京都大数学系 院試過去問解答
数学II(代数)

nabla *

2024年7月30日

目 次

*Twitter:@nabla_delta

はじめに

京大理学研究科数学系の院試問題の解答です．解答が正しいという保証はありません．また，一部の解答は math.stackexchange.com で見つけたものを参考にしています．別解がある（かもしれない）場合でも解答は一つだけしか書いてありませんし，ここの解答より簡単な解答もあるかもしれません．この文書を使用して何らかの不利益が発生しても，私は責任を負いません．転載は禁止です．

2006 年度 (平成 18 年度)

問 2

p は素数とする．R は単位元を持つ環で元の個数が p^2 であるとする．このとき次の問に答えよ．
(1) R は可換であることを示せ．
(2) R はどのような環になるか，同型類を全て記述せよ．

解答. (2) 加法群としての 1 の位数は p, p^2 のどちらか．p^2 の時は R は巡回群だから $R \cong \mathbb{Z}/p^2\mathbb{Z}$. p の時を考える．R は $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ を含むから $x \in R \setminus \mathbb{F}_p$ が取れる．この時 $\{ax + b;\, a, b \in \mathbb{F}_p\}$ は $\mathbb{F}_p$ 上の 2 次元ベクトル空間だから位数は p^2. よってこれが R であるから，$x^2 = ax + b$ となる $a, b \in \mathbb{F}_p$ が取れる．$f(T) = T^2 - aT - b \in \mathbb{F}_p[T]$ とおく．

- $f(T)$ が既約の場合：$R = \mathbb{F}_p[T]/(f(T)) \cong \mathbb{F}_{p^2}$.
- $f(T)$ が相異なる 2 根を持つ場合：根を α, β とおくと，中国剰余定理より

$$R = \mathbb{F}_p[T]/((T-\alpha)(T-\beta)) \cong \mathbb{F}_p[T]/(T-\alpha) \times \mathbb{F}_p[T]/(T-\beta) \cong \mathbb{F}_p^2.$$

- $f(T)$ が重根を持つ場合：$f(T)$ の根を α とおくと $R = \mathbb{F}_p[T]/((T-\alpha)^2) \cong \mathbb{F}_p[T]/(T^2)$.

以上から

$$\mathbb{Z}/p^2\mathbb{Z}, \qquad \mathbb{F}_{p^2}, \qquad \mathbb{F}_p^2, \qquad \mathbb{F}_p[T]/(T^2).$$

(1) (2) から明らか. □

2005 年度 (平成 17 年度)

問 1

$\mathbb{Z}$ 上の n 変数多項式環 $\mathbb{Z}[x_1, x_2, \ldots, x_n]$ の極大イデアルは $n+1$ 個の元で生成されることを示せ.

解答. $\mathfrak{m}$ を $\mathbb{Z}[x_1, \ldots, x_n]$ の極大イデアルとする. 東大数理 2007 年度専門問 2 と同様に, 素数 p があって $\mathfrak{m} \cap \mathbb{Z} = p\mathbb{Z}$ となる. よって $\mathbb{Z}[x_1, \ldots, x_n]/(p) \cong \mathbb{F}_p[x_1, \ldots, x_n] =: R$ の極大イデアルが n 個の元で生成されることを示せば良い.

改めて $\mathfrak{m}$ を R の極大イデアルとする. $R/\mathfrak{m}$ は体であり, 有限生成 $\mathbb{F}_p$ 代数だから, Zariski の補題より $\mathbb{F}_p$ 上の有限次拡大である. よって x_i の $R/\mathfrak{m}$ における同値類を y_i とおくと, y_i の $\mathbb{F}_p$ 上最小多項式 $f_i(x)$ が存在する. この時 $f_i(y_i) = 0$ より $f_i(x_i) \in \mathfrak{m}$ だから, $\mathfrak{m}$ は R 上一次独立な n 個の元 $f_i(x_i)$ を含む. 一方 $R/(f_1(x_1), \ldots, f_n(x_n))$ は体なので, $(f_1(x_1), \ldots, f_n(x_n))$ は R の極大イデアルである. 従って $\mathfrak{m} = (f_1(x_1), \ldots, f_n(x_n))$ だから示された. □

2004 年度 (平成 16 年度)

問 1

自然数 m に対して $\zeta_m = e^{2\pi i/m}$ とおく．$3 \leq n \in \mathbb{Z}$ と n と互いに素な整数 a に対して

$$E = \frac{\sin(a\pi/n)}{\sin(\pi/n)}$$

とおく．また n と互いに素な整数 t に対して，$\sigma(t)$ は $\zeta_n \mapsto \zeta_n^t$ で定まる $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ の元を表す．

(1) $E \in \mathbb{Q}(\zeta_n)$ であることを示せ．

(2) n が偶数ならば

$$E^{\sigma(t)} = \frac{\sin(at\pi/n)}{\sin(t\pi/n)}$$

であることを示せ．n が奇数ならばどうなるか．

解答. (1)

$$E = \frac{\zeta_{2n}^a - \zeta_{2n}^{-a}}{\zeta_{2n} - \zeta_{2n}^{-1}} = \zeta_{2n}^{1-a}\frac{\zeta_{2n}^{2a}-1}{\zeta_{2n}^2-1} = \zeta_{2n}^{1-a}\frac{\zeta_n^a-1}{\zeta_n-1}$$

である．a が奇数なら $\zeta_{2n}^{1-a} = \zeta_n^{(1-a)/2} \in \mathbb{Q}(\zeta_n)$. a が偶数なら，$(a,n)=1$ より n は奇数なので

$$-\zeta_n^{(n+1)/2} = -e^{(n+1)\pi i/n} = e^{\pi i/n} = \zeta_{2n}$$

より $\zeta_{2n} \in \mathbb{Q}(\zeta_n)$. いずれにしても $E \in \mathbb{Q}(\zeta_n)$.

(2) • n が偶数の時：$(n,a)=1$ より a は奇数だから

$$E^{\sigma(t)} = \zeta_n^{t(1-a)/2}\frac{\zeta_n^{ta}-1}{\zeta_n^t-1} = \frac{\zeta_n^{ta/2}-\zeta_n^{-ta/2}}{\zeta_n^{t/2}-\zeta_n^{-t/2}} = \frac{\sin(ta\pi/n)}{\sin(t\pi/n)}. \qquad (*)$$

• n が奇数の時：a が奇数なら，上と同様に $(*)$ が成り立つ．a が偶数なら $\zeta_{2n}^{\sigma(t)} = -\zeta_n^{t(n+1)/2} = (-1)^{t+1}\zeta_{2n}^t$ だから，

$$E^{\sigma(t)} = (-1)^{(t+1)(1-a)}\zeta_{2n}^{t(1-a)}\frac{\zeta_n^{ta}-1}{\zeta_n^t-1} = (-1)^{t+1}\frac{\sin(ta\pi/n)}{\sin(t\pi/n)}.$$

□

2003 年度 (平成 15 年度)

問 1

(1) $\mathbb{Z}[\sqrt{5}]$ は整閉でないことを示せ.

(2) p, q を平方因子を含まない 1 と異なる奇数で，$p \neq q$ とする．このとき，$R = \mathbb{Z}[\sqrt{p}, \sqrt{q}]$ は整閉でないことを示せ.

解答. 環 R の商体を $Q(R)$ と書く.

(1) $(1+\sqrt{5})/2 \in Q(\mathbb{Z}[\sqrt{5}])$ は monic な多項式 $X^2 - X - 1 \in \mathbb{Z}[\sqrt{5}][X]$ の根なので $\mathbb{Z}[\sqrt{5}]$ 上整であるが，$\mathbb{Z}[\sqrt{5}]$ の元ではない．よって $\mathbb{Z}[\sqrt{5}]$ は整閉ではない.

