31.05.2010

Сергей Юрьевич Рыбаков

$K = \mathbb{F}_q$, $\operatorname{char} K = p$

Опр. Абелево многообразие A над K — это алгебраическое многообразие + алг. группа

Опр. $A \xrightarrow{\varphi} B$ — изогения, если φ — сюръект., конечной степени

Утв. A и B изогенны — ОЭ.

$A \sim B$

Пример Эндоморфизм Фробениуса $F: A \longrightarrow A$:

F постоянно на точках, $f \longmapsto f^q$ на функциях

$\deg F = q^{\dim(A)}$, в его ядре 1 точка

Утв. (Вейль) $\deg(t - F)$ — многочлен $= f_A(t) \in \mathbb{Z}[t]$

$t \in \mathbb{Z}$

$\deg f_A = 2g$, $g = \dim A$

$(t-F)(a) = ta - Fa$

$K = \mathbb{C}$

$\sim A = \mathbb{C}^n / \Lambda$, $\Lambda \simeq \mathbb{Z}^{2n}$

$\ell \neq p$, ℓ — простое

$$[\ell^n]: A \longrightarrow A$$
$$a \longmapsto \ell^n a$$

$$A_n = \operatorname{Ker}[\ell^n](K) \simeq \left(\mathbb{Z}/\ell^n\mathbb{Z}\right)^{2g}$$

$$A_n \xleftarrow{\ell} A_{n+1} \xleftarrow{\ell} A_{n+2}$$ — согласована с действием Фробениуса

Модуль Тейта

$$T_\ell(A) = \varprojlim A_n$$

Утв. (Вейль) $T_\ell(A) \cong \mathbb{Z}_\ell^{2g}$

F индуцирует полупростой оператор на $T_\ell A \otimes \mathbb{Q}_\ell$

Утв. (Вейль) $\det(t - F | T_\ell A) = f_A(t)$

Теорема (Тейт–Хонда) $A \sim B \Leftrightarrow f_A = f_B$

Пример: $\dim A = 1$ $\quad f_A(t) = t^2 - bt + q$

$|b| \leq 2\sqrt{q}$

а) $(b, p) = 1$

б) $b = 0, \pm\sqrt{q}, \pm 2\sqrt{q}$

в) $p = 2$
$p = 3$

$A[\ell] = \mathrm{Ker}[\ell]$

Задача: описать $A[\ell](k)$, где A пробегает класс изогении

$$A[\ell](k) \simeq \mathbb{F}_\ell^{2g} \circlearrowleft F$$

$T_\ell A / \ell T_\ell A$ $\qquad$ $f_A \bmod \ell$ — хар. многочлен

$$V = T_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \xrightarrow{\sim} \left(\mathbb{Q}_\ell[t] / f_A(t)\mathbb{Q}_\ell[t]\right)^{ss}$$

$$f_A = \prod f^{(i)}$$

$f^{(i)} \mid f^{(i+1)}$
и у $f^{(i)}$ нет кратных корней

$$\| \qquad \bigoplus \left(\mathbb{Q}_\ell[t] / f^{(i)}\mathbb{Q}_\ell[t]\right)$$

мин. многочлен F

$$R = \mathbb{Z}_\ell[t] / f^{(1)}\mathbb{Z}_\ell[t]$$

Тогда V — R-модуль, $T \subseteq V$ — $\mathbb{Z}_\ell$-решетка и R-модуль

$$T/\ell T = ?$$

Редукция к случаю $f \equiv t^d \ (\ell)$ $\quad // \ d = \deg f$

$M \in \mathrm{Mat}_d(\mathbb{Z}_\ell)$
$N \in \mathrm{Mat}_d(\mathbb{F}_\ell)$
$N^d = 0$. Найти M:
- $M \equiv N \pmod{\ell}$
- $\det(t - M) = f(t)$
- M полупроста

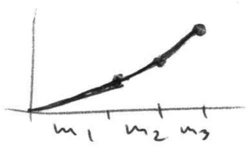
$$V = \mathbb{Q}_\ell[t] / f(t)\mathbb{Q}_\ell[t]$$

(если в f нет кратных корней, это то же самое)

$\rightsquigarrow$ N определяется набором размеров жордановых клеток $(m_1, \ldots, m_s)$
$m_1 \geq \ldots \geq m_r$

