$
   Докажем вложенность в обе стороны.
   $a + \operatorname{Ker} f \subset f^{-1}(b)$ т.к. $\forall x \in \operatorname{Ker} f f(a + x) = f(a) + f(x) = f(a) + 0 = f(a) = b$
   В другую сторону: пусть есть элемент $t \notin a + \operatorname{Ker} f\ :\ f(t) = b$, тогда $0 = f(t) - f(a) = f(t - a) \Rightarrow t - a \in \operatorname{Ker} f \Rightarrow t - a + a \in a + \operatorname{Ker} f \Rightarrow t \in a + \operatorname{Ker} f$ Протворечие
4. f — инъективна $\Rightarrow \forall x \in B\ |f^{-1}(x)| \leqslant 1 \Rightarrow |\operatorname{Ker} f| = |f^{-1}(0)| \leqslant 1$ Но там есть хотя бы 0, значит, строго 1. В обратную строну очевидно. Если ядро нетривиально, значит, хотя бы прообраз нуля ломает инъективность.

□

Замечание. Единица не всегда сохраняется, даже если она есть во втором кольце.

Пример. A — абелева группа, есть $+$, 0. $x, y \in A$: $x \cdot y := 0$.

***Определение* 1.13.** Гомоморфизм нулевой, если он переводит все элементы в 0.

Утверждение 1.1. Если $f\colon A \to B$ ненулевой гомоморфизм колец. A — кольцо (ассоциативное, коммутативное) с 1. B — область целостности, то $f(1_A) = 1_B$.

Доказательство. $f(1_A) = f(1_A * 1_A) = f(1_A) * f(1_A)$

$f(1_A) - f(1_A) * f(1_A) = 0_B$

$f(1_A)(1_B - f(1_A)) = 0_B$.

Так как B — область целостности, то $f(1_A) = 0$ или $f(1_A) = 1_B$.

Если $f(1_A) = 0_B$, то $\forall a \in A$: $f(a) = f(1 * a) = f(1)\, f(a) = 0\, f(a) = 0 \implies f$ — нулевой.

Следовательно $f(1_A) = 1_B$. □

Замечание. Далее гомоморфизм колец с единицей означает гомоморфизм колец, обладающий свойством выше ($f(1_A) = 1_B$).

Лемма. Если $f\colon A \to B$ — гомоморфизм колец с единицей, то $\forall x \in A^*$: $f(a^{-1}) = f(a)^{-1}$

Доказательство.
Если a обратим, то $aa^{-1} = 1$. Тогда $1 = f(1) = f(aa^{-1}) = f(a)f(a^{-1}) \Rightarrow f(a)^{-1} = f(a^{-1})$ □

Лемма. Если $f\colon A \to B$ — гомоморфизм колец, то

$\operatorname{Im} f$ — подкольцо B.

$\operatorname{Ker} f$ — двусторонний идеал A.

Доказательство. Оставлено в качестве упражнения. □

1.4. Подкольца и идеалы

***Определение* 1.14.** Непустое подмножество кольца R называется подкольцом, если

- $\forall a, b \in A$: $a + b$, $-a$, $ab \in A$

***Определение* 1.15.** Аддитивная подгруппа $I \leqslant R^+$ называется:

- Левым идеалом, если $\forall r \in R, \forall s \in I$: $rs \in I$ (иначе говоря, $RI \subseteq I$)
- Правым идеалом, если $\forall r \in R, \forall s \in I$: $sr \in I$ (иначе говоря, $IR \subseteq I$).
- Двусторонним идеалом, если она и левый и правый идеал.

// Все примеры живут в конспекте так как в билете они не требуются. Итак он очень большой

***Определение* 1.16.** R — кольцо, $X \subseteq R$. Идеалом (левым, правым, двусторонним), порождённым подмножеством X называется наименьший по включению идеал (левый, правый, двусторонний), содержащий X.

Упражнение: пересечение всех идеалов, содержащих данное множество X является идеалом, порождённым множеством X.

Доказательство.

Во-первых, пересечение идеалов – идеал. (Идеалы это подгруппы, пересечение подгрупп = подгруппа. Соблюдение свойства идеала проверяется так: возьмем элемент из пересечения, домножим на любое r. Полученный элемент лежал в обоих идеалах, значит и в пересечении тоже. Успех)
Во вторых, мы получим не меньше чем нужный идеал. Пусть не так. Тогда какие-то 2 идеала пересеклись и мы получили меньше чем нужный идеал. Но в результате пересечения мы получили идеал и он также содержал множество . Значит, наименьший идеал не наименьший. Противоречие.
В-третьих, мы получим не больше, так как в пересечении уже лежит искомый идеал. □

Замечание. Для правых идеалов:

$$\bigcap_{\substack{I \supseteq X \\ \text{I} - \text{идеал R}}} I = \sum_{x \in X} xR$$

***Определение* 1.17.**

- (X) — идеал, порождённый множеством X, в зависимости от ситуации левый, правый или двусторонний.
- (a) — идеал, порождённый элементом a, где $a \in R$, в зависимости от ситуации левый, правый или двусторонний.
- Идеал, порождённый одним элементом называется *Главным идеалом.*

Замечание. Для левых идеалов $(a) = Ra$.

Лемма. Подкольцо, порождённое множеством X, то есть наименьшее подкольцо, содержащее это множество, состоит из всех сумм из элементов $\pm x_1 x_2 x_3 \dots x_n$, где $x_i \in X$

Доказательство. □

2. Билет 2

***Определение* 2.1.** Пусть R — кольцо с 1, введём *канонический гомоморфизм* $\phi : \mathbb{Z} \to R$:

$$\phi(n) = \begin{cases} 0 & n = 0 \\ \underbrace{1_R + 1_R + \ldots + 1_R}_{n \text{ раз}} & n > 0 \\ -\phi(-n) & n < 0 \end{cases}$$

Действительно является гомоморфизмом (следствие дистрибутивности).

***Определение* 2.2.** Если канонический гомоморфизм ϕ — инъективен ($\operatorname{Ker}\phi = \{0\}$), то характеристика ноль ($\operatorname{Char} R := 0$)

Иначе ядро нетривиально. Но в $\mathbb{Z}$ любое нетривиальное ядро имеет вид $n\mathbb{Z}$ (для некоторого $n \geqslant 1$, ибо ядро – это подгруппа), такое n и называется характеристикой кольца R ($\operatorname{Char} R = n$).

Любой идеал I по определению является подгруппой аддитивной подгруппы кольца и задаёт разбиение кольца на смежные классы или классы вычетов по модулю I, о чём пойдёт речь дальше.

***Определение* 2.3.** a и b сравнимы по модулю I ($a \equiv b \pmod I$), если $a - b = a + (-b) \in I$,

Где $a, b \in R$, I — идеал R (левый, правый, или двусторонний).

Лемма. Если I — двусторонний идеал, $a \equiv a' \pmod I$, $b \equiv b' \pmod I$, то

1. $a + b \equiv a + b' \equiv a' + b' \pmod I$.
2. $ab \equiv ab' \equiv a'b' \pmod I$

Доказательство.

1. $a + b - (a + b') = b - b' \in I \Rightarrow a + b \equiv a + b'$. Остальное аналогично
2. $ab - ab' = a(b - b') \in I$. (так как $b - b' \in I$, и I — идеал) □

***Определение* 2.4.** Пусть I — двусторонний идеал R.

- Фактор-кольцом по I называется множество смежных классов в сравнимости по модулю.
- Зададим сложение: R/I: $(r_1 + I) + (r_2 + I) = r_1 + r_2 + I$.
- Зададим умножение: R/I: $(r_1 + I)(r_2 + I) = r_1 r_2 + I$.
- Проверим дистрибутивность слева: $(r_1+I)(r_2+I+r_3+I) = (r_1+I)(r_2+r_3+I) = r_1r_2+r_1r_3+I$.
- Дистрибутивность справа. $(r_2 + I + r_3 + I)(r_1 + I) = (r_2 + r_3 + I)(r_1 + I) = r_2r_1 + r_3r_1 + I$.
- **Упражнение:** Доказать корректность (независимость результата сложения и умножения от выбора представителя). План доказательства: Взять 2 класса вычетов, из каждого взять по 2 элемента. Показать (сравнимостью), что неважно, какой из элементов из одного класса мы будем брать, мы всё равно попадем в один класс.

Пример 1. $\mathbb{Z}/_{n\mathbb{Z}}$ теперь является не только фактор-группой, но и фактор-кольцом.

Пример 2. $K[x]/_{(f(x))}$
K — поле, $f \in K[x]$.

3. Билет 3

Теорема 3.1 (Теорема о гомоморфизме)**.** Пусть f — гомоморфизм колец с 1. Тогда

$A/_{\operatorname{Ker} f} \simeq \operatorname{Im} f$.

Доказательство. Из теоремы о гомоморфизме групп у нас есть: $\phi\colon A/_{\operatorname{Ker} f} \to \operatorname{Im} f$

Нужно показать гомоморфизм умножения: $\phi(ab) = \phi(a)\phi(b)$.

А я тем временем напомню, что в теореме о гомоморфизме у нас было отображение $\phi : a + I \to f(a)$ Проверим, что предлагается проверить. $\phi((a + I)(b + I)) = \phi(ab + I) = f(ab) = f(a)f(b) = \phi(a + I)\phi(b + I)$

□

***Определение* 3.1.** Пусть R_1, R_2 — кольца.

Определим $R_1 \oplus R_2 = \{(r_1, r_2)\}$, кольцо.

