問題6-1 K, L は $\mathbb{C}$ の部分体であるとし, L/K は有限次拡大であるとする.
このとき, L/K が Galois 拡大であることと次の条件 (4) が同値であることを示せ.

(4) 任意の $\alpha \in L$ について, α の K 上でのすべての共役元が L に含まれる.

解答例

1 (4) $\Rightarrow$ L/K は Galois 拡大を示そう.

(4) の条件における α として, $L = K(\theta)$ をみたす $\theta \in L$ をとると,
(4) より θ のすべての共役元は L に含まれる. これより, L/K は Galois 拡大である.

注 以下の条件は有限次拡大(標数0) L/K が Galois 拡大であることを特徴付ける互いに同値な条件になっている:

(1) L の K 上での任意の共役体は L に等しい.
(K 上での任意の体の同型 $\varphi : L \hookrightarrow \mathbb{C}$ について $\varphi(L) = L$.)

(2) θ の K 上での任意の共役元は L に含まれる. ← $L = K(\theta)$ と仮定している.
(θ の K 上での最小多項式のすべての根が L に含まれる.)

(3) ある $F(x) \in K[x]$ が存在して, L は $F(x)$ の K 上での最小分解体になる.
(L は K に $F(x)$ のすべての根を付け加えてできる体になる.)

$\boxed{2}$ L/K が Galois 拡大 $\Rightarrow$ (4) を示そう.

L/K は Galois 拡大であるとし, 任意に $\alpha \in L$ をとる.

$\beta \in \mathbb{C}$ は K 上での α の任意の共役元であるとする.

(4) を示すためには $\beta \in L$ を示せばよい.

$K(\alpha) \cong K[x]/(F_\alpha(x)) \cong K(\beta)$

($F_\alpha(x)$ は α の K 上での最小多項式)

(β は $F_\alpha(x)$ の根)

このとき, K 上の体同型 $\varphi : K(\alpha) \hookrightarrow \mathbb{C}$, $f(\alpha) \mapsto f(\beta)$ $(f(x) \in K[x])$ が存在する.

もしも $K(\alpha) = L$ ならば L/K が Galois 拡大であることより, $L = \varphi(L) = \varphi(K(\alpha)) = K(\beta) \ni \beta$.

$K(\alpha) \subsetneq L$ と仮定する. 単拡大定理より, $L = K(\alpha)(\theta)$, $\theta \in L$ と書ける.

θ の $K(\alpha)$ 上での最小多項式を $F(x) = \sum_i a_i x^i \in K(\alpha)[x]$, $a_i \in K(\alpha)$ と書く.

$G(x) = \sum_i \varphi(a_i) x^i \in \varphi(K[\alpha])[x] = K(\beta)[x]$ とおき, $G(x)$ の根 $\eta \in \mathbb{C}$ を任意にとる.

このとき, K 上の体の同型 $\tilde{\varphi} : L \hookrightarrow \mathbb{C}$ を $\tilde{\varphi}\left(\sum_i b_i \theta^i\right) = \sum_i \varphi(b_i)\eta^i$ $(b_i \in K(\alpha))$ と作れる:

$$L = K(\alpha)(\theta) \cong K(\alpha)[x]/(F(x)) \cong K(\beta)[x]/(G(x)) \cong K(\beta)(\eta) \subset \mathbb{C}$$
$$\sum a_i \theta^i \longleftrightarrow \overline{\sum a_i x^i} \longleftrightarrow \overline{\sum \varphi(a_i) x^i} \longleftrightarrow \sum \varphi(a_i)\eta^i.$$

L/K が Galois 拡大であることより, $L = \tilde{\varphi}(L) = K(\beta)(\eta) \ni \beta$.

