4 квітня

§12. Розв'язки рівнянь над скінченними полями

Озн-ня Алгебраїчний многовид над кільцем R це множина спільних нулів набору многочленів від кількох змінних з коефіцієнтами в R.

$\underline{x} = (x_1, \dots, x_n)$

$f_1, \dots, f_m \in R[x_1, \dots, x_n]$ задають алгебраїчний многовид X над R

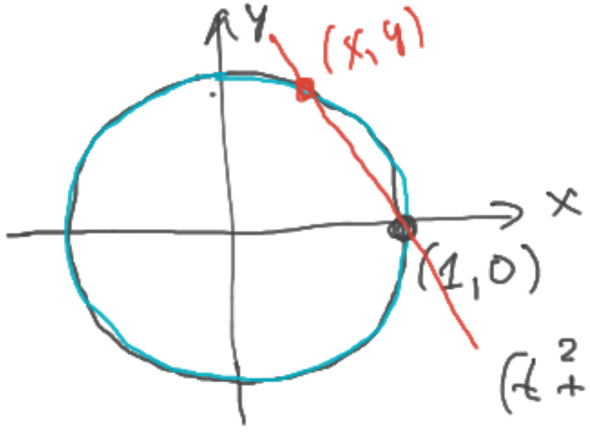
Позначення: X / R

Для будь-якого кільця $R' \supseteq R$ множина точок X над R' це

$$X(R') = \{ \underline{x} \in (R')^n : f_1(\underline{x}) = f_2(\underline{x}) = \dots = f_m(\underline{x}) = 0 \}.$$

Приклад $\{ x^2 + y^2 = 1 \} = X / \mathbb{Z}$

$X(\mathbb{R})$ $\qquad$ $X(\mathbb{Q})$ - ?



$y = t(x-1)$ ← наклон

$x^2 + t^2(x-1)^2 = 1$

$(t^2+1)x^2 - 2t^2 x + (t^2-1) = 0$

$\mathcal{D} = 4t^4 - (t^2+1)(t^2-1) = 4$

$$x_{1,2} = \frac{2t^2 \pm 2}{2(t^2+1)} = \begin{cases} 1 \\ \frac{t^2-1}{t^2+1} \end{cases} \Rightarrow y = \frac{-2t}{t^2+1}$$

$$X(\mathbb{Q}) = \left\{ \left(\frac{t^2-1}{t^2+1}, \frac{-2t}{t^2+1} \right) ; t \in \mathbb{Q} \right\} \cup \{(0,1)\}$$

Зауважимо, що для $N>2$ описати $X(\mathbb{Q})$ для $X=\{x^N+y^N=1\}$ буде дуже важко / неможливо /.

X алг. многовид над $\mathbb{F}_p$

Нехай $N_s = \#X(\mathbb{F}_{p^s})$, $s\geq 1$.

Озн-ня Формальний ряд

$$Z_X(T) = \exp\left(\sum_{s=1}^{\infty} N_s \frac{T^s}{s}\right)$$

$$= 1 + N_1 T + \ldots \in \mathbb{Q}[[T]]$$

називається дзета-функцією многовида X над $\mathbb{F}_p$.

Приклад $X = \{x = 0\}$ "точка"

$N_s = 1$, $s = 1, 2, 3, \ldots$

$$Z_X(T) = \exp\left(\sum_{s=1}^{\infty} \frac{T^s}{s}\right)$$

$$= \exp(-\log(1-T))$$

$$= \frac{1}{1-T}$$

Теорема (гіпотеза Вейля доведена Дворкіном в 1960) André Weil Bernard Dwork

Для будь-якого многовида $X/\mathbb{F}_p$ $Z_X(T) \in \mathbb{Q}(T)$.