Зададим сложение: $(a,\ b) + (c,\ d) = (a + b,\ c + d)$

Зададим умножение: $(a,\ b) * (c,\ d) = (ab, cd)$.

Замечание. Аналогично вводится прямая сумма для большего числа слагаемых.

Замечание. Иногда преподаватели алгебры применяют обозначение $\times$ вместо $\oplus$ (смотрите далее).

Замечание. В данной конструкции много делителей нуля.

Действительно, любой элемент вида $(r,\ 0)$ или $(0,\ r)$ (в случае двух колец) является делителем нуля.

4. Билет 4

Здесь и далее в главе R означает коммутативное кольцо, а I, J – его идеалы.

Лемма. $I \cap J$ идеал.

Доказательство. Доказано выше где-то здесь. (1.16). □

***Определение* 4.1.** Определим $I + J = \{a + b \mid a \in I, b \in J\}$ как все возможные суммы.

Замечание. $I + J$ является идеалом, так как:

- $I + J$ несомненно образует подгруппу аддитивной группы кольца.
- $\forall a \in I, b \in J\ a + b \in I + J$. $\forall r \in R\ r(a + b) = ra + rb, ra \in I, rb \in J \Rightarrow ra + rb \in I + J$

Замечание. $I + J$ наименьший идеал содержащий и I и J. Иначе говоря, $I + J = (I \cup J)$, то есть идеал порождённый объединением.

***Определение* 4.2.** Произведение идеалов $IJ = (\{ab \mid a \in I, b \in J\})$ — это идеал порождённый всеми попарными произведениями.

Замечание. $IJ \neq \{ab \mid a \in I, b \in J\}$, так как полученное множество идеалом не является.

$$IJ = \{\sum a_i b_i \mid a_i \in I, b_i \in J\}.(ra)b, ra \in I$$

.

***Определение* 4.3.** Идеалы I, J называются взаимно простыми, если $I + J = R$.

Здесь и далее все кольца имеют единицу.

Лемма. Если I, J взаимно просты, то $IJ = I \cap J$

Доказательство.

- $IJ \subseteq I \cap J$.

  $\forall r \in IJ\colon r = \sum\limits_{i=1}^{N} a_i b_i$, где $a_i b_i \in I \cap J$ но это значит, что и их сумма лежит в пересечении. Мне тут было неочевидно, почему бы вдруг $a_i b_i \in I \cup J$. Так вот из определения идеала. $a_i \in I \Rightarrow a_i b_i \in I$, (если домножаемся на любой элемент и в том числе на b_i – попадаем в то же кольцо). Аналогично для J (помним про наличие коммутативности).

- $IJ \supseteq I \cap J$.

  I и J — взаимно просты $\implies I + J = R \ni 1$.

  $\implies \exists a \in I, b \in J$ такие что $a + b = 1$ (см 4.1)

  $\forall x \in I \cap J\colon x = x * 1 = x * (a + b) = xa + xb$.

  $xa \in (I \cap J)I$, $xb \in (I \cap J)J$. (Ну понятно для обоих произведений. $I \cup J$ – это меньше, и чем I, и чем J и одновременно их подмножества)

  $xa + xb \in IJ$. □

Замечание. Обратите внимание, что $IJ \subseteq I \cap J$ для всех идеалов I, J, так как в первой части леммы не пользуемся тем, что I, J — взаимно простые.

Теорема 4.1. Пусть R — коммутативное ассоциативное кольцо с 1, а I, J — взаимно простые идеалы.

Тогда $R/IJ \cong R/I \oplus R/J$

Замечание. В частном случае мы уже знаем это утверждение, если $(n, m) = 1$, то:

$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$.

Доказательство. $f\colon R \to R/I \oplus R/J$.

Сопоставим объекту два его класса по модулям I, J: $f(r) := (r \mod I, r \mod J)$, где $r \mod I = r + I$.

Каждая проекция является гомоморфизмом, значит f тоже гомоморфизм.

$\operatorname{Ker} f = \{r \in R \mid r \in I, r \in J\} = I \cap J = IJ$

По теореме о гомоморфизме колец (см 3.1) получаем требуемое. Осталось доказать, что полученное – эпиморфизм. Т.к. I и J взаимно простые, то $\exists a \in I, b \in J : \ a + b = 1$, тогда $\forall x, y \in R \ xb + ya$ – прообраз $(x + I, y + J)$.

□

Лемма. Пусть R — ассоциативное коммутативное кольцо с 1.

Если идеал I взаимно прост с каждым из идеалов $J_1, \ldots, J_k$, то I взаимно прост с их произведением $J_1 J_2 \ldots J_k$

Доказательство. $R = I + J_1 = I + J_1 R = I + J_1(I + J_2) = I + J_1 I + J_1 J_2 \subset I + J_1 J_2$

И, видимо, так как $I + J_1 J_2 \subset R$ как идеал кольца, то в последнем переходе можно поставить равенство.

И так далее до любого конечного k:

$R = I + J_1 J_2 = I + J_1 J_2 R = I + J_1 J_2 (I + J_3) = \ldots = I + J_1 J_2 J_3$

Здесь мы пользуемся определением идеала (1.15), суммы идеалов (4.1), определением взаимной простоты (4.3). □

5. Билет 5

Теорема 5.1 (Китайская Теорема об Остатках)**.** Пусть $I_1, I_2, \ldots, I_n$ — попарно взаимнопростые идеалы в R.

Тогда $R/_{I_1 I_2 \ldots I_n} \cong R/_{I_1} \oplus R/_{I_2} \oplus \ldots \oplus R/_{I_n}$

Доказательство. Доказательство теоремы несложно получить из индукции, предыдущей леммы и теоремы 4.1.

Есть такое. Если неочевидно, то индукция такая:
База: тривиальный фактор. Тогда всё изоморфно само себе, говорить не о чем.
Переход: отщепим любой нетривиальный нужный нам идеал I, взаимнопростой с оставшимися. По теореме, получим изоморфизм по факторам I и $J_1 J 2_2 \ldots$. Из леммы выше знаем, что если I взаимнопросто с оставшимися идеалами, то I и $J_1 J_2 \ldots$ тоже взаимнопросты. Применяем индукцию и радуемся □

Замечание. Если R — кольцо целых чисел, то теорему можно сформулировать следующим образом:

Пусть $m_1, m_2, \ldots, m_k$ — попарно взаимнопростые целые числа, $n := m_1 m_2 ... m_k$.

Тогда $\mathbb{Z}/_{n\mathbb{Z}} \cong \mathbb{Z}/_{m_1\mathbb{Z}} \oplus \ldots \oplus \mathbb{Z}/_{m_k\mathbb{Z}}$

Теорема 5.2 (Решение систем сравнений в целых числах)**.**
Для любого набора остатков $r_1 \ldots r_k$ $\exists x \in \mathbb{Z}$, такой что:

$$\begin{cases} x \equiv r_1 \mod m_1 \\ x \equiv r_2 \mod m_2 \\ \ldots \\ x \equiv r_k \mod m_k \end{cases} \qquad (m_i, m_j) = 1 \text{ для } i \neq j.$$

Причём если x и y являются решениями этой системы, то $x \equiv y \pmod n$.

Доказательство.

Определим $n := m_1 m_2 \ldots m_k$, $n_i := n/m_i$.

Так как m_i и n_i взаимнопросты, то $\exists x_i, y_i \in \mathbb{Z}$: $m_i x_i + n_i y_i = r_i$

С практической точки зрения их можно найти, например, с помощью алгоритма Евклида.

Заметим, что

- $n_i y_i \equiv r_i \pmod{m_i}$
- $n_i y_i \equiv 0 \pmod{m_j}$ для $j \neq i$

Первое следует из $m_i x_i + n_i y_i = r_i$, второе из $n_i = n/m_i = m_1 m_2 \ldots m_{i-1} m_{i+1} \ldots m_k$.

Определим $x := \sum_{i=1}^{k} n_i y_i$.

Тогда $\forall i$: $x \equiv n_i y_i \equiv r_i \pmod{m_i}$.

Вторая часть доказательства проще:

Пусть x — решение системы.

- Если y — решение, то $y - x \vdots m_i$, значит $y - x \vdots n$.

- Если y таков, что $y - x \vdots n$, то $y = x + nt$, подставляем в систему, nt сокращается.

□

6. Билет 6

***Определение* 6.1.** Элемент b делит элемент a (записывается как $b \mid a$), если $a = bc$ для некоторого $c \in R$.

Утверждение 6.1.

- $b|a \iff a \in bR \iff aR \subseteq bR$
- $a \in R^* \iff aR = R$

Доказательство.

- $a = bc\ c \in R \Rightarrow a \in bR \Rightarrow aR = b(cR) \subseteq bR$ так как $cR \subset R$
  И в обратную: $aR \subseteq bR \Rightarrow \forall x \in R \exists y \in R:\ ax = by \Rightarrow a * 1 = a \in bR \Rightarrow \exists c : a = bc \Rightarrow b|a$
- $\forall x \in R a^{-1}x \in R \Rightarrow aa^{-1}x = x \in aR$
  $\forall x \in R \exists y \in R : x = ay \Rightarrow \exists y : 1 = ay \Rightarrow a$ – обратим.

□

***Определение* 6.2.** Пусть I — идеал, тогда I простой, если $\forall a, b \in R$: $ab \in I \implies a \in I \vee b \in I$.

***Определение* 6.3.** I — максимальный, если для любого идеала J: $I \subsetneq J \subset R \implies J = R$.

Лемма. Пусть I — идеал R, тогда $\exists J$ — идеал, $I \subseteq J \subseteq R$ и J максимальный.

