28/02/2023

§5. Числові поля, існування первісного елемента та огляд факторизації ідеалів

Позначення: K/k розширення полів $k \subset K$

$[K : k] = \dim_k K$ степінь розширення

<u>Озн-ня</u> Розширення полів K/k наз-ся скінченним якщо K є скінченно-вимірним векторним пр-ром над k.

Скінченні розширення поля $\mathbb{Q}$ наз-ся числовими полями.

Приклад: $\xi \in \overline{\mathbb{Q}}$ $\quad f \in \mathbb{Q}[x]$ $\quad f(\xi) = 0$ мінімальний многочлен

$$\mathbb{Q}(\xi) = \{ g(\xi) : g \in \mathbb{Q}[x] \} = \sum_{i=0}^{n-1} \mathbb{Q}\xi^i$$

де $n = \deg(f)$

$[\mathbb{Q}(\xi) : \mathbb{Q}] = n$ $\quad$ просте розширення

$$\mathbb{Q}(\xi) \cong \mathbb{Q}[x]/\langle f \rangle$$

$\xi_1, \dots, \xi_m \in \overline{\mathbb{Q}}$ $\quad \mathbb{Q}(\xi_1, \dots, \xi_m) = \{ P(\xi_1, \dots, \xi_m) : P \in \mathbb{Q}[x_1, \dots, x_m] \}$

степінь – ?

$\leq \deg(f_1) + \dots + \deg(f_m)$

<u>Теорема 1</u> $K/\mathbb{Q}$ числове поле

$\exists\, \theta \in K$ т.щ. $K = \mathbb{Q}(\theta)$

Кожен такий елемент θ наз-ся первісним елементом.

Наприклад: $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ $\quad \theta = \sqrt{2} + \sqrt{3}$

$\sqrt{2} = \frac{1}{2}(\theta^3 - 9\theta)$ $\quad \sqrt{3} = -\frac{1}{2}(\theta^3 - 11\theta)$ $\quad \theta^4 - 10\theta^2 + 1 = 0$

$[K : \mathbb{Q}] = 4$

Дов-ня: $\alpha \in K \setminus \mathbb{Q}$
Припустимо $\mathbb{Q}(\alpha) \neq K$, нехай $\beta \in K \setminus \mathbb{Q}(\alpha)$
Достатньо показати, що існує первісний елемент для $\mathbb{Q}(\alpha, \beta)$. Застосовуючи цей крок щонайбільше $[K:\mathbb{Q}]$ разів ми покажемо існування θ для K.

$\mathbb{Q}(\alpha, \beta)$ $f, g \in \mathbb{Q}[x]$ мінімальні многочлени α, β відп.

$\alpha = \alpha_1, \ldots, \alpha_m \in \mathbb{C}$ всі корені f

$\alpha_i \neq \alpha_j$ коли $i \neq j$

Лема: незвідний многочлен не має кратних коренів.

$\text{н.с.д.}(\underset{\text{незвідний}}{f(x)}, f'(x)) = 1$

$\exists\ p(x), q(x)$ т. щ.

$p(x) f(x) + q(x) f'(x) = 1$ (*)

Якщо α кратний корінь f, то $f(\alpha) = f'(\alpha) = 0$ – суперечить (*).

$\beta = \beta_1, \ldots, \beta_k \in \mathbb{C}$ всі корені g $\beta_i \neq \beta_j$ коли $i \neq j$

Розглянемо елемент $\gamma = \alpha + \lambda\beta$, $\lambda \in \mathbb{Q}$.
За яких умов $\beta \in \mathbb{Q}(\gamma)$? Якщо це так, то $\alpha = \gamma - \lambda\beta$ також належить $\mathbb{Q}(\gamma)$ і тому $\mathbb{Q}(\gamma) = \mathbb{Q}(\alpha, \beta)$.

$f(\gamma - \lambda x) =: h(x) \in \mathbb{Q}(\gamma)[x]$
$h(\beta) = 0$

$u(x) := \text{н.с.д.}(g(x), h(x))$ в $\mathbb{Q}(\gamma)[x]$

$$\begin{array}{l} \text{Або} \\ \text{або} \end{array} \left[\begin{array}{l} u(x) = x - \beta \ (\Rightarrow \beta \in \mathbb{Q}(\gamma)) \\ \deg(u) \geq 2 \end{array}\right.$$

Якщо $\deg(u) \geq 2$ тоді u має ще один корінь $\beta' \neq \beta$.

