

Введение в теорию Галуа - семинар 5

13 октября 2025

- (1) Пусть ζ — это примитивный корень из 1 степени 7. Постройте промежуточное расширение $\mathbb{Q} \subset M_2 \subset \mathbb{Q}[\zeta]$, такое что $[M_2 : \mathbb{Q}] = 2$ и покажите, что $M_2 = \mathbb{Q}[\sqrt{-7}]$.
- (2) Пусть $a \in \mathbb{Q}, a > 0$, не является квадратом. Докажите, что тогда поле разложения L многочлена $X^4 - a \in \mathbb{Q}[X]$ является $\mathbb{Q}(\sqrt[4]{a}, i)$ и имеет группу Галуа D_4 . Опишите все подполя в L , используя соответствие Галуа и описание всех подгрупп в D_4 .
- (3) 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.
- (4) Циклотомические расширения \mathbb{Q} .
 - (a) Пусть p — простое число, $f \in \mathbb{Z}[X]$ — многочлен со старшим коэффициентом 1, такой что многочлен $f \pmod{p} \in \mathbb{F}_p[X]$ 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 $f(\alpha^p) = 0$. Докажите, что тогда $P(\alpha^p) = 0$.
 - (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 $R(X) = \prod_{i \in (\mathbb{Z}/n\mathbb{Z})^*} (X - \zeta^i)$.
 - (e) Пусть E — это поле разложения многочлена $X^n - 1$. Покажите $\text{Gal}(E/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$.
- (5) 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 $G = \text{Gal}(E/\mathbb{Q})$; тогда $G = (\mathbb{Z}/(p))^*$. 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 $\sigma \in G \setminus H$, 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:

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

- (6) Полная группа Галуа.
 - (a) Предположим, что транзитивная подгруппа $G \subset S_5$ содержит транспозицию. Докажите, что тогда $G = S_5$.

- (b) Пусть $P \in \mathbb{Z}[X]$ - многочлен степени 5 со старшим коэффициентом 1. Предположим, что P неприводим, и что P имеет ровно два невещественных комплексных корня. Покажите, что тогда группа Галуа поля разложения многочлена P равна S_5 .
- (c) Докажите, что группа Галуа поля разложения многочлена $P(X) = X^5 - 4X + 2$ равна S_5 .