

(первая часть лекции и вторая часть лекции на видео).

Пусть $(E, \underline{0})$ — плант. кривая.

Тогда было доказано, что кривые изоморфизма, т.е. $\lambda: E \rightarrow E$, т.е. $\lambda(\underline{0}) = \underline{0}$

существует симметрическое скалярное произведение $(\lambda, \mu) \in \mathbb{Q}$.

Было также доказано, что существование такого скалярного произведения эквивалентно равенству

$$(*) \quad \deg(\lambda - \mu) + \deg(\lambda + \mu) = 2(\deg(\lambda) + \deg(\mu)),$$

где λ, μ — любые изоморфизмы,

$$\text{и } \deg(\underline{0}) = 0.$$

вытекает
изоморфизм

Пусть $[m]: E \rightarrow E$ — умножение на $m \in \mathbb{Z}$.

$$\text{Тогда } \deg[1] = 1.$$

По индукции, из $(*)$ получаем, что

$$\deg[m] = m^2.$$

Пусть $f: E \rightarrow E$ над k

$$\deg f = [k(E) : f^* k(E)]$$

f - сепар. морфизм, если все разложения имеют сепарабельные.

$\text{char } k = 0$ - нет проблем.

Если f - не сепарабельно, то $\deg f = p^n \cdot d$.

Пусть $(\text{char } k, m) = 1$, тогда

из $\deg [m] = m^2 \Rightarrow [m]$ - сепарабельный морфизм.

Отсюда следует: f - сепарабельный, тогда
существует открытое U в E ,
такое что $\forall x \in U(\bar{k}) : \# f^{-1}(x) = \deg f$.

Зам. При этом условии

- 1) $\# \ker [m] = m^2$ (над $\bar{k}$).
- 2) $\forall x \in E(\bar{k}), \# [m]^{-1}(x) = m^2$
- 3) $[k(E) : [m]^* k(E)]$ - разложение $\deg f$
с абелевой группой $\deg f$ $G = \# \ker [m]$,
где $K \supset k$, так что $E(K) \supset \ker [m](\bar{k})$

Зам. 1) $[m]$ - гомоморфизм групп.

$$\Rightarrow \forall x, y \in E(\bar{k}) \quad \# f^{-1}(x) = \# f^{-1}(y) = \ker [m].$$

$$2) \# \ker [m] = m^2$$

$$\forall x \in \ker [m].$$

$$T_x: E \rightarrow E \text{ над } K.$$

$$y \mapsto y + x.$$

линейн. автоморфизм.

$$K(E) \text{ над } [m]^* K(E).$$

$\xrightarrow{\text{см.}, \text{см.}, \text{с.}} \text{с.}$

$$k(E) \hookleftarrow E(E) = k(E) \cdot E = k(E) \cdot [m] \cdot E(E) \quad (12)$$

$$\wedge \quad \wedge \quad \quad \quad | \quad m \cdot k(E) \cdot E(E)$$

$$[m]k(E) \subset [m]E(E) = m k(E) \cdot E$$

$$\text{Gal}(k(E) \cdot E / m \cdot k(E) \cdot E) \cong \text{Gal}(k(E) /$$

$$k(E) \subset E(E)$$

$$\wedge \quad \wedge$$

$$[m]k(E) \subset [m]E(E)$$

$$\text{Gal}(E(E) / [m]E(E)) \cong \text{Gal}(k(E) /$$

$$\frac{L/k}{\quad} \quad \text{Gal}(L^M/kM) \cong$$

$$\cong \text{Gal}(L/L^M)$$

$$E \xrightarrow{y \mapsto y^m} E$$

$$\downarrow [m]$$

$$E \xleftarrow{[m]} E$$

Ух координаты = степень расширения + что сейчас $\Rightarrow$
 $\Rightarrow$ форм. range.

Прим. Уж тож, то $\deg[m] = m^2$, $(m, \text{char } k) = 1$
 следовательно $E[m] \stackrel{\text{by}}{\cong} \ker[m] \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$
 (над $\mathbb{Z}$).