(2) $\alpha_\pm = 1 \pm \sqrt{p}, \beta_\pm = 1 \pm \sqrt{q}$ として

$$x_1 = \frac{\alpha_+\beta_+}{2}, \quad x_2 = \frac{\alpha_+\beta_-}{2}, \quad x_3 = \frac{\alpha_-\beta_+}{2}, \quad x_4 = \frac{\alpha_-\beta_-}{2}$$

とおく．$\alpha_+ + \alpha_- = \beta_+ + \beta_- = 2, x_1 + x_2 = \alpha_+, x_3 + x_4 = \alpha_-$ であるから

$$\sum_{j=1}^{4} x_j = \frac{(\alpha_+ + \alpha_-)(\beta_+ + \beta_-)}{2} = 2,$$

$$\prod_{j=1}^{4} x_j = \frac{(\alpha_+\alpha_-\beta_+\beta_-)^2}{2^4} = \left(\frac{(1-p)(1-q)}{2^2}\right)^2,$$

$$\begin{aligned}\sum_{1\le j<k\le 4} x_j x_k &= x_1x_2 + (x_1+x_2)(x_3+x_4) + x_3x_4 = \frac{\alpha_+^2(1-q)}{4} + \alpha_+\alpha_- + \frac{\alpha_-^2(1-q)}{4} \\ &= \frac{(1+p)(1-q)}{2} + (1-p) = \frac{3-p-q-pq}{2},\end{aligned}$$

$$\begin{aligned}\sum_{1\le i<j<k\le 4} x_i x_j x_k &= x_1x_2(x_3+x_4) + (x_1+x_2)x_3x_4 = \frac{\alpha_+^2(1-q)}{4}\alpha_- + \alpha_+\frac{\alpha_-^2(1-q)}{4} \\ &= \frac{\alpha_+\alpha_-(1-q)}{4}(\alpha_+ + \alpha_-) = \frac{(1-p)(1-q)}{2}\end{aligned}$$

は全て整数である．よって $x_1 \in Q(R)$ は monic な R 係数多項式の根なので R 上整であるが，R の元ではない．従って R は整閉ではない.

(別解) $p \equiv 1 \bmod 4$ の時，$p = 4n+1$ とおくと $(1+\sqrt{p})/2 \in Q(R)$ は monic な多項式 $X^2 - X - n \in R[X]$ の根なので R 上整であるが，R の元ではない．よって R は整閉ではない．$q \equiv 1 \bmod 4$ の時も同様．上記のいずれでもない時は，$pq \equiv 3^2 \equiv 1 \bmod 4$ なので $(1+\sqrt{pq})/2$ について同様の議論をすれば良い. □

問 2

(1) 乗法の単位元 1 を持つ可換環 R は整域 A の部分環とする．商体の間の拡大 $Q(A) \supset Q(R)$ が代数的ならば，A の $\{0\}$ でないイデアル I について $I \cap R \neq \{0\}$ であることを示せ．

(2) (1) において $Q(A)/Q(R)$ が代数拡大という条件を外すと主張が必ずしも成り立たないことを，例を挙げて示せ．

(3) 可換環 A は部分環 R 上の整拡大とする．P は R の素イデアルとし，A の相異なる素イデアル Q_1, Q_2 が $R \cap Q_1 = R \cap Q_2 = P$ を満たすとする．Q_1 と Q_2 には含む含まれるの関係はないことを示せ．

解答. (1) $a \in I \setminus \{0\}$ を任意に取る．a の $Q(R)$ 上最小多項式を $f(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_1X + c_0$ とする．A が整域であることと次数の最小性から $c_0 \neq 0$ である．$sf(X) \in R[X]$ となる $s \in R \setminus \{0\}$ が取れる．この時 $sc_0 = -s(a^n + c_{n-1}a^{n-1} + \cdots + c_1a) \in I$ だから $sc_0 \in I \cap R$. また A は整域だから $sc_0 \neq 0$ である．

(2) $R = \mathbb{Q}, A = \mathbb{Q}[x]$ とする．ただし x は不定元である．この時 $Q(R) = \mathbb{Q}, Q(A) = \mathbb{Q}(x)$ であり $Q(A)/Q(R)$ は超越拡大．また A のイデアル $I = (x)$ は $I \cap R = \{0\}$ を満たす．

(3) $Q_1 \subset Q_2$ であったとする．仮定から A/Q_1 は R/P の整拡大であり，これらは整域である．また Q_2/Q_1 は A/Q_1 の素イデアルである．さらに $R \cap Q_1 = R \cap Q_2 = P$ より $(R/P) \cap (Q_2/Q_1) = \{0\}$ であるから，(1) より $Q_2/Q_1 = \{0\}$. よって $Q_1 = Q_2$ となって矛盾． □

2002 年度 (平成 14 年度)

問 1

単位元 1 を持つ可換環 A のイデアル I について，A の元 a がイデアル I の根基 $\sqrt{I}$ に含まれるための必要十分条件は，A 上の 1 変数多項式環 $A[T]$ の中で I と $1-aT$ が生成するイデアルが 1 を含むことであることを示せ.

解答. • $a \in \sqrt{I}$ の時：$a^n \in I$ となる $n \in \mathbb{N}$ が取れる．この時

$$1 = (1-aT)(1+aT+a^2T^2+\cdots+a^{n-1}T^{n-1}) + a^nT^n \in (I, 1-aT).$$

• $1 \in (I, 1-aT)$ の時：$x \in A$ の A/I における同値類を $\overline{x}$ で表すことにする．

$$\{0\} = A[T]/(I, 1-aT) \cong (A/I)[T]/(1-\overline{a}T)$$

であるから，$1 = (1-\overline{a}T)f(T)$ となる $f \in (A/I)[T]$ が存在する．$f(0) = 1$ より $f(T) = 1+\overline{c_1}T+\cdots+\overline{c_n}T^n$ とおけて，代入すると

$$1 = 1 + (\overline{c_1}-\overline{a})T + (\overline{c_2}-\overline{ac_1})T^2 + \cdots + (\overline{c_n}-\overline{ac_{n-1}})T^n - \overline{ac_n}T^{n+1}.$$

これより帰納的に $\overline{c_j} = \overline{a}^j$ $(j = 1, 2, \ldots, n)$ であり，T^{n+1} の係数から $\overline{a}^{n+1} = 0$ となるから $a \in \sqrt{I}$. □

2000 年度 (平成 12 年度)

問 1

$\zeta = e^{2\pi i/85} \in \mathbb{C}, K = \mathbb{Q}(\zeta) \cap \mathbb{R}$ とするとき，K の $\mathbb{Q}$ 上の Galois 群 $\mathrm{Gal}(K/\mathbb{Q})$ を求めよ．

解答. $L = \mathbb{Q}(\zeta)$ とおく．$L/\mathbb{Q}$ は Galois 拡大である．$\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ を $z \mapsto \bar{z}$ で定まるものとすると $\mathbb{Q}(\zeta + \zeta^{-1}) \subset L^{\langle\sigma\rangle}$ であるが，

$$[L : \mathbb{Q}(\zeta + \zeta^{-1})] = 2 = \#\langle\sigma\rangle = [L : L^{\langle\sigma\rangle}]$$

