Algebruh 2

Содержание

1 Лекция 1

1.1 Формальные степенные ряды

Definition 1.1. Кольцо формальных степенных рядов

Пусть R - коммутативное кольцо, тогда кольцом формальных степенных рядов $R[[x]]$ называется множество отображений $f : \mathbb{Z}_{\geq 0} \to R$ (f по факту является последовательностью $(a_0, a_1, \dots)$) со следующими операциями:

- сложение: $(a_i)_{i=0}^{\infty} + (b_i)_{i=0}^{\infty} = (a_i + b_i)_{i=0}^{\infty}$
- умножение(свертка):

$$(a_i)_{i=0}^{\infty} * (b_i)_{i=0}^{\infty} = (c_i)_{i=0}^{\infty}, \text{ где } c_i = \sum_{j=0}^{i} a_j * b_{i-j}$$

Правила неформально представляют собой обычное умножение и сложение многочленов, привычных нам.

Theorem 1.1.

Это действительно кольцо(коммутативное, ассоциативное, с 1 если таковым было R)

Доказательство. Для сложения все наследуется из R, так как оно действует покоординатно. Нулем будет $(0)_{i=0}^{\infty}$, обратный к $(a_i)_{i=0}^{\infty}$ это $(-a_i)_{i=0}^{\infty}$.

Пусть R содержит единицу, тогда единицей в $R[[x]]$ будет $(1, 0, 0, \dots)$.

Дистрибутивность — упр...

Коммутативность умножения

$$c_i = \sum_{j=0}^{i} a_j * b_{i-j} = \sum_{j+k=i} a_j * b_k = \sum_{j=0}^{i} b_j * a_{i-j}$$

Получили в конце формулу свертки для $(b)_{i=0}^{\infty}(a)_{i=0}^{\infty}$

Ассоциативность: $\forall f, g, h \in R[[x]](f \cdot g) \cdot h = f \cdot (g \cdot h)$. Введем много обозначений: $f = (a_n), g = (b_n), h = (c_n), f \cdot g = (d_n), g \cdot h = (e_n), (f \cdot g) \cdot h = (k_n), f \cdot (g \cdot h) = (l_n)$

Хотим доказать, что $k_n = l_n \ \forall n \in \mathbb{Z}_{\geq 0}$. Тогда

$$k_n = \sum_{i=0}^{n} d_i c_{n-i} = \sum_{i=0}^{n} (\sum_{j=0}^{i} a_j b_{i-j}) c_{n-i}.$$

Воспользуемся дистрибутивностью:

$$k_n = \dots = \sum_{\substack{0 \leq i \leq n \\ 0 \leq j \leq i}} a_j b_{i-j} c_{n-i}.$$

Определим $s \coloneqq i - j, t \coloneqq n - i$, тогда

$$k_n = \dots = \sum_{\substack{j,s,t \geq 0 \\ j+s+t=n}} a_j b_s c_t..$$

Аналогично для l_n:

$$l_n = \ldots = \sum_{\substack{j,s,t\geq 0 \\ j+s+t=n}} a_j b_s c_k..$$

□

Lemma 1.1.

Отображение $i : R \to R[[x]]$ т.ч. $x \mapsto (x, 0, 0, \ldots)$ это инъективный гомоморфизм колец.

Доказательство. Инъективность очевидна. Единица переностися очевидно.

$$(x + y, 0, 0, \ldots) = i(x + y) = i(x) + i(y) = (x, 0, 0, \ldots) + (y, 0, 0, \ldots)$$

$$i(xy) = (xy, 0, 0, \ldots) = (x, 0, 0, \ldots) * (y, 0, 0, \ldots)$$

□

Далее будем отождествлять R с $i(R)$.
Положим по определению $x = (0, 1, 0, 0, \ldots)$.

Lemma 1.2.

$x^n = (0, 0, \ldots, 1, 0, \ldots)$, где 1 стоит на n-м месте.

Доказательство. Индукция по n. База $n = 1$.
По правилу свертки $x^k * x = (c_i)_{i=0}^{\infty}$. $c_i = 1$ при $i = k + 1$, иначе 0. □

Corollary. *Пусть* $k \in \mathbb{N}$ *и* $a_0, a_1, \ldots, a_k \in R$.
Тогда $a_0 + a_1 x + a_2 x^2 + \ldots, a_k x^k = (a_0, a_1, a_2, \ldots, a_k, 0, 0)$

Произвольную последовательность $(a_i)_{i=0}^{\infty}$ будем также обозначать $\sum_{i=0}^{\infty} a_i x^i$.

Theorem 1.2.

Пусть K-поле и $f \in K[[x]]$. Тогда f-обратим $\iff$ $a_0 \neq 0$.

Example. $\frac{1}{1+x} = 1 - x + x^2 - x^3 + \ldots$.

Доказательство. Пусть $f \in K[[x]]$. Ищем $\frac{1}{f} = b_0 + b_1 x + b_2 x^2 + \ldots$. Отсюда получим:

$$1 = a_0 * b_0 \text{ , } b_0 \text{ существует, так как } a_0 \neq 0$$
$$0 = a_0 * b_1 + a_1 * b_0 \text{ выражаем } b_1$$
$$\vdots$$
$$0 = a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0 \Rightarrow b_n = -\frac{1}{a_0} \sum_{i=1}^{n} a_i b_{n-i}$$

Так найдем все коэффициенты. □

Corollary. *Любой $f \in K[[x]]$ представим в виде $x^n(a_0 + a_1 x \dots)$.*
Отсюда x – единственное простое

Definition 1.2. Кольцо многочленов

Кольцо многочленов $R[x]$ является подкольцом $R[[x]]$ которое равно

$$\{(a_i)\ R[[x]] \mid \exists N : \forall n \geq N\ : a_n = 0\}$$

Доказательство. Докажем, что это подкольцо.
0,1 очевидно лежат в нем.
Замкнутость по сложению: $a_n = 0, n \geq N_1, b_n = 0, n \geq N_2$, значит $a_n + b_n = 0, n \geq \max(N_1, N_2)$.
Замкнутость по умножению: $c_n = 0,\ n \geq N_1 + N_2$. □

Другими словами, $R[x]$ – множество конечных сумм вида $a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$.

Definition 1.3. Степень многочлена

$\deg(f) = \operatorname{argmax}_k\{a_k \neq 0\}$ и $\deg(0) = -\infty$.

Lemma 1.3.

$\deg(fg) \leq \deg(f) + \deg(g)$. $=$ только в области целостности
$\deg(f + g) = \max(\deg(f), \deg(g))$, если $\deg(f) \neq \deg(g)$.
$\deg(f + g) \leq \max(\deg(f), \deg(g))$ всегда

Remark. $\max(a, -\infty) = a$
$a + -\infty = -\infty$

Theorem 1.3. Универсальное свойство кольца многочленов

Пусть R коммутативное, ассоциативное кольцо, $a \in R$. Тогда $\exists!$ гомоморфизм(эвалюация) колец $ev_a : R[x] \to R$ такой, что $ev_a(r) = r\ \forall r \in R$ и 0, если $deg(f) = -\infty$

Доказательство. $ev(a_0 + a_1 x + \dots + a_n x^n) = a_0 + a_1 * a + \dots + a_n * a^n$. □

Definition 1.4.

