数理解析研究所 院試過去問解答
専門科目 (代数)

nabla *

2024 年 5 月 13 日

目 次

*Twitter:@nabla_delta

はじめに

数理研の院試問題の解答です．一部の問題には図がありましたが，入れるのがめんどくさいので省略してあります．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．

平成 25 年度 (2012 年 8 月実施)

問 1

p と ℓ を相異なる素数とする．複素数体 $\mathbb{C}$ 内の部分体 F, K, L を次式で定義する．

$$F = \mathbb{Q}(p^{1/\ell}), \quad K = \mathbb{Q}(e^{2\pi i/\ell}), \quad L = F \cdot K = \mathbb{Q}(p^{1/\ell}, e^{2\pi i/\ell}).$$

このとき，部分体の拡大次数について，$[F : \mathbb{Q}] = [L : K] = \ell$ を証明せよ．

解答. $f(X) = X^\ell - p \in \mathbb{Q}[X]$ は Eisenstein の既約判定法により $\mathbb{Q}$ 上既約．これと $f(p^{1/\ell}) = 0$ より f は $p^{1/\ell}$ の $\mathbb{Q}$ 上最小多項式である．よって $[F : \mathbb{Q}] = \deg f = \ell$. また $[K : \mathbb{Q}] = \varphi(\ell) = \ell - 1$ だから

$$[L : K](\ell - 1) = [L : K][K : \mathbb{Q}] = [L : \mathbb{Q}] = [L : F][F : \mathbb{Q}] = [L : F]\ell.$$

ℓ は素数だから $[L : K]$ は ℓ の倍数である．一方 $f \in K[X]$ は $p^{1/\ell}$ を根に持つので $[L : K] \leq \deg f = \ell$. 従って $[L : K] = \ell$. □

問 2

環 $R = \mathbb{C}[x, y, z]/(x^2 - yz)$ とそのイデアル $I = (x, y)$ を考える．このとき，次の (i), (ii), (iii) を証明せよ．

(i) R は整域である．

(ii) I は単項イデアルではない．

(iii) I と $\mathrm{Hom}_R(I, R)$ は R 加群として同型である．

解答. □

問 3

p を素数とする．有限群 G に対して，その位数が $p^n\,(n=0,1,2,\dots)$ となるとき，G を p 群という．また，$\mathrm{Aut}(G)$ を G の自己同型写像全体のなす群とする．このとき，次の (i), (ii), (iii) に解答せよ．

(i) 位数が 1 より大きい p 群は位数が p の元を持つことを証明せよ．

(ii) 位数が p より大きい可換な p 群 G に対して，$\mathrm{Aut}(G)$ は位数が p の元を持つことを証明せよ．

(iii) p 群 G であって，$\mathrm{Aut}(G)$ が位数 p の元を持たないもの（の同型類）をすべて求めよ．

解答. (i) Sylow の定理より G は位数 p の部分群を持つ．それは巡回群だから，生成元は位数 p である．

(ii) $|G|=p^n\,(n\geq 2)$ とする．有限生成 Abel 群の基本定理より $\mathrm{Aut}(G)\cong\mathrm{Aut}(\otimes_{j=1}^k(\mathbb{Z}/p^{e_j}\mathbb{Z}))$ である．(ただし $e_1+\cdots+e_k=n$.)

• $n>k$ の時：$|\mathrm{Aut}(\mathbb{Z}/p^{e_j}\mathbb{Z})|=|(\mathbb{Z}/p^{e_j}\mathbb{Z})^\times|=p^{e_j-1}(p-1)$ であるから，$\mathrm{Aut}(\otimes_{j=1}^k(\mathbb{Z}/p^{e_j}\mathbb{Z}))$ の部分群 $\otimes_{j=1}^k\mathrm{Aut}(\mathbb{Z}/p^{e_j}\mathbb{Z})$ の位数は $\prod_{j=1}^k p^{e_j-1}(p-1)=p^{n-k}(p-1)^k$. よって Sylow の定理より位数 p^{n-k} の部分群が存在するので，(i) より位数 p の元が存在する．

• $n=k$ の時：$\mathrm{Aut}(G)\cong\mathrm{Aut}(\mathbb{F}_p^n)$ である．$\mathrm{diag}(J(1,2),I_{n-2})\in GL_n(\mathbb{F}_p)$ の位数は p だから，$\mathrm{Aut}(\mathbb{F}_p^n)$ の元 $(x_1,\dots,x_n)\mapsto(x_1,x_1+x_2,x_3,\dots,x_n)$ の位数も p である．[1]

