Лекция 19 мая (вторая половина)

Наоборот: Пусть $\mathbb{F} \supset \mathbb{k}$ - циклическое расширение Галуа. Тогда $\mathbb{F} = \frac{\mathbb{k}[x]}{x^n - b}$ где $x^n - b$ - неприводим, и $\mathbb{F}$ - это поле разложения этого многочлена (при условии, что $\mathbb{k}$ содержит все $\sqrt[n]{1}$)

Док-во: Фиксируем образующую $g \in \mathrm{Gal}(\mathbb{F}/\mathbb{k})$, первообразный корень $\xi \in \mu_n(\mathbb{k})$. Пусть $|\mathrm{Gal}(\mathbb{F}/\mathbb{k})| = n$

$$L_{g,\xi} = \sum_{i=0}^{n-1} \xi^i g^i : \mathbb{F} \to \mathbb{F}$$

$\mathbb{k}$ - линейное отображение

$g^i : \mathbb{F} \to \mathbb{F}$

$L_{g,\xi} \neq 0.$

$\underline{1, g, g^2, \dots, g^{n-1}}$, линейно независимы.

каждое $g^i : \mathbb{E}^\times \longrightarrow \mathbb{E}^\times$ – мультипликативный характер абелевой группы $\mathbb{E}^\times$ со значениями в поле $\mathbb{E}$

$$g L_{g,\xi} = g + \xi g^2 + \dots + \xi^{n-1} \cdot \underset{\substack{\shortparallel \\ 1}}{g^n} =$$

$$= \underset{\substack{\shortparallel \\ \xi^{n-1}}}{\xi^{-1}} L_{g\xi}$$

$$\boxed{(g-\xi^{-1})L_{g\xi}=0} \quad \overset{\neq 0}{L_{g\xi}}(\mathbb{E}) <$$

собственном подпр-ве g с собств. значением ξ^{-1}

$\exists\, a \in \mathbb{E} : ga = \xi^{-1} a$ ненулевой собств. вектор.

$a, \xi a, \dots, \xi^{n-1} a$ – полная Gal-орбита a

$$\prod_{i=0}^{n} (x - \xi^i a) = x^n - a^n \in \mathbb{K}[x]$$

↖ неприводим с к-тами из $\mathbb{K}$.

$b = a^n \in \mathbb{k}$

$$\frac{\mathbb{k}[x]}{x^n - b} \text{ — поле разложения } \mathbb{E}$$

$$/\!/$$

$$\mathbb{E}$$

Теорема Абеля:

Расширение Галуа $\mathbb{E} \supset \mathbb{k}$ называется разрешимым, если

$Gal(\mathbb{F}/\mathbb{k})$ имеет циклические факторы Жордана-Гёльдера.

(т.е. группа разрешима).

$$\Updownarrow$$

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright G_3 \dots \triangleright G_m = e$$

все факторы G_i / G_{i+1} абелевы.

$\mathbb{F}/\mathbb{k}$

Теор. Если группа Галуа разрешима, то до поля $\mathbb{E}$ можно дотянуться башней циклических расширений ? (в предположении, что $\operatorname{char} \mathbb{k} = 0$ или $\operatorname{char} \mathbb{k}$ не делит порядок ни одного из факторов Ж-Г.).

$$\mathrm{Gal} \rhd G_1 \rhd G_2 \rhd \dots \rhd G_n = e$$

$$G_i / G_{i+1} = \mathbb{Z}/(p_i)$$

$$\mathbb{k} < \mathbb{L}_1 < \mathbb{L}_2 < \dots < \mathbb{L}_n = \mathbb{E}$$

$$L_{i+1} = \mathbb{L}_i[x]/(x^{p_i} - a) = \mathbb{L}_i[\sqrt[p_i]{a_i}]$$

где $x^{p_i} - a$ – неприводим

Теорема ? : Если какой-то корень неприводимого многочлена $f \in \mathbb{k}[x]$

выражается в радикалах (т.е. получается при помощи сложения, умножения, вычитания, деления и извлечения корней из элементов поля $\mathbb{K}$), то все корни выражаются в радикалах и группа Галуа $\mathbb{L}/\mathbb{K}$ разрешима.

