31 березня

§10. Формула обернення Мебіуса

$$\mathbb{N} = \{1, 2, 3, \dots\} = \mathbb{Z}_{\geq 1}$$

Озн-ня Функція Мебіуса

$$\mu : \mathbb{N} \longrightarrow \{0, 1, -1\}$$

$$\mu(n) = \begin{cases} 1, & n = 1 \\ 0, & n \text{ не вільне від квадратів} \\ (-1)^k, & n = p_1 \cdot \dots \cdot p_k \end{cases}$$

Лема 1 Для $n > 1$ виконується

$$\sum_{d \mid n} \mu(d) = 0.$$

Дов-ня $n = p_1^{e_1} \dots p_r^{e_r}$

$$\sum_{d \mid n} \mu(d) = \underset{\vec{d=1}}{1} + \sum_{\ell=1}^{r} \binom{r}{\ell} (-1)^\ell$$

$$= (1-1)^r = 0$$

$$(x+y)^r = \sum_{\ell=0}^{r} \binom{r}{\ell} x^\ell y^{r-\ell} \quad \boxtimes$$

Озн-ня Для $f, g : \mathbb{N} \to \mathbb{C}$ добуток Діріхле

$$(f \circ g)(n) = \sum_{d \mid n} f(d)\, g\left(\frac{n}{d}\right)$$

$f \circ g : \mathbb{N} \to \mathbb{C}$

- комутативність $f \circ g = g \circ f$

- асоціативний

$$f \circ (g \circ h) = (f \circ g) \circ h$$

$$\sum_{(d_1, d_2, d_3) \in \mathbb{N}^3 \text{ т.щ. } d_1 d_2 d_3 = n} f(d_1)\, g(d_2)\, h(d_3)$$

Позначимо: $\mathbb{I}(n) = \begin{cases} 1, & n = 1 \\ 0, & n > 1 \end{cases}$

$\mathbb{1}(n) = 1, \ \forall n$

$f \circ \mathbb{I} = f \quad \forall f$

$$(f \circ \mathbb{1})(n) = \sum_{d \mid n} f(d)$$

$\begin{cases} \text{Лема 1} \iff \mu \circ \mathbb{1} = \mathbb{I} \\ \mu(1) = 1 \end{cases}$

Теорема 2 (формула обернення Мебіуса)

$f : \mathbb{N} \to \mathbb{C}$

і нехай $\forall n \ g(n) = \sum_{d \mid n} f(d)$.

$(g = f \circ \mathbb{1})$.

Тоді $\forall n \ f(n) = \sum_{d \mid n} \mu(d)\, g\left(\frac{n}{d}\right)$

$(f = g \circ \mu)$

Довед-ня $(g = f \circ \mathbb{1}) \circ \mu$

$\Rightarrow g \circ \mu = f \circ \mathbb{1} \circ \mu = f \circ \mathbb{I} = f$

↑ лема 1

∎

§11. Скінченні поля

Приклад $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

p просте число

Чи існують інші поля зі скінченною кількістю елементів?

Нехай F це скінченне поле і $q = \#F$.

Тоді $F^* = F \setminus \{0\}$

з операцією $\cdot$ це група з $q-1$ елементів

$\Rightarrow \forall \alpha \in F^* \quad \alpha^{q-1} = 1$

$\Leftrightarrow \forall \alpha \in F \quad \alpha^q = \alpha$

Тв-ня 1 В кільці $F[x]$

$$x^q - x = \prod_{\alpha \in F} (x - \alpha)$$

Дов-ня $F = \{\alpha_1, \dots, \alpha_q\}$

$f(x) = x^q - x$

$f(\alpha_1) = 0 \Rightarrow f(x) = (x - \alpha_1) f_1(x)$

$0 = f(\alpha_2) = (\alpha_2 - \alpha_1) f_1(\alpha_2) \Rightarrow f_1(\alpha_2) = 0$

$\Rightarrow f(x) = (x - \alpha_1)(x - \alpha_2) f_2(x)$

$\dots$

$f(x) = (x - \alpha_1) \dots (x - \alpha_q) f_q(x)$

$\deg(f) = q \Rightarrow \deg(f_q) = 0$

коректований $f_q = 1$ ∎

Наслідок 2 Нехай $F \subset K$ для деякого поля K. Тоді $\alpha \in K$ належить до F т.т.т.к. $\alpha^q = \alpha$.