Зафиксируем $f \in R[x]$. $F_f : R \to R$ т.ч. $a \mapsto ev_a(f)$.
F – полиномиальная функция.

Далее будем обозначать $F_f(a) = f(a)$.

Definition 1.5.

Пусть $f \in R[x]$, $a \in R$. a-корень f, если $f(a) = 0$

Theorem 1.4.

Пусть $f, g \in K[x]$, $g \neq 0$, K-поле, тогда $\exists! r, q \in K[x]$ т.ч. $f = q * g + r$ и $\deg(r) < \deg(g)$.

Доказательство. Единственность: Пусть $f = q_1 g + r_1 = q_2 g + r_2$. Тогда $g(q_1 - q_2) = r_2 - r_1$.
Пусть $q_1 \neq q_2 \Rightarrow deg(g * (q_1 - q_2)) \geq deg(g)$, а $\deg(r_1 - r_2) \leq \max(\deg(r_1), \deg(r_2)) < \deg(g)$. Противоречие..

Существование: Фиксируем g. Индукция по $\deg(f) = n$.

База: $n = 1 \dots \deg(g) - 1$. В этом случае $f = 0 * g + f$.

Переход: $n \to n + 1$.

Пусть $\deg(f) = n + 1 \geq m = \deg(g)$. Перепишем $f = ax^{n+1} + \widehat{f}$ и $g = b * x^m + \widehat{g}$, где $\deg(\widehat{f}) \leq n, \deg(\widehat{g}) < m$.

Рассмотрим $f_0 = f - \frac{a}{b}x^{n+1-m} * g = \widehat{f} - \frac{a}{b}x^{n+1-m}\widehat{g}$. При этом $\deg(f_0) \leq \max(\deg(\widehat{f}), \deg(\frac{a}{b}x^{n+1-m}\widehat{g})) \leq \max(n, n + 1 - m + m - 1) = n$.

Значит по индукционному предположению $f_0 = q * g + r$ и $\deg(r) < \deg(g)$. Тогда $f = g(q + \frac{a}{b}x^{n+1-m}) + r$. □

Corollary. *Частный случай: теорема Безу.*

Остаток деления f на $x - a$ это $f(a)$.

Доказательство. $f = q(x - a) + r$, $\deg(r) < 1$. То есть r–константа.

Применив гомоморфизм эвалюации в точке a получим $f(a) = r$ □

Corollary. *Если $\deg(f) = n$ и $f \neq 0$, то у него не более n корней в поле.*

Доказательство. Индукция по n.

База: n = 0, тогда $f = r \in K$ имеет 0 корней.

Переход: Рассмотрим $\deg(f) = n + 1$. Если нет корней, то все выполнено.

Пусть есть корень a. Тогда $f = (x - a) * \widehat{f} \Rightarrow \deg(f) = \deg(\widehat{f}) + 1$. По индукции $\widehat{f}$ имеет не более чем n корней.

$f(b) = 0 \underset{\text{Потому что мы в поле}}{\iff} (b - a) * \widehat{f(b)} = 0$. Значит либо $b = a$ либо b корень $\widehat{f}$. Итого у f не более $n + 1$ корня □

2 Лекция 2

Example 2.1.

Для не поля неверно
Пусть $K = \mathbb{Z}/8\mathbb{Z}$. $f = x^2 - 1 = (x - 1)(x + 1)$. При этом у f есть корни ± 1,3,5,7.

Remark. *Если $f \in K[x]$ и $a_1, \dots, a_n$ его различные корни, то $f = (x - a_1) \dots (x - a_n)g$.*

Theorem 2.1. О формальном и функциональном равенстве

1. Пусть f, g многочлены над полем, степени $\leq n$. Тогда, если для различных $x_1, x_2, \dots, x_{n+1} \in K$ и $f(x_i) = g(x_i)$, то $f = g$.
2. Если K бесконечное поле, f, g такие, что $f(a) = g(a)\ \forall a \in K$, то $f = g$.

Доказательство. 1) Пусть $h = f - g$. Тогда $\deg(h) \leq \max(\deg(f), \deg(g)) \leq n$. При этом у него $n + 1$ различный корень. Тогда $h = 0 = f - g$.

2) Пусть $f - g \neq 0$, тогда есть $k = \deg(f - g)$. Выберем $k + 1$ элемент поля k и получим искомое. □

Example 2.2.

Пусть $K = \mathbb{Z}/p\mathbb{Z}$. $f = x^p, g = x$. Тогда $\forall a \ : f(a) = g(a)$.
Как функции равны, но формально нет.

2.1 Интерполяция

Интерполяционная задача: K - поле. Заданы $x_1, \ldots, x_n \in K$ –различные узлы интерполяции. И заданы $y_1, \ldots, y_n \in K$.

Задача: найти многочлен над K такой что $f(x_i) = y_i$.

Theorem 2.2.

1. Для любой задачи $\exists!\ f_0 \in K[x]$ – решение и $\deg(f_0) < n$.
2. Множество всех решений имеет вид $A = \{f_0 + (x - x_1) \ldots (x - x_n) * g\}$.

Доказательство.

1. Если f_0 решение $f \in A$, то $f_0(x_i) = f(x_i)$, тогда f тоже решение.
   С другой стороны, если f - решешение. Тогда $f(x_i) = y_i = f_0(x_i)$, тогда $f - f_0 = (x - x_1)(x - x_2) \ldots (x - x_n)\widehat{f}$.
2. Единственность: Пусть f_0, f_1 решение и $\deg(f_0, f_1) < n$. Тогда $f_0 - f_1$ имеет n корней, значит они равны.
   Существование: Рассмотрим вспомогательную задачу L_i: $x_j = 0$, $x_i = 1$.
   Решение вспомогательной задачи: $\frac{(x-x_1)\ldots(x-x_{i-1})(x-x_{i+1})\ldots(x-x_n)}{(x_i-x_1)\ldots(x_i-x_{i-1})(x_i-x_{i+1})\ldots(x_i-x_n)} = \prod_{j\neq i} \frac{x-x_j}{x_i-x_j}$.
   Построим $f_0 = y_1L_1 + \cdots + y_nL_n$. Тогда $L_i(x_j) = \delta_{i,j} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$. $f(x_i) = y_i$, $L_i(x_i) = y_i$.
   При этом $\deg(f_0) \leq \max(\deg(L_i)) \leq n - 1$.
   $f_0 = \sum_i y_i \prod_{j\neq i} \frac{x-x_j}{x_i-x_j}$ – интерполяционная формула Лагранжа.

□

Remark. *Мы решили задачу* $f(x_i) = y_i \iff f \equiv 0 \mod (x - x_i)$

2.2 Цикличность $(\mathbb{Z}/p\mathbb{Z})^*$

Theorem 2.3. Первообразный корень

$(\mathbb{Z}/p\mathbb{Z})^*$ - циклическая

Доказательство. Надо доказать, что существует $a \in (\mathbb{Z}/p\mathbb{Z})^*$, порядок которого равен $p-1$.

Lemma 2.1.

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

Доказательство. Пронумеруем делители n.