Доказательство. Рассмотрим множество $X = \{K \mid K$ — идеал в$R, K \supseteq I, K \neq R\}$, введём на нём частичный порядок включения ($\subseteq$).

Покажем, что любое линейно упорядоченное подмножество X имеет верхнюю грань.

Пусть $\{L_i\}$ — произвольное линейно упорядоченное подмножество, $L := \bigcup L_i$.

Рассмотрим произвольные $a, b \in L$, тогда $a \in L_i, b \in L_j$ (для некоторых i, j).

Но множество линейно упорядоченно, значит одно лежит в другом (совпадение тоже допускается), без потери общности давайте считать, что $L_i \subseteq L_j$.

Следовательно $a, b \in L_j \implies a - b \in L_j \subseteq L$.

Также $\forall r \in R$: $ra \in L_j \subseteq L$.

Итого мы получаем по определению (1.15), что L — идеал. Значит любое линейное упорядоченное подмножество X имеет верхнюю грань, значит (по лемме Цорна) в множестве X есть максимальный элемент.

Соответственно этот максимальный элемент и является максимальным идеалом. □

Замечание. R — область целостности $\iff \{0\}$ — простой идеал.

Область целостности $\iff ab = 0 \implies a = 0 \vee b = 0$.

Идеал простой $\iff ab \in \{0\} \implies a \in \{0\} \vee b \in \{0\}$.

Утверждение 6.2. Пусть R — коммутативное ассоциативное кольцо с 1, I — идеал в R, тогда:

1. I — простой $\iff R/_I$ — область целостности.
2. I — максимальный $\iff R/_I$ — поле.
3. Если I — максимальный, то I — простой.

Доказательство.

“$\to$”. (!) в $R/_I$ нет делителей нуля.

$(a+I)(b+I) = I \implies a \in I \vee b \in I$.

$(a+I)(b+I) = ab + I$

“$\leftarrow$” $(a+I)(b+I) = I \Rightarrow a + I \in I \vee b + I = I \Rightarrow a \in I \vee b \in I$

Тут было написано что-то не очень похожее на правду. Смотрите следствие 9 в конспекте лектора □

Далее R область целостности

Утверждение 6.3. В кольце главных идеалов R любой ненулевой простой идеал I является максимальным

Доказательство. $I = pR$, пусть $I \subsetneq J \subseteq R$, J — идеал.

R — КГИ $\implies J = qR \;\; pR \subseteq qR \subseteq R$

$p = qr$, pR — простой $\implies (q \in pR \implies pR = qR) \vee (r \in pR \implies r = ps)$.

$p = qr = qspp(1 - qs) = 0 \implies q \in R^* \iff qR = R$.

Если не получилось, страница 32 конспекта лектора, там даже нет слова «очевидно» □

7. Билет 7

Пусть R — область целостности.

***Определение* 7.1.** $a, b \in R$, a и b ассоциированные, если $aR = bR$.

(или, эквивалентно, $aR \subseteq bR$, $bR \subseteq aR \iff a|b, b|a$).

Пример 1. В $\mathbb{Z}$ n и m ассоциированы, если $n = m$ или $n = -m$.

Пример 2. В $K[x]$ (где K — поле) f и g ассоциированы, если $f(x) = cg(x)$, $c \in K[x] \setminus \{0\}$.

Пусть $a \sim b$, если a ассоциирован с b.

***Определение* 7.2.** Пусть $a \in R \setminus R^*$. Элемент a неприводим, если $a = bc \implies a \sim b \vee a \sim c$.

***Определение* 7.3.** Пусть $p \in R \setminus R^*$. Элемент p называется простым, если $p \mid ab \Rightarrow p \mid a \vee p \mid b$.

Замечание. Ассоциированость является отношением эквивалентности.

Лемма. Пусть $a, b \in R \setminus \{0\}$, тогда:

1. $a \sim b \iff a = b\varepsilon$, где $\varepsilon \in R^*$.
2. a — неприводим $\iff (a = cd \implies c \in R^* \vee d \in R^*)$.

Доказательство.

1. - “$\implies$”

     $a \sim b \iff \begin{cases} b|a \implies a = b\varepsilon \implies a = a\delta\varepsilon \implies a(1 - \delta\varepsilon) = 0 \implies \delta\varepsilon = 1 \implies \varepsilon \in R^* \\ a|b \implies b = a\delta \end{cases}$

     Пользуемся тем, что мы в области целостности, а также тем, что $a \neq 0$.
   - “$\impliedby$”

     a и b ассоциированные $\iff a \mid b$, $b \mid a$.

     $a = b\varepsilon$, $b = a\varepsilon^{-1}$ (пользуемся коммутативностью, обратимостью ε).

     После этого делимость очевидна по определению (см 6.1)
2. $a = bc \implies (a \sim b \vee a \sim c)$

   Пусть б.п.о. $a \sim b \implies a = b\varepsilon, \varepsilon \in R^* \implies b\varepsilon = bc \implies b(\varepsilon - c) = 0 \implies c = \varepsilon$. $a = bc$

□

***Определение* 7.4.** R — область целостности. R — факториально, если любой элемент единственным образом раскладывается в произведение неприводимых.

Единственность вплоть до порядка и ассоциированости:

Если $\varepsilon p_1 p_2 \dots p_n \sim \Theta q_1 q_2 \dots q_m$ (где p_i, q_j неприводимы, $\varepsilon, \Theta \in R^*$), то $n = m$ и $\exists \sigma \in S_n \colon p_i \sim q_{\sigma(i)}$

Теорема 7.1. Если R — кольцо главных идеалов, то R факториально.

Доказательство состоит из нескольких лемм:

Лемма (1)**.** R — кольцо главных идеалов, $a, c \in R, c$ — неприводим, $\neg c|a \implies aR + cR = R$

Доказательство. R — кольцо главных идеалов $\implies aR + cR = bR \implies c \in bR \implies c = bd$.

Так как c неприводим, то $c \sim b$ или $b \in R^*$.

Но $c \sim b \iff cR = bR$, но тогда $a \in bR = cR$, т.е. $c|a$, но это ложь.

$b \in R^* \iff bR = R$, что мы и хотели. □

Лемма (2)**.** R — кольцо главных идеалов, $a, b, c \in R$, c неприводим.

Тогда $(c|ab \implies c|a \vee c|b)$

Иначе говоря, cR простой: $ab \in cR \implies a \in cR \vee b \in cR$

Доказательство. $c|ab$, пусть $\neg c|a$ и $\neg c|b$.

Тогда по предыдущей лемме $cR + aR = R$ и $cR + bR = R$, из чего по какой-то лемме из китайской теоремы об остатках следует, что cR взаимно прост с $(aR)(bR) = abR$.

Итого: $cR + abR = R$ и $ab \in cR$.

Но $cR + abR = cR$ (так как $c|ab$), следовательно $cR = R$, что возможно $\iff$ обратим.

Но c неприводим, противоречие. □

***Определение* 7.5.** Кольцо R называется нётеровым, если для любой последовательности идеалов I_n в R, такой что $I_1 \leqslant I_2 \leqslant I_3 \leqslant \ldots$, все идеалы начиная с некоторого места совпадают.

Лемма (3)**.** Если R — кольцо главных идеалов, то R нётерево.

Доказательство. Так как R — кольцо главных идеалов, то каждый идеал $I_k = r_k R$ для некоторого r_k.

Докажем, что $I := \bigcup\limits_{i=1}^{\infty} I_i$ идеал:

- $a, b \in I \implies a, b \in I_i \implies a - b \in I_i \implies a - b \in I$
- $a \in I \implies a \in I_i \implies \forall r\colon ra \in I_i \implies \forall r\colon ra \in I$

(Первое условие гарантирует, что I — является подгруппой аддитивной группы кольца, хотя это немного не очевидно сходу. Hint: a может быть равно 0).

Следовательно $I = qR$, для некоторого $q \in R$ (так как мы в кольце главных идеалов).

Следовательно $\exists n\colon q \in I_n = r_n R$ (Если $I = qR$, то q лежит в объединении, значит, q лежит в каком-то идеале начиная с какого-то n)

$q \in I_{n+1} = r_{n+1}R \implies qR \subseteq I_{n+1}$, но $qR \supseteq I_{n+1} \implies qR = I_{n+1}$. □

8. Билет 8

Напомню, что мы доказываем такую теорему:

Если R — кольцо главных идеалов, то R факториально.

Лемма (4)**.** Пусть R — кольцо главных идеалов. Тогда любой ненулевой необратимый элемент раскладывается в произведение неприводимых.

Доказательство. $r \in R \setminus R^*, r \neq 0$.

rR содержится в некотором максимальном идеале M.

$M = p_1R, rR \subseteq p_1R \iff r = p_1r_1, r_1 \in R$

p_1R — max $\implies$ p_1R — простой $\implies$ $(ab \vdots p_1 \implies a \vdots p_1 \vee b \vdots p_1)$

$p_1 = ab \implies a \sim p_1 \vee b \sim p_1$

И из всего этого следует, что p_1 неприводим, т.е.

$r = p_1r_1$, p_1 неприводим.

Если $r_1 \in R^*$, то $r = p_1r_1$ — искомое разложение. Хз.

Если $r_1 \notin R^*$, то $r_1R \neq R$, поэтому $r_1R \subseteq p_2R$ — максимальный. $r = p_1p_2r_2$.

И так далее можно продолжать раскладывать.

