Алгебра

Кабашный Иван

(по материалам конспекта старшекурсников,
написанном на основе лекций В. А. Петрова,
а также других источников)

22 января 2020 г.

Честно говоря, ненависть к этой вашей топологии просто невообразимая.

Содержание

1 Билеты

1.1 Определение кольца. Простейшие следствия из аксиом. Примеры. Области целостности

Определение 1. *Кольцом* называется множество R вместе с бинарными операциями $+$ и $\cdot$ (которые называются сложением и умножением соответственно), удовлетворяющим аксиомам:

- операция сложения ассоциативна;
- по отношению к сложению существует нейтральный элемент;
- у каждого элемента есть обратный по сложению
- операция сложения коммутативна;
- умножение ассоциативно;
- умножение дистрибутивно по сложеиню.

Также можно добавить, что если на множестве выполныны три первые аксиомы, то оно будет называться *группой*, а если выполнены первые четыре, то это уже *абелева группа*. Нейтральный по сложению элемент кольца называют *нулём*.

Пример(ы) 1. Кольцо называется:

- *коммутативным*, если оно коммутативно по умножению;
- *кольцом с единицей*, если оно содержит нейтральный элемент по умножению (единица);
- *телом*, если в нём есть 1, и для любых $a \neq 0 \to a \cdot a^{-1} = a^{-1} \cdot a = 1$;
- *полем*, если это коммутативное тело;
- *полукольцом*, если нет требования противоположного элемента по сложению.

Следствие 1. Некоторые следствия из аксиом:

- $0 \cdot a = 0$

  Доказательство.
  $$0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$$
  Прибавим к обеим частям $-0 \cdot a$ и получим требуемое. □

- Нейтральный элемент по сложению единственный

  Доказательство. Рассмотрим их сумму справа и слева. □

- $a \cdot 0 = 0$

Доказательство.

$$a \cdot 1 = a \Longrightarrow (0+1)a = a \Longrightarrow 0 \cdot a + 1 \cdot a = a \Longrightarrow 0 \cdot a = 0$$

□

Определение 2. Коммутативное кольцо R с единицей, обладающее свойством

$$xy = 0 \Longrightarrow x = 0 \vee y = 0 \ (\forall x, y \in R)$$

называется *областью целостности* или просто *областью*.

Определение 3. Число $d \neq 0$ называется *делителем нуля*, если существует такое $d' \neq 0$, что $dd' = 0$.

Нетрудно понять, что область целостности - в точности коммутативное кольцо с единицей без делителей нуля.

1.2 Евклидовы кольца. Евклидовость $\mathbb{Z}$. Неприводимые и простые элементы.

Для начала, некоторые связанные понятия, не упомянутые в билетах.

Определение 4. Говорят, что d *делит* p и пишут $d|p$, если $p = dq$ для некоторго $q \in R$.

Определение 5. Элемент ε называется *обратимым*, если он делит единицу, то есть существует такое $\varepsilon^{-1} \in R$, что $\varepsilon^{-1} \cdot \varepsilon = 1$.

Определение 6. Будем говорит, что элементы a и b *ассоциированы* и писать $a \sim b$, если выполнено одно из двух эквивалентных условий:

- существует обратимый элемент ε, для которого $a = \varepsilon b$;
- $a|b$ и $b|a$.

Покажем, что эти условия действительно эквивалентны.

Доказательство. Докажем в обе стороны:
$\Rightarrow$ Если $a = \varepsilon b$, то $\varepsilon^{-1}a = b$. Это и есть второе условие.
$\Leftarrow$ Пусть $a = bc$ и $b = ac'$ для каких-то c, c'. Тогда $a = (ac')c = a(cc') \leftrightarrow a(1 - cc') = 0$. Тогда либо $a = 0$, либо $cc' = 1$, потому что делителей нуля в нашем кольце нет. В любом случае, a и b отличаются на обратимый: либо они оба равны нулю, либо c - обратимый. □

А теперь, что касается самого билета.

Определение 7. Область целостности R называется *евклидовым кольцом*, если существует евклидова норма $N : R \to \mathbb{N}_0$ такая, что $N(0) = 0$ и для любых элементов $a, b \in R$, где $b \neq 0$, существует меньший чем b по норме элемент $r \in R$ такой, что выполнено равенство $a = bq + r$.

Пример(ы) 1. Кольцо целых чисел $\mathbb{Z}$ евклидово.

Доказательство. Пусть у нас имеются целое число a и ненулевое целое b. Тогда существуют такие целые числа q и r, что модуль r меньше модуля b, а также $a = bq + r$. Отметим на оси все ератные b. Тогда если число a попало на отрезок $[kb, (k+1)b]$, k будет частным, а $a - kb$ - остатком. Дальнейшую формализация можно провести индукцией. □

Опять несколько небольших новых определений перед тем как перейти к последнему пункту билета (их можно упустить).

Определение 8. Пусть R - область целостности; a,$b \in R$. Элемент $d \in R$ называется *наибольшим общим делителем* a и b, если

- $d|a$ и $d|b$;
- для любого $d' \in R$, который также делит a и b, выполнено также, что он делит d.

Теорема 1. *(О линейном представлении НОД в евклидовых кольцах). Пусть R - евклидово кольцо, $a, b \in R$. Тогда существуют $d := \gcd(a,b)$ и такие x,$y \in R$, что $d = ax + by$.*

Теперь про простые и неприводимые.

Определение 9. Пусть R - область. Необратимый элемент $p \in R$ - *неприводимый*, если

$$\forall d \in R : d|p \Longrightarrow d \sim 1 \vee d \sim p$$

Определение 10. Пусть R - область. Ненулевой необратимый элемент $p \in R\backslash 0$ называется *простым*, если $\forall a$,$b \in R : p|ab \Longrightarrow p|a \vee p|b$.

Лемма 1. *(Простые $\subset$ неприводимые). Если p - простой элемент произвольного коммутативног кольцв с единицей, то p - неприводим.*

Доказательство. Пусть d - какой-то делитель p, что эквивалентно равенству $p = da$ для какого-то a. Проверим, что либо $d \sim 1$, либо $d \sim p$. Раз p - простой, то либо он делит d, либо он делит a. Если первое, что сразу $d \sim p$.Если второе, перепишем в виде $da = p|a$. Это то же самое, что $bda = a$ для некоторого b. Здесь либо $a = 0$, то тогда $p = o$, что невозможно по определению простого, либо мы можем сократить на a и получим $bd = 1$, тогда d ассоциирован с 1. □

Теперь немного добавки про простые и неприводимые, на всякий случай.

Лемма 2. *(Неприводимые $\subset$ простые в ОГИ). Пусть p - неприводимый в области главных идеалов. Тогда p - простой.*

Доказательство. Пусть $p|ab$, хотим показать, что $p|a \vee p|b$. Воспользуемся тем, что мы в области главных идеалов: $(p,a) = (d)$, где $d := \gcd(a,p)$, а тогда $px + ay = d$ для каких-то x, y. $d|p$, воспользуемся неприводимостью p: либо $d \sim p$, либо $d \sim 1$.

В первом случае $p|d$, тогда $p|d|a$.

Во втором случае можно после домножения на обратимые считать, что $px + ay = 1$. Потом домножим на b : $pbx + aby = b$. p явно делит первое слагаемое, ровно как и второе (по предположению). Значит, $p|b$.

В любом случае, приходим к желаемому. □

1.3 Идеалы, главные идеалы. Евклидово кольцо как кольцо главных идеалов

Определение 11. Подмножество

$$(a_1, \ldots, a_n) := \{a_1x_1 + \cdots + a_nx_n | x_i \in R \text{ для всех } i\}$$

коммутативного кольца R называется *идеалом*, порождённым $a_1, \ldots, a_n$.

Определение 12. Подкольцо I кольца R называется *левым идеалом*, если оно замкнуто относительно домнодения слева на элементы кольца: $RI = I$. Соответственно, также различают *правые* и *двусторонние идеалы*.

Также идеал можно задать следующими свойствами:

- $\forall x, y \in I \Longrightarrow x + y \in I$;
- $\forall x \in I, \forall r \in R \Longrightarrow xr \in I$;
- $-x \in I$;
- I - непустой.

Определение 13. Идеал называется *главным*, если он порождён одним элементом.

Определение 14. *Область главных идеалов* - область целостности, в который каждый идеал главный.

Теорема 2. *(Евклидовы кольца $\subset$ ОГИ). Пусть R - евклидово кольцо, $I \trianglelefteq R$ - идеал. Тогда I - главный.*

Доказательство. Найдём элемент, который порождает идеал I.

Вырожденный случай: если $I = \{0\}$, тогда $I = (0)$.

Иначе возьмём $d \in I \backslash 0$ с минимальной нормой (по принципу индукции мы можем это сделать). Хотим показать, что $I = (d)$. Покажем это в обе стороны.

$\Rightarrow$ Легко видеть, что $(d) \subset I$.

$\Leftarrow$ Пусть $a \in I$, тогда поделим a на b с остатком: $a = bd + r$. Предположим, $r \neq 0$, $N(r) < N(d)$. Выразим r линейной комбинацией $a \in I$ и $d \in I$: $r = a - bd \in I$ - противоречие с минимальностью нормы d. Значит, $r = 0$, а тогда $a = bd \in (d)$. □

1.4 Основная теорема арифметики

Сначала опять немного информации, которая к билету не относится, но к нему логично подводит.

Определение 15. Коммутативное кольцо с единицей R удовлетворяет *условию обрыва возрастающих цепей главных идеалов* или, что то же самое, является *нётеровым кольцом*, если не существует бесконечной строго возрастающей цепочки главных идеалов $(d_1) \subsetneq (d_2) \subsetneq \dots$ Иначе говоря, бесконечной цепочки $\dots | d_2 | d_1$, где все d_i попарно не ассоциированы.

Теорема 3. *(ОГИ $\subset$ нётеровы кольца). Область главных идеалов удовлетворяет условию обрыва возрастающих цепей главных идеалов (далее - УОВЦГИ).*

Доказательство. Предположим, что нашлась такая бесконечная цепочка $\{d_i\}$. Объединим $I := \bigcup_{i=0}^{\infty} (d_i)$.

Покажем, что I - идеал. $0 \in I$. Пусть $u \in (d_i)$ и $v \in (d_j)$, где $i \leq j$, проверяем остальные условия. $u + v \in (d_j)$, потому что $u \in (d_j)$, с остальными аналогично, не очень сложно.

Вспомним, что мы находимся в ОГИ, то есть, каждый идеал главный. Пусть d - *генератор* I ($I = (d)$). Любой (d_i) строго содержится в (d_{i+1}), а этот содержится в (d) : $(d_i) \subsetneq (d_{i+1}) \subset (d)$, значит, любой из $\{(d_i)\}$ строго содержится в (d). Но сам генератор d тоже должен принадлежать какому-то из $\{(d_i)\}$, а значит, на каком-то моменте $(d) \subset (d_i)$. Противоречие. □

Определение 16. Кольцо называется *факториальным*, если одновременно выполнено:

- R - область;
- любой неприводимый элемент R - простой;
- R - нетёрово.

Пример(ы) 1. Как мы уже знаем, ОГИ $\subset$ факториальные кольца.

А теперь, к основному.

Теорема 4. *(Основная теорема арифметики). Пусть R - факториальное кольцо.*

Тогда любой элемент $x \in R$, если он не нуль и не обратимый, представляется в виде $r = p_1 \dots p_n$, где $n \geq 1$, а $\{p_i\}$ - простые.

При этом, если $r = q_1 \dots q_m$ - другое такое разложение, то $m = n$ и существует перестановка индексов $\pi : n \to n$, такая, что $p_i \sim q_{\pi_i}$ для всех i.

Доказательство. Докажем существование. Зафиксируем x. Если он неприводимый, то он и простой по определению факториального кольца, поэтому сам будет своим подходящим разложением. Пусть $x = yz$, где $y, z \nsim 1$.Если y необратим и приводим, разложим и его: $y = y_1 z_1$, где $y_1, z_1 \nsim 1$. Будем раскладывать так игреки, пока можем, и получим строго возрастающую цепочку идеалов $(y) \subsetneq (y_1) \subsetneq (y_2) \subsetneq \dots$ Вспомним нетёровость нашего кольца: бесконечно возрастать она не может, значит, на каком-то моменте заработаем для x один не приводимый делитель $p : x = pw$ для какого-то w. Если w необратим и приводим, разложим и его: $w = p_1 w_1$. Продолжим и получим ещё одну возрастающую цепочку идеалов: $(x) \subsetneq (w) \subsetneq (w_1) \subsetneq \dots$ К тому времени, когда она оборвётся, у нас будет разложение x в конечное произведение неприводимых: $x = p_1 \dots p_n$. Существование доказано.

