Введение в теорию Галуа - семинар 7

10 ноября 2025

(1) Пусть $\mathbb{Q} \subset E$ — это расширение Галуа и группа $\mathrm{Gal}(E/\mathbb{Q})$ — абелева. Покажите, что если $F \subset E$ — подполе, то $\mathbb{Q} \subset F$ — расширение Галуа и $\mathrm{Gal}(F/\mathbb{Q})$ — абелева группа.

(2) Пусть $f \in \mathbb{Q}[X]$ — это неприводимый многочлен степени 4. Обозначим через E поле разложения f и предположим, что $\mathrm{Gal}(E/\mathbb{Q}) = A_4$ и α — корень f в E. Докажите, что у расширения $\mathbb{Q} \subset \mathbb{Q}[\alpha]$ нет промежуточных расширений, то есть полей L таких, что $\mathbb{Q} \subsetneq L \subsetneq \mathbb{Q}[\alpha]$.

(3) Пусть F —это поле из 16 элементов. Сколько корней имеет в поле F каждый из следующих многочленов? $X^3 - 1; X^4 - 1; X^{15} - 1; X^{17} - 1$.

(4) Пусть $F \subset E$ — расширение конечных полей.
   (a) Докажите, что $E \setminus \{0\}$ с операцией умножения — циклическая группа. (Подсказка: это было в листке к первому семинару.)
   (b) Выведите, что $F \subset E$ — это простое расширение.

(5) Пусть p — это простое число.
   (a) Пусть E — поле разложения многочлена $f(X) = X^q - X, q = p^n$ над $\mathbb{F}_p$. Проверьте, что $\mathbb{F}_p \subset E$ — это расширение Галуа и что $|E| = p^n$.
   (b) Докажите, что для любого $n \geqslant 1$ поле $\mathbb{F}_{p^n}$ существует и единственно с точностью до изоморфизма.
   (c) Докажите, что $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ — это циклическая группа. Какой автоморфизм $\mathbb{F}_{p^n}$ является ее образующей?
   (d) Пусть E —это поле из p^n элементов. Докажите, что для каждого делителя $m \geqslant 0$ числа n поле E содержит ровно одно подполе из p^m элементов.
   (e) Каждый приведенный неприводимый многочлен f степени $d \mid n$ в $\mathbb{F}_p[X]$ является делителем многочлена $X^{p^n} - X$ с кратностью 1. В частности, степень поля разложения f не больше чем d.
   (f) Постройте алгебраическое замыкание $\mathbb{F}_p$.

(6) Покажите, что многочлен f степени $n = \prod_{i=1}^{k} p_i^{r_i}$ неприводим над $\mathbb{F}_q$ тогда и только тогда, когда $\gcd\Big(f(x), x^{q^{n/p_i}} - x\Big) = 1$ для всех i.

(7) Пусть F — это конечное поле порядка $q = p^n$, где $p \neq 2$. Докажите что $X^2 = -1$ имеет решение в F если и только если $q \equiv 1 \bmod 4$.

(8) Докажите, что для любых $a, b \in \mathbb{F}_{p^n}$ если $x^3 + ax + b$ — это неприводимый многочлен, то $-4a^3 - 27b^2$ — это квадрат в $\mathbb{F}_{p^n}$.

(9) Рассмотрим многочлен $f(X) = X^3 + X + 1 \in F[X]$ над полем $F = \mathbb{F}_2$. Обозначим через E поле разложения f над F.
   (a) Докажите, что f — неприводим над F.
   (b) Пусть α — корень f в E. Докажите, что α^2 — тоже корень f.
   (c) Посчитайте группу Галуа $\mathrm{Gal}(E/F)$.