(iii) • $|G|=1$ の時：$\mathrm{Aut}(G)=\{1\}$ は位数 p の元を持たない．

• $|G|=p$ の時：$G\cong\mathbb{Z}/p\mathbb{Z}$ だから $\mathrm{Aut}(G)\cong(\mathbb{Z}/p\mathbb{Z})^\times=\mathbb{Z}/(p-1)\mathbb{Z}$ は位数 p の元を持たない．

• $|G|=p^n\,(n\geq 2)$ の時：G が Abel 群なら (ii) より不適．よって G は非 Abel 群．ここで $g\in G$ に対し $\varphi_g:G\to G$ を $\varphi_g(x)=gxg^{-1}$ で定め，$i:G\to\mathrm{Aut}(G)$ を $i(g)=\varphi_g$ で定める．この時

$$\mathrm{Ker}\,i=\{g\in G;\,\varphi_g=\mathrm{id}_G\}=\{g\in G;\,\forall x\in G, gxg^{-1}=x\}=Z(G)$$

なので $G/Z(G)\cong\mathrm{Im}\,i$ である．G は p 群だから $Z(G)$ も p 群で，従って $\mathrm{Im}\,i$ も p 群である．さらに $Z(G)\neq G$ だから $|\mathrm{Im}\,i|=|G/Z(G)|>1$. 従って (i) より $\mathrm{Im}\,i(\subset\mathrm{Aut}(G))$ は位数 p の元を持つ．
以上から $G\cong\{1\},\mathbb{Z}/p\mathbb{Z}$. □

[1] $SL_n(\mathbb{F}_p)\subset\mathrm{Aut}(\mathbb{F}_p^n)$ とみなせる．行列式を取る写像により $GL_n(\mathbb{F}_p)/SL_n(\mathbb{F}_p)\cong\mathbb{F}_p^\times$ だから，$SL_n(\mathbb{F}_p)$ の位数は平成 22 年度問 2 と同様に計算できる．これと (i) を用いることで示すこともできる．

平成 24 年度 (2011 年 8 月実施)

問 1

K は有理数体 $\mathbb{Q}$ の有限次拡大とする．K の部分環 R と整数 $N \geq 1$ に対して，K 内で R と $\frac{1}{N}$ で生成される部分環を $R[1/N]$ と表す．また，K 成分の n 次正則行列全体の成す群を $GL_n(K)$ と表す．

(i) K の部分環 R は $\mathbb{Z}$ 上有限生成な環であると仮定する．このとき，$R[1/N]$ が $\mathbb{Z}[1/N]$ 加群として有限生成かつ自由となるような整数 $N \geq 1$ が存在することを示せ．

(ii) $G \subseteq GL_n(K)$ は有限生成な部分群とし，$g \in G$ は単位行列 I と異なる元とする．このとき，$g \notin H$ となるような指数有限な部分群 $H \subseteq G$ が存在することを示せ．

解答. (i) $R = \mathbb{Z}[a_1, \ldots, a_n]$ とする．K は $\mathbb{Q}$ の有限次拡大だから，$c_{i,d_i} a_i^{d_i} + \cdots + c_{i,1} a_i + c_{i,0} = 0$ となる $c_{i,j} \in \mathbb{Z}\,(c_{i,d_i} > 0)$ が存在する．よって $N = c_{1,d_1} \cdots c_{n,d_n}$ とおくと

$$a_i^{d_i} = \frac{1}{N}(c'_{i,d_i-1} a_i^{d_i-1} + \cdots + c'_{i,0})$$

となる $c'_{i,j} \in \mathbb{Z}$ が存在する．従って a_i は $\mathbb{Z}[1/N]$ 上整だから，$R[1/N] = \mathbb{Z}[1/N][a_1, \ldots, a_n]$ は $\mathbb{Z}[1/N]$ 上有限生成．これが自由であることは明らか．

(ii) G の生成元の成分，その行列式とその逆数で生成される $\mathbb{Z}$ 上の環を R とする．$G \subset GL_n(R)$ であるとして良い．$g - I$ の 0 でない成分 x を任意に取る．$x \notin \sqrt{0} = \bigcap_{P \in \operatorname{Spec} R} P$ だから，$x \notin P$ となる R の素イデアル P が存在する．この時 $\mathbb{Z}$ のイデアル $P \cap \mathbb{Z}$ は $\{0\}$ でない．実際これが $\{0\}$ であるとすると，$t \in P$ に対し $a_n t^n + \cdots + a_1 t + a_0 = 0$ となる $a_0, \ldots, a_n \in \mathbb{Z}, a_0 \neq 0$ が存在する．ところが $-a_0 = a_n t^n + \cdots + a_1 t \in P$ より $a_0 \in P \cap \mathbb{Z} = \{0\}$ となって矛盾．これより $P \cap \mathbb{Z} = p\mathbb{Z}$ となる素数 p が存在する．従って R/P は有限整域なので有限体である．今 $\phi : GL_n(R) \to GL_n(R/P)$ を成分毎の自然な射影とすると，P の取り方から $g \notin \operatorname{Ker} \phi$. また準同型定理より

$$[GL_n(R) : \operatorname{Ker} \phi] = |\operatorname{Im} \phi| = |GL_n(R/P)| < \infty$$