Либо $r_k \in R^*$, тогда успех.

$$r_1 = p_2r_2, r_1R \subseteq r_2R \tag{1}$$
$$r_2 = p_3r_3, r_2R \subseteq r_3R \tag{2}$$

$\implies r_1R \subsetneq r_2R \subsetneq r_3R \ldots$, далее всё хорошо по лемме 3. □

Лемма (5)**.** Если:
- R — область целостности.
- $\forall$ неприводимого элемента его идеал прост.
- $\forall$ ненулевого необратимого элемента есть разложение в произведение

То R — факториально.

Доказательство. Достаточно доказать единственность разложения, воспользуемся индукцией по $\min(n, m)$

$n = 0$, ...

Переход: $n > 0 p_n$ — неприводим $\implies$ p_nR — прост.

$\exists l\colon 1 \leqslant l \leqslant m, q_l \in p_nR, q_l \vdots p_n$. Объяснение от меня (возможно, есть проще): $\theta q_1q_2 \ldots q_m = p_n(\epsilon p_1p_2 \ldots p_{n-1}) \in p_nR \Rightarrow \theta \in p_nR \vee q_1q_2 \ldots q_m \in p_nR$. Если из них лежит обратимый, то p_nR – всё кольцо. Короче, $q_1q_2 \ldots q_m \in p_nR$ 100% Теперь $q_1 \in p_nR \vee q_2 \ldots q_m \in p_nR$ и так далее... Приходим к тому, что $\exists q_l \in p_nR$.

a) q_l — неприводим, $q_l = p_n\delta$ (т.к. q_l в кольце), $\delta \in R^* \implies q_l \sim p_n$.

b) Также $\varepsilon p_1 \ldots p_n \sim \Theta q_1 \ldots q_m$

(a), (b) $\implies \varepsilon p_1 \ldots p_{n-1} \sim \Theta q_1 \ldots q_{l-1}q_{l+1} \ldots q_m$.

По предположению индукции $n - 1 = m - 1 \implies n = m$

$\exists$ биекция $t\colon \{1, \ldots, n-1\} \to \{1, \ldots l-1, l+1, \ldots m\}$, $p_i \sim q_{t(i)}$.

$$sigma \in S_n \colon \sigma(i) = \begin{cases} t(i) & i \leqslant n-1 \\ l & i = n \end{cases}$$ □

Замечание. Из всего вышесказанного следует теорема о факториальности кольца главных идеалов.

9. Билет 9

***Определение* 9.1.** Пусть R — область целостности, назовём R евклидовым, если $\exists \nu\colon R\setminus\{0\} \to \mathbb{N}\sqcup\{0\}$:

$\forall a, b \in R\setminus\{0\}$:

1) $\nu(ab) \geqslant \nu(a)$

2) $\exists q, r \in R\colon a = bq + r$ и $r = 0 \vee \nu(r) < \nu(b)$

Функция ν называется евклидовой нормой.

Пример 1. $\mathbb{Z}$, $\nu(x) = |x|$.

Пример 2. K — поле, рассмотрим $K[x]$: $\nu(f) = \deg f$.

Пример 3. $\mathbb{Z}[i] := \mathbb{Z}[x]/_{(x^2+1)},\ \nu(a+bi) = a^2 + b^2$

Пример 4. $\mathbb{Z}[i] := \mathbb{Z}[x]/_{(x^2+x+1)},\ \nu(a+bi) = a^2 + b^2 - ab$

Утверждение 9.1. Евклидовы кольца $\subset$ кольца главных идеалов $\subset$ факториальные $\subset$ области целостности.

Доказательство. Покажем, что R — евклидово кольцо, то R — кольцо главных идеалов.

Рассмотрим произвольный нетривиальный идеал I в R (если $I = \{0\}$, то $I = 0R$)

Рассмотрим элемент $b \in I$ с минимальной нормой: $\nu(b) = \min\limits_{r\in I} \nu(r)$, покажем, что $bR = I$.

Пусть $a \in I$, тогда $\exists q, r\colon a = bq + r$, причём $r = 0 \vee \nu(r) < \nu(b)$.

Но $r = a - bq \in I$, так как $a \in I, bq \in I$.

Так как b имеет минимальную норму, то $r = 0$ или $\nu(r) \geqslant \nu(b)$, следовательно $r = 0$, $a = bq$.

Так как выбрать a можно произвольно, получаем, что идеал I главный $(I = bR)$ □

10. Билет 10

R — область целостности.

***Определение* 10.1.** $d = \gcd(a, b)$, если $d|a$, $d|b$, и из $c|a$, $c|b$, следует $c|d$.

Замечание.

1. $d = gcd(a, b) \iff dR$ — наименьший главный идеал, содержащий и a и b. $(aR + bR)$.
2. gcd Определён с точностью до ассоциативности.

Теорема 10.1.
Пусть R — кольцо главных идеалов.

$a, b \in R$, тогда $\exists x, y \in R$: $ax + by = gcd(a, b)$.

Доказательство. R — кольцо главных идеалов $\implies$
$aR + bR = dR$ и $gcd(a, b) = d \in dR = aR + bR = \{ax + by \mid x, y \in R\}$. □

***Определение* 10.2.** a, b — взаимно простые, если у них нет необратимых общих делителей.

Утверждение 10.2. R — кольцо главных идеалов, $a, b \in R$. Тогда a,b — взаимно простые $\iff$ aR, bR — взаимно простые.

Доказательство. a, b — взаимно простые $\iff$ $1 = gcd(a, b)$ $\iff$ $1 = ax + by$ $\iff$ $R = aR + bR$ $\iff$ aR, bR — взаимно простые. □

***Определение* 10.3.** $a, b \in R, l = \operatorname{lcm}(a, b)$, если $a \mid l$, $b \mid l$, и если $a \mid c, b \mid c \implies l \mid c$.

Замечание. $l = \operatorname{lcm}(a, b) \iff lR$ — наибольший главный идеал, содержащийся в $aR \cap bR$.

Замечание. $a|b \iff bR \subseteq aR$.

Теорема 10.3. a, b — кольцо главных идеалов, $a, b \in R \setminus \{0\}$, тогда $\operatorname{lcm}(a, b) = ab/gcd(a, b)$.

При этом последнее равенство верно с точностью до ассоциированности.

Доказательство. $d = \gcd(a, b)$.

$a = a'd$, $b = b'd$, $a', b' \in R$.

$d = ax + by \implies 1 = a'x + b'y$, более формально:

$d(1 - a'x - b'y) = 0$, но $d \neq 0$ а R — область целостности, следовательно $1 - a'x - b'y = 0$.

$\operatorname{lcm}(a, b)R = aR \cap bR$. (Т.к. все идеалы главные, а мы ищем максимальный из всех вложенных)

$ab/d = a'b'd$.

$c \in aR \cap bR$

$c \in bR, ca' \in ba'R$, $c \in aR, cb' \in ab'R$

$c = c * 1 = ca'x + cb'y \in ba'R + ab'R = a'b'dR$.

$\operatorname{lcm}(a, b)R = aR \cap bR \subseteq a'b'dR = \frac{ab}{d}R$

“$\supseteq$”,

$$a'b'd = ab' \in aR \tag{3}$$

$$a'b'd = ba' \in bR \tag{4}$$

$a'b'd \in aR \cap bR \implies a'b'dR \subseteq aR \cap bR \Rightarrow lcm = a'b'd = \frac{ab}{d}$ с точностью до ассоциативности.

□

11. Билет 11

Далее мы требуем Евклидовости кольца.

Лемма. $\forall a, b, c \in R\colon\ \gcd(a, b) = \gcd(a - bc, b)$.

Доказательство. $\gcd(a, b)R =^{?} \gcd(a - bc, b)R$.

$\gcd(a, b)R = aR + bR$, $\gcd(a - bc, b)R = (a - bc)R + bR$.

"$\supseteq$" $a - bc \in aR + bR, b \in aR + bR$.

"$\subseteq$" $b \in bR \subseteq (a - bc)R + bR$, $a = (a - bc) + bc \in (a - bc)R + bR$. □

Лемма. $\gcd(a, 0) = a$

Замечание. $\gcd(a, b)R = aR + bR = (a,\ b)$, где последнее означает идеал, порождённый a и b.

Поэтому часто наибольший общий делитель обозначают через $(a,\ b)$.

Алгоритм:

$a, b \in R, \nu$ — евклидова норма.

$a = bq_0 + r_0\ b = r_0q_1 + r_1$

...

$r_i = r_{i+1}q_{i+2} + 0$

(Если здесь вам стало плохо, в конспекте лектора есть пояснение в словах. Алгоритм Евклида стр. 36)

Утверждается, что $r_{i+1} = (a, b)$.

$r_0 = 0 \vee \nu(r_0) < \nu(b)$, $(a, b) = (a - bq_0,\ b) = (r_0,\ b) = (b,\ r_0)$

$r_1 = 0 \vee \nu(r_1) < \nu(r_0)$, $(b,\ r_0) = (r_0,\ r_1)$

Также полезен факт, что мы движемся строго по убыванию евклидовой нормы, откуда понятно, что процесс конечен .

12. Билет 12

Теорема 12.1. Пусть $f, g \in K[x]$, $g \neq 0$. Тогда $\exists! \, q, r \in K[x] \colon f = gq + r$, где $\deg r < \deg g$.

Доказательство.

