НМУ | Алгебра-2 | Лекция 10 |

Т-ма (о примитивном эл-те :)

Пусть $\mathbb{F}/_{\mathbb{K}}$ - конечное сепарабельное расширение, тогда $\exists \alpha \in \mathbb{F} : \mathbb{F} = \mathbb{K}(\alpha)$.

Д-во Считаем, что $\mathbb{K}$ - бесконечно, т.к. для конечных всё умеем д-ть.

Пусть $\mathbb{F} = \mathbb{K}(\alpha, \beta) = \mathbb{K}[\alpha, \beta]$.

Р-м сопряженные $\alpha_1, \dots, \alpha_n$ - корни $\mu_\alpha(x)$ ⟸ минимальные мн-ны.
$\beta_1, \dots, \beta_m$ - корни $\mu_\beta(x)$

Подберём число $c \in \mathbb{K}$ так, чтобы все числа $\alpha_i + c\beta_j$ были различны.

Это можно сделать т.к. поле бесконечное

$$\alpha_i + c\beta_j = \alpha_{i'} + c\beta_{j'} \iff c = \frac{\alpha_{i'} - \alpha_i}{\beta_j - \beta_{j'}}.$$

Тогда утверждается, что $\mathbb{F} = \mathbb{K}(\alpha + c\beta)$. $\gamma := \alpha + c\beta$.

Р-м многочлен $\mu_\beta(x)$ и $\mu_\alpha(\gamma - cx)$ они имеют общий корень β.

$$\Rightarrow \mu_\alpha(\gamma - cx) \,\vdots\, (x - \beta).$$

$$\Rightarrow \gcd(\mu_\beta(x), \mu_\alpha(\gamma - cx)) \in \mathbb{F}(\gamma)[x]$$

$$(x-\beta) =$$

$$\Rightarrow \beta \in \mathbb{F}(\gamma) \Rightarrow \alpha = \gamma - c\beta \in \mathbb{F}(\gamma).$$

По индукции получаем, что если $\mathbb{F}/_{\mathbb{K}}$ - конечное, сепарабельное, и $\mathbb{F} = \mathbb{K}(\alpha_1, \dots, \alpha_k) = \mathbb{F}[\cancel{\alpha_1}\gamma_2, \dots, \gamma_{k-1}] = \mathbb{F}(\gamma_1)$. $\square$.

Замечание γ можно выбрать в виде $\alpha_1 + c_1\alpha_2 + \dots + c_k\alpha_k$, $c_i \in \mathbb{K}$.

Сл-ие Если $\mathbb{F}/_{\mathbb{K}}$ - расширение Галуа с группой Галуа $G = \{g_1, \dots, g_n\}$ то $\exists \alpha \in \mathbb{F} : g_1\alpha, g_2\alpha, \dots g_n\alpha$ - образуют базис $\mathbb{F}/_{\mathbb{K}}$

$$\mathbb{F} = \mathbb{K}(\alpha) = \mathbb{K}[x]/_{\mu_\alpha(x)}.$$

Поэтому $\mathbb{F}$ - является $\mathbb{K}$-лин. пр-ем группы G изоморфным $\mathbb{K}G$.
(регулярному предст.)

Замечание Любое сепарабельное расширение можно вложить в Галуа.

$\mathbb{F} = \mathbb{K}(\alpha_1, \dots, \alpha_s)$ $\quad \tilde{\mathbb{F}} := \mathbb{K}_f$, $f = \mu_{\alpha_1}(x) \dots \mu_{\alpha_s}(x)$

Зам. $\mathbb{F} = \mathbb{K}(\alpha)$, то лишь конечное число промежуточных полей.

$\overset{\cup}{\mathbb{L}}$? тогда $\mu_\alpha^{\mathbb{L}}(x) = a_0 + a_1 x + \dots + a_m$. $\mu_\alpha^{\mathbb{K}}(x) \mid \mu_\alpha$

тогда $[\mathbb{F} : \mathbb{L}] = m$.

$\mathbb{L} \supset \mathbb{L}' = \mathbb{K}(a_0, \dots, a_m) \Rightarrow [\mathbb{F} : \mathbb{L}'] = m$.

Теор. (Дедекинда о лин. нез-ти характеров)

Пусть $\mathbb{F}$ - поле, G - (~~конечная~~) группа.

и $\chi_1, \dots, \chi_s : G \to \mathbb{F}^*$ набор характеров (одномерных представлений)

тогда $\chi_1, \dots, \chi_s$ - линейно независимы над $\mathbb{F}$.