Тобто $Z_X(T) = \frac{P(T)}{Q(T)}$

$P, Q \in 1 + T\mathbb{Q}[T]$

$$Z_X(T) = \frac{\prod_{i=1}^{k}(1-\alpha_i T)}{\prod_{j=1}^{l}(1-\beta_j T)}$$

над $\mathbb{C}$

$\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_l \in \overline{\mathbb{Q}}$ алгебрайчни числа

Вони наричаме се обернени корени на дзета-функцията

$$\sum_{s=1}^{\infty} N_s \frac{T^s}{s} = \sum_{i=1}^{k} \log(1-\alpha_i T) - \sum_{j=1}^{l} \log(1-\beta_j T)$$

$$= \sum_{s=1}^{\infty} \left(\sum_{j=1}^{l} \beta_j^s - \sum_{i=1}^{k} \alpha_i^s \right) \frac{T^s}{s}$$

$$\Rightarrow N_s = \sum_{j=1}^{l} \beta_j^s - \sum_{i=1}^{k} \alpha_i^s$$

$X = \{ x^2 + y^2 = 1 \}$ $\boxed{p>2}$

$$\#X(\mathbb{F}_p) = \sum_{\substack{a,b \in \mathbb{F}_p \\ a+b=1}} \#\{x \in \mathbb{F}_p : x^2 = a\} \cdot \#\{y \in \mathbb{F}_p : y^2 = b\}$$

$$= \sum_{a+b=1} \left(1+\left(\frac{a}{p}\right)\right)\left(1+\left(\frac{b}{p}\right)\right)$$

$$= p + \underbrace{\sum_{a \in \mathbb{F}_p} \left(\frac{a}{p}\right)}_{\text{"0"}} + \underbrace{\sum_{b \in \mathbb{F}_p} \left(\frac{b}{p}\right)}_{\text{"0"}} + \sum_{a+b=1} \left(\frac{a \cdot b}{p}\right)$$

$$= p + \sum_{a \in \mathbb{F}_p} \left(\frac{a(1-a)}{p}\right) =$$

$$= p + \sum_{a \in \mathbb{F}_p \setminus \{1\}} \left(\frac{a/(1-a)}{p} \right)$$

$$\frac{a}{1-a} = c \qquad a = c - ac \qquad a = \frac{c}{1+c}$$

$$c \neq -1$$

$$= p + \sum_{c \in \mathbb{F}_p \setminus \{-1\}} \left(\frac{c}{p} \right)$$

$$= p - \left(\frac{-1}{p} \right) = p - (-1)^{\frac{p-1}{2}}$$

$\#X(\mathbb{F}_{p^s}) - ?$

Озн-ня G скінченна комутативна група.

Гомоморфізми

$$\chi : G \to \mathbb{C}^\times$$

наз-ся характерами G.

$\chi(1) = 1$

$\chi(g_1 g_2) = \chi(g_1)\chi(g_2)$

$\forall g \in G \quad g^{\#G} = 1 \Rightarrow$

$\chi(g)^{\#G} = \chi(g^{\#G}) = \chi(1) = 1$

Образ $\chi(G) \subset \{$ корені ступеня $\#G$ з $1\}$

Позн-ня $\widehat{G} = \{$ характери $G \}$

також ком. група

$$(\chi_1 \cdot \chi_2)(g) = \chi_1(g)\,\chi_2(g)$$

$\varepsilon \in \widehat{G}$ тривіальний характер

$\varepsilon(g) = 1 \quad \forall g$

$\in$ одиницею $\widehat{G}$

Приклад

$G = \mathbb{F}_p^{\times}$ $\quad \chi(g) = \left(\frac{g}{p}\right)$

$\left(\frac{\cdot}{p}\right) \in \widehat{G}$

елемент порядка 2 $\quad \left(\frac{\cdot}{p}\right)^2 = \varepsilon$

Лема 1 $\quad \forall\, \chi \in \widehat{G}$

$$\sum_{g \in G} \chi(g) = \begin{cases} \#G & \chi = \varepsilon \\ 0 & \chi \neq \varepsilon \end{cases}$$

Дов-ня Для $\chi = \varepsilon$ очевидно.

Нехай $\chi \neq \varepsilon$ і $g_0 \in G$ є таким що $\chi(g_0) \neq 1$.

