Введение в теорию Галуа - семинар 8

17 ноября 2025

(1) Пусть $f \in \mathbb{F}_q[X]$ — многочлен степени $n = \prod_{i=1}^{k} p_i^{r_i}$.
   (a) Покажите, что если f — неприводим над $\mathbb{F}_q$, то f — делитель многочлена $X^{q^n} - X$.
   (b) Покажите, что если f — неприводим над $\mathbb{F}_q$, то $\gcd\left(f, X^{q^{n/p_i}} - X\right) = 1$ для всех i.
   (c) Покажите, что если f делит многочлен $X^{q^n} - X$ и $\gcd\left(f, X^{q^{n/p_i}} - X\right) = 1$ для всех i, то f — неприводим над $\mathbb{F}_q$.

(2) 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 $q \equiv 1 \bmod 4$.

(3) 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 $\mathbb{F}_{p^n}$.

(4) Докажите, что если $f(X) = X^3 + pX + q \in \mathbb{Z}[X]$ неприводим, то $D = -4p^3 - 27q^2$ — это целое число, не равное $0, \pm 1$.

(5) 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 $\mathrm{Gal}(E/F)$.

(6) Докажите, что $\mathbb{Q}(\sqrt[3]{2})$ не является подполем циклотомического расширения $\mathbb{Q}$.

(7) Пусть $f = X^4 + aX^2 + b \in \mathbb{Q}[X]$ — неприводимый многочлен над $\mathbb{Q}$, а E — поле разложения f.
   (a) Покажите, что $[E\colon \mathbb{Q}] = 4$ или 8.
   (b) Покажите, что $\mathrm{Gal}(E/\mathbb{Q})$ может быть равно $\mathbb{Z}/2 \times \mathbb{Z}/2$, $\mathbb{Z}/4$ или D_4 и постройте примеры для каждого из случаев.
   (c) Покажите, что расширение $\mathbb{Q} \subset F$ степени 4 может быть порождено одним корнем f над $\mathbb{Q}$ тогда и только тогда, когда F содержит квадратичное расширение $\mathbb{Q}$.