Теперь перейдём к доказательству единственности. Разложим двумя способами: $r = p_1 \dots p_n = q_1 \dots q_m$. По индукции пожно вывести из определения простого, что

Лемма 3. *Если p - простой и $p | a_1 \dots a_n$, то $p | a_i$ для какого-то i.*

Воспользуемся этим фактом:например, мы теперь знаем: что $q_m | p_i$ для какого-то i. Но p_i неприводим, поэтому любой его делитель либо обратим, либо ассоциирован с ним. q_m не боратим, так как он простой; значит, $q_m \sim p_i$. Переставим p_i и p_n и считаем, что q_m теперь $\sim p_n$. Осталось вывести следующий факт:

Лемма 4. *Пусть $a \sim b$, $ac \sim bd$, а $b \neq 0$. Тогда $c \sim d$.*

Доказательство. $a = \varepsilon b$и $ac = \varepsilon bc = \nu bd$ для каких-то обратимых ε и ν. Последнее равенство можем сократить на $b \neq 0$, потому что мы в области. □

Теперь $p_1 \dots p_{n-1} \sim q_1 \dots q_{m-1}$. Можем теперь сказать, что равенство $p_1 \dots p_{n-1} = q_1 \dots q_{m-1}$ верно по предположению индукции по n. Так же по индукции $n = m$, потому что получим противоречие, если какая-то из серий сомножителей $\{p_i\}$, $\{q_i\}$ закончится раньше. □

Пример(ы) 2. Обыкновенное кольцо $\mathbb{Z} \in$ евклидовы кольца $\subset$ ОГИ $\subset$ факториальные кольца.

1.5 Кольцо вычетов $\mathbb{Z}/_{n\mathbb{Z}}$. Китайская теорема об остатках

Пример(ы) 1. Множество $\mathbb{Z}/_{n\mathbb{Z}} = \{[0], \dots, [n-1]\}$ остатков при делении на $n \in \mathbb{N}$ - коммутативное кольцо с единицей. *Кольцо вычетов* (остатков) по модулю.

Определение 17. m, n *взаимно просты*, если $(m,n) = (1) = R$.

Лемма 5. *Пусть R - факториальное кольцо, $m, n \in R$ - взаимно простые элементы. Пусть, к тому же, m и n - делители r : $m,n|r$. Тогда их произведение тоже делит $r : mn|r$.*

Доказательство. Можно вывести из ОТА. □

Теорема 5. *(Китайская теорема об остатках). Если $(m,n) = (1)$, то $\mathbb{Z}/(m) \times \mathbb{Z}/(n) \cong \mathbb{Z}/(mn)$.*

Доказательство. Пусть x - классы, соответствующие числу x в $\mathbb{Z}/(m)$ и $\mathbb{Z}/(n)$, соответственно. Рассмотрим гомеоморфизм $f = x \mapsto ([x]_m, [x]_n)$.

Его ядро - числа, которые делятся и на m, и на n, а поскольку они взаимно просты, то и на mn. Значит, $\mathrm{Ker} f = (mn)$.

Проверим f на сюръективность. Для этого просто хитро покажем, что $\mathrm{Im} f \cong \mathbb{Z}/(mn)$. Тогда $mn = |\mathbb{Z}/(mn)| = |\mathrm{Im} f|$. При этом $\mathrm{Im} f \subset \mathbb{Z}/(m) \times \mathbb{Z}/(n)$ по определению (подкольцо) и $|\mathbb{Z}/(m) \times \mathbb{Z}/(n)| = mn$ простым подсчётом, откуда следует, что $\mathrm{Im} = \mathbb{Z}/(m) \times \mathbb{Z}/(n)$. □

Следствие 1. $\mathbb{Z}/(n)$ - область целостности $\iff$ n - простое.

1.6 Определение поля. $\mathbb{Z}/_{p\mathbb{Z}}$ как поле. Поле частных целостного кольца

Напомним ещё раз определение поля.

Определение 18. *Поле* - коммутативное кольцо с единицей, в котором также существует обратный элемент по умножению для ненулевых элементов.

Пример(ы) 1. $\mathbb{Z}/_{p\mathbb{Z}}$ - поле.

Доказательство. Мы уже много чего знаем про эту структуру (см. конец предыдущего билета). Для доказательства вышеприведённого факта нужно показать, что у каждого элемента есть обратный по умножению (кроме, конечно, нуля). Рассмотрим ненулевой элемент a, и умножим его на все остатки по модулю p, получим $\{0a, 1a, \dots, (p-1)a\}$. Заметим, что все полученные остатки различны. Предположим противное: $ka \equiv ma \Leftrightarrow (k-m)a \equiv 0$, но так как мы находимся в области, то либо $a = 0$ (сразу нет), либо $k - m = 0$, но так как они оба меньше p, то такого тоже, очевидно, не бывает. Тогда мы получили, что все остатки, полученные таким образом, различны. Но так как их ровно p, то найдётся и равный 1, элемент на который мы умножаем в том случае и будет обратным к a. □

В общем и целом, мы сейчас будем получать что-то вроде $\mathbb{Q}$, но над любым кольцом R. Введём отношение $\sim$ на множестве пар $R \times (R \backslash 0)$. Пусть $(a,b) \sim (a',b') \Leftrightarrow ab' = a'b$. Проверим, что мы получили отношение эквивалентности:

Доказательство. Нужно показать рефлексивность, симметричность и транзитивность. Первые два утверждения очевидны, покажем последнее. Пусть $(a,b) \sim (a',b')$ и $(a',b') \sim (a'',b'')$, мы хотим показать, что $(a,b) \sim (a'',b'')$, то есть, $ab'' = a''b$. Воспользуемся тем, что мы находимся в области целостности - домножим левую часть последнего равенства на ненулевой b' и преобразуем, используя гипотезы:

$$(ab')b'' = b(a'b'') = bb'a''.$$

Теперь сократим на b'. □

Определение 19. Фактор $R/\sim$ называется *полем частных* области целостности R и обозначается за Frac$R$. Элементы будем обозначать дробями.

Сложение и умножение определяется как в обычной жизни. Осталось проверить, что это действительно поле.

Доказательство. Нужно выполнить совсем немного проверок:

- $\frac{0}{1}$ - нуль;
- $\frac{1}{1}$ - единица;
- $\frac{-a}{b}$ - обратный к $\frac{a}{b}$ по сложению;
- $\frac{b}{a}$ - обратный к $\frac{a}{b}$ по умножению для ненулевых.

□

1.7 Определение гомоморфизма и изоморфизма колец. Фактор-кольцо

Определение 20. Пусть R и S - кольца. Функция $f : R \to S$ называется *гомоморфизмом колец*, если для произвольных элементов выполняется

- $f(r_1 + r_2) = f(r_1) + f(r_2)$;
- $f(r_1 r_2) = f(r_1)f(r_2)$.

Лемма 6. *Если f - гомоморфизм, то $f(0) = 0$ и $f(-r) = -r$.*

Доказательство. В обоих пунктах - подсчёт двумя способами:

- $f(0) + f(0) = f(0 + 0) = f(0)$;
- $f(r) + f(-r) = f(r + (-r)) = f(0) = 0$

□

Кстати говоря, не любой гомоморфизм сохраняет единицу.

Пример(ы) 1. Пусть $f : r \to R \times S$ и $f = r \mapsto (r,0)$. Тогда $f(1) = (1,0) \neq 1$.

Определение 21. Если для гомоморфизма f выполнено $f(1) = 1$, то говорят, что он *сохраняет единицу.*

С гомоморфизмом связаны два важных понятия, которые мы рассмотрим далее.

Определение 22. *Ядро* Ker$f$ гомоморфизма $f : R \to S$ - полный прообраз нуля, $f^{-1}(0)$.

Лемма 7. *Гомоморфизм f инъективен тогда и только тогда, когда его ядро тривиально: $Ker f = \{0\}$.*

Доказательство. Потому что $f(x_1) = f(x_2) \iff f(x_1 - x_2) = 0$ □

Лемма 8. *$Ker f$ - двусторонний идеал в R.*

Доказательство. Пусть $k \in \mathrm{Ker} f$, тогда для любого $r \in R$ $f(rk) = f(r)f(k) = f(r) \cdot 0 = 0 = 0 \cdot f(r) = f(kr)$. Ещё, например, $f(k_1 + k_2) = f(k_1) + f(k_2) = 0$. Остальные пункты из определения так же очевидны. □

Определение 23. *Образ* области определения гомоморфизма f обозначается как $\mathrm{Im} f$.

Лемма 9. *Если $f : R \to S$ - гомоморфизм, то $f(R)$ - кольцо.*

Доказательство. $f(a) + f(b) = f(a + b)$, $f(a)f(b) = f(ab)$ - как раз. □

Определение 24. *Изоморфизм* - биективный гомоморфизм. Пишут $R \cong S$, если между ними существует изоморфизм.

А теперь про фактор-кольца.

Определение 25. Пусть R - кольцо (возможно, некоммутативное и без единицы), а I - двусторонний идеал. Говорят, что a *сравнимо* с b по модулю I и пишут $a \equiv b \mod I$, если $a - b \in I$.

Лемма 10. *Сравнимость по модулю - отношение эквивалентности.*

Так как мы получили отношение эквивалентности, по нему можно факторизовать. Тогда аналогами классов эквивалентности становятся множества вида $[a] := \{b \in \mathbb{R} | b \equiv a \mod I\}$. Обозначим кмножество всех этих классов за R/I. Осталось ввести структуру кольца на этом множестве.

Определим действия: $[a] + [b] = [a + b]$ и $[a][b] = [ab]$. Нетрудно понять, что действия над классами не зависят от выбора *представителя*. Сложение вообще очевидно, а при умножении нужно "прибавить и вычесть", чтобы собрать.

Теорема 6. *Пусть R - произвольное кольцо, возможно, некоммутативное и без единицы; $I \trianglelefteq R$ - двустронний идеал.*

Обозначим за R/I фактор R по отношению эквивалентности $\{a \equiv b | a - b \in I\}$, за $[a]$ - класс эквивалентности элемента $a \in R$.

Тогда:

- *операции $[a] + [b] = [a + b]$ и $[a][b] = [ab]$ определены корректно и задают на R/I структуру кольца;*
- *если R коммутативно, то R/I - тоже;*
- *если R - кольцо с единицей, то $[1]$ - единица R/I.*

Доказательство. В первом пункте мы уже проверили все неочевидные пункты в определении кольца, остальное - тривиально. □

Определение 26. R/I - *фактор-кольцо* R по I.

1.8 Теорема о гомоморфизме

Теорема 7. *(Теорема о гомоморфизме). Пусть $f : R \to S$ - гомоморфизм колец. Тогда $f(R) \cong R/Kerf$.*

Доказательство. Что мы будем делать по сути: вместо того, чтобы сразу отправлять элемент из R в S посредством f, сначала спроецируем его в $R/\mathrm{Ker}f$ и оттуда уже отобразим в $f(R)$. Проверяем следующее для формальности:

- *Корректность определения.* Пусть $[r] = [r']$. Тогда $r' - r \in \mathrm{Ker}f$, что равносильно $f(r' - r) = 0$, а тогда $f(r) = f(r')$.
- *Сюръективность.* По определению $f(R)$ любой элемент оттуда - это $f(r)$ для какого-то элемента $r \in R$, а $f(r)$ - образ $[r]$ при нашем отображении.
- *Инъективность.* Пусть $f(r_1) = f(r_2)$, тогда $f(r_1 - r_2) = 0$. Значит, $r_1 - r_2 \in \mathrm{Ker}f$, что эквивалентно $r_1 \equiv r_2 \mod \mathrm{Ker}f$.
- *Сохраняет операции.* $\varphi([a]) + \varphi([b]) = \varphi([a] + [b]) = \varphi([a + b]) = f(a + b) = f(a) + f(b) = \varphi([a]) + \varphi([b])$. С умножением - агалогично.

□

Так как билет и так короткий - припишем сюда ещё одну теорему, которой почему-то нет в билетах.

Теорема 8. *(Универсальное свойство фактор-кольца). Пусть R - кольцо, $I \trianglelefteq R$ - двусторонний идеал, $\pi : R \to R/I$ - канонический гомоморфизм, $\varphi : R \to S$ - гомоморфизм колец, ядро которого содержит I: $\varphi(I) = \{0\}$. Тогда:*

- *существует единственный гомоморфизм $\bar{\varphi} : R/I \to S$ такой, что $\varphi = \bar{\varphi} \circ \pi$;*
- *$\bar{\varphi}$ задаётся формулой $\bar{\varphi} = [x] \mapsto \varphi(x)$.*

Доказательство. Раз уж теоремы в списке нет, то доказывать её не будем. Если вкратце, то сначала несложно проверяется единственность, затем - корректность, и, наконец, рутинная проверка на гомоморфизм. □

1.9 Кольцо многочленов. Целостность и евклидовость кольца многочленов над полем

Определение 27. *Многочлен* - комбинация вида $\sum_{i=0}^{\infty} a_i x^i$, где почти все (кроме конечного числа) $\{a_i\}$ равны нулю. В кольце может и не быть единицы, но даже тогда мы определяем $a_0 x^0 := a_0$ для удобства нотации.

Определение 28. *a коммутриует* с b, если $ab = ba$.