Тоді

$$\sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(g g_0) = \chi(g_0) \sum_{g \in G} \chi(g)$$

$g \longmapsto g \cdot g_0$ це бієкція $G \to G$

$(1 - \chi(g_0)) \sum_{g \in G} \chi(g) = 0$

$1 - \chi(g_0) \neq 0 \Rightarrow \sum_g \chi(g) = 0$ ∎

Для $G = \mathbb{F}_{p^s}^\times$ нехай

$\chi_2 \in \widehat{G}$ це (єдиний)

характер порядка 2.

$G = \langle g_s \rangle \quad \chi_2(g_s) = -1$

Домовленість 1 Характер

$\chi \in \widehat{\mathbb{F}_{p^s}^\times}$ продовжується

до функції $\chi : \mathbb{F}_{p^s} \to \mathbb{C}$

як

$$\chi(0) = \begin{cases} 1, & x = \varepsilon, \\ 0, & x \neq \varepsilon. \end{cases}$$

Тоді $\chi_2(0) = 0$.

$\chi_2(g_s^m) = (-1)^m$

Для $a \in \mathbb{F}_{p^s}$ маємо

$$\#\{x \in \mathbb{F}_{p^s} : x^2 = a\} = 1 + \chi_2(a)$$

$$\#X(\mathbb{F}_{p^s}) = \sum_{\substack{a,b \in \mathbb{F}_{p^s} \\ a+b=1}} (1+\chi_2(a))(1+\chi_2(b))$$

$$\underset{\text{лема 1}}{=} p^s + \sum_{a \in \mathbb{F}_{p^s} \setminus \{1\}} \chi_2\left(\frac{a}{1-a}\right)$$

$$= p^s - \chi_2(-1)$$

$X = \{x^2 + y^2 = 1\}$

$\#X(\mathbb{F}_{p^s}) = p^s - \chi_2(-1)$

$x^2 = -1$ має корені в $\mathbb{F}_{p^s}^\times$

т.т.т.к. $4 \mid (p^s - 1)$

$p \equiv 1 \pmod 4 \quad \chi_2(-1) = 1 \quad \forall s$

$p \equiv -1 \pmod 4 \quad \chi_2(-1) = (-1)^s \quad \forall s$

$\#X(\mathbb{F}_{p^s}) = p^s - \left((-1)^{\frac{p-1}{2}}\right)^s$

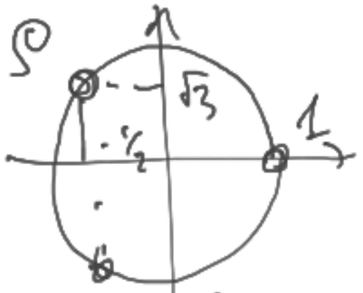
$\beta \uparrow \quad \uparrow \alpha$

$$Z_X(T) = \frac{1 - (-1)^{\frac{p-1}{2}} T}{1 - pT}$$

$\{x^3 + y^3 = 1\} = X$

Для простоти нехай

$\boxed{p \equiv 1 \pmod 3}$



$\bar\rho = \rho^2$

$\rho = \exp\left(\frac{2\pi i}{3}\right) = \frac{-1 + \sqrt{-3}}{2}$

$\rho^3 = 1$

$\mathbb{F}_{p^s}^\times = \langle g_s \rangle$

Розглянемо характер порядка 3

$\chi_3(g_s^i) = \rho^i, \quad i = 0, 1, 2, \dots$

$\#\{x \in \mathbb{F}_{p^s} : x^3 = a\} = \begin{cases} 0, & 3 \nmid i \\ 3, & 3 \mid i \end{cases} =$

$a \in \mathbb{F}_{p^s} \qquad a = g_s^i$

$$\#\{x \in \mathbb{F}_{p^s} : x^3 = a\}$$

$$= 1 + \chi_3(a) + \chi_3(a)^2$$

також: вірно для $a = 0$ за домовленістю 1.

Тому

$$\#X(\mathbb{F}_{p^s}) = \sum_{a+b=1} \left(\sum_{i=0}^{2} \chi_3(a)^i \right) \left(\sum_{j=0}^{2} \chi_3(b)^j \right)$$

Домовленість 2

$\chi^0 = \varepsilon$

$$= \sum_{i,j=0}^{2} \left(\sum_{a+b=1} \chi_3^i(a)\, \chi_3^j(b) \right)$$

Озн-ня Для пари характерів χ, ψ на $\mathbb{F}_{p^s}^*$ сума

$$J(\chi, \psi) = \sum_{\substack{a,b \in \mathbb{F}_{p^s} \\ a+b=1}} \chi(a)\,\psi(b)$$

наз-ся сумою Якобі.