なので $L^{\langle\sigma\rangle} = \mathbb{Q}(\zeta + \zeta^{-1})$ が成り立つ．よって $K = L^{\langle\sigma\rangle} = \mathbb{Q}(\zeta + \zeta^{-1})$. $L/\mathbb{Q}$ は Abel 拡大ゆえ $K/\mathbb{Q}$ は Galois 拡大で $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Gal}(L/\mathbb{Q})/\langle\sigma\rangle$ である．また

$$\mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/85\mathbb{Z})^\times \cong (\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z})^\times \cong (\mathbb{Z}/5\mathbb{Z})^\times \times (\mathbb{Z}/17\mathbb{Z})^\times = \langle 2\rangle \times \langle 3\rangle$$

である．($(\mathbb{Z}/17\mathbb{Z})^\times = \langle 3\rangle$ であることは，位数が 16 で mod17 で $3^2 = 9, 3^4 = 13, 3^8 = 16$ となることからわかる．) 同型 $\mathbb{Z}/85\mathbb{Z} \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z}$ による -1 の像は $(-1 \bmod 5, -1 \bmod 17) = (2^2 \bmod 5, 3^8 \bmod 17)$ なので，

$$\begin{aligned}\mathrm{Gal}(K/\mathbb{Q}) &\cong \mathrm{Gal}(L/\mathbb{Q})/\langle\sigma\rangle \cong (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z})/\langle(2,8)\rangle \\ &\cong \mathbb{Z}^2/((4,0)\mathbb{Z} + (0,16)\mathbb{Z} + (2,8)\mathbb{Z}) \\ &\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}.\end{aligned}$$

ただし最後の同型は基本変形

$$\begin{pmatrix} 4 & 0 \\ 0 & 16 \\ 2 & 8 \end{pmatrix} \to \begin{pmatrix} 0 & 0 \\ 0 & 16 \\ 2 & 0 \end{pmatrix}$$

による． □

1996 年度 (平成 8 年度)

問 1

$SL(n,\mathbb{Z})$ の位数が有限である元 A を考える．A の位数を $m \geq 2$ とするとき，次の問に答えよ．
(1) $n \geq 2$ を一つ固定すると，m の取りうる値は有限個であることを示せ．
(2) $n = 2$ のとき，A を全て求めよ．

解答. (1) $\zeta_n = e^{2\pi i/n}$ とおき，$\Phi_n(x) = \prod_{(n,k)=1}(x - \zeta_n^k)$ を円分多項式とする．$A^m = I$ より A の最小多項式 $f(x)$ は $x^m - 1 = \prod_{d|m} \Phi_d(x)$ を割り切る．$f(x) \in \mathbb{Z}[x]$ であり $\Phi_d(x)$ は $\mathbb{Z}$ 上既約だから，m の約数 $1 \leq d_1 < \cdots < d_k \leq m$ が存在して $f(x) = \Phi_{d_1}(x) \cdots \Phi_{d_k}(x)$ と書ける．よって次数から

$$\sum_{i=1}^{k} \varphi(d_i) = \deg f \leq n$$

である．n を固定した時，$m = \prod_j p_j^{e_j}$ を m の素因数分解とすれば，p_j としてあり得るのは $n+1$ 以下の有限個．よって e_j の取りうる値も有限個だから，m としてあり得るのも有限個．

(2) $\varphi(d) = 1$ となる d は $1, 2$ の 2 個．$\varphi(d) = 2$ となる d を求める．$d = \prod_j p_j^{e_j}$ を素因数分解とすると，$\prod_j p_j^{e_j - 1}(p_j - 1) = 2$ だから d の素因数としてあり得るのは $2, 3$.

$$\varphi(2^j) = 2^{j-1}, \quad \varphi(3^j) = 2 \cdot 3^{j-1}, \quad \varphi(2^i 3^j) = 2^i 3^{j-1}$$

より $d = 4, 3, 6$ である．よって A の最小多項式としてあり得るのは

$$\Phi_1(x) = x - 1, \quad \Phi_2(x) = x + 1, \quad \Phi_3(x) = x^2 + x + 1, \quad \Phi_4(x) = x^2 + 1, \quad \Phi_6(x) = x^2 - x + 1$$

である．Φ_1 の時は $A = I$ で $m = 1$ なので不適．Φ_2 の時は $A = -I$. それ以外の時は上の $\Phi_d(x)$ は A の固有多項式でもあるから，$A^2 - (\operatorname{tr} A)A + I = 0$ とから $(\operatorname{tr} A - c)A = 0$ となる．(ただし c は $\Phi_d(x)$ の x の係数.) これより $\operatorname{tr} A = c$ だから $|\operatorname{tr} A| \leq 1$ である．逆に $A \in SL(2,\mathbb{Z})$ が $|\operatorname{tr} A| \leq 1$ を満たす時，A の固有多項式は $x^2 - (\operatorname{tr} A)x + 1 = 0$ なので，$\Phi_m(A) = 0$ となる $m \in \{3, 4, 6\}$ が存在する．よって $A^m = I$ となる．

以上から答えは $-I$ および $|\operatorname{tr} A| \leq 1$ を満たすもの全て． □

1995 年度 (平成 7 年度)

問 1

(1) 可換体 K 上の零でない 2 変数多項式 $f(x,y), g(x,y) \in K[x,y]$ が共通因子を持たないとき，$f(x,y), g(x,y)$ が 2 変数多項式環 $K[x,y]$ で生成するイデアル $I = (f(x,y), g(x,y))$ は $F(x), G(y)$ の形の元を含むことを示せ．ただし $F(x) \neq 0, G(y) \neq 0$ とする．
（ヒント：$K(x)$ を K 上の 1 変数有理関数体とするとき $K[x,y] \subset K(x)[y]$ と考えられる．）

(2) $0 < b < a < 1$ のとき

$$f(x,y) = x^2 + y^2 - 1, \qquad g(x,y) = \frac{x^2}{a^2} + \frac{y^2}{b^2} - 1$$

が実数体 $\mathbb{R}$ 上の多項式環 $\mathbb{R}[x,y]$ で生成するイデアル $I = (f(x,y), g(x,y))$ を含む $\mathbb{R}[x,y]$ の極大イデアル M を全て求めよ．

解答. (1) $K(x)$ は体だから，$f, g \in K[x,y] \subset K(x)[y]$ と見ると仮定より $a(x,y)f(x,y) + b(x,y)g(x,y) = d(x)$ となる $a(x,y), b(x,y) \in K(x)[y]$ と零でない $d(x) \in K(x)$ が存在する．零でない $K[x]$ の元を掛けることで $a, b \in K[x,y], d \in K[x]$ とできて，この時 $d(x) \in I, d \neq 0$ なので示された．

(2)

$$\begin{pmatrix} a^2 & -a^2b^2 \\ b^2 & -a^2b^2 \end{pmatrix} \begin{pmatrix} f \\ g \end{pmatrix} = \begin{pmatrix} (a^2-b^2)x^2 - a^2(1-b^2) \\ (b^2-a^2)y^2 - b^2(1-a^2) \end{pmatrix}$$

であり，左辺の 2 次行列は正則だから

$$\begin{aligned} I &= ((a^2-b^2)x^2 - a^2(1-b^2), (a^2-b^2)y^2 + b^2(1-a^2)) \\ &= (x^2 - c^2, y^2 + d^2). \end{aligned}$$

ここで $c = \sqrt{\frac{a^2(1-b^2)}{a^2-b^2}}, d = \sqrt{\frac{b^2(1-a^2)}{a^2-b^2}}$ とおいた．よって

$$M_\pm = (x \pm c, y^2 + d^2)$$

は I を含み，$\mathbb{R}[x,y]/M_\pm \cong \mathbb{C}[x]/(x \pm c) \cong \mathbb{C}$ は体だから，これは $\mathbb{R}[x,y]$ の極大イデアルである．一方 M/I は $\mathbb{R}[x,y]/I$ の極大イデアルであり，

$$\mathbb{R}[x,y]/I \cong \mathbb{C}[x]/(x^2 - c^2) \cong \mathbb{C}[x]/(x-c) \times \mathbb{C}[x]/(x+c) \cong \mathbb{C}^2$$

