Семинар 20, 20.02.24 – Бельдиев

$Z(GL_n(\mathbb{R}))$

$\lambda E \in Z(GL_n(\mathbb{R}))$ $\quad \lambda E = \begin{pmatrix} \lambda & & 0 \\ & \ddots & \\ 0 & & \lambda \end{pmatrix}$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} c & d \\ a & b \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & a \\ d & c \end{pmatrix}$$

$$A=\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \in Z(GL_n(\mathbb{R}))$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \dots$$

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \dots$$

$$i \to \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & 1 & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix} + \begin{pmatrix} 1 & & & \\ & 1 & & 0 \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix} = \begin{pmatrix} 1 & & & \\ & 1 & & 0 \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix} \in GL_n(\mathbb{R})$$

Рассмотрим $E_{ij} + E$

$$A(E_{ij} + E) = (E_{ij} + E)A$$

$$AE_{ij} + \cancel{AE} = E_{ij}A + \cancel{EA}$$

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}\begin{pmatrix} & & j & \\ & & \vdots & \\ \dots & \dots & 1 & \dots \\ & & \vdots & \\ & & & \end{pmatrix}_i = \begin{pmatrix} & & j & \\ 0 & \dots & a_{1i} & 0 \\ & & a_{2i} & \\ & & \vdots & \\ & & a_{ni} & \end{pmatrix}_i$$

$$\begin{pmatrix} & & j & \\ & & \vdots & \\ \dots & \dots & 1 & \dots \\ & & \vdots & \\ & & & \end{pmatrix}_i \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} = \begin{pmatrix} 0 & & & \\ a_{j1} & a_{j2} & \dots & a_{jn} \\ & 0 & & \end{pmatrix}_i$$

$$\Rightarrow \begin{cases} a_{1i} = 0 \\ a_{2i} = 0 \\ a_{ni} = 0 \\ a_{j1} = 0 \\ a_{j2} = 0 \\ \dots \\ a_{jn} = 0 \end{cases}$$

Кроме a_{ii} и a_{jj}

$$\boxed{a_{jj} = a_{ii}}$$

Автоморфизмы

$f: G \xrightarrow{\sim} G$

$G \xrightarrow{f} G \xrightarrow{\tilde{f}} G$

Пример: ① $Aut(\mathbb{Z}_5) = ?$

$\{0,1,2,3,4\} \to \{0,1,2,3,4\}$

$f_a: 0 \mapsto 0$
$1 \mapsto a$
$2 \mapsto 2a$
$3 \mapsto 3a$
$4 \mapsto 4a$

автоморфизмы:
$a \neq 0$
$a = 1, 2, 3, 4$

$f_a \circ f_b = f_{ab}, \; a, b \in \mathbb{Z}_5^{\times}$

$Aut(\mathbb{Z}_n)$

$f_a: \mathbb{Z}_n \to \mathbb{Z}_n$
$1 \mapsto a$

$(a,n) = 1 \Leftrightarrow f_a$ - автом.

$(a,n) = 1$
$1 \mapsto a$
$k \mapsto ka : n \Rightarrow k : n$

$Aut(\mathbb{Z}_5) \cong \mathbb{Z}_5^*$

$\mathbb{Z}_5^{\times} \to Aut(\mathbb{Z}_5)$
$a \mapsto f_a$
$b \mapsto f_b$
$\Rightarrow ab \mapsto f_{ab} = f_a \circ f_b$

$\mathbb{Z}_5^\times \cong \mathbb{Z}_4$ 2 - порождающий эл-т (Почему 2? - Угадали 😉)

(~~$2^0=1$~~; $2^1=2$, $2^2=4$, $2^3=8 \Rightarrow 3$, $2^4=16 \to 1$) по мод. 5

② $Aut(\mathbb{Z}_4)$ $\{0, 1, 2, 3\}$

$f_a: 1 \mapsto a$ чтобы было $\mathbb{Z}_4$ - проще с 4

f_a - автоморфизм $\Leftrightarrow$ $a=1$, $a=3$ $\Leftrightarrow$ $a = \pm 1$

$Aut(\mathbb{Z}_4) \cong \mathbb{Z}_2$

③ $Aut(\mathbb{Z}_2 \times \mathbb{Z}_2)$ $\{(0;0), (0;1), (1;0), (1;1)\}$

$(0;0) \mapsto (0;0)$
$(0;1) \mapsto (0,1)$
$(1;0) \mapsto (1,1)$
$(1;1) \mapsto (1,0)$

$Aut(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$

④ $Aut(S_3) = ?$

$\{id, (12), (13), (23), (123), (132)\}$

$\{id, (12), (13), (23), (123), (132)\}$

$id \mapsto id$

$\{(12), (13), (23)\} \mapsto \{(12), (13), (23)\}$

Внутренний автоморфизм

$G \to G$
$g \mapsto aga^{-1}$

S_3: $a = (1?$

$(12)(12)(12)^{-1} = (12)$

$(12)(13)(12)^{-1} = (23)$

$(12)(23)(12)^{-1} = (13)$

Протокол Диффи-Хеллмана
Криптосистема Эль-Гамаля (Эля-Галя)

$\mathbb{Z}_p^x \ (= G)$

А: a - закрытый ключ, g^a - открытый ключ

Б: b - закрытый ключ, g^b - открытый ключ

$A \underset{g^b}{\overset{g^a}{\rightleftarrows}} Б$

$a, g^b \qquad g^b \qquad b, g^a$

$(g^b)^a = g^{ab} = (g^a)^b$

Пример: $\mathbb{Z}_{23}^x \cong \mathbb{Z}_{22} \quad g = 5$

А: $a = 6$; $5^6 \underset{23}{\equiv} 25^3 = 8$

Б: $b = 15$ $\quad 5^{15} \underset{23}{\equiv} 19$

$A \underset{19}{\overset{8}{\rightleftarrows}} Б$

А: $19^6 \underset{23}{\equiv} (2)$

Б: $8^{15} \underset{23}{\equiv} (2)$

$\mathbb{Z}_p^x \qquad s = g^{ab}$

А: $m \in \mathbb{Z}_p^x$

$A \xrightarrow{sm} Б$

$s^{-1}(sm) = m$

Пример отправки сообщения:

$G = \mathbb{Z}_{17}^x \qquad g = 3 \qquad m = 13$

$A \underset{12 = g^b = 3^b}{\overset{g}{\rightleftarrows}} Б$ $\quad 13 \cdot 8 \equiv 2$

$a = 2$

$s = (3^b)^a = 12^a = 12^2 = 144 \underset{17}{\equiv} 8$

$g^a = 3^2 = 9$

$s = g^{ab} = 9^{13} \underset{17}{\equiv} 8$

$2 \cdot 8^{-1} \underset{17}{\equiv} 2 \cdot 8^{15} \underset{17}{\equiv} 2 \cdot 8 (8^2)^7 \equiv$

$\equiv -64^7 \equiv 4^7 \equiv (4^2)^3 \cdot 4 \equiv$

$\equiv -4 \equiv 13$