08.05.2013

Еще раз об ограниченном порождении

А. Смоленский

(Carter–Keller, Bounded elementary generation of $SL_n(\mathcal{O})$)

$\boxed{\text{I}}$ $n \geq 3$ $\quad w_E(SL_n(\mathcal{O})) \leq \frac{1}{2}(3n^2-n) + 68\Delta - 1$

Δ — число различных простых делителей дискриминанта

(иногда $\frac{1}{2}(3n^2-n)+51$)

(когда число классов $=1$
или когда дискриминант — степень простого.

$\boxed{\text{Лемма 1}}$ R — кольцо

$$A = \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} a^k & b & 0 \\ x & y & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

k-ую степень A можно перегнать в B с помощью 16 элементарных преобразований

<u>Док-во</u> $f_n(t),\quad g_n(t) \in \mathbb{Z}[t]$

$f_0(t) = 1 \qquad g_0(t) = 0$

$f_{n+1}(t) = -g_n(t), \quad g_{n+1}(t) = t g_n(t) + f_n(t)$

$f = f_k(\operatorname{tr} L) \qquad g = g_k(\operatorname{tr} L)$

$L^2 - \operatorname{tr} L \cdot L + I$ — хар. многочлен $L \to L^k = fI + gL$

$\Rightarrow g_{l+1}(t)\, g_{l-1}(t) = (g_l(t))^2 - 1,$

$f_l(t) \mid g_l(t)^2 - 1$

подставим $l=k$, $t = \operatorname{tr} L$ $\longrightarrow$ $\quad f = f^+ f^- \qquad g+1 = j f^+ \qquad g-1 = i f^-$

$$G = \begin{pmatrix} 1 & & \\ & 1 & f^- \\ & & 1 \end{pmatrix}\begin{pmatrix} 1 & & \\ & 1 & \\ & i & 1 \end{pmatrix} = \begin{pmatrix} 1 & & \\ & g & f^- \\ & k & 1 \end{pmatrix}$$

$$H = \begin{pmatrix} 1 & & \\ & 1 & \\ -1 & 1 & \end{pmatrix} \begin{pmatrix} 1 & & 1-f^+ \\ & 1 & \\ & & 1 \end{pmatrix} \begin{pmatrix} 1 & & \\ -f^- & 1 & \\ j & & 1 \end{pmatrix} = \begin{pmatrix} * & 0 & * \\ -f^- & 1 & 0 \\ g & 0 & f^+ \end{pmatrix}$$

G — произведение двух элем. образующих,
H — произведение четырех элем. образующих

$$Y = GH = \begin{pmatrix} * & 0 & * \\ 0 & g & f \\ 1 & * & * \end{pmatrix} \xrightarrow{4} K = \begin{pmatrix} 1 & 0 & -b \\ 0 & g & f+ga \\ * & * & * \end{pmatrix}$$

(произв. 10 образующих

Рассмотрим эти матрицы по модулю $\epsilon(b)$

A — нижнетреугольная mod $\epsilon(b)$

$\rightsquigarrow f+ga \equiv a^k \mod (b)$

$$B \xrightarrow{1} \left(\begin{array}{cc|c} f+ga & b & \\ s & y & \\ \hline & & 1 \end{array}\right) = C$$

$$U = CK = \begin{pmatrix} f+ga & bg & 0 \\ * & * & 1 \\ * & * & * \end{pmatrix} \xrightarrow{5} A^k$$

□

<u>Обозначение</u> $a \in R$ $\quad \epsilon(a)$ = экспонента $(R/aR)^*$
= 0, если эксп = ∞

Лемма 2 $A = \begin{pmatrix} a & b & \\ c & d & \\ & & 1 \end{pmatrix}$, $\gcd(\varepsilon(b), \varepsilon(c)) \mid \delta$

Тогда $A^\delta \in E(3,R)$ $\quad w_E(A^\delta) \le 36$

Док-во: Выберем $\rho, \sigma \in \mathbb{N}$

т.ч. $\rho\,\varepsilon(b) - \sigma\,\varepsilon(c) = \pm\delta$

$\to \exists\, b', c' \in R:\quad a^{\rho\varepsilon(b)} = 1 + bb'$

$d^{\sigma\varepsilon(c)} = 1 + cc'$

$$B = \begin{pmatrix} 1 & b & \\ & 1 & \\ & & 1 \end{pmatrix}\begin{pmatrix} 1 & & \\ b' & 1 & \\ & & 1 \end{pmatrix} = \begin{pmatrix} a^{\rho\varepsilon(b)} & b & 0 \\ b' & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$C = \begin{pmatrix} 1 & -c & \\ & 1 & \\ & & 1 \end{pmatrix}\begin{pmatrix} 1 & & \\ -c' & 1 & \\ & & 1 \end{pmatrix} = \begin{pmatrix} d^{\sigma\varepsilon(c)} & -c & \\ -c' & 1 & \\ & & 1 \end{pmatrix}$$