の極大イデアルは $\mathbb{C} \times \{0\}, \{0\} \times \mathbb{C}$ の 2 つだから，M としてあり得るのは 2 個．従って答えは $M_\pm$ の 2 個． □

1993 年度 (平成 5 年度)

問 1

n は 2 以上の自然数とする．複素数体 $\mathbb{C}$ 上の変数 X および $X^n + X^{-n}$ を $\mathbb{C}$ につけ加えて得られる有理関数体 $L = \mathbb{C}(X)$ および $K = \mathbb{C}(X^n + X^{-n})$ を考える．

(1) L は K 上の Galois 拡大になることを示し，その Galois 群を求めよ．

(2) $n = 3$ のとき，体の拡大 L/K の中間体を全て求めよ．

解答. (1) $Y = X^n + X^{-n}$ とおく．$f(T) = T^{2n} - YT^n + 1$ は Y について 1 次だから $K[T] = \mathbb{C}[T](Y)$ の元として既約である．また $f(X) = 0$ より $f(T)$ は X の K 上最小多項式である．

$$f(T) = T^{2n} - (X^n + X^{-n})T^n + 1 = (T^n - X^n)(T^n - X^{-n})$$

より X の K-共役元は $\zeta^k X^{\pm 1}\,(k = 0, 1, \ldots, n-1)$ である．ただし $\zeta = e^{2\pi i/n}$. これらは全て L の元だから L/K は正規拡大．またこれは分離拡大なので，Galois 拡大になっている．$\sigma, \tau \in \mathrm{Gal}(L/K)$ を

$$\sigma(X) = \zeta X, \qquad \tau(X) = X^{-1}$$

で定めると，$\sigma^n = \tau^2 = \mathrm{id}_L, \tau\sigma\tau = \sigma^{-1}$ より $\langle \sigma, \tau \rangle \cong D_n$ である．$\#\mathrm{Gal}(L/K) = \deg f = 2n$ だから，位数を比較して $\mathrm{Gal}(L/K) = \langle \sigma, \tau \rangle \cong D_n$.

(2) $\mathrm{Gal}(L/K) \cong D_3 = S_3$ の位数は 6 だから，部分群の位数は $2, 3$ のどちらか．$\langle \sigma \rangle$ の位数は 3. $(\sigma^j\tau)^2 = \sigma^j\tau\sigma^j\tau = \sigma^j(\tau\sigma\tau)^j = \sigma^j\sigma^{-j} = 1$ より $\sigma^j\tau$ の位数は 2. よって $\mathrm{Gal}(L/K)$ の部分群は $\langle \sigma \rangle, \langle \tau \rangle, \langle \sigma\tau \rangle, \langle \sigma^2\tau \rangle$ の 4 個．$\sigma\tau(X) = \zeta^{-1}X^{-1}, \sigma^2\tau(X) = \zeta^{-2}X^{-1}$ より

$$\mathbb{C}(X^3) \subset L^{\langle \sigma \rangle}, \quad \mathbb{C}(X + X^{-1}) \subset L^{\langle \tau \rangle}, \quad \mathbb{C}(\zeta X + X^{-1}) \subset L^{\langle \sigma\tau \rangle}, \quad \mathbb{C}(\zeta^2 X + X^{-1}) \subset L^{\langle \sigma^2\tau \rangle}$$

である．それぞれの左辺の体を $L_i\,(i = 1, \ldots, 4)$ とおく．$[L : L_1] = 3 = \#\langle \sigma \rangle = [L : L^{\langle \sigma \rangle}]$ であるから $L^{\langle \sigma \rangle} = L_1$ となる．他の L_i についても同様なので，L/K の中間体はこれら 4 個の L_i. □

1991 年度 (平成 3 年度)

問 1

部分群を丁度 5 個持つような有限群 G の構造を決定せよ．ただし，G 自身および $\{1\}$ も部分群として数える．

解答. Sylow の定理より $|G|$ の素因数は高々 3 個である．以下 p, q, r を素数とする．

• $|G|$ の素因数が 3 個の時：$p^2 \mid |G|$ なら Sylow p 部分群の部分群は 2 個以上となるから，$|G|$ の部分群は 6 個以上となって不適．q, r についても同様なので $|G| = pqr$. この時 G の Sylow n 部分群 $(n = p, q, r)$ を H_n とおくと，$G \rhd H_n$ より H_pH_q, H_qH_r, H_rH_p も G の部分群だから，G の部分群は 8 個以上となって不適.

• $|G|$ の素因数が 2 個の時：上と同様にして $|G| = pq, p^2q$ である．$|G| = pq$ の時，Sylow p 部分群は 2 個，Sylow q 部分群は 1 個として良い．この時 Sylw p 部分群の個数について $2 \equiv 1 \bmod p$ となるから不適．$|G| = p^2q$ の時，Sylow p 部分群は 1 個であり，それを H_p とすると位数 p^2 だから Abel 群である．よって $H_p \cong (\mathbb{Z}/p\mathbb{Z})^2, \mathbb{Z}/p^2\mathbb{Z}$. $H_p \cong (\mathbb{Z}/p\mathbb{Z})^2$ とすると，H_p の位数 p の部分群は $\langle (0,1) \rangle, \langle (1,y) \rangle$ $(y \in \mathbb{Z}/p\mathbb{Z})$ の $p+1$ 個あるから，G の部分群は $\{1\}, H_p, H_q, G$ と合わせて $p+5$ 個以上となり不適．$H_p \cong \mathbb{Z}/p^2\mathbb{Z}$ とすると，G の Sylow q 部分群は 1 個だから $G \rhd H_p, H_q$ である．$H_p = \langle x \rangle, H_q = \langle y \rangle$ とすると $y^{-1}xy = x^n$ となる $n \in \mathbb{Z}$ が存在するから，$y = x^{-1}yx^n$ より $xyx^{-1} = yx^{n-1} \in H_q$. よって $n = 1$ だから $xy = yx$. 従って $G \cong \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/p^2q\mathbb{Z}$ となるが，これは位数が p, p^2, q, pq の真部分群を持つから不適.

• $|G|$ の素因数が 1 個の時：$|G| = p^n$ とすると Sylow p 部分群は $n+1$ 個以上の部分群を持つから $n \leq 4$ が必要．また $|G| = p$ の時は $G \cong \mathbb{Z}/p\mathbb{Z}$ で不適なので $n \geq 2$ が必要.

(1) $n = 2$ の時は G は Abel 群で $G \cong (\mathbb{Z}/p\mathbb{Z})^2, \mathbb{Z}/p^2\mathbb{Z}$ である．$(\mathbb{Z}/p\mathbb{Z})^2$ の位数 p の部分群は，上で見たように $p+1$ 個あるから $p = 2$ である．$\mathbb{Z}/p^2\mathbb{Z}$ の位数 p の部分群は $\langle p \rangle$ の 1 個だけだから不適.

