# Лекция 12 мая (первая половина)

$\mathbb{F} \supset \mathbb{k}$ - расширение Галуа

$G = Gal(\mathbb{F}/\mathbb{k}) = Aut_{\mathbb{k}} \mathbb{F}$

Имеется каноническая биекция между полями $\mathbb{L}$ : $\mathbb{k} \subset \mathbb{L} \subset \mathbb{F}$ и подгруппами $H < G$.

$\mathbb{L} \to Aut_{\mathbb{L}} \mathbb{F} = Gal(\mathbb{F}/\mathbb{L}) < G$

($\mathbb{L} < \mathbb{F}$ - автоматически расширение Галуа)

$H < G \longrightarrow \mathbb{F}^H \subset \mathbb{F}$

расширение Галуа с группой Галуа $H$.

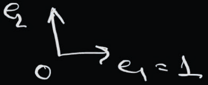
$\mathbb{L} \supset \mathbb{k}$ - расширение Галуа $\Leftrightarrow H \triangleleft G$

$Gal(\mathbb{L}/\mathbb{k}) = G/H.$

соответствие обращивает включения и переводит пересечение подгрупп в композиты Полей, а пересечения полей - в группу, порождённую группами этих полей

Пример: построение циркулем и линейкой на евклидовой плоскости.

$\mathbb{R}^2 \simeq \mathbb{C}$

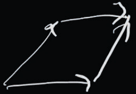


Даны точки $0, 1 \in \mathbb{C}$.

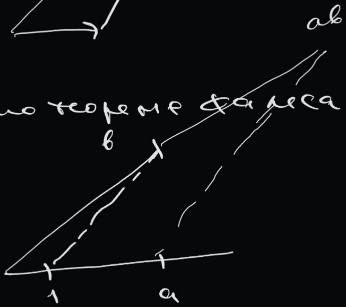
Какие точки $z \in \mathbb{C}$ можно построить циркулем и линейкой?

---

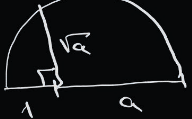
$z_1$ и $z_2$ можно построить $\Rightarrow$ $z_1 \pm z_2$, $z_1 z_2$, $z_1/z_2$ (при $z_2 \neq 0$) тоже можно построить.



$a, b \in \mathbb{R}$ $ab$ – по теореме Фалеса если есть 0 и 1.



Можно построить $\sqrt{a}$ если есть 0 и 1



Если поле $\mathbb{L}$ получается

башней квадратичных расширений

$$\mathbb{Q} < \mathbb{L}_1 < \dots < \mathbb{L}_n = \mathbb{L}$$

$$\mathbb{L}_{i+1} = \mathbb{L}_i[\sqrt{a_i}] = \frac{\mathbb{L}_i[x]}{x^2-a_i} \quad a_i \in \mathbb{L}_i \setminus \mathbb{L}_i^2$$

то любой элемент поля $\mathbb{L}$ можно построить циркулем и линейкой

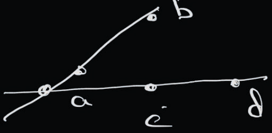
Утв. Наоборот: если число $\xi$ можно построить циркулем и линейкой, то $\xi \in \mathbb{L}$, где $\mathbb{L}$ - получается башней квадратичных расширений, причём

$\forall i \ \overline{\mathbb{L}_i} = \mathbb{L}_i$ $\qquad (\mathbb{L}_i < \mathbb{C})$ $\circlearrowleft$ $z \mapsto \bar{z}$

Док-во: $\mathbb{Q} < \mathbb{Q}[i] = \mathbb{L}_1$

Построение $\xi$ распадается на шаги:

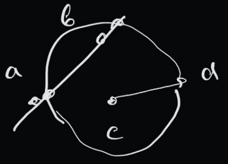
Даны $a, b, c, d$



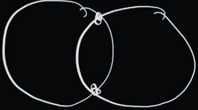
(1) строим $(ab) \cap (cd)$

(2) строим $(ab) \cap S(c,d)$

окружность с центром $c$ и радиусом $[c,d]$



(3) строим $S(a,b) \cap S(c,d)$



$a, b, c, d \in \mathbb{L}$,

$(ab) \cap (cd) \in \mathbb{L}$

по правилу Крамера.