なので，$H = \operatorname{Ker} \phi$ は条件を満たす．

(補足) (ii) の性質は Residual finite (Residually finite) と呼ばれ，$GL_n(\mathbb{C})$ に対するものは Selberg's Lemma (Malcev-Selberg Theorem) と呼ばれるらしい.[2] また $P \cap \mathbb{Z} \neq 0$ の一般化が 2003 年度 (平成 15 年度) 数学系数学 II 問 2 に出題されている． □

[2] https://392c.wordpress.com/2009/01/26/3-residual-finiteness-from-alan-reid/, https://www.e-periodica.ch/digbib/view?pid=ens-001:1987:33::94#402 を参照．(ii) の証明も最初の URL の Examples (2) による．2 番目の URL にある証明が (i) を用いるもの？(詳しく見てない)

問 2

複素数体 $\mathbb{C}$ を部分環として含む局所環 R は，積写像 $\mathbb{C}\times R\to R$ によって複素ベクトル空間となる．そのような環 R のうち，複素ベクトル空間としての次元が 5 であるものを，全て決定したい．

(i) $\mathfrak{m}$ を R の極大イデアルとし，$d=\dim_{\mathbb{C}}\mathfrak{m}/\mathfrak{m}^2$ とおく．$1\le d\le 4$ を示せ．

(ii) $d=1$ または 4 であるような R を，同型を除いて全て決定せよ．

(iii) $d=3$ であるような R を，同型を除いて全て決定せよ．

(iv) $d=2$ であるような R を，同型を除いて全て決定せよ．

解答. (i) $\mathbb{C}\subset R^\times$ より $\mathfrak{m}=R\setminus R^\times\neq R$ なので $d\le\dim_{\mathbb{C}}\mathfrak{m}<\dim_{\mathbb{C}}R=5$. また $d=0$ とすると $\mathfrak{m}=\mathfrak{m}^2$ であるから，中山の補題より $\mathfrak{m}=0$. よって $R^\times=R$ だから R は体となるが，この時 $R=\mathfrak{m}=0$ となり矛盾．

(ii) $\mathbb{C}\subset R$ だから，R の $\mathbb{C}$ ベクトル空間としての基底は $1,a_1,\dots,a_4$ とおける．全射準同型 $\mathbb{C}[x_1,\dots,x_4]\to\mathbb{C}[a_1,\dots,a_4],x_i\mapsto a_i$ の核を I とおくと，準同型定理より $\mathbb{C}[x_1,\dots,x_4]/I\cong R$ である．また $\mathbb{C}\cap I=\emptyset$ であるから $(\mathbb{C}[x_1,\dots,x_4]/I)/((x_1,\dots,x_4)/I)=\mathbb{C}/I\cong\mathbb{C}$ は体．よって $\mathfrak{m}=(x_1,\dots,x_4)/I$ である．この時 $\mathfrak{m}/\mathfrak{m}^2\cong(x_1,\dots,x_4)/(x_1,\dots,x_4)^2$ の次元が d であるから，$x_{d+1},\dots,x_4$ は $x_1,\dots,x_d$ の単項式であるとして良い．従って $R\cong\mathbb{C}[x_1,\dots,x_d]/I$. 以下 $x_1=x,x_2=y,x_3=z,x_4=w$ とおく．

• $d=4$ の場合：x,y,z,w は $\mathbb{C}$ 上一次独立だから

$$\begin{aligned}R&\cong\mathbb{C}[x,y,z,w]/(x^2,y^2,z^2,w^2,xy,xz,xw,yz,yw,zw)\\&=\mathbb{C}[x,y,z,w]/(x,y,z,w)^2.\end{aligned}$$

