Algebra III : PROBLEMS

1 体の拡大

1.1 $L : K$ を体の拡大とし、$S, T \subset L$ とする。このとき、$K(S \cup T) = K(S)(T)$ であることを示せ。特に、L の元 α, β について、$K(\alpha)(\beta) = K(\alpha, \beta)$ である。

1.2 $L : K$ を体の拡大、$\alpha \in L$ とし、$K[\alpha] = \{f(\alpha) \mid f(t) \in K[t]\}$ とする。この時、$K[\alpha] \subset K(\alpha)$ であり、かつ $K(\alpha) = \{f(\alpha)/g(\alpha) \mid f(t), g(t) \in K[t],\ g(\alpha) \neq 0\}$ であることを示せ。

1.3 $L : K$ を体の拡大、$\alpha \in L$ とするとき、$K[\alpha] = K(\alpha)$ であることと、α が K 上代数的であることは同値であることを示せ。

1.4 $L : K$ を体の拡大とし、$\alpha_1, \alpha_2, \ldots, \alpha_n \in L$ とする。
(1) $K(\alpha, \alpha_2, \ldots, \alpha_n) = \{f(\alpha_1, \alpha_2, \ldots, \alpha_n)/g(\alpha_1, \alpha_2, \ldots, \alpha_n) \mid f, g \in K[t_1, t_2, \ldots, t_n], g(\alpha_1, \alpha_2, \ldots, \alpha_n) \neq 0\}$.
(2) $\alpha_1, \alpha_2, \ldots, \alpha_n$ が K 上代数的ならば、$K(\alpha_1, \alpha_2, \ldots, \alpha_n) = K[\alpha_1, \alpha_2, \ldots, \alpha_n]$ であることを示せ。ここで、$K[\alpha_1, \alpha_2, \ldots, \alpha_n]$ は K 上の n 変数多項式環に $\alpha_1, \alpha_2, \ldots, \alpha_n$ を代入したものとする。

1.5 下のそれぞれの $\boldsymbol{C}$ の元について、K 上の最小多項式を求めよ。ただし、$i = \sqrt{-1}$ とする。

(1) $i,\ K = \boldsymbol{Q}$　(2) $i,\ K = \boldsymbol{R}$　(3) $i,\ K = \boldsymbol{C}$
(4) $\sqrt{2},\ K = \boldsymbol{Q}$　(5) $(\sqrt{5}+1)/2,\ K = \boldsymbol{Q}$　(6) $(-1+\sqrt{-3})/2,\ K = \boldsymbol{Q}$

1.6 次の体は、$\boldsymbol{Q}$ の単純拡大であることを示せ。($K = \boldsymbol{Q}(\alpha)$ となる α を見つけよ。)
(1) $\boldsymbol{Q}(\sqrt{3}, \sqrt{5})$　(2) $\boldsymbol{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$　(3) $\boldsymbol{Q}(\sqrt[5]{2}, \sqrt{-1})$

1.7 実数体 $\boldsymbol{R}$ は、有理数体 $\boldsymbol{Q}$ の単純拡大ではないことを示せ。
ヒント： 可算濃度の体の単純拡大は、また可算濃度となることを示せ。

1.8 $K = \boldsymbol{Z}_2$ とする。K 上の 6 次以下の既約多項式をすべて求めよ。

1.9 $K = \boldsymbol{Z}_3$ とする。K 上の 4 次以下の既約多項式をすべて求めよ。

1.10 $K = \boldsymbol{Z}_p$ (p は素数)、$m(t)$ を K 上の n 次の既約多項式とする。このとき、$K[t]/(m(t))$ は、p^n 個の元からなる体であることを示せ。

1.11 (1) 4 個の元からなる体の、和、積の表をつくれ。
(2) 8 個の元からなる体の、和、積の表をつくれ。

1.12 $\boldsymbol{C}$ の元 α が、次のような最小多項式を持つとき、$\boldsymbol{Q}(\alpha)$ を求めよ。
例：$t^2-5 \Rightarrow \boldsymbol{Q}(\sqrt{5}) = \{a+b\sqrt{5} \mid a,b \in \boldsymbol{Q}\}$.
(1) t^3+2　(2) $t^4+t^3+t^2+t+1$　(3) $t^4-10t+1$　(4) t^3-1