Д-во: Пусть $\sum a_i \chi_i(-) \equiv 0$

(по индукции) тогда $\forall g \in G$ имеем $\sum a_i \chi_i(g-) = \sum a_i \chi_i(g) \chi_i(-) \equiv 0$

Но $\exists$ i, j и элемент $g \in G$, т.ч. $\begin{vmatrix} \chi_1(g) & \chi_2(g) \\ 1 & 1 \end{vmatrix} \neq 0$

$\Rightarrow$ Найдётся линейная замена и числа b_j:

$$\sum_{j=2}^{n} b_j \chi_j(-) \equiv 0 \quad \square$$

Сл-ие Если $\sigma_1, \dots, \sigma_n : \mathbb{F} \to \mathbb{E}$ различные, то они лин. независимы $/\mathbb{E}$.

Д-во: Р-м $\chi_i : \mathbb{F}^* \to \mathbb{E}^*$ - характеры.

Сл-ие Пусть $\mathbb{F}/\mathbb{K}$ - конечное сепарабельное расширение с базисом $\{\alpha_1, \dots, \alpha_n\}$.

Пусть $\sigma_1, \dots, \sigma_n : \mathbb{F} \to \Omega/_{\mathbb{K}}$ набор лин. независимых вложений $/_{\mathbb{K}}$

Тогда м-ца $\|\sigma_i(\alpha_j)\|$ - обратима.

Д-во: Если не обратима, то $\exists$ набор $c_1, \dots, c_n$ т.ч. $\sum c_i \sigma_i(\alpha_j) = 0$ $\forall j$

$\Rightarrow \sum c_i \sigma_i \equiv 0$.

<u>Приложение</u> к теор о не разрешимости в радикалах:

<u>Лемма</u> Пусть $\mathbb{F}$ – поле содержащее корни n-ой степ. из 1,
и $\operatorname{char}\mathbb{F} = 0$, тогда

$$\operatorname{Gal}(\mathbb{F}/\mathbb{K}) = \mathbb{Z}/n\mathbb{Z} \iff \exists\, \alpha \in \mathbb{F} : \mathbb{F} = \mathbb{K}[\alpha]$$
и $\alpha^n \in \mathbb{F}$ минимальная степень.

<u>Д-во</u> $\Leftarrow$ $\mu_\alpha(x)$ – делитель мн-на $x^n - a = (x-\alpha)(x-\zeta\alpha)(x-\zeta^2\alpha)\dots$

Имеем $\mathbb{F}$ – поле разлож $x^n - a \Rightarrow \mathbb{F}/\mathbb{K}$ – Галуа

$$\Rightarrow i : \operatorname{Gal}(\mathbb{F}/\mathbb{K}) \longrightarrow \mathbb{Z}/n\mathbb{Z}$$
$$\sigma \longmapsto \frac{\sigma(\alpha)}{\alpha}$$

инъективность следует из того, что $\mathbb{F}$ - порождено α.
сюръективность: если образ не всё $\mathbb{Z}/n\mathbb{Z}$, а собств. подгруппа.
то $\operatorname{Gal}(\;) = \mathbb{Z}/d\mathbb{Z} = \langle \zeta^d \rangle$.

$\Rightarrow$ сопряжённые к α имеют вид: $\alpha, \zeta^d\alpha, \zeta^{2d}\alpha, \dots \zeta^{d(n-1)}$

$$\Rightarrow \mu_\alpha(x) = x^{n/d} - \alpha^{n/d} \notin \mathbb{K}[x].$$

$\Rightarrow$ $\operatorname{Gal}(\mathbb{F}/\mathbb{K}) = \mathbb{Z}/n\mathbb{Z}$.

тогда воспользуемся теор. Дедекинда и получим,
что г-змы $\{1, \sigma, \sigma^2, \sigma^3, \dots, \sigma^{n-1}\} = \mathbb{Z}/n\mathbb{Z} : \mathbb{F}^* \to \mathbb{F}^*$
линейно независимы. $\Rightarrow$ эл-нт $\sum \sigma^i \zeta^i \not\equiv 0$

$$\Rightarrow \exists_{\alpha}\, \gamma = \sum \sigma^i \zeta^i(\alpha).$$

Имеем $\sigma\alpha = \sum \sigma^{i+1} \zeta^i(\alpha) = \zeta^{-1} \sum \sigma^{i+1} \zeta^{i+1} \alpha = \zeta^{-1}\alpha$. $\square$

<u>Кольца целых</u> $R \subset S$ – (целостных) расширение колец.

Напомним, что $\alpha \in S$ называется целым алгебраич,
если существует приведённый мн-н $f(x) \in R[x]$ аннулирующий α.

Нас будет интересовать $\mathcal{O}_{\mathbb{F}} \subset \mathbb{F}/\mathbb{Q}$ – эл-ты целые над $\mathbb{Q}$

Теорема $\mathcal{O}_{\mathbb{F}}$ — свободная абелева группа ранга $[\mathbb{F}:\mathbb{Q}]$.