Пусть $A = \{1, 2, \dots, n\}$. Пусть $A_i = \{a \in A \,|(a, n) = d_i\}$. Тогда $n = |A| = |\cup A_i| = \sum |A_i|$.

$$|A_i| = |\{d_i b \in A \mid (d_i b, d_i \frac{n}{d_i}) = d_i\}|$$

$d_i b \in A \iff b = 1, \dots, \frac{n}{d_i}$. То есть $|A_i| = |\{b = 1, \dots, \frac{n}{d_i} \,|(b, \frac{n}{d_i} = 1)\}| = \varphi(\frac{n}{d_i})$.
То есть $n = \sum_{d|n} \varphi(\frac{n}{d}) = \sum_{d|n} \varphi(d)$ □

Lemma 2.2.

Пусть $d \mid p - 1$. Тогда в $(\mathbb{Z}/p\mathbb{Z})^*$ есть либо 0, либо $\varphi(d)$ элементов порядка d.

Доказательство. Пусть есть a: $ord(a) = d$. Значит есть $|\langle a \rangle| = d$ различных решений уравнения $x^d = 1$. И других у него нет(т.к. степень d). То есть все решения это a^i, где $i = 0 \dots, d-1$.
$\{x \,: ord(x) = d\} = \{a^i | i = 0 \dots d - 1, ord(a^i) = d\} = \{a^i | a^{ik} \neq 1, \forall k < d\} = \{i \,: \forall k \; d \nmid ik\} = \varphi(d)$. □

Вернемся к доказательству теоремы:
$\{1, \dots, p-1\} = \cup_{d|p-1} B_d$, где B_d это элементы порядка d.
Знаем, что $\sum_{d|p-1} \varphi(d) = p - 1 = \sum_{d|p-1} |B_d| = \sum_{d|p-1} \varepsilon(d)$, где $\varepsilon(d) = 0$ или $\varphi(d)$. То есть нулей нет, значит есть $\varphi(d)$ элементов порядка d. То есть и порядка $p - 1$. □

2.3 Делимость в кольцах

Пусть R кольцо. $b|a (a \vdots b) \iff \exists\, c \,:\, a = bc$.

Definition 2.1. Область целостность

R – область целостности если есть коммутативность(для делимости с обеих сторон) и отсутствуют делители нуля(для единственности).

Definition 2.2. Евклидово кольцо

R – область целостности называется Евклидовым кольцом, если $\exists\; \varphi : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ т.ч. $\forall a, b \in R, b \neq 0 \,:\, \exists q, r \,: a = bq + r \; \varphi(r) < \varphi(b) \vee r = 0$.

Example 2.3.

1. $R = \mathbb{Z}$, тогда $\varphi(a) = |a|$
2. $R = K[x]$, тогда $\varphi(f) = \deg(f)$
3. R - поле, тогда все делится на все и φ любая

Remark. *Мы не требуем единственности разложения!*

Definition 2.3.

Идеал $I \in R$ если
1. $I \neq 0$
2. $a, b \in I \Rightarrow a + b \in I$
3. $a, b \in I \Rightarrow a - b \in I$

Definition 2.4.

I – главный, если $I = \langle a \rangle = \{ax | x \in R\}$

Definition 2.5.

Кольцо главных идеалов, если любой идеал главный

Theorem 2.4.

Евклидово кольцо – кольцо главных идеалов

Example 2.4. Не кольца главных идеалов

$Z[x]$, $K[x, y]$
$K[x, y]$ рассмотрим идеал $\{f | f(0, 0) = 0\} = \langle x, y \rangle$ не главный. Если главный, то $x, y | d \Rightarrow d = 1$, но $1 \notin$

3 Лекция 3

3.1 Евклидовы кольца

Theorem 3.1.

Евклидово кольцо является областью главных идеалов

Доказательство. Пусть I - идеал в R. Либо $I = \{0\} = \langle 0 \rangle$ - главный. Либо $I \neq \{0\}$. Тогда рассмотрим $\varphi(I) = \{\varphi(x) \mid x \in I\} \subset \mathbb{Z}_{\geq 0}$. Значит в $\varphi(I)$ существует минимальный элемент $\varphi(x)$.

Докажем, что $I = \langle x \rangle$. Раз $x \in I$, то и $\langle x \rangle \subset I$ по определению.

Возьмем $y \in I$. $y = qx + r$. При этом $\varphi(r) < \varphi(x)$, но $r = y - qx \in I$ и $\varphi(x)$ - минимальный, значит $r = 0$. Значит $y \in \langle x \rangle \Rightarrow I \subset \langle x \rangle$ □

Definition 3.1.

Пусть R - область целостности, $a, b \in \mathbb{R}$. a ассоциирован с b ($a \sim b$), если выполнено одно из равносильных утверждений

1. $\langle a \rangle = \langle b \rangle$
2. {делители a} = {делители b}
3. $a \vdots b \wedge b \vdots a$
4. $a = \varepsilon b$, $\varepsilon \in R^*$

Доказательство. Доказательство равносильности утверждений:

$1 \Rightarrow 3$: $a \in \langle b \rangle \Rightarrow b \vdots a$. Аналогично $a \vdots b$.

$3 \Rightarrow 2$: $b \vdots c,\ a \vdots b \Rightarrow a \vdots c$. Аналогично наоборот.

$3 \Rightarrow 1$ и $2 \Rightarrow 3$ аналогично

$4 \Rightarrow 3$:

$a = \varepsilon b$, $\varepsilon \in R^*$, тогда $\exists \varepsilon^* : \varepsilon\varepsilon^* = 1$. Значит $b = \varepsilon^* a$ т.е. $b \vdots a$.

$3 \Rightarrow 4$: $a = bc \wedge b = ac^* \Rightarrow a = ac^*c \Rightarrow 1 = cc^*$ т.е. $c \in R^*$. □

Lemma 3.1.

$\sim$ отношение эквивалентности

Example 3.1.

$R = \mathbb{Z}$. $a \sim b \iff a = \pm b$.

Definition 3.2.

R - область целостности, $a \in \mathbb{R}$. a называется неприводимым(неразложимым), если $a \notin R^* \wedge a \neq 0$ и если $a = bc \Rightarrow b \in R^* \vee c \in R^*$

Definition 3.3. НОД

R - область целостности, $a, b \in R$, $d = (a, b) \iff \begin{cases} a \vdots d, b \vdots d \\ a \vdots d', b \vdots d' \Rightarrow d \vdots d' \end{cases}$

Remark. *Пусть $d_1, d_2 = (a, b)$, тогда $d_1 \vdots d_2 \wedge d_2 \vdots d_1 \Rightarrow d_1 \sim d_2$.*
То есть НОД определен с точностью до ассоциированности

Theorem 3.2.

Если R - ОГИ, то $\forall a, b\, \exists (a, b) \wedge\ \exists x, y : d = ax + by$

Corollary. $ab \vdots c \wedge (a, c) = 1 \Rightarrow b \vdots c$

Definition 3.4.

R - область целостности, $a \in R$, тогда a называется простым, если $a \neq 0, a \notin R^*$ и $\forall b, c \in R\, bc \vdots a \Rightarrow b \vdots a \vee c \vdots a$

Theorem 3.3.

R - область целостности, тогда p - простой $\Rightarrow$ неприводим
R - ОГИ, тогда p - неприводим $\Rightarrow$ простой

Доказательство. 1. p - простой $\Rightarrow p \notin R^*$. Пусть $p = ab \Rightarrow ab \vdots p \Rightarrow a \vdots p \vee b \vdots p$

Не умаляя общности $a \vdots p$, но из равенства $p \vdots a \Rightarrow p \sim a \Rightarrow b \in R^*$.