これで (4) が示された. $\square$

問題6-2 M/K は体の拡大であるとし，L_1, L_2 はその中間体であるとする．

このとき，L_1/K，L_2/K が有限次拡大ならば $L_1 \cap L_2/K$ も L_1L_2/K も有限次拡大になり，

$$[L_1 \cap L_2 : K] \leqq \min\{[L_1 : K], [L_2 : K]\}, \quad [L_1L_2 : K] \leqq [L_1 : K][L_2 : K]$$

となることを示せ．

ここで L_1L_2 は L_1 と L_2 の両方を含む M の最小の部分体を表す． □

解答例 $[L_1 : K] = m < \infty$，$[L_2 : K] = n < \infty$ と仮定する．

$\boxed{1}$ $[L_1 \cap L_2 : K] \leqq \min\{m, n\}$ を示そう．

$L_1 \cap L_2 \subset L_1$ より，$[L_1 \cap L_2 : K] = \dim_K L_1 \cap L_2 \leqq \dim_K L_1 = m$.

$L_1 \cap L_2 \subset L_2$ より，$[L_1 \cap L_2 : K] = \dim_K L_1 \cap L_2 \leqq \dim_K L_2 = n$.

ゆえに，$[L_1 \cap L_2 : K] \leqq \min\{m, n\}$.

$\boxed{2}$ $[L_1L_2 : K] \leqq mn$ を示そう。

単拡大定理より、K上代数的なある $\theta \in L_1$ が存在して、$L_1 = K(\theta)$ となる。

L_1L_2 は L_2 と θ を含むので、$L_2(\theta)$ の最小性より $L_2(\theta) \subset L_1L_2$.

任意の $\beta \in L_1 = K(\theta)$ はある $f(x) \in K[x]$ によって $\beta = f(\theta)$ と表わされ、
$f(x) \in L_2[x]$ でもあるので $\beta = f(\theta) \in L_2(\theta)$ となり、$L_2(\theta)$ は L_1 と L_2 の両方を含む。
ゆえに、L_1L_2 の最小性より、$L_1L_2 \subset L_2(\theta)$.
これで、$L_1L_2 = L_2(\theta)$ となることが示された。

$F_\theta(x) \in K[x]$ を θ の K上での最小多項式とすると、$F_\theta(x) \in L_2[x]$ でかつ $F_\theta(\theta) = 0$ となるので、

$$[L_1L_2 : L_2] = [L_2(\theta) : L_2] = (\theta \text{ の } L_2 \text{上での最小多項式の次数})$$
$$\leqq \deg F_\theta(x) = [K(\theta) : K] = [L_1 : K].$$

ゆえに、

$$[L_1L_2 : K] = [L_1L_2 : L_2][L_2 : K] \leqq [L_1 : K][L_2 : K] = mn.$$

(注 $[L:K]$ は $[L/K]$ と書くこともある。) □

$\boxed{\text{問題 6-3}}$ K, L_1, L_2 は $\mathbb{C}$ の部分体であるとする。

L_1/K と L_2/K が有限次Galois拡大ならば，

$L_1 \cap L_2/K$ と L_1L_2/K も有限次Galois拡大になることを示せ。

ここで L_1L_2 は L_1 と L_2 の両方を含む $\mathbb{C}$ の最小の部分体を表す。 $\square$

$\boxed{\text{解答例}}$ $L_1 \cap L_2/K$ と L_1L_2/K が有限次拡大になることは問題6-2の解答例で示した。

$\boxed{1}$ $L_1 \cap L_2/K$ がGalois拡大になることを示そう。

$\alpha \in L_1 \cap L_2$ を任意にとる。

$i = 1, 2$ について，L_i/K がGalois拡大であることと

問題6-1の結果と $\alpha \in L_i$ より，α のすべての K 上での共役元は L_i に含まれる。

ゆえに，α のすべての K 上での共役元は $L_1 \cap L_2$ に含まれる。

したがって，問題6-1の結果より，$L_1 \cap L_2/K$ は Galois拡大である。

② L_1L_2/K がGalois拡大になることを示そう.

L_1L_2の任意の元γは, ある$\alpha_1, \cdots, \alpha_r \in L_1$, $\beta_1, \cdots, \beta_s \in L_2$と
$f(x_1, \cdots, x_r, y_1, \cdots, y_s) \in K(x_1, \cdots, x_r, y_1, \cdots, y_s)$が存在して,
$\gamma = f(\alpha_1, \cdots, \alpha_r, \beta_1, \cdots, \beta_s)$と表される.