Дов-во Мн-н $X^q - X$ має не більше ніж q різних коренів в K. Оскільки $\#F = q$ є різними коренями цього многочлена, то інших коренів в K немає.

Наслідок 3 Якщо $f \in F[x]$ ділить $X^q - X$, то f має $d = \deg(f)$ різних коренів в F.

Твірка 4 Мультиплікативна група $F^\times$ є циклічною.

Дов-во Якщо $d \mid q-1$ то $x^d - 1 \mid x^{q-1} - 1$ (вправа)

Наслідок 3 $\Rightarrow$ $X^d - 1$ має d різних коренів в F

Нехай $\psi(d) :=$ кількість елементів порядка d в $F^\times$

Тоді

$$d = \#\{\alpha \in F : \alpha^d - 1\} = \sum_{c \mid d} \psi(c)$$

Лема 1 б §8 : $d = \sum_{c \mid d} \psi(c)$

Формула обернення Мебіуса:

$$\psi(d) = \sum_{c \mid d} \mu(c) \frac{d}{c} = \varphi(d)$$

Зокрема

$$\psi(q-1) = \varphi(q-1) > 0,$$

і тому існують ел-ти порядка $q-1$. ☒

адитивна структура

$$\lambda : \mathbb{Z} \longrightarrow F$$

$$n \longmapsto n\cdot 1 = \begin{cases} \underbrace{1+\dots+1}_{n} & n \geq 1 \\ 0 & n = 0 \\ \underbrace{-1-\dots-1}_{-n} & n < 0 \end{cases}$$

гомоморфізм кілець (зберігає операції) + та $\cdot$

$\lambda(\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}$ для деякого $m > 0$

(оскільки $\#F < \infty$)

$\lambda(\mathbb{Z}) \subset F$

F поле $\Rightarrow$ $\lambda(\mathbb{Z})$ не область цілості

(немає дільників 0)

$\mathbb{Z}/m\mathbb{Z}$ є областю цілості т.т.т.к. m не просте число

$m = p$

Цілі кратні $1 \in F$ утворюють підполе $\mathbb{F}_p \subset F$.

$\Rightarrow F$ є векторним пр-ром над $\mathbb{F}_p$

Нехай $\omega_1, \dots, \omega_n \in F$ не деякий базис, тобто $\dim_{\mathbb{F}_p}(F) = n$.

$$F = \sum_{i=1}^{n} \mathbb{F}_p \omega_i$$

$$q = \#F = p^n$$

Ми довели

Тв-ня 5 Кількість елементів у скінченному полі є степенем простого числа.

Озн-ня : Для довільного поля K, розглянемо (якщо воно існує) найменше $m \in \mathbb{N}$ таке що $m \cdot 1 = \underbrace{1+\ldots+1}_{m} = 0$ в K. З міркувань вище $m = p \in$ простим числом.

Воно наз-ся характеристикою поля K.

Якщо $m \cdot 1 \neq 0 \ \forall m \in \mathbb{N}$, то говорять що хар-ка $= 0$.

Позначення: $\mathrm{char}(K) = \begin{cases} p \\ 0 \end{cases}$

Поля з $\mathrm{char}(K) = p$ наз-ся полями скінченої хар-ки.

Наприклад, $K = \mathbb{F}_p(t)$ поле раціональних функцій з коефіцієнтами в $\mathbb{F}_p$ є полем хар-ки $p > 0$.

Тв-ня 6 Нехай K не поле, $\mathrm{char}(K) = p > 0$. Тоді для всіх $d \geq 1$ маємо

$$(\alpha + \beta)^{p^d} = \alpha^{p^d} + \beta^{p^d}$$

для будь-яких $\alpha, \beta \in K$.