2. Пусть p неприводим и $bc \vdots p$. Рассмотрим $(b,p) = d$. $p \vdots d \Rightarrow d \sim p \vee d \sim 1$. Если $d \sim 1$, то $(p,b) = 1 \Rightarrow c \vdots p$. А если $d \sim p$, то $b \vdots d \Rightarrow b \vdots p$.

□

Theorem 3.4. Основная теорема арифметики

Пусть R - ОГИ, тогда $\forall a \in R \setminus \{0\}$ единственным с точностью до ассоциированности и порядка образом представляется в виде $p_1 \dots p_n$, где p_i неприводимы.

Доказательство. Единственность: пусть $p_1 \dots p_n = q_1 \dots q_m$. Все неприводимы.

Тогда $p_1 \dots p_n \vdots q_1 \Rightarrow p_1 \vdots q_1 \vee p_2 \dots p_n \vdots q_1 \Rightarrow p_1 \vdots q_1 \vee p_2 \vdots q_1 \vee \dots \vee p_n \vdots q_n$. Значит $\exists i \ : p_i \vdots q_1$. Т.к. p_i неприводим, то $q_1 \sim 1 \vee q_1 \sim p_1$, но первый вариант невозможен т.к. q_1 тоже неприводим. Значит $q_1 = p_i\varepsilon$, где $\varepsilon \in R^*$.

Получили $p_1 \dots p_n = \varepsilon p_i q_2 \dots q_m$. Сократим на p_i и применим индукцию! Получим искомое.

Существование:

Lemma 3.2.

Если R - ОГИ, $a_1, a_2, \dots \in R$ и $a_i \vdots a_{i+1}$. Тогда существует $N : \forall n > N \ a_n \sim a_{n+1}$.

Доказательство. $a \vdots b \iff \langle a \rangle \subseteq \langle b \rangle$. Значит имеем $\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \dots$

Пусть $I = \bigcup \langle a_i \rangle$. I - идеал.

$a, b \in I \Rightarrow \exists m, n \ a \in \langle a_m \rangle, \ b \in \langle a_n \rangle \Rightarrow a, b \in \langle a_{\max(n,m)} \rangle \Rightarrow a + b \in I$

Умножение аналогично.

Раз идеал и мы в ОГИ, тогда $I = \langle x \rangle$. Значит $x \in \bigcup \langle a_i \rangle \Rightarrow x \in \langle a_j \rangle$.

$x \vdots a_j \Rightarrow x \vdots a_{j+1}$ и так далее. Но $a_j, a_{j+1} \in \langle x \rangle \Rightarrow a_j \vdots x \wedge a_{j+1} \vdots x$.

Получили, что $\forall m, n > j \ a_n \sim x \sim a_m \Rightarrow a_n \sim a_m$. □

Lemma 3.3.

$a \in R$, $a \notin R^* \Rightarrow \exists p$ - неприводимый, такой что $a \vdots p$.

Доказательство. Если a неприводим, то $p = a$.

Пусть a разложим, $a = x_1 x_2$, $x_i \notin R^*$. Либо x_i неразложим, либо $x_i = x_1' x_2'$. Получаем цепочку $a \vdots x_1 \vdots x_1' \vdots \dots$. По лемме цепочка оборвется, значит $\exists i \ x_i$ неразложим! □

Вернемся к существованию.

$a \in R$. По 2 лемме $a = p_1 p_2$, причем p_1 неприводим. Если p_2 не неприводим, то продолжаем процесс выделения неприводимых. Он не может продолжаться бесконечно, иначе опять появится бесконечная цепочка. Значит в какой-то момент получим $a = p_1 p_2 \dots p_k \varepsilon$. □

Example 3.2.

Пусть $R = K[x]$. $K[x]$ - евклидово $\Rightarrow$ ОГИ. Что такое $(K[x])^*$?

Lemma 3.4.

$(K[x])^* = K^*$

Доказательство. $a \in K^* \Rightarrow a \in (K[x])^*$ очевидно.
$f \in (K[x])^* \Rightarrow f\tilde{f} = 1 \Rightarrow \deg(f\tilde{f}) = 0$. При этом $\deg(f) + \deg(\tilde{f}) = 0 \Rightarrow \deg(f) = 0 \Rightarrow f \in K^*$ □

Definition 3.5.

Область целостности, в котором выполняется ОТА называется факториальным кольцом

Remark. *Можно доказать, что если R - факториально, то $R[x]$ факториально. То есть $(K[x])[y] = K[x, y]$ факториально, хоть и не удовлетворяет ОГИ*
Заметим, что $\forall f \in K[x] \setminus \{0\}$ и $\exists! f_0$, $f \sim f_0$ при этом f_0 уникальный. $f_0 = x^n + \tilde{f}_0$, где $deg(\tilde{f}_n < n)$.

Theorem 3.5. ОТА для $K[x]$

$\forall f \in K[x] \setminus \{0\}$ представим в виде $f = \varepsilon f_1 \dots f_n$, где $\varepsilon \in K^*$, f_i неприводимы. И такое представление единственно с точностью до перестановки

3.2 Производная

Definition 3.6.

Производная $f \in K[x]$ называется многочлен $f'(x) = \frac{f(x)-f(y)}{x-y}|_{y=x}$

Lemma 3.5. Свойства производной

1. $(x^n)' = nx^{n-1}$
2. $(f + g)' = f(x)' + g(x)'$
3. $(fg)' = f'g + fg'$
4. $k \in K$, $(kf)' = kf'$

Доказательство. 1. $\frac{x^n-y^n}{x-y} = x^{n-1} + x^{n-2}y + \dots y^{n-1}|_{y=x} = nx^{n-1}$

2.
$$(f+g)' = \frac{f(x) - f(y) + g(x) - g(y)}{x-y}|_{y=x} = \frac{f(x) - f(y)}{x-y} + \frac{g(x) - g(y)}{x-y} = f' + g'$$

3.
$$(fg)' = \frac{f(x)g(x) - f(y)g(y)}{x-y} = \frac{f(x)g(x) - f(y)g(x) + f(y)g(x) - f(y)g(y)}{x-y} = f'g + fg'$$

□

Corollary. $f = a_0 + a_1 x + \cdots + a_n x^n \Rightarrow f' = a_1 + 2a_2 x + \ldots n a_n x^{n-1}$

Definition 3.7. Кратный корень

$f \in K[x]$, $f \neq 0$. $a \in K$, $f(a) = 0$. a - корень кратности m, если $f \vdots (x-a)^m$ и $f \not\vdots (x-a)^{m+1}$
$m = v_{(x-a)}(f)$.

Definition 3.8. Характеристика

K - поле. K называется полем характеристики 0, если $1 + 1 + \cdots + 1 \neq 0$ в K.
Если $\exists\, p : \underbrace{1 + 1 + \cdots + 1}_{p} = 0$ и p минимальное такое, то $p = charK$ - характеристика.

Lemma 3.6.