(2) $n = 3$ の時，G が可換群とすると $\mathbb{Z}/p^3\mathbb{Z}, \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, (\mathbb{Z}/p\mathbb{Z})^3$ のいずれかに同型．$\mathbb{Z}/p^3\mathbb{Z}$ の真部分群は $\langle p^2 \rangle, \langle p \rangle$ の 2 個だから不適．$\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ は $\langle (1,0) \rangle, \langle (p,0) \rangle, \langle (1,1) \rangle, \langle (p,1) \rangle$ を真部分群に持つから不適．$(\mathbb{Z}/p\mathbb{Z})^3$ は $\langle (1,y,0) \rangle, \langle (0,y,1) \rangle$ $(y \in \mathbb{Z}/p\mathbb{Z})$ を真部分群に持つから不適．よって G は非可換群であることが必要．G の中心を Z とおく．G は p 群だから $|Z| = p, p^2$ である．また G は非可換群ゆえ G/Z が巡回群でないことが必要なので，$|Z| = p, G/Z \cong (\mathbb{Z}/p\mathbb{Z})^2$ となる．上で見たように $(\mathbb{Z}/p\mathbb{Z})^2$ は位数 p の真部分群を $p+1$ 個持つから，G は真部分群を少なくとも $2(p+1)$ 個持つ．これは不適.

(3) $n = 4$ の時は数学系 1998 年度数学 I 問 5 と同様に $G \cong \mathbb{Z}/p^4\mathbb{Z}$.

以上から答えは，p を素数として

$$(\mathbb{Z}/2\mathbb{Z})^2, \qquad \mathbb{Z}/p^4\mathbb{Z}.$$

□

問 2

可換体 K 上の多元環（K-algebra）R について，$\mathrm{Aut}(R)$ は K 上の多元環としての自己同型群を表すものとする．x は K 上の変数として，次のことを示せ．

(1) $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2,K)$ に対して，写像 $x \mapsto \dfrac{ax+b}{cx+d}$ を対応させることによって，

$$\mathrm{Aut}(K(x)) \cong PGL(2,K) = GL(2,K)/K^{\times} I.$$

ここで $I \in GL(2,K)$ は単位行列である．

(2) S_3 を 3 次対称群とするとき

$$\mathrm{Aut}\left(K\left[x, \frac{1}{x(x-1)}\right]\right) \cong S_3.$$

解答. (1) $\Phi : GL(2,K) \to \mathrm{Aut}(K(x))$ を $\Phi(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right))(x) = \frac{ax+b}{cx+d}$ で定める．任意の $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), A' = \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right) \in GL(2,K)$ に対し

$$\begin{aligned} \Phi(AA')(x) &= \Phi\left(\begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix}\right)(x) = \frac{(aa'+bc')x + (ab'+bd')}{(ca'+dc')x + (cb'+dd')} \\ &= \frac{a(a'x+b') + b(c'x+d')}{c(a'x+b') + d(c'x+d')} = \frac{a\Phi(A')(x) + b}{c\Phi(A')(x) + d} = (\Phi(A) \circ \Phi(A'))(x) \end{aligned}$$

だから $\Phi(AA') = \Phi(A) \circ \Phi(A')$. よって Φ は準同型である．$\Phi(A)(x) = \mathrm{id}_K$ となるのは $a = d, b = c = 0$ の時だから $\mathrm{Ker}\,\Phi = K^{\times} I$. また $\mathrm{Aut}(K(x))$ の元は $x \mapsto \frac{ax+b}{cx+d}\,(ad - bc \neq 0)$ と書けるから Φ は全射である．よって準同型定理から示された．

(2) $R = K[x, \frac{1}{x(x-1)}]$ とおく．$R \subset K(x)$ だから，(1) より $\varphi \in \mathrm{Aut}(R)$ は $\varphi(x) = \frac{ax+b}{cx+d}\,(ad - bc \neq 0)$ とおける．$\varphi(x) \in R$ より $cx + d$ の根は（あるならば）$x = 0, 1$ のみ．$\varphi(x^{-1}) \in R$ だから $ax + b$ も同様．よって $\varphi(x)$ としてあり得るのは

$$ax, \quad a(x-1), \quad \frac{a}{x}, \quad \frac{a(x-1)}{x}, \quad \frac{a}{x-1}, \quad \frac{ax}{x-1}$$

の 6 個．それぞれについて $\varphi(\frac{1}{x-1})$ は

$$\frac{1}{ax-1}, \quad \frac{1}{a(x-1)-1}, \quad \frac{x}{a-x}, \quad \frac{x}{a(x-1)-x}, \quad \frac{x-1}{a-(x-1)}, \quad \frac{x-1}{ax-(x-1)}.$$

これが R に入ることと $a \neq 0$ より，a の値は順に $1, -1, 1, 1, -1, 1$. よって $\mathrm{Aut}(R)$ は

$$\varphi_1(x) = x, \quad \varphi_2(x) = 1 - x, \quad \varphi_3(x) = \frac{1}{x}, \quad \varphi_4(x) = \frac{x-1}{x}, \quad \varphi_5(x) = \frac{1}{1-x}, \quad \varphi_6(x) = \frac{x}{x-1}$$

の 6 個の元からなるから，$\mathrm{Aut}(R)$ は $\mathbb{Z}/6\mathbb{Z}$ または S_3 に同型．

$$\varphi_2(\varphi_3(x)) = 1 - \frac{1}{x} \neq \frac{1}{1-x} = \varphi_3(\varphi_2(x))$$

より $\mathrm{Aut}(R)$ は Abel 群ではないから $\mathrm{Aut}(R) \cong S_3$. □

1990 年度 (平成 2 年度)

問 1

有理数体 $\mathbb{Q}$ の代数拡大体 $K = \mathbb{Q}(\sqrt[6]{3} + \sqrt{-3})$ について，次の問に答えよ．

(1) K を含む最小の $\mathbb{Q}$ 上の Galois 拡大 L は K と一致するかどうか．

(2) L の $\mathbb{Q}$ 上の Galois 群を求めよ．

(3) L の部分体のうち，$\mathbb{Q}$ 上 6 次拡大であるものを全て求めよ．

解答. (1) $\alpha = 3^{1/6}, \zeta = e^{2\pi i/6}, \theta = \alpha + \sqrt{3}i$ とおき，$f(x)$ を θ の $\mathbb{Q}$ 上最小多項式とする．$(\theta - \sqrt{3}i)^6 = 3$ より $g(\theta) + \sqrt{3}ih(\theta) = 3$ となる $g(x), h(x) \in \mathbb{Q}[x]$ が存在する．

$$\begin{aligned} h(\theta) &= \frac{1}{\sqrt{3}i}\Big[6\theta(-\sqrt{3}i)^5 + 20\theta^3(-\sqrt{3}i)^3 + 6\theta^5(-\sqrt{3}i)\Big] \\ &= -6\theta(9 - 10\theta^2 + \theta^4) = -6\theta(1-\theta^2)(9-\theta^2) \neq 0 \end{aligned}$$

より $\sqrt{3}i = (3 - g(\theta))/h(\theta) \in K, \alpha = \theta - \sqrt{3}i \in K$ である．これより $\mathbb{Q}(\alpha, \zeta) \subset K$ であるが，逆の包含は明らかなので $K = \mathbb{Q}(\alpha, \zeta)$. この時 $K/\mathbb{Q}$ は Galois 拡大なので $L = K$.

(2) $[L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 6 = 12$ である．$\sigma, \tau \in \mathrm{Gal}(L/\mathbb{Q})$ を

$$\sigma : (\alpha, \zeta) \mapsto (\alpha\zeta, \zeta), \qquad \tau : (\alpha, \zeta) \mapsto (\alpha, \zeta^{-1})$$

で定めると $\sigma^6 = \tau^2 = \mathrm{id}_L$. また

$$\tau\sigma\tau(\alpha) = \tau\sigma(\alpha) = \tau(\alpha\zeta) = \alpha\zeta^{-1}, \quad \tau\sigma\tau(\zeta) = \tau\alpha(\zeta^{-1}) = \tau(\zeta^{-1}) = \zeta$$

より $\tau\sigma\tau = \sigma^{-1}$ だから，$\langle \sigma, \tau \rangle \cong D_6$. よって位数の比較から，これが $\mathrm{Gal}(L/\mathbb{Q})$ である．

(3) 求める部分体に対応する $\mathrm{Gal}(L/\mathbb{Q})$ の部分群は位数 2 である．1993 年度問 1 と同様にして，それは $\langle \sigma^j\tau \rangle$ $(j = 0, 1, \ldots, 5)$ と $\langle \sigma^3 \rangle$ の 7 個．

• $\langle \sigma^3 \rangle : \mathbb{Q}(\alpha^2, \zeta) \subset L^{\langle \sigma^3 \rangle}$ であり，$[L : \mathbb{Q}]$ の計算と同様に $[\mathbb{Q}(\alpha^2, \zeta) : \mathbb{Q}] = 6$ だから $\mathbb{Q}(\alpha^2, \zeta) = L^{\langle \sigma^3 \rangle}$.