Определение 29. *Кольцо многочленов* $R[x]$ - кольцо R вместе с некоторыми $x \notin R$, для которых выполняются следующие свойства:

- $\forall a \in R : ax = xa$;
- $\sum a_i x^i + \sum b_i x^i = \sum (a_i + b_i) x^i$;

- $-\sum a_i x^i = \sum -a_i x^i$;
- нуль есть $\sum 0x^i$;
- умножение по формуле свёртки: если

$$\left(\sum_i a_i x^i\right)\left(\sum_j b_j x^j\right) = \sum_k c_k x^k,$$

то

$$c_k = a_k b_0 + a_{k-1} b_1 + \cdots + a_0 b_k = \sum_{i+j=k} a_i b_j.$$

Определение 30. *Степень многочлена* $\deg \sum a_i x^i$ - наибольшее i такое, что $a_i \neq 0$. Если таких i нет (многочлен нулевой), то его степень определять не будем.

Следствие 1. Из определения степени сразу следует несколько свойств:

- $\deg(f+g) \leq \deg f + \deg g$;
- $\deg(fg) \leq \deg f + \deg g$ для ненулевых f, g;
- $\deg(fg) = \deg f + \deg g$ для ненулевых f, g, если мы находимся в области целостности.

Последнее получается постольку поскольку старшие коэффициенты просто перемножаются, поэтому можно сформулировать такую лемму:

Лемма 11. *Если R - область, то и $R[x]$ - область.*

А сейчас будем учиться делить многочлены с остатком, тем самым, покажем, что полученное кольцо евклидово (не всегда, конечно).

Лемма 12. *Пусть R - кольцо, $f = a_n x^n + \cdots \in R[x]$, $g = b_m x^m + \cdots \in R[x]$, $\forall i : b_m^{n-m+1} | a_i$. Тогда существуют многочлены q,$r \in R[x]$ такие, что $f = gq + r$ и $r = 0 \vee \deg r < \deg g$.*

Доказательство. Докажем индукцией по n. База: если $n < m$, то положим $q := 0$ и $r := f$.

Пусть теперь $n \geq m$. По условию делимости $b_m^{n-m-1} c := a_n$ для некоторог c. Посмотрим на $f_1 := f - tg$, где $t := c b_m^{n-m} x^{n-m}$ - страший член неполного частного. $\deg tg = n$, потому старший член сократился при делении. Предположение индукции верно для пары f_1,g, так как единственный аспект под вопросом - делимость коэффициентов, но он тоже верен, что видно из определения f_1. Тогда применим индукцию: $f_1 = q_1 g + r$. Подставим $f = (t+q_1)g + r$. r найден. □

Следствие 2. Пусть F - поле. Тогда $F[x]$ - евклидово кольцо.

Доказательство. По доказанному выше, $\deg : F[x] \backslash 0 \to \mathbb{N}_0$ - евклидова норма, потому что старший коэффициент ненулевого многочлена всегда обратим. □

Примечание 1. А вот для евклидова R, $R[x]$ не обязательно будет евклидовым кольцом.

1.10 Лемма Гаусса

Определение 31. *Содержание* $\operatorname{cont} f$ для $f \in R[x]$ - это gcd всех коэффициентов f.

Видно, что для любого многочлена f существует $f_1 : f_1 \operatorname{cont} f$ для некоторого f_1 такого, что $\operatorname{cont} f \sim 1$.

Лемма 13. *(Лемма Гаусса). Если* $\operatorname{cont} f \sim 1$ *и* $\operatorname{cont} g \sim 1$, *то* $\operatorname{cont} fg \sim 1$.

Доказательство. Пусть $p \in R$ - простой и $p|\operatorname{cont} fg$, ради противоречия. Раз у fg все коэффициенты делятся на p, то по модулю (p) он нулевой: $fg = 0$ в $R/(p)[x]$. (Конечно, здесь мы имеем в виду его образ при проекции $R[x] \to R/(p)[x]$, которую естественным образом индуцирует каноническая проекция $\pi : R \to R/(p) : \sum a_i x^i \mapsto \sum \pi(a_i)x^i$). Но поскольку p простой, $R/(p)$ - это область (посмотрим, что такое нуль фактор-кольца и соотнесём с определением простого), а тогда $f = 0 \vee g = 0$ в $R/(p)[x]$ (см), что противоречит определению f и g. □

Следствие 1. $(\operatorname{cont} f)(\operatorname{cont} g) \sim cont fg$.

Доказательство. Раз $f_1 : f_1 \operatorname{cont} f$ b $g_1 : g_1 \operatorname{cont} g$ для некоторых $f_1, g_1 : \operatorname{cont} f_1, \operatorname{cont} g_1 \sim 1$, то $\operatorname{cont} f_1 g_1 \sim 1$, а тогда $\operatorname{cont} fg = \operatorname{cont}(f_1 g_1 \operatorname{cont} f \operatorname{cont} g) \sim \operatorname{cont} f_1 g_1 \operatorname{cont} f \operatorname{cont} g \sim \operatorname{cont} f \operatorname{cont} g$. □

1.11 Факториальность кольца многочленов

Щас дикий пиздец будет. Пристегнитесь, мы взлетаем. Начнём с леммы, которая встречается в теореме, но доказывалась раньше.

Лемма 14. *Если* R *- нетёрова область. то* $R[x]$ *тоже нетёрова область.*

Доказательство. Что область, мы уже знаем (см). Поймём нетёровость.

Предположим противное: пусть $\ldots | f_2 | f_1$ - бесконечная цепочка попарно не ассоциированных многочленов. С ростом индексов степень невозрастает, значит, с какого-то момента она стабилизируется. Тогда отбросим начальный отрезок цепочки (конечно, конечный) и будем считать: что все степени равны n.

Однако теперь посмотрим на i-ый коэффициент в каждом многочлене и поймём, что для любых двух последовательных $a_i c = b_i$. Однако опять получается бесконечная цепочка, противоречие. □

Теперь будем плавно переходить к $(\operatorname{Frac} R)[x]$. Пусть f там и лежит. Но тогда заметим, что существует $\tilde{f} \in R[x]$ и $c \in R$ такие, что $f = \frac{\tilde{f}}{c}$. Определим тогда

$$\operatorname{cont} f := \frac{\operatorname{cont} \tilde{f}}{c}.$$

При таком определении всё окей с предыдущими леммами, которые нам понядобятся.

Лемма 15. *Пусть* $f, g \in R[x]$. *Тогда следующие условия эквивалентны:*

- $f|g$ *внутри* $R[x]$;
- $f|g$ *внутри* $(\operatorname{Frac} R)[x]$, *и* $\operatorname{cont} f|\operatorname{cont} g$ *внутри* R.

Доказательство. В разные стороны поочерёдно:

$\Rightarrow$ Пусть $g = fh$ для какого-то $h \in R[x]$. Тогда сразу имеем первое условие, а второе вытекает из мультипликативности: $\operatorname{cont} g \sim \operatorname{cont} f \operatorname{cont} h$.

$\Leftarrow$ Пусть $g := f\frac{\tilde{h}}{c}$ для некоторых $\tilde{h} \in R[x]$ и $c \in R$. То же самое: $gc = f\tilde{h}$. Применим cont: $c \operatorname{cont} g = (\operatorname{cont} f)(\operatorname{cont} \tilde{h})$. По гипотезе, $\operatorname{cont} g \sim d \operatorname{cont} f$ для некоторого $d \in R$. В итоге $cd \operatorname{cont} f \sim \operatorname{cont} f \operatorname{cont} \tilde{h}$, а мы умеем сокращать в обрастях целостности, тогда $cd \sim \operatorname{cont} \tilde{h}$. Значит, $\operatorname{cont} \tilde{h}$ делитная на c, и начальное равенство можно сократить: $g \sim f\hat{h}$, где $\hat{h}$ - какой-то многочлен из $R[x]$. Тогда точно $f|g$ внутри $R[x]$. □

А теперь главное блюдо этого билета.

Теорема 9. *(Теорема Гаусса). Если R факториально, то $R[x]$ факториально.*

Доказательство. Про область мы уже знаем, про нетёровость тоже (из всех этих прошлых лемм). Тогда осталось только понять, что если $p \in R[x]$ неприводим, то он прост.

Первый случай: $\deg p > 0$.

Лемма 16. *Если $p \in R[x]$ - неприводимый многочлен степени хотя бы 1, то* $\operatorname{cont} p \sim 1$.

Доказательство. Предположим противное, пусть $\exists c \nsim 1 : c| \operatorname{cont} p$. Запишем тривиальное разложение $p = c \cdot \frac{p}{c}$. p неприводим и, по определению, неообратим, значит, по крайней мере, один из этих сомножителей ассоциирован с p. Если оба с ним ассоциированы, то $p \sim p^2$, откуда, поскольку мы в области, $p \sim 1$, что , опять же, невозможно. Если $c \sim p$ и $\frac{p}{c} \sim 1$, то $\deg p = 0$ - это не случай, который мы рассматриваем. Иначе $c \sim 1$ и $\frac{p}{c} \sim p$ - противоречие с определением уже c. □

Лемма 17. *Если $p \in R[x]$ - такой же, как и в предыдущей лемме, то p неприводим в* $(\operatorname{Frac} R)[x]$.

Доказательство. Предположим противное: пусть $p := \frac{\tilde{g}}{c}\frac{\tilde{h}}{d}$, где $\tilde{g}, \tilde{h} \in R[x]$ и $\frac{\tilde{g}}{c}, \frac{\tilde{h}}{d} \nsim 1$ в $(\operatorname{Frac} R)[x]$. Пепепишем: $cdp = \tilde{g}\tilde{h}$. По первой лемме, $\operatorname{cont} p \sim 1$, значит, беря содержание обеих частей, получаем

$$cd \sim (\operatorname{cont} \tilde{g})(\operatorname{cont} \tilde{h}).$$

Вернёмся к изначальному $p = \frac{\tilde{g}}{c}\frac{\tilde{h}}{d}$. Здесь $\tilde{g} = (\operatorname{cont} \tilde{g})\hat{g}$ и $\tilde{h}(\operatorname{cont} \tilde{h})\hat{h}$ для некоторых $\hat{g}, \hat{h} \in R[x]$, поэтому

$$p = \frac{(\operatorname{cont} \tilde{g})(\operatorname{cont} \tilde{h})}{cd}\hat{g}\hat{h} \sim \hat{g}\hat{h}.$$

Воспользуемся неприводимостью p в R: скажем, $\hat{g} \sim 1$. Тогда, раз мы в поле,

$$\frac{\tilde{g}}{c} \sim \frac{\operatorname{cont} \tilde{g}}{c} \sim 1,$$

что и требовалось. □

Следствие 1. Более того, в последней лемме $(\operatorname{Frac} R)[x]$ - евклидово, как мы знаем, так что p ещё и простой.

Осталось показать, что от также простой в $R[x]$.

Лемма 18. *Если p - всё тот же, то он простой в $R[x]$.*

Доказательство. Пусть $p|ab$ для каких-то a,$b \in R[x]$. По следствию из второй леммы, p простой в $(\operatorname{Frac} R)[x]$, тогда, без ограничения общности, $p|a$ в $(\operatorname{Frac} R)[x]$. По первой лемме, $\operatorname{cont} p \sim 1$, а тогда $\operatorname{cont} p | \operatorname{cont} a$. Вывели, что $p|a$ в $R[x]$ по лемме, которая была перед теоремой. □

Второй случай: $p \in R$ неприводимый в $R[x]$ и $\deg p = 0$.

Лемма 19. *p неприводим и в R.*

Доказательство. Пусть $p = ab$. a и b - тоже какие-то константы, потому что мы в области целостности, и при умножении степени сохраняются. При этом, без ограничения общности, $a \sim 1$ в $R[x]$. Но тогда $a \sim 1$ и в R, потому что $R^\times = R[x]^\times$ (это, похоже, обратимые элементы). □

R факториально, поэтому p простой и в R по определению факториальности. Значит, $R/(p)$ - область, а тогда $R/(p)[x]$ - тоже область. И тут наша последняя лемма:

Лемма 20. $R/(p)[x] \cong R[x/(p)]$.

Доказательство. Посмотрим на $f = \sum a_i x^i \mapsto \sum [a_i] x^i$. Видно, что он сюръективен, а его ядро - это ровно $(p) \subseteq R[x]$. (Тут типа применяется теорема о гомоморфизме). □

Значит, $R[x]/(p)$ - тоже область. Значит, p - простой в $R[x]$.

□

1.12 Теорема Безу. Производная многочлена и кратные корни

Теорема 10. *(Универсальное свойство кольца многочленов). Пусть $i : R \to R[x]$ - стандартное вложение (отправляет каждый элемент в себя), $f : R \to S$ - гомоморфизм колец, $r \in R$ - произвольный элемент. Тогда существует единственный гомоморфизм ё$\bar{f} : R[x] \to S$ такой, что $f = \bar{f} \circ i$ и $\bar{f}(x) = f(r)$.*

Доказательство. Раз уж в билетах нет, то и доказательства не будет. Определить его не сложно, показать, что гомоморфизм - тоже. □

Определение 32. По универсальному свойству кольца многочленов дл $f := \mathrm{id}_R$ и произвольного $r \in R$ существует единственный $\bar{f} : R[x] \to R$ такой, что $\bar{f}(x) = f(r) = r$. В этом случае $\bar{f}$ называется *гомоморфизмом вычисления* и обозначается за ev_r.