Шаг 1 $\mathcal{O}_{\mathbb{F}}$ — подкольцо — произведение и сумма целых алгебр. — алгебраич.

Шаг 2 Если $\alpha \in \mathcal{O}_{\mathbb{Z}}$, то $\mu_\alpha(x) \in \mathbb{Z}[x]$.

Д-во: $\mu_\alpha(X) = (x-\alpha_1)\ldots(x-\alpha_s)$ α_i — сопряжённые с α в подходящем расширении Галуа. $\mathbb{E} \supset \mathbb{F} \supset \mathbb{Q}$.

тогда $\mu_\alpha(x) \mid \underset{\in \mathbb{Z}[x]}{f_\alpha(x)}$ — аннулирующий для α.

$\Rightarrow$ Все α_i также целые алгебраич.

$\Rightarrow$ $\mu_\alpha(x) \in \mathcal{O}_{\mathbb{F}}[x] \cap \mathbb{Q}[x]$, но $\mathbb{Q} \cap \mathcal{O}_{\mathbb{F}} = \mathbb{Z}$.

Кольцо $\mathbb{Z}$ - целозамкнуто в своём поле частных.

$$\Rightarrow \begin{array}{l} tr(\alpha) := \alpha_1 + \ldots + \alpha_s \\ N(\alpha) := \alpha_1 \cdot \ldots \cdot \alpha_s \end{array} \in \mathbb{Z}.$$

Шаг 3 Форма $tr_{\mathbb{F}/\mathbb{Q}}$ — невырождена т.к. $\mathbb{F}/\mathbb{Q}$ - сепарабельно и целочисленна, т.е. $\langle a,b\rangle := Tr(ab) \in \mathbb{Z}$, если $a, b \in \mathcal{O}_{\mathbb{F}}$.

Шаг 4 Если $\alpha \in \mathbb{F}$ то $\exists c \in \mathbb{Q} : c\alpha \in \mathcal{O}_{\mathbb{F}}$.

Д-во: Пусть $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x]$ — аннулирующий для α

тогда $(a_n\alpha)^n + a_{n-1} a_n^{n-1}\alpha^{n-1} + \ldots + a_0 a_n^{n-1} = 0$

$\Rightarrow$ $x^n + a_{n-1}x^{n-1} + a_{n-2}a_n x^{n-2} + \ldots + a_0 a_n^{n-1}$ - аннул. для $a_n\alpha$.

$\Rightarrow \exists \alpha_1, \ldots, \alpha_m \in \mathcal{O}_{\mathbb{F}}$ образующие базис $\mathbb{F}/\mathbb{Q}$. $\Rightarrow \mathcal{O}_{\mathbb{F}} \supset \mathbb{Z}^n = \mathbb{Z}\langle\alpha_1, \ldots \alpha_n\rangle$

Шаг 5 Пусть $\alpha_1^\vee, \ldots, \alpha_n^\vee$ - двойственный базис. относ. форм Tr.

тогда $\forall \beta \in \mathcal{O}_{\mathbb{F}}$ имеем $\beta = \sum \underset{\in \mathbb{Z}}{(\alpha_i, \beta)} \cdot \alpha_i^\vee \Rightarrow \mathcal{O}_{\mathbb{F}} \subset \mathbb{Z}^n = \mathbb{Z}\langle\alpha_1^\vee, \ldots, \alpha_n^\vee\rangle$

Имеем $\quad \mathbb{Z}^n \subset \mathcal{O}_{\mathbb{F}} \subset \mathbb{Z}^n \Rightarrow \mathcal{O}_{\mathbb{F}} \simeq \mathbb{Z}^n$.

поскольку все подгруппы своб. абелевой группы свободны.

Пример.

$$\begin{array}{ccc} \mathbb{Z} & \subset & \mathbb{Z}\langle 1, \frac{1+i\sqrt{3}}{2} \rangle \\ \cap & & \cap \\ \mathbb{Q} & \subset & \mathbb{Q}(i\sqrt{3}) \end{array}$$

, Вообще для квадратичных $\mathbb{Q}(\sqrt{n})$ $n \in \mathbb{Z}$ и свободно от квадрата

имеем $\mathcal{O}_{\sqrt{n}} \simeq \begin{cases} \langle 1, \sqrt{n} \rangle \\ \langle 1, \frac{a+b\sqrt{n}}{2} \rangle. \end{cases}$

Пример. $\mathbb{Q}(\zeta) \supset \mathbb{Z}[\zeta]$

Вопрос Что можно сказать про обобщение:

R – целозамкнуто в своём поле частных $\mathbb{K}$.

S – целое замыкание в конечном расширении $\mathbb{F}/\mathbb{K}$. ?