• $d=1$ の場合：$I=(f)\,(f\in\mathbb{C}[x])$ とおけて $\deg f=\dim_{\mathbb{C}}R=5$. 今 f が $x-a,x-b\,(a\neq b)$ で割り切れるとすると，$(x-a),(x-b)$ はともに R の極大イデアルになって矛盾．よって

$$R\cong\mathbb{C}[x]/((x-a)^5)\cong\mathbb{C}[x]/(x^5).$$

(iii) (ii) の議論から R の $\mathbb{C}$ ベクトル空間としての基底としてありうるのは $\{1,x,y,z,x^2\},\{1,x,y,z,xy\}$. それぞれの場合の R を R_1,R_2 とおき，環準同型 $\varphi:R_1\to R_2$ を $x\mapsto x+y,y\mapsto y,z\mapsto z$ で定義すると，$\varphi(x^2)=(x+y)^2=2xy$ だから φ は全射．また $c_1+c_2x+c_3y+c_4z+c_5x^2\in\operatorname{Ker}\varphi$ とすると，$c_1+c_2(x+y)+c_3y+c_4z+2c_5xy=0$ から $c_1=\cdots=c_5=0$ なので φ は単射．よって $R_1\cong R_2$ なので

$$R\cong\mathbb{C}[x,y,z]/(x^3,y^2,z^2,xy,xz,yz).$$

(iv) 上と同様に R の $\mathbb{C}$ ベクトル空間としての基底としてありうるのは

$$\{1,x,y,x^2,x^3\},\quad\{1,x,y,x^2,y^2\},\quad\{1,x,y,x^2,xy\}.$$

それぞれの場合の R を $R_i\,(i=1,2,3)$ とおく．

• 環準同型 $\varphi:R_2\to R_3$ を $x\mapsto x,y\mapsto x+y$ で定義すると，$\varphi(x^2)=x^2,\varphi(y^2-x^2)=2xy$ だから φ は全射．また $c_1+c_2x+c_3y+c_4x^2+c_5y^2\in\operatorname{Ker}\varphi$ とすると，$c_1+c_2x+c_3(x+y)+c_4x^2+c_5(x^2+2xy)=0$ から $c_1=\cdots=c_5=0$ なので φ は単射．よって $R_2\cong R_3$.

• 環同型 $\varphi:R_1\to R_2$ があったとする．R_i の極大イデアルを $\mathfrak{m}_i$ とおく．$\varphi(R_1^\times)=R_2^\times$ だから $\varphi(\mathfrak{m}_1)=\mathfrak{m}_2$. また $\varphi|_{\mathfrak{m}_1}:\mathfrak{m}_1\to\mathfrak{m}_2$ は $\mathbb{C}$ ベクトル空間の同型写像でもある．今任意の $a\in\mathfrak{m}_2$ は $a^3=0$ を満たすから，$\varphi(x^3)=\varphi(x)^3=0$ となり $\varphi|_{\mathfrak{m}_1}$ が単射であることに矛盾．よって $R_1\ncong R_2$.

以上から R は

$$R_1=\mathbb{C}[x,y]/(x^4,y^2,xy),\quad R_2=\mathbb{C}[x,y]/(x^3,y^3,xy)$$

のどちらかに同型．□

問 3

A をネーター局所環，M を有限生成 A 加群，n を正の整数とし，A 加群の準同型写像 $f : M \to A^{\oplus n}$ を考える．A の剰余体 k に対し，f に $\otimes_A k$ を施して得られる k 線形写像を $f_k : M \otimes_A k \to A^{\oplus n} \otimes_A k$ と書く．次の (i), (ii) を示せ．

(i) f_k が全射ならば，A 加群の準同型写像 $\varphi : A^{\oplus n} \to M$ で $f \circ \varphi$ が $A^{\oplus n}$ の恒等写像となるものが存在する．

(ii) f_k が単射ならば，A 加群の準同型写像 $\psi : A^{\oplus n} \to M$ で $\psi \circ f$ が M の恒等写像となるものが存在する．

解答. □

平成 23 年度 (2010 年 8 月実施)

問 1

p と ℓ は素数とし，$p < \ell$ と仮定する．有限群 G に対して次の条件 $(*_{p,\ell})$ を考える．

$(*_{p,\ell})$　　G は，位数 $p\ell$ の非アーベル群である．

(i) 有限群 G が $(*_{p,\ell})$ を満たすと仮定する．このとき，G の中に位数 ℓ の部分群がただ一つ存在し，かつ正規部分群になることを示せ．
(ii) $(*_{p,\ell})$ を満たす有限群 G が存在するとき，$\ell - 1$ は p で割り切れることを示せ．
(iii) 有限群 G_1, G_2 が $(*_{p,\ell})$ を満たすとき，G_1 と G_2 は有限群として同型であることを示せ．
(iv) ガロア群 $\mathrm{Gal}(L/K)$ が $(*_{p,\ell})$ を満たすような，素数 $p < \ell$ と，体の有限次ガロア拡大 L/K が存在することを示せ．

解答. (i) G の Sylow ℓ 部分群の個数を n とすると，Sylow の定理より $n \equiv 1 \bmod \ell$ かつ $n \mid p\ell$ だから，p, ℓ が素数であることより $n = 1$. 従ってこの唯一の Sylow ℓ 部分群を H とすると $G \rhd H$.

