Лекция 8

Пример

Пример 30. Рассмотрим многочлен $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$, $G = \mathrm{Gal}_{\mathbb{Q}} f = S_5 \Longrightarrow$ уравнение $f(x) = 0$ неразрешимо в радикалах.

1) $f(x)$ неприводим над $\mathbb{Q}$ по критерию Эйзенштейна $\Longrightarrow$ группа G транзитивна действует на корнях $\Longrightarrow 5 \mid |G| \Longrightarrow G$ ∋элемент порядка $5 \Longrightarrow \sigma \in S_5$ — цикл длины 5.

   Факт. Группа $G \curvearrowright X$ транзитивно $\Longleftrightarrow$ орбита одна — все X, $|X| < \infty$. Следовательно, по формуле орбит порядок $|X|$ делит порядок $|G|$: $|X| \mid |G|$.

2) Число действительных корней многочлена $f = N$. Имеем $f(0) = 2$, $f(1) = -1$. Следовательно, $N \geq 3$. Производная равна

$$f'(x) = 5x^4 - 4$$

   — два действительных корня. По теореме Ролля между любыми двумя корнями функции лежит корень ее производной. Так как у производной их 2, то у функции корней не более 3. Следовательно, $N = 3$.

3) существует два комплексно сопряженных корня $x_5 = \bar{x}_4 \Longrightarrow z \to \bar{z} \in G$.

Теорема Кронекера

Теорема 39. *Если неприводимый над $\mathbb{Q}$ многочлен простой степени $p \geqslant 3$ имеет корень, выражаемый в радикалах, то число его действительных корней равно 1 или p.*

Пример 31. $f(x) = x^p - 4x + 2$ неприводим над $\mathbb{Q}$ по признаку Эйзенштейна.
$p \geqslant 5$ $f'(x) = px^{p-1} - 4$ — 2 корня $\Longrightarrow$ у $f \leqslant 3$ корней в $\mathbb{R}$.

Критерий разрешимости неприводимых уравнений степени p

Теорема 40 (Критерий Абеля–Галуа)**.** *Пусть* $\mathrm{char}\, K = 0$, *f неприводим над K,* $\deg f = p$ *— простое число. Тогда следующие условия равносильны*

1) $f(x) = 0$ разрешим в радикалах над K

2) $G = \mathrm{Gal}_K(P)$ сопряжена с подгруппой в M_p.

3) поле разложения f: $L = K(x_i, x_j)$ для любых различных корней x_i и x_j многочлена f.

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

Теория делимости в областях целостности

Пусть A — *область целостности*, т.е. коммутативное ассоциативное кольцо с 1 без делителей 0, $Q(A)$ — поле частных области A:

$$Q(A) = \{ab^{-1} \mid a, b \in A, b \neq 0\}.$$

Пусть A^* — группа обратимых элементов. ($\mathbb{Z}^* = \{\pm 1\}$).

Определение 30. 1) $a \mid b \iff \exists c \in A,\ ac = b$.

2) $a \mid b$, $b \mid a$, $a, b \neq 0 \iff a$ и b ассоциированы $\iff u \in A^*$: $b = au$.

3) $d = (a, b) \iff$

$$\begin{cases} d \mid a, b \\ \forall d' :\ d' \mid a, d' \mid b \Longrightarrow d' \mid d. \end{cases}$$

3')

$$\begin{cases} a, b \mid [a, b] \\ a, b \mid c \Longrightarrow [a, b] \mid c. \end{cases}$$

Заметим, что НОК и НОД не всегда существуют.

Неприводимый элемент

Определение 31. 1) Элемент $p \in A$ неприводим $\iff p \neq 0$, $p \in A^*$ и $\forall a, b \in A$: $p = ab \Longrightarrow a \in A^*$ или $b \in A^*$.

2) Элемент p прост $\iff p \neq 0$, $p \notin A^*$ и $\forall a, b \in A$: $p \mid ab \Longrightarrow p \mid a$ или $p \mid b$.

Определение 32. Кольцо A факториально $\iff \forall a \in A/0$ существует $n \in \mathbb{N}_0$, $\exists p_1, \ldots, p_n \in A$ — неприводимы.

$$a = p_1, \ldots, p_n.$$

Для всяких $m, n \in \mathbb{N}_0$ $\forall p_1, \ldots, p_n, q_1, \ldots, q_m$ неприводимых

$$a = p_1, \ldots, p_n, q_1, \ldots, q_m \Longrightarrow m = n.$$

Существуют $u_1, \ldots, u_n \in A^*$, $\exists \sigma \in S_n$:

$$q_i = u_i p_{\sigma(i)}.$$

Если кольцо факториально, то существует и единственно разложение на неприводимые.