Оскільки $u(x) \mid g(x)$ і g не має кратних коренів, то u також не має кратних коренів.

$\beta' = \beta_i$ для деякого $i > 1$

$$0 = h(\beta') = f(\gamma - \lambda\beta')$$

$\Rightarrow$ $\alpha' := \gamma - \lambda\beta'$ є коренем f

$\alpha' = \alpha_j$ для деякого $j > 1$

Підставимо $\gamma = \alpha + \lambda\beta$ в рівність $\alpha' = \gamma - \lambda\beta'$:

$$\alpha' = \alpha + \lambda\beta - \lambda\beta' \Rightarrow \lambda = \frac{\alpha' - \alpha}{\beta - \beta'}.$$

Тобто випадок $\deg(u) > 2$ можливий для скінченної кількості значень $\lambda = \frac{\alpha_j - \alpha}{\beta - \beta_i}$.

Для будь-якого іншого λ маємо $\beta \in \mathbb{Q}(\gamma)$. Це доводить що $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\gamma)$ для деякого $\gamma = \alpha + \lambda\beta$. $\boxtimes$

<u>Наслідок 2</u> Кількість проміжних полів

$$K \supset F \supset \mathbb{Q}$$

є скінченною.

<u>Дов-ня</u> Будемо користуватися мультиплікативністю степеня розширення:

$$L / K / k \Rightarrow [L:k] = [L:K] \cdot [K:k]$$

(вправа)

Виберемо деякий первісний ел-т

$K = \mathbb{Q}(\theta)$ $\quad f \in \mathbb{Q}[x]$ $\quad f(\theta) = 0$

мінімальний многочлен для θ

Нехай $g \in F[x]$ мінімальний для θ:

$g(\theta) = 0$

Тоді $f(x) = g(x) h(x)$ для деякого $h \in F[x]$

Нехай $F' := \mathbb{Q}(\text{коеф-ти } g(x)) \subseteq F$.

Тоді $g(x)$ є також мінімальним многочленом для θ в $F'[x]$

$K = \mathbb{Q}(\theta) = F'(\theta) = F(\theta)$

$[K : F'] = \deg(g) = [K : F]$ $\quad$ тому що $g(x)$ є мінімальним як над F так і над F'

З іншого боку $F' \subset F \subset K \Rightarrow$

$[K : F'] = [K : F] \cdot [F : F']$

$\Rightarrow [F : F'] = 1 \Rightarrow F' = F$

Тобто довільно вибране проміжне поле F виявилося породженим коефіцієнтами деякого многочлена $g(x)$ який ділить $f(x)$ в $\mathbb{C}[x]$. Таких дільників g скінченна кількість.

$\boxtimes$

$K / \mathbb{Q}$ числове поле степеня n

$\alpha \in K \rightsquigarrow L_\alpha : K \to K$ $\quad \mathbb{Q}$-лінійний оператор

$\beta \mapsto \alpha\beta$

$f_\alpha(x) := \det(x \cdot Id - L_\alpha)$ характеристичний $\in \mathbb{Q}[x]$

$Tr(\alpha) := Tr(L_\alpha) \in \mathbb{Q}$ $\quad$ слід

$N(\alpha) := \det(L_\alpha) \in \mathbb{Q}$ $\quad$ норма

$$K = \mathbb{Q}(\theta) \cong \mathbb{Q}[x]/\langle f \rangle$$

$f(\theta) = 0$ $\quad f \in \mathbb{Q}[x]$ мінімальний

$\theta = \theta_1, \theta_2, \dots, \theta_n$ корені f (нагадаймо: всі різні)

$$S := \{\sigma_1, \dots, \sigma_n\}$$

$$\sigma_i : K \hookrightarrow \mathbb{C} \qquad \text{вкладення в } \mathbb{C}$$
$$\theta \longrightarrow \theta_i$$

<u>Тв-ння 3</u> $\quad f_\alpha(x) = \prod_{\sigma \in S} (x - \sigma(\alpha))$

$$\mathrm{Tr}(\alpha) = \sum_{\sigma \in S} \sigma(\alpha)$$

$$N(\alpha) = \prod_{\sigma \in S} \sigma(\alpha)$$

(вправа)

<u>Озн-ня</u> Нехай $\alpha_1, \dots, \alpha_n$ деякий базис $K/\mathbb{Q}$ (як векторного пр-ру).