$charK = 0$ или простое

Доказательство. Пусть $charK = mn$. Значит

$$\underbrace{1 + 1 + \cdots + 1}_{mn} = (\underbrace{1 + 1 + \cdots + 1}_{m})(\underbrace{1 + 1 + \cdots + 1}_{n}) = 0$$

Так как в поле нет делителей нуля, значит одна из скобочек 0, значит mn не минимальное. □

Theorem 3.6.

$f \in K[x]$. a - корень кратности $m \geq 1$. Тогда
1. a - корень f' кратности $\geq m - 1$
2. Если $charK = 0$, то a корень f' кратности $m - 1$
3. a корень f кратности 1, тогда a не корень f'

Доказательство.

$$f = (x-a)^m g,\ g \not\vdots (x-a)$$
$$f' = m(x-a)^{m-1} g + (x-a)^m g' = (x-a)^{m-1}(mg + (x-a)g')$$
$$\text{При этом } (mg + (x-a)g') \not\vdots (x-a)$$

□

4 Лекция 4

Если $charK = 0$, то $\exists q^{-1} \forall q \in Z$, значит и инъективный гомоморфизм полей $\mathbb{Q} \to K$, $\frac{p}{q} \mapsto (\underbrace{1 + \cdots + 1}_{p}) * (\underbrace{1 + \cdots + 1}_{q})^{-1}$.

Если $charK = p$, то K содержит $\mathbb{Z}/p\mathbb{Z}$.

4.1 Формула Тейлора

Theorem 4.1. Формула Тейлора

Пусть $f \in K[x], a \in K$, $deg(f) = n$ и $n < charK \vee charK = 0$, тогда

$$f = \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(x-a)^k$$

Считаем $(x-a)^0 = 1, f^{(0)} = f, f^{(k+1)} = (f^{(k)})'$

Remark. *$n < charK$, значит $\frac{1}{k!}$ корректно определена для $k \leq n$.*

Доказательство. Индукция по n. База $n = 0$, тогда $f = k \in K = \frac{f^{(0)}(a)}{0!}(x-a)^0 = k$
Переход:
$deg(f) = n \Rightarrow deg(f') = n-1$ т.к. $charK \nmid n$. По индукции $f' = \sum_{k=0}^{n-1} \frac{f'^{(k)}(a)}{k!}(x-a)^k$.
$\widehat{f} = \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(x-a)^k$.

$$(\widehat{f})' = \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}k(x-a)^{k-1} = \sum_{k=1}^{n} \frac{f'^{(k-1)}(a)}{(k-1)!}(x-a)^{k-1} =$$
$$= \sum_{k=0}^{n-1} \frac{f'^{(k)}(a)}{k!}(x-a)^k = f'$$

Итак, $\widehat{f'} = f' \Rightarrow (\widehat{f} - f)' = 0 \Rightarrow_{charK \text{хорошая}} \widehat{f} = f + c$
Применим гомоморфизм эвалюации в точке a: $\widehat{f}(a) = f(a) = f(a) + c \Rightarrow c = 0$. □

Remark. *Легко видеть, что для любого поля K и любого f $\exists a_k \in K : f = \sum a_k(x-a)^k$ (a_0 - остаток от деления на $x-a$ и т.д. или делаем замену $y - a = x$ и подставляем в многочлен).*

4.2 Многочлены и кольца вычетов

Definition 4.1.

Пусть K - поле, $f \in K[x]$
$f \equiv_h g \iff f - g \vdots h$

Definition 4.2.

I - идеал в кольце R
$f \equiv_I g \iff f - g \in I$

Lemma 4.1.

1. $\equiv_h$ – отношение эквивалентности
2. $\widehat{f} + / * \widehat{g} = \widehat{f + / * g}$ корректно задают структуру коммутативного кольца на $K[x]/\equiv_h$
3. h – неразложим $\iff$ $K[x]/(h)$ - поле

Доказательство. Первые два пункта аналогично как в целых числах.

$\widehat{g} = 0 \iff g \vdots h$. Если h неразложим, значит $\forall f : f \vdots h \vee (f,h) = 1 \iff \widehat{f} = 0 \vee \exists v : fv \equiv 1$
h – разложим, тогда есть делители нуля, значит точно не поле $\square$

Пусть $h = \sum a_k x^k, a_k \in K$. Предположим, что h неразложим и $deg(h) > 1$ (у h нет корней в K).

Замечание: есть инъективный гомоморфизм $K \to K[x]/h$, позволяющий говорить про элементы K как элементы $K[x]$. Поэтому

$$h(\widehat{x}) = a_0 + a_1\widehat{x} + \cdots + a_n(\widehat{x})^n = \widehat{h(x)} = 0$$

То есть в $K[x]/(h)$ у h есть корень $\widehat{x}$.

Example. *$h = x - a$, тогда $f = f(a) + h(x-a) \Rightarrow \widehat{f} = f(a)$. То есть $K[x]/(x-a) \cong K$.*

Example. *$h = x^2 - 1$. Рассмотрим $\mathbb{Q}[x]/(x^2-1) = \mathbb{Q}[x]/(x-1)(x+1) \cong \mathbb{Q}[x]/(x-1) \times Q[x]/(x+1) \cong Q \times Q$ - не поле*

Example. *$h = x^2 + 1$, $K = \mathbb{R}$. Получаем $\mathbb{R}[x]/(x^2+1) := \mathbb{C}$ - поле комплексных чисел.*

4.3 Простейшие свойства комплексных чисел

Пусть $\widehat{f} \in \mathbb{C} = \mathbb{R}[x]/(x^2+1)$, тогда $f = (x^2+1)q + h$, где $deg(h) < 2 \iff h = a + b * x$.
$\widehat{f} = \widehat{a + b * x} = a + b\widehat{x}$ и все они попарно различны.
Итого $\mathbb{C} = \{a + b\widehat{x} \mid a, b \in \mathbb{R}\} = \{a + bi | a, b \in \mathbb{R}\}$ - поле.
Обозначим $\widehat{x} = i$, тогда $i^2 = \widehat{x}^2 = -1$.

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$
$$(a + bi) * (c + di) = (ac - bd) + (bc + ad)i$$

$z = a + bi$ – алгебраическая форма записи комплексного числа, $a = Re(z), b = Im(z)$. Обратный элемент:

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

Definition 4.3.

Пусть $z = a + bi \in \mathbb{C}$ сопряженный к z это элемент $\overline{z} = a - bi$

Lemma 4.2.

1. $\overline{\overline{z}} = z$ (сопряжение – инволюция)
2. $\{z = \overline{z}\} = \mathbb{R}$
3. $z \mapsto \overline{z}$ – автоморфизм
4. $z + \overline{z}, z * \overline{z} \in \mathbb{R}$ то есть это корни $x^2 - 2ax + (a^2 + b^2)$ (любое уравнение с отрицательным дискриминантом имеет такой вид)

Remark. *Инволюция – биективна*

Definition 4.4.

$z * \overline{z} = a^2 + b^2 = |z|^2$ - модуль

Lemma 4.3.

1. $a \in \mathbb{R}\, |a|_{\mathbb{R}} = |a|_{\mathbb{C}}$
2. $|z| \in \mathbb{R}_{\geq 0}$, $|z| = 0 \iff z = 0$
3. $|z_1 * z_2| = |z_1||z_2|$

4.4 Геометрический смысл и тригонометрическая форма

$z = a + bi \mapsto (a, b) \in \mathbb{R} \times \mathbb{R} \mapsto$ точка на декартовой плоскости. В этом случае $|z|$ - длина соответствующего вектора.