• $\langle \sigma^{2j}\tau \rangle$ $(j = 0, 1, 2) : \mathbb{Q}(\alpha\zeta^j) \subset L^{\langle \sigma^{2j}\tau \rangle}$ である．$\alpha\zeta^j$ を根に持つ $x^6 - 3 \in \mathbb{Q}[x]$ は Eisenstein の既約判定法 $(p = 3)$ より $\mathbb{Q}$ 上既約だから $[\mathbb{Q}(\alpha\zeta^j) : \mathbb{Q}] = 6$. よって $L^{\langle \sigma^{2j}\tau \rangle} = \mathbb{Q}(\alpha\zeta^j)$.

• $\langle \sigma^3\tau \rangle : \mathbb{Q}(\alpha(\zeta - \zeta^{-1})) \subset L^{\langle \sigma^3\tau \rangle}$ である．$(\alpha(\zeta - \zeta^{-1}))^6 = (\alpha\sqrt{3}i)^6 = -3^4$ であり，$x^6 + 81 \in \mathbb{Q}[x]$ は $\mathbb{Q}$ 上既約（後で示す）だから上と同様に $L^{\langle \sigma^3\tau \rangle} = \mathbb{Q}(\alpha(\zeta - \zeta^{-1}))$.

• $\langle \sigma^{\pm 1}\tau \rangle : \mathbb{Q}(\alpha(1+\zeta^{\pm 1})) \subset L^{\langle \sigma^{\pm 1}\tau \rangle}$ である．$1 + \zeta^{\pm 1} = \sqrt{3}(\frac{\sqrt{3}}{2} \pm \frac{1}{2}i) = \sqrt{3}e^{\pm \pi i/6}$ より $(\alpha(1+\zeta^{\pm 1}))^6 = -3^4$ であるから，上と同様にして $L^{\langle \sigma^{\pm 1}\tau \rangle} = \mathbb{Q}(\alpha(1 + \zeta^{\pm 1}))$.

以上から答えは

$$\mathbb{Q}(\alpha^2, \zeta), \quad \mathbb{Q}(\alpha\zeta^j)\,(j = 0, 1, 2), \quad \mathbb{Q}(\alpha(\zeta - \zeta^{-1})), \quad \mathbb{Q}(\alpha(1 + \zeta^{\pm 1})).$$

• $x^6 + 81 \in \mathbb{Q}[x]$ の既約性：$x^6 + 81$ の根は $3^{2/3}\xi^{2j+1}$ $(\xi = e^{\pi i/6}, j = 0, 1, \ldots, 5)$ であり，これらは実数でないから，既約因子は $p_j(x) := (x - 3^{2/3}\xi^{2j+1})(x - 3^{2/3}\xi^{6-(2j+1)})$ で割り切れる．今定数でない $f, g \in \mathbb{Q}[x]$ が存在して $x^6 + 81 = f(x)g(x)$ と書けたとすると，$p_0(x), p_1(x), p_2(x)$ のうち少なくとも 1 つは f または g に等しい．ところがこれらは $\mathbb{Q}[x]$ の元でないから矛盾． □

問 2

多項式 $f(X) \in \mathbb{Q}[X]$ が与えられたとする．任意の代数的整数 a に対して，$f(a)$ が代数的整数になるならば，$f(X) \in \mathbb{Z}[X]$ となることを示せ．ここで，$\mathbb{Q}$ は有理数体，$\mathbb{Z}$ は有理整数環を表す．

解答. 代数的整数の集合を $\overline{\mathbb{Z}}$ とおく．$f(X) = a_0 + a_1 X + \cdots + a_n X^n$ とする．素数 $p \geq n+2$ を取り $\zeta = e^{2\pi i/p}$ とおくと

$$a_0 + a_1\zeta + \cdots + a_n\zeta^n = f(\zeta) \in \mathbb{Q}(\zeta) \cap \overline{\mathbb{Z}} = \mathbb{Z}[\zeta]$$

である．$1, \zeta, \ldots, \zeta^{p-2}$ は $\mathbb{Z}[\zeta]$ の $\mathbb{Z}$ 上の基底なので，a_j たちは全て整数である． □

1989 年度 (平成元年度)

問 1

単位元を持つ可換環 R に関する次の命題 1, 2, 3 のおのおのについて，次の問に答えよ．

(1) 命題が正しいかどうか，理由をつけて答えよ．

(2) 命題が正しくない場合には，R に適当な条件をつけ加えて正しい命題にして，それを証明せよ．

命題 1. $a_1, \ldots, a_n \in R, f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ に対し，$\{c \in R;\, f(c) = 0\}$ の元数は n 以下である．

命題 2. $a \in R$ が R を含むある可換環（単位元は R と共通）の中に逆元 a^{-1} を持っていて，さらに $R[a^{-1}]$ が R-加群として有限生成であれば $a^{-1} \in R$.

命題 3. R 上の 1 変数多項式環 $R[x]$ において逆元を持つ元は R の元に限る．

解答. (1) • 命題 1 : 正しくない．$R = \mathbb{Z}/16\mathbb{Z}$ とすると $f(x) = x^2$ の根は $x = 0, 4, 8, 12$ の 4 個．

• 命題 2 : 正しい．仮定から a^{-1} は R 上整だから，$a^{-d} + c_{d-1}a^{-(d-1)} + \cdots + c_1 a^{-1} + c_0 = 0$ となる $c_j \in R$ が存在する．この時 $a^{-1} = -(c_{d-1} + \cdots + c_1 a^{d-2} + c_0 a^{d-1}) \in R$.

• 命題 3 : 正しくない．$R = \mathbb{Z}/4\mathbb{Z}$ とすると $(1 + 2x)^2 = 1$ より $1 + 2x$ は逆元を持つ．

(2) • 命題 1 : R が整域である時正しいことを $\deg f$ の帰納法で示す．$\deg f = 1$ の時は根は $x = -a_1$ のみだから正しい．ある n に対し $\deg f < n$ の時正しいとする．$\deg f = n$ なる $f \in R[x]$ を任意に取る．f が R において根を持たないときは正しい．f が R において根 $x = a$ を持つ時，$f(x) = (x - a)g(x)$ となる monic な $(n-1)$ 次式 $g \in R[x]$ が存在する．帰納法の仮定より g の R における根の数は $n - 1$ 以下だから，f の R における根の数は $1 + (n - 1) = n$ 以下である．よって示された．

• 命題 3 : R が整域である時正しいことを示す．$a_0 + a_1 x + \cdots + a_d x^d \in R[x]\,(d \geq 1, a_d \neq 0)$ が逆元 $b_0 + b_1 x + \cdots + b_{d'} x^{d'}\,(b_{d'} \neq 0)$ を持つとすると，積を取って最高次係数から $a_d b_{d'} = 0$ となるが，仮定から矛盾． □

1980 年度 (昭和 55 年度)

問 1

有理整数環 $\mathbb{Z}$ 上の 1 変数多項式環 $\mathbb{Z}[X]$ を考える.