1.13 $\alpha \in \boldsymbol{C}$ を、t^3-t-1 の根とし、$K = \boldsymbol{Q}(\alpha)$ をする。このとき、α^{-1}, $(\alpha+1)^{-1}$, $(\alpha^2+\alpha+1)^{-1}$ を、α の多項式として求めよ。

1.14 $\omega = (-1+\sqrt{-3})/2$ としたとき、$\boldsymbol{Q}(\sqrt[3]{2})$ から $\boldsymbol{Q}(\sqrt[3]{2}\omega)$ への、同型写像を具体的に一つ定めよ。

2　拡大の次数と作図問題

2.1 次の体の拡大の次数を求めよ。
(1) $\boldsymbol{C} : \boldsymbol{Q}$　(2) $\boldsymbol{R}(\sqrt{5}) : \boldsymbol{R}$　(3) $\boldsymbol{Q}(\sqrt[3]{2}) : \boldsymbol{Q}$　(4) $\boldsymbol{Q}(\sqrt{3}, \sqrt{5}) : \boldsymbol{Q}$　(5) $\boldsymbol{Q}(\sqrt[7]{3}) : \boldsymbol{Q}$

2.2 $\boldsymbol{Q}(\sqrt{3}, \sqrt{5})$ の各元は、$a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15}$, $a, b, c, d \in \boldsymbol{Q}$ の形に一意的に書き表せることを示せ。また、$(a, b, c, d) \neq (0, 0, 0, 0)$ のとき、この元の逆元を具体的に求めよ。

2.3 $[L : K]$ が素数ならば、$K \subset M \subset L$ なる L の部分体は K か L のみ。

2.4 $L : K$ を体の拡大とする。L の元で K 上代数的なもの全体の集合を M とすると、M は、体となることを示せ。M を、L の体 K 上の代数閉包という。

2.5 A を $\boldsymbol{Q}$ 上代数的な $\boldsymbol{C}$ の元全体とするとき、次を示せ。
(1) A は体。　(2) $[A : \boldsymbol{Q}] = \infty$　(3) $[\boldsymbol{C} : A] = \infty$
(4) A の代数拡大は、A のみである。

2.6 $L : K$ を有限拡大、$p(t)$ を K 上の既約多項式で、$\deg p(t) > 1$ なるものとする。$([L : K], \deg p(t)) = 1$ ならば、$p(t)$ は、L の中に根を持たないことを示せ。

2.7 (1) $L : K$、$M : L$ を共に代数拡大とすると、$M : K$ も代数拡大であることを示せ。
(2) $L : K$、$M : L$ を共に体の拡大、$M : K$ を代数拡大とすると、$M : L$、$L : K$ も代数拡大であることを示せ。

2.8 $(0, 0)$ と $(1, 0)$ からは、定規とコンパスで正 9 角形は作図できないことを示せ。
ヒント： $(\cos(\pi/9), 0)$ が作図出来ないことを示せばよい。$\beta = 2\cos(\pi/9)$ とし、$\cos(3\theta) = 4\cos^3\theta - 3\cos\theta$ を用い、$\beta^3 - 3\beta - 1 = 0$ を示せ。

2.9 正 5 角形を作図せよ。
ヒント： $(\cos(2\pi/5), 0)$ を $(0, 0)$ と $(1, 0)$ から作図できれば良い。$z = \cos(2\pi/5) + \sqrt{-1}\sin(2\pi/5)$ は、$z^5 = 1 \neq z$ を満たすから、$t^4 + t^3 + t^2 + t + 1 = 0$ の根である。これを $u = t + 1/t$ を用いて表し、$\cos(2\pi/5)$ を求めよ。

2.10 (1) 定規とコンパスを用い、$\pi/4$ を 3 等分せよ
(2) 正 n 角形、正 m 角形 が作図できれば、正 $2^t \cdot l$ 角形も作図可能である。ここで、t は任意の非負整数、l は、n と m の最小公倍数である。

2.11 角 θ を定規とコンパスで 3 等分する事が出来るための必要十分条件は、多項式 $4t^3 - 3t - \cos\theta$ が、$\boldsymbol{Q}(\cos\theta)$ 上で可約となることであることを示せ。

