Алгебра

Кабашный Иван
(по материалам конспекта старшекурсников,
написанном на основе лекций В. А. Петрова)

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

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

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

Определение 12. Подкольцо I кольца R называется *левым идеалом*, если оно замкнуто относительно домножения 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 $a = bd \in (d)$. $\square$

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 *нетёровым 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 $\subset$ нетёровы 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. $\square$

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. $\square$

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 $\mathrm{Im} = \mathbb{Z}/(m) \times \mathbb{Z}/(n)$. $\square$

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. $\square$

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

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

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

Лемма 8. *$Kerf$ - 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. $\square$

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. $\square$

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. $\square$

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 перемножеются, 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. $(\operatorname{cont} f)(\operatorname{cont} g) \sim \operatorname{cont} fg$.

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 понадобятся.

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 осталость 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, необратим, 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. $\square$

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). $\square$

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). $\square$

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

$\square$

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. $\square$

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, $f \in (x-a)R[x] \Leftrightarrow f(a = 0)$. $\square$

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 $R[x]/(x-a) \cong R[x]/(x) \cong R$. $\square$

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, $\{a_0, \dots, a_n\}$ - набор его различных элементов. Тогда*

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

посредством

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

Доказательство. Докажем, что его ядро есть $((x-a_0)\dots(x-a_{n-1}))$. Спроецируем F^n на F и применим теорему Безу. Условно говоря, f лежит в ядре $\mathrm{ev}_{a_0,\dots,a_{n-1}}$, 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 $(b_0, \dots, b_{n-1})$.

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

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.

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

Доказательство. Опять-таки рассмотрим гомоморфизм $f \mapsto (f + (x-a_0)^{m_0} F[x]), \dots, f + (x-a_n)^{m_n} F[x])$. 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 $R[x]/((x-a)^m) \longleftrightarrow (f(a), f'(a), \dots, f^{(m-1)})$ (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. $\square$

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. $\square$

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

Учимся раскладывать $\frac{f(x)}{g(x)}$, где $g(x) = (x - \alpha_1)^{m_1} \ldots (x - \alpha_k)^{m_k}$, 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

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

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 насловo, 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 $q(x)$,

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

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**

1.20 **Размерность векторного пространства**

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

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

1.23 **Элементарные преобразования. Метод Гаусса. Системы линейных уравнений**

1.24 **Теорема Кронекера-Капелли**

1.25 **Определение группы. Циклическая группа. Порядок элемента**

1.26 **Группа перестановок. Циклы, транспозиции. Знак перестановки**

1.27 **Действие группы на множестве. Орбиты. Классы сопряженности**

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

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

1.30 **Многочлены деления круга**

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.