З-бс: Пусть p - простое, $(p, \text{char } k) = 1$.

$$E[p] = \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$$

(max-бс элементов = p^2)

$$p \in E[p] = 0.$$

$$E[m] = A(p_1) \times A(p_2) \times \dots$$

$$A(p_i) = \mathbb{Z}/p_i^{n_1} \times \mathbb{Z}/p_i^{n_2} \times \dots$$

$$n_1 \geq n_2 \geq \dots$$

$p_1, p_2, \dots$
 различные, простые
 делители m

$$E[p_i] \subset E[m]$$

и-модуль p_i

$$E[m] = \begin{bmatrix} \mathbb{Z}/p_1^{n_1} \\ \times \\ \mathbb{Z}/p_1^{n_2} \\ \vdots \\ \mathbb{Z}/p_1^{n_m} \end{bmatrix} \times \begin{bmatrix} \mathbb{Z}/p_2^{n_1} \\ \times \\ \mathbb{Z}/p_2^{n_2} \\ \vdots \\ \mathbb{Z}/p_2^{n_m} \end{bmatrix}$$

$E[p_1] \rightarrow$
 $\parallel$
 $\mathbb{Z}/p_1 \times \mathbb{Z}/p_1$

$$E[m] = \begin{bmatrix} \mathbb{Z}/p_1^{n_1} \\ \times \\ \mathbb{Z}/p_1^{n_2} \end{bmatrix} \times \begin{bmatrix} \mathbb{Z}/p_2^{n_1'} \\ \times \\ \mathbb{Z}/p_2^{n_2'} \end{bmatrix} \times \dots$$

$$\# E[m] = m^2 \Rightarrow n_1 = n_2, n_1' = n_2', \dots$$

$$E[m] = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

$$\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/p_1^{n_1} \times \dots \times \mathbb{Z}/p_2^{n_2}$$

(лем. Теорема)
 об остатках

что k — простое поле, $\text{char } k = p > 0$, то

см. определение

$$E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z} \quad \forall e = 1, 2, 3, \dots$$

в абелев. гр.

$$E[p^e] = \mathbb{Z}/p^e\mathbb{Z} \quad \forall e = 1, 2, 3, \dots$$

и-модуль

k -сепар. $\left. \begin{array}{l} \text{Hasse inv} = 1 \end{array} \right\}$

$\left. \begin{array}{l} \text{и-модуль} \\ \text{и не сепар.} \end{array} \right\} \left. \begin{array}{l} \text{Hasse inv} = 0 \\ \text{(supersingular) не сепар.} \end{array} \right\}$
 $\text{End}(E) \cong \mathbb{F}_p, \# E(k) = p+1$

End может быть только из трех типов

(139)

1) $\text{End} = \mathbb{Z}$

2) End - порожден в некотором миним.
квадр. расщ. над $\mathbb{Q}$ (комп. упрощ.)

3) End - порожден в некоторой
миним. алгебре квадратичной.

(то есть $\text{End} \cong \mathbb{Q}^A$, алг. конечного $\mathbb{Z}$ -модуля)
и $A \otimes \mathbb{Q} = \mathbb{Q}^A$.

$$\mathcal{H} = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta$$

quaternion
algebra

$$\alpha^2, \beta^2 \in \mathbb{Q}, \quad \alpha^2 < 0, \quad \beta^2 < 0, \quad \beta\alpha = -\alpha\beta$$

Неравенство Хассе - Вейля

14

C — н. нрвн. арт. кр. / $\mathbb{F}_q$.

$g(C) = 1$ Хассе, $g(C) > 1$ Вейль.

$$N = \# C(\mathbb{F}_q)$$

$$|N - q - 1| \leq 2g\sqrt{q}$$

Значит
Равенство
на C .

Докажем для $g(C) = 1$

$\exists$ каноническое произведение

на кривых $(E, 0) \rightarrow (E, \infty)$

(Всегда $\exists$ раз. точка на $E/\mathbb{F}_q$)

Рассм. φ — отображение Фробениуса

$$\begin{aligned} X &\mapsto X^q \\ Y &\mapsto Y^q \end{aligned}$$

$$k(E) \xrightarrow{\varphi^*} k(E), \quad a \mapsto a^q$$

Так как $g(C) > 1$ имеет
расщепление

$\mathbb{Q} \times \mathbb{Q}$ и т.д.