註： 角 θ が与えられたとき、その 3 等分を作図することは可能なときも、不可能なときもある。しかし、定規上の任意の位置の長さを測ることを許せば 3 等分も可能になる。その方法に興味のある人は、参考書のスチュアートの本参照。

2.12 $(1,0)$, $(a,0)$ が与えられているとき、定規とコンパスで $(\sqrt{a},0)$ を作図せよ。

2.13 $E:F$ を有限拡大とし、$M:F$ を任意の体の拡大、E, M を体 K の部分体のとする。$EM=E(M)$ とすると、$[EM:M]\leq[E:F]$ であることを示せ。
ヒント： $E=F(\alpha)$ の場合に、まず示し、帰納法を用いよ。

3　自己同型、不変体、分解体

3.1 $L : K$ を体の拡大。M を中間体とする。
(1) $\Gamma(L : K), \Gamma(L : M)$ はともに群で、かつ $\Gamma(L : M) \leq \Gamma(L : K)$ であることを示せ。
(2) $H \leq \Gamma(L : K)$ ならば、$H^+ = \{a \in L \mid \sigma(a) = a \text{ for all } \sigma \in H\}$ は、拡大 $L : K$ の中間体であることを示せ。
(3) $M \subset (M^*)^+$ かつ、$H \subset (H^+)^*$ であることを示せ。

3.2 次の拡大 $L : K$ について $\Gamma(L : K)$ を求めよ。
(1) $\boldsymbol{Q}(\sqrt{2}) : \boldsymbol{Q}$　　(2) $\boldsymbol{Q}(\sqrt[5]{2}) : \boldsymbol{Q}$　　(3) $\boldsymbol{Q}(\sqrt{2}, \sqrt{3}) : \boldsymbol{Q}$

3.3 前問のそれぞれの拡大の中間体を全て求めよ。

3.4 L を 4 個の元からなる体とする。(1.8 参照) $K = \{0, 1\} \subset L$ とするとき、$\Gamma(L : K)$ を求めよ。また、$L : K$ の中間体を全て求めよ。

3.5 3.2, 3.4 の拡大において、$\phi : \mathcal{F} \to \mathcal{G}$ $(M \mapsto M^*)$ と、$\psi : \mathcal{G} \to \mathcal{F}$ $(H \mapsto H^+)$ が全単射となるのはどれか。ここで、$\mathcal{F}$ は、拡大 $L : K$ の中間体全体、$\mathcal{G}$ は、$\Gamma(L : K)$ の部分群全体を表すものとする。

3.6 K を体とするとき、$S = \{n \in \boldsymbol{N} \mid n \cdot 1 = 0\}$ が、$S = \emptyset$ のときは、$\mathrm{char}K = 0$、$S \neq \emptyset$ のときは、$\mathrm{char}K = \min S$ とする。$\mathrm{char}K$ を、体 K の標数という。このとき、$\mathrm{char}K$ は、0 又は、素数であることを示せ。

3.7 標数 0 の体 L は、有理数体 $\boldsymbol{Q}$ と同型な体 K を含む。さらに、L の自己同型はすべて、$\Gamma(L : K)$ の元である。

3.8 K を標数 $p > 0$ の体とし、$L : K$ を体の拡大とする。$a \in K$ にたいし、$t^p - a$ のひとつの根を $\alpha \in L$ とする。このとき、$K(\alpha)$ は、$t^p - a$ の分解体であることを示せ。

3.9 (1) K を体、$f \in K[t]$、Σ を K 上 f の分解体、$\alpha_1, \ldots, \alpha_n$ を Σ における f の根とする。$\sigma \in \Gamma(\Sigma : K)$ とするとき、$\{\sigma(\alpha_1), \ldots, \sigma(\alpha_n)\} = \{\alpha_1, \ldots, \alpha_n\}$ すなわち、f の根の置換を引き起こすことを示せ。
(2) (1) の置換において、$\sigma(\alpha_i) = \alpha_i$ $(i = 1, 2, \ldots, n)$ ならば、σ は、Σ 上で恒等写像であることを示せ。

