代数II　小テスト　2019–12–18

答えと簡単な解説

[問 1] 以下の文のそれぞれについて，正しいものには ○ を，正しくないものには × をカッコ内に記せ． ただし，$\overline{K}$ は 体 K の代数的閉包である．

(×) $\alpha \in \overline{K}$ に対して，一般に $|\mathrm{Aut}(K(\alpha)/K)| = |\mathrm{Conj}(\alpha, K)|$ が成り立つ．
【解説】　$K(\alpha)/K$ が正規でない場合は成り立たない． たとえば，$\mathrm{Conj}(\sqrt[4]{2}, \mathbb{Q}) = \left\{\sqrt[4]{2}, -\sqrt[4]{2}, \sqrt[4]{2}i, -\sqrt[4]{2}i\right\}$ は 4 個の元をもつが，$\mathbb{Q}(\sqrt[4]{2})$ は実数体に含まれるから，$\mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q})$ は位数 2 の群．

(○) K を標数 0 の体とする． $\alpha, \beta \in \overline{K}$ に対して $L = K(\alpha, \beta)$ とおくとき，$\mathrm{Conj}(\alpha, K) \subset L$ かつ $\mathrm{Conj}(\beta, K) \subset L$ が成り立てば，L/K はガロア拡大である．
【解説】　分離拡大であることは標数が 0 からわかるので，正規拡大であることを確かめる． 任意の $\sigma \in \mathrm{Aut}(\overline{K}/K)$ に対して，仮定より $\sigma(\alpha) \in \mathrm{Conj}(\alpha, K) \subset L$，したがって $\sigma(\alpha) \in L$，同様に $\sigma(\beta) \in L$ だから，$\sigma(L) = K(\sigma(\alpha), \sigma(\beta)) \subset L$． よって L/K は正規．

(○) L/K が正規拡大ならば，任意の $\alpha \in L$ と任意の $\sigma \in \mathrm{Aut}(\overline{K}/K)$ に対して，$\sigma(\alpha) \in L$ が成り立つ．
【解説】　L/K の正規性より $\mathrm{Conj}(\alpha, K) \subset L$． 一方，$\sigma(\alpha)$ は α の K 上の共役元なので，$\sigma(\alpha) \in L$．

(○) 代数拡大 L/K と $\mathrm{Aut}(L/K)$ の部分群 H に対して，$H \subset \mathrm{Aut}(L/L^H)$ がつねに成り立つ．
【解説】　$\sigma \in H$ とすると，σ は L の自己同型写像である．さらに，L^H の定義から，任意の $x \in L^H$ について $\sigma(x) = x$ だから，$\sigma \in \mathrm{Aut}(L/L^H)$．よって $H \subset \mathrm{Aut}(L/L^H)$．

(○) 有限次ガロア拡大 L/K に対して，つねに $[L : K] = |\mathrm{Gal}(L/K)|$ が成り立つ．
【解説】　ガロア拡大は分離拡大だから $L = K(\alpha)$ と表せる． ここで，一般に $|\mathrm{Aut}(K(\alpha)/K)| \leq |\mathrm{Conj}(\alpha, K)| \leq [K(\alpha) : K]$ が成り立つが，正規性より前の不等号が等号に，分離性より後の不等号が等号になるから，$[L : K] = |\mathrm{Aut}(L/K)|$．

(○) 体の拡大 L/K がガロア拡大ならば，任意の中間体 M について，L/M はガロア拡大である．

【解説】　L/K が分離的ならば L/M も分離的であり，L/K が正規ならば L/M も正規である．

(×) M を体の拡大 L/K の中間体とするとき，$L/M,\ M/K$ がともにガロア拡大ならば L/K もガロア拡大である．
【解説】　$M=\mathbb{Q}(\sqrt{2}),\ L=\mathbb{Q}(\sqrt{1+\sqrt{2}})$ とすると，$M/\mathbb{Q}$ も L/M も2次のガロア拡大であるが，$\sqrt{1+\sqrt{2}}$ の $\mathbb{Q}$ 上の共役元である $\sqrt{1-\sqrt{2}}$ は L に属さない（だって $L\subset\mathbb{R}$ だけど $\sqrt{1-\sqrt{2}}\notin\mathbb{R}$ だもん）ので，$L/\mathbb{Q}$ はガロアではない．

(○) $[L:K]$ が素数であるガロア拡大 L/K のガロア群は巡回群である．
【解説】　素数位数の群は巡回群である．

(○) $\mathbb{Q}(\sqrt{2019})/\mathbb{Q}$ はガロア拡大である．
【解説】　標数0の体の拡大はすべて分離的である（以下の各問もすべて）．さらに，2次拡大は正規である．