Ходим от индекса на
группе

$S_{m-2} \times S_{m-2}$ на $\mathbb{F}_1$
значит Равенство

$$k = \mathbb{F}_q$$

$$k(E) \supset \varphi^* k(E)$$

$$\cup \deg = 2$$

$$\cup \deg = 2$$

$$k(x) \supset (k(x))^q = k(x^q)$$

$$\deg = q$$

$$\varphi_{\text{sur}}$$

$$\Rightarrow \deg \varphi = q.$$

Рассмотрим
отображение

$$a + b\varphi, \quad a + b \in \mathbb{Z}.$$

$$h(a + b\varphi) = (a + b\varphi, a + b\varphi),$$

который.

Напомним, что

$$n = \deg. \quad (\text{обозначение})$$

$$\text{frac}(k[x])$$

$$k[x] \quad k[x^q]$$

генер.

$$1, x, \dots, x^{q-1}$$

базис.

$$f \in k[x]$$

$$\exists g \in k[x] :$$

$$fg \in k[x^q].$$

$$\frac{1}{f} = \frac{g}{fg}$$

$$f: k[x] \rightarrow k[x]$$

$$f(x) - \lambda E = 0$$

как $k[x]$ —
модуль

$$n(a+b\varphi) = a^2 n(1) + 2ab(1, \varphi) + b^2 q \quad (*) \quad (15)$$

$$\text{Уменьш, } n(a+b\varphi) \geq 0 \Rightarrow$$

(otherwise.)

$$2^2(1, \varphi)^2 - 4n(1)b^2q \leq 0 \quad \left(\frac{a}{b}\right)^2 + 2\frac{a}{b}(1, \varphi) + q \geq 0$$

$\forall a, b \in \mathbb{Z}$

$$|(1, \varphi)|$$

$$4(1, \varphi)^2 - 4q \leq 0$$

$$|(1, \varphi)| \leq \sqrt{q}$$

(***)

Уз (*) следует, что

$$2(1, \varphi) = n(1-\varphi) - q - 1.$$

Отсюда и (***) $\Rightarrow$

$$|n(1-\varphi) - q - 1| \leq 2\sqrt{q}.$$

$$\text{При этом } n(1-\varphi) = \deg(1-\varphi)$$

Докажем, что $1-\varphi: E \rightarrow E$ сепараб. морфизм,
т.е. $k(E) \supset (1-\varphi)^*k(E)$ сепараб. морф.

Тожд., т.к. $1-\varphi$ — автоморфизм, то

$$\nexists x \in E(E): (1-\varphi)(x) = 0$$

"

$$\deg(1-\varphi) \quad \ker(1-\varphi) = \emptyset(k).$$

$$|\#E(k) - q - 1| \leq 2\sqrt{q}.$$

Кривая, отображ. $\varphi: C \rightarrow C$ сепараб. $\Leftrightarrow$

$$\exists x \in C(k):$$

$1-\varphi$ — сепараб.

$$\left\{ \begin{array}{l} \text{Нужно } \exists x \in C(k); \text{ т.н. } d\varphi|_x = 0 \Rightarrow \\ \Rightarrow \varphi \text{ сепараб.} \end{array} \right.$$

$$d\varphi|_0 = 0 \Leftrightarrow \text{т.н.}$$

$$\Rightarrow d(1-\varphi)|_0 = 0.$$

см. осязат.

$$x \xrightarrow{\varphi} y$$

$$m_y/2 \xrightarrow{\sim} m_x/2$$

$$b_x \notin m_y \subset \varphi^*(k(C)) \subset k(C)^p$$

$$0 \times 0 \in C \times C$$

$$0 \times 0 \xrightarrow{\oplus} 0$$

$$d \oplus (x, y) = x + y$$

$$C \xrightarrow{id \times \varphi} C \times C$$

$$d(id \times \varphi) = id \times d\varphi = id \times 0$$

$$C \xrightarrow{id \times \varphi} C \times C \xrightarrow{\oplus} C$$

$$T_{0 \times 0} = T_0 \times T_0$$

$$\underline{0} \xrightarrow{\underline{\varphi}} \underline{0}$$

$$C \xrightarrow{\quad} C \times C \xrightarrow{\oplus} C$$

$$x \mapsto x \times 1 \quad = id$$

$$C \xrightarrow{\quad} C \times C \xrightarrow{\oplus} C$$

$$y \mapsto 1 \times y \quad = id$$

Объяснение, по чему ~~$d(1+\varphi)$~~
 $d(1-\varphi) = d(1) + d(-\varphi) = d(1) = 0$

где C — нл. кривая, φ — морфизм Фробениуса.