$d(\alpha_1, \dots, \alpha_n) := \det(\sigma_i(\alpha_j))^2$ дискримінант цього базиса

<u>Тв-ння 4</u> (i) $d(\alpha_1, \dots, \alpha_n) \in \mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$

(ii) $\mathbb{Q}$-білінійна форма

$$K \times K \longrightarrow \mathbb{Q}$$
$$\alpha \times \beta \longmapsto \mathrm{Tr}(\alpha\beta)$$

є невиродженою.

<u>Дов-ння</u> (i) При заміні базиса $\det(\sigma_i(\alpha_j))$ помножиться на визначник оборотної матриці з елементами в $\mathbb{Q}$:

$$\alpha_j' = \sum_k \alpha_k T_{kj} \qquad T_{kj} \in \mathbb{Q}$$
$$\det(T_{kj}) \in \mathbb{Q}^\times$$

$$\sigma_i(\alpha_j') = \sum_k \sigma_i(\alpha_k)\, T_{kj}$$

$$\det(\sigma_i(\alpha_j')) = \det(\sigma_i(\alpha_k)) \det(T_{kj})$$

Тому достатньо перевірити (i') у деякому одному базисі, нп.

$1, \theta, \dots, \theta^{n-1}$

$$\det\begin{pmatrix} 1 & \sigma_1(\theta) & \dots & \sigma_1(\theta)^{n-1} \\ 1 & \sigma_2(\theta) & \dots & \sigma_2(\theta)^{n-1} \\ & & \dots & \end{pmatrix} = \det\begin{pmatrix} 1 & \theta_1 & \dots & \theta_1^{n-1} \\ 1 & \theta_2 & \dots & \theta_2^{n-1} \\ & & \dots & \end{pmatrix} = \prod_{1\le i<j\le n}(\theta_j - \theta_i)$$

визначник Вандермонда

$$d(1, \theta, \dots, \theta^{n-1}) = \prod_{1\le i<j\le n}(\theta_j - \theta_i)^2$$

це дискримінант мінімального многочлена $f(x) \in \mathbb{Q}[x]$

Дискримінант є однорідним многочленом степеня $2(n-1)$ з коефф. в $\mathbb{Z}$ від коефіцієнтів $f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n$

і не дорівнює 0 тттк f не має кратних коренів.

(ii) вправа

⊠

$\mathcal{O}_K = K \cap \overline{\mathbb{Z}}$ кільце цілих елементів

<u>Тв-ня 5</u> $\alpha \in \mathcal{O}_K^\times \iff \alpha \in \mathcal{O}_K, \ N(\alpha) = \pm 1$

<u>Дов-ня</u> $(\Rightarrow)$ $\alpha \cdot \beta = 1 \Rightarrow N(\alpha) N(\beta) = N(1) = 1$

$N(\mathcal{O}_K) \subseteq \mathbb{Z}$ (вправа) $\Rightarrow N(\alpha) = \pm 1$

$(\Leftarrow)$ $1 = \pm N(\alpha) \underset{\text{Тв-ня 3}}{=} \pm \prod_{\sigma \in S} \sigma(\alpha)$

$\boxtimes$

<u>Теорема 6</u> Кожен скінченно-породжений $\mathcal{O}_K$ - підмодуль в K

$$\left(M = \sum_{i=1}^{m} \mathcal{O}_K \beta_i \subset K \right)$$

є вільним $\mathbb{Z}$ - модулем рангу $n = [K : \mathbb{Q}]$.
Тобто існують $\alpha_1, \ldots, \alpha_n \in M$ лінійно-незалежні над $\mathbb{Q}$ такі що

$$M = \sum_{i=1}^{n} \mathbb{Z} \alpha_i .$$

[Не будемо доводити: див. книгу J. Neukirch Algebraic number theory про це та все, що буде далі.]