Дов-ня Для $d = 1$

$$(\alpha+\beta)^p = \alpha^p + \sum_{k=1}^{p-1} \binom{p}{k} \alpha^k \beta^{p-k} + \beta^p$$

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} \equiv 0 \pmod{p}$$

$$(*) \quad = \alpha^p + \beta^p$$

Для більших d доводимо за індукцією: якщо для деякого d тв-ня вірне

$$(*)(*) \quad (\alpha+\beta)^{p^d} = \alpha^{p^d} + \beta^{p^d} \quad \forall \alpha, \beta$$

підносимо до p-го степеня:

$$(\alpha+\beta)^{p^{d+1}} = \left(\alpha^{p^d} + \beta^{p^d}\right)^p = \alpha^{p^{d+1}} + \beta^{p^{d+1}}$$

$(*)(*)$ пр-ня індукції; $(*)$

□

Зауваження: $\Phi: K \to K$, $\alpha \mapsto \alpha^p$ є ендоморфізмом поля. Він наз-ся ендоморфізмом Фробеніуса.

Проміжні поля

F поле з $q = p^n$ ел-тів

Нехай $L \subset F$ не деяке підполе.

$m = \dim_L(F)$

Тоді якщо $\#L = (p')^d$

то

$$p^n = \#F = (\#L)^m = (p')^{d \cdot m}$$

$$\Rightarrow p' = p \quad і \quad d \mid n$$

Тв-ка 7 Підполе $L \subset F$ знаходиться у бієктивній відповідності з дільниками $d \mid n$.

Дов-во Вище ми показали що кожне $L \subset F$ має p^d ел-тів для деякого $d \mid n$.

Нехай тепер $d \mid n$ не деякий дільник. Розглянемо множину

$$L = \{ \alpha \in F : \alpha^{p^d} = \alpha \} \subset F.$$

Вправа: В $K[x]$ для $\forall$ поля K маємо

$$x^l - 1 \mid x^m - 1 \text{ т.т.т.к. } l \mid m$$

$d \mid n \underset{\text{Вправа}}{\Rightarrow} p^d - 1 \mid p^n - 1$

$\underset{\text{Вправа}}{\Rightarrow} X^{p^d-1} - 1 \mid X^{p^n-1} - 1$

Наслідок 3 $\Rightarrow \#L = p^d$.

L не поле: $\alpha, \beta \in L$

$(\alpha \cdot \beta)^{p^d} = \alpha^{p^d} \cdot \beta^{p^d} = \alpha \cdot \beta$

$\Rightarrow \alpha \cdot \beta \in L$

$(\alpha + \beta)^{p^d} = \alpha^{p^d} + \beta^{p^d} = \alpha + \beta$

Тв-ка 6

$\Rightarrow \alpha + \beta \in L$

$0, 1 \in L \quad (-\alpha)^{p^d} = (-1)^{p^d} \cdot \alpha^{p^d} = (-1)^p \cdot \alpha$

$= -\alpha \ (\underset{\text{коли } p=2}{-1=1})$

$\alpha^{-1} = \alpha^{p^d-2}$ для $\alpha \neq 0$.

Нехай $L' \subset F$ є іншим підполем з p^d елементів то за наслідком 2

$L' = \{\alpha \in F : \alpha^{p^d} = \alpha\}$

$\Rightarrow L' = L$ ⊠

Існування

Фіксуємо p

Теорема 8 Для кожного $n \geq 1$ існує єдине (з точністю до ізоморфізма) поле з p^n елементами.

Позначення: $\mathbb{F}_{p^n}$.

(т. мав)
⇑

Теорема 9 Для $d \geq 1$ позначимо

$F_d(x)$ = добуток всіх нормованих незвідних многочленів степеня d в $\mathbb{F}_p[x]$.

або = 1 якщо таких многочленів не існує.

Тоді для $n \geq 1$

$$x^{p^n} - x = \prod_{d \mid n} F_d(x).$$

Дов-ня Зауважимо що якщо $f(x) \mid x^{p^n} - x$ і $\deg(f) \geq 1$ то $f(x)^2 \nmid x^{p^n} - x$. Чому?

Якщо $x^{p^n} - x = f(x)^2 g(x)$

застосуємо $\frac{d}{dx}$

$$-1 = 2f(x)f'(x)g(x) + f(x)^2 g'(x)$$

$f(x) \mid 1$ суперечність.