Существование, индукция по степени f

- Если $\deg f < \deg g$, то $r = f, q = 0$.
- $f(x) = a_0 + a_1 x + \dots a_n x^n$, $g(x) = b_0 + b_1 x + \dots b_m x^m$, $a_n \neq 0, b_m \neq 0$.
  $f_1(x) := f(x) - g(x)\frac{a_n}{b_m} x^{n-m}$, здесь мы пользуемся тем, что в поле можно делить на любой ненулевой элемент.
  $\deg f_1 < n \overset{\text{по индукции}}{\Longrightarrow} \exists q_1, r_1 \colon f_1 = q_1 g + r_1, deg(r_1) < deg(g)$
  $f = g\frac{a_n}{b_m} x^{n-m} + f_1 = g\frac{a_n}{b_m} x^{n-m} + gq_1 + r_1 = g(\frac{a_n}{b_m} x^{n-m} + q_1) + r_1$

Покажем единственность

- Пусть есть разные разложения.
- $f = q_1 g + r_1 = q_2 g + r_2$, где $q_1, q_2, r_1, r_2 \in K[x]$, $\deg r_1, \deg r_2 < \deg g$.
- $(q_1 - q_2)g = r_2 - r_1$, если $q_1 \neq q_2$, то степень слева строго больше степени справа. Если $q_1 = q_2$, то $r_1 = r_2$.
- Противоречие. □

Утверждение 12.2. Пусть R — область целостности.

$\forall f, g \in R[x], \ g \neq 0, \ g = b_k x^k + b_{k-1} x^{k-1} + \dots + b_0, \ b_k \in R^* \cup \{0\}$.

Тогда $\exists q, r \in R[x] \colon f = gq + r$, такие что $\deg r < \deg g$.

Замечание. Обратите внимание, что достаточно обратимости только элемента b_k, так как мы всегда делим именно на него.

Доказательство. Аналогично предыдущему доказательству. Вот вообще аналогично. Я могла бы сделать ctr-c ctrl-v. □

13. Билет 13

Пример 1. Рассмотрим $\mathbb{R}[x]$ (множество многочленов с вещественными коэффициентами).

Примеры его идеалов:

- $\mathbb{R}[x]$
- $\{0\}$
- $I = \{f \in \mathbb{R}[x] \mid f(0) = 0\} = x\,\mathbb{R}[x]$ (свободный коэффициент нулевой, а значит можно поделить на x, что и записано в последнем равенстве).
- $I = P(x)\,\mathbb{R}[x]$, где $P(x) \in \mathbb{R}[x]$
- Первые три пункта тоже подходят под последний. На самом деле (факт без доказательства) все идеалы имеют такой вид.

Пример 2. Рассмотрим $\mathbb{Z}[x]$ (множество многочленов с целыми коэффициентами):

- $P(x)\mathbb{Z}[x]$, где $P(x) \in \mathbb{Z}[x]$
- Но не все идеалы имеют такой вид, например: $(x-3)\mathbb{Z}[x] + 2\mathbb{Z}[x]$.
- **Упражнение:** понять почему последнее действительно идеал. (Потому что это сумма идеалов)

Утверждение 13.1. Если в кольце R нет делителей нуля, то в $R[x]$ их тоже нет.

Доказательство. Пусть в $R[x]$ есть делители нуля, иначе говоря

$(a_t x^t + \ldots + a_1)(b_k x^k + \ldots + b_1) = 0$.

Потребуем, что $a_t \neq 0$ и $b_k \neq 0$, т.е. это старшие коэффициенты в соответствующих многочленах.

Заметим, что при степени x^{t+k} будет коэффициент $a_t b_k$. Но так как справа нулевой многочлен, то все коэффициенты произведения равны 0.

То есть $a_t b_k = 0$, но в R нет делителей нуля, противоречие. □

Как мы обсуждали выше, $K[x]$ является полем, если полем является K. При чём в этом поле все идеалы имеют вид $f(x)K[x]$, обозначим этот идеал как $I = f(x)K[x] = (f(x))$. (напомним, что запись в скобках означает идеал, порождённый элементом, см 1.17).

Также мы обсуждали, что многочлены можно делить с остатком:

Для любого $g(x)$ существуют единственные $q(x), r(x)$, такие что $g(x) = q(x)f(x) + r(x)$ и $\deg r < \deg f$

Замечание. $g(x) \equiv r(x) \pmod{I}$, просто по определению mod (см 2.3).

Замечание. Тем самым все многочлены, имеющие одинаковый остаток при делении на какой-то многочлен $f(x)$ сравнимы друг с другом по модулю.

Лемма. Если $r_1, r_2, f \in K[x]$, $r_1 \equiv r_2 \mod (f(x)K[x])$ и $\deg r_1, \deg r_2 < \deg f$, то $r_1 = r_2$

Доказательство.

$r_1 \equiv r_2 \pmod{f(x)K[x]} \implies r_1 - r_2 = fh$ для некоторой функции h.

- Если $h(x) = 0$, то $r_1 = r_2$.
- Но если $h(x) \neq 0$, то $\deg(fh) \geqslant \deg(f)$, но $\deg(r_1 - r_2) < \deg(f)$. Противоречие. □

Замечание. Неформально можно думать о факторе $K[x]/_{f(x)K[x]}$ как о многочленнах со степенью меньшей f. $K[x]/I \simeq \{r \in K[x] \mid \deg r < \deg f\}$.

Лемма. Пусть R — область целостности (как частный случай — поле), $f, g \in R[x],\ \alpha \in R$

1. Если $f(\alpha) = 0$, то $f(x) = (x - \alpha)q(x)$, где $q(x) \in R[x]$, $\deg q = deg f - 1$.
2. Если $n = \deg f$, то f имеет не более n различных корней в R.
3. Если $\deg f = \deg g = n$ и $f(\alpha_1) = g(\alpha_1), \ldots, f(\alpha_{n+1}) = g(\alpha_{n+1})$. где $\alpha_i \in R$ и различны. Тогда многочлены равны (т.е. попарно равны все коэффициенты).

Доказательство.

1. Поделим f на $x - \alpha$ с остатком:

   $f(x) = (x - \alpha)q(x) + r,\ \deg r < deg(x - \alpha) = 1 \implies \deg r = 0 \implies r$ – константа.

   $f(x) = (x - \alpha)q(x) + C$.

   $f(\alpha) = 0 + C \implies C = 0$ (так как α — корень).

2. Индукция по n:

   База ($n = 1$). $f(x) = ax + b$ ($a \neq 0$) корней явно не более, чем один. Если a необратим, то вообще ноль.

   Переход. Пусть f имеет корни (иначе $0 \leqslant n$) и α — один из них.

   $f(x) = (x - \alpha)\, q(x)$, $\deg q = n - 1$

   q имеет не более чем $n - 1$ корень. Конец.

3. $h(x) = f(x) - g(x)$, $\deg h \leqslant n$, $h(\alpha_i) = 0$ для $n + 1$ альф.

   Но многочлен не может иметь более n корней, следовательно он нулевой. □

Замечание. Можно считать, что $\deg 0 = \infty$, тогда все равенства остаются верными и для этого случая.

Замечание. Лемма выше верна только в области целостности

14. Билет 14

Краткое содержание предыдущих серий:

- $K[x]$ — поле многочленов.
- $K[x]$ — евклидово с нормой deg.
- Многочлены можно делить с остатком.
- Остаток от деления многочлена p на $(x-\alpha)$ есть $p(\alpha)$.

***Определение* 14.1.** Для многочлена $f(x) = a_n x^n + \dots a_1 x + a_0$:

$f'(x) = n a_n x^{n-1} + \dots + a_1$

Под $f^{(k)}(x)$ понимается как производная взятая $k \in \mathbb{N} \sqcup \{0\}$ раз, (причём $f^{(0)}(x) := f(x)$).

Замечание. Многочлены и производные мы понимаем как формальное выражение, в частности многочлен это конечная(!) последовательность коэффициентов, записывающаяся особым образом, а производная — это функция из множества многочленов в его же самого.

Лемма. 1. $(p \pm q)' = p' + q'$

2. $(pq)' = p'q + pq'$
3. $(\alpha p)' = \alpha p'$
4. $(p \circ q)' = (p' \circ q)q'$.

Замечание. Нужно отметить, что эти утверждения НЕ следуют из соответствующих утверждений математического анализа, например по тому, что здесь производная определяется другим образом.

Более того, если рассмотреть $K = \mathbb{Z}/_{p\mathbb{Z}}$, то многочлены $x^p - x$ и 0 — это разные многочлены, хотя если рассмотреть их как функции, то они обе тождественно равны 0.

Доказательство.

1. $(p \pm q)' = (\sum a_i x^i \pm b_i x^i)' = (\sum x^i (a_i \pm b_i))' = \sum i x^{i-1}(a_i \pm b_i) = \sum i x^{i-1} a_i \pm i x^{i-1} b_i = p' + q'$
2. $(pq)' = (\sum\sum x^{i+j} a_i b_j)' = \sum (\sum x^{i+j} a_i b_j)' = \sum\sum (i+j) x^{i+j-1} a_i b_j = \sum\sum i x^{i-1} x^j a_i b_j + j x^{j-1} x^i a_i b_j = \sum\sum i x^{i-1} x^j a_i b_j + \sum\sum j x^{j-1} x^i a_i b_j = \sum i x^{i-1} a_i (\sum x^j b_j) + \sum j x^{j-1} b_j (\sum x^i a_i) = (\sum i x^{i-1} a_i)(\sum x^j b_j) + (\sum j x^{j-1} b_j)(\sum x^i a_i) = p'q + q'p$
3. Можно я скажу, что это очевидно?
4. $(p \circ q)' = (\sum a_i q^i)' =^! \sum i a_i q^{i-1} q'$
   Доказательство по индукции. $n = 1$ (длина p, а так мне лень прописывать суммы)
   $n - 1 \to n$.

$$(\sum a_i q^i)' = (q \sum a_i q^{i-1} + a_0)' = q' \sum a_i q^{i-1} + q(\sum a_i q^{i-1})' \overset{\text{предположение}}{=}$$
$$q' \sum a_i q^{i-1} + q q' \sum a_i (i-1) q^{i-2} = q' \sum a_i (q^{i-1} + (i-1) q_{i-1}) = q' \sum a_i i q_{i-1} = q'(p' \circ q)$$

□

Лемма (5)**.** $f(x) = \sum\limits_{i=0}^{n} \frac{f^{(i)}(a)}{l!}(x-a)^l$

Доказательство. Оставлено в качестве упражнения. □

15. Билет 17

Лемма. $d = \gcd(a, m)$, $|\{x \in \mathbb{Z}/_{m\mathbb{Z}} \mid ax = b\}| = \begin{cases} 0 & \neg d \mid b \\ |d| & d \mid b \end{cases}$

Если $d \mid b$, то $\{x \in \mathbb{Z}/_{m\mathbb{Z}} \mid ax = b\} = \{x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \ldots, x_0 + (d-1)\frac{m}{d}\}$.