このとき, K上の体同型$\varphi : L_1L_2 \hookrightarrow \mathbb{C}$について,
そのL_k上への制限がK上の体同型になることと, L_k/KがGalois拡大であることより,
$\varphi(\alpha_i) \in L_1$, $\varphi(\beta_j) \in L_2$となる. ゆえに,

$$\varphi(\gamma) = f(\varphi(\alpha_1), \cdots, \varphi(\alpha_r), \varphi(\beta_1), \cdots, \varphi(\beta_s)) \in L_1L_2.$$

これでL_1L_2/KがGalois拡大であることがわかった. □

(注 上で$\varphi(L_1L_2) \subset L_1L_2$が示せており, L_1L_2と$\varphi(L_1L_2)$のK上でのベクトル空間としての次元は有限次元で等しいので$\varphi(L_1L_2) = L_1L_2$.)

$\boxed{\text{問題 6-4}}$ 以下の体の拡大がGalois拡大であるかどうかを判定せよ.

(1) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, (2) $\mathbb{Q}(\sqrt[3]{3})/\mathbb{Q}$, (3) $\mathbb{Q}(\sqrt[4]{7})/\mathbb{Q}$,

(4) $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$, (5) $\mathbb{Q}(\sqrt[3]{3},\sqrt{-3})/\mathbb{Q}$, (6) $\mathbb{Q}(\sqrt[4]{7},\sqrt{-1})/\mathbb{Q}$,

(7) $\mathbb{Q}(\sqrt[3]{3},\sqrt{-3})/\mathbb{Q}(\sqrt{-3})$, (8) $\mathbb{Q}(\sqrt[4]{7},\sqrt{-1})/\mathbb{Q}(\sqrt{-1})$.

$\boxed{\text{解答例}}$ (1), (4), (5), (6), (7), (8) はGalois拡大だが, (2), (3) はそうではない.

$\omega = e^{2\pi i/3} = \dfrac{-1+\sqrt{-3}}{2}$, $i=\sqrt{-1}$ とおく.

$\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$, $\mathbb{Q}(\sqrt[3]{3},\sqrt{-3}) = \mathbb{Q}(\sqrt[3]{3},\omega)$, $\mathbb{Q}(\sqrt[4]{7},\sqrt{-1})$ はそれぞれ

x^2-2, x^4-10x^2+1, x^3-3, x^4-7 の $\mathbb{Q}$ 上での

最小分解体なので $\mathbb{Q}$ のGalois拡大である.

$\mathbb{Q}(\sqrt[3]{3},\sqrt{-3}) = \mathbb{Q}(\sqrt[3]{3},\omega) = \mathbb{Q}(\sqrt[3]{3},\omega\sqrt[3]{3},\omega^2\sqrt[3]{3})$ は

$\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\omega)$ 上での x^3-3 の最小分解体なので $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\omega)$ のGalois拡大である.

$\mathbb{Q}(\sqrt[4]{7},\sqrt{-1}) = \mathbb{Q}(\sqrt[4]{7},i) = \mathbb{Q}(\sqrt[4]{7}, i\sqrt[4]{7}, -\sqrt[4]{7}, -i\sqrt[4]{7})$ は

$\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$ 上での x^4-7 の最小分解体なので $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$ のGalois拡大である.

$\mathbb{Q}(\sqrt[3]{3})$ は $\mathbb{Q}$ 上での $\sqrt[3]{3}$ の共役元 $\omega\sqrt[3]{3}$ を含まないので $\mathbb{Q}$ のGalois拡大ではない.

$\mathbb{Q}(\sqrt[4]{7})$ は $\mathbb{Q}$ 上での $\sqrt[4]{7}$ の共役元 $i\sqrt[4]{7}$ を含まないので $\mathbb{Q}$ のGalois拡大ではない. $\square$