21/02/2023

34. Цілі елементи та розклад на множники у квадратичних полях

$m \in \mathbb{Z}$ $m \neq 0, 1$ вільне від квадратів

$K = \mathbb{Q}(\sqrt{m})$ квадратичне поле

$K = \{ a + b\sqrt{m} : a, b \in \mathbb{Q} \}$

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

Питання: коли $\xi = a + b\sqrt{m}$ є цілим?

<u>Озн-ня</u> $\overline{\xi} = a - b\sqrt{m}$ спряжений ел-т

$$N(\xi) = \xi \cdot \overline{\xi} = (a + b\sqrt{m})(a - b\sqrt{m}) = a^2 - mb^2$$

норма

$$Tr(\xi) = \xi + \overline{\xi} = 2a \quad \text{слід}$$

$$(x - \xi)(x - \overline{\xi}) = x^2 - Tr(\xi)x + N(\xi)$$

$\boxed{b = 0}$ мінімальний многочлен $\xi = a$ це $x - a$, тому $a \in \overline{\mathbb{Z}}$ тттк $a \in \mathbb{Z}$

$\boxed{b \neq 0}$ мінімальний мн-н ξ це $x^2 - Tr(\xi)x + N(\xi)$ ← незвідний бо не має коренів у $\mathbb{Q}$

тому

$$\xi \in \overline{\mathbb{Z}} \iff Tr(\xi), N(\xi) \in \mathbb{Z}$$

<u>Тв-ня 1</u> Якщо $m = 4n+2, 4n+3$ то

$$\mathcal{O}_K = \{ a + b\sqrt{m} : a, b \in \mathbb{Z} \}.$$

Якщо $m = 4n+1$ то

$$\mathcal{O}_K = \left\{ \frac{a + b\sqrt{m}}{2} : \begin{matrix} a, b \in \mathbb{Z} \\ 2 \mid (a-b) \end{matrix} \right\} = \left\{ c + d\,\frac{1+\sqrt{m}}{2} : c, d \in \mathbb{Z} \right\}.$$

Дов-ня: вправа.

Питання: описати одиниці кільця O_K $O_K^\times$ - ?
прості елементи в O_K - ?
чи є O_K областю головних ідеалів?
чи є факторизація однозначною?

Тв-ня 2 (i) $\xi \in O_K^\times$ тттк $N(\xi) = 1$

(ii) Якщо $\xi \in O_K$ ~~відповідно~~
~~має~~ $N(\xi) = \pm p$ для деякого простого числа $p \in \mathbb{N}$
тоді ξ є незвідним елементом.

Лема 3 $N: K \to \mathbb{Q}$ є мультиплікативною, тобто $N(\xi_1 \cdot \xi_2) = N(\xi_1) \cdot N(\xi_2)$.

Дов-ня: грубою силою / brute force

$$\xi_i = a_i + b_i \sqrt{m}$$
$$\xi_1 \xi_2 = (a_1 a_2 + m b_1 b_2) + (a_1 b_2 + a_2 b_1)\sqrt{m}$$
$$N(\xi_1 \xi_2) = (a_1 a_2 + m b_1 b_2)^2 - (a_1 b_2 + a_2 b_1)^2 m$$
$$= (a_1^2 - m b_1^2)(a_2^2 - m b_2^2)$$

Ось дещо розумніший підхід:
$\mathbb{Q}(\sqrt{m})$ це векторний простір розмірності 2 над $\mathbb{Q}$
виберемо базис, н.п. $\{1, \sqrt{m}\}$
і для кожного $\xi = a + b\sqrt{m}$ розглянемо лінійний оператор "множення на ξ"

$$L_\xi : \mathbb{Q}(\sqrt{m}) \to \mathbb{Q}(\sqrt{m})$$
$$\alpha \longmapsto \xi \cdot \alpha$$

У базисі $\{1, \sqrt{m}\}$

$$L_\xi(1) = a + b\sqrt{m}$$
$$L_\xi(\sqrt{m}) = (a + b\sqrt{m})\sqrt{m} = mb + a\sqrt{m} \qquad L_\xi = \begin{pmatrix} a & mb \\ b & a \end{pmatrix}$$

$$\mathrm{Tr}(L_\xi) = 2a = \mathrm{Tr}(\xi)$$
$$\det(L_\xi) = a^2 - mb^2 = N(\xi)$$

$$L_{\xi_1} \cdot L_{\xi_2} = L_{\xi_1 \xi_2} \Rightarrow N(\xi_1) N(\xi_2) = N(\xi_1 \xi_2) \quad \boxtimes$$

Дов-ня Тв-ня 2 $\quad N(O_K) \subseteq \mathbb{Z}$

(i) $\Rightarrow$ Нехай $\xi \in O_K^\times \iff \xi, \frac{1}{\xi} \in O_K$

$$N(\xi)\, N\left(\frac{1}{\xi}\right) = N(1) = 1$$

$$\Rightarrow N(\xi) \in \mathbb{Z}^\times = \{1, -1\}$$

$\Leftarrow$ Нехай $N(\xi) = \pm 1$. Тоді

$$\frac{1}{\xi} = \frac{\bar{\xi}}{\xi \cdot \bar{\xi}} = \pm \bar{\xi} \in O_K.$$