(×) $\mathbb{Q}(\sqrt[3]{15})/\mathbb{Q}$ はガロア拡大である．
【解説】　ω を1の原始3乗根とすると，$\sqrt[3]{15}\omega$ は $\sqrt[3]{15}$ の $\mathbb{Q}$ 上の共役元であるが，実数でないので $\mathbb{Q}(\sqrt[3]{15})$ に属さないので $\mathbb{Q}$ 上正規でない．

(○) $\mathbb{Q}\big(\sqrt[3]{17},\omega\big)$ は $\mathbb{Q}$ 上ガロアである．ただし，ω は1の原始3乗根．
【解説】　$\mathrm{Conj}(\sqrt[3]{17},\mathbb{Q})=\big\{\sqrt[3]{17},\sqrt[3]{17}\omega,\sqrt[3]{17}\omega^2\big\}$ と $\mathrm{Conj}(\omega,\mathbb{Q})=\{\omega,\omega^2\}$ は，どちらも $\mathbb{Q}\big(\sqrt[3]{17},\omega\big)$ に含まれるから $\mathbb{Q}$ 上正規である．

(×) $\mathbb{Q}(\sqrt{7})/\mathbb{Q}$ のガロア群は位数7の巡回群である．
【解説】　$\big|\mathrm{Gal}(\mathbb{Q}(\sqrt{7})/\mathbb{Q})\big|=\big[\mathbb{Q}(\sqrt{7}):\mathbb{Q}\big]=2$ だから，ガロア群は位数2である．

(×) $\mathbb{Q}(\sqrt{2},\sqrt{-2})$ は $\mathbb{Q}$ 上のガロアであり，そのガロア群は巡回群である．
【解説】　$\mathbb{Q}(\sqrt{2},\sqrt{-2})$ は，分離多項式 $X^4-4=(X^2-2)(X^2+2)$ の $\mathbb{Q}$ 上の最小分解体だからガロアであるが，以下に示すように巡回拡大ではない．$L=\mathbb{Q}(\sqrt{2},\sqrt{-2}),\ M_1=\mathbb{Q}(\sqrt{2}),\ M_2=\mathbb{Q}(\sqrt{-2})$ とおくと，$L/M_1,\ L/M_2$ はともに2次ガロア拡大であり，したがって $L/\mathbb{Q}$ のガロア群は位数2の部分群を（少なくとも）2つもつから，巡回群ではない（実際には，$\mathrm{Gal}(L/\mathbb{Q})$ はふたつの位数2の巡回群の直積になる）．

(×) $\mathbb{Q}(\sqrt[3]{2},\sqrt{-3})$ は $\mathbb{Q}$ 上のガロアであり，そのガロア群はアーベル群である．
【解説】　ω を1の原始3乗根とし，$L=\mathbb{Q}(\sqrt[3]{2},\omega)$ とおくと，L は X^3-2 の $\mathbb{Q}$ 上の最小分解体なので，$L/\mathbb{Q}$ はガロア拡大．さらに，$\omega=\dfrac{-1+\sqrt{-3}}{2}$ だから $L=\mathbb{Q}(\sqrt[3]{2},\sqrt{-3})$．しかし，以下に示すように $L/\mathbb{Q}$ はアーベル拡大ではない．$G=\mathrm{Gal}(L/\mathbb{Q})$ とおき，これがアーベル群であると仮定する．$L/\mathbb{Q}$ は6次拡大だから，G の位数も6である．

位数 6 の群は，巡回群または 3 次対称群のどちらかだが，3 次対称群は非アーベルなので，G は巡回群である． ここで，$j = 0, 1, 2$ に対して $M_j = \mathbb{Q}(\sqrt[3]{2}\omega^j)$ とおくと，これらはすべて $L/\mathbb{Q}$ の中間体で $\mathbb{Q}$ 上の 3 次拡大体だから，L/M_j は 2 次ガロア拡大，したがって G は位数 2 の部分群を（少なくとも）3 つもつから巡回群とはなり得ず，矛盾する．

(○) ζ を 1 の原始 20 乗根とすると，$\mathbb{Q}(\zeta)$ は $\mathbb{Q}$ 上のガロア拡大で，そのガロア群はアーベル群である．

