

問題 8-1  $K, L$  は  $\mathbb{C}$  の部分体 であるとする.

← 標数 0 を使う,

- (1)  $L/K$  が 2 次拡大 ならば  $L/K$  は Galois 拡大 であることを示せ.
- (2) 3 次以上の有限次拡大  $L/K$  で  $L$  の  $K$  上での体の自己同型 が  $\text{id}_L$  しか存在しないものの例を具体的に 1 つ挙げよ.

ヒント (1)  $L$  は  $L = K(\alpha)$ ,  $\alpha \in L$ ,  $\alpha \notin K$ ,  $\alpha^2 \in K$  の形になる.

←  $-\alpha \neq \alpha$  を使う.

(注) 標数 2 だと  $-\alpha = \alpha$

- (2)  $\mathbb{Q}$  の 3 次拡大 で そのような例 を 作れる.
- もしも 3 次拡大  $L/\mathbb{Q}$  が Galois 拡大 ならば,

$|\text{Gal}(L/\mathbb{Q})| = [L:\mathbb{Q}] = 3$  なので  $\text{Gal}(L/\mathbb{Q}) \cong C_3 \neq \{\text{id}_L\}$  となる.

だから,  $L/\mathbb{Q}$  の自己同型 ( $L$  の  $\mathbb{Q}$  上での自己同型) が  $\text{id}_L$  しか存在しないものを 作るためには, Galois 拡大 ではない 3 次拡大  $L/\mathbb{Q}$  を 作ら なければ いけない. しかし, そのような例は 問題 7-? で す で に 作 っ て い る. □

**定義**  $n$  次の置換群  $S_n$  の部分群  $G$  が 推移的 (可移的, transitive) であるとは、  
任意の  $i, j \in \{1, 2, \dots, n\}$  について ある  $\sigma \in G$  で  $\sigma(i) = j$  をみたすものが  
存在することと定める。

**問題 8-2**  $S_3$  の推移的部分群をすべて挙げよ。  $\square$

**問題 8-3**  $S_4$  の以下の 11 個の部分群を考える:

$$H_1 = \{1\}, \quad H_2 = \langle (1, 2) \rangle, \quad H_3 = \langle (1, 2)(3, 4) \rangle, \quad H_4 = \langle (1, 2, 3) \rangle,$$

$$H_5 = \langle (1, 2, 3, 4) \rangle, \quad H_6 = \langle (1, 2), (3, 4) \rangle, \quad H_7 = \{1, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\},$$

$$H_8 = \langle (1, 2), (2, 3) \rangle \cong S_3, \quad H_9 = \langle (1, 2, 3, 4), (1, 3) \rangle, \quad H_{10} = A_4, \quad H_{11} = S_4.$$

(1) 各々の位数を求めよ、

(2) 各々について  $S_4$  の正規部分群かどうか判定せよ、

(3) 各々について推移的であるかどうか判定せよ、

$\square$

**定理**  $p$  は素数であるとする. このとき,  $S_p$  の推移的な部分群  $G$  で  
互換を1つ以上含むものは  $S_p$  全体に一致する.

**証明** ①  $\{1, 2, \dots, p\}$  に同値関係  $\sim$  を

$$\lambda \sim j \iff \lambda = j \text{ または } \lambda \neq j \text{ で } (\lambda, j) \in G$$

$\lambda$  と  $j$  の互換

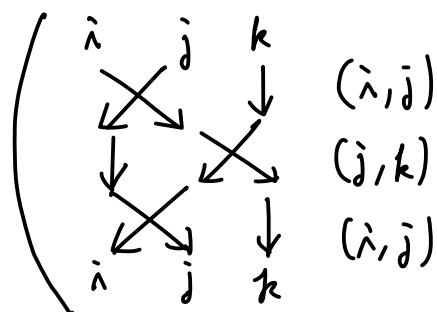
この定理は  
問題8-4で  
使われる.

と定められることを示そう.

反射律 ( $\lambda \sim \lambda$ ) と対称律 ( $\lambda \sim j \Rightarrow j \sim \lambda$ ) をめたすことは自明なので,  
推移律 ( $\lambda \sim j$  かつ  $j \sim k \Rightarrow \lambda \sim k$ ) のみを示せばよい.

$\lambda \sim j$  かつ  $j \sim k \Rightarrow \lambda \sim k$  を  $\lambda, j, k$  が互いに異なる場合に示せばよい.  
 $\lambda \neq j, \lambda \neq k, j \neq k, \lambda \sim j, j \sim k$  と仮定する.

$(\lambda, j), (j, k) \in G$  なので  $G \ni (\lambda, j)(j, k)(\lambda, j) = (\lambda, k)$  となり,  $\lambda \sim k$  となる.  
これで  $\sim$  が同値関係になることが示された.



← この図を見れば  $(\lambda, j)(j, k)(\lambda, j) = (\lambda, k)$  となることがわかる.  
 $(j, k)(\lambda, j)(j, k)$  も成立している.

□ 2  $\sigma \in G$  かつ  $i \sim j \Rightarrow \sigma(i) \sim \sigma(j)$  となることを示そう.

$\sigma \in G$ ,  $i \sim j$  と仮定する.