(ii) $|G/H| = p$ より $G/H \cong \mathbb{Z}/p\mathbb{Z}$ である．この生成元を gH $(g \in G \setminus H)$ とすると $K := \langle g \rangle \cong \mathbb{Z}/p\mathbb{Z}$ である．また $(p, \ell) = 1$ より $H \cap K = \{1\}$ であり，位数の比較から $G = HK$ である．よって群準同型 $\sigma : K \to \mathrm{Aut}(H)$ が存在して $G \cong H \rtimes_\sigma K$ となる．$\sigma(g) = \mathrm{id}_H$ とすると，$G \cong H \times K$ は Abel 群となって矛盾するから $\sigma(g) \neq \mathrm{id}_H$ である．これと $\sigma(g)^p = \sigma(g^p) = \sigma(1) = \mathrm{id}_H$ より $\sigma(g) \in \mathrm{Aut}(H) \cong \mathbb{Z}/(\ell-1)\mathbb{Z}$ の位数は p である．よって示された．

(iii) $H = \langle h \rangle$ とする．$G \rhd H$ だから $g^{-1}hg = h^r$ となる r が存在する．$(*_{p,\ell})$ より $r \not\equiv 1 \bmod \ell$ である．また帰納的に $g^{-k}hg^k = h^{r^k}$ だから $h^{r^p} = g^{-p}hg^p = h$. すなわち $r^p \equiv 1 \bmod \ell$ だから，$\mathbb{Z}_\ell^\times$ の位数 p の元 r を用いて

$$G = \langle g, h \,|\, h^\ell = g^p = 1, g^{-1}hg = h^r \rangle$$

と書ける．これを G_r とおく．$\mathbb{Z}_\ell^\times$ の位数 p の元 s に対し，$G_r \cong G_s$ を示せば良い．(ii) より $\mathbb{Z}_\ell^\times \cong \mathbb{Z}/(\ell-1)\mathbb{Z}$ は位数 p の部分群を持ち，しかもそれは唯一つである．その生成元を a とすれば，$\mathbb{Z}_\ell^\times$ の位数 p の元は $a, a^2, \ldots, a^{p-1}$ である．よって $r^k \equiv s \bmod \ell$ となる $k \in \mathbb{Z}$ が存在する．$s \not\equiv 1 \bmod \ell$ だから k は p と互いに素である．従って g^k は位数 p であり，$g^{-k}hg^k = h^{r^k} = h^s$ だから

$$G_r = \langle g^k, h \,|\, h^\ell = (g^k)^p = 1, (g^k)^{-1}hg^k = h^s \rangle \cong G_s.$$

(iv) $p = 2, \ell = 3, K = \mathbb{Q}, L = \mathbb{Q}(2^{1/3}, e^{2\pi i/3})$ とすれば $\mathrm{Gal}(L/K) \cong D_3$ である．[3] □

[3] Galois 理論の教科書を参照.

問 2

複素 1 変数多項式環 $\mathbb{C}[x]$ の部分環 R について考える．R は $\mathbb{C}$ を含み，商ベクトル空間 $\mathbb{C}[x]/R$ は $\mathbb{C}$ 上 1 次元であると仮定する．

(i) $q(x) \in R$ かつ $xq(x) \in R$ を満たす 2 次式 $q(x)$ が存在することを示せ．

(ii) 次の (a), (b) のいずれかが成立することを示せ．

(a) 二つの相異なる複素数 α, β が存在して，

$$R = \Big\{ f(x) \in \mathbb{C}[x] \,\Big|\, f(\alpha) = f(\beta) \Big\}.$$

(b) 複素数 α が存在して，

$$R = \Big\{ f(x) \in \mathbb{C}[x] \,\Big|\, \frac{df}{dx}(\alpha) = 0 \Big\}.$$

