

W3D2

04/06/2012

1277

$$K = \mathbb{Q}[\sqrt[4]{7}, i] \supset \mathbb{Q}$$

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt[4]{7}] \subset \mathbb{Q}[\sqrt[4]{7}, i] = K$$

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt[4]{7}] \subset \mathbb{Q}[\sqrt[4]{7}, i] = K$$

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt[4]{7}] \subset \mathbb{Q}[\sqrt[4]{7}, i] = K$$

$$|G_{K/\mathbb{Q}}| = 8$$

$$\sigma(\sqrt[4]{7}) = ?$$

$$\sigma(i) = ?$$

$$\sigma(\sqrt[4]{7}) = \zeta \sqrt[4]{7}$$

$$\sigma(i) = \pm i$$

$$\zeta^4 = 1$$

$$\zeta^2 = -1$$

$$\zeta \in \{ \pm 1, \pm i \}$$

$$\sigma \in \{ \pm 1 \}$$

$$G = G_{K/\mathbb{Q}}$$

$$G_{K/\mathbb{Q}} = \{ \sigma_{\zeta, \epsilon} \mid \zeta^4 = 1, \epsilon^2 = 1 \}$$

$$4 \text{ roots } a$$

$$2 \text{ roots } b$$

$$a = \zeta, 1$$

$$b = \zeta, -1$$

$$H = \langle a \rangle = \{ id_K, a, a^2, a^3 \}$$

$$G = \langle b \rangle = \{ id_K, b \}$$

$$(b^{-1} = b)$$

$$bab^{-1} = a^{-1}$$

$$bab^{-1}(\sqrt[4]{7}) = ba(\sqrt[4]{7}) = b(i\sqrt[4]{7}) = -i\sqrt[4]{7}$$

$$= a^3(\sqrt[4]{7}) = a^{-1}(\sqrt[4]{7})$$

$$bab^{-1}(i) = ba(-i) = b(i) = i = a^{-1}(i)$$

$$bab^{-1} = a^{-1}$$

$$G_{K/\mathbb{Q}} \cong D_8$$

$$= \text{Dihedral group of order 8}$$

$$= \text{Dihedral group of order 8}$$

הוכחה:

אם B חסרה חלקי מילה כך סיבוכים -

3" $B \subset H$, $|B| = 1, 2, 4$ חסר

$B = \{id, a^2\}$, $H = \{id, a, a^2, a^3\}$

אם B מילה כך סקופ

3" B חסר 2, $\{a^2, id, ab, ba\}$, $\{id, b\}$

אם B מילה סקופ וזו סיבוכ

3" B מילה חסר סקופ (מילה - סקופ וסיבוכ הקיבוצ)

4" סיבוכ ההכרה כיוון $|B| \mid 8$, $|B| = 4$

3" $|B| = 4$

$B = \{id, a^k, a^l b, a^{k+l} b\}$

מכאן $a^k \cdot a^{k+l} \cdot b = a^l \cdot b$

$$\Rightarrow a^{2k} = 1$$

אם $H = \langle a \rangle \leq \langle a, b \rangle \leq 4/2k$ (כ"א)

אם

אם $B = \{id, a^2, a^l b, a^{2+l} b\}$

$B = \{id, a^2, b, a^2 b\}$

$B = \{id, a^2, ab, a^2 b\}$

בסיס מוצאן 10 מילה (כולל D_8)

המשפט הראשון

$$B = \{id, a^2\}$$

①

$$a^2(\sqrt{7}) = -\sqrt{7}$$

$$a^2(i) = i$$

המשפט השני

$$\sqrt{7}^2 = 7$$

כן

כן

$$K^B \supset \mathbb{Q}[\sqrt{7}, i]$$

$$[K:K^B] = |B| = 2$$

כן

$$[K^B:\mathbb{Q}] = 4 = [\mathbb{Q}[\sqrt{7}, i]:\mathbb{Q}]$$

כן

כן

$$K^B = \mathbb{Q}[\sqrt{7}, i]$$

כן

$$a(i) = i$$

$$B = \langle a \rangle = \{id, a, a^2, a^3\}$$

②

$$K^B \supset \mathbb{Q}[i]$$

$$[K:K^B] = |B| = 4$$

$$\Rightarrow [K^B:\mathbb{Q}] = \frac{[K:\mathbb{Q}]}{[K:K^B]} = \frac{8}{4} = 2 = [\mathbb{Q}[i]:\mathbb{Q}]$$

$$\Rightarrow K^B = \mathbb{Q}[i]$$

$$B = \{id, a^2, a^4, a^6\}$$

③

$$a^4 b(\sqrt{7}) = i^4 \sqrt{7}$$

$$a^4 b(i) = -i$$

$$\mathbb{Q}[\sqrt{7}] \subset K^B$$

$$: K=0$$

$$[K:K^B] = |B| = 2$$

המשפט הראשון

$$[K^B:\mathbb{Q}] = 4 = [\mathbb{Q}[\sqrt{7}]:\mathbb{Q}]$$

כן

$$K^B = \mathbb{Q}[\sqrt{7}] \Leftarrow$$

: $k=1$

$$: K^B \text{ is not a CN} \quad B = \{id, ab\}$$

$$ab(\sqrt[4]{7}) = i\sqrt[4]{7}$$

$$ab(i) = -i$$

$$z = x + yi \quad x, y \in \mathbb{Q}[\sqrt[4]{7}] \quad \text{is}$$

$$x = x_0 + x_1\sqrt[4]{7} + x_2\sqrt[4]{7}^2 + x_3\sqrt[4]{7}^3$$

$$x_0, \dots, x_3 \in \mathbb{Q}$$

$$y = y_0 + y_1\sqrt[4]{7} + y_2\sqrt[4]{7}^2 + y_3\sqrt[4]{7}^3$$

: CN

$$z = ab(z) = a(x) - a(y)i = (x_0 + y_1\sqrt[4]{7} - x_2\sqrt[4]{7}^2 + y_3\sqrt[4]{7}^3) + i(-y_0 + x_1\sqrt[4]{7} + y_2\sqrt[4]{7}^2 - x_3\sqrt[4]{7}^3)$$

$$x_1 = y_1$$

$$y_0 = -y_0$$

: EP

$$x_2 = -x_2$$

$$y_1 = x_1$$

$$y_3 = -x_3$$

$$x_3 = y_3$$

$$y_2 = y_2$$

$$y_0 = 0 \quad x_2 = 0$$

$$K^B = \mathbb{Q}[\sqrt[4]{7}(1+i)] \quad \text{EP}$$

$$: \{id, b\}$$

is not a CN

$$(a^k b) \cdot b \cdot (a^k b)^{-1} = \begin{cases} b & k=0 \\ a^2 b & k=1 \end{cases}$$

$$k=0$$

$$k=1$$

$$K^{\{id, a^2 b\}} = ab(K^{\{id, b\}}) = ab(\mathbb{Q}[\sqrt[4]{7}]) =$$

$$\mathbb{Q}[i\sqrt[4]{7}]$$

$$: \{id, ab\}$$

is not a CN

$$a^k \cdot ab \cdot a^{-k} = \begin{cases} ab & k=0 \\ a^3 b & k=1 \end{cases}$$

$$k=1$$

$$K^{\{id, a^2 b\}} = a(K^{\{id, ab\}}) = a\mathbb{Q}[\sqrt[4]{7}(1+i)] = \mathbb{Q}[\sqrt[4]{7}(1-i)]$$