Застосуємо до ідеалів кільця цілих

$\mathfrak{a} \subset \mathcal{O}_K$ ідеал є $\mathcal{O}_K$ - модулем

$$\Rightarrow \mathfrak{a} = \sum_{i=1}^{n} \mathbb{Z} \alpha_i . \qquad (***)$$

<u>Оз-ня</u> $d(\mathfrak{a}) := d(\alpha_1, \ldots, \alpha_n)$ дискримінант ідеала $\mathfrak{a}$

не залежить від вибору базису $\alpha_1, \ldots, \alpha_n$ в $(***)$

$d(\mathcal{O}_K)$ наз-ся дискримінантом поля K $=: d_K$

Вправа: доведіть, що $d_K \neq 0$.

Доведіть порівняння Стікельбергера для дискримінанта числового поля (Stickelberger's discriminant relation)

$$d_K \equiv 0,\ 1 \mod 4.$$

<u>Тв-ня 7</u> $d(\mathfrak{a}) = \#(\mathcal{O}_K/\mathfrak{a})^2 \cdot d_K$

(кількість ел-тів$)^2$

(Вправа*)

Ідея: $\lambda : K \longrightarrow V \cong \mathbb{R}^n \subset \mathbb{C}^n$

$$\alpha \longmapsto (\sigma_1(\alpha), \dots, \sigma_n(\alpha))$$

$\lambda(K) \subset \mathbb{C}^n$
вкладається у $\mathbb{R}$-підпростір розмірності n нерухомих точок інволюції $i : \mathbb{C}^n \to \mathbb{C}^n$

означеної так:

нехай $\sigma(K)$ <u>дійсне</u> вкладення якщо $\sigma(K) \subset \mathbb{R}$

Маємо $\sigma_1, \dots, \sigma_r$ дійсні

$\sigma_{r+1}, \overline{\sigma_{r+1}}, \dots, \sigma_{r+s}, \overline{\sigma_{r+s}}$ спряжені пари уявних вкладень: $\theta_{r+i}, \overline{\theta_{i+i}}$

r або s можуть $= 0$

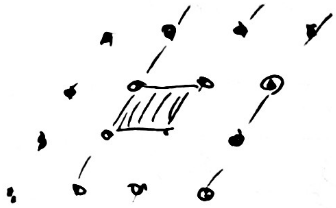
$r + 2s = n$

$$i(v_1, \dots, v_r, u_{r+1}, w_{r+1}, u_{r+2}, w_{r+2}, \dots)$$
$$= (\overline{v_1}, \dots, \overline{v_r}, \overline{w_{r+1}}, \overline{u_{r+1}}, \overline{w_{r+2}}, \overline{u_{r+2}}, \dots)$$

$\lambda(\mathfrak{a})$ = решітка в $\mathbb{R}$-просторі $V \cong \mathbb{R}^n$ породжена $\lambda(\alpha_1), \dots, \lambda(\alpha_n)$

$$0 \neq d(\alpha) = \det(\lambda(\alpha_1), \dots, \lambda(\alpha_n))^2$$
$$= \mathrm{vol}(\lambda(\alpha_1), \dots, \lambda(\alpha_n))^2$$

так званий ко-об'єм решітки
= об'єм її фундаментальної комірки



Решітка максимальної розмірності: ко-об'єм $\neq 0$

<u>Теорема Діріхле про одиниці</u>

Розглянемо відображення логарифма

$$\mathrm{Log} : K^* = K \setminus \{0\} \longrightarrow \mathbb{R}^{r+s}$$
$$\alpha \longmapsto (\log|\sigma_1(\alpha)|, \dots, \log|\sigma_r(\alpha)|,$$
$$2 \cdot \log|\sigma_{r+1}(\alpha)|, \dots, 2 \cdot \log|\sigma_{r+s}(\alpha)|).$$

Образ групи одиниць кільця
$$\mathrm{Log}(\mathcal{O}_K^\times) \subset \mathbb{R}^{r+s}$$
є решіткою максимальної розмірності у підпросторі
$$W = \{(w_1, \dots, w_{r+s}) \in \mathbb{R}^{r+s} : w_1 + \dots + w_{r+s} = 0\} \cong \mathbb{R}^{r+s-1}.$$