Доказательство.

1. Пусть $\neg d \mid b$.

   Если x_0 — решение, $ax_0 - b = mk$, где $k \in \mathbb{Z}$.

   $d \mid a, d \mid m$, $b = ax_0 - mk = da'x_0 - dm'k = d(a'x_0 + m'k) \implies d \mid b$

2. $d \mid b$ $(b = db')$

   $d = \gcd(a, m) \implies \exists x, y\colon ax + my = d$ (см в расширенный алгоритм Евклида)

   $ab'x + mb'y = db' = b \implies ab'x = b \pmod m$

   $x_0 = b'x$ — решение.

3. а) Если x_0 — решение, то $x_0 + k\frac{m}{d}$

   б) Пусть x_1 — решение, т.е. $ax_1 \equiv b \pmod m$, $ax_0 \equiv b \pmod m \implies a(x_1 - x_0) \equiv 0 \pmod m$

   $\frac{a}{d}(x_1 - x_0) \equiv 0 \pmod{\frac{m}{d}}$

□

Замечание. $\gcd(a, b) = d = ax + my \implies 1 = \frac{a}{d}x + \frac{m}{d}y \iff \frac{a}{d}, \frac{m}{d}$ — взаимно простые.

$\frac{a}{d}(x_1 - x_0) \vdots \frac{m}{d}$

$x_1 - x_0 \equiv 0 \pmod{\frac{m}{d}}$

$x_1 = x_0 + l\frac{m}{d}$.

§Диофантовы уравнения в целых числах

Лемма. $d = \gcd(a, b)$

Тогда если $\neg d \mid c$, то "$ax + by = c$" неразрешимо в $\mathbb{Z}$

А если $d \mid c$, то "$ax + by = c$" разрешимо и все решения имеют вид:

$x = x_0 + \frac{b}{d}k, y = y_0 - \frac{a}{d}k$, $k \in \mathbb{Z}$.

Доказательство. 1) Если $x_0, y_0 \in \mathbb{Z}$, $ax_0 + by_0 = c$, то $d \mid a$, $d \mid b$, $d \mid (ax_0 + by_0)$, т.е $d \mid c$.

2) Если $d \mid c$, то $c = dc'$

$d = \gcd(a, b) \implies ax + by = d$, $x, y \in \mathbb{Z}$.

$axc' + byc' = dc' = c \implies x_0 = xc', y_0 = yc'$.

3) Если $ax_1 + by_1 = c$, $ax_0 + by_0 = c \implies a(x_1 - x_0) + b(y_1 - y_0) = 0$.

$\frac{a}{d}(x_1 - x_0) = -\frac{b}{d}(y_1 - y_0)$.

$d = (a, b) \implies \frac{a}{d}, \frac{b}{d}$ — взаимно простые.

$x_1 - x_0 \vdots \frac{b}{d} \implies x_1 - x_0 = k\frac{b}{d}, y_1 - y_0 = -k\frac{a}{d}$, где $k \in \mathbb{Z}$. □

16. Билет 18

***Определение* 16.1.** Функция Эйлера — это $\phi(n) :=$ порядок группы $(\mathbb{Z}/_{n\mathbb{Z}})^*$

Замечание. Напоминание, "$*$" означает обратимую часть моноида, в данном случае.

Лемма. Класс элемента m обратим в $(\mathbb{Z}/_{n\mathbb{Z}})^* \iff \gcd(m, n) = 1$.

Доказательство. Нужно решить $mx = 1 \pmod n$

Это тоже самое, что решать $mx + tn = 1$, найти m, t.

Расширенный алгоритм Евклида вам в помощь. □

Следствие. $\phi(n) =$ количество чисел от 1 до $n - 1$ взаимнопростые с n

Следствие. Если p — простое, то $\phi(p) = |(\mathbb{Z}/_{n\mathbb{Z}})^*| = p - 1$

Лемма. Пусть R — кольцо с 1, $R = \bigoplus_{i=1}^{n} R_i$.

Тогда $R^* \cong \times_{i=1}^{n} R_i^*$

Доказательство. У нас уже есть $R \cong \bigoplus_{i=1}^{n} R_i$ и соответсвующий изоморфизм ψ.

Заметим, что если $r \in R^*$, то ему соответствует кортеж обратимых элементов.

Действительно, обратимый элемент при гомоморфизме переходит в какой-то обратимый $(r_1, r_2, \ldots, r_n)$.

То есть есть $(t_1, t_2, \ldots, t_n)$, такой что $(r_1, r_2, \ldots, r_n)(t_1, t_2, \ldots, t_n) = (1, 1, \ldots, 1)$.

Да, что и требовалось, каждый из r_i обратим.

Также если у нас есть элемент в $\times_{i=1}^{n} R_i^*$, то ему, очевидно (очевидно, когда знаешь слово изоморфизм), соответствует элемент из R^* (так как его можно обратить, просто обратив каждую из компонент).

Тем самым $\psi(R^*) = \times_{i=1}^{n} R_i^*$ и мы достигли успеха (можно сузить гомоморфизм ψ на R^*, при этом он гомоморфизмом и останется. □

Теорема 16.1.

1. Если $\gcd(a, b) = 1$, то $\phi(ab) = \phi(a)\phi(b)$
2. Если p — простое, $k \in \mathbb{N}$, то $\phi(p^k) = p^{k-1}(p - 1)$
3. Если $n = \prod\limits_i p_i^{k_i}$, то $\phi(n) = \prod\limits_i p_i^{k_i - 1}(p_i - 1) = n \prod\limits_i \frac{p_i - 1}{p_i}$

Доказательство.

1. По китайской теореме об остатках $\mathbb{Z}/_{ab\mathbb{Z}} \cong \mathbb{Z}/_{a\mathbb{Z}} \oplus \mathbb{Z}/_{b\mathbb{Z}}$.
   Применим лемму, $(\mathbb{Z}/_{ab\mathbb{Z}})^* \cong (\mathbb{Z}/_{a\mathbb{Z}})^* \times (\mathbb{Z}/_{b\mathbb{Z}})^*$
   $\phi(ab) = |(\mathbb{Z}/_{a\mathbb{Z}})^* \times (\mathbb{Z}/_{b\mathbb{Z}})^*| = \phi(a)\phi(b)$
2. $\phi(p^k) = p^k - \frac{p^k}{p} = p^{k-1}(p - 1)$
   Среди всех чисел от 0 до $p^k - 1$ подойдут все, кроме $\vdots\, p$, а такой у нас ровно каждый p-тый.
3. Следует из индукции, и первых двух пунктов. □

17. Билет 19

Теорема 17.1 (Эйлера)**.** Если $\gcd(a,\, n) = 1$, то $a^{\phi(n)} = 1 \pmod n$

Замечание (Формулировка в теории групп). Если $\gcd(a,\, n) = 1$, то $\bar{a}^{\phi(n)} = 1$ в $(\mathbb{Z}/_{n\mathbb{Z}})^*$, где $\bar{a}$ — класс числа a.

Доказательство. Рассмотрим $x \in (\mathbb{Z}/_{n\mathbb{Z}})^*$, по теореме лагранжа порядок элемента x делит порядок группы.

Иначе говоря, $x^s = 1$, где $s = |(\mathbb{Z}/_{n\mathbb{Z}})^*|$, но $s = \phi(n)$ по определению. □

Следствие (Малая теорема Ферма). Если p — простое, и $\gcd(a,\, p) = 1$, то $a^{p-1} \equiv 1 \pmod p$

Теорема 17.2 (Вильсона)**.** Если p — простое, то $(p-1)! \equiv -1 \pmod p$.

Доказательство. Рассмотрим поле $Z/_{p\mathbb{Z}}$ (так как p — простое, то всё обратимо, см леммы выше).

$f(x) := x^{p-1} - 1$, $g(x) := (x-1)(x-2)\dots(x-(p-1))$.

Заметим, что $f(x) = g(x) = 0$ для всех $x \neq 0$, $x \in \mathbb{Z}/_{p\mathbb{Z}}$.

Рассмотрим $h(x) := f(x) - g(x)$, моном x^{p-1} сократится, значит в разности получится многочлен степени $\leqslant p-2$.

Но у него есть $p-1$ корень — 1, 2, …, $p-1$, по вот по этой лемме

$h(x) = 0$ — нулевой многочлен. Значит $f(x) = g(x)$ (как многочлены).

