Корни из единицы. Круговой многочлен.

Конспект лекции

Содержание

1 Критерий Эйзенштейна и лемма Гаусса

1.1 Критерий Эйзенштейна

Теорема 1.1 (Критерий Эйзенштейна)**.** *Пусть* $f \in \mathbb{Z}[x]$*:*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

где $a_i \in \mathbb{Z}$*. Пусть* p *— простое число такое, что* $p \mid a_i$ *для всех* $i = 0, \ldots, n-1$*,* $p \nmid a_n$*,* $p^2 \nmid a_0$*. Тогда многочлен* $f(x)$ *неприводим над* $\mathbb{Z}$ *(и, следовательно, над* $\mathbb{Q}$*).*

Доказательство. Предположим противное: $f = gh$, где $g, h \in \mathbb{Z}[x]$ — нетривиальные многочлены. Рассмотрим редукцию по модулю p. В кольце $\mathbb{F}_p[x]$ имеем

$$\overline{f}(x) = \overline{a_n} x^n.$$

Так как $\mathbb{F}_p[x]$ — область уникального разложения, то

$$\overline{f}(x) = \overline{g}(x)\overline{h}(x),$$

где

$$\overline{g}(x) = b_m x^m, \qquad \overline{h}(x) = c_l x^\ell,$$

где $m + \ell = n$ и $b_m, c_l \in \mathbb{F}_p^*$. Также сами многочлены $g, h \in \mathbb{Z}[x]$ имеют вид:

$$g = \sum_{i=0}^{m} b_i x_i, \;\; h = \sum_{i=0}^{l} c_i x_i,$$

а $\overline{g}, \overline{h} \in \mathbb{F}_p[x]$:

$$\overline{g} = b_m x_m, \;\; \overline{h} = c_l x_l.$$

Это возможно лишь в том случае, если все коэффициенты g, h, кроме старших, делятся на p. В частности, $p \mid b_0$ и $p \mid c_0$, где b_0, c_0 — свободные члены g, h. Но тогда

$$a_0 = b_0 c_0 \quad \Rightarrow \quad p^2 \mid a_0,$$

что противоречит условию. □

1.2 Лемма Гаусса

Определение 1.2. Многочлен $f \in \mathbb{Z}[x]$ называется *примитивным*, если наибольший общий делитель всех его коэффициентов равен 1.

Лемма 1.3 (Лемма Гаусса)**.** *Многочлен $f \in \mathbb{Z}[x]$ неприводим над $\mathbb{Z}$ тогда и только тогда, когда он неприводим над $\mathbb{Q}$.*

Доказательство. Одно направление очевидно. Докажем обратное. Пусть f приводим над $\mathbb{Q}$, то есть

$$f = gh, \qquad g, h \in \mathbb{Q}[x],$$

где $\deg g, \deg h > 0$. Существуют такие $a, b \in \mathbb{Q}^*$, что многочлены

$$g_1 = ag, \qquad h_1 = bh$$

имеют целые коэффициенты и являются примитивными. Тогда

$$f_1 = abf(x) = ag(x) \cdot bh(x) = g_1(x)h_1(x).$$

Пусть простое $p \mid ab$. Тогда p делит все коэффициенты f_1, и редукция $0 = \overline{f}_1 = \overline{g}\overline{h_1}(mod\, p)$. Следовательно,

$$\overline{g}_1 \cdot \overline{h}_1 = 0 \quad \text{в } \mathbb{F}_p[x].$$

Так как в $\mathbb{F}_p[x]$ здесь нет делителей нуля, то $\overline{g}_1 = 0$ или $\overline{h}_1 = 0$, что означает, что p делит все коэффициенты g_1 или h_1. Это противоречит примитивности этих многочленов. Следовательно, $ab = \pm 1$, и f приводим над $\mathbb{Z}$. □

2 Применение критерия Эйзенштейна и формальная производная

Утверждение 2.1. *Пусть p — простое число. Тогда многочлен*

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

неприводим над $\mathbb{Q}$.

Доказательство. Рассмотрим $f(x+1)$. Имеем

$$f(x) = \frac{x^p - 1}{x - 1},$$

откуда

$$f(x+1) = \frac{(x+1)^p - 1}{x}.$$

По биному Ньютона

$$(x+1)^p = x^p + \binom{p}{1}x^{p-1} + \cdots + \binom{p}{p-1}x + 1,$$

$$f(x+1) = x^{p-1} + \binom{p}{1}x^{p-2} + \cdots + \binom{p}{p-1}.$$

Все биномиальные коэффициенты, кроме коэффициента при старшей степени, делятся на p, а свободный член после деления на x не делится на p^2. По критерию Эйзенштейна $f(x+1)$ неприводим, следовательно, неприводим и $f(x)$. □

2.1 Формальная производная

Определение 2.2. Пусть K — поле и

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in K[x].$$

Формальной производной многочлена f называется многочлен:

$$f'(x) = na_n x^{n-1} + \cdots + 2a_2 x + a_1.$$

Утверждение 2.3. *Для любых $f, g \in K[x]$ выполняются свойства:*

(i) $(f+g)' = f' + g'$,

(ii) $(fg)' = f'g + fg'$.

Лемма 2.4. *Пусть α — корень $f \in K[x]$. Тогда α является кратным корнем тогда и только тогда, когда $f'(\alpha) = 0$.*

3 Корни из единицы. Круговые поля.

