Лекция 11

Долг с прошлого раза:

<u>Теор-ма</u> (о нормальном базисе)

Если $\mathbb{F}/\mathbb{K}$ — расширение Галуа с группой Галуа G, тогда $\exists \alpha \in \mathbb{F}$ т.ч. эл-ты $\{\sigma\alpha \mid \sigma \in G\}$ образуют базис в $\mathbb{F}/\mathbb{K}$.

<u>Д-во:</u> (для случая $\mathbb{K}$ — бесконечно).

<u>Шаг 1</u> Если $f \in \mathbb{K}[x_1, \dots, x_n]$ такой что

$\forall \alpha \in \mathbb{F} \quad f(\sigma_1\alpha, \sigma_2\alpha, \dots, \sigma_n\alpha) \equiv 0$, где $G = \{\sigma_1, \dots, \sigma_n\}$.

Тогда $f \equiv 0$.

<u>Д-во шага 1</u>: рассмотрим $g(y_1, \dots, y_n) := f\left(\sum_{i=1}^n y_i \sigma_1\alpha_i, \sum_{i=1}^n y_i \sigma_2\alpha_i, \dots\right)$

$\quad = f(\sigma_1\tilde\alpha, \sigma_2\tilde\alpha, \dots, \sigma_n\tilde\alpha)$.

т.е. я вместо s-ого аргумента у f подставляю выраж $\sigma_s\left(\sum y_i\alpha_i\right) = \sum y_i \sigma_s(\alpha_i)$.

где $\alpha_1, \dots, \alpha_n$ — базис в $\mathbb{F}/\mathbb{K}$, а $\tilde\alpha := \sum y_i\alpha_i$ $\quad y_i \in \mathbb{K}$.

$\Rightarrow$ Если $f(\sigma_1\alpha, \dots, \sigma_n\alpha) = 0 \quad \forall \alpha \in \mathbb{F}$, то

$g(y_1, \dots, y_n) = 0 \quad \forall (y_1, \dots, y_n) \in \mathbb{K}^n$.

$\Rightarrow g \equiv 0$. как мн-н.

Тогда $f \equiv 0$ как мн-н. так как м-ца $\{\sigma_s(\alpha_i)\}$ — обратима

Было доказано в прошлый раз.

шаг 1 доказан.

<u>Шаг 2.</u> Р-м. $h(x_1, \dots, x_n) := \det\left(x_{\sigma_i\sigma_j}\right)$ $\quad \{\sigma_1, \dots, \sigma_n\} = G$ $\leftrightarrow$ $\{x_1, \dots, x_n\}$

Т-да $h(1, 0, \dots, 0) = \pm 1 \not\equiv 0$.

т.к. в каждой строке и в каждом столбце ровно 1 ненул. эл-т.

$\Rightarrow \exists \alpha \in \mathbb{F}$ т.ч. $h(\sigma_1\alpha, \sigma_2\alpha, \dots, \sigma_n\alpha) \not\equiv 0$. (ввиду шага 1).

$$\underset{\det(\sigma_i\sigma_j(\alpha))}{\overset{\|}{}} \Rightarrow \text{числа } \sigma_1(\alpha), \dots, \sigma_n(\alpha) \text{ образуют базис в } \mathbb{F}/_{\mathbb{K}}$$

$\Rightarrow$ М-ца $\left\{ \sigma_i \begin{pmatrix} \sigma_1(\alpha) \\ \vdots \\ \sigma_n(\alpha) \end{pmatrix} \right\}$ - обратима $\Leftrightarrow$ - из прошлого раза.

Сл-ие. $G = \mathrm{Gal}(\mathbb{F}/\mathbb{K})$, то $\mathbb{F}$ - рассматриваемое, как $\mathbb{K}$-линейное, представление группы G $\simeq$ регулярному.

$\mathbb{F} \simeq \mathbb{K}[G]$ как левый G-модуль.

Воспоминание о теор. пр-ий конечных групп! (комплекс)

G - конечная группа $\curvearrowright (V, \rho)$ - пр-ие $/\mathbb{K}$

если задан г-зм $\rho: G \to GL_{\mathbb{K}}(V)$.

Теор-ма (Машке) Любое конечномерное пр-ие вполне приводимо.

(т.е. изоморфно прямой сумме неприводимых).

под $(\mathrm{char}\,\mathbb{K}, \#G) = 1$.

Д-во: Усреднение по группе для проектора / над произв. полем

Усреднение по группе эрмитово скал. произв. / над $\mathbb{C}$.

Поле $\mathbb{C}$ удобно для использования леммы Шура:

Если V - неприводимо, то любой его автоморфизм - обратим

(над $\mathbb{C}$ или алгебр. замкн. полем - скаляр).

Характером пр-ие наз-ся $\chi_V : G \to \mathbb{C}$

$$g \mapsto \mathrm{tr}_V(g).$$

Теор. Характеры однозначно определяют пр-ие.