(i) $\mathbb{Z}[X]$ の任意の素イデアル $\mathfrak{p} \neq 0$ は，$\mathbb{Z}[X]$ の既約元を含みかつ有限個の既約元によって生成されることを示せ.

(ii) $\mathbb{Z}[X]$ の任意の素イデアル $\mathfrak{p}$ は高々 2 個の元で生成されることを示せ.

(iii) $\mathbb{Z}[X]$ のイデアルで 2 個以下の元では生成されない例を示せ.

解答. (i),(ii) 東大数理 1999 年度専門問 2 の解答を参照.

(iii) $\mathfrak{m} = (2, x), I = \mathfrak{m}^2 = (4, 2x, x^2)$ とおく．$\mathbb{Z}[X]/\mathfrak{m} = \mathbb{F}_2$ は体であるから，$\mathfrak{m}$ は $\mathbb{Z}[X]$ の極大イデアルである．よって $I/\mathfrak{m}I = I/\mathfrak{m}^3$ は $\mathbb{F}_2$ 上のベクトル空間である．ここで $4, 2x, x^2 \in I/\mathfrak{m}I$ は $\mathbb{F}_2$ 上一次独立であることを示す.

$$4a + 2bx + cx^2 \in \mathfrak{m}^3 = (8, 4x, 2x^2, x^3) \quad (a, b, c \in \mathbb{F}_2)$$

とすると $4a + 2bx + cx^2 \in (8, 4x, 2x^2)$ より $4a + 2bx + cx^2$ の係数は全て偶数なので $c = 0$. 定数項は 8 の倍数なので $a = 0$. この時 $2bx \in (8, 4x)$ となるから，$2b$ は 4 の倍数ゆえ $b = 0$. よって示された．これより $\dim_{\mathbb{F}_2} I/\mathfrak{m}I \geq 3$ だから，I の生成元の個数も 3 以上（従って丁度 3 個）である． □

問 3

次の命題は正しいか.

(i) $\mathbb{Q}$ に 1 の原始 n 乗根 $\zeta\,(n \geq 2)$ を添加した体 $\mathbb{Q}(\zeta)$ は $\mathbb{Q}$ 上の巡回拡大体である.

(ii) $f(X)$ が $\mathbb{Z}[X]$ で既約な多項式であれば，適当な素数 p を取れば，$f(X) \bmod p$ は $(\mathbb{Z}/p\mathbb{Z})[X]$ の多項式として既約である.

解答. どちらも正しくない．東大数理専門（代数）実施年度不明 4 問 4 を参照. □

1979 年度 (昭和 54 年度)

問 1

位数 867 の非可換群の同型類はいくつあるか．ただし $867 = 3 \times 17^2$.

解答. 群を G とおく．数理研平成 23 年度専門問 1 と同様にして，位数 17^2 の G の正規部分群 H と $K \cong \mathbb{Z}/3\mathbb{Z}$, 準同型 $\sigma : K \to \mathrm{Aut}(H)$ があって $G \cong H \rtimes_\sigma K$ となる．$|H|$ は素数の平方だから，H は $\mathbb{Z}/17^2\mathbb{Z}, (\mathbb{Z}/17\mathbb{Z})^2$ のどちらかに同型である．$H \cong \mathbb{Z}/17^2\mathbb{Z}$ とすると，$\mathrm{Aut}(H) \cong (\mathbb{Z}/17^2\mathbb{Z})^\times$ より $|\mathrm{Aut}(H)| = 17^2 - 17 = 17 \cdot 16$ は 3 と互いに素だから $\sigma(g) = \mathrm{id}_H\, (g \in K)$ である．この時 $G = H \times K$ は Abel 群なので不適．よって $H \cong (\mathbb{Z}/17\mathbb{Z})^2 = \mathbb{F}_{17}^2$ だから，$\mathrm{Aut}(H)$ は $GL_2(\mathbb{F}_{17})$ と同一視できる．そこで $GL_2(\mathbb{F}_{17})$ の位数 3 の元 A を求める．$A^3 = I$ より A の固有値は $1, \omega, \omega^2$ のいずれかである．ただし $\omega \in \mathbb{F}_{17^2}$ は 1 の原始 3 乗根．もし 1 を固有値に持つと，$\mathrm{tr}\, A \in \mathbb{F}_{17}$ より固有値は共に 1 となるが，$(3, 17) = 1$ より A は I に共役，すなわち $A = I$ となって不適．よって A の固有値は ω, ω^2 だから，A は $\mathrm{diag}(\omega, \omega^2)$ に共役である．従って σ は共役を除いて一意だから，G の同型類は 1 個． □

1977 年度 (昭和 52 年度)

問 1

体 k およびその拡大体 K の組 (k, K) で次の条件 $(*)$ を満たすものはどんなものか？

$(*)$ K/k は有限次ガロア拡大であり，そのガロア群 $\mathrm{Gal}(K/k)$ は巡回群である．さらに，K の k 上のある生成元 $\alpha\,(K = k(\alpha))$ と $\mathrm{Gal}(K/k)$ のある生成元 σ について

$$\sigma(\alpha) = m\alpha + n \cdot 1_k \qquad (m, n \in \mathbb{Z})$$

が成り立つ．ただし 1_k は k の乗法の単位元である．

解答. $\mathrm{Gal}(K/k) \cong \mathbb{Z}/N\mathbb{Z}\,(N \geq 1)$ とおける．帰納的に $\sigma^j(\alpha) = m^j\alpha + n(1 + m + \cdots + m^{j-1})$ となるから，$\sigma^N(\alpha) = \alpha$ より

$$m^N = 1, \qquad n(1 + m + \cdots + m^{N-1}) = 0.$$

k の標数が 0 の時は第 1 式より $m = 1$, 第 2 式より $n = 0$ だから $\sigma(\alpha) = \alpha$. よって $\sigma = \mathrm{id}_K$ となるから $K = k$ である．以下 k の標数を $p > 0$ とする．

• $m = 1$ の時：$nN = 0$ である．$p \mid n$ なら k の標数が 0 の時と同様に $K = k$ となるから $p \nmid n$ とする．この時 $p \mid N$. 一方 K/k が N 次 Galois 拡大であることから，α の k 上最小多項式 $f(T)$ は N 次で k-共役元は $\sigma^j(\alpha) = \alpha + jn\,(j = 0, 1, \ldots, N-1)$ である．α が k 上分離的であることから任意の $0 \leq i < j \leq N-1$ に対し $\alpha + in \neq \alpha + jn$, すなわち $i \neq j$ なので $N \leq p$ である．以上から $N = p$ なので

$$\begin{aligned} f(T) &= \prod_{j=0}^{p-1}(T - (\alpha + jn)) = \prod_{j=0}^{p-1}(T - (\alpha + j)) \\ &= (T - \alpha)^p - (T - \alpha) = T^p - T - (\alpha^p - \alpha). \end{aligned}$$

ただし 2 番目の等号は $(n, p) = 1$ による．$f(T) \in k[T]$ より $c := \alpha^p - \alpha \in k$ が必要．逆に α が多項式 $f(T) = T^p - T - c \in k[T]$ の根であれば，$f(T)$ は 1 次式の積に分解するか k 上既約である．前者の時は $K = k$ であり，後者の時は K/k は巡回 Artin-Schreier 拡大だから $(*)$ を満たす.