解答. (i) $f(x) \in \mathbb{C}[x]$ を $\mathbb{C}[x]/R$ の基底とすると $\mathbb{C}[x] = R \oplus \mathbb{C}f(x)$. 今 $ax + b \in R\,(a \neq 0)$ とすると，$\mathbb{C} \subset R$ より $x = a^{-1}((ax+b) - b) \in R$ だから $R = \mathbb{C}[x]$. これは $\dim_{\mathbb{C}} \mathbb{C}[x]/R = 1$ に矛盾．よって R は 1 次式を含まない．特に $x \in \mathbb{C}f(x)$ だから $f(x) = ax\,(a \in \mathbb{C})$, 従って $\mathbb{C}[x] = R \oplus \mathbb{C}x$ である．ここで x^2 の $\mathbb{C}[x]/R = \mathbb{C}x$ における像を $c_1 x$ とすると $g(x) := x^2 - c_1 x \in R$. さらに $xg(x)$ の $\mathbb{C}[x]/R$ における像を $c_2 x$ とする．この時 $q(x) = g(x) - c_2 \in R$ とすれば $xq(x) = xg(x) - c_2 x \in R$.

(ii) 任意の $N \geq 2$ は $n, m \geq 0$ があって $2n + 3m = N$ と書けることから，$\deg f \geq 2$ なる任意の $f \in R$ に対し $\deg(f - cq^n(xq)^m) \leq \deg f - 1$ となる $c \in \mathbb{C}, n, m \geq 0$ が存在する．同様にして $g(x) \in \mathbb{C}[q(x), xq(x)]$ が存在して $\deg(f - g) \leq 1$ と出来る．$f - g \in R$ であるが，R は 1 次式を含まないから，これは定数．それを c とおくと $f = c + g \in \mathbb{C} \oplus q\mathbb{C}[x]$. 従って $R \subset \mathbb{C} \oplus q\mathbb{C}[x]$ となるが，

$$\mathbb{C}x = \mathbb{C}[x]/R \supset \mathbb{C}[x]/(\mathbb{C} \oplus q\mathbb{C}[x]) = \mathbb{C}x$$

だから包含は等号が成立し $R = \mathbb{C} \oplus q\mathbb{C}[x]$. よって $q = (x - \alpha)(x - \beta)$ とおけば

$$R = \Big\{ c + (x - \alpha)(x - \beta)p(x) \,;\, c \in \mathbb{C}, p \in \mathbb{C}[x] \Big\}$$

であるから，$\alpha \neq \beta$ なら (a) が，$\alpha = \beta$ なら (b) が成立する． □

問 3

R を複素 n 変数形式的ベキ級数環 $\mathbb{C}[\![X_1, \ldots, X_n]\!]$ とし，$\sigma : R \to R$ を $\mathbb{C}$ 代数としての自己同型写像とする．自然数 $k \geq 2$ について，$\sigma^k = \overbrace{\sigma \circ \cdots \circ \sigma}^{k}$ が R の恒等写像であるならば，以下の (i), (ii) を満たす R の元 $z_1, \ldots, z_n$ と 1 の k 乗根 $\zeta_1, \ldots, \zeta_n$ が存在することを示せ．

(i) $Rz_1 + \cdots + Rz_n$ は R の極大イデアル．

(ii) すべての $i = 1, 2, \ldots, n$ に対し，$\sigma(z_i) = \zeta_i z_i$.

解答. □

平成 22 年度 (2009 年 8 月実施)

問 1

k は代数閉体とし，$k_0 \subseteq k$ はその部分体とする．また，$M_2(k), M_2(k_0)$ はそれぞれ k, k_0 の元を成分とする 2 次正方行列全体とし，$\lambda, \mu \in k$ に対して

$$S(\lambda, \mu) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(k) \,\middle|\, ad - bc = \lambda, a + d = \mu \right\}$$

とおく．このとき，k_0 係数の多項式 $f(X, Y, Z, T) \in k_0[X, Y, Z, T]$（ただし，$X, Y, Z, T$ は不定元）に対して定義される関数 $\phi : M_2(k) \longrightarrow k$

$$M_2(k) \ni A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \phi(A) = f(a, b, c, d) \in k$$

が次の条件を満たすと仮定する: 任意の $A, B \in M_2(k_0)$ に対して $\phi(AB) = \phi(BA)$.

