Лекция №13. Лемма Гензеля и принцип Хассе.

1 Нормированные и ультраметрические поля

Определение 1.1. Пусть K — поле. Отображение $\varphi : K \to \mathbb{R}_{\geq 0}$ называется *нормой*, если для всех $x, y \in K$ выполнено:

1. $\varphi(x) = 0 \iff x = 0$;
2. $\varphi(xy) = \varphi(x)\varphi(y)$;
3. $\varphi(x + y) \leq \varphi(x) + \varphi(y)$.

Определение 1.2. Норма φ называется *ультраметрической*, если вместо (3) выполнено

$$\varphi(x + y) \leq \max\{\varphi(x), \varphi(y)\}.$$

Лемма 1.3. *Ультраметрическая норма индуцирует метрику*

$$d(x, y) = \varphi(x - y),$$

удовлетворяющую усиленному неравенству треугольника.

Доказательство. Так как φ — норма, то $d(x, y) = 0 \iff x = y$, симметрия очевидна. Для треугольника:

$$d(x, z) = \varphi(x - z) = \varphi((x - y) + (y - z)) \leq \max\{\varphi(x - y), \varphi(y - z)\}.$$

$\square$

2 p-адическая норма и поле $\mathbb{Q}_p$

Определение 2.1. Пусть p — простое число. Для $x \in \mathbb{Q}^\times$ представимого в виде

$$x = p^n \frac{a}{b}, \quad (a, b, p) = 1,$$

определим *p-адическую валюацию*

$$v_p(x) = n.$$

Полагаем $v_p(0) = +\infty$.

Определение 2.2. *p-адическая норма* определяется формулой

$$|x|_p = p^{-v_p(x)}, \quad |0|_p = 0.$$

Лемма 2.3. *Функция* $|\cdot|_p$ *является ультраметрической нормой на* $\mathbb{Q}$.

Доказательство. Свойства (1) и (2) следуют из свойств валюации. Для суммы используем:

$$v_p(x+y) \geq \min\{v_p(x), v_p(y)\},$$

откуда

$$|x+y|_p \leq \max\{|x|_p, |y|_p\}.$$

□

Определение 2.4. Поле $\mathbb{Q}_p$ — пополнение $\mathbb{Q}$ по метрике $|\cdot|_p$.

3 Кольцо p-адических целых

Определение 3.1.

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}.$$

Лемма 3.2. $\mathbb{Z}_p$ *является кольцом, а множество*

$$\mathfrak{m} = \{x \in \mathbb{Q}_p : |x|_p < 1\}$$

— его максимальный идеал.

Доказательство. Если $|x|_p, |y|_p \leq 1$, то

$$|x+y|_p \leq \max(|x|_p, |y|_p) \leq 1, \quad |xy|_p \leq 1.$$

Максимальность $\mathfrak{m}$ следует из того, что любой $x \notin \mathfrak{m}$ обратим в $\mathbb{Z}_p$. □

Следствие 3.3. *Поле вычетов* $\mathbb{Z}_p/\mathfrak{m} \simeq \mathbb{F}_p$.

4 Полнота

Теорема 4.1. *Поле* $\mathbb{Q}_p$ *полно.*

Доказательство. По построению $\mathbb{Q}_p$ как пополнения метрического пространства $\mathbb{Q}$ относительно $|\cdot|_p$. □

Следствие 4.2. $\mathbb{Z}$ *плотно в* $\mathbb{Z}_p$.

5 Формальные производные

Определение 5.1. Пусть
$$f(x) = a_0 + a_1 x + \cdots + a_n x^n.$$
Формальная производная:
$$f'(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}.$$
Лемма 5.2 (Формула Тейлора)**.** *Для $f \in \mathbb{Z}_p[x]$ и $h \in \mathbb{Z}_p$:*
$$f(x+h) = f(x) + f'(x)h + \frac{f''(x)}{2!}h^2 + \dots$$
Доказательство. Доказательство стандартно и следует из биномиальной формулы. □

6 Лемма Гензеля

Теорема 6.1 (Лемма Гензеля)**.** *Пусть $f \in \mathbb{Z}_p[x]$ и существует $a_0 \in \mathbb{Z}_p$ такое, что*
$$f(a_0) \equiv 0 \pmod p, \quad f'(a_0) \not\equiv 0 \pmod p.$$
Тогда существует единственный $\alpha \in \mathbb{Z}_p$, для которого
$$f(\alpha) = 0, \quad \alpha \equiv a_0 \pmod p.$$
Доказательство. Построим последовательность
$$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}.$$
Индукцией доказывается:
$$f(a_n) \equiv 0 \pmod{p^{2^n}}, \quad |a_{n+1} - a_n|_p \le p^{-2^n}.$$
Последовательность фундаментальна, а полнота $\mathbb{Z}_p$ даёт предел α. Переход к пределу в равенстве $f(a_n) = 0$ даёт $f(\alpha) = 0$. Единственность следует из ультраметричности. □

7 Следствия

Следствие 7.1. *Если уравнение $f(x) \equiv 0 \pmod p$ имеет простой корень, то оно имеет корень в $\mathbb{Z}_p$.*

Следствие 7.2. *Пусть $(m, p) = 1$. Тогда уравнение $x^m = a$ разрешимо в $\mathbb{Q}_p$ тогда и только тогда, когда оно разрешимо по модулю p.*

Доказательство. Рассматриваем $f(x) = x^m - a$ и применяем лемму Гензеля. □

8 Принцип Хассе

Теорема 8.1 (Принцип Хассе для квадратичных форм)**.** *Пусть F — квадратичная форма над $\mathbb{Q}$. Тогда уравнение $F = 0$ имеет нетривиальное решение в $\mathbb{Q}$ тогда и только тогда, когда оно имеет решение в $\mathbb{R}$ и во всех $\mathbb{Q}_p$.*