3.10 下記の多項式について、$\boldsymbol{Q}$ 上の分解体を $\boldsymbol{C}$ の部分体として求めよ。
(1) $t^3 - 1$　　(2) $t^4 + 5t^2 + 6$　　(3) $t^6 - 8$

3.11 前問で求めた分解体の $\boldsymbol{Q}$ 上の拡大次数を求めよ。

3.12 Σ が、体 K 上 f の分解体で、$K \subset L \subset \Sigma$ であれば、Σ は L 上 f の分解体であることを示せ。

3.13 f は、体 K 上の n 次の多項式とし、Σ を f に対する分解体とするとき $[\Sigma : K]$ は、$n!$ の約数であることを示せ。

3.14 $L = K(\alpha)$ を K の単純代数拡大とする。この時、$|\Gamma(L : K)| \leq [L : K]$ であることを示せ。α の K 上の最小多項式を $f(x)$ とする。上で等号が成立すれば L は、K 上 $f(x)$ の分解体である。

4　正規性と分離性

4.1 $f \in \boldsymbol{C}[t]$ とする。f は、$\boldsymbol{C}$ で分解する（代数学の基本定理）ことを証明せよ。（例えば、整関数に関する Liouville の定理を用いよ。）

4.2 t を $\boldsymbol{Q}$ 上超越的な元とする。このとき、$\boldsymbol{Q}(t)$ の元で、$\boldsymbol{Q}$ 上代数的な元は $\boldsymbol{Q}$ の元に限ることを示せ。特に、$\boldsymbol{Q}(t)$ は $\boldsymbol{Q}$ 上正規。

4.3 下記の拡大のうちで正規拡大はどれか。
(1) $\boldsymbol{Q}(\sqrt{-5}) : \boldsymbol{Q}$　　(2) $\boldsymbol{Q}(\sqrt[7]{5}) : \boldsymbol{Q}$　　(3) $\boldsymbol{Q}(\sqrt{5}, \sqrt[7]{5}) : \boldsymbol{Q}(\sqrt[7]{5})$
(4) $\boldsymbol{R}(\sqrt{-7}) : \boldsymbol{R}$

4.4 ２次の拡大は全て正規拡大であることを示せ。

4.5 F を有限体とすると、F は、$\boldsymbol{Z}_p$ と同型な部分体 $\boldsymbol{F}_p$ を含む。ここで、$p = \mathrm{char}F$ で、p は素数である。$[F : \boldsymbol{F}_p] = n$ とすると、$|F| = p^n$ かつ、F は、$t^{p^n} - t$ の $\boldsymbol{F}_p$ 上の分解体であることを示せ。

4.6 $L : K$ を正規拡大。$L \supset M \supset K$ を中間体とすると、$L : M$ は正規拡大であることを示せ。また、$M : K$ は正規拡大とは限らない。$L : K$ は、正規拡大であるが、$M : K$ は、正規拡大ではない例をあげよ。

4.7 $L : K$ を体の拡大。$|L| < \infty$ とする。このとき、$L : K$ は、正規かつ分離拡大であることを示せ。さらにある素数 p について、$|L| = p^n$, $|K| = p^m$ で、かつ、$m \mid n$ となっていることを示せ。

4.8 $t^4 - 2$ の $\boldsymbol{C}$ の中での $\boldsymbol{Q}$ 上の分解体を L とする。このとき、$[L : \boldsymbol{Q}]$ および、$\Gamma(L : \boldsymbol{Q})$ の元を全て求めよ。

4.9 $\gamma = \sqrt{2 + \sqrt{2}}$ とする。$\boldsymbol{Q}(\gamma) : \boldsymbol{Q}$ は、正規拡大で、$\Gamma(\boldsymbol{Q}(\gamma) : \boldsymbol{Q})$ は、アーベル群であることを示せ。

4.10 p を素数、K を標数が 0 または、p と互いに素な体とする。L を、$t^p - 1$ の K 上の分解体とする。このとき、$\Gamma(L : K)$ は、アーベル群であることを示せ。（p は素数でなくても $\Gamma(L : K)$ は、アーベル群となる。このことを示せ。）

4.11 n を正の整数、K を標数が 0 または、n と互いに素な体とする。$t^n - 1$ は、K で分解しているとする。$a \in K$、L を、$t^n - a$ の K 上の分解体とするとき、$\Gamma(L : K)$ は、アーベル群であることを示せ。