Теорема 11. *(Теорема Безу). $R[x]/(x-a) \simeq R$ посредством $[f(x)] \mapsto f(a)$, где R - коммутативное кольцо с единицей.*

Доказательство. Понятно, что $x - a \in \operatorname{Ker} \mathrm{ev}_a$, тогда и идеал $(x-a) \subset \operatorname{Ker} \mathrm{ev}_a$.

Теперь нужно показать в обратную сторону. Здесь делим с остатком: пусть $f := (x-a)g + c$, где $c = f(a)$. Тогда $[f] = [c]$ в $R[x]/(x-a)$. Значит, $f \in (x-a)R[x] \Leftrightarrow f(a = 0)$. □

В общем, опять очередное применение теоремы о гомоморфизме, про образ мы уже понимаем, сам он задаётся корректно, а мы лишь проверяем, что идеал $(x-a)$ есть ядро.

Доказательство. (Второе доказательство). Сначала заметим, что для $R[x]/(x) \cong R$ теорема очевидна, а затем при помощи универсального свойства кольца многочленов, выполним замену переменной на $(x-a)$. Условно, у нас есть гомоморфизмы в обе стороны $x \to (x-a)$ и наоборот $(x+a) \leftarrow x$. Тогда $R[x]/(x-a) \cong R[x]/(x) \cong R$. □

Определение 33. Для $f = \sum a_i x^i$ определим $f' := \sum i a_i x^{i-1}$.

Тогда видно, что $(f+g)' = f' + g'$, а также $(fg)' = f'g + fg'$, что уже проверить сложнее.

Лемма 21. *a - кратный (кратности больше 1) корень f тогда и только тогда, когда a - корень многочлена и его производной.*

Доказательство. Поделим f на $(x-a)$: $f = (x-a)g + f(a) = (x-a)g$. a - кратный корень f тогда и только тогда, когда $g(a) = 0$. Теперь давайте продифференцируем это выражение: $f' = g + (x-a)g'$. Отсюда $f'(a) = g(a)$. Что и требовалось. □

1.13 Интерполяция Лагранжа

Теорема 12. *(Частично Лагранж). Пусть F - поле, $\{a_0, \ldots, a_n\}$ - набор его различных элементов. Тогда*

$$\frac{F[x]}{(\Pi(x - a_i))} \cong F^n$$

посредством

$$f \mapsto (f(a_0), \ldots, f(a_{n-1})).$$

Доказательство. Докажем, что его ядро есть $((x-a_0)\ldots(x-a_{n-1}))$. Спроецируем F^n на F и применим теорему Безу. Условно говоря, f лежит в ядре $\mathrm{ev}_{a_0,\ldots,a_{n-1}}$, но тогда и в ядре ev_{a_i}, где ev_{a_i} - композиция $F[x] \to F^n \to F$, то есть, вычисление значения в конкретной точке. Тогда по теореме Безу мы получили, что $x - a_i | f$, но над полем они неприводимы и взаимно просты. Тогда по основной теореме арифмитики получим, что их lcm есть их произведение, тогда f делится на это произведение. И наоборот, если $\Pi(x - a_i) | f$, то $\forall i : f(a_i) = 0$. Получилось.

Докажем теперь сюръективность. найдём прообраз $(b_0, \ldots, b_{n-1})$.

$$\sum_i b_i \cdot \frac{\Pi_{j \neq i}(x - a_j)}{\Pi_{j \neq i}(a_i - a_j)}$$

подходит, нетрудно убедиться. Это и есть *интерполяция по Лагранжу* (возможно, надо рассказать только про неё, но тогда совсем пустой билет выходит). □

1.14 Интерполяция Эрмита

Концептуально, мы хотим научиться ещё как-нибудь интерполировать. Например, по точкам и значениям производных в них (до каких-то определённых порядков).

Теорема 13.

$$\frac{F[x]}{(\Pi(x - a_i)^{m_i})} \cong \frac{F[x]}{((x - a_0)^{m_0})} \times \cdots \times \frac{F[x]}{((x - a_n)^{m_n})}$$

Доказательство. Опять-таки рассмотрим гомоморфизм $f \mapsto (f + (x - a_0)^{m_0} F[x]), \ldots, f + (x - a_n)^{m_n} F[x])$. Аналогично предыдущему билету, показываем, что ядро - произведение этих разностей в нужных степенях. Так же раскладываем в проекции по каждому элементу произведения (а была на лекциях такая лемма, что $f[x]$ в $R[x]/((x-a)^m) \longleftrightarrow (f(a), f'(a), \ldots, f^{(m-1)})$ (биекция)). f принадлежит ядру, а это равносильно тому, что $(x - a_i)^{m_i} | f(x)$, тогда в силу взаимной простоты, произведение $\Pi(x - a_i)^{m_i}$ делит $f(x)$. Тогда ядро и равно этому произведению.

Теперь нам нужно доказать сюръективность. Зафиксируем $l_i < m_i$. Хотим найти такую f, что

- $f^{(l)}(a_j) = 0$ для $l < m_j, j \neq i$;
- $f^{(l)}(a_i) = 0$ для $l < m_i, l \neq l_i$;
- $f^{(l_i)}(a_i) = 1$.

Будем считать, что для больших значений l_i (то есть, $\{l_i + 1, \dots, m_i - 1\}$) мы уже всё проделали.

Первое условие гласит, что a_j должен быть корнем кратонсти хотя бы m_j. Значит, $\Pi_{j\neq i}(x - a_j)^{m_j} | f$. Второе и третье же влекут, что $\frac{1}{l_i!}(x - a_i)^{l_i} | f$. Рассмотрим тогда

$$f := C(a_i) \cdot \frac{1}{l_i!}(x - a_i)^{l_i} \Pi_{j\neq i}(x - a_j)^{m_j},$$

где

$$C(x) := \left(\left((x - a_i)^{l_i} \Pi_{j\neq i}(x - a_j)^{m_j} \right)^{(l_i)} \right)^{-1}.$$

Он удовлетворяет первому и третьему условию. Единственная проблема состоит в том, чтопроизводные $f^{(l)}$ порядком l выше l_i могут принимать какие-то лишние значения $f^l(a_i)$ в точке a_i, но эту проблему можно решить, ведь из предположения индукции мы можем вычесть какие-то базисные многочлены с соответствующими коэффициентами и получить новый многочлен, который будет удовлетворять уже всем условиям.

Это была *интерполяция Эрмита*. Простой формулы нет. □

1.15 Поле разложение многочлена

Пусть F - поле и $f \in F[x]$. Поле многочленов евклидово и факториально, значит, у f есть неприводимый делитель g ($f = gh$) для некоторого h. Рассмотрим теперь $F[x]/(g)$ - область, поскольку g - простой из-за факториальности $F[x]$. Более того, выполнена лемма:

Лемма 22. *Пусть R - коммутативное кольцо главных идеалов с единице, а $p \in R$ - простой. Тогда $R/(p)$ - поле.*

Доказательство. Пусть $[t] \in R/(p)$ таков, что $[t] \neq [0]$. Тогда $(t, p) = (1)$ по определению p, и существует линейной представление НОД: $tu + pv = 1$ для некоторых u, v, откуда сразу $[tu] = [t][u] = 1 - [pv] = [1] - [0]$. То есть, вот мы и нашли для каждого обратный по умножению. □

То есть, что мы тут делаем. Если g - многочлен над $F[x]/(g)$, то у него появляются корни - $[x]$, например, $g([x]) = [g(x)] = [0]$. Тем более, $[x]$ - корень f. То есть, его, допустим, у нас есть какой-то многочлен, то по нему можно отфакторизовать и получить R расширенное с дополнительными корнями. Пусть тогда $F[x]/(g)$ - это F_1, тогда если $a \in F_1$ - найденный нами в F_1 корень f, то многочлен по теореме Безу представляется как $f = (x - a)f_1$ для некоторого f_1 на единицу меньшей степени. Тогда будем так по индукции присоединять корни f, пока не придём к полю F_n, где $n := \deg f$.

Определение 34. F_n из рассуждений выше называется *полем разложения* f.

Теорема 14. *Пусть: F - поле, $f \in F[x]$ - многочлен, $n := deg f$, F_n - поле разложения, $\varphi : F \to F_n, \psi : F \to K$ - какие-то вложения, в $K[x]$ f раскладывается на линейные множители.*

Тогда существует (не обязательно единственное) вложение $\bar{\psi} : F_n \to K$ такое, что $\psi = \bar{\psi} \circ \varphi$. Вэтом смысле, F_n - наименьшее поле, которое содержит все корни f.

Доказательство. Инъективность $\bar{\psi}$, как и $\varphi c \psi$, следует попросту из того, что любой гомоморфизм полей инъективен или тривиален (это обсуждалось на лекциях), а $\bar{\psi}$ должен сохранять единицу, так как ψ и φ её сохраняют.

Будем одказывать факт по индукции. Изначально, мы можем взять в качестве $\bar{\psi}$ просто ψ, когда мы ещё не присоединили никаких корней. Теперь доказываем переход. Предполагаем, что $F_i \to K$ имеется. Тогда рассмотрим новый для какого-то свежеприсоединённого $Y : F[Y] \to F[Y]/(g(Y)) \dashrightarrow K$. Нам нужно: придумать куда отправить Y, а также, чтобы было выполнено $g(a) = 0$ (для всех остальных элементов всё и так уже прекрасно). То есть, нам нужно выбрать корень $g(x)$ внутри K, но такой есть в силе того, что f раскладывается внтури этого поля на множители, тогда и g раскладывается (как его делитель по основной теореме арифметики), оттуда и выберем (любой, отсюда и пропадает единственность). Переход доказан. □

Некоторые свойства поля разложение, на всякий случай:

Лемма 23. *Пусть R - коммутативное кольцо с 1 и задан гомоморфизм $\varphi : \mathbb{Z} \to R$, $\varphi(1) = 1_R$, $\mathrm{Ker}(\varphi) = (p)$. Если R - область, то p - простое или нуль.*

Лемма 24. *Пусть R - коммутативное кольцо с единицей. Если $\mathrm{char}(R) = p$ - простое, то отображение $\varphi : R \to R, \varphi(x) = x^p$ - гомоморфизм колец.*

Лемма 25. *Пусть $f(x), g(x) \in F[x]$, F вкладывается в E. Тогда $\gcd_{F[x]}(f(x), g(x)) \sim \gcd_{E[x]}(f(x), g(x))$*

Лемма 26. *У многочлена $f(x) \in F[x]$ есть кратный корень тогда и только тогда, когда $f(x)$ и $f'(x)$ не взаимно просты.*

1.16 Комплексные числа. Решение квадратных уравнений в

Пусть есть поле $\mathbb{R}$. Рассмотрим поле разложения $x^2 + 1 \Rightarrow \mathbb{R}[y]/(y^2 + 1)$. Будем обозначать это поле за $\mathbb{C}$ и называть *полем комплексных чисел*. При этом вместо y пишут i. Это поле хорошо тем, что всякий многочлен в нём имеет корень. Покажем это для квадратных многочленов. Пусть дан многочлен $ax^2 + bx + c$, поделим его на a и сделаем замену переменной, полуичим многочлен вида z^2=d. То есть, нам нужно научить ся извлекать корень из комплексного числа. Это делается либо "тупо в лоб", либо через формулу Муавра: $z^n = e^{i\varphi n} = \cos(\varphi n) + i \sin(\varphi n)$. Распишем $c = s(\cos\psi + i \sin\psi)$ для параметров $s, \psi \in \mathbb{R}, s \geq 0$, тогда подойдёт

$$z = s^{\frac{1}{n}}(\cos(\psi/n) + i \sin(\psi/n)).$$

Во время рассказа можно упомянуть, что такое модуль и сопряжённое, а также несколько их свойств (которые слишком уж очевидны).

Определение 35. Поле называется *алгебраически замкнутым*, если любой многочлен $f(x) \in F[x]$ степени хотя бы 1 имеет хот ябы один корень. То есть все многочлены в $F[x]$ раскладываются на линейные множители.