Док-во: Фиксируем $\overline{\mathbb{K}} \supset \mathbb{K}$

Пусть $\alpha \in \overline{\mathbb{K}}$ выражается в радикалах,

$$\alpha \in \mathbb{L} \supset \mathbb{L}_{n-1} \supset \dots \supset \mathbb{L}_1 \supset \mathbb{K}$$

$$\mathbb{L}_{i+1} = \mathbb{L}_i[\sqrt[n_i]{a_i}] = \mathbb{L}_i[x] / \underbrace{x^{n_i} - a_i}_{\leftarrow}$$

неприводим

Надо показать, что $\mathbb{L} \subset \mathbb{L}'$ с разрешимой группой Галуа (тогда

$$\mathrm{Gal}(\mathbb{L}/\mathbb{K}) = \mathrm{Gal}(\mathbb{L}'/\mathbb{K}) / \mathrm{Gal}(\mathbb{L}', \mathbb{L})$$

фактор разрешимой группы разрешим)

упражнение.

$L'_0 \supset k$: L'_0 содержит все корни из 1 всех степеней, равных степеням радикалов, участвующих в разложении α.

$L'_{i+1} \supset L'_i$: поле разложения многочлена $\underline{\underline{x^{n_i} - a_i}}$ над L'_i

$$\begin{tikzcd}
k \arrow[r, phantom, "\subset"] & L'_0 \arrow[r, phantom, "\subset"] & L'_1 \arrow[r, phantom, "\subset"] \arrow[d, phantom, "\cup"] & L'_2 \arrow[r, phantom, "\subset"] \arrow[d, phantom, "\cup"] & \dots & L'_n \arrow[d, phantom, "\cup"] \\
 & & L_1 & L_2 & & L
\end{tikzcd}$$

циклическое расширение

Корень выражается в радикалах $\Leftrightarrow$ группа Галуа разрешима (если $\operatorname{char} k = 0$).

Пример (теорема Абеля)

Общее уравнение степени $\underline{n}$,

k — любое поле $\operatorname{char} k = 0$

$\mathbb{E} = \mathbb{k}(a_1, \dots, a_n)$. – поле рациональных функций

$t^n + a_1 t^{n-1} + \dots + a_n = f$ – общий? многочлен степени n над $\mathbb{k}$

$\cap$

$\mathbb{E}[t]$

$a_i \longrightarrow \alpha_i \in \mathbb{k}$

$$\boxed{\begin{array}{c} t^2 + pt + q \\ \dfrac{-p \pm \sqrt{p^2 - 4q}}{2} \end{array}}$$

Пусть $t_1, \dots, t_n$ корни f в поле разложения. $\mathbb{L}$

$\mathbb{L}$ как алгебра порождается $t_1, \dots, t_n \Rightarrow$ среди них можно выбрать базис трансцендентности $\mathbb{L}$ над $\mathbb{k}$.

$\mathbb{L} \supset \mathbb{E}$ $\quad$ $\boxed{\operatorname{tr\,deg} \mathbb{E}/\mathbb{k} = n}$

$\operatorname{tr\,deg} \mathbb{L}/\mathbb{k} \geq n \Rightarrow t_1, \dots, t_n$ – базис трансцендентности $\mathbb{L}$ над $\mathbb{k}$ (в частности корни различны, f сепарабелен)

$\mathbb{L} \supset \mathbb{E}$ – расширение Галуа.

$t_1 \ldots t_n$ – алг. независимы, любая перестановка продолжается до автоморфизма $\mathbb{L}/\mathbb{k}$ $e_i(t_1 \ldots t_n) = a_i$

$$\mathrm{Gal}(\mathbb{L}/\mathbb{F}) = S_n$$

при $n \geq 5$ она не разрешима

$$A_n \lhd S_n$$

Нет универсальной формулы решающей уравнение степени ≥ 5.

Зам Не смотря на отсутствие общей формулы некоторые конкретные уравнения решаются в радикалах (если $\mathrm{Gal}\, f/\mathbb{k}$ разрешима).

- Экзамен будет в воскресенье 22 мая в 10:00 на сайте курса.

Решения прислать до 14:00 на gorod@itep.ru.