(i) $k = k_0$ のとき，任意の $\lambda, \mu \in k$ に対して ϕ が $S(\lambda, \mu)$ の上で定数関数になることを示せ．

(ii) k_0 が有限体のとき，ϕ が $S(\lambda, \mu)$ の上で定数関数にならないような $\lambda, \mu \in k_0, f(X, Y, Z, T) \in k_0[X, Y, Z, T]$ の例を挙げよ．

解答. (i) 仮定から，任意の $A \in M_2(k)$ に対し $P \in GL_2(k)$ と Jordan 標準形 $D \in M_2(k)$ であって $P^{-1}AP = D$ となるものが存在する．この時 $\phi(A) = \phi(APP^{-1}) = \phi(P^{-1}AP) = \phi(D)$ だから，Jordan 標準形の像を調べれば良い．$S(\lambda, \mu)$ の元の Jordan 標準形は高々 2 種類であり，ちょうど 2 種類になるのは固有値が等しい時である．よって任意の $a \in k$ に対し $\phi(\left(\begin{smallmatrix} a & \\ & a \end{smallmatrix}\right)) = \phi(\left(\begin{smallmatrix} a & 1 \\ & a \end{smallmatrix}\right))$ を示せば十分．$\left(\begin{smallmatrix} a & x \\ & a \end{smallmatrix}\right)$ $(x \neq 0)$ と $\left(\begin{smallmatrix} a & 1 \\ & a \end{smallmatrix}\right)$ は最小多項式がともに $(t-a)^2$ だから，$GL_2(k)$ 共役である．よって $x \neq 0$ に対し $\phi(\left(\begin{smallmatrix} a & x \\ & a \end{smallmatrix}\right)) = \phi(\left(\begin{smallmatrix} a & 1 \\ & a \end{smallmatrix}\right))$. 一方 $\phi(\left(\begin{smallmatrix} a & x \\ & a \end{smallmatrix}\right)) \in k[x]$ と k が無限体であることより，この等式は任意の $x \in k$ で成り立つ．特に $x = 0$ として示すべき式を得る．

(ii) $\#k_0 = q$ とし，k_1 を k_0 の 2 次拡大体とする．$\alpha \in k_1 \setminus k_0$ を任意に取ると，$\alpha^2 - \mu_0\alpha + \lambda_0 = 0$ を満たす $\lambda_0, \mu_0 \in k_0$ が存在する．この時

$$(\lambda, \mu) = (\lambda_0, \mu_0), \qquad f = X^q + T \in k_0[X, Y, Z, T]$$

が条件を満たすことを示す．$A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(k_0)$ に対し $\phi(A) = a^q + d = a + d = \operatorname{tr} A$ だから，任意の $A, B \in M_2(k_0)$ に対し $\phi(AB) = \phi(BA)$ である．一方

$$A_1 = \begin{pmatrix} \mu_0 & -\lambda_0 \\ 1 & 0 \end{pmatrix}, A_2 = \begin{pmatrix} \alpha & \\ & \mu_0 - \alpha \end{pmatrix} \in S(\lambda_0, \mu_0)$$

に対し $\phi(A_1) = \operatorname{tr} A_1 = \mu_0$ であるが，$\alpha \notin k_0$ より $\phi(A_2) = \alpha^q + (\mu_0 - \alpha) \neq \mu_0$. よって ϕ は $S(\lambda, \mu)$ 上で定数でない． □

問 2

p は素数とし，$\mathbb{F}_p$ を濃度 p の有限体とする．$G = GL_n(\mathbb{F}_p)$ を $\mathbb{F}_p$ を成分とする可逆な n 次正方行列の成す群とし，

$$U = \left\{ \begin{bmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{bmatrix} \right\}$$

を対角成分がすべて 1 の上三角行列の成す部分群とする．

(i) U は G の Sylow p 部分群であることを示せ．

(ii) G の Sylow p 部分群の個数を求めよ．

解答． (i) $|G|$ は，$\mathbb{F}_p^n$ 上の n 本の一次独立な列ベクトルの組 $(v_1, \ldots, v_n)$ の個数に等しい．v_1 の選び方は 0 以外の $p^n - 1$ 通り．$v_1, \ldots, v_{k-1}$ まで選んだ時，$\mathbb{F}_p^n$ の元のうち $v_1, \ldots, v_{k-1}$ の一次結合で書けるものは $a_1v_1 + \cdots + a_{k-1}v_{k-1}\,(a_1, \ldots, a_{k-1} \in \mathbb{F}_p)$ の p^{k-1} 個だから，v_k の選び方は $p^n - p^{k-1}$ 通り．よって

$$|G| = \prod_{i=1}^{n}(p^n - p^{i-1}) = p^{n(n-1)/2}\prod_{i=1}^{n}(p^i - 1).$$

また，n 次正方行列の上三角部分の成分の個数は $\frac{1}{2}(n^2 - n) = \frac{n(n-1)}{2}$ だから $|U| = p^{n(n-1)/2}$ である．$\prod_{i=1}^{n}(p^i - 1)$ は p で割り切れないから U は G の Sylow p 部分群となる．