Значит $-1 = f(0) = g(0) = (p-1)! * (-1)^{p-1} = (p-1)!$ □

18. Билет 20

***Определение* 18.1.** Пусть G — группа. Экспонентой G называется минимальное $d \in \mathbb{N}$, такое что $g^d = e$ (для всех $g \in G$).

Если такого d несуществует, то экспонента принимается равной ∞

Упражнение: Если G конечна, то экспонента делит $|G|$

Hint: Осознайте связь экспоненты с порядками элементов, воспользуйтесь теоремой Лагранжа.

Лемма. Пусть G — группа, a, $b \in G$, $ab = ba$, $\gcd(\operatorname{ord} a, \operatorname{ord} b) = 1$.

Тогда $\operatorname{ord}(ab) = \operatorname{ord}(a)\operatorname{ord}(b)$

Доказательство. Пусть $\operatorname{ord} a = n$, $\operatorname{ord} b = m$.

Тогда $(ab)^{mn} = \underbrace{ababab\ldots ab}_{mn \text{ times}} = a^{mn}b^{mn} = e$.

Значит $mn \vdots \operatorname{ord} ab$.

Пусть $(ab)^k = e$. Тогда $a^k = b^{-k} = t$, причём $t \in \langle a\rangle \cap \langle b\rangle = \{e\}$.

(Потому что пересечение двух циклических групп будет циклической группой с порядком, являющимся делителем обоих исходных порядков, т.е. пересечение тривиально).

$\implies a^k = b^k = e \implies m \vdots k, n \vdots k \implies mn \vdots k$.

Тем самым $\operatorname{ord} ab = mn$. □

Следствие. Пусть G — конечная абелева группа, тогда:

1. Экспонента G — это $m = \operatorname{lcm}_{g\in G} \operatorname{ord} g$
2. $\exists g \in G\colon \operatorname{ord} g = m$
3. G — циклическая $\iff m = |G|$.

Доказательство.

1. $\forall g \in G\colon g^m = e \implies m \vdots \operatorname{ord} g$

   $g^{\operatorname{lcm}_{g\in G} \operatorname{ord} g} = e \implies \operatorname{lcm}_{g\in G} \operatorname{ord} g \vdots m$

   Из двух делимостей следует равенство.

2. Разложим m на простые: $m = p_1^{k_1}p_2^{k_2}\ldots p_l^{k_l}$

   Заметим из того, что $m = lcm$, что для любого i существует хотя бы одно слагаемое порядка кратного $p_i^{k_i}$. Потому что если нет, то экспонента была бы меньше.

   Соответственно для любого i существует $g_i \in G$, такое что $\operatorname{ord} g_i = p_i^{k_i}$ (Если неочевидно, что и в какие степени нужно повозводить для этого, смотри в конспекте лектора, см. Следствие 13).

   По предыдущей лемме и индукции: $\operatorname{ord} g_1g_2\ldots g_l = m$.

3. G — циклическая $\implies m = |G|$. Очевидно, так как порядок порождающего — $|G|$, пользуемся первым пунктом.

   G — циклическая $\impliedby m = |G|$. По предыдущему пункту есть элемент порядка $|G|$, он и порождает всю группу. □

19. Билет 21

Теорема 19.1. Пусть R — область целостности, $G \leqslant R^*$, G — конечна. Тогда G — циклическая.

Доказательство. Пусть $|G| = m$. Достаточно показать, что экспонента G равна m, остальное следует из предыдущего следствия.

Пусть d — экспонента G. Значит для любого $g \in G$, $g^d = 1$.

Следовательно все элементы G — корни многочлена $x^d - 1$ в $G[x]$.

Следовательно, так как у многочлена степени d не может быть более d корней, то $m = |G| \leqslant d$. С другой стороны $m \vdots d$. (см упражнение из начала предыдущего билета) $\Rightarrow d \leqslant m$.

Следовательно $d = m$, а группа G — циклическая. □

Замечание. Зачем нужно требовать целостности? Иначе нельзя сослаться на лемму о том, что не более deg корней у многочлена.

Следствие. Конечные подгруппы мультипликативной группы поля — циклические.

Замечание. Поле действительно является областью целостности:

Если не область целостности, то есть $x \neq 0, y \neq 0 \colon xy = 0$.

Рассмотрим $x^{-1}y^{-1}xy = x^{-1}y^{-1}0$.

Слева получаем 1, справа — 0.

Следствие. $(\mathbb{Z}/_{p\mathbb{Z}})^*$ — **циклическая** группа порядка $p - 1$.

20. Билет 22

Лемма.

1. $x^n - 1 = (x-1)\sum\limits_{k=0}^{n-1} x^k$
2. $(a+b)^l = \sum\limits_{k=0}^{l} C_l^k a^k b^{l-k}$

Доказательство. Должно быть известно из школьного курса □

Лемма. Пусть $n, m \in \mathbb{N}$, $n \not\vdots 2$.

Тогда $(n+1)^{n^{m-1}} - 1 = n^m \pmod{n^{m+1}}$.

Доказательство. Индукция по m:

Не будем доказывать утверждение для $n = 1$ (в таком случае мы сравниваем два числа по модулю $1^{m+1} = 1$, очевидно, корректно, бесполезно.

Если же $n \neq 1$, то $n \geqslant 3$ (так как $n \not\vdots 2$).

База ($m = 1$) При подстановке утверждение становится очевидно: $(n+1)^1 - 1 \equiv n^1 \pmod{n^2}$.

База ($m = 2$) Подставляем: $(n+1)^n - 1 = n^2 \pmod{n^3}$

Применим пункт 1 предыдущей леммы (запишем весь хвост разложения в $n^3 t$):

$(n+1)^n - 1 = 1 + C_n^1 n + C_n^2 n^2 + n^3 t - 1 \equiv 1 + n^2 + n^2 * n(n-1)/2 - 1 \equiv n^2 + n^3(n-1)/2 \pmod{n^3}$

Так как n — нечётно, то $(n-1) \vdots 2$, а $n^3(n-1)/2 \vdots n^3$.

Итого, $(n+1)^n - 1 \equiv n^2 \pmod{n^3}$

Также здесь мы пользуемся, что $n \geqslant 3$, Чтобы уметь расписывать биномиальную сумму до нужного члена.

Переход ($m \to m+1$) $\text{Ans} = (n+1)^{n^m} - 1 = ((n+1)^{n^{m-1}})^n - 1$.

Применим пункт 2 предыдущей леммы: $\text{Ans} = ((n+1)^{n^{m-1}} - 1)\sum\limits_{i=0}^{n-1}(n+1)^{in^{m-1}}$

Так как $m \geqslant 2$, то $(n+1)^{in^{m-1}} \equiv 1 \pmod{n^2}$ (так как $(n+1)^{n^{m-1}} \equiv 1 + n^m \pmod{n^m} \equiv 1 \pmod{n^2}$ по индукции и т.к. $m > 1$).

Из этого следует, что $\sum\limits_{i=0}^{n-1}(n+1)^{in^{m-1}} \equiv n \pmod{n^2}$

По предположению индукции мы знаем, что $(n+1)^{n^{m-1}} - 1 \equiv n^m \pmod{n^{m+1}}$

Подставим всё: $\text{Ans} = (n^m + n^{m+1}t)(n + n^2 t') \equiv n^{m+1} \pmod{n^{m+2}}$ □

Как написано выше $|(\mathbb{Z}/_{p^k\mathbb{Z}})^*| = \phi(p^k) = p^{k-1}(p-1)$

Лемма. В группе $(\mathbb{Z}/_{p^k\mathbb{Z}})^* = \langle d \rangle$:

1. $\text{ord}(p+1) = p^{k-1}$

2. Пусть $\langle d \rangle = (\mathbb{Z}/_{p^k\mathbb{Z}})^*$

   Тогда $\operatorname{ord} d^{p^{k-1}} = p - 1$

3. $(p+1)d^{p^{k-1}}$ — первообразный корень по модулю p^k, т.е:

   $(\mathbb{Z}/_{p^k\mathbb{Z}})^*$ — циклическая.

Доказательство.

1. (по лемме, которую мы только что долго и нудно доказывали) $n = p, m = k$ (Рассматриваем случай $p \neq 2$).

   $(p+1)^{p^{k-1}} \equiv 1 + p^k \pmod{p^{k+1}}$

   $(p+1)^{p^{k-1}} \equiv 1 \pmod{p^k} \implies \operatorname{ord}(p+1) \mid p^{k-1}$

   Если $\operatorname{ord}(p+1) < p^{k-1}$, то $\operatorname{ord}(p+1) \mid p^{k-2}$.

   Но по лемме $(n = p,\ m = k-1)$ $(p+1)^{p^{k-2}} \equiv 1 + p^{k-1} \pmod{p^k}$

   А теперь мы живем в мире, где $p = 2$

   $|(\mathbb{Z}/_{2^k\mathbb{Z}})^*| = \phi(2^k) = 2^{k-1}$. $ord\ 3 = 2^{k-1}$ = порядку группы т.к. 3 и 2^{k-1} взаимнопросты.