Приложение к теории кодирования

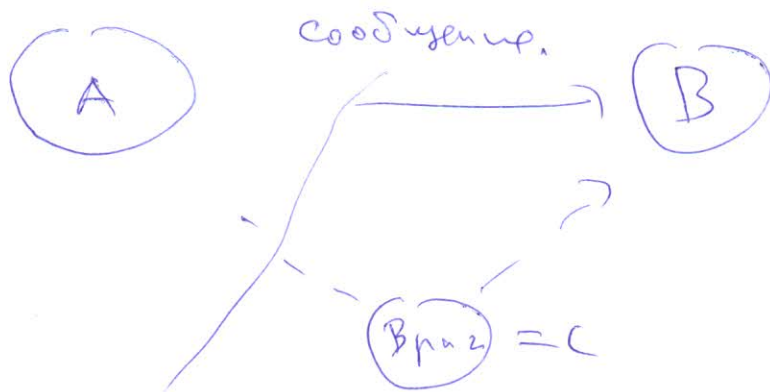
26.

Угн. Пусть задана группа E , т.е.
умножение в E задано. "вещным образом",
при этом для групп. $m \in \mathbb{Z}$: $x \in E$, ~~$y \in E$~~

$$x \mapsto mx = y$$

"обратно, если мы знаем y и x
найти m , такое что $mx = y$.

целое:



кодиров. $x, y \in E$, т.е.
 $mx = y$.

$m \in \mathbb{N}$ — код.
(Знаем A и B ,
но не знаем
 C !)

В) получаем x, y , проверяем, если
 $mx = y$, то все ок, соотнесение кодировки.

С) необходимо было соотнесение и имеет
составное логичное допущение : нужно проверить,
 $x', y' \in E$, т.е. $mx' = y'$.
Так как нужно найти $m \in \mathbb{N}$ (код) $\Rightarrow$
нужно, очень важно.

В качестве E рассмотрим кольцо

(17)

$$(\mathbb{Z}/n\mathbb{Z})^* = E$$

и то ~~$\cong$~~ $(E, 0)$
или, что

$$E(\mathbb{F}_q) = E$$

Важная вытекающая из Харди-Литтлвуда
на $\# E(\mathbb{F}_q)$ (мощность
Группы Ли)

Пример (группы) $(E, 0) = \{ y^2 = x^3 + Ax + B \}$
и то для всех $(x, y) \in E$
или, что

Рассмотрим ψ_m — полиномы от x, y ,
задаваемые по индукции:

$$\psi_1 = 1, \quad \psi_2 = 2Y$$

$$\psi_3 = 3X^4 + 6AX^2 + 12BX - A^2$$

$$\psi_4 = 4Y(X^6 + 5AX^4 + 20BX^3 - 5A^2X^2 - 4ABX - 8B^2 - A^3)$$

и по индукции получаем:

$$\psi_{2m} = 2\psi_m(\psi_{m+2}\psi_{m-1} - \psi_{m+2}^2\psi_{m+1}^2)$$

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3$$

Таким образом, ψ_m (или m четно) и

$Y^{-1}\psi_m$ (или m нечетно) — многочлен от x, A, B

с coeff. из $\mathbb{Z}$. Показано,

$$\psi_m = X\psi_m^2 - \psi_{m-1}\psi_{m+1}$$

$$4Y\omega_m = \psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2,$$

так что ψ_m — многочлен от x, A, B степеней
в x со степенями coeff. 1 и $Y^{-1}\omega_m$ (или
и нечетно), ω_m (или m четно) — многочлен от
 x, A, B тогда

$$[m](X, Y) = \left(\frac{\psi_m}{Y^2}, \frac{\omega_m}{Y^3} \right)$$

см. о.д.ф.е