• $m \neq 1$ の時：$k^\times$ における m の位数を r とおくと，

$$\sigma^r(\alpha) = m^r\alpha + n\frac{m^r - 1}{m - 1} = \alpha$$

より $\sigma^r = \mathrm{id}_K$. また $\sigma^j(\alpha)$ の α の係数から $\sigma^j \neq \mathrm{id}_K\,(1 \leq j \leq r-1)$ なので $N = r$ である．$r \mid (p-1)$ より $p \nmid r$ であり，K は 1 の原始 r 乗根 m を含むので，K/k は巡回 Kummer 拡大である．すなわち $a \in k$ があって，K は既約多項式 $T^r - a$ の最小分解体 $k(a^{1/r})$ である．

以上から答えは

(1) $K = k$ または，

(2) k の標数が $p > 0$ で，K は $T^p - T - c \in k[T]$ の最小分解体，または

(3) k の標数が $p > 0$ で，K は既約多項式 $T^r - a \in k[T]$ の最小分解体（ただし $r \mid (p-1)$）.

□

問 3

k は標数が 2 でない代数的閉体とする．k 上の 2 変数多項式環 $k[x,y]$ を単項イデアル (x^2+y^2-1) で割った剰余環を R とする：$R = k[x,y]/(x^2+y^2-1)$. このとき，

(i) R は k 上の 1 変数有理関数体のある部分環に同型であることを示せ．

(ii) R の環としての自己同型で k 上では恒等写像となるもの全体の作る群 $\mathrm{Aut}_k R$ の構造を記述せよ．

解答． (i) 仮定から $i := \sqrt{-1}, 1/2 \in k$ なので，$X = x+iy, Y = x-iy$ とおくと $x = (X+Y)/2, y = (X-Y)/2i$ である．よって

$$R \cong k\left[\frac{X+Y}{2}, \frac{X-Y}{2i}\right]/(XY-1) = k[X,Y]/(XY-1) \cong k[X,X^{-1}].$$

(ii) $R' = k[X,X^{-1}]$ とおく．$\varphi \in \mathrm{Aut}_k R'$ は $\varphi(X) = p(X)/q(X)\,(p,q \in k[X])$ とおける．$p(X)/q(X) \in R'$ より $q(X) = X^j\,(j \in \mathbb{N})$ であることが必要．また $X^j/p(X) = \varphi(X^{-1}) \in R'$ より $p(X) = cX^k\,(k \in \mathbb{N})$ であることが必要．よって $\varphi(X) = cX^j\,(j \in \mathbb{Z})$ とおけるが，$j \neq \pm 1$ なら $\varphi(R') = k[X^j, X^{-j}] \subsetneq R'$ で同型にならないから $j = \pm 1$ が必要．以上から $\varphi(X) = cX^{\pm 1}$ とおけるが，これは明らかに $\mathrm{Aut}_k R'$ の元になっている．従って

$$\mathrm{Aut}_k R \cong \mathrm{Aut}_k R' = \{\varphi(X) = cX^{\pm 1}\,;\, c \in k^\times\} \overset{(*)}{=} k^\times \times \mathbb{Z}/2\mathbb{Z}$$

である．ただし $(*)$ は集合としての等号である．$\varphi(X) = c_1X^{r_1}, \psi(X) = c_2X^{r_2} \in \mathrm{Aut}_k R'$ に対し $\varphi(\psi(X)) = c_1c_2^{r_1}X^{r_1r_2}$ だから，$k^\times \times \mathbb{Z}/2\mathbb{Z}$ の積は $(c_1,r_1)\cdot(c_2,r_2) = (c_1c_2^{r_1}, r_1r_2)$ で与えられる．すなわち準同型 $\sigma : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(k^\times)$ を $1 \mapsto (c \mapsto c^{-1})$ で定めると

$$\mathrm{Aut}_k R \cong k^\times \rtimes_\sigma \mathbb{Z}/2\mathbb{Z}.$$

□

1976 年度 (昭和 51 年度)

問 2

k を可換体とする．

(i) k 上の 3 変数多項式環 $k[x,y,z]$ のイデアル

$$(z-xy)k[x,y,z]+(y^2-xz)k[x,y,z]$$

は素イデアルか否か，理由をつけて答えよ．

(ii) n を正の奇数，$k[x,y]$ を k 上の 2 変数多項式環として，

$$R_n=k[x,y]/(x^2-y^n)k[x,y]$$

とおく．$n\neq 1$ のとき，R_n は整閉でない整域であることを示せ．さらに，R_n の（商体の中での）整閉包を求めよ．

解答. (i) $I=(z-xy,y^2-xz)$ とおく．$y,y-x^2\notin I$ を示す．$y=(z-xy)f+(y^2-xz)g\,(f,g\in I)$ とすると z^0 の係数から $y=-xyf(x,y,0)+y^2g(x,y,0)$. この両辺を y で割れば，$k[x,y]$ のイデアル (x,y) は 1 を含むことがわかる．従って $(x,y)=k[x,y]$ となるが，これは矛盾．$y-x^2=(z-xy)f+(y^2-xz)g$ とすると z^0 の係数から $y-x^2=-xyf(x,y,0)+y^2g(x,y,0)$. よって $y-y^2g(x,y,0)$ は x で割り切れることになるが，y^1 の係数からこれは 0 でない多項式なので矛盾．以上から $y,y-x^2$ は $R:=k[x,y,z]/I$ の元として 0 でない．一方 $y(y-x^2)=(y^2-xz)+x(z-xy)\in I$ だから，$y(y-x^2)$ は R の元として 0 である．従って R は整域ではないから，I は素イデアルではない.[1]

(ii) R_n が整域であることは数理研平成 20 年度専門問 3(1) と同様．またその証明から $R_n\cong A:=k[t^2,t^n]$ である．A の商体を $Q(A)$ と書き，$n=2m+1$ とおく．$t=t^n/(t^2)^m\in Q(A)$ であり，t は monic な多項式 $T^2-t^2\in A[T]$ の根であるが，$t\notin A$ だから A は整閉ではない．従って R_n も整閉ではない．

A の商体における整閉包を $\overline{A}$ とおく．$f/g\in\overline{A}$ とし，f,g は A の代数閉包において共通因子を持たないとする．この時 f/g はある $T^n+a_{n-1}T^{n-1}+\cdots+a_1T+a_0\in A[T]$ の根であるから $f^n=-(a_{n-1}f^{n-1}g+\cdots+a_1fg^{n-1}+a_0g^n)$. $\deg g\geq 1$ とすると，この右辺は g の根において 0 だから f もそう．これは f,g が共通因子を持たないことに反する．よって $g\in k$ が必要だから $\overline{A}\subset k[t]$. 上で見たように t は A 上整だから，この包含は逆も成り立つ．R_n と A の間の同型は $x\mapsto t^n,y\mapsto t^2$ で与えられたから，R_n の商体における整閉包は

$$k\left[\frac{x}{y^{(n-1)/2}}\right].$$

□

[1] 環準同型 $\Phi:k[x,y,z]\to k[t]$ を $x\mapsto t,y\mapsto t^2,z\mapsto t^3$ で定める．$I\subset\mathrm{Ker}\,\Phi$ である．逆の包含を示そうとすると，$y^2-x^2y=(y^2-xz)+x(z-xy)\in I$ より $k[x,y,z]$ の元は $f=\sum(a_i+b_iy)x^i+g\,(g\in I)$ と書ける．これが $\mathrm{Ker}\,\Phi$ の元とすると，Φ の像から係数を求めて $a_0=a_1=0,a_i=-b_{i-2}$ となる．これから $\sum(a_i+b_iy)x^i=\sum b_i(y-x^2)x^i$ となるから $\mathrm{Ker}\,\Phi\subset I$ は言えない．実際 $y-x^2\in\mathrm{Ker}\,\Phi$ だが，上で示したようにこれは I の元ではない．