Потрібно з суми Якобі над $\mathbb{F}_p$. Для цього корисно означити

Суми Гаусса для характера $\chi \in \mathbb{F}_p^\times$:

$$g(\chi) = \sum_{x \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}} \chi(x) \zeta_p^x \in \overline{\mathbb{Q}}$$

де $\zeta_p = \exp\left(\frac{2\pi i}{p}\right)$, $\zeta_p^p = 1$.

Тв-ня 2 $g(\varepsilon) = 0$ і для $\chi \neq \varepsilon$ $|g(\chi)| = \sqrt{p}$.

Довед-ня: ε : вправа

$\chi \neq \varepsilon$

Введемо допоміжні суми з параметром $a \in \mathbb{F}_p$

$$g_a(\chi) = \sum_{x \in \mathbb{F}_p} \chi(x) \zeta_p^{ax}$$

$a = 0$: $g_0(\chi) = \sum_{x \in \mathbb{F}_p} \chi(x) = 0$

$a \neq 0$: $g_a(\chi) = \sum_x \chi(a^{-1}) \chi(ax) \zeta_p^{ax}$

$$= \chi(a^{-1}) \sum_y \chi(y) \zeta_p^y = \chi(a^{-1}) g(\chi)$$

Обчислимо суму двома способами:

$$\sum_{a \in \mathbb{F}_p} g_a(\chi) \overline{g_a(\chi)} = |g(\chi)|^2 \sum_a |\chi(a)|^2$$

$$= (p-1) |g(\chi)|^2$$

$$\sum_{a\in\mathbb{F}_p} g_a(x)\,\overline{g_a(x)}$$

$$= \sum_{a\in\mathbb{F}_p} \sum_{x,y\in\mathbb{F}_p} \chi(x)\overline{\chi(y)}\, \zeta_p^{a(x-y)}$$

$z = x-y$

$$\left| \sum_{a\in\mathbb{F}_p} \zeta_p^{az} = \begin{cases} p, & z=0 \\ 0, & z\neq 0 \end{cases} \right.$$

$z\in\mathbb{F}_p$

$$= p \sum_{x} |\chi(x)|^2$$

тільки складників

$z^x = y$

$$= p(p-1)$$

$$(p-1)\,|g(x)|^2 = p(p-1)$$

$\boxtimes$

Тв-ма 3 Для сум Якобі над $\mathbb{F}_p$ виконується:

i) $J(\varepsilon,\varepsilon) = p$

ii) $J(\varepsilon,\chi) = 0 \quad \chi\neq\varepsilon$

iii) $J(\chi,\chi^{-1}) = -\chi(-1) \quad \chi\neq\varepsilon$

$\chi(-1) \in \{\pm 1\}$

iv) $\chi,\psi,\chi\cdot\psi \neq \varepsilon$

$$J(\chi,\psi) = \frac{g(\chi)\,g(\psi)}{g(\chi\psi)}$$

Наслідок: $|J(\chi,\psi)| = \sqrt{p}$

(Твки 2 і 3) коли $\chi,\psi,\chi\cdot\psi\neq\varepsilon$

Доб-во i) $\mathcal{J}(\varepsilon,\varepsilon) = \sum_{a+b=1} 1 = p$

ii) $\mathcal{J}(\varepsilon,\chi) = \sum_a \chi(a) \overset{\text{лемма 1}}{=} 0$

iii) $\mathcal{J}(\chi,\chi^{-1}) = \sum_{a\in\mathbb{F}_p\setminus\{1\}} \chi\left(\frac{a}{1-a}\right)$