4.12 K を無限個の元を含む体とする。任意の有限分離拡大 $L : K$ は単純拡大である。
ヒント：以下のステップを参考にして示しても良い。

(a) ２元で生成される $L = K(\beta, \gamma)$ の場合に示せばい。

(b) $g(x)$、$h(x)$ をそれぞれ β、 γ の K 上の最小多項式とする。M を $g(x)h(x)$ の L 上の分解体とすると、$g(x)$、$h(x)$ はどちらも M において、重根を持たない。

(c) M における、$g(x)$、$h(x)$ の根をそれぞれ、$\beta_1 = \beta, \ldots, \beta_n$、$\gamma_1 = \gamma, \ldots, \gamma_m$ とし、c を $(\beta - \beta_i)/(\gamma - \gamma_j)$、$(i = 2, \ldots, n,\ j = 2, \ldots, m)$ のいずれとも異なる K の元とする。このような、c をとることができる。$\alpha = \beta + c\gamma$ とする。この時、$h(x)$ と、$\bar{g}(x) = g(\alpha - cx) \in K(\alpha)[x]$ の共通根は、γ のみである。

(d) γ の $K(\alpha)$ 上の最小多項式を $f(x)$ とする。すると、$f(x)$ は、$h(x)$ も $\bar{g}(x)$ も割りきる。このことより、$f(x) = x - \gamma$ を得る。従って、 $K(\alpha) = K(\beta, \gamma)$。

5 次数と位数

5.1 $L:K$ を有限正規拡大、$L \supset M \supset K$ を中間体とするとき次を示せ。
(1) $\tau : M \to L$ が、K-単射準同型 (i.e., 単射準同型で、$\tau_{|K} = id$) ならば、$\sigma_{|M} = \tau$ となる $\sigma \in \Gamma(L:K)$ が存在することを示せ。
(2) $p(t) \in K[t]$ を、$\alpha,\ \beta \in L$ に対して $p(\alpha) = p(\beta) = 0$ となる既約多項式とすると、$\sigma(\alpha) = \beta$ となる $\sigma \in \Gamma(L:K)$ が存在することを示せ。

5.2 F を $\mathrm{char}F = p$ なる体とする。このとき次を示せ。
(1) $\sigma : F \to F\ (x \mapsto x^p)$ とすると、σ は単射準同型であることを示せ。特に、$|F| < \infty$ ならば、σ は自己同型である。(Frobenius 自己同型と呼ばれる。)
(2) $|F| = p^n$、K を L の素体、すなわち $K = \{0, 1, \ldots, p-1\} \subset L$ とすると、$\mathrm{Aut}(F) = \Gamma(F:K) =< \sigma >$ であることを示せ。

5.3 $K = \boldsymbol{Q}(\omega)$、$\omega = \mathrm{e}^{2\pi i/7} \in \boldsymbol{C}$ とするとき、$G = \Gamma(K:\boldsymbol{Q})$ の元を求めよ。$G^+ = \boldsymbol{Q}$ であることを示せ。

5.4 前問の G の部分群をすべて求め、それぞれについて不変体を求めよ。

5.5 $L = K(\zeta)$、ζ は、1 の n 乗根 (すなわち、$\zeta^n = 1$) とする。このとき、$\boldsymbol{Z}_n^* \to \Gamma(L:K)$ なる全準同型があることを示せ。特に、$\Gamma(L:K)$ はアーベル群である。

5.6 $K = \boldsymbol{Q}(\sqrt{2}, \sqrt{3})$ とし、$G = \Gamma(K:\boldsymbol{Q})$ のすべての部分群について、不変体を求めよ。

5.7 p を素数、n を自然数、$q = p^n$ とする。F を $K = \boldsymbol{Z}_p$ 上 $t^q - t$ の分解体とする。このとき、$|F| = q$ であることを示せ。
ヒント： F の中で、$t^q - t$ の根全体が体になることを示せ。

5.8 $K = \boldsymbol{Q}(\gamma)$、$\gamma = \sqrt{2 + \sqrt{2}}$ とする。$\Gamma(\boldsymbol{Q}(\gamma) : \boldsymbol{Q})$ の部分群をすべて求め、それぞれについて不変体を求めよ。