При сложении векторов происходит то же, что и при сложении комплексных чисел.

В частности $f_a(z) = z + a$ – параллельный перенос на вектор a.

Рассмотрим единичную окружность $|z| = 1$, тогда $z_\alpha = \cos(\alpha) + i\sin(\alpha)$.

$$\begin{aligned} z_\alpha \cdot z_\beta &= (\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta) = \\ &= (\cos\alpha\cos\beta - \sin\alpha\sin\beta) + i(\cos\alpha\sin\beta + \cos\beta\sin\alpha) = \\ &= \cos(\alpha+\beta) + i\sin(\alpha+\beta) = z_{\alpha+\beta} \end{aligned}$$

Возьмем $z \in \mathbb{C}^*$, тогда $z = \frac{z}{|z|} \cdot |z|$, при этом $|\frac{z}{|z|}| = 1$, значит $\frac{z}{|z|} = (\cos(\alpha) + i\sin(\alpha))$. Поэтому можем записать любое комплексное в виде $z = r(\cos(\varphi) + i\sin(\varphi))$, $r \in \mathbb{R}_{>0}$ - модуль числа, $\varphi = argz$ - аргумент.

При этом $z_1 z_2 = r_1 r_2(\cos(\alpha+\beta) + i\sin(\alpha+\beta))$

В частности $f_\alpha(z) = z_\alpha z$ - поворот на α.

Что такое аргумент? Рассмотрим $(\mathbb{R}, +)$, $a \equiv b(mod 2\pi)$ – это отношение эквивалентности с корректной операцией сложения.

$argz \in \mathbb{R}/2\pi\mathbb{Z}$ – группа углов $\mathbb{T}$.

5 Лекция 5

$\mathbb{T}_1 = \{z : |z| = 1\}$. $\overline{\varphi} \mapsto cos(\varphi) + i\sin(\varphi)$ – изомофризм $\mathbb{T}_\mathbb{1}$ и $\mathbb{T}$.

Рассмотрим $(\mathbb{R}_{>0}, \circ)$ - группа по умножению, $\mathbb{T}$ - группа углов.

$\mathbb{R}_{>0} \times \mathbb{T} \to \mathbb{C}^* \ (r, \varphi) \mapsto re^{i\varphi}$ – изоморфизм групп.

При этом $(\mathbb{C}, +) \cong \mathbb{R} \times \mathbb{R}$.

Экспоненциальная форма запици комплексного числа: $\cos(\varphi) + i\sin(\varphi) \stackrel{\text{def}}{=} e^{i\varphi}$.(можно достичь "равенства"рассмотрев ряды Тейлора)

5.1 Комплексные числа и геометрические преобразования

Definition 5.1.

1. $\mathbb{R}^2$ – плоскость. $f : \mathbb{R}^2 \to \mathbb{R}^2$ - биекция называется движением, если сохраняет расстояния.
2. Называется подобием, если $\forall x \neq y \neq z \neq t$

$$\frac{|f(x)f(y)|}{|f(z)f(t)|} = \frac{|xy|}{|zt|} \iff \frac{|f(x)f(y)|}{|xy|} = k - \text{коэффициент подобия}$$

p.s. Это не произведение, а так записаны отрезки с концами x, y.

Example. *Гомотетия с центром O и коэффициентом $k \in \mathbb{R}_{>0}$ – преобразование подобия*

Exercise 5.1.

Любое преобразование подобия это композиция движения и гомотетии

Доказательства не было на лекции но пусть будет

Доказательство. Возьмем $x \neq y$, f — преобразование подобия. $\Rightarrow \forall x, y \colon x \neq y \Rightarrow |f(x)f(y)| = k|xy|$.

Поэтому $h \circ f$, где h — гомотетия с коэффициентом $\frac{1}{k}$ — движение ($x, y \in \mathbb{R}^2$):

$$|(h \circ f)(x)(h \circ f)(y)| = \frac{1}{k}|f(x)f(y)| = \frac{1}{k} \cdot k|xy| = |xy|.$$

А значит, $h \circ f = g$, h^{-1} — гомотетия с коэффициентом k, а значит $f = h^{-1} \circ g$. □

Theorem 5.1. Шаля

Любое движение плоскости это либо параллельный перенос, поворот вокруг точки или осевая симметрия(скользящая)

В комплексных числах

1. $a \in \mathbb{C}$ $f(z) = z + a$ - параллельный перенос на вектор a
2. $k \in \mathbb{R}_{>0}$, $f(z) = kz$ – гомотетия в нулеб $k = -1$ - центральная симметрия в нуля.
3. $k = e^{i\varphi}$ $f(z) = kz$ – поворот на φ против часовой
4. В общем случае $k \in \mathbb{C}$ – поворотная гомотетия

Remark. *Движения делятся на 2 класса - сохраняющие ориентацию и меняющие ориентацию*

Example 5.1.

Поворотная гомотетия вокруг точки a: $f(z) = (z-a)k + a$ - линейная функция.
В частности, любое движение сохраняющее ориентацию – линейная функция.

Lemma 5.1.

Любая линейная функция это поворотная гомотетия или перенос.

Доказательство. $f(z) = pz + q$. Если $p = 1$, то это перенос на q.
Иначе: достаточно подобрать $k, a : pz + q = kz + a(1-k)$. То есть $p = k, q = a(1-k) \Rightarrow k = p, a = \frac{q}{1-p}$. □

Corollary. *Композиция поворотных гомотетий это параллельный перенос или поворотная гомотетия*

Итого: преобразование подобия, сохраняющее ориентацию = линейная функция.
Это группа относительно композиции $\cong \mathbb{R}^* \lambda(\mathbb{R}, +)$ - полупрямое произведение(фан факт).
Преобразования, меняющие ориентацию:
Осевая симметрия относительно OX - $f(z) = \overline{z}$.
Относительно произвольной прямой: перенесем ее в начало, переверном, сопряжем и обратно.... $f(z) = \overline{(z+a)e^{-i\varphi}}e^{+i\varphi} - a = k\overline{z} + l$

Lemma 5.2.

Любое преобразование, меняющее ориентацию задается $k\overline{z} + l$.