$= \sum_{c\in\mathbb{F}_p\setminus\{-1\}} \chi(c) = -\chi(-1)$

iv) $g(\chi)g(\psi) = \sum_{x,y} \chi(x)\psi(y)\zeta_p^{x+y}$

$= \sum_{t\in\mathbb{F}_p} \zeta_p^t \sum_{x+y=t} \chi(x)\psi(y)$

$= \sum_x \chi(x)\psi(-x) + \sum_{t\in\mathbb{F}_p^*} \zeta_p^t \sum_{x'+y'=1} \chi(tx')\psi(ty')$

$t=0$ ↑ $t\neq 0$ ↑ $x=tx',\ y=ty'$

$= \psi(-1)\sum_x (\chi\cdot\psi)(x) + \sum_{t\in\mathbb{F}_p^*} \zeta_p^t \chi(t)\psi(t)$

лемма 1 ↑ $\underbrace{\quad}_{x}$ ↑ 0 ↑ $\times\ \mathcal{J}(\chi,\psi)$

$= g(\chi\psi)\cdot\mathcal{J}(\chi,\psi)$ ☒

$X = \{x^3+y^3=1\}$

$\#X(\mathbb{F}_p) = \sum_{i,j=0}^{2} \mathcal{J}(\chi_3^i,\chi_3^j)$

$p\equiv 1 \pmod 3$

$|\mathcal{J}(\chi_3^i,\chi_3^j)|$ — за Тв. изм 3

i \ j	0	1	2
0	p	0	0
1	0	$\sqrt{p}$	1
2	0	1	$\sqrt{p}$

Суми Гаусса та Якобі для $\mathbb{F}_{p^s}$

Слід

$$Tr : \mathbb{F}_{p^s} \longrightarrow \mathbb{F}_p$$

$$x \longmapsto x + x^p + x^{p^2} + \ldots + x^{p^{s-1}}$$

Тв-ня 4 Слід є $\mathbb{F}_p$-лінійним сюр'єктивним відображенням.

Дов-ня Тв-ня 6 §11 $\Rightarrow (x+y)^{p^d} = x^{p^d} + y^{p^d}$, $d \geq 1$

тому $Tr(x+y) = Tr(x) + Tr(y)$.

Для $a \in \mathbb{F}_p$ $a^{p^d} = a$, $d \geq 1$.

Тому

$$Tr(ax) = \sum_{d=1}^{s-1} (ax)^{p^d} = a \sum_{d=1}^{s-1} x^{p^d} = a\,Tr(x).$$

Лінійність доведено.

Сюр'єктивність: рівняння $x + x^p + \ldots + x^{p^{s-1}} = 0$ має не більше p^{s-1} розв'язків в $\mathbb{F}_{p^s}$. $\# \mathbb{F}_{p^s} = p^s$, тому існує $z \in \mathbb{F}_{p^s}$ т.щ. $Tr(z) \neq 0$, $Tr(z) = c \in \mathbb{F}_p$.

Тоді для $\forall b \in \mathbb{F}_p$

$$Tr\left(\left(\tfrac{b}{c}\right) z\right) = \frac{b}{c} Tr(z) = b. \quad \boxtimes$$

де $\frac{b}{c} \in \mathbb{F}_p$.

Озн-ня Сума Гаусса для $\chi \in \widehat{\mathbb{F}_{p^s}^{\times}}$ це

$$g(\chi) = \sum_{x \in \mathbb{F}_{p^s}} \chi(x)\, \zeta_p^{Tr(x)}.$$

$$g(\chi) = \sum_{x \in \mathbb{F}_{p^s}} \chi(x)\, \zeta_p^{\mathrm{Tr}(x)}$$

Вправи: 1) Нехай

$$\lambda : \mathbb{F}_{p^s} \to \mathbb{C}^\times$$
$$x \longmapsto \zeta_p^{\mathrm{Tr}(x)}$$

Доведіть що

- $\lambda(x+y) = \lambda(x)\lambda(y)$
- $\exists\, z \in \mathbb{F}_{p^s}$ т.ч. $\lambda(z) \neq 1$
- $\sum_{x \in \mathbb{F}_{p^s}} \lambda(x) = 0$!

