Введение в теорию Галуа - семинар 2

15 сентября 2025

Пусть F — это подполе $\mathbb{R}$. Назовем **F-прямой** прямую в $\mathbb{R}\times\mathbb{R}$ проходящую через две точки, определенные над F. Такие прямые заданы уравнениями

$$ax+by+c=0, \quad a,b,c\in F.$$

Назовем **F-окружностью** окружность в $\mathbb{R}\times\mathbb{R}$, центр которой является F-точкой и радиус которой является элементом F. Такие окружности задаются уравнениями:

$$(x-a)^2+(y-b)^2=c^2, \quad a,b,c\in F$$

(1) Пусть $L\neq L'$ — это F-прямые и пусть $C\neq C'$ — это F-окружности.
  (a) $L\cap L'=\emptyset$ или состоит из единственной F-точки.
  (b) $L\cap C=\emptyset$ или состоит из одной или двух точек, определенных над полем $F[\sqrt{e}]$, где $e\in F$ и $e>0$.
  (c) $C\cap C'=\emptyset$ или состоит из одной или двух точек, определенных над полем $F[\sqrt{e}]$, где $e\in F$ и $e>0$.

(2) Вещественное число x называется **конструируемым над** F, если оно получается как длина некоторого отрезка, который можно построить, проводя F-прямые и F-окружности.
  (a) Если числа c и d — конструируемы, то числа $c+d, -c, cd,$ и $\frac{c}{d}(d\neq 0)$ — также конструируемы.
  (b) Если число $c>0$ — конструируемо, то $\sqrt{c}$ — тоже конструируемо.

(3) (a) Множество конструируемых чисел является полем.
  (b) Число α является конструируемым тогда и только тогда, когда оно содержится в подполе $\mathbb{R}$ такого вида:

$$\mathbb{Q}\left[\sqrt{a_1},\dots,\sqrt{a_r}\right], \quad a_i\in\mathbb{Q}\left[\sqrt{a_1},\dots,\sqrt{a_{i-1}}\right], \quad a_i>0.$$

(4) Если α — конструируемо, то α — это алгебраическое число над $\mathbb{Q}$, и $[\mathbb{Q}[\alpha]:\mathbb{Q}]=2^n$ для некоторого $n\in\mathbb{N}$.

(5) Число $\sqrt[3]{2}$ не является конструируемым над $\mathbb{Q}$.

(6) Существуют числа α, для которых невозможно произвести трисекцию угла α с помощью циркуля и линейки.

(7) (a) Если p — простое число, то многочлен $X^{p-1}+\cdots+1$ неприводим. Таким образом, поле $\mathbb{Q}\left[e^{2\pi i/p}\right]$ имеет степень $p-1$ над $\mathbb{Q}$.
  (b) Докажите, что если правильный p-угольник построим[1], то $(p-1)/2=2^k$ для некоторого $k\in\mathbb{N}$.

(8) Посчитайте $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]$.

(9) (a) Проверьте, что $\mathbb{Q}(\sqrt{2})$ содержится в $\mathbb{Q}(\sqrt{2}+\sqrt{3})$, и найдите $[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}(\sqrt{2})]$.

[1] Обратное тоже верно, мы это обсудим позже.

(b) Пусть $K = \mathbb{Q}(\sqrt{2})$. Найдите $[K(\sqrt[3]{2}) : \mathbb{Q}]$ и $[K(\sqrt[3]{2}) : K]$.

(10) Пусть ζ — некоторый первообразный корень степени n из единицы. Расширение $\mathbb{Q}(\zeta)$ называется **круговым полем**.

(a) Найдите степень кругового поля $\mathbb{Q}(\zeta)$, где ζ — это первообразный корень степени n из единицы, для $n = 3, 4, 5$ и 6.

(b) Докажите, что степень расширения $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ равна функции Эйлера $\varphi(n)$.