и образуют ортонормированный базис в кольце функций, постоянных на классах сопряжённости $G \to \mathbb{C}$, относительно скалярного произведения:

$$\langle \varphi, \psi \rangle := \frac{1}{|G|} \sum_{g\in G} \varphi(g)\cdot \overline{\psi(g)}.$$

Теор. Если V – неприводимое неодномерное пр-ие группы G, то $\exists g\in G$ т.ч. $\chi_V(g)=0$.

Пример. S_3

	e	(12)	(123)
$\mathbb{C}_+$	1	1	1
$\mathbb{C}_-$	1	-1	1
$\mathbb{C}^2$	2	0	-1

Появился 0.

Д-во: Заметим, для конечной группы G пор N

$\forall g\in G \quad g^N=1 \Rightarrow \rho(g)$ – диагонализуем, собственные значения – корни N-ой степ из 1.

$$\Rightarrow \chi_V(g) = \varepsilon_1 + \ldots + \varepsilon_k \in \mathbb{Q}(\zeta), \quad \zeta=\sqrt[N]{1}.$$

$\varepsilon_i^N=1, \quad \varepsilon_i=\zeta^{m_i}$

в частности пр-ие опр-но над полем $\mathbb{Q}(\zeta)/\mathbb{Q}$

$\Rightarrow \chi_V(g)$ – целое алгебраич. число, $\Rightarrow \overline{\chi_V(g)}$ – тоже.

$$\sum_{g\in G} \chi_V(g)\cdot\overline{\chi_V(g)} = |G|\cdot\langle \chi_V,\chi_V\rangle = |G|.$$

$\cap$ целое алгебраич.

$\cup\!\mid$

$$\underbrace{(\dim V)^2}_{\geq 1} + \sum_{g\neq 1} |\chi_V(g)|^2$$

, если $\chi_V(g)\neq 0$, то $|\chi_V(g)|\geq 1$.

$(\#G-1)$-слагаемое

Так как $\left|\prod_{\sigma\in Gal(\mathbb{Q}(\zeta)/\mathbb{Q})} \sigma(\chi_V(g))\right| \in \mathbb{Q}\cap\mathcal{O}$ (целые алгебр) $= \mathbb{Z}$, $\neq 0$.

каждое $|\,|\geq 1$.

Противоречие с правой частью.

Пусть $\sigma \in Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ тогда $\sigma: \zeta \to \zeta^k$, где $(k,N)=1$.

если $\rho(g) = \begin{pmatrix} \zeta^{m_1} & & 0 \\ & \ddots & \\ 0 & & \zeta^{m_s} \end{pmatrix}$, то $\sigma(\rho(g)) = \begin{pmatrix} \zeta^{km_1} & & 0 \\ & \ddots & \\ 0 & & \zeta^{km_s} \end{pmatrix} = \rho(g^k)$.

Отображение $g \to g^k$ - биекция на группе G.

$\alpha := \chi_V(g)$ - алгебраич $\Rightarrow$ $\sigma(\alpha)$ - тоже алгебраич.

$$\prod_{\sigma \in Gal} \sigma(\alpha) \in [\mathbb{Q}(\zeta)]^{Gal} = \mathbb{Q} \cap \underbrace{\mathcal{O}_{\mathbb{Z}}}_{\text{целые алгебр}} = \mathbb{Z}$$

$$(N-1) > \sum_{g\neq 1} |\chi_V(g)|^2 \geqslant (N-1) \Big(\underbrace{\prod_{g\neq 1} |\chi_V(g)|^2}_{\in \mathbb{Z}_{>0}}\Big)^{1/(N-1)} \geqslant (N-1).$$ - противоречие

$\square$

Теор 2 Порядок неприводимого (комплексного) пр-ия делит порядок группы.

Лемма Пусть C_g - класс сопряженности в G эл-та g. V - неприводимое $/\mathbb{C}$.

тогда число $\dfrac{\#C_g \cdot \chi_V(g)}{\dim V}$ - целое алгебраическое число

Д-во: Рассмотрим $P := \sum_{h \in C_g} h \in \mathbb{Z}[G]$.

$gPg^{-1} = P \quad \forall g \in G \Rightarrow P \in Z(\mathbb{Z}[G])$.

$\Rightarrow P$ - действует скаляром в любом непривод. пр-ии.

Вычислим скаляр λ: (Сл-ие леммы Шура $/\mathbb{C}$).

$$tr(P) = \sum_{h \in C_g} \chi_V(h) = \#C_g \cdot \chi_V(h)$$

$$tr(P) = \lambda \cdot \dim V \Rightarrow \boxed{\lambda = \frac{\#C_g \cdot \chi_V(g)}{\dim V}}.$$

если $x \in \mathbb{Z}[G]$, то оператор умножения на x

в базисе из $\{g \mid g \in G\}$ - целочисленный $\Rightarrow$

собств. значения x — аннулируются её x-м ми-ном,

$\Rightarrow$ целые алгебраические.

Р-м $\displaystyle\sum_{\substack{C_i\text{-класс}\\ \text{сопряж.}}} \left(\frac{\# C_i \chi_V(g_i)}{\dim V} \right) \cdot \overline{\chi_V(g_i)}$, $g_i \in C_i$.