5.9 $L:K$ を有限拡大、N を L を含む K の正規拡大とする。また、$\alpha \in L$、$m(t)$ をその最小多項式とする。このとき、次を示せ。
(1) $K(\alpha)$ から N の中への相異なる K 単射準同型の数は、高々$\deg m(t)$ である。
(2) $K(\alpha)$ から N の中への相異なる K 単射準同型の数が $\deg m(t)$ であることと、α が、K 上分離的であることとは同値である。
(3) L から N の中への相異なる K 単射準同型の数は、高々$[L:K]$ である。また、この数が丁度 $[L:K]$ となるのは、$L:K$ が分離拡大の時、またその時に限る。

5.10 $f(x) = g(x)h(x) \in K[x]$ とし、L を K 上 $f(x)$ の分解体、M、N をそれぞれ K 上 $g(x)$、$h(x)$ の分解体とする。この時、$\Gamma(L:K)$ は、$\Gamma(M:K) \times \Gamma(N:K)$ の部分群と同型であることを示せ。

5.11 K を標数 p の体、F を K に含まれる素体（$F \simeq \boldsymbol{Z}/p\boldsymbol{Z}$）とし、$f(t) = t^p - t - c \in K[t]$ とする。また、L を K の拡大体とする。

(1) $\alpha \in L$ が、$f(t) = 0$ の根であれば、任意の $a \in F$ に対して $\alpha + a$ も根である。

(2) $f(t)$ は、K 上既約であるかまたは、K で分解しているかのいずれかである。

(3) $c \in F$ であれば、$f(t)$ は、F 上既約である。

(4) $f(t)$ は、K 上既約であるとし、$\alpha \in L$ をその根とする。この時、$\Gamma(K(\alpha) : K)$ は、位数 p の巡回群である。

6 ガロワの定理

6.1 $L:K$ を有限拡大とするとき、次を示せ。

$$L:K \quad \text{正規かつ分離拡大} \quad \Leftrightarrow \quad K \quad \text{は} \quad \Gamma(L:K) \quad \text{の不変体}$$

6.2 ガロワ理論の基本定理 (1), (2), (3) を証明せよ。

6.3 $L:K$ を有限正規分離拡大、M をその中間体とする。このとき次を示せ。
(1) $\tau \in \Gamma(L:K) \Rightarrow (\tau(M))^* = \tau M^* \tau^{-1}$.
(2) ガロワ理論の基本定理 (4), (5) を証明せよ。

6.4 $L:K$ を有限正規分離拡大（有限ガロア拡大)、M をその中間体とする。$\Gamma(L:K)$ がアーベル群ならば、$M:K$ は、正規拡大であり、そのガロア群 $\Gamma(M:K)$ もアーベル群であることを示せ。

6.5 体 K の標数が 2 でなければ、$[L:K]=2$ であることと、L がある既約多項式 t^2-a $(a \in K)$ の分解体を成すことは同値であることを示せ。またこのとき、$|\Gamma(L:K)|=2$ である。

6.6 t^3-2 の $\boldsymbol{Q}$ 上の分解体について、そのガロワ群、部分体をすべて求めよ。

6.7 t^4-2t^2+9 の $\boldsymbol{Q}$ 上の分解体は、$\boldsymbol{Q}(\sqrt{-1},\sqrt{2})$ であることを示し、その $\boldsymbol{Q}$ 上のガロワ群、部分体をすべて求めよ。

6.8 t^4-2 の $\boldsymbol{Q}$ 上の分解体について、そのガロワ群、部分体をすべて求めよ。

6.9 $L:K$ は、3 次正規分離拡大 L のある元 α に対して、$\sigma \in \Gamma(L:K)$ で、$\sigma(\alpha)=\alpha+1$ となるものがあるとする。このとき、K の標数および α の最小多項式を求めよ。

6.10 $L:K$ を 3 次正規分離拡大で L のある元 $\alpha \neq 0$ に対して、$\sigma \in \Gamma(L:K)$ で $\sigma(\alpha)=2\alpha$ となるものがあるとする。このとき、　K の標数と α の最小多項式を求めよ。