5.2 Формула Муавра

$$z = re^{i\varphi} \Rightarrow z^n = r^n e^{in\varphi}$$
$$r^n(\cos(n\varphi) + i\sin(n\varphi)) = (r(cos(\varphi) + i\sin(\varphi)))^n$$

Remark. *Для $n \in \mathbb{Z}$ тоже верно.*

Применение:

$$(\cos(\varphi) + i\sin(\varphi))^n = \cos(n\varphi) + i\sin(n\varphi)$$
$$\cos(\varphi)^n + i\cos(\varphi)^{n-1}\sin(\varphi)\binom{n}{1} + \cdots = \sum_{k=0}^{[\frac{n}{2}]}(-1)^k\cos(\varphi)^{n-2k}\sin(\varphi)^{2k}\binom{n}{2k} + \sum_{k=0}^{[\frac{n}{2}]}(\dots) * i$$

Получили формулы кратных углов...

$$\cos n\varphi = \sum_{k=0}^{[\frac{n}{2}]}(-1)^k\binom{n}{2k}\cos(\varphi)^{n-2k}(1-\cos(\varphi)^2)^{2k} = T_n(\cos(\varphi))$$

$T_n(x) \in \mathbb{R}[x]$ – многочлены Чебышева.

$$1+\cos(x)+\cdots+\cos(nx) = Re(1+e^{ix}+\cdots+e^{nix}) = Re\left(\frac{e^{i(n+1)x}-1}{e^{ix}-1}\right) =$$

$$Re\left(\frac{e^{\frac{inx}{2}}(e^{\frac{i(n+1)x}{2}}-e^{-\frac{i(n+1)x}{2}})}{e^{\frac{ix}{2}}-e^{-\frac{ix}{2}}}\right) = Re\left(\frac{e^{\frac{inx}{2}}\sin x\frac{n+1}{2}}{\sin(\frac{x}{2})}\right) = \frac{\sin(x\frac{n+1}{2})\cos(\frac{nx}{2})}{\sin(\frac{nx}{2})}$$

5.3 Корни из 1

Пусть $z_0 \in \mathbb{C}$. Хотим $\sqrt[n]{z_0}$ – это множество решений уравнения $z^n = z_0$.

1. $z_0 = 0 \Rightarrow z = 0$
2. $z_0 = re^{i\varphi}$, $z = qe^{i\psi}$

$$\begin{cases} q^n = r \\ n\overline{\psi} = \overline{\varphi} \end{cases} \Rightarrow \begin{cases} q = \sqrt[n]{r} \\ \psi = \frac{\varphi}{n} + \frac{2\pi k}{n} \end{cases}$$

Итак, $\sqrt[n]{z} = \{\sqrt[n]{r}(\cos(\frac{\psi}{n}+\frac{2\pi k}{n}) + i\sin(\frac{\psi}{n}+\frac{2\pi k}{n})) \,|k \in \mathbb{Z}/n\mathbb{Z}\}$

Когда $\psi_1 = \psi_2 \iff \frac{\psi}{n}+\frac{2\pi k}{n} = \frac{\psi}{n}+\frac{2\pi l}{n} \iff k \equiv_n l$

Геометрически – вершины правильного n-угольника с центром в нуле.

Корни из $1 = \{\cos(\frac{2\pi k}{n}) + i\sin(\frac{2\pi k}{n}) \,|k = 0,\ldots,n-1\}$

Случай $n = 3$. Имеем $\{1, -\frac{1}{2} \pm \frac{\sqrt{3}i}{2}\}$

Пусть K - поле, $\mu_n(K) = \{a \in K | a^n = 1\}$.

Lemma 5.3.

$\mu_n(K)$ – группа по умножению

Lemma 5.4.

Если K - поле, то $\mu_n(K)$ - циклическая группа

Доказательство аналогично очев трив((c)), но все же

Доказательство. $\mu_n = \{e^{\frac{2\pi ik}{n}}\} = \{(e^{\frac{2\pi i}{n}})^k, : k = 0,\ldots,n-1\} =$
$= \{\varepsilon^k \;:\; k = 0,\ldots,n-1\} \cong \mathbb{Z}/n\mathbb{Z}$
Произведение корней из 1 тоже корень из 1, обратный тоже.. 1 тоже корень.. Значит группа! □

Remark. $\mathbb{Z}/p\mathbb{Z}$ – *циклическая* $\iff$ $\mu_{p-1}(\mathbb{Z}/p\mathbb{Z})$ – *цикл.*

Доказательство. В $\mathbb{C}$ все очев. $\varepsilon_1 = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$, тогда ε_1^n – все корни. □

Definition 5.2.

Пусть $\varepsilon \in \mu_n(\mathbb{C})$ называется первообразный корень из единицы, если $\langle\varepsilon\rangle = \mu_n(\mathbb{C})$.
Эквивалентно: $\mathrm{ord}(\varepsilon) = n$, то есть не существует $k < n \;: \varepsilon^k = 1$.
$\varepsilon = e^{i\frac{2\pi k}{n}}$ – первообразный $\iff$ $(k,n) = 1$.

6 Лекция 6

Lemma 6.1.

Пусть $\mu_n(\mathbb{C})$. $\sum_{\varepsilon\in\mu_n}\varepsilon^k = \begin{cases}0,\ n\nmid k\\ n,\ n|k\end{cases}$

Доказательство. $k\vdots n$ $\sum\varepsilon^k = \sum(\varepsilon^n)^{k/n} = 1+1+\cdots+1 = n$

Иначе возьмем первообразный корень. $\sum\varepsilon^k = 1^k+\varepsilon^k+(\varepsilon^2)^k\cdots = \frac{(\varepsilon^k)^n-1}{\varepsilon^k-1} = \frac{0}{\ldots\neq 0} = 0.$ □

6.1 Дискретное преобразование Фурье

Пусть есть $\{f\in\mathbb{C}[x] \ : \ deg(f) < n\}$ Каждой f можем сопоставить его коэффициенты $(a_0,\ldots,a_{n-1})\in\mathbb{C}^n$. Пусть $\mu_n = \langle\varepsilon\rangle$. Рассмотрим $b_i = f(\varepsilon^i)$, тогда многочлену соответствует $(b_0,\ldots,b_{n-1})\in\mathbb{C}^n$. Возникает преобразование $(a_i)\underset{F}{\to}(b_i)$, где $b_i = \sum_{j=0}^{n-1}a_j\varepsilon^{ij}$. F называется дискретным преобразованием Фурье.

Хотим F^{-1}.

Theorem 6.1.

$a_i = \frac{1}{n}\sum_{i=0}^{n-1}b_j\varepsilon^{-ij}$

Доказательство. $b_i = \sum_{j=0}^{n-1}a_j\varepsilon^{ij}$. Зафиксируем j_0 и поделим равенство на ε^{ij_0}. Получим $\frac{b_i}{\varepsilon^{ij_0}} = \sum_{j=0}^{n-1}a_j\varepsilon^{i(j-j_0)}$. Сложим все такие равенства.

$$\sum_i b_i\varepsilon^{-ij_0} = \sum_i\sum_j a_j\varepsilon^{i(j-j_0)} = \sum_j a_j\sum_i\varepsilon^{i(j-j_0)} = \sum_j a_j\sum_{\alpha\in\mu_n}\alpha^{j-j_0} = na_{j_0}$$

т.к. $j, j_0 < n$, значит $j-j_0\vdots n \iff j = j_0$ и используем предыдущую лемму. ЧТД. □

Example. *Быстрое умножение многочленов.*

Обычное умножение требует вычисления свертки, значит n^2 умножений. Можно быстрее.

$f\to(b_0,\ldots,b_{n-1})$ и $g\to(b'_0,\ldots,b'_{n-1})$. Покомпонентно умножим их. А теперь обратным Фурье.

6.2 Алгебраическое замыкание и круговые многочлены

Definition 6.1.

Поле K называется алгебраические замкнутым, если любой многочлен($\deg(f) > 0$) имеет корень в K.

Theorem 6.2.

1. Для любого поля существует алгебраическое замыкание.
2. Если K алгебраически замкнутно, то любой многочлен раскладывается на линейные множители.

