Введение в теорию Галуа - семинар 4

6 октября 2025

(1) Пусть F поле характеристики p и α алгебраичен над F.
   (a) Покажите, что минимальный многочлен α сепарабелен тогда и только тогда, когда $F(\alpha) = F\left(\alpha^{p^n}\right)$ для всех $n \in \mathbb{N}$.
   (b) Покажите, что если F — совершенно, что α либо лежит в F, либо $F(\alpha) = F\left(\alpha^{p^n}\right)$ для всех $n \in \mathbb{N}$, то есть любое алгебраическое расширение совершенного поля — совершенно.

(2) Пусть ζ — это прмитивный корень из 1 степени 7.
   (a) Покажите, что $\mathbb{Q} \subset \mathbb{Q}[\zeta]$ — это расширение Галуа и $G = \mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}) = (\mathbb{Z}/7\mathbb{Z})^{\times}$.
   (b) Постройте промежуточное расширение $\mathbb{Q} \subset M_3 \subset \mathbb{Q}[\zeta]$, такое что $[M_3 : \mathbb{Q}] = 3$ и покажите, что M_3 — это поле разложения многочлена $X^3 + X^2 - 2X - 1$.
   (c) Постройте промежуточное расширение $\mathbb{Q} \subset M_2 \subset \mathbb{Q}[\zeta]$, такое что $[M_2 : \mathbb{Q}] = 2$ и покажите, что $M_2 = \mathbb{Q}[\sqrt{-7}]$.

(3) Посчитайте группу Галуа для поля разложения многочлена $X^5 - 2$ над $\mathbb{Q}$.

(4) Пусть F — это поле характеристики 0 и пусть $E = F\left(X^2\right) \cap F\left(X^2 - X\right)$.
   (a) Найдите автоморфизм $\sigma \in \mathrm{Aut}(F(X)/F)$ порядка 2, сохраняющий поле $F\left(X^2\right)$.
   (b) Найдите автоморфизм $\tau \in \mathrm{Aut}(F(X)/F)$ порядка 2, сохраняющий поле $F\left(X^2 - X\right)$. Посчитайте порядок композиции $\sigma \circ \tau$.
   (c) Докажите, что если $E \subset F(X)$ — это конечное расширение, то $\mathrm{Aut}(F(X)/E)$ — это конечная группа. Выведите отсюда, что $E = F$.

(5) Циклотомические расширения $\mathbb{Q}$.
   (a) Пусть p — простое число, $f \in \mathbb{Z}[X]$ — многочлен со старшим коэффициентом 1, такой что многочлен $f (\bmod\ p) \in \mathbb{F}_p[X]$ не имеет кратных корней в поле разложения. Покажите, что многочлен f над $\mathbb{Q}$ не имеет кратных корней.
   (b) Пусть $\mathbb{Q} \subset L$ — поле разложения многочлена f из пункта (a), $\alpha \in L$ — некоторый корень многочлена f, и пусть P — минимальный многочлен элемента α над $\mathbb{Q}$. Предположим, что $f\left(\alpha^p\right) = 0$. Докажите, что тогда $P\left(\alpha^p\right) = 0$.
   (c) Пусть $\zeta \in \mathbb{C}$ - примитивный корень степени n из 1. Покажите, что минимальный многочлен R элемента ζ над $\mathbb{Q}$ обращается в нуль в ζ^p для любого p, взаимно простого с n.
   (d) Покажите, что $R(X) = \prod_{i \in (\mathbb{Z}/n\mathbb{Z})^*} \left(X - \zeta^i\right)$.
   (e) Пусть E — это поле разложения многочлена $X^n - 1$. Покажите $\mathrm{Gal}(E/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$.

(6) Пусть p — это простое число, не равное 2, и пусть ζ — это примитивный p-ый корень из 1 в $\mathbb{C}$. Пусть $E = \mathbb{Q}[\zeta]$ и пусть $G = \mathrm{Gal}(E/\mathbb{Q})$; тогда $G = (\mathbb{Z}/(p))^{\times}$. Пусть H — это подгруппа индекса 2 в G. Положим $\alpha = \sum_{i \in H} \zeta^i$ и $\beta = \sum_{i \in G \setminus H} \zeta^i$. Покажите:
   (a) α и β инвариантны относительно H;

(b) если $\sigma \in G \backslash H$, то $\sigma\alpha = \beta, \sigma\beta = \alpha$;

(c) α и β — это корни многочлена $X^2 + X + \alpha\beta \in \mathbb{Q}[X]$;

(d) Покажите равенство:

$$E^H = \begin{cases} \mathbb{Q}[\sqrt{p}], & \text{если } p \equiv 1 \bmod 4; \\ \mathbb{Q}[\sqrt{-p}], & \text{если } p \equiv 3 \bmod 4. \end{cases}$$

(7) Пусть $M = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ и $E = M[\sqrt{(\sqrt{2}+2)(\sqrt{3}+3)}]$ (и то, и другое — подполя $\mathbb{R}$).

(a) Покажите, что M — это расширение Галуа над $\mathbb{Q}$ и группа Галуа этого расширения равна $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(b) Покажите, что E — это расширение Галуа над $\mathbb{Q}$ и группа Галуа этого расширения равна группе кватернионов.