6.11 $\zeta_n = \mathrm{e}^{2\pi i/n}$ とする。次のそれぞれについて、ガロワ群 $\Gamma(\boldsymbol{Q}(\zeta_n):\boldsymbol{Q})$ および、部分体を求めよ。
(1) $n=3$　　(2) $n=4$　　(3) $n=5$　　(4) $n=6$
(5) $n=7$　　(6) $n=8$

6.12 L および F を、体 E の部分体とする。$L:K$ を有限正規分離拡大、$F:K$ を有限拡大とする。このとき、次を示せ。
(1) $LF:F$ は、有限正規分離拡大である。
(2) $\Gamma(LF:F)$ は、$\Gamma(L:L\cap F)$ と同型である。
(3) $[LF:F]=[L:L\cap F]$、かつ $[LF:L]=[F:L\cap F]$。

7　べき根による解の存在

7.1 G を群、H を G の部分群、N を G の正規部分群とする。このとき、次を示せ。
(1) G が可解ならば、H も可解である。
(2) G が可解であることと、N および G/N が可解であることとは同値である。

7.2 n 次交代群 A_n および n 次対称群 S_n は、$n \geq 5$ の時、可解群ではないことを示せ。
(I-5-7 参照)

7.3 G を可解な有限群、N をその極大正規部分群 ($N \lhd G \neq N$ かつ $N \subset H \lhd G \Rightarrow N = H$ or G) とする。このとき、G/N は素数位数の巡回群であることを示せ。

7.4 群 G の元 g, h に対して、$[g,h] = g^{-1}h^{-1}gh$ を g, h の交換子という。また、G の交換子全体で生成された G の部分群 $D(G) = [G,G] =< [g,h] \mid g^{-1}h^{-1}gh,\ g,h \in G >$ を G の交換子群という。
(1) $gh = hg[g,h]$ であり、$D(G) \lhd G$
(2) $G/D(G)$ はアーベル群である。
(3) $N \lhd G$ に対して、次の２つの条件は同値。
　　*(a) $N \lhd G$ かつ、G/N は、アーベル群。
　　*(b) $N \supset D(G)$。

7.5 G を群とし、$D_0(G) = G$、$D_{i+1}(G) = D(D_{i-1}(G))$ とする。特に、$D_1(G) = D(G)$ である。この時、ある n について、$D_n(G) = 1$ であることと、G が可解群であることは同値であることを示せ。

7.6 $f(x) \in K[x]$、$f(x)$ の分解体における根を $X = \{\alpha_1, \ldots, \alpha_n\}$ とする。$f(x)$ のガロア群 G が、X 上の置換群として、可移であることと $f(x)$ が既約であることは同値であることを示せ。

7.7 次のそれぞれの f について、$\boldsymbol{Q}$ 上 f のガロワ群の元を f の根の置換で表せ。
(1)　$f = (t^2-2)(t^2-3)$　　(2)　$f = t^3 - 2$　　(3)　$f = t^4 - 2$

7.8 p を素数とし、G を対称群 S_p の部分群で、その位数が p で割り切れかつ G は S_p のある互換 (i,j) を含むものとする。このとき、$G = S_p$ であることを示せ。

7.9 p を素数、f を $\boldsymbol{Q}$ 上既約な p 次多項式とする。f が $\boldsymbol{C}$ の中に丁度２個の虚根を持てば f の $\boldsymbol{Q}$ 上のガロワ群は S_p と同型となることを示せ。
ヒント：τ を複素共役とすると、τ は f のガロワ群の元でかつ、f の根の置換として、互換であることを示せ。

7.10 次のような $\boldsymbol{C}$ の元を含む、$\boldsymbol{Q}$ のべき根による拡大を求めよ。
(1) $(\sqrt{11} - \sqrt[7]{23})/\sqrt[4]{5}$　　(2) $(\sqrt{6} + 2^3\sqrt{5})^4$
(3) $(2\sqrt[5]{5} - 4)/\sqrt{1+\sqrt{99}}$

7.11 次の $\boldsymbol{Q}$ 上の多項式はべき根で解けないことを示せ。
(1) $t^5 - 6t + 3$　　(2) $t^5 - 4t + 2$　　(3) $t^5 - 4t^2 + 2$
(4) $t^5 - 6t^2 + 3$　　(5) $t^7 - 10t^5 + 15t + 5$