$S(c,d)$ с $(ab)$ или с $S(a,b)$

$\mathbb{L} = \overline{\mathbb{L}}$

$$(z-c)(\bar{z}-\bar{c}) = (d-c)(\bar{d}-\bar{c})$$

подставить $z = a + t(b-a)$

параметрическое уравнение

прямой $(ab)$ при $t \in \mathbb{R}$

окружности $S(a,b)$ при $t \in \mathbb{U}_1 \subset \mathbb{C}$

$\bar{t} = t$

$\bar{t} = t^{-1}$

$$(a+t(b-a)-c)(\bar{a}+t(\bar{b}-\bar{a})-\bar{c})$$

единичная окружность

$$(a+t(b-a)-c)(\bar{a}+t^{-1}(\bar{b}-\bar{a})-\bar{c}) = (d-c)(\bar{d}-\bar{c})$$

в случае 1 получаем квадратное уравнение на $t$ с веществ. коэф-тами и $\mathbb{L}$

в случае 2 " ―――――――――――― "

коэфф-ты и вещественны по дискриминант

будет веществ.

D - дискриминант

в одних случаях $\quad \underline{\alpha} t^2 + \underset{\mathbb{R}}{\underset{\cap}{\beta}} t + \underline{\underline{\alpha}}$

корни лежат в $\mathbb{L}[\sqrt{D}]$

$\pm i\sqrt{|D|}$

воспроизводим предположение индукции.

---

Лемма: Расширение Галуа $\mathbb{E} \supset \mathbb{Q}$ содержится в башне квадратичных расширений $\iff \deg(\mathbb{E}/\mathbb{Q}) = 2^m$

Док-во $(\Rightarrow)$ $\mathbb{Q} \subset \mathbb{E} \subset \mathbb{L} = \mathbb{L}_n \supset \dots \supset \mathbb{L}_1 \supset \mathbb{Q}$

$\deg(\mathbb{F}/\mathbb{Q})$ делит $\deg(\mathbb{L}/\mathbb{Q}) = 2^n$

$$\Downarrow$$

$$\deg(\mathbb{E}/\mathbb{Q}) = 2^k$$

$(\Leftarrow)$

$\deg(\mathbb{E}/\mathbb{Q}) = 2^k \Rightarrow \mathrm{Gal}(\mathbb{E}/\mathbb{Q})$ это 2 группа.

$$G \triangleright G_1 \triangleright G_2 \triangleright \dots \triangleright G_n = e$$

Ряд Жордана Гёльдера

$G_i/G_{i+1}$ — простые. $\boxed{\mathbb{Z}/(2)}$

по соотв. Галуа

$$\mathbb{Q} = \mathbb{L}_0 \subset \dots \subset \mathbb{L}_{n-1} \subseteq \mathbb{E}$$

все расширения квадратичные с группой

$Z/(2)$.

---

Если корень неприводимого многочлена $f(t) \in \mathbb{Q}[t]$ можно построить циркулем и линейкой то тогда все корни этого многочлена можно построить циркулем и линейкой и степень поля разложения $f$ равна $2^k$

Наоборот если степень поля разложения $f$ равна $2^k$, то все корни строятся циркулем и линейкой

---

Пусть $\mathbb{L}_f$ - поле разложения $f$, пусть $[\mathbb{L}_f : \mathbb{Q}] = 2^m$ $\quad \mathbb{L}_f \supset \mathbb{Q}$ - расширение Галуа.

По лемме $\mathbb{L}_f \subset \mathbb{L} \supset \mathbb{L}_{n-1} \supset \ldots \supset \mathbb{L}_1 \supset \mathbb{Q}$

$\Downarrow$

все элементы $\mathbb{L}_f$ можно построить циркулем и линейкой.