2) Доведіть для характерів над $\mathbb{F}_{p^s}$:

$g(\varepsilon) = 0$ і $|g(\chi)| = p^{s/2}$ $\forall \chi \neq \varepsilon$

$\mathcal{Y}(\varepsilon, \varepsilon) = p^s$

$\mathcal{Y}(\varepsilon, \chi) = 0 \quad \forall \chi \neq \varepsilon$

$\mathcal{Y}(\chi, \bar{\chi}^{-1}) = -\chi(-1) \in \{\pm 1\}$ $\forall \chi \neq \varepsilon$

$\chi, \psi, \chi\psi \neq \varepsilon$

$$\mathcal{Y}(\chi, \psi) = \frac{g(\chi)\, g(\psi)}{g(\chi\psi)}$$

$$\left(\Rightarrow |\mathcal{Y}(\chi, \psi)| = p^{s/2} \right)$$

$N: \mathbb{F}_{p^s} \to \mathbb{F}_p$ норма

$$x \longmapsto x^{1+p+p^2+\ldots+p^{s-1}}$$

Вправа: 1) $N(xy) = N(x)N(y)$

2) Якщо $\mathbb{F}_{p^s}^{\times} = \langle g_s \rangle$

то $g = N(g_s)$ породжує $\mathbb{F}_p^{\times}$:

$\mathbb{F}_p^{\times} = \langle g \rangle$.

3) N є сюр'єктивною

Озн-ня Для хар-ра $\chi \in \widehat{\mathbb{F}_p^{\times}}$ характер над $\mathbb{F}_{p^s}$ індукований χ

це $\tilde{\chi} = \chi \circ N : \mathbb{F}_{p^s}^{\times} \to \mathbb{C}^{\times}$.

Теорема 5 (співвідношення Хасе – Давенпорта)

$$g(\tilde{\chi}) = g(\chi)^s.$$

(Можна прочитати доведення в Ireland, Rosen A Classical Introduction to Modern Number Theory)

Тепер можемо перевірити Теорему Дворка для $X = \{ x^N + y^N = 1 \}$

(у випадку $p \equiv 1 \bmod N$ - для простоти).

$N \mid (p-1) \Rightarrow$ існує характер порядка N на $\mathbb{F}_p^\times$.

Виберемо генератор $\mathbb{F}_p^\times = \langle g \rangle$ і нехай

$$\chi_N(g) = \zeta_N = \exp\left(\frac{2\pi i}{N}\right) \in \mathbb{C}^\times.$$

Тоді для $a \in \mathbb{F}_{p^s}$

$$\#\{ x \in \mathbb{F}_{p^s} : x^N = a \} = \sum_{j=0}^{N-1} \tilde{\chi}_N^j(a).$$

і маємо

$$\#X(\mathbb{F}_{p^s}) = \sum_{i,j=0}^{N-1} J(\tilde{\chi}_N^i, \tilde{\chi}_N^j) =$$

$$= p^s + \sum_{\substack{i+j \neq N \\ i,j \geq 1}} J(\chi_N^i, \chi_N^j)^s - \sum_{i=1}^{N-1} \chi_N(-1)^{si}$$

Тут є ще одна корисна властивість:

Твердження 7

Якщо $\chi \in \widehat{\mathbb{F}_{p^s}^{\times}}$, $\chi \neq \varepsilon$

то $g(\chi)\, g(\bar{\chi}^{-1}) = \chi(-1)\, p^s$

Дов-ня: Вправа.

$$\Downarrow$$

$$J(\chi^{-1}, \psi^{-1}) = \frac{p^s}{J(\chi, \psi)}.$$

$\chi, \psi, \chi\psi \neq \varepsilon$

$$X = \{ x^N + y^N = 1 \}$$

$$\#X(\mathbb{F}_{p^s}) = p^s - \sum_{i=1}^{N-1} \chi_N(-1)^{is} + \sum_{\substack{i,j \geq 1 \\ i+j<N}} \left(J(\chi_N^i, \chi_N^j)^s + \left(\frac{p}{J(\chi_N^i, \chi_N^j)} \right)^s \right)$$

Видно обернені корені дзета-функції.

Їх $|\cdot|$ це p, 1 та $\sqrt{p}$.