З огляду на це зауваження, достатньо довести наступне: якщо $f \in \mathbb{F}_p[x]$ це незвідний многочлен степеня d, $d \mid n$, то $f \mid x^{p^n} - x$ т.т.т.к.

(⇒) Припустимо що

$$x^{p^n} - x = f(x)\, g(x)$$

Γ

незвідний степеня d

в $\mathbb{F}_p[x]$.

Розглянемо поле $K = \mathbb{F}_p[x]/\langle f \rangle$.

Нехай $\beta \in K$ є образом x в K.

Тобто $f(\beta) = 0$. Тоді

$1, \beta, \dots, \beta^{d-1}$ не базис K

над $\mathbb{F}_p$. Тому $\#K = p^d$

і кожен $\alpha \in K$, $\alpha \neq 0$

задовольняє $\alpha^{p^d - 1} = 1$.

$$\beta^{p^n} - \beta = f(\beta) g(\beta) = 0$$

Π

0

Довільний ел-т

$$\alpha = a_0 + a_1\beta + \dots + a_{d-1}\beta^{d-1} \in K$$

$a_0, a_1, \dots, a_{d-1} \in \mathbb{F}_p$

задовольняє рівність

$\alpha^{p^n} - \alpha$:

$$\alpha^{p^n} = (a_0 + \dots + a_{d-1}\beta^{d-1})^{p^n}$$

$$= \underset{\text{Тв-ка 6}}{} a_0^{p^n} + a_1^{p^n}\beta^{p^n} + \dots + a_{d-1}^{p^n}(\beta^{p^n})^{d-1}$$

$$= a_0 + a_1\beta + a_2\beta^2 + \dots + a_{d-1}\beta^{d-1}$$

$a_i^{p} = a_i$ $\forall i$

$\beta^{p^n} = \beta$

$$= \alpha$$

$\Downarrow$

$$\prod_{\alpha \in K}(X - \alpha) = X^{p^d} - X \;\Big|\; X^{p^n} - X \quad \text{в } K[x]$$

$\Rightarrow$ Тв-ка 1

$\alpha^{p^d} = \alpha \quad \forall \alpha \in K$

$\Rightarrow \quad x^{p^d-1}-1 \mid x^{p^n-1}-1$

Вправа $\Rightarrow \quad p^d-1 \mid p^n-1$

Вправа: Дм $a \in \mathbb{Z}$, $a \geq 2$ та $1 \leq l \leq m$

$a^l-1 \mid a^m-1$ т.т.т.к. $l \mid m$

$\Rightarrow \quad d \mid n$

(⇐) Нехай $d = \deg(f) \mid n$. (f — незвідний)

Хочемо показати, що $f(x) \mid x^{p^n}-x$.

Розглянемо $K = \mathbb{F}_p[x]/\langle f \rangle$ та $\beta \in K$ т.ц. $f(\beta)=0$. (β ← образ x в факторі)

Оскільки $\#K = p^d$, то $\beta^{p^d-1} = 1$. Значить

$x^{p^d-1}-1 \in \langle f \rangle$,

тобто $f \mid x^{p^d-1}-1$ в $\mathbb{F}_p[x]$.

$d \mid n \underset{\text{Вправа}}{\Rightarrow} x^{p^d-1}-1 \mid x^{p^n-1}-1$

$\Rightarrow f \mid x^{p^n-1}-1$ ⊠

Нас-к 10 Нехай

N_d = # незвідних нормованих м-нів степеня d в $\mathbb{F}_p[x]$

Тоді

$$p^n = \sum_{d \mid n} d \cdot N_d$$

Нас-к 11 $\Rightarrow$ формула Мебіуса

$$N_n = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) p^d$$

$\binom{\infty\ \infty}{\infty}$

Дов-ня Теореми 8 (існування) в $\binom{\infty\ \infty}{\infty}$

число $\sum_{d \mid n} \mu\left(\frac{n}{d}\right) p^d$

$= p^n \pm \dots + \mu(n)\, p$

є сумою різних степенів p з коеф-тами ± 1.

Тому ще сума $\neq 0$:

$\pm p^{d_1} \pm p^{d_2} \pm \dots \quad d_1 < d_2 < \dots$

$\not\equiv 0 \mod p^{d_1+1}$.