**Наоборот.** Пусть какой-то корень $\theta$ многочлена $f$ можно построить циркулем и линейкой.

Нужно вложить $\mathbb{L}_f$ ← поле разложения $f$ в какую-нибудь башню квадратичных расширений

$$\mathbb{Q}[\theta] < \mathbb{L} = \mathbb{L}_n \supset \mathbb{L}_{n-1} \supset \dots \supset \mathbb{L}_1 \supset \mathbb{Q}.$$

$$\mathbb{L}_{i+1} = \mathbb{L}_i[\sqrt{a_i}]$$

Пусть $\theta'$ — другой корень. $\exists$ вложение

$$\begin{tikzcd}
\mathbb{Q}[\theta] \arrow[r, "\varphi"] \arrow[d, phantom, "\cap"] & \mathbb{L}_f \arrow[r, phantom, "\subset"] & \mathbb{C} \\
\mathbb{L} \arrow[urr, bend right] & &
\end{tikzcd}$$

$$\theta \longmapsto \theta'$$

$\exists \tilde{\varphi}$ $\mathbb{L} \hookrightarrow \mathbb{C}$

$\theta \to \theta'$

Применив $\tilde{\varphi}$ к башне $\mathbb{L}$ получим башню квадратичных расширений

$$\theta' \in \underset{\tilde{\varphi}(\mathbb{L})}{\underset{\parallel}{\mathbb{L}'}} \supset \underset{\tilde{\varphi}(\mathbb{L}_{n-1})}{\underset{\parallel}{\mathbb{L}'_{n-1}}} \supset \dots \supset \mathbb{L}'_1 \supset \mathbb{Q}$$

$$\mathbb{L}'_{i+1} = \mathbb{L}'_i[\sqrt{a_i'}]$$

$a_i' = \bar{\varphi}(a_i)$

$\theta, \theta' \in \mathbb{L}'$

$\subset \mathbb{L}_{n-1} \subset \mathbb{L} \subset \mathbb{E}_1 \subset \dots \subset \mathbb{E}_m = \mathbb{L}'$

на каждом шагу к предыдущему полю добавляется не лежащий в нём $\sqrt{a_i'}$

} по индукции получаем башню квадратичных расширений, содержащую все корни $f$ $\Rightarrow$ содержа. уже поле разложения $\mathbb{L}_f$. $\Rightarrow$ по предложению $\deg(\mathbb{L}_f / \mathbb{Q}) = 2^k$

---

$\deg f \mid \deg \mathbb{L}_f \Rightarrow$ если $\deg \mathbb{L}_f / \mathbb{Q} = 2^m$

$$\Downarrow$$

$\deg f = 2^n$.

$\frac{\mathbb{Q}[x]}{(f)} \subset \mathbb{L}_f$

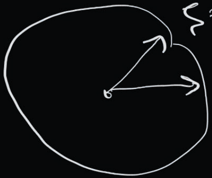
Следствие: если $\deg f \neq 2^n$ и $f$ неприводим $\Rightarrow$ корни $f$ нельзя построить циркулем и линейкой.

Следствие! Нельзя удвоить куб (построить куб вдвое большего объёма чем данный)

$x^3-2=0$
неприводим

- Нельзя построить правильный 7-угольник

$\zeta = e^{2\pi i/7}$



$$\Phi_7(x) = \frac{x^7-1}{x-1} = x^6+x^5+\dots+1$$

неприводим

- Нельзя разделить на 3 равные части угол $\underset{3\varphi}{\underset{\parallel}{\pi/3}}$: подсказка

$$\cos 3\varphi = \cos^3\varphi - \cos\varphi\cdot \underset{\substack{\parallel\\(1-\cos^2)}}{\sin^2\varphi}\cdot 3$$

кубическое уравнение на $\cos\varphi$

---

Если даны не только 0 и 1, а ещё какие-то, то что тогда?

Можно считать что данные точки образуют подполе $\mathbb{K} < \mathbb{C}$.

поле побочных (данных чисел) иррациональностей.