(i)  $i = j$  のとき  $\sigma(i) = \sigma(j)$  なので  $i \sim j$ .

(ii)  $i \neq j$ ,  $(i, j) \in G$  のとき,  $\sigma(i) \neq \sigma(j)$  かつ  $G \ni \sigma(i, j)\sigma^{-1} = (\sigma(i), \sigma(j))$   
なので  $\sigma(i) \sim \sigma(j)$ .

↑  
 $\sigma$  は全単射

一般に, 巡回置換  $(i_1, \dots, i_\ell)$  ( $i_1, \dots, i_\ell$  が互いに異なり,  $i_{\ell+1} = i_1$  とおくと,  
 $(i_1, \dots, i_\ell)$  は  $i_\nu$  を  $i_{\nu+1}$  にうつす) について,

$$\sigma(i_1, \dots, i_\ell)\sigma^{-1}(\sigma(i_\nu)) = \sigma(i_1, \dots, i_\ell)(i_\nu) = \sigma(i_{\nu+1})$$

なので  $\sigma(i_1, \dots, i_\ell)\sigma^{-1} = (\sigma(i_1), \dots, \sigma(i_\ell))$ .

これで,  $\sigma \in G$  かつ  $i \sim j \Rightarrow \sigma(i) \sim \sigma(j)$  が示された.

③  $\sim$  のすべての同値類の元の個数が等しいことを示そう.

$\lambda$  の同値類を  $[\lambda]$  と書き,  $\lambda, j \in \{1, 2, \dots, p\}$  を任意にとる.

$G$  は推移的なので ある  $\sigma \in G$  が存在して  $\sigma(i) = j$  となる.

□2 より, 任意の  $i', j' \in \{1, 2, \dots, p\}$  について,

$$\lambda \sim \lambda' \stackrel{\textcircled{1}}{\Rightarrow} j \sim \sigma(\lambda') \quad \text{かつ} \quad j \sim j' \stackrel{\textcircled{2}}{\Rightarrow} \lambda \sim \sigma^{-1}(j')$$

なので,  $\sigma([i]) = \{\sigma(i') \mid i \sim i'\} = [j]$  となることがわかる.  $\leftarrow$

$\left( \begin{array}{l} j' \in \sigma([i]) \text{ のとき, } j' = \sigma(i'), i \sim i' \text{ と書けるので ①より } i \sim j' \text{ となるので } j' \in [j], \\ j' \in [j] \text{ のとき, } i' = \sigma^{-1}(j') \text{ とおくと, ②より } i \sim i' \text{ となり, } j' = \sigma(i') \text{ となるので} \\ j' \in \sigma([i]) \text{ となる.} \end{array} \right)$

$\sigma$  は  $\{1, 2, \dots, p\}$  からそれ自身への全単射なので、

$[i]$ と $[j]$ の元の個数は等しい。

これで  $\sim$  のすべての同値類の元の個数が等しいことが示された.

④  $\sim$  の同値類は  $\{1, 2, \dots, p\}$  の全体になることを示そう. (ここで  $p$  が素数なことを使う.)

$G$  は互換を 1 つ以上含むので, 2 つ以上の元を含む同値類が存在する.

③ より,  $\{1, 2, \dots, p\}$  は 2 以上の同じ個数の元を含む同値類たちに分割されていることになる.

しかし,  $p$  は素数なのでそのような分割での同値類は  $\{1, 2, \dots, p\}$  のただ 1 つだけになる.

⑤  $G$  が  $S_p$  のすべての互換を含むことを示そう.

$i \in \{1, 2, \dots, p\}$  を任意にとる. ④ より

$$[i] = \{j \mid i=j \text{ または } i \neq j \text{ で } (i, j) \in G\} = \{1, 2, \dots, p\}$$

なので,  $i$  とは異なるすべての  $j$  について  $(i, j) \in G$ .

⑥  $S_p$  はすべての互換から生成されるので ⑤ より  $G = S_p$ .

□

**問題 8-4**  $f(x) \in \mathbb{Q}[x]$  は  $\mathbb{Q}$  上既約な多項式であるとし,

$L$  は  $f$  の  $\mathbb{Q}$  上での最小分解体であるとし,  $G = \text{Gal}(L/\mathbb{Q})$  とおく. 以下を示せ.

(1)  $f(x)$  の互いに異なる根全体を  $\alpha_1, \dots, \alpha_n \in L$  と書くと,  $G = \text{Gal}(L/\mathbb{Q})$  は  $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$  に推移的に作用する. ←  $f$  の  $\mathbb{Q}$  上での既約性を使う.

(任意の  $i, j \in \{1, 2, \dots, n\}$  についてある  $\sigma \in G$  が存在して  $\sigma(\alpha_i) = \alpha_j$ .)

(2)  $n = \deg f$  が素数でかつ  $f(x)$  がちょうど  $n-2$  個の実根を持つならば  $G = \text{Gal}(L/\mathbb{Q}) \cong S_n$  となる. ← 前ページまでに説明した定理を使う.

(3)  $f(x) = x^5 - 16x + 2$  が  $\mathbb{Q}$  上既約で,

$f$  の  $\mathbb{Q}$  上での最小分解体  $L$  について,  $\text{Gal}(L/\mathbb{Q}) \cong S_5$ .

□