Лекция 9 | НМУ | Алгебра-1

В прошлый раз мы доказали соответствие Галуа: $\mathbb{F}/\mathbb{K}$ – конечное расширение Галуа. с $G = Gal(\mathbb{F}/\mathbb{K})$.

(1) $\{$ Подгруппы в $Gal(\mathbb{F}/\mathbb{K})\}$ $\underset{Gal(\mathbb{F}/\mathbb{L}) \hookleftarrow \mathbb{L}}{\overset{H \hookrightarrow \mathbb{F}^H}{\rightleftarrows}}$ $\{$ Подполя $\mathbb{K} \subset \mathbb{L} \subset \mathbb{F}\}$

(2) $\{H_1 \subset H_2\} \longleftrightarrow \{\mathbb{F}^{H_1} \supset \mathbb{F}^{H_2}\}$.

(3) $(gHg^{-1}) \longleftrightarrow g(\mathbb{F}^H)$.

(4) $H \lhd G \longleftrightarrow \mathbb{F}^H/\mathbb{K}$ – расширение Галуа

Д-во (4) $gHg^{-1} = H \Leftrightarrow H \lhd G \Rightarrow \forall g \in Aut(\mathbb{F}/\mathbb{K})$ имеем $g(\mathbb{F}^H) = \mathbb{F}^H$,

Значит G действует на $\mathbb{F}^H$ – автоморфизмами, $(\mathbb{F}^H)^G = \mathbb{K}$

$\Rightarrow \mathbb{F}^H/\mathbb{K}$ – расширение Галуа степени $(G:H) = \#G/H$.

Имеем $G/H = Aut(\mathbb{F}^H)$.

Приложения

Построения циркулем и линейкой.

Как построить заданный угол?

Ну или правильный n-угольник.

Нельзя построить

3, 5, ~~4~~, ~~6~~, ~~15~~, 17

Задача о построении 17-ти угольника была решена Гауссом

Определение Назовём (вещественное) число α – построяемым (constructible), если отрезок длины α можно построить циркулем и линейкой.

Замечание Мн-во построяемых чисел $\mathbb{F}$ образуют поле.

В реальности мы умеем строить прямые

$$ax + by + c = 0 \quad a, b, c \in \mathbb{F}$$

$$(x-\alpha)^2 + (y-\beta)^2 = r^2 \quad \alpha, \beta, r^2 \in \mathbb{F}.$$

Хотим решить квадратное уравнение.

$\Leftrightarrow$ Рассмотреть $\mathbb{F}(\sqrt{e})$.

Теор. $\alpha \in \mathbb{R}$ – построимо $\Leftrightarrow \exists\, F \subset \mathbb{R}$, $F = \mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n})$, $a_i \in \mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_{i-1}})$ / $\mathbb{R}$ ✗.

$\Leftarrow$ $\alpha \in F/\mathbb{Q}$, т.ч. $F/\mathbb{Q}$ – расширение Галуа степени 2^k.

Д-во: Первая равносильность по определению.

Вторая $\Leftarrow$ Имеем

$G = \mathrm{Gal}(F/\mathbb{Q})$ и $\#G = 2^k \Rightarrow G$ – разрешима

и $\exists$ ряд Жордана – Гёльдера

$1 = G_0 \subset G_1 \subset G_2 \subset \dots \subset G_k = G$, т.ч. $\#G_i / G_{i-1} = 2$.

$\Rightarrow F = F_0 \supset F_1 \supset \dots \supset F_k = \mathbb{Q}$.

и $[F_i : F_{i+1}] = 2$. $\Rightarrow F_i = F_{i+1}(\sqrt{a_i})$. –

т.к. у неприв. мн-на $x^2 - ax + b = 0$ $\exists$ замена

$y = (x - \frac{a}{2})$ т.ч. $y^2 - c^2 = 0$.

Сл-ие Если α – построимо, то $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^s$.

Сл-ие $\cos\frac{2\pi}{p}$ – построимо $\Leftrightarrow p = 2^n + 1$

Д-во: имеем $\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right) : \mathbb{Q}\right] = \frac{1}{2}[\mathbb{Q}(\zeta) : \mathbb{Q}] = \frac{p-1}{2}$.

Более того $\mathbb{Q}(\zeta)/\mathbb{Q}$ – расширение Галуа с группой Галуа – $\mathbb{Z}/(p-1)\mathbb{Z}$.

Почему циклическая, аккуратно обсудим в следующем сюжете.

Циклотомические расширения

(когда группа Галуа – циклическая?).

Теор. $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = (\mathbb{Z}/N\mathbb{Z})^*$, если $\zeta = e^{(2\pi i/N)}$.

Вообще $F(\zeta)/F$ – расширение Галуа с $\mathrm{Gal}(F(\zeta)/F) \hookrightarrow \mathbb{Z}/N\mathbb{Z}$.
если $\mathrm{char} F = 0$, то

Д-во: Пусть $\sigma \in \mathrm{Aut}(\mathbb{Q}(\zeta)/\mathbb{Q})$, поскольку $\Phi_n(\zeta) = \prod_{(k,n)=1} (x - \zeta^k)$.

имеем расширение Галуа $\Rightarrow \forall\, \sigma \in \mathrm{Aut}$ $\sigma(\zeta) = \zeta^k$ и этим σ определяется.