(ii) Нехай $\xi \in O_K$ є звідним, тобто $\xi = \xi_1 \cdot \xi_2$ для деяких $\xi_1, \xi_2 \notin O_K^\times$.
Тоді $N(\xi) = N(\xi_1)\, N(\xi_2)$ і жодне з чисел $N(\xi_i)$ не дорівнює ± 1 в силу (i).
Тобто $N(\xi) \in \mathbb{Z}$ є складеним числом. $\boxtimes$

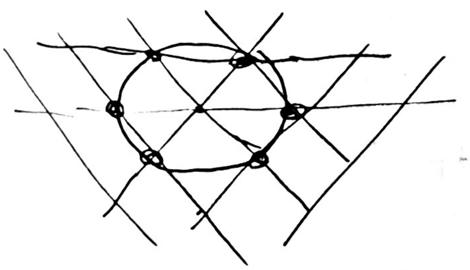
Тв-ня 3 $\quad m < 0$ вільне від квадратів
$K = \mathbb{Q}(\sqrt{m})$

Якщо $m \neq -1, -3$ то $O_K^\times = \{1, -1\}$.

$$O^\times_{\mathbb{Q}(\sqrt{-1})} = \{1, -1, \sqrt{-1}, -\sqrt{-1}\}$$

$\mathbb{Z} + \mathbb{Z}\sqrt{-1}$

$$O^\times_{\mathbb{Q}(\sqrt{-3})} = \left\{1, -1, \frac{1+\sqrt{-3}}{2}, \frac{1-\sqrt{-3}}{2}, -\frac{1+\sqrt{-3}}{2}, -\frac{1-\sqrt{-3}}{2}\right\}$$



$$\mathbb{Z} + \mathbb{Z}\,\frac{1+\sqrt{-3}}{2}$$

Дов-ня: вправа.

$m < 0 \quad \mathbb{Q}(\sqrt{m})$ уявне квадратичне поле
щільне в $\mathbb{C}$

$m > 1 \quad \mathbb{Q}(\sqrt{m})$ дійсне квадратичне поле
щільне в $\mathbb{R}$

Діофантове рівняння

$$a^2 - m b^2 = \pm 1 \qquad (m > 1)$$

називається рівнянням Пелля.
Виявляється що воно має нетривіальні розв'язки для кожного вільного від квадратів $m > 1$.

Приклад: $K = \mathbb{Q}(\sqrt{2})$

$$\mathcal{O}_K = \{ a + b\sqrt{2} \ : \ a, b \in \mathbb{Z} \}$$

$1 + \sqrt{2} \in \mathcal{O}_K^\times$ оскільки $(1+\sqrt{2})(1-\sqrt{2}) = 1 - 2 = -1$

$$\frac{1}{1+\sqrt{2}} = \sqrt{2} - 1 \in \mathcal{O}_K$$

<u>Теорема 4</u> $m > 1$ вільне від кв-ів
$K = \mathbb{Q}(\sqrt{m})$

Існує єдина одиниця кільця $\varepsilon \in \mathcal{O}_K^\times$ така що $\bar{\varepsilon} < 1 < \varepsilon$

і

$$\mathcal{O}_K^\times = \{ \pm \varepsilon^n \ : \ n \in \mathbb{Z} \}.$$

(Без дов-ня, див. теорію рів-ня Пелля.)
[NMZ] Розділ 7

Ця одиниця ε наз-ся фундаментальною одиницею ~~кільця~~ поля $\mathbb{Q}(\sqrt{m})$.
Нп. $\varepsilon = 1 + \sqrt{2}$ є фундаментальною одиницею $\mathbb{Q}(\sqrt{2})$.

$m \in \mathbb{Z}$, $m \neq 0, 1$ вільне від кв-ів

Коли факторизація в $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ є однозначною?

Пригадаймо:

евклідові області $\subset$ ОГІ $\subset$ ООФ

<u>Теорема 5</u> $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ є ООФ ТТТК коли це кільце є ОГІ

(Без доведення. Це випливає з теорії так званих кілець Дедекінда. Твердження є вірним для кілець цілих у числових полях, про які ми поговоримо у наступному §.)

Приклад: $O_{\mathbb{Q}(\sqrt{-6})}$ не є ООФ

$$10 = 2\cdot 5 = (2+\sqrt{-6})(2-\sqrt{-6}) \qquad (*)$$

Покажемо, що $2, 5$ та $2 \pm \sqrt{-6}$ є незвідними елементами.

$$N(a+b\sqrt{6}) = a^2 + 6b^2$$

$\Rightarrow$ в O_K немає елементів ξ з $N(\xi) = 2$ або $N(\xi) = 5$.