1.17 Основная теорема алгебры

Теорема 15. *(Основная теорема алгебры). - алгебраисески замунутое поле (см конец предыдущего билета).*

Доказательство. Будем доказывать, через модули чисел (для комплексных и вещественных это одно и то же). Будем говорить, что последовательность $\{z_n\}_{n\in\mathbb{N}} \subset \mathbb{C}$ сходится к z_0, если

$$\forall\varepsilon > 0 \exists N \in \mathbb{N} \forall n > N : |z_n - z_0| < \varepsilon.$$

Лемма 27. *Пусть z_n - последовательность комплексных чисел, x_n и y_n - её вещественная и мнимая части. $\{z_n\}$ сходится к z_0 тогда и только тогда, когда $\{x_n\} \to x_0 := Rez_0$ и $\{y_n\} \to y_0 := Imz_0$.*

Доказательство. $\Leftarrow$ Возьмём $\varepsilon/2$ и такие моменты начиная с N_1, N_2 для x_1, x_2 соответственно, начиная с которых мнимые и вещественные части попадают в выбранную окрестность. Теперь выберем максимальный из этих моментов и получим требуемое. $\Rightarrow$ Возьмём ε, выберем натуральное N так, чтобы $\forall n > N |z_n - z_0| < \varepsilon$. То есть, $\sqrt{(x_n - x_0)^2 + (y_n - y_0)^2} < \varepsilon$, но тогжа и расстояние от мнимой, и расстояние от вещественной части до предела меньше ε. □

Лемма 28. *(Непрерывность арифметики). Пусть $\{z_n\} \to z_0, \{w_n\} \to w_0$. Тогда выполнены правила предела суммы и произведения пределов.*

Следствие 1. (Непрерывность многочленов). Пусть $f(z)$ - многочлен из $\mathbb{C}[z], \{z_n\} \to z_0$. Тогда $\{f(z_n)\} \to f(z_0)$.

Лемма 29. *(Секвенциальная компактность диска). Пусть последовательность $\{z_n\}$ такова, что последовательность из её модулей $\{|z_n|\}$ ограничена. Тогда из $\{z_n\}$ можно выбрать сходящуюся подпоследовательность $\{z_{n_k}\} \to z_0$, где $|z_n|$ - конечное число.*

Доказательство. Пусть $z_n = x_n + y_n i$. Тогда сначала выберем подпоследовательность по x_i (ну она ограничена, по матану мы так умеем), а потом из соответствующих им y_j также выберем сходящуюся подпоследовательность. □

Лемма 30. *Пусть $f(x) \in \mathbb{C}[z]$ - многочлен ненулевой степени, а $\{z_n\}$ расходится. Тогда $\{f(z_n)\}$ также расходится.*

Доказательство. Пусть

$$f(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_0.$$

Тогда

$$\frac{f(z)}{z^n} = a_n + \frac{a_{n-1}}{z} + \cdots + \frac{a_0}{z^n}.$$

При $z \to \infty$ все члены, кроме a_n, стремятся к 0. По непрерывности арифметики получим, что при $z \to \infty$ $\frac{f(z)}{z^n} \to a_n$. А значит, $f(z)$ тем более стремится к бесконечности. □

Лемма 31. *Пусть $f \in \mathbb{C}[z]$ - многочлен ненулевой степени. Пусть z_0 - не корень f. Тогда существует $z_1 \in \mathbb{C}$ такое, что $|f(z_1)| < |f(z_0)|$.*

Доказательство. Можно считать, что $z_0 = 0$ (через замену переменной). Без ограничения общности, $f(0) = 1$, так как можем сначала поделить на $f(0)$, а затем обратно домножить. Значит, мы получили, что свободный член равен единице. Пусть k - следующий посне 0 номер ненулевого коэффициента, тогда

$$f(z) = 1 + c_k z^k + \cdots + c_n z^n, c_k \neq 0.$$

Возьмём $z = wt$, где $t \in (0,1)$ - небольшое вещественное число, а w таково, что $c_k w^k = -1$. Подставим это в f и вынесем t^k:

$$f(z) = 1 - t^k + c_{k+1} w^{k+1} t^{k+1} + \cdots + c_n w^n t^n = 1 - t^k + t^k (c_{k+1} w^{k+1} t + \cdots + c_n w^n t^{n-k}).$$

Здесь последний множительно в скобках не превосходит $A \cdot (n-k) \cdot t$ для какой-то положительной константы A, которая зависит от $\{c_i\}$ и w. Таким образом, при

$$t < \frac{1}{(n-k)A}$$

этот множитель меньше единицы: $|c_{k+1} w^{k+1} t + \cdots + c_n w^n t^{n-k}| < 1$, а тогда $|f(z| < (1 - t^k) + t^k = 1)$, что и требовалось. □

Осталось доказать основную теорему алгебры. Рассмотрим

$$\inf_{z \in \mathbb{C}} |f(z)| = m.$$

Если он достигается, то по лемме не может быть положительным, так что ь = 0. Пусть не достигается, тогда выберем подпоследовательность $\{z_n\}$ такую, что $\{|f(z_n)|\} \to m$. Тогда $\{|z_n|\}$ ограничена, иначе бы из неё можно было выбрать подпоследовательность, которая стремится к бесконечности, а тогда и многочлен на этой подпоследовательности стремился бы к бесконечности. По секвенциальной компактности диска, выбираем сходящуюся подпоследовательность, стремящуюся к z_0. Тогда по непрерывности f, значение в z_0 равно пределу значений сходящейся подпоследовательности, инфимум всё же достигается.

Мы поняли, что $\inf |f(z_n)| = 0$, при этом этот инфинум всё же достигается. Значит, существует z_0 такое, что $|f(z_0)| = 0$. Таким образом, у f есть хотя бы один корень. □

1.18 Разложение рациональной функции в простейшие дроби над $\mathbb{C}$ и над $\mathbb{R}$

Учимся раскладывать $\frac{f(x)}{g(x)}$, где $g(x) = (x - \alpha_1)^{m_1} \dots (x - \alpha_k)^{m_k}$, в сумму дробей вида $\frac{c}{(x-\alpha_i)^{l_i}}, c \in \mathbb{C}$, то есть, хотим найти разложение

$$\frac{f(x)}{\Pi(x - \alpha_i)^{m_i}} = \sum_{i=1}^{k} \sum_{l=1}^{m_i} \frac{c_{i,l}}{(x - \alpha_i)^{l_i}}$$

Теорема 16. *Разложение правильной дроби в $\mathbb{C}(x)$ в сумму простейших существует и притом единственно.*

Доказательство. Домножим разложение, которое мы хотим найти, на $g(x)$. Теперь хотим найти разложение

$$f(x) = \sum_{i=1}^{k} \sum_{l=1}^{m_i} c_{i,l} (x - \alpha_i)^{m_i - l} \Pi_{j \neq i} (x - \alpha_j)^{m_j}.$$

Заметим, что в $f(\alpha_i)$ обнуляется всё, кроме одного слагаемого вида $c_{i,l}(a_i - a_i)^0 \Pi_{j\neq i}(\alpha_i - a_j)^{m_j}$. Тогда

$$c_{i,m_i} = \frac{f(\alpha_i)}{\Pi_{j\neq i}(a_i - a_j)^{m_j}}.$$

Теперь из $f(x)$ вычтем те слагаемые из этой суммы, из которых мы нашли коэффициенты. Пусть

$$f_i(x) := f(x) - \sum_i c_{i,m_i}\Pi_{j\neq i}(x - \alpha_j)^{m_j}.$$

Этот многочлен делится на $(x - \alpha_i)$ для любого i. Вычтенное сокращается:

$$f_1 = \sum_{i=1}^{k}\sum_{l=1}^{m_i-1} c_{i,l}(x - \alpha_i)^{m_i-l}\Pi_{j\neq l}(x - \alpha_j)^{m_j}.$$

Большинство слагаемых при оставшихся коэффициентах делятся на $(x - \alpha_i)^2$, а при взятии производной и вычислении на α_i они будут обнуляться. Одно слагаемое останется: то, которое привязано к c_{i,m_i-1}. Из значения $f'(\alpha_i)$ так же полкчаем формулу для следующей партии коэффициентов c_{i,m_i-1}, по индукции найдём для всех остальных. Из этого сразу будет следовать единственность.

Будем теперь считать, что мы знаем $c_{i,l}$. Возьмём h равным тому исходному выражению для f:

$$h(x) := \sum_{i=1}^{k}\sum_{l=1}^{m_i} c_{i,l}(x - \alpha_i)^{m_i-l}\Pi_{j\neq i}(x - \alpha)^{m_j}.$$

Хотим показать, что $f(x) = h(x)$. Что мы знаем об этих функциях? По определению коэффициентов $c_{i,j}$ производные f и g в точках $\{\alpha_i\}$ равны, а именно, для каждого i

$$f(\alpha_i) = h(\alpha_i), \ldots, f^{(m_i-1)(\alpha_i)=h^{(m_i-1)(\alpha_i)}}.$$

А это задача интерполяции Эрмита, у неё единственное решение нужной степени, из этого $h(x) = f(x)$. □

Теорема 17. *Разложение правильной дроби в $\mathbb{R}(x)$ в сумму простейших существует и притом единственно.*

Доказательство. Есть дробь $\frac{f(x)}{g(x)}$, представим знаменатель $g(x) = \Pi p_i^{m_i}$, где $p_i(x)$ - неприводимые, попарно не ассоциированные. Для начала давайте найдём разложение

$$\frac{f(x)}{g(x)} = \sum_i \frac{a_i(x)}{p_i^{m_i}},$$

где все дроби в сумме правильные. Домножим на знаменатель:

$$f(x) = \sum_i a_i(x)\Pi_{j\neq i}p_j^{m_j}.$$

Здесь все слагаемые, кроме одного, делятся на $p_i^{m_i}$.

Теперь нам надо перейти к фактор-кольцу $F[x]/(p_i^{m_i})$, тогда нам необходимо будет равенство

$$[f(x)] = [a_i(x)]\left[\Pi_{j\neq i}p_j^{m_j}\right],$$

при этом элементы $[f(x)]$ и $\left[\Pi_{j\neq i}p_j^{m_j}\right]$ мы также знаем, а значит, можем восстановить и $[a_i(x)]$, нам нужно лишь обратимость $\left[\Pi_{j\neq i}p_j^{m_j}\right]$ в $F[x]/(p_i^{m_i})$. В $F[x]/(p_i^{m_i})$ обратимыми будут те элементы, которые взаимно просты с $p_i^{m_i}$, так как $F[x]$ - евклидово кольцо и работает линейное представление НОД. Наше произведение $\left[\Pi_{j\neq i}p_j^{m_j}\right]$ взаимно просто с $p_i^{m_i}$, поэтому обратимо. Можем найти $[a_i(x)]$. При этом мы можем выбрать такой представитель этого класса эквивалентности, что $\deg a_i < \deg p_i^{m_i}$. Получилось, что если разложение существует, то оно единственно.

Докажем существование. Давайте этим методом составим некоторый многочлен $h(x)$. Тогда мы знаем, что для любого i $h(x) \equiv f(x \mod p_i^{m_i})$. По КТО h и f сравнимы и по модулю произведения $\{p_i^{m_i}\}$, то есть, g. А из-за того, что $\deg f < \deg g, \deg h < \deg g$, получаем, что $f(x) = h(x)$.

Осталось каждую дробь суммы $\frac{a_i(x)}{p_i^{m_i}}$ разложить в сумму простейших, то есть

$$\frac{a_i}{p_i^{m_i}} = \sum_{l=1}^{m_i} \frac{a_{i,l}(x)}{p_i^l(x)},$$

где $\deg a_{i,l} < \deg p_i$. Опять же, нам нужно разложение

$$a_i = \sum_l a_{i,l} p_i^{m_i - l}.$$

В это можно и поверить наслово, но ниже приведём краткое доказательство. □

Лемма 32. *(Та самая). Пусть F - поле, p - многочлен ненулевой степени из $F[x]$. Тогда любой многочлен $a \in F[x]$ может быть записан единственным образом в виде*

$$a = a_0 + a_1 p + \cdots + a_n p^n,$$

где дл/ всякого i либо $\deg a_i < \deg p$, либо $a_i = 0$.

Доказательство. Существование по индукции по степени $a(x)$. База: если $\deg a < \deg p$, то просто возьмэм $a_0(x) = a(x)$. Если же $\deg a \geq \deg p$, то поделим $a(x)$ на $p(x)$ с остатком, получим $a(x) = p(x)q(x) + r(x)$, при этом $\deg r(x) < \deg p(x)$. Посмотрим на степень $q(x)$,

$$\deg q(x) = \deg(a(x) - r(x)) - \deg p(x) = \deg a(x) - degp(x) < \deg a(x),$$

так как $\deg a(x) > \deg r(x)$, а значит, можно применить предположение индукции для $q(x)$:

$$q(x) = a_1(x) + a_2(x)p(x) + \cdots + a_n(x)(p(x))^{n-1},$$

тогда

$$a(x) = r(x) + q(x)p(x).$$

Единственность тоже по индукции, теперь по n. Заметим: что $a_0(x) \equiv b_0(x) \mod p(x)$, так как всё остальное на $p(x)$ делится, при этом их степени меньше степени $p(x)$, а значит, $a_0(x) = b_0(x)$. Тогда сократим эти члены, поделим на $p(x)$ и применим индекционное предположение. □

1.19 Определение векторного пространства. Линейная зависимость. Существование базиса

Для начала введём понятия, которых нет в билетах, а также некоторые их свойства, которые пригодятся для определения объектив в этом билете.