2. $d \in (\mathbb{Z}/_{p^k\mathbb{Z}})^*, |(\mathbb{Z}/_{p^k\mathbb{Z}})^*| = p^{k-1}(p-1) \Rightarrow ord\ d | p^{k-1}(p-1) \Rightarrow ord\ d^{p^{k-1}} | p-1$

   Ну раз так то найдем $l \leqslant p-1 : d^{p^{k-1}l} = 1 \pmod{p^k}$

   $d^{p^{k-1}l} \equiv 1 \pmod{p^k} \implies d^{p^{k-1}l} \equiv 1 \pmod{p}$

   $\implies p^{k-1}l \vdots (p-1) = \phi(p) \iff p - 1 \geqslant l \vdots (p-1) \implies l = p-1 \implies \operatorname{ord}(d^{p^{k-1}}) = p-1$

3. $\operatorname{ord}((p+1)d^{p^{k-1}}) =$ (по лемме про взаимнопростые порядки из самого начала 18 билета) $= (p-1)p^{k-1} = |(\mathbb{Z}/_{p^k\mathbb{Z}})^*|$

□

Если $k = 1$, то $(\mathbb{Z}/_{2\mathbb{Z}})^* = \{1\}$.

Если $k = 2$, то $(\mathbb{Z}/_{4\mathbb{Z}})^* = \{1, 3\} \cong C_2$.

Лемма. В группе $(\mathbb{Z}/_{p^k\mathbb{Z}})^*$, при $k \geqslant 2$:

1. $m \in \mathbb{N} \setminus \{1\} \implies 5^{2^{m-2}} - 1 \equiv 2^m \pmod{2^{m+1}}$
2. В $(\mathbb{Z}/_{2^k\mathbb{Z}})^*$:
   (a) $\operatorname{ord}(-1) = 2, \operatorname{ord}(5) = 2^{k-2}$
   (b) $\langle -1 \rangle \cap \langle 5 \rangle = \{1\}$
3. $(\mathbb{Z}/_{2^k\mathbb{Z}})^* \simeq C_2 \times C_{2^{k-2}}$.

Доказательство. **TODO: Перенести доказательство Андрея сюда.** □

21. Билет 23

Теорема 21.1. Пусть $n \in \mathbb{N}$, $n = p_1^{k_1} \cdot \ldots \cdot p_l^{k_l}$ — разложение на простые, причём если $n \vdots 2$, то $p_1 = 2$.

$\mathbb{Z}/n\mathbb{Z} \cong \bigoplus_i \mathbb{Z}/p_i^{k_i}\mathbb{Z}$ — по КТО.

$(\mathbb{Z}/n\mathbb{Z})^* \cong \times_i (\mathbb{Z}/p_i^{k_i}\mathbb{Z})^*$ — по лемме из 18 билета.

$(\mathbb{Z}/p^k\mathbb{Z})^* \cong C_{p^{k-1}(p-1)}$ при $p \neq 2$. А для любых случаев выполняется:

$$(\mathbb{Z}/_{n\mathbb{Z}})^* \simeq \begin{cases} C_{p_1^{k_1-1}(p_1-1)} \times \ldots \times C_{p_l^{k_l-1}(p_l-1)} & n \not\vdots 2 \vee n \vdots 4, n \not\vdots 8 \\ C_{p_2^{k_2-1}(p_2-1)} \times \ldots \times C_{p_l^{k_l-1}(p_l-1)} & n \vdots 2, n \not\vdots 4 \\ C_2 \times C_{2^{k_1-2}} \times C_{p_2^{k_2-1}(p_2-1)} \times \ldots \times C_{p_l^{k_l-1}(p_l-1)} & n \vdots 8 \end{cases}$$

Доказательство. Ничего умного, расширяем запись. Если $n \not\vdots 2$, написали по лемме. Если $n \vdots 4, n \not\vdots 8$, то $p_1 = 2$, $k_1 = 2$ в произведение групп входит группа $C_{2^{2-1}(2-1)} = C_2$. Остальные случаи аналогично, по п. 3 последней леммы из 22. □

Теорема 21.2. $(\mathbb{Z}/n\mathbb{Z})^*$ циклическая $\iff$ $n = 2, 4, p^k, 2p^k$, где $p > 2$ — простое.

Доказательство. $\Leftarrow$. Уже знаем.

$\Rightarrow$. Знаем, что $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ — циклична $\Leftrightarrow (a, b) = 1$.

Пусть $p, q > 2$ — простые. Тогда $\mathbb{Z}/pq\mathbb{Z} \cong C_{p-1} \times C_{q-1}$, где $(p-1, q-1) \vdots 2 \to \mathbb{Z}/pq\mathbb{Z}$ — не циклична. Из этого перебором вариантов, как может выглядить разложение n на протые получаем, что только подходят только указанные 4 случая. В остальных случаях нод будет делиться на 2.

□

***Определение* 21.1.** $G = \langle d \rangle$ — конечная циклическая группа. $|G| = n$.

$exp_d : \mathbb{Z}/n\mathbb{Z} \to G$ — изоморфизм, назовём дискретная экспонента.

$exp_d : a \mapsto d^a$

$log_d = exp_d^{-1}$ — дискретный логарифм.

Лемма. Критерий существования дискретного логарифма. В циклической группе $G = \langle d \rangle$ уравнение вида $d^x = y$ всегда разрешимо.

Доказательство. Действительно, d — порождает группу, то есть его степени образуют все возможные элементы y. □

22. Билет 24

***Определение* 22.1.** Функция Карлмайка $\lambda\colon \mathbb{N} \to \mathbb{N}$.

λ — экспонента группы $(Z/_{n\mathbb{Z}})^*$

$\lambda(n) \mid \phi(n)$, Пусть $n = p_1^{k_1} \cdot \ldots \cdot p_l^{k_l}$

Теорема 22.1.

1. Если $n \not\vdots 8$, то $\lambda(n) = \mathrm{lcm}_{1 \leqslant i \leqslant l}(p_i^{k_i - 1}(p_i - 1))$
2. Если $n = 2^k m$, где $k \geqslant 3$, а $m \not\vdots 2$, то $\lambda(n) = \mathrm{lcm}(\mathrm{lcm}_{1 \leqslant i \leqslant l}(p_i^{k_i - 1}(p_i - 1)), 2^{k-2})$
3. Если $\gcd(a,\, n) = 1$, то $a^{\lambda(n)} \equiv 1 \pmod{n}$.

Доказательство.

1. Если $n \not\vdots 8$, то $\lambda(n) = \mathrm{lcm}_{1 \leqslant i \leqslant l}(p_i^{k_i - 1}(p_i - 1))$
2. Если $n = 2^k m$, где $k \geqslant 3$, а $m \not\vdots 2$, то $\lambda(n) = \mathrm{lcm}(\mathrm{lcm}_{1 \leqslant i \leqslant l}(p_i^{k_i - 1}(p_i - 1)), 2^{k-2})$
3. Если $\gcd(a,\, n) = 1$, то по теореме Эйлера $a^{\phi(n)} = 1 \pmod{n} \Rightarrow a$ – первообразный корень по модулю n (образует группу обратимых элементов, а значит, в ней содержится) $\Rightarrow a^{\lambda(n)} = 1 \pmod{n}$.

□

23. Билет 25

Тест Ферма на простоту

n — простое $\implies a^{n-1} \equiv 1 \pmod n$ $((a,\, n) = 1,\, 1 < a < n)$.

$T \subseteq \mathbb{Z}/_{n\mathbb{Z}} \setminus \{0\}$ — множество тех a, для которых тест пройден.

Если n — простое, то $T = (\mathbb{Z}/_{n\mathbb{Z}})^*$

Тест Ферма $T = \{a \mid a^{n-1} \equiv 1 \pmod n\}$

***Определение* 23.1.** Составные числа n, такие что $|T_n| = |\mathbb{Z}/_{n\mathbb{Z}}/\{0\}|$ называются псевдопростыми для данного теста.

***Определение* 23.2.** Числа Карлмайкла — псевдопростые числа для теста Ферма. Таких чисел бесконечно много. Наименьшее число Карлмайкла — это 561.

Тест Эйлера:

Незачем тестировать чётные числа с ними и так всё ясно. Давайте тестировать только нечётные.

$T = \{a \mid a^{\frac{n-1}{2}} \equiv 1 \pmod n\}$

Увы тоже есть псевдопростые. Пример: 1729

Если составное, то вероятность детектирования через 10 запусков: $1 - \frac{1}{k^{10}}$

Тест Соловея-Штрассена

$$T := \{a \in (\mathbb{Z}/_{n\mathbb{Z}})^* \mid a^{\frac{n-1}{2}} = (\frac{a}{n})\}$$

Для k случайных значений a мы проверим выполнение условия $a \in T$

Утверждение 23.1. Пусть n – нечетное составное число. Тогда $|T| < \frac{\phi(n)}{2}$. (Факт из воздуха, ничего с ним делать не нужно). Таким образом, если для k случайных значений $a \in (\mathbb{Z}/n\mathbb{Z})^*$

Тогда если для k случайных a выполнено $a \in T$, то n простое с вероятностью не меньше чем $1 - \frac{1}{2^k}$

Тест Миллера-Рабина

Пусть $n - 1 = 2^m k, 2 \nmid k$.

$$T := \{a \mid a^k = 1 \text{ или } \exists j < m : a^{2^j k} = -1\}$$

Если n простое, то $T = (\mathbb{Z}/_{n\mathbb{Z}})^*$. (Летор утверждает, что это легко понять из того, что $x^2 = 1$ в нашем поле имеет только 2 решения).

Утверждение 23.2. n – нечетное составное число $3 \nmid n$ и $n - 1 = 2^m k, 2 \nmid k$. Тогда $|T| \leqslant \frac{\phi(n)}{4}$ (Факт из воздуха).

Тогда если для k случайных a выполнено $a \in T$, то n простое с вероятностью не меньше чем $1 - \frac{1}{4^k}$ Если при фиксированном n число a проходит тест Миллера-Рабина и не показывает, что n составное, то для теста Соловея-Штрассена результат будет тем же.