(ii) Sylow の定理から，求めるものは $(G : N_G(U))$ である．$g = (g_{ij}) \in N_G(U)$ とすると，任意の $u = (u_{ij}) \in U$ に対し $v = (v_{ij}) \in U$ があって $gu = vg$, すなわち $g(u - I) = (v - I)g$. この (i, j) 成分より

$$\sum_{k=1}^{j-1} g_{ik}u_{kj} = \sum_{k=i+1}^{n} v_{ik}g_{kj}. \qquad (*)$$

ここで $g_{ij} = 0\,(j < i)$ となることを i についての降下法で示す．$i = n$ の時は $(*)$ の右辺は 0 であり，これが任意の u に対して成り立つことから $g_{nk} = 0\,(1 \le k \le j - 1, 1 \le j \le n)$ となり正しい．$i + 1$ 以上で成り立つ時，$j < i + 1$ ならば $(*)$ の右辺は 0 だから $g_{ik} = 0\,(1 \le k \le j - 1, j < i + 1)$. よって i の時も成り立つ．これで示せた．よって $g \in N_G(U)$ は正則な上三角行列であることが必要．逆に g が正則な上三角行列であれば，gug^{-1} は対角成分が全て 1 の上三角行列だから $gug^{-1} \in U$. よって $N_G(U)$ は正則な上三角行列のなす部分群であるから，$|N_G(U)| = (p - 1)^n p^{n(n-1)/2}$. 従って

$$(G : N_G(U)) = \frac{|G|}{|N_G(U)|} = \prod_{i=1}^{n}\frac{p^i - 1}{p - 1}.$$

□

問 3

k を体とする．$k[x]$ を k 係数一変数多項式環とする．R は k を含む $k[x]$ の部分環であり，次数が互いに素な二つの定数でない多項式を含んでいるものとする．このとき次を示せ．

(i) 商ベクトル空間 $k[x]/R$ は k 上有限次元である．

(ii) $k[x]$ の零でないイデアルであって R に含まれるものが存在する．

解答. (i) R に含まれる，次数が互いに素な多項式を f, g とし，$\deg f = n, \deg g = m$ とする．まず任意の整数 $N > nm - n - m$ は，非負整数 a, b が存在して $N = an + bm$ と書けることを示す．$(n, m) = 1$ だから $bm \equiv N \bmod n$ となる $0 \leq b < n$ が存在する．ところが

$$N - bm > (nm - n - m) - bm = (n - 1 - b)m - n \geq -n$$

だから，$a \geq 0$ があって $N - bm = an$ と書ける．これで示せた．これにより $\deg h > nm - n - m$ なる任意の $h \in k[x]$ に対し，$c \in k, i, j \geq 0$ があって $\deg(h - cf^i g^j) < \deg h$ と出来る．同様にして $\widetilde{h} \in k[f, g]$ があって $\deg(h - \widetilde{h}) \leq nm - n - m$ と出来る．よって h の $k[x]/R$ における代表元を $\overline{h}$ とすると $\deg \overline{h} \leq nm - n - m$ だから，$\dim_k k[x]/R \leq nm - n - m + 1$.

(ii) $d = \dim_k k[x]/R$ とおく．もし $xh \in R$ となる $h \in R \setminus \{0\}$ が存在すれば，$0 \leq i \leq d - 1$ に対し $x^i h^{d-1} = (xh)^i h^{d-1-i} \in R$ となる．これと (i) より，任意の $p(x) \in k[x]$ に対し $ph^{d-1} \in R$ だから，(h^{d-1}) が条件を満たすイデアルとなる．よって R の商体 $Q(R)$ が x を含むことを示せば良い．$F(T) = T^\ell + a_{\ell-1}(x)T^{\ell-1} + \cdots + a_0(x) \in Q(R)[T]$ を x の $Q(R)$ 上の最小多項式とする．$f(T) - f(x) \in Q(R)[T]$ は x を零点に持つから $F(T)$ で割り切れ，従って n は ℓ で割り切れる．同様に m は ℓ で割り切れる．（これは嘘．そのうち修正する） ところが $(n, m) = 1$ だから $\ell = 1$. よって $0 = F(x) = x + a_0(x)$ なので $x = -a_0(x) \in Q(R)$. □

平成 21 年度 (2008 年 8 月実施)

問 1

R を正規局所環（整閉整域でありかつ局所環である可換環）とし，$\mathfrak{m}$ を R の極大イデアル，K を R の商体，k を剰余体 $R/\mathfrak{m}$ とする．多項式 $f(x) \in R[x]$ を考え，$k[x]$ における $f(x)$ の像が 0 でないと仮定する．K の元 u が $f(u) = 0$ をみたすとき