Определение 36. Пусть R - кольцо. Тогда *левый R-модуль* - это абелева группа M вместе с операцией $R \times M \to M, (r, m) \mapsto r \cdot m$, удовлетворяющая следующим свойствам:

- $r \cdot (a + b) = r \cdot a + r \cdot b$;
- $(r + s) \cdot a = r \cdot a + s \cdot b$;
- $(rs) \cdot a = r \cdot (s \cdot a)$;
- (если R - кольцо с 1) $1 \cdot a = a$.

Аналогично определяется *правый R-модуль*, только там всё с другой стороны.

Определение 37. Пусть M, N - R-модули. *Прямая сумма R-модулей* - R-модуль $M\oplus$ с носителем $M \times N$ и покомпонентными операциями:

$$r \cdot (m,n) := (r \cdot m, r \cdot n), (m_1, n_1) + (m_2, n_2) := (m_1 + n_1, m_2 + n_2).$$

Все свойства R-модуля выполняются покоординатно, значит, выполняются.

Определение 38. Пусть M и N - левые R-модули. Отображение $\varphi : M \to N$ между ними, которое сохраняет операции:

$$\varphi(rm) = r\varphi(m) \text{ и } \varphi(m_1 + m_1) = \varphi(m_1) + \varphi(m_2),$$

называется *гомоморфизмом модулей* или *линейным отображением*.

Определение 39. Обозначим за $\{m_i\}$ произвольные элементы модуля, за $\{r_i\}$ - элементы соответствующего кольца.

- Уравнение
$$\sum_{i=1}^{n} m_i r_i = 0$$
называется *линейной зависимостью*.
- Линейная зависимость *тривиальна*, если все $\{r_i\}$ равны нулю.
- Конечный набор $m_1, \ldots, m_n$ *линейно независим*, если любая его линейная зависимость тривиальна.
- Бесконечный набор $\{m_i\}$ линейно независим, если любой его конечный поднабор линейно независим.

Лемма 33. *Пусть $\{m_i\}_{i\in I}$ - набор элементов свободного модуля $R^{(I)}$. Любой конечный поднабор $\{m_i\}$ линейно независим тогда и только тогда, когда линейное отображение $f \mapsto \sum f(i)m_i$ инъективно.*

Доказательство. Вспомним, что гомоморфизм групп инъективен тогда и только тогда, когда его ядро тривиально. Тогжа обратим внимание на определение линейной независимости и линейного отображения и поймём, что здесь сказано одно и то же. □

Определение 40. Набор $\{m_i\}$ называется *системой образующих*, если линейное отображение $f \mapsto \sum f(i)m_i$ сюръективно.

Следствие 1. Эквивалентно, любой элемент модуля можно представить линейной комбинацией конечного поднабора $\{m_i\}$ (в нормальной жизни это называлось порождающей системой).

Лемма 34. *Подмножество $\{m_i\}$ модуля - линейно независимая система образующих тогда и только тогда, когда линейное отображение $f \mapsto \sum f(i)m_i$ - изоморфизм.*

Определение 41. *Базис* - линейно независимая система образующих.

Определение 42. Пусть F - поле. F-модуль называется *векторным пространством* над F.

Теорема 18. *(О существовании базиса). Любую линейно независимую систему в векторном пространстве можно дополнить до базиса. В частности, в любом векторном пространстве есть базис.*

Доказательство. Будем доказывать через лемму Цорна, рассмотрим частично упорядоченное множество S, носитель которого - множество линейно независимых систем, содержащих данную, а отношение порядка - включение.

Рассмотрим супремум (обхединение) некоторой цепи и линейную зависимость какого-то конечного подмножества этого объединения. Каждый вектор в этой линейной зависимости лежит в некотором из элементов цепи. Всего таких векторов конечное число, а цепь по определению линейно упорядочена, поэтому мы можем выбрать наибольший элемент цепи, который содержит каждый их векторов. Этот наибольший набор по определению линейно независим, значит, вся рассматриваемая линейная комбинация тривиальна, Получается, что объединение тоже линейно независимо и содержит исходную систему.

Теперь применяем лемму Цорна: в нашем линейно упорядоченном множестве S существует максимальный элемент, то есть, максимальная линейно независимая система среди линейно независимых систем, содержащих данную. Но так как любая линейно назависимая система, содержащая максимальную систему, содержит и данную, то максимальная система будет максимальной линейно независимой среди всех линейно независимых систем. По одной из переформулировок это и есть базис (мы их, конечно, не привели, но нетрудно догадаться, что базис это минимальная по включению система образующих или максимальная по включению линейно независимая система). □

1.20 Размерность векторного пространства

Определение 43. *Размерность* $\dim V$ векторного пространства V - мощность его базиса.

Далее мы докажем, что все бащисы векторного пространства равномощны, тем самым определение будет корректно.

Теорема 19. *Все базисы одного векторного пространства равномощны.*

Доказательство. 1 случай (конечный). Рассмотрим два конечный базиса V: $\{v_1, \dots, v_n\}$ и $\{u_1, \dots, u_m\}$. Представим v_n в виде $v_n = \sum_{i=1}^{m} u_i\alpha_i, \alpha_i \in F$, причём не все α_i равны нулю, так как иначе $v_n = 0$ - нетривиальная линейная зависимость первого набора. Не умаляя общности, пусть $\alpha_m \neq 0$. Тогда $v_n\alpha_m^{-1} = u_m + \sum_{i=1}^{m-1} u_i\alpha_i\alpha_m^{-1}$. Заменим в первом базиче v_n на $v_n\alpha_m^{-1}$, и первый базис останется базисом (понятно, что они опять-таки всё порождают, поделим изначальный коэффициент того или иного разложения на α_m^{-1}. аналогично, они линейно независимы, так как можно поделить последний коэффициент). Во втором базисе заменим u_m на $u_m + \sum_{i=1}^{m-1} u_i\alpha_i\alpha_m^{-1}$, и второй базис также останется базисом, покажем это.

Предположим, что полученный набор линейно зависим, то есть, $\sum_i = 1^{m-1}u_i\beta_i + (u_m + \sum_{i=1}^{m-1})\beta_m = 0$ - некоторая нетривиальная линейная зависимость нового набора. $\beta_m \neq 0$, так как иначе существовала бы нетривиальная зависимость набора $\{u_1, \dots, u_{m-1}\}$. Раскроем скобки, приведём подобные, получим некоторую линейную линейную зависимость изначального второго набора, причём нетривиальную, так как коэффициент при u_m будет равен β_m, то есть, будет ненулевым. Противоречие с тем, что изначальный второй набор - базис. Значит, полученный набор линейно независим. Аналогично, полученный набор - система образующих, а значит, базис. Таким образом, мы получили два базиса, у которых хотя бы один элемент общий. Так будем преобразовывать бащисы, увеличивая количество общих элементов. В конце концов окажется, что один базис содержится в другом, а тогда они совпадают, так как базис - минимальная по включению система образующих. При этом на каждом шаге мы меняли только по вектору из каждого бащиса, а количество векторов в базичах не меняли. Значит, изначальные базисы равномощны.

2 случай (бесконечный). Пусть $u = \{u_i\}_{i\in I}, v = \{v_j\}_{j\in J}$ - базисы, причём $|I| > |J|$ и $|I|$ бесконечна. Выразим элементы u через v : $u_i = \sum_{j\in J_i} v_j\alpha_j, |J_i| < \infty$. Рассмотрим отображение из I в множество конечных подмножеств J, которое мы обозначаим как J', действующее по правилу $i \mapsto J_i$. Воспользуемся утверждением, доказанным в курсе теории множеств: если J конечно, то $|J'| = 2^{|J|}$, то есть, J' конечно, иначе $|J'| = |J|$. С исходным неравенством это становится $|I| > |J'|$ (если J конечно: то неравенство верно, так как I бесконечно, а J' конечно: иначе $|I| > |J| = |J'|$).

Рассмотрим конечное подмножество K индексов второго базиса и посчитаем число его прообразов в первом базисе при отображении $i \mapsto J_i$. Векторов, которые переходят в K, не может быть больше $|K|$, поскольку в ином случае, в пространстве, которо порождено векторами K, нашлась бы ли линейно независимая система из $|K|+1$ векторов (любое подмножество базиса u линейно независимо), а это невозможно по рассуждению для конечного случая. Значит, у K конечное число прообразов в I.

Таким образом, опять же по теоретико-множественным соображениям, либо J' конечно, и, следовательно, I тоже конечно, как объединение конечного числа конечных множеств, либо J' бесконечно, и, следовательно, $|I| = |J| = |J'|$, так как I - объединение $|J|$ множеств конечной мощности каждое.

Так или иначе, мы получили противоречие с изначальными условиями на I и J. □

Следствие 1. Любое векторное пространство V над F изоморфно свободнуму модулю $F^{(I)}$, причём $|I|$ определена однозначно.

Теперь изначальное определение корректно.

1.21 Линейные отображения векторных пространств. Подпространство, фактор-пространство. Ранг линейного отображения

Определение линейного отображения мы уже упоминали в прошлом билете. И тем не менее, сначала опять несколько определений, которые нужны для понимания того, что происходит

в самом билете.

Определение 44. Подмножество модуля, которое само является модулем над тем же кольцом и замкнуто относительно всех операций, называется *подмодулем*.

Определение 45. Пусть M - левый R-модуль, N - подмодуль. *Факторомодулем* R/N называется фактор R по отношению эквивалентности

$$a \equiv b \iff a - b \in N$$

с определёнными на нём операциями

$$[a] + [b] := [a + b], r \cdot [a] := [ra].$$

Нетрудно теперь заменить несколько слов и понять, что такое подпространство и факторпространство.

Определение 46. *Коразмерность* $\operatorname{codim}_V U$ подпространства $U \leq V$ равна $\dim V/U$.

Определение 47. Пусть $U \leq V$ - векторные пространства. Тогда *относительный базис* - дополнение какого-то базиса U до базиса V.

Теперь можно немного подробнее поговорить о линейных отображениях именно векторных пространств.

Пусть $f : V \to W$ - линейное. Скажем, что ядро есть $U \leq V$, тогда найдём относительный базис $\{v_i\}_{i \in I}$. Тогда f определяется своими значениями именно на этом относительном базисе. Значения $\{f(v_i)\}_{i \in I}$ внутри W должны быть линейно независимы, иначе:

$$\sum_i f(v_i)\alpha_i = 0 \Leftrightarrow f(\sum_i v_i\alpha_i) = 0, \text{ но тогда } \sum_i v_i\alpha_i \in \operatorname{Ker} f = U,$$

а затем $\{f(v_i)\}_{i \in I}$ дополняется до базиса в W. То есть, базис V разбивается на две части: одна зануляется, другая во что-то переходит и как-то дополняется в W до базиса там.

Определение 48. Пусть f - линейное отображение векторных пространств. Тогда размерность образа f называется *рангом* f и обозначается

$$\operatorname{rank} f := \dim \operatorname{Im} f = \operatorname{codim} \operatorname{Ker} f.$$

(на более простом языке - это количество единичных столбцов в матрице преобразования, написанной для правильных базисов).

1.22 Матрица линейного отображения. Композиция линейных отображений и произведение матриц. Кольцо матриц

Матрица линейного отображения $F^n \to F^m$ будет выглядеть так: n столбцов высоты m, где каждый столбец - образ какого-то элемента базиса первого пространства (то есть, его разложение в базис второго пространства по строчкам).

Пусть у нас имеется композиция линейных отображений $b \circ a, a : F^n \to F^m, b : F^m \to F^p$. Пусть $\{e_j\}$ - базис первого, $\{f_i\}$ - базис второго, $\{g_k\}$ - базис третьего. Тогда

$$a(e_j) = \sum_{i=1}^{m} f_i a_{ij},$$

где a_{ij} - матричные коэффициенты на пересечении i-ой строки и j-го столбца. Аналогично задаём образ второго базиса:

$$b(f_i) = \sum_{k=1}^{p} g_k b_{ki}.$$

Тогда мы можем найти $b \circ a$:

$$(b \circ a)(e_j) = b(\sum_{i=1}^{m} f_i a_{ij}) = \sum_{i=1}^{m} b(f_i) a_{ij} = \sum_{i=1}^{m} \sum_{k=1}^{p} g_k b_{ki} a_{ij}.$$

Конечно, знаки суммирования можно переставить. И что всё это означает? Это означает, что если мы хотим найти матричный коэффициент композиции, то нужно рассмотреть сумму:

$$(b \circ a)_{kj} = \sum_{i=1}^{m} b_{ki} a_{ij}.$$

То есть, количество строк матрицы преобразования a должно совпасть с количеством столбцов матрицы преобразования b.

Отсюда видно, что квадратные матрицы образуют кольцо (причём некоммутативное при размерности большей 1). Сложение в этом кольце определено покоординатно, умножение мы задали, остаётся только проверить свойства, проверяется это покоординатно.

1.23 Элементарные преобразования. Метод Гаусса. Системы линейных уравнений

Предупреждение: в билете происходит словесный понос, так как в начале, по традиции, немного "предыстории", а затем идёт описание сюжета, зачем и почему мы получаем элементарные преобразования и другие объекты, а также, самый сок: метод Гаусса и решение СЛУ. Так что, при ответе на билет можете "выжать" важную информацию отсюда, которая обозначена красными определениями, а также, небольшую часть общего рассуждения.