Доказательство.
1. (набросок) Присоединяем корни как в построении комплексных чисел пока можем...
2. Индукция по степени: берем корень, по теореме Безу раскладывем в $(x-a)g$, g уже раскладывается.

□

Corollary. *В алгебраически замкнутом поле многочлен степени n имеет n корней с учетом кратности*

Theorem 6.3. Основная теорема алгебры

$\mathbb{C}$ алгебраически замкнуто.
Док-ва не будет, Антипов принял #####.

Theorem 6.4.

Неразложимые многочлены над $\mathbb{R}$ это $(x-a)$, $a \in \mathbb{R}$ и (x^2+px+q), где $p^2-4q<0$ и только такие.
Другими словами $\forall f \in \mathbb{R}[x]\ f = a_0 \prod_i (x-a_i) \prod_i (x^2+p_ix+q_i)$

Lemma 6.2.

Пусть $f \in \mathbb{R}[x]$, $z \in \mathbb{C}$ - корень, тогда $f(\overline{z}) = 0$.

Доказательство. Подставим z и сопряжем все.

$$\overline{0} = 0 = f(z) = \overline{\sum a_i z^i} = \sum a_i \overline{z}^i = f(\overline{z})$$

□

Доказательство. Вернемся к теореме

Пусть $f \in \mathbb{R}[x]$ и он неразложим. По ОТА $\exists z \in \mathbb{C}$ - корень f. Если $z \in \mathbb{R}$, тогда по теореме Безу $f = (x-z)\widehat{f}$, но из неразложимости $\widehat{f} = const$, значит $f \sim (x-a)$.

Пусть $z \notin \mathbb{R}$. Тогда $z, \overline{z}$ различные корни f. В $\mathbb{C}[x]$ f делится на $(x-z)(x-\overline{z})$. Но $(x-z)(x-\overline{z}) \in \mathbb{R}[x]$, т.к. это $(x^2-(z+\overline{z})x+z\overline{z})$ и каждый коэффициент $\in \mathbb{R}$. Значит $f = (x^2-(z+\overline{z})x+z\overline{z}))\widehat{f}$, но f неразложим, значит получили искомое аналогично предыдущему. □

Example 6.1.

Разложить на множители $x^n - 1$.

1. Над $\mathbb{C}$ $x^n - 1 = \prod(x - e^{\frac{2\pi ik}{n}})$
2. Над $\mathbb{R}$ Если n нечетно, то

$$x^n - 1 = (x-1)\prod(x - e^{\frac{2\pi ik}{n}}) = (x-1)\prod_{k=1}^{\frac{n-1}{2}}(x^2 - 2\cos\frac{2\pi k}{n}x + 1)$$

3. Над $\mathbb{Q}$ чуть сложнее..

$$x^n - 1 = \prod_{d|n}\Phi_d$$

Definition 6.2. Круговой многочлен

$\Phi_n(x) = \prod_{\varepsilon\text{- первообразный}}(x - \varepsilon)$ - круговой многочлен

Lemma 6.3.

1. $\Phi_d(x) \in \mathbb{Z}[x]$
2. $\Phi_d(x)$ неразложим в $\mathbb{Q}[x]$

Доказательство. Все следует из рекурсивной формулы $\Phi_n(x) = \frac{x^n-1}{\prod_{d|n, d\neq n}\Phi_d(x)}$.

1. Индукция $\Phi_1 = x - 1$. Переход:
   При делении не возникает дробей, потому что оба многочлена с 1 старшим коэффициентом(деление с остатоком хорошее).
2. Неразложимость без доказательства

□

Theorem 6.5.

Пусть $f \in \mathbb{R}[x]$, $f(a) \geq 0\ \forall a \in \mathbb{R}$. Тогда $\exists g, h\ f = g^2 + h^2$.

Доказательство. Если $f \geq 0$, значит

$$f = (x-a)^2(x-b)^2\ldots(x^2 + p_1x + q_1)\cdots = g^2((x + \frac{p_1}{2})^2 + c_1^2)\ldots$$

Дальше волшебная формула $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$.

Итого можем превратить в сумму двух квадратов весь f. □

6.3 Гауссовы числа и Рождественская теорема

Вопрос: какие целые представляются как $a^2 + b^2$.

Definition 6.3. Кольцо Гауссовых чисел

Кольцо гауссовых чисел называется $Z[i] = \{a + bi\,|a, b \in \mathbb{Z}\}$.

Это очевидно кольцо, так как сумма и умножение целых - целое.

Не все простые числа остаются простыми. $2 = (1+i)(1-i)$.

Theorem 6.6.

$Z[i]$ – евклидово

Доказательство. Положим $\varphi(z) = |z|$. Надо доказать, что $\forall x, y \in \mathbb{Z}[i]\ \exists q, r : x = qy + r \wedge |r| < |y|$.

Переформулируем. $\frac{x}{y} = q + \frac{r}{y} \wedge |\frac{r}{y}| < 1 \iff |\frac{x}{y} - q| < 1$.

Если докажем, что $\forall z \in \mathbb{C}\ \exists q \in \mathbb{Z}[i]\ |z - q| < 1$, то победим.

Посмотрим на квадратик целочисленной решетки на $\mathbb{C}$, в котором лежит z. Пусть левый нижний угол это $a + bi$, а правый верхний $a + 1 + (b+1)i$. Разобъем его на 4 маленьких квадратика. Тогда существует $q \in \mathbb{Z}[i]$(уголок), который лежит в одном с z маленьком квадратике, со сторонами $\frac{1}{2}$, а расстояние между любыми точками там $|z - q| < \frac{1}{\sqrt{2}} < 1$. ЧТД! (остаток при этом может быть не единственным) □

Corollary. *В $Z[i]$ верна ОТА и все прочее.*

Theorem 6.7. Рождественская теорема Ферма

Пусть p - простое и $p = 4k + 1$. Тогда $\exists x, y \in \mathbb{Z}\ : p = x^2 + y^2$.
($p = 4k + 3$ никогда не представимы, можем посмотреть на остатки по модулю 4)
Упражнение - единственность такого представления(надо посмотреть на модуль числа).

Доказательство. $\exists x\ : x^2 + 1 \vdots p$.

Если ε первообразный корень $mod p$. Тогда $(\varepsilon^{\frac{p-1}{2}})^2 = 1 \Rightarrow \varepsilon^{\frac{p-1}{2}} = -1$. Значит $x = \varepsilon^{\frac{p-1}{4}}$.

$x^2 + 1 = py, y \in \mathbb{Z}$. Перейдем к гауссовым. Разложим $(x - i)(x + i) = py$.

$(x - i)(x + i) \vdots p$ в гауссовых, но каждое не делится, значит p составное в $\mathbb{Z}[i]$. То есть $p = (a + bi)(a - bi) = a^2 + b^2$ □

Дальше можно не читать

Remark. *Если подушнить(цитата) то мы доказали только $p = (a + bi)(c + di)$.*

Можно закончить например так: $p^2 = (a^2 + b^2)(c^2 + d^2)$ При этом $a^2 + b^2 \neq 1 \wedge c^2 + d^2 \neq 1$. Так как иначе p не составное(числе с модулем 1 - 4 $\pm 1, \pm i$).

Тогда возможен только вариант, что $p = a^2 + b^2 \wedge p = c^2 + d^2$. В любом случае получили искомое.

Так,

Все извините