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

Пример 32. Приведем пример, когда нет единственности разложения. на неприводимые. Кольцо

$$\mathbb{Z}[\sqrt{-3}] = \{a + bi\sqrt{3} \mid a, b \in \mathbb{Z}\}.$$

не факториально — эйлеровы числа. Например,

$$(1 + i\sqrt{3})(1 - i\sqrt{3}) = 2 \cdot 2.$$

Но

$$\mathbb{Z} = [\frac{1 + i\sqrt{3}}{2}]$$

— факториальное кольцо — эйзенштейновы числа.

Пример 33. Рассмотрим

$$\{f \in K[x] \mid f = a_0 + a_2x^2 + a_3x^3 + \ldots + a_nx^n,\ a_i \in K, n \in \mathbb{N}_0\}$$

Здесь x^2 и x^3 неприводимы:

$$x^3 \cdot x^3 = x^2 \cdot x^2 \cdot x^2.$$

Но x^2 и x^3 не просты: $x^2 \mid ab$, но $x^2 \nmid a, b$ при $a = b = x^3$.

Утверждение 9. *1) Простота $\Longrightarrow$ неприводимость.*

2) Обратное неверно.

3) Обратное верно в факториальных кольцах.

4) Если $\forall$ неприводимый элемент прост, то есть однозначность разложения на неприводимые.

Доказательство. 1) p — прост, $p = ab \Longrightarrow p \mid a$ или $p \mid b$. Кроме того, $a, b \mid p$. Следовательно, p ассоциировано с a или с b. Следовательно, $b \in A^*$ или $a \in A^*$.

2) $K \oplus Kx^2 \oplus Kx^3 \ldots \ni x^2$ — неприводимый, но не простой.

3) p неприводимо в факториальном кольце A, $p \mid ab$, $p \nmid a$, $p \nmid b$

$$a = p_1 \ldots p_m,$$

$$b = q_1 \ldots q_n$$

— разлагаются на неприводимые

$$\frac{ab}{p} = r_1 \ldots r_l.$$

$$ab = p_1 \ldots p_m q_1 \ldots q_n = pr_1 \ldots r_l$$

— противоречие.

4) $p_1 \ldots p_m = q_1 \ldots q_n$, p_i, q_j — неприводимые. Так как p_1 прост, то $p_1 \mid q_1(q_2 \ldots q_n)$ $\Longrightarrow p_1 \mid q_1$ либо $q_2 \ldots q_n$.

Следовательно, $\exists j : p_1 \mid q_j \Longrightarrow p_1 \sim q_j$.

□

Существование разложения на неприводимые

Пример 34. $A = \{f \in \mathbb{Q}[x] \mid f(0) \in \mathbb{Z}\} = \mathbb{Z} \oplus \mathbb{Q}x \oplus \mathbb{Q}x^2 \oplus \dots$

$$x = 2 \cdot \frac{x}{2} = 2 \cdot 2 \cdot \frac{x}{4}.$$

$$p_1 \dots p_n = ax \cdot b_1 \dots b_k,$$

где $p_1 \dots p_n$ неприводимые, ax — неприводимо, $a \in \mathbb{Q}$.

Утверждение 10. *Следующие условия на кольцо (коммутативное и ассоциативное) A равносильны:*

1) $\forall I \lhd A$ *конечно порожден:*

$$\exists n \in \mathbb{N}\ \exists a_1, \dots a_n :\ I = (a_1, \dots, a_n) = a_1 A + \dots a_n A.$$

2) *любая нестрого возрастающая цепь идеалов стабилизируется*

$$I_1 \subseteq I_2 \subseteq \dots \subseteq I_n = I_{n+1} = \dots$$

3) *Не существует бесконечных строго возрастающих цепей идеалов. Такие кольца A называются* нетеровыми.

$$\text{КГИ} \Longrightarrow \text{Нетеровость} \Longrightarrow \text{существование разложения}$$

Евклидово кольцо

Определение 33. Целостное кольцо называется евклидовым относительно нормы $N : A/0 \longrightarrow \mathbb{N}_0$:

$$\begin{cases} \forall a, b \in A,\ b \neq 0 \exists q, r \in A :\ \ a = bq + r,\ N(r) < N(b),\ \text{либо } r = 0. \\ \forall a, b \neq 0\ \ N(ab) > N(a), N(ab) = N(a) \Longleftrightarrow b \in A^*. \end{cases}$$

A евклидово $\Longleftrightarrow$ A евклидово относительно некоторой нормы.

Кольца Безу

Утверждение 11. *Следующие условия на целостное кольцо A равносильны:*

1) *каждый конечно порожденный идеал — главный.*

2) $\forall a, b \in A\ \exists (a, b) = au + bv$ *— соотношение Безу.*

Такие кольца называются кольцами Безу.

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