Упр.: Показать, что корень неприводимого многочлена $f \in \mathbb{Q}[x]$ можно построить циркулем и линейкой $\iff [\mathbb{L}_f\mathbb{K} : \mathbb{K}] = 2^m$

$\mathbb{L}_f$ - поле разложения $f$ над $\mathbb{Q}$, $\mathbb{L}_f\mathbb{K}$ - композит. $=$ $\mathbb{Q}$-линейная оболочка произведений $\varsigma\xi$, $\varsigma \in \mathbb{L}_f$, $\xi \in \mathbb{K}$,

Теорема о побочных иррациональностях:

$\Bbbk < \mathbb{E}, \mathbb{L} < \mathbb{K}$ - алгебраически замкнуто

Если расширение $\mathbb{E} > \Bbbk$ конечно и является расширением Галуа, то $\mathbb{E}\mathbb{L} > \mathbb{L}$ тоже конечно и является расширением Галуа и $\mathrm{Gal}(\mathbb{E}\mathbb{L}/\mathbb{L})$

$\cong$

группе, соотв. по Галуа промеж. полю $\mathbb{L} \cap \mathbb{E}$ $\longrightarrow$ $H = \mathrm{Gal}(\mathbb{E}/\mathbb{E} \cap \mathbb{L})$

$\Bbbk < \mathbb{E}$ $\quad$ $\Bbbk < \underline{\mathbb{L} \cap \mathbb{E}} < \mathbb{E}$

$\overset{\cap}{\mathbb{L}}$ $\overset{\cap}{\mathbb{F}\mathbb{L}}$ $\overset{\updownarrow}{H < \mathrm{Gal}(\mathbb{F}/\mathbb{K})}$

---

Док-во: $\mathbb{F}\mathbb{L} \supset \mathbb{L}$ – конечное расширение Галуа.

$\boxed{\mathbb{K} < \mathbb{F}}$ – сепараб (нормально)

$\Downarrow$

$\boxed{\mathbb{L} < \mathbb{F}\mathbb{L}}$ – сепараб (нормально)

сепарабел. $\Leftrightarrow$ минимальный? многочлен любого $\theta \in \mathbb{F}$ сепарабелен (все корни различны в $\overline{\mathbb{K}} < \mathbb{K}$)

$\boxed{\mu \in \mathbb{F}\mathbb{L}}$ его минимальный? многочлен над $\mathbb{L}$ делит миним. многочлен $\mu$ над $\mathbb{K}$

---

нормальность – все вложения над $\mathbb{K}$ $\mathbb{F} \hookrightarrow \overline{\mathbb{K}}$ имеют один и тот же образ $\mathbb{F} \subset \overline{\mathbb{K}}$

$\mathbb{E}\mathbb{L} \overset{\varphi}{\hookrightarrow} \overline{\mathbb{K}}$ тоже имеют один и тот же обр.

над $\mathbb{L}$

и

$\mathbb{L}$ - линейно

$\mathbb{E} \xhookrightarrow{\varphi|_{\mathbb{E}}} \overline{\mathbb{K}}$

тождественное на $\mathbb{L}\cap\mathbb{E}$

все образы совпадают с $\mathbb{EL}$ поскольку образы всех $\varphi|_{\mathbb{F}}$ совпадают с $\mathbb{E}$.

$\mathbb{EL}$ порождается над $\mathbb{L}$ алгебраически теми же элементами, что $\mathbb{E}$ над $\mathbb{K}$

---

Сравнение групп Галуа

$\mathbb{E} \supset \mathbb{K}$ - $\mathbb{E}$ - поле разложения многочлена $f \in \mathbb{K}[x]$

пусть у $\mathbb{F}$ корни $\theta_1, \dots, \theta_m$

они же порождают $\mathbb{LF}$ над $\mathbb{L}$

$\boxed{\mathbb{E}} = \mathbb{K}[\theta_1 \dots \theta_m] \ni \varphi$

$\boxed{\mathbb{LF}} = \mathbb{L}[\theta_1 \dots \theta_m] \ni \varphi \Leftrightarrow \varphi$ $\mathbb{L}$-линейн

$\Uparrow$

$\varphi|_{\mathbb{L}\cap\mathbb{F}} = \mathrm{Id}$

---