$\uparrow$ целое алгебр. по лемме. $\uparrow$ целое алгебр.

$$\| \quad \frac{1}{\dim V} \sum_C \# C \, \chi_V(C) \cdot \overline{\chi_V(C)} = \frac{1}{\dim V} \cdot \langle \chi_V, \chi_V \rangle \cdot |G| = \frac{|G|}{\dim V} \in \mathbb{Q}.$$

$$\Rightarrow \frac{|G|}{\dim V} \in \mathbb{Z} \Rightarrow |G| \,\vdots\, \dim V.$$

Теор. (Бернсайда) Группа порядка $p^a q^b$ — разрешима.

Лемма Пусть V — неприводимое пр-ие конечной гр-ны G,
C — класс сопр т.ч. $(|C|, \dim V)$ — взаимно просты.

Тогда $\forall g \in C$ или $\chi_V(g) = 0$ или g действует скаляром.

Д-во: знаем $\dfrac{|C| \, \chi_V(g)}{\dim V}$ — целое алгебр. если $(|C|, \dim V) = 1$
$\chi_V(g)$ — целое.

то $\exists m, n \in \mathbb{Z}$: $m|C| + n \dim V = 1$.

$$\Rightarrow \frac{\chi_V(g)}{\dim V} = \frac{(m|C| + n\dim V)\,\chi_V(g)}{\dim V} = m \cdot \frac{|C|\chi_V(g)}{\dim V} + n \cdot \chi_V(g). \quad \text{— целое алгебр.}$$

$$\rho(g) = \begin{pmatrix} \varepsilon_1 & & 0 \\ & \ddots & \\ 0 & & \varepsilon_k \end{pmatrix}$$ ε_i — корни из 1,
$k = \dim V$.

и мы знаем, что $\frac{1}{k}(\varepsilon_1 + \ldots + \varepsilon_k)$ — целое алгебр.

Утв-ся, если не все ε_i совпадают, то $\underline{\underline{\sum \varepsilon_i = 0}}$.

Если $\sigma \in Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$. $\quad |\varepsilon_i| = 1 \Rightarrow |\alpha| \leq 1$, $|\alpha| = 1 \Leftrightarrow \varepsilon_i$ - совпадают.

$\alpha = \frac{1}{k}(\varepsilon_1 + \ldots + \varepsilon_k)$, то $\sigma(\alpha)$ — целое алгебраич

$$\beta = \prod_{\sigma \in Gal} |\sigma(\alpha)| = \Big|\prod_{\sigma \in Gal} \sigma(\alpha)\Big| \in \mathbb{Q} \cap \mathcal{O}_{\mathbb{Z}} \Rightarrow \beta \in \mathbb{Z}.$$

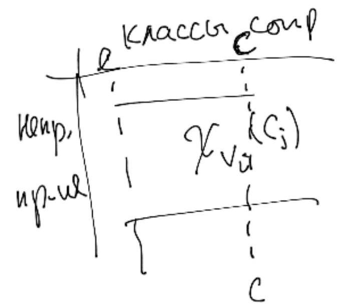
$\beta = 0 \Leftrightarrow \alpha = 0$.

$\beta = 1 \Leftrightarrow |\alpha| = 1$

$\Rightarrow \varepsilon_i$ - совп. $\Rightarrow \rho(g) = \begin{pmatrix} \varepsilon & & \\ & \ddots & \\ & & \varepsilon \end{pmatrix} = \varepsilon \cdot Id_V$.

Лемма 2 Пусть G - конечная, C класс. сопр порядка p^k.

Тогда $\exists$ собств. нормальная подгруппа.



Д-во:

$$\sum_{V \in Irr(G)} \chi_V(g) \cdot \dim V = 0 \quad , g \in C.$$

$\uparrow$ из ортогональности х-ров.

$$\| \quad 1 + \sum_{V:\, \dim V \,\vdots\, p} p\left(\frac{\dim V}{p} \cdot \chi_V(g)\right) + \sum_{\dim V \not\vdots\, p} \dim V\, \chi_V(g). \in \mathbb{Z}[\zeta].$$

1 $\uparrow$ тривиальное

$\| \quad p \cdot (\text{целое алгебр.})$

$\neq 0$.

$\dim V \not\vdots\, p$.

$\Rightarrow \exists V \in Irrep$ т.ч. $\chi_V(g) \neq 0$. $\Rightarrow$ C_g - действует константой

и эл-ты вида ab^{-1}, $a, b \in C_g$ - действуют тривиально.

$\Rightarrow \ker \varphi_V \neq e$, если $\# C_g > 1$.

$\ker \varphi_V \neq G$ т.к. V - нетрив. пр-ие.

$\Rightarrow \exists$ собств. норм. подгруппа.

Если $\# G = p^k q^l$. $\Rightarrow$ разрешима.

Если есть класс сопр $\# p^s$ или $\# q^t$ то $\exists$ норм подгр.

$\Rightarrow$ по инд. разр.

Если нет $\Rightarrow$ # классов сопр $\vdots\, pq$.

$$p^k q^l = \# G = \sum \#\text{класс. сопр.} = 1 + pq \cdot (\ldots) \quad \text{- противоречие.}$$

$\square$.