Для начала рассмотрим *замену базиса*, которую вряд ли можно назвать элементарным преобразованием, но тем не менее. Когда мы совершаем линейное отображение, важно, какой базис мы выбрали, потому что от этого зависит, как будет выглядеть матрица отображения. Однако давайте заметим, что базис можно поменять посредством тождественного преобразования из векторного пространства в себя, которое записывается *квадратной матрицей*, в которой каждый ноэлемент одного базиса расписан через элементы второго. Тогда чтобы найти, как выглядит матрица преобразования в другом базисе, нужно умножить матрицу преобразования базиса на матрицу отображения. Также можно заменить базис получившегося пространства, но по сути, это то же самое, только умножаем мы с другой стороны.

Определение 49. Такая матрица смены базиса называется *матрицей перехода*.

Определение 50. *Ранг* матрицы отображения, конечно, не превосходит длин сторон матрицы (лучше рассматривать всё это в правильных базисах (с единичками)), то есть, $r \leq \min(n, m)$, а если $r = \min(m,n)$, то отображение будет называться отображением *полного ранга*.

Для того, чтобы определить метод Гаусса, обратимся к такой задаче:

Пример(ы) 1. Дана матрица $m \times n$ (m строк, n столбцов), необходимо найти все обратимые матрицы $m \times m$ и $n \times n$ (то есть, такие, что в произведении они дадут следующую матрицу).

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

То есть, она диагональная до какого-то момента, а потом всё - нули (и, конечно, она не обязательно квадратная). В общем и целом, мы сейчас будем искать набор каких-то заведомо обратимых матриц.

Определение 51. *Трансвекция* (или элементарное преобразование первого рода) - квадратная матрица, полученная из единичной путём добавления на ij-ую позицию какого-то элемента ξ, записывается это так: $t_{ij}(\xi)$ - трансвекция.

Следствие 1. Трансвекции обратимы: $t_{ij}(\xi) \times t_{ig}(-\xi) = I$ (кстати, вообще, $t_{ij}(\alpha) \times t_{ig}(\beta) = t_{ig}(\alpha + \beta)$), единичная матрица (кстати, тоже трансвекция, только от нуля).

Следствие 2. Что же вообще они дают?

- Умножение матрицы *слева* на $t_{ij}(\xi)$, прибавляет к i-ой строчке j-ую строчку, домноженную на ξ (слева);
- Умножение матрицы *справа* на $t_{ij}(\xi)$, прибавляет к j-му столбцу i-ый столбец, домноженный на ξ (справа).

Далее для удобства будем рассматривать только умножение слева на произведение трансвекций. И давайте поймём, как можно переставлять строчки в матрице. Если мы хотим переставить строчки i, j, то нужно выполнить умножение на таукю матрицу:

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

Где просто в прямоугольничке, образованном i, j строками и столбцами мы переставили 0 и 1 в углах. Если умножит матрицу на такую слева, то мы как раз переставим i, j - строки (если справа, то, конечно, столбцы). Но такую матрицу получить невозможно. А возможно такую:

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & -1 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix}$$

Но тогду у новой j-ой строчки мы поменяем знак. Делаем мы это при помощи трансвекций таким образом: $(u,v) \to (u+v,v) \to (u+v,-u) \to (v,-u)$, где u,v мы обозначили строчки. Тогда даже можно выразить явную формулу: $t_{ij}(1) \times t_{ij}(-1) \times t_{ij}(1)$.

Определение 52. *Псевдоотражение* ($\mathrm{di}_i(\varepsilon)$) - преобразование (элементарное второго рода), которое представляется в виде матрицы, у которой на пересечении i-ой строки и столбца стоит не 1, а ε. Описывает она домножение строки (или столбца, в зависимости от того, с какой стороны умножаем), на ε. Однако получить её путём умножения трансвекций мы не можем. Также $\varepsilon \in R^\times$, то есть, в поле не равен нулю.

Однако, мы можем при помощи трансвекций получить достаточно похожую матрицу:

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & \varepsilon & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & \varepsilon^{-1} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix}$$

Которая на диагонали содержит взаимно обратную "пару" к элементу, который мы размещаем. Такую матрицу можно получить произведением шести трансвекций, всё это можно проделать на матрицах размерности 2. Тогда при умножении матрицы на данную, мы i-ую строчку умножим на ε, а j-ую на него поделим.

Итого, у нас есть определённый набор операций (которые мы можем получить из произведения трансвекций). Или же, *элементарные преобразования*:

- прибавить к строчке какую-то другую с коэффициентом;
- переставить две строчки (у одной из них изменится знак);
- умножить одну строчку на элемент, но другую на него поделить.

Теперь мы этими операциями будем приводить матрицу *методом Гаусса* (сведение к ступенчатому виду).

Будем приводить матрицу к *эшелонированному виду*. Рекомендуется заглянуть в лекцию №19, потому что всё же, я не нарисую все картинки с доски, а ограничусь только краткими словесными рассуждениями.

Для начала умножаем только слева на трансвекции (работаем только со строками). Рассмотрим первый (слева направо) ненулевой столбец, поменяем строчки местами так, чтобы в первой строке в этом столбце стоял не нуль. Теперь успешно повычитаем первую строку с коэффициентом из остальных так, чтобы уничтожить все остальные ненулевые элементы в первом столбце. Теперь рассмотрим матрицу без первых нулевых и этого столбца, а также верхней строки. Проделаем для неё ту же самую операцию, и так далее много раз. В итоге либо "упрёмся в стенку", либо снизу останутся нулевые строки. Теперь все *ведущие* элементы (которые мы оставляли сверху в столцах, и количество которых, кстати, равно рангу матрицы), поочерёдно будем превращать в единицы, путём деления одного на себя, и умножая на него следующий. Если снизу остались нулевые строки, то в единичку мы можем превратить и последний ведущий элемент, иначе это невозможно.

Теперь вспоминаем, что мы ещё умеем умножать на трансвекции справа, и уничтожим всё в строках, кроме ведущих. И, наконец, переставим их последовательно (у последнего ведущего опять же может остаться знак "-", но с этим ничего не поделаешь, это инвариант матрицы, который называется *определителем*, однако сейчас не об этом). То есть, если матрица не квадратная матрица, то мы всегда можем выстроить по диагонали единицы, а в случае квадратной матрицы, в последней позиции диагонали мы можем получить не 1, а некоторый другой элемент.

Наконец, *системы линейных уравнений* - система вида:

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \cdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \end{cases}$$

Где a_{ij} и b_i - какие-то элементы поля, я x_j - переменные, значения которых мы хотим выяснить.

Скажем, что у нас есть несколько матриц:

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}, x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$$

Они есть $A : F^n \to F^m, x \in F^n, b \in F^m$.

Бывает, конечно, два случая: либо решений нет, либо решение есть. Если решение есть, то мы можем из него получить и все остальные, путём прибавления элементов из ядра A. Но тогда нужно как-то решить уравнение $Ax = 0$, что не сильно-то легче, чем решить изначальное уравнение $Ax = b$. Кстати, здесь можно также заметить, что решение системы существует тогда и только тогда, когда $b \in \operatorname{Im} A$. Теперь в ходе рассуждений можно упомянуть следующую лемму, которой, конечно, в билетах нет:

Лемма 35. *(Размеронсти ядра и образа). Пусть $f : V \to V'$ - линейное отображение векторных пространств. Тогда*

$$\dim V = \dim \operatorname{Im} f + \dim \operatorname{Ker} f$$

А так как ранг есть размерность образа, то $\dim \operatorname{Ker} A = n - \operatorname{rank} A$. Но вообще, это не очень-то и важно, а просто как вспомогательный факт. Нам же нужно научиться понимать, есть ли решения у системы, и, если есть, то как их находить.

Если у нас имеется $Ax = b$, то можно домножить это уравнение на некую квадратную матрицу $P \Rightarrow PAx = Pb$, где P - обратимая матрица, чтобы не потерять никакой информации, то есть, она выражается через трансвекции. Так как мы умножаем слева, то по сути, мы решаем систему "школьным методом" - комбинирование строк. Приводим матрицу к ступенчатому виду, причём лучше сразу привести матрицу к *расширенному виду*, то есть, к матрице A приписать справа столбец b и производить все операции сразу на такой расширенной матрице. Тогда если мы получили, что в части только с A есть нулевые строчки, которые равны каким-то ненулевым значениям в столбце b, то мы получили противоречие, решений нет. Иначе рассмотрим последнюю ненулевую строку, для всех переменных кроме одной выберем произвольные значения (параметры), а последнее будет задано тогда однозначно. И так дальше будем подниматься по строчкам, получим решение всей системы.

Перед тем, как дорешать систему, мы пришли как раз к теореме Кронекера-Капелли, так как как раз количество ведущих элементов равно рангу, и если в матрице A и в матрице расширенной количество ведущих совпадает, то и противоречия с последними ненулевыми строками не будет. Иначе, оно появляется, и только в таком случае система решений не имеет.

1.24 Теорема Кронекера-Капелли

Теорема 20. *(Теорема Кронекера-Капелли). Система линейных уравнений имеет решение тогда и только тогда, когда ранг исходной матрицы равен рангу расширенной матрицы.*

Все рассуждения см. начиная с системы линейных уравнений в предыдущем билете.

1.25 Определение группы. Циклическая группа. Порядок элемента

Определение 53. *Группой* называется множество G, если на нём задана операция $\cdot$ со следующими свойствами:

- ассоциативность;
- существование нейтрального элемента (e);
- существование обратного элемента.

Определение 54. *Подгруппой* H группы G называется её подмножество, замкнутое относительно операции и содержащее нейтральный элемент и обратный для каждого элемента группы.

В любой группе G могут быть определены *степени* элемента g с целыми показателями. Вместе они образуют подгруппу, которая называется *циклической подгруппой*, порождённой элементом g. Обозначается она как $\langle g \rangle$. Возможны два случая при рассмотрении такой группы: либо она бесконечна (такое, конечно, бывает), либо конечна, то есть, существует такие натуральные k,l : $g^k = g^l \Leftrightarrow g^{k-l} = e$. Наименьшее из таких чисел m, что $g^m = e$, называют *порядком* элемента g и обозначают как $\operatorname{ord} g$.

Определение 55. Группа G называется *циклической*, если существует такой элемент $g \in G$, что $G = \langle g \rangle$. Всякий такой элемент называется *порождающим* элементом группы G.

1.26 Группа перестановок. Циклы, транспозиции. Знак перестановки

Любую перестановку π можно явно записать, как биекцию, например:

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \pi(1) & \pi(2) & \cdots & \pi(n) \end{pmatrix}$$

Вообще, можно сказать, что мы рассматриваем множество X, и множество биекций из него самого в себя: $\{\varphi : X \to X | \varphi \text{ - биекция}\} := S_X$. Тогда S_X - группа по композиции с нейтральным элементом - тождественным отображением. Такая группа и называется *группой перестановок* или симметрической группой.

С другой стороны, можно рассмтреть некоторую точку i и её *орбиту* под действием π:

$$(i, \pi(i), \pi(\pi(i)), \dots).$$

Этот путь является циклом, потому что если бы он замкнулся на отличной от i точке j, то у j было бы два прообраза. То есть, всю перестановку можно представить в виде дизъюнктного объединения таких орбит. Если говорить строго, то можно определить отношение эквивалентности и по нему отфакторизовать:

$$i \sim j \Leftrightarrow \exists x \in \mathbb{Z} : \pi^k(i) = j.$$

Определение 56. Пусть π - перестановка. i нахывается *неподвижной точкой* π, если $\pi(i) = i$. Множество всех неподвижных точек обозначается за $\mathrm{Fix}\pi$. Аналогично определяется множество *подвижных точек*: $\mathrm{Mob}\pi$.

Определение 57. Две перестановки *независимы*, если множества их подвижных точек дизъюнктны.

Определение 58. *Транспозиция* - цикл длины 2.

Определение 59. *Фундаментальная транспозиция* - цикл вида $(i, i+1)$ для некоторого i.

Определение 60. Пусть π - перестановка. *Инверсия* - пара (i, j) такая, что $i < j \wedge \pi(i) > \pi(j)$. Число таких пар обозначается за $\mathrm{Inv}\pi$

Лемма 36. *При домножении перестановки π на транспозицию $s_k = (k,k+1)$ количество инверсий меняется на 1: $inv(s_k\pi) = inv(\pi)1$.*

Доказательство. Пусть $i,j \in \{1,\dots,n\}, i < j$. В ходе решения нужно рассмотреть 4 случая:

- $\{\pi(i), \pi(j)\} \cap \{k,k+1\} = \emptyset$. В этом никакие инверсии не появляются и не пропадают, у π и $s_k\pi$ количество инверсий совпадает.
- $i = \pi^{-1}(k), j \neq \pi^{-1}(k+1)$. В этом случае также не появляются и не исчезают никакие перестановки.
- $i = \pi^{-1}(k+1), j \neq \pi^{-1}(k)$. Аналогичен предыдущему.
- Наконец, $\{\pi(i), \pi(j)\} = \{k,k+1\} = \emptyset$. Здесь как раз появляется разница в количестве инверсий. При $i = \pi^{-1}(k), j = \pi^{-1}(k+1)$, то количество инверсий увеличивается на 1, а если наоборот - то уменьшается на 1.