- Многоугольник Юнга $Y_p(N)$

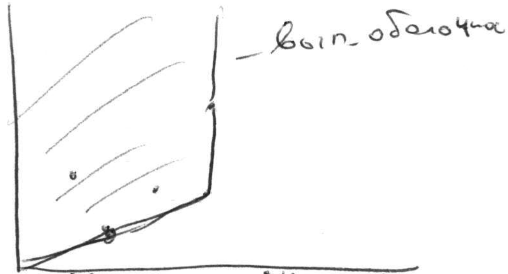
$$\left(\sum_{i=1}^{s} m_i, s\right)$$



• многоугольник Ньютона $f \equiv t^d (\ell)$

$$f(t) = \sum a_i t^{d-i}$$

$(i, \mathrm{ord}_\ell\, a_i)$



Теорема ∃ решетка $T \subseteq V$ такая, что N — матрица действия на $T/\ell T$

$\Updownarrow$ (1)

$\mathcal{N}_\ell(N) \prec N_\ell(f)$

не выше

$M \in \mathrm{Mat}_d\, \mathbb{Z}_\ell \rightsquigarrow \det(t-M)$

$\mathcal{N}_\ell(M^{(i)} \bmod \ell)$

$M \bmod \ell = N_d + N$

диаг. нильп.

$N_d = \mathrm{diag}(\lambda_1, \dots, \lambda_1, \lambda_2, \dots, \lambda_2, \dots)$

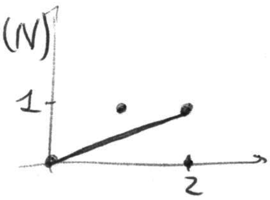
$M_d := \mathrm{diag}(\tilde\lambda_1, \dots, \tilde\lambda_1, \tilde\lambda_2, \dots)$

$\Rightarrow M - M_d$ — уже хорошая:

$$\det(-M+M_d-t) = \prod_i \det(t-M^{(i)})$$

$$f(t) = t^2 - \ell t - \ell$$

$N_1 = \begin{pmatrix}0&1\\0&0\end{pmatrix}$ $\quad N_\ell(f) = \mathcal{N}_\ell(N)$



$M = \begin{pmatrix}0&1\\ \ell&\ell\end{pmatrix}$

$N_2 = \begin{pmatrix}0&0\\0&0\end{pmatrix}$

$M_2 = \ell M_2' \rightsquigarrow \det \vdots\, \ell^2$

Если кр. корни есть: $R = \mathbb{Z}_\ell[t]/g\,\mathbb{Z}_\ell[t]$ $\quad g, f \in \mathbb{Z}_\ell[t]$

$(g = f^{(1)})$ $\quad S = \mathbb{Z}_\ell[t]$, $r \in \mathbb{N}$ $\quad S \ni t \mapsto x \in R$

Опр. Матричное разложение: $X, Y \in \mathrm{Mat}_{r\times r}(S)$:

• $XY = YX = g \cdot E_r$

• $\det X = f$

$$S^r \xrightarrow{X} S^r \longrightarrow T \longrightarrow 0$$

T — R-модуль

$\boxed{\text{Утв.}}$ Если $f \equiv t^d (\ell)$, $\deg f = d$
$\Rightarrow T$ своб. над $\mathbb{Z}_\ell$ ранга d $\quad \det(t - X) = f(t)$

$\boxed{\text{Утв.}}$ T — R-модуль, своб., ранга d над $\mathbb{Z}_\ell$
Пусть T порожден над R r элементами
Пусть действие X на $T/\ell T$ нильпотентной матрице N
$\sim m_1 \geq \ldots \geq m_r$

Тогда $\exists$ пара X, Y — матричное разложение:

$$X \equiv \operatorname{diag}(x^{m_1}, \ldots, m^r) \pmod{\ell}$$

$g(t) = (t^2 - bt + c)t$

$f(t) = g(t) \cdot t$

$$N = \begin{pmatrix} 0 & 1 & & 0 \\ 0 & 0 & & \\ & & 0 & 1 \\ 0 & & 0 & 0 \end{pmatrix}$$

можно поднять

$\Updownarrow$

$\ell^2 \mid c$

T над $R \longrightarrow (X, Y)$
$X \equiv \operatorname{diag}(x^2, x^2)(\ell)$

$Y \rightsquigarrow T'$

$Y \equiv \operatorname{diag}(x, x)$

T' — модуль над $S/(t^2 - bt + c)$

$\det Y \cdot \det X = g^2$

$\det X = f = g \cdot t$

$\rightsquigarrow \det Y = t^2 - bt + c$