【解説】 （円分拡大の例） ζ は $X^{20} - 1$ の根だから，ζ の $\mathbb{Q}$ 上の最小多項式は $X^{20} - 1$ の因子であり，分解

$$X^{20} - 1 = (X - 1)(X - \zeta)(X - \zeta^2) \dots (X - \zeta^{19})$$

より，

$$\mathrm{Conj}(\zeta, \mathbb{Q}) \subset \left\{1, \zeta, \zeta^2, \dots, \zeta^{19}\right\} \subset \mathbb{Q}(\zeta)$$

がわかるから，$\mathbb{Q}(\zeta)/\mathbb{Q}$ はガロアである． $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ とおく．いま $\sigma \in G$ に対して，

$$\sigma(\zeta)^{20} = \sigma(\zeta^{20}) = \sigma(1) = 1$$

だから，$\sigma(\zeta)$ も 1 の 20 乗根であり，したがって $\sigma(\zeta) = \zeta^j$ $(j \in \mathbb{Z})$ と書ける（j は 20 を法として定まることに注意）． ここで，$\sigma, \tau \in G$ に対して，$\sigma(\zeta) = \zeta^j$, $\tau(\zeta) = \zeta^k$ であれば，

$$(\sigma\tau)(\zeta) = \sigma(\tau(\zeta)) = \sigma(\zeta^k) = \sigma(\zeta)^k = (\zeta^j)^k = \zeta^{jk}.$$

さらに $\tau = \sigma^{-1}$ ととれば，$\zeta^{jk} = \zeta$，よって $jk \equiv 1 \pmod{20}$，とくに j は 20 と互いに素である． したがって，G から 20 を法とする既約剰余類群への準同型写像

$$\Gamma : G \longrightarrow (\mathbb{Z}/20\mathbb{Z})^\times, \quad \sigma \mapsto j$$

が定義できることがわかる． さらに，$\sigma \in \mathrm{Ker}\,\Gamma$ ならば $\sigma(\zeta) = \zeta^1 = \zeta$ だから σ は恒等写像であり，よって Γ は単射である． 以上より G は $(\mathbb{Z}/20\mathbb{Z})^\times$ の部分群と同型であり，とくにアーベル群である．

(○) ζ を 1 の原始 20 乗根とし $K = \mathbb{Q}(\zeta)$ とすると，$\alpha^{20} \in K$ をみたす任意の $\alpha \in \overline{K}$ について，$K(\alpha)/K$ はガロア拡大で，そのガロア群は巡回群である．

【解説】 （クンマー拡大の例） $a = \alpha^{20}$ とすると，α は K 上の多項式 $X^{20} - a$ の根である． よって α の K 上の最小多項式は $X^{20} - a$ の因子であり，前問のように ζ を 1 の原始 20 乗根とすると，分解

$$X^{20} - a = (X - \alpha)(X - \alpha\zeta)(X - \alpha\zeta^2) \dots (X - \alpha\zeta^{19})$$

より，

$$\mathrm{Conj}(\alpha, K) \subset \left\{\alpha, \alpha\zeta, \alpha\zeta^2, \ldots, \alpha\zeta^{19}\right\} \subset K(\alpha)$$

がわかるから，$K(\alpha)/K$ はガロアである． $G = \mathrm{Gal}(K(\alpha)/K)$ とおく．いま $\sigma \in G$ に対して，

$$\sigma(\alpha)^{20} = \sigma(\alpha^{20}) = \sigma(a) = a = \alpha^{20}$$

だから，$\sigma(\alpha) = \alpha\zeta^j$ と書ける（j は 20 を法として定まることに注意）．ここで，$\sigma, \tau \in G$ に対して，$\sigma(\alpha) = \alpha\zeta^j$, $\tau(\alpha) = \alpha\zeta^k$ であれば，$\zeta \in K$ より $\sigma(\zeta) = \zeta$ だから

$$(\sigma\tau)(\alpha) = \sigma(\tau(\alpha)) = \sigma(\alpha\zeta^k) = \sigma(\alpha)\zeta^k = \alpha\zeta^j\zeta^k = \alpha\zeta^{j+k}.$$

これにより，G から 20 を法とする剰余環の加法群への準同型写像

$$\Delta : G \longrightarrow \mathbb{Z}/20\mathbb{Z}, \quad \sigma \mapsto j$$

が定義できることがわかる．さらに，$\sigma \in \mathrm{Ker}\,\Delta$ ならば $\sigma(\alpha) = \alpha\zeta^0 = \alpha$ だから σ は恒等写像であり，よって Δ は単射である． 以上より G は $\mathbb{Z}/20\mathbb{Z}$ の部分群と同型であるが，加法群 $\mathbb{Z}/20\mathbb{Z}$ は巡回群だからその部分群も巡回群であり，したがって G は巡回群である．