$\boxed{\text{問題 8-1}}$ 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) 2 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 id_L しか存在しないものの例を具体的に1つ挙げよ。

$\boxed{\text{ヒント}}$ (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、
$|\mathrm{Gal}(L/\mathbb{Q})| = [L:\mathbb{Q}] = 3$ なので $\mathrm{Gal}(L/\mathbb{Q}) \cong C_3 \neq \{\mathrm{id}_L\}$ 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 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 ?-? ですでに作っている。 $\square$

$\boxed{\text{定義}}$ n次の置換群S_nの部分群Gが<u>推移的</u>(<u>可移的</u>, <u>transitive</u>)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だと定める.

$\boxed{\text{問題8-2}}$ S_3の推移的部分群をすべて挙げよ. $\square$

$\boxed{\text{問題8-3}}$ S_4の以下の11個の部分群を考える:

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

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

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

(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. $\square$

$\boxed{\text{定理}}$ 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.

この定理は問題8-4で使われる.

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

$$i \sim j \iff i=j \text{ または } i\neq j \text{ で } \underbrace{(i,j)}_{i\text{と}j\text{の互換}} \in G$$

と定められることを示そう.

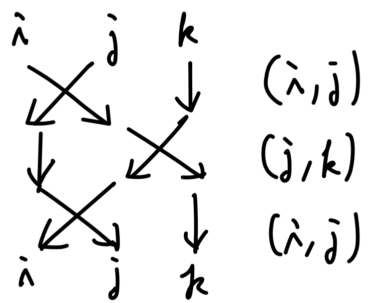
反射律 $(i\sim i)$ と対称律 $(i\sim j \Rightarrow j\sim i)$ をみたすことは自明なので, 推移律 $(i\sim j$ かつ $j\sim k \Rightarrow i\sim k)$ のみを示せばよい.

$i\sim j$ かつ $j\sim k \Rightarrow i\sim k$ を i,j,k が互いに異なる場合に示せばよい.

$i\neq j$, $i\neq k$, $j\neq k$, $i\sim j$, $j\sim k$ と仮定する.

$(i,j),(j,k)\in G$ なので $G\ni (i,j)(j,k)(i,j)=(i,k)$ となり, $i\sim k$ 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 $(i,j)(j,k)(i,j)=(i,k)$ となることがわかる.

$(j,k)(i,j)(j,k)$ も成立している.

$\boxed{2}$ $\sigma \in G$ 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、$\sigma(i) \neq \sigma(j)$ でかつ $G \ni \sigma(i, j)\sigma^{-1} = (\sigma(i), \sigma(j))$

なので $\sigma(i) \sim \sigma(j)$。

$\Uparrow$ σ は全単射

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

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

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

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

$\boxed{3}$ ～のすべての同値類の元の個数が等しいことを示そう。

iの同値類を$[i]$と書き，$i, j \in \{1, 2, \dots, p\}$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。

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

$$i \sim i' \underset{①}{\Rightarrow} \underset{\sigma(i)}{\underset{\shortparallel}{j}} \sim \sigma(i') \quad \text{かつ} \quad j \sim j' \underset{②}{\Rightarrow} \underset{\sigma^{-1}(j)}{\underset{\shortparallel}{i}} \sim \sigma^{-1}(j')$$

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

（$j' \in \sigma([i])$のとき，$j' = \sigma(i')$，$i \sim i'$と書けるので①より$j \sim j'$なので$j' \in [j]$，
$j' \in [j]$のとき，$i' = \sigma^{-1}(j')$とおくと，②より$i \sim i'$となり，$j' = \sigma(i')$となるので
$j' \in \sigma([i])$となる。）

σ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～のすべての同値類の元の個数が等しいことが示された。

$\boxed{4}$ $\sim$ 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。

$\boxed{3}$ 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。

$\boxed{5}$ 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。$\boxed{4}$ 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 $(i,j) \in G$。

$\boxed{6}$ S_p はすべての互換から生成されるので $\boxed{5}$ より $G = S_p$。

$\square$

$\boxed{\text{問題 8-4}}$ $f(x) \in \mathbb{Q}[x]$ 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, $G = \mathrm{Gal}(L/\mathbb{Q})$ 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, ← (f の $\mathbb{Q}$上での既約性を使う.)

$G = \mathrm{Gal}(L/\mathbb{Q})$ は $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ に推移的に作用する.

(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

$G = \mathrm{Gal}(L/\mathbb{Q}) \cong S_n$ 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, $\mathrm{Gal}(L/\mathbb{Q}) \cong S_5$. □