Зауваження: $\mathrm{Log}(\mathcal{O}_K^\times) \subset W$ бо

$$1 = |N(\alpha)| = |\sigma_1(\alpha)| \cdot \ldots \cdot |\sigma_r(\alpha)| \cdot |\sigma_{r+1}(\alpha)|^2 \cdot \ldots \cdot |\sigma_{r+s}(\alpha)|^2$$

застосовуємо $\log$:

$$0 = \log|\sigma_1(\alpha)| + \ldots + 2 \cdot \log|\sigma_{r+1}(\alpha)| + \ldots$$

<u>Озн-ня</u> Ко-об'єм решітки $\mathrm{Log}(\mathcal{O}_K^\times)$ у просторі $W \cong \mathbb{R}^{r+s-1}$ називається регулятором поля K, $R_K \in \mathbb{R}^*$.

Факторизація ідеалів

$\mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$ не є ООФ, нп.

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$$

Едуард Куммер 1810-1893 :
вкласти $\mathcal{O}_K$ у більшу множину "ідеальних чисел" де
$3 = \mathfrak{p}_1 \cdot \mathfrak{p}_2$ $7 = \mathfrak{p}_3 \cdot \mathfrak{p}_4$ $1+2\sqrt{-5} = \mathfrak{p}_1 \mathfrak{p}_3$ $1-2\sqrt{-5} = \mathfrak{p}_2 \mathfrak{p}_4$

"ідеальні числа" $\rightsquigarrow$ ідеали кільця $\mathcal{O}_K$
Річард Дедекінд 1831-1916

$\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}_K$ ідеали

$$\mathfrak{a} + \mathfrak{b} = \{ \alpha + \beta : \alpha \in \mathfrak{a}, \beta \in \mathfrak{b} \}$$

$$\mathfrak{a}\mathfrak{b} = \{ \sum_{i=1}^{m} \alpha_i \beta_i : \overset{m \geq 1}{\alpha_i \in \mathfrak{a}}, \beta_i \in \mathfrak{b} \}$$

$\{$ ідеали $\mathcal{O}_K \}$ це кільце

~~[illegible] $\mathcal{O}_K$ простий якщо з $\mathfrak{a} \mid \mathfrak{b}\mathfrak{c}$ випливає $\mathfrak{a} \mid \mathfrak{b}$ або $\mathfrak{a} \mid \mathfrak{c}$~~

<u>Озн-ня</u> Ідеал $I \subsetneq R$ ← комутативне кільце називається простим якщо з $a, b \in R$, $a \cdot b \in I$ випливає $a \in I$ або $b \in I$.

<u>Теорема</u> Кожен ідеал $\mathfrak{a} \subsetneq \mathcal{O}_K$, $\mathfrak{a} \neq (0)$ допускає однозначну факторизацію у добуток простих ідеалів

$$\mathfrak{a} = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$$

(з точністю до порядку множників)

Група класів ідеалів

відношення еквівалентності

$\mathfrak{a} \sim \mathfrak{b}$ — ідеали в $\mathcal{O}_K$

якщо існують $\alpha, \beta \in \mathcal{O}_K$ т. щ.

$$\langle \alpha \rangle \mathfrak{a} = \langle \beta \rangle \mathfrak{b}$$

$$Cl_K := \{\text{ненульові ідеали в } \mathcal{O}_K\} / \sim$$

є групою (твердження!)

яка наз-ся групою класів ідеалів.

Теорема $\# Cl_K < \infty$.

$h_K := \# Cl_K$ число класів

Теорема $h_K = 1 \iff \mathcal{O}_K$ є ОГІ

$\iff \mathcal{O}_K$ є ООФ

Головна теорема алгебраїчної (?) теорії чисел

$$\zeta_K(s) := \sum_{\mathfrak{a} \subseteq \mathcal{O}_K} \frac{1}{\#(\mathcal{O}_K/\mathfrak{a})^s}$$ дзета функція Дедекінда

$$\lim_{s \to 1} (s-1) \zeta_K(s) = \frac{2^r (2\pi)^s h_K R_K}{\sqrt{|d_K|} \cdot w_K}$$

де $w_K = \# \{ \alpha \in K : \exists m \geq 1 ; \text{ т. щ. } \alpha^m = 1 \}$
кількість коренів з одиниці в K

r, s = кількість дійсних / пар уявних вкладень

d_K = дискримінант, R_K = регулятор поля K

h = число класів