$B \xrightarrow{16} A^{\rho\varepsilon(b)}$, — шир. 18

$C \xrightarrow{16} \left(A^{-\sigma\varepsilon(c)}\right)^t$, — шир. 18 $\to A^{\delta}$ имеет ширину 36 $\square$

$\boxed{\text{Лемма } 3}$ $\forall L_1 \in SL_2(\mathcal{O}) \Rightarrow \exists\, a, b \in \mathcal{O}$:

(1) $b\mathcal{O}$ — простой идеал, $m \notin b\mathcal{O}$,
 — кол-во корней из 1 в K

$b\mathcal{O}$ не ветвится

(2) $L_1 \xrightarrow{4} \begin{pmatrix} a^m & b \\ * & * \end{pmatrix}$

$\boxed{\text{Лемма } 4}$ $\mathfrak{a} \neq 0$ — главный идеал, $\forall\, b \overset{\in \mathcal{O}}{\neq} 0$ такого, что
$\trianglelefteq \mathcal{O}$

(1) $b\mathcal{O}$ — простой, $\left(\operatorname{char}(\mathcal{O}/b\mathcal{O}), m\right) = 1$

(2) $b\mathcal{O} + \mathfrak{a} = \mathcal{O}$

Тогда

$\forall u \in \mathcal{O}^* \quad \exists\, c:\ bc \equiv u \mod \mathfrak{a}$, $\gcd(\varepsilon(b), \varepsilon(c)) = m\gamma$,
причем все простые делители γ ветвятся в K (т.е. делят дискриминант K)

Кроме того, c можно выбрать так, что γ взаимно просто с любым наперед заданным p, ветвящимся в K. Если же число классов K равно 1, можно взять c такое, что $\gamma = 1$

Д-во Теоремы:

разложение Басса-Кольстера

$$SL(n+1,R) = SL(n,R)\, U_n^+ U_n^- U_n^+ U_n^-$$

U_n^+

$\frac{1}{2}(3n^2-n-10)$

$$A_1 = \begin{pmatrix} a_1 & b_1 & \\ c_1 & d_1 & \\ & & 1 \end{pmatrix} \xrightarrow{4} A_2 = \begin{pmatrix} a^m & b & \\ c_2 & d_2 & \\ & & 1 \end{pmatrix}$$

— для a, b из Леммы 3

$b\mathcal{O}$ — простой как в пункте 1 Леммы 4

Возьмем $\mathfrak{a} = a\mathcal{O}$, $u = -1$

$\rightsquigarrow$ по Лемме 4 $\exists\, c:\ bc \equiv -1 \mod (a)$

Пусть получилось так, что $\gamma = 1$,

т.е. $\gcd(\varepsilon(b), \varepsilon(c)) = m$

$$A_2 \xrightarrow{16} A^m \qquad A = \begin{pmatrix} a & b & \\ c & d & \\ & & 1 \end{pmatrix}$$

у A^m ширина 36

$\rightarrow \frac{1}{2}(3n^2-n-10) + 4 + 16 + 36$

Пусть $p_1, \dots, p_s$ — различные простые делители дискриминанта.

Для каждого p_i можно по лемме 4 построить

c_i т.ч. $b c_i \equiv -1 \pmod{(a)}$, $\gcd(\varepsilon(b), \varepsilon(c_i)) = m\gamma_i$,

γ_i не делится на p_i

$(\gamma_1, \dots, \gamma_\Delta) \in Um_\Delta(\mathcal{O}) \rightsquigarrow \exists \beta_i : \sum \beta_i \gamma_i = 1$

$$A_2 = A_2^{\beta_1\gamma_1} \dots A_2^{\beta_\Delta\gamma_\Delta}$$

Смотрим на $A_2^{|\beta_i\gamma_i|}$ — покажем, что ее ширина ≤ 68

$$\Big\downarrow 16$$

$$B_i = \begin{pmatrix} a^{m|\beta_i\gamma_i|} & b & \cdot \\ x_i & y_i & \cdot \\ - & \sim & 1 \end{pmatrix}$$

$$\Big\downarrow 16$$

$$C_i^{m|\beta_i\gamma_i|}, \text{ где } C_i = \begin{pmatrix} a & b & \cdot \\ c_i & d_i & \cdot \\ - & \cdot & 1 \end{pmatrix}$$

ширина $= 36$ и $\gcd(\varepsilon(b), \varepsilon(c_i)) = m\gamma_i$

$$36 + 16 + 16 = 68$$

$\square$

Clifford Queen, Some arithmetic properties of subrings of function fields over finite fields