3.1 Корни из единицы

Рассмотрим многочлен $x^n - 1$ над $\mathbb{C}$, где

$$x^n - 1 = \prod_{k=1}^{n}(x - e^{2\pi ik/n}), \qquad k = 0, 1, \ldots, n-1.$$

Его корни имеют вид

$$\zeta_n^k = e^{2\pi ik/n}.$$

Определение 3.1. Множество

$$U_n = \{\zeta_n^k \mid 0 \le k < n\}$$

называется *группой корней степени n из единицы* ($\sqrt[n]{1}$). Элемент $\zeta \in U_n$ называется *примитивным корнем* $\sqrt[n]{1}$, если $\mathrm{ord}(\zeta) = n$.

3.2 Круговые поля

Определение 3.2. Пусть K — поле, то *n-тым круговым полем над K* называется поле разложения многочлена $x^n - 1$ над K. Обозначается $K^{(n)}$.

4 Структура группы корней из единицы

Теорема 4.1. *Пусть K — поле и $\operatorname{char} K = p \geq 0$.*

(i) Если $p \nmid n$, то группа U_n циклическая порядка n.

(ii) Если $p \mid n$ и $n = p^e m$, где $p \nmid m$, то $U_n = U_m$.

Доказательство. Если $p \nmid n$, то $(x^n - 1)' = nx^{n-1}$ не обращается в ноль на корнях, следовательно, все корни простые и $|U_n| = n$. Далее доказывается цикличность стандартным групповым аргументом, используя разложение n на простые множители и построение элемента порядка n. В случае $p \mid n$ имеем

$$x^n - 1 = (x^m - 1)^{p^e},$$

откуда утверждение. □

5 Круговые многочлены

Пусть $n \geq 1$, характеристика поля K не делит n, и ζ — примитивный корень степени n из единицы.

Определение 5.1. *n-тым круговым многочленом* называется многочлен

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ (k,n)=1}} (x - \zeta^k).$$

Утверждение 5.2. *Выполняются следующие свойства:*

(i) $\deg \Phi_n = \varphi(n)$;

(ii)

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x);$$

(iii) $\Phi_n(x)$ имеет коэффициенты в простом подполе K (в частности, $\Phi_n(x) \in \mathbb{Z}[x]$ при $K = \mathbb{Q}$).

Доказательство. Корни многочлена $x^n - 1$ — все корни степени n из единицы. Каждый такой корень имеет некоторый порядок $d \mid n$, и является примитивным корнем степени d. Группируя корни по порядкам, получаем разложение. Степень Φ_n равна числу примитивных корней, то есть $\varphi(n)$. □

Лемма 5.3. *Элемент ζ является примитивным корнем степени n из единицы тогда и только тогда, когда $\Phi_n(\zeta) = 0$.*

Теорема 5.4. *Круговой многочлен $\Phi_n(x)$ неприводим над $\mathbb{Q}$.*

6 Круговые многочлены над конечными полями

Пусть p — простое число, $p \nmid n$.

6.1 Круговое поле над $\mathbb{F}_p$

Пусть ζ — примитивный корень степени n из единицы в некотором расширении поля $\mathbb{F}_p$.

Утверждение 6.1. *Пусть d — наименьшее натуральное число такое, что*

$$p^d \equiv 1 \pmod{n}.$$

Тогда $\zeta \in \mathbb{F}_{p^d}$, и поле разложения многочлена $x^n - 1$ над $\mathbb{F}_p$ изоморфно $\mathbb{F}_{p^d}$.

Доказательство. Если $\zeta \in \mathbb{F}_{p^k}$, то порядок элемента ζ делит $p^k - 1$, следовательно $n \mid (p^k - 1)$. Минимальность d означает, что d есть порядок p в группе $(\mathbb{Z}/n\mathbb{Z})^\times$. Поэтому $\zeta \in \mathbb{F}_{p^d}$, и меньшего поля не существует. □

6.2 Разложение $\Phi_n(x)$ над $\mathbb{F}_p$

Теорема 6.2. *Пусть d — порядок p по модулю n. Тогда круговой многочлен $\Phi_n(x)$ над $\mathbb{F}_p$ раскладывается в произведение*

$$\Phi_n(x) = f_1(x) f_2(x) \cdots f_r(x),$$

где:

(i) *все $f_i(x)$ неприводимы над $\mathbb{F}_p$;*

(ii) $\deg f_i = d$ *для всех i;*

(iii) $r = \varphi(n)/d$.

Доказательство. Минимальный многочлен элемента ζ над $\mathbb{F}_p$ имеет степень d, так как

$$\mathbb{F}_p(\zeta) = \mathbb{F}_{p^d}.$$

Его корни имеют вид

$$\zeta, \zeta^p, \zeta^{p^2}, \ldots, \zeta^{p^{d-1}},$$

и являются примитивными корнями степени n. Следовательно, минимальный многочлен делит $\Phi_n(x)$. Все примитивные корни разбиваются на такие орбиты, откуда и следует утверждение. □

Замечание 6.3. Разложение $\Phi_n(x)$ описывается действием автоморфизма Фробениуса

$$\sigma(\alpha) = \alpha^p$$

на множестве примитивных корней степени n из единицы.

Дополнительные замечания

Замечание 6.4 (Интерпретация результатов). Содержание лекции можно суммировать следующим образом: структура разложения кругового многочлена $\Phi_n(x)$ над конечным полем $\mathbb{F}_p$ полностью определяется порядком p по модулю n.

Замечание 6.5 (Связь с конечными полями). Каждое конечное поле характеристики p изоморфно $\mathbb{F}_{p^d}$, а его мультипликативная группа циклическая. Корни из единицы и круговые многочлены дают удобный язык для описания таких расширений.

Замечание 6.6 (Действие Фробениуса). Автоморфизм Фробениуса

$$\alpha \mapsto \alpha^p$$

описывает сопряжения корней и объясняет, почему все неприводимые множители $\Phi_n(x)$ над $\mathbb{F}_p$ имеют одинаковую степень.