□

Таким образом,

Лемма 37. *При домножении π на транспозицию $\sigma_k = (k, k+1)$, количество инверсий меняется на 1:*

$$inv(s_k\pi) =$$
$$\begin{cases} inv(\pi) + 1, \ \text{если } \pi^{-1}(x) < \pi^{-1}(k+1), \\ inv(\pi) - 1, \ \text{если } \pi^{-1}(x) > \pi^{-1}(k+1). \end{cases}$$

Теорема 21. *Любую перестановку можно представить в виде произведения фундаментальных транспозиций.*

Доказательство. Пусть $\pi \in S_n$. Будем домножать π слева на фундаментальные перестановки так, чтобы $\text{inv}(\pi)$ уменьшалась. В какой-то момент количество инверсий станет равным нулю, значит, перестановка будет тождественной. Получим выражение для исходной перестановки π в виде произведения фундаментальных транспозиций.

Итак, доказываем индукцией по количеству инверсий. База $\text{inv}(\pi) = 0$ - это случай тождественной перестановки, для неё, очевидно, утверждение теоремы выполняется. Далее, пусть имеется перестановка $\pi \in S_n$.Мы хотим найти такую транспозицию s_k, что $\text{inv}(s_k\pi) = \text{inv}(\pi) - 1$. По утверждению предыдущей леммы это то же самое, что найти $k : \pi^{-1}(k) > \pi^{-1}(k+1)$. Если такого k нет, то $\pi^{-1} : \{1, \dots, n\} \to \{1, \dots, n\}$ - биекция, сохраняющая порядок. Такая биекция существует всего одна и это тождественная перстановка. Таким образом, если π не тождественна: то мы нашли требуемое k, тогда

$$s_k\pi = s_{i_1} \cdot \dots \cdot s_{i_m},$$

следовательно,

$$\pi = s_k \cdots s_{i_1} \cdot \dots \cdot s_{i_m}.$$

Что и требовалось. □

Определение 61. *Гомоморфизмом знака* будем называть отображение $\text{sgn} : S_n \to \{1\}$, действующее по правилу $\text{sgn}(\pi) = (-1)^{\text{inv}(\pi)}$.

1.27 Действие группы на множестве. Орбиты. Классы сопряженности

Пусть G - группа, X - множество, $\varphi : G \to S_X$ - гомоморфизм. Чтобы задать этот гомоморфизм, для каждой пары $(g, x), g \in G, x \in X$, нужно определить значение $\varphi(g)(x) \in X$. Обозначим $g \cdot x := \varphi(g)(x)$.

Для новой операции $G \times X \to X, (g, x) \to g \cdot x$, зная, что φ - гомоморфизм, выведем для неё некоторые аксиомы:

- $(gh) \cdot x = g \cdot (hx)$, так как $\varphi(gh)(x) = \varphi(g)\varphi(h)(x)$. $(\forall g, h \in G, x \in X)$,
- $e \cdot x = x$, потому что $\varphi(e)(x) = x$. $(\forall x \in X)$.

Определение 62. Операция $G \times X \to X$, удовлетворяющая аксиомам выше, называется *действием группы на множестве*.

Пример(ы) 1. Приведём несколько примеров действий над группами:

- Группа G действует на множестве G *сдвигами* (такое действие называют регулярным): операция переводит пару $(g, x) \in G^2$ в $g \cdot x$. Посмотрим, как описать это действие на языке гомоморфизмов. Пусть $\varphi : G \to S_g$ - гомоморфизм, который задаёт регулярно едействие на группе. Заметим, что φ - инъекция. Действительно, пусть $g \in \operatorname{Ker}\varphi$. Значит, $\varphi(g)$ - тождественная перестановка G, то есть, $\varphi(g)(h) = g \cdot h = h$ для всех h. В частности, если подставить $h = e$, то получим равенство $g = e$. Получается, ядро тривиально. Из того, что φ - вложение, следует такая теорема:

  Теорема 22. *(Теорема Кэли). Любая конечная группа изоморфна некоторой подгруппе в S_n для $n = |G|$.*

- Группа G действует на себя *сопряжениями*: $(g, h) \mapsto ghg^{-1}$.

Пусть группа G действует на множестве X. Определим на X. Определим на X бинарное отношение, это отношение эквивалентности (нетрудно проверить):

$$x \equiv y, \text{ если } \exists g \in G : y = g \cdot x.$$

Определение 63. Классы эквивалентности отношения $\equiv$ называются *орбитами*.

Определение 64. Если группа G действует на множестве X, и у X всего одна орбита, то такое действуие называют *транзитивным*.

Определение 65. Орбиты относительно действия G на G сопряжением называют *классами сопряжённости*.

1.28 Группа обратимых элементов кольца. Вычисление обратимых элементов $\mathbb{Z}/_{n\mathbb{Z}}$. Функция Эйлера

Определение 66. Множество всех обратимых элементов кольца образует мультипликативную группу, называемую *группой обратимых элементов*. Эта группа всегда непустая, так как содержит, как минимум, единицу. Обозначается $R^\times$.

Пусть R - коммутативное кольцо с 1, $R^\times$ - множество обратимых элементов, тогда $(R^\times, \cdot)$ - абелева группа. Можно проверить, что $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$ - абелева группа порядка $\varphi(n)$, где φ - *функция Эйлера*, сопоставляющая числу n количество взаимно простых с ним среди $\{1, \ldots, n\}$ (то есть, $\varphi(1) = 1$).

По поводу вычисления можно сказать, что их количество мы знаем из функции Эйлера, а также подходят только взаимно простые, так как иначе элемент необратим.

1.29 Гомоморфизмы и изоморфизмы групп. Смежные классы, теорема Лагранжа. Теорема Эйлера

Определение 67. *Гомоморфизм* групп - отображение φ между группами со свойствами:

- $\varphi(ab) = \varphi(a)\varphi(b)$;
- $\varphi(1) = 1$ (не обязательное условие, оно выводится).

А *изоморфизм*, естественно, биективный гомоморфизм.

Лемма 38. $\varphi(a^{-1}) = (\varphi(a))^{-1}$.

Определение 68. Подгруппа $H \leq G$ называется *нормальной*, если

$$\forall h \in H, \forall g \in G : g^{-1}hg \in H.$$

Иначе говоря, нормальные подгруппы - те, которые *устойчивы* относительно сопряжения.

Лемма 39. *Ядро гомоморфизма групп - нормальная подгруппа.*

Доказательство. $\varphi(g^{-1}hg) = (\varphi(g))^{-1}\varphi(h)\varphi(g) = (\varphi(g))^{-1}\varphi(g)$. □

Пусть H - подгруппа G. Введём следующее отношение (эквивалентности, что нетрудно проверить) на G:

$$x \sim y \Leftrightarrow x^{-1}y \in H$$

Иначе говоря, $g_2 = g_1 \cdot h, h \in H$.

Можно видеть, что класс эквивалентности элемента x состоит из произведений вида $hx, g \in H$. То есть, его корректно отображать за Hx. Классы эквивалентности по нашему определению имею специальное название:

Определение 69. Пусть H - подгруппа G, x - элемент G. Множество Hx называется *правым смежным классом* x по подгруппе H. Множество всех правых смежных классов по подгруппе H обозначается за $H\backslash G$, а левых - за G/H.

Лемма 40. *На самом деле, число правых смежных классов по подгруппе равно числу левых смежных классов.*

Определение 70. Пусть H - подгруппа G. *Индексом* G по H называется число смежных классов G по H. Обозначается как $|G : H|$.

Теорема 23. *(Теорема Лагранжа). Пусть H - подгруппа конечной группы G. Тогда $|G| = |G : H| \cdot |H|$.*

Доказательство. Пусть

$$C := \{gH | g \in G\}$$

- множество левых смежных классов по H. Построим явную биекцию между G и $C \times H$. Выберем каждому смежному классу представитель x и отобразим

$$(x, h) \mapsto xh$$

Сюръективность. Если x - представитель смежного класса gH, то $(x, x^{-1}g)$ будет прообразом g.

Инъективность. Если $x_1h_1 = x_2h_2$, то $x_2^{-1}x_1 = h_2h_1^{-1}$. Значит, x_2 и x_1 лежат в одном классе эквивалентности, а у каждого из последних представитель всего один: $x_1 = x_2$. То есть, предпоследнее равенство приводится к виду $1 = h_2h_1^{-1}$. □

Следствие 1. Порядок любой группы делит порядок надгруппы.

Теорема 24. *(Теорема Эйлера). Пусть натуральные числа a и n взаимно просты, то есть,* $\gcd(n,a) = 1$. *Тогжа верно тождество* $a^{\varphi(n)} \equiv 1 \mod n$, *где $\varphi(n)$ - фугкция Эйлера.*

Доказательство. Применим теорема Лагранжа к группе $(\mathbb{Z}/n\mathbb{Z})^\times$. Обозначем её за A. A состоит из вычетов, взаимно простых с n, поэтому $|A| = \varphi(n)$. К тому же, раз a и n взаимно просты, $[a]$ лежит в A. Пусть C - подгруппа, порождённая $[a]$. Как мы уже выяснили ранее, размер C равен порядку $[a]$. Кроме того, из теоремы Лагранжа следует, что $|C||A|$, то есть, $\mathrm{Ord}([a])||A|$. По определению порядка, $[a]^{\mathrm{Ord}(a)} = 1$, значит, $[a]^{|A|} = [a]^{\varphi(n)} = 1$, что и требовалось. □

1.30 Многочлены деления круга

Циклическую группу из n элементов мы обозначаем как C_n.

Определение 71. Если представить C_n как комплексные корни из единицы степени n с произведением, то образующие называются *первообразными* корнями.

Определение 72. Зафиксируем n. *Многочлен деления круга* (*циклотомический* многочлен) - многочлен вида

$$\Phi_n(x) := \Pi_\zeta(x - \zeta),$$

где произведение берётся по первообразным корням из единицы степени n.

Следствие 1. Из 28 билета: $\deg \Phi_n(x) = \varphi(x)$.

Теорема 25.

- $x^n - 1 = \Pi_{d|n}\Phi_d(x)$ *при всех* n.
- *Все* $\Phi_n(x)$ *имеют целые коэффициенты.*
- *Содержание всех* $\Phi_n(x)$ *(как элементов* $\mathbb{Z}[x]$*) равен 1.*

Доказательство. Первый пункт. Если мы покажем, что корни многочленов справа и слева совпадают с точностью до кратности, то равенство будет следовать из совпадения старших коэффициентов. Это и покажем

- Пусть ζ - корень многослена слева. ζ будет порождать циклическую группу порядка $\mathrm{Ord}\zeta$, а по минимальности порядка $\mathrm{Ord}\zeta | n$ (так как $\zeta^n = 1$). Значит, ζ содержится в разложении многочлена справа.
- Пусть ζ - корень многочлена справа. Тогда $\zeta^n = 1$, поскольку, ζ - первообразный корень с порядкам d для некоторого $d|n$.
- При этом, если ζ - корень Φ_d, то ζ не может быть корнем другого циклотомического многочлена $\Phi_{d'}$ с $d \neq d'$, поскольку $\mathrm{Ord}\zeta = d \neq d'$. Таким образом, любой корень правого многочлена имеет кратность 1. То же верно для левого.

Первый пункт доказан.

Индукция по n. База: $\Phi_1 = x - 1$ - многочлен с содержанием 1. Переход: используя предположение индукции, разложим правую часть как $\Phi_n \cdot g$ для некоторого многочлена g с целыми коэффициентами и содержанием 1. Мы в области целостности, поэтому можем сократить обе части на g. При этом справа останется то, что осталось бы при делении $x^n - 1$ на g с остатком в $\mathbb{Q}[x]$ (вспомним определение деления с остатком). А останется, конечно, многочлен с рациональными клэффициентами. С другой стороны, это Φ_n. Поскольку содержание $x^n - 1$ - единица и содержание мультипликативно, содержание Φ_n - тоже единица. Значит, его коэффициенты целые и взаимно просты в совокупности. Что и требовалось. □

Следствие 2.

$$n = \sum_{d|n} \varphi(d).$$

1.31 Конечные поля (существование, единственность, цикличность мультипликативной группы)

1.32 Фактор-группа, теорема о гомоморфизме

1.33 Определитель матрицы. Инвариантность при элементарных преобразованиях, разложение по строчке и столбцу

1.34 Присоединенная матрица. Формула Крамера. Определитель транспонированной матрицы

1.35 Вычисление определителя методом Гаусса

1.36 Принцип продолжения алгебраических тождеств. Определитель произведения матриц

И в заключение...

2 Пофамильный указатель всех мразей

Быстрый список для особо заебавшегося поиска.