7.12 (1) 6次方程式 $t^6 + 2t^5 - 5t^4 + 9t^3 - 5t^2 + 2t + 1 = 0$ をべき根で解け。
(2) $t^4 + t^3 + t^2 + t + 1 = 0$ をべき根で解け。

7.13 既約多項式のガロワ群は多項式の根の上の置換群として可移であることを示せ。

8 ガロワ群の可解性

8.1 任意の体 K に対し、t^3-3t+1 は、K 上既約であるか、または、K で分解しているかのいずれかであることを示せ。

8.2 K を標数0の体とする。$L:K$ を有限正規拡大で、そのガロワ群を $G=\{\tau_1,\tau_2,\ldots,\tau_n\}$ とする。トレースを

$$T=T_{L/K}:L\to L \qquad (a\mapsto \tau_1(a)+\tau_2(a)+\cdots+\tau_n(a))$$

とする。このとき、T は、$T(L)=K$ なる K-線形写像であることを示せ。

8.3 前問において、$G=<\tau>$ ならば、次が成立することを示せ。

$$T(a)=0 \quad\Longleftrightarrow\quad \exists b\in L \text{ such that } a=b-\tau(b)$$

8.4 $L:M$、$M:K$ を共に有限ガロワ拡大とするとき次を示せ。
(1) $N_{M/K}N_{L/M}=N_{L/K}$ (2) $T_{M/K}T_{L/M}=T_{L/K}$

8.5 以下の $\boldsymbol{Q}$ 上の多項式をべき根で解け。
(1) t^3-7t+5 (2) t^3-7t+6 (3) t^4+5t^3-2t-1
(4) t^4+4t+2

8.6 (1) 体 K 上の3次方程式 $t^3+c_2t^2+c_1t+c_0=0$ は、t を適当な $t-c$ で置き換えることにより、$t^3+at+b=0$ の形に変形できることを示せ。
(2) $t^3+at+b=0$ の根を $\alpha_1,\alpha_2,\alpha_3$ とする。$D=((\alpha_1-\alpha_2)(\alpha_2-\alpha_3)(\alpha_3-\alpha_1))^2$ とすると、$D=-4a^3-27b^2$ である。
(3) $L=K(\alpha_1,\alpha_2,\alpha_3)$ とすると、$L=K(\alpha_1,\sqrt{D})$ であることを示せ。
(4) $\delta=\dfrac{-b+\sqrt{-D/27}}{2}$、$\alpha=\delta-\dfrac{a}{3\delta}$ とすると、α は、$t^3+at+b=0$ の根であることを示せ。

8.7 4次方程式のべき根による解法を説明せよ。

8.8 P を点 $(0,0)$ および $(1,0)$ を含む $\boldsymbol{R}^2$ の部分集合、K を P の点の座標により生成された $\boldsymbol{R}$ の部分体とする。このとき、点 (α,β) が P から、コンパスと定規で作図可能であることと、α,β を含む体 K の拡大体 L とその中間体の列、$K=K_0\subset K_1\subset\cdots\subset K_r=L$ で、$[K_i:K_{i-1}]=2$ $(i=1,2,\ldots,r-1)$ となるものが存在することとは同値であることを示せ。

8.9 正 n 角形が定規とコンパスで作図可能であることと、$n=2^rp_1\cdots p_s$ r, s 負でない整数で、p_i は、$p_i=2^{2^{r_i}}+1$ という形の奇素数、という形に書けることは同値であることを示せ。
ヒント： Step 1. 素数べき位数の群は可解。 Step 2. $L:K$ 正規、$[L:K]$ 2べき、

$\alpha, \beta \in L$ ならば、点 (α, β) は、P から、定規とコンパスで作図可能である。ここで、K は、前問のものとする。　Step 3. 正 n 角形が作図可能ならば、n の任意の約数 m について、正 m 角形は作図可能である。　Step 4. ζ_n を 1 の原始 n 乗根とすると、$[\boldsymbol{Q}(\zeta_p) : \boldsymbol{Q}] = p - 1$、$[\boldsymbol{Q}(\zeta_{p^2}) : \boldsymbol{Q}] = p(p-1)$ が任意の素数 p について成立する。