Если $\zeta \in \mathbb{K}$, $\mathbb{F} = \mathbb{K}(\sqrt[n]{a})$, $\mathrm{char}(\mathbb{K}) \nmid n$.

Не очень важно, какой минимальной ми-л у $\sqrt[n]{a}$, важно что этим эл-ом порождается расширение $\mathbb{F}/\mathbb{K}$ и $\sigma \in \mathrm{Aut}(\mathbb{F}/\mathbb{K})$ должен переводить $\sqrt[n]{a} \to \zeta\sqrt[n]{a}$. $\zeta^n = 1$.

$\mathrm{Gal}(\mathbb{F}/\mathbb{K}) \subset \mathbb{Z}/n\mathbb{Z}$

$\sigma : \sqrt[n]{a} \to \zeta\sqrt[n]{a}$, $\sigma^2(\sqrt[n]{a}) = \zeta^2\sqrt[n]{a}$

имеем вложение $\mathrm{Gal}(\mathbb{F}/\mathbb{K}) \hookrightarrow \mathbb{Z}/n\mathbb{Z}$

$\sigma \longmapsto \dfrac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}$.

Теор. Если $f(x)$ -разрешимо в радикалах,

то $\mathbb{Q}_f/\mathbb{Q}$ -расширение Галуа с разрешимой группой.

Д-во:

($\Rightarrow$)

$\mathbb{F}'$

$\mathbb{Q} \subset \mathbb{Q}(\zeta) \subset \mathbb{Q}(\zeta, \sqrt[n]{a_1}) \subset (\sqrt[n]{a_2}) \subset \dots$

Gal - разрешима.

$$\mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{F}/\mathbb{Q}) \Big/ \mathrm{Gal}(\mathbb{F}/\mathbb{Q}_f)$$

$\uparrow$ разрешима.

($\Leftarrow$)

Пусть $\langle\sigma\rangle = \mathrm{Gal}(\mathbb{F}/\mathbb{Q})$, $\zeta = e^{\frac{2\pi i}{n}}$.

Если мы найдём эл-т $\sigma\alpha = \zeta^{-1}\alpha$ имеет $\alpha, \sigma\alpha, \sigma^2\alpha, \dots, \sigma^{n-1}\alpha$ -различны $\Rightarrow M_\alpha(x) = (x^n - \alpha^n)$.

$[\mathbb{F}:\mathbb{Q}] = n$ из (теор. Дедекинда) $\sum \zeta^i \sigma^i \neq 0 \Rightarrow \exists \alpha = \sum_{i=0}^{n-1} \zeta^i \sigma^i(\gamma)$.

Но $\sigma\alpha = \zeta^{-1}\alpha$.

Будет в следующий раз.

Сл-ие Ур-ия степеней 2, 3, 4 разрешимы в радикалах,

а вот ур-ие степени ≥ 5 может не быть.

Д-во: S_2, S_3, S_4 – разрешимы

A_5, S_5 – нет

↑ первая неразрешимая группа.

Остаётся показать, что такие мн-ки существуют.

Это не совсем просто и требует выхода в char k = p.

Замечание

Когда $G_f \subset A_n$. $f(x) = x^n + a_1 x^{n-1} + \dots + a_n = \prod (x - \alpha_i)$

$$\Delta(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j),$$

Мы знаем, что $\Delta(f)^2 = D(f) \in k$.

Если $\sigma \in Gal(f) \subset S_n$, то $\sigma(\Delta(f)) = (-1)^\sigma \Delta(f)$.

Если $G_f \subset A_n$, то сопряжённые к $\Delta(f)$ только $\Delta(f) \in k$

иначе $\Delta(f), -\Delta(f)$

Имеем

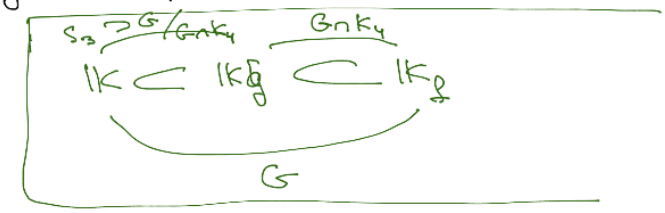
$$\begin{array}{ccccc} k & \subset & k(\Delta(f)) & \subset & k_f \\ \updownarrow & & \updownarrow & & \updownarrow \\ G & \supset & G \cap A_n & \supset & e \end{array}$$

Или $D(f)$ – квадрат в k,

или G_f содержит нечётные эл-ты.

Для $n = 4$ нужно проделать аналогичную историю

$e \subset K_4 \subset A_4 \subset S_4$



Нужно $K_4 = \{(12)(34), (13)(24), (14)(23)\}$.

Имеем $\alpha = \alpha_1\alpha_2 + \alpha_3\alpha_4$

рациональные эл-ты $\beta = \alpha_1\alpha_3 + \alpha_2\alpha_4$

$\gamma = \alpha_1\alpha_4 + \alpha_2\alpha_3$

Имеем $\overset{g(x)}{\Rightarrow} (x - \alpha)(x - \beta)(x - \gamma) \in k[x]$

можно явно выразить.

резольвента