$\Rightarrow N_n \neq 0$

Єдиність

Нехай F це деяке поле з p^n ел-тами.

$$\prod_{\alpha \in F} (x - \alpha) = x^{p^n} - x$$

(твердження 1)

$$= \prod_{d \mid n} \prod_{\substack{f \in \mathbb{F}_p[x] \\ \text{незвідний} \\ \text{нормований} \\ \text{степеня } d}} f(x)$$

$N_n \neq 0$: існують незвідні $f(x)$ степеня n і для кожного такого $f(x)$ існує $\alpha_f \in F$ т.ч. $f(\alpha_f) = 0$.

Тому $\mathbb{F}_p[x]/\langle f \rangle \cong F$

$$x \longmapsto \alpha_f$$

це ізоморфізм полів.

Робимо висновок, що всі поля $\mathbb{F}_p[x]/\langle f \rangle$ де $f \in$ незвідним многочленом степеня n $\in$ ізоморфними між собою, і також ізо-ними кожному полю з p^n ел-тами. ☒

Задача 5 / 7 списку

a) $p \equiv 1 \ (4)$

$\rightsquigarrow p = a^2 + b^2$ "однозначно"

p розщеплюється в $\mathbb{Z}[i]$

$= \mathcal{O}_K$

т.т.т.к.

$p \equiv 1 \ (4)$ $\quad K = \mathbb{Q}(i)$

$i = \sqrt{-1}$

$\Rightarrow \exists \ a + bi \in \mathbb{Z}[i]$

т.що. $p = (a+bi)(a-bi)$

$= a^2 + b^2$

Єдиність: розклад на прості множники однозначний з точністю до одиниць кільця

б) a або b в п. а) має бути парним ...

c)* $\sum_{x=0}^{p-1} \left(\frac{x^3 + Ax}{p} \right) =: S_p(A)$

$A \in \mathbb{Z}/p\mathbb{Z}$

$x \mapsto rx \quad r \in \mathbb{F}_p^\times \Rightarrow$ $= \mathbb{F}_p$

$S_p(r^2 A) = \left(\frac{r}{p}\right) S_p(A)$

$\Rightarrow$ якщо g примітивний корінь то

$S_p(A) = \pm 2\alpha \quad A = g^{4i}$ або g^{4i+2}

$= \pm 2\beta \quad A = g^{4i+1}$ або g^{4i+3}

для деяких $\alpha, \beta \in \mathbb{Z}$.

(Парність S_p випливає з $x \mapsto -x$)

α, β - ?

$$\sum_{A \in \mathbb{F}_p} S_p(A) = 2(p-1)(\alpha^2+\beta^2)$$

$$\sum_{A,x,y}^{11} \left(\frac{x^3+Ax}{p}\right)\left(\frac{y^3+Ay}{p}\right)$$

$$= \sum_{x,y} \left(\frac{xy}{p}\right) \sum_{A} \left(\frac{(x^2+A)(y^2+A)}{p}\right)$$

$A \to A + x^2$

$$= \sum_{x,y} \left(\frac{xy}{p}\right) \sum_{A} \left(\frac{A(A+y^2-x^2)}{p}\right)$$

Заважимо

$$\sum_{A} \left(\frac{A(A+z)}{p}\right) = \begin{cases} p-1 & z=0 \\ \gamma & z \neq 0 \end{cases}$$

↑ деяке число

бо сума не залежить від z: $A \mapsto Az$

$$\sum_{z} \sum_{A} \left(\frac{A(A+z)}{p}\right) = 0 \Leftarrow \sum_{z \in \mathbb{F}_p} \left(\frac{z}{p}\right) = 0$$

$\alpha \leftrightarrow$

$\Rightarrow \gamma = -1$

$$\sum_{x,y} \left(\frac{xy}{p}\right)\left(-1 + p \cdot \mathbb{1}_{x^2=y^2}\right)$$

$$= 2p(p-1)$$

$\mathbb{1}_{x^2=y^2} = \begin{cases} 0, & x^2 \neq y^2 \\ 1, & x^2 = y^2 \end{cases}$