$N(2) = 2^2$ $\qquad$ $2 = \xi_1 \cdot \xi_2$ звідний якщо $N(\xi_1) = N(\xi_2) = 2$ $\times$

$N(5) = 5^2$ $\qquad$ $5 = \xi_1 \cdot \xi_2$ звідний якщо $N(\xi_1) = N(\xi_2) = 5$ $\times$

$N(2 \pm \sqrt{-6}) = 10$ $\qquad$ $N(\xi_1) = 2,\ N(\xi_2) = 5$ $\times$

Якщо $O_{\mathbb{Q}(\sqrt{-6})}$ це ООФ, тоді це ОГІ за Теоремою 5 і незвідні елементи є простими. З іншого боку, жодне з $2 \pm \sqrt{-6}$ не є асоційованим з 2 або 5, тобто розклад $(*)$ не є однозначним.

<u>Теорема 6</u> Для $m = -11, -7, -3, -2, -1, 2, 3, 5, 13$

кільце цілих O_K в $K = \mathbb{Q}(\sqrt{m})$ є евклідовою областю з евклідовою нормою $\lambda(\xi) = |N(\xi)|$.

Доведення: вправа.

Теорема Heilbronn – Linfoot 1934
Heegner 1952
Baker, Stark 1966-67

Єдиними квадратичними полями $K = \mathbb{Q}(\sqrt{-m})$, $m<0$ вільне від квадратів для яких кільце цілих O_K є ООФ є випадки

$$m = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

Про дійсні квадратичні поля $(m>1)$ ми знаємо набагато менше. Існує гіпотеза, що нескінченно багато з них мають властивість однозначної факторизації в O_K. Експерименти показують, що приблизно 75% з них є ООФ.

m:	2	3	5	6	7	10	11	13	14	15
ООФ	+	+	+	+	+	−	+	+	+	−

Нехай вільне від кв-ів $m \in \mathbb{Z}$, $m \neq 0,1$ є таким, що O_K в $K = \mathbb{Q}(\sqrt{m})$ є ООФ.
Чи можемо ми описати прості елементи в O_K (з точністю до асоційованих)?

Нагадаємо: Тв-ня 2 $\Rightarrow$

якщо $\xi \in O_K$ ~~простий~~ має $\overbrace{\xi \cdot \bar{\xi}}^{N(\xi)} = \pm p$ для деякого простого $p \in \mathbb{N}$, то ξ є простим. Виявляється, що всі прості елементи повстають як дільники деякого простого $p \in \mathbb{N}$.

Твердження 7 Нехай $m \in \mathbb{Z}$ $m \neq 0,1$ вільне від кв-в є таким що кільце цілих O_K в $K = \mathbb{Q}(\sqrt{m})$ є ООФ. Тоді:

(i) кожне просте число $p \in \mathbb{N}$ є або простим в O_K або добутком $p = \pi_1 \cdot \pi_2$ двох простих елементів, не обов'язково різних;

(ii) кожен простий елемент $\pi \in O_K$ є дільником єдиного простого $p \in \mathbb{N}$.

Дов-ня (ii) Нехай

$$n = \min \{ k \in \mathbb{Z}_{>1} : \pi \mid k \}.$$

Ця множина не пуста бо $\pi \mid N(\pi) \in \mathbb{Z}$.

Припустимо що n є складеним: $n = n_1 \cdot n_2$. Оскільки π є простим елементом, то $\pi \mid n_1$ або $\pi \mid n_2$ (з означення простоти). Оскільки $1 < n_i < n$, це суперечить означенню числа n. З цього випливає, що n є простим числом, $n =: p$.

Єдиність: $\pi \mid p \Rightarrow N(\pi) \mid N(p) = p^2$, тобто p однозначно визначене самим π.

(i) Якщо просте $p \in \mathbb{N}$ не є простим в O_K, то $p = \pi \cdot \alpha$ для деякого простого $\pi \in O_K$ та деякого $\alpha \in O_K \setminus O_K^\times$.

$p^2 = N(p) = N(\pi) \cdot N(\alpha)$ і $N(\pi), N(\alpha) \neq \pm 1$

$\Rightarrow N(\pi) = N(\alpha) = \pm p \Rightarrow \alpha$ простий за Тв-ням 2. $\boxtimes$

Для простого $p \in \mathbb{N}$ є дві можливості:

<u>Озн-ня</u> $p = \pi_1 \cdot \pi_2$ "p розщеплюється в O_K"

або

p є простим в O_K "не розщеплюється"

Приклад:

p	розщеплення в $\mathbb{Q}(\sqrt{2})$
2	$2 = (\sqrt{2})^2$ $N(\sqrt{2}) = -2 \Rightarrow \sqrt{2}$ є простим
3	простий (бо немає елементів з нормою 3)
5	простий
7	$7 = (3-\sqrt{2})(3+\sqrt{2})$ не асоційовані
11	простий
13	простий
17	$17 = (5-2\sqrt{2})(5+2\sqrt{2})$
19	простий
23	$23 = (5-\sqrt{2})(5+\sqrt{2})$
...	

p розщеплюється $\Longleftrightarrow$ існують елементи O_K з нормою $\pm p$

$a^2 - m b^2 = \pm p$

Питання: описати, ~~закон розщеп~~ які прості p розщеплюються в $\mathbb{Q}(\sqrt{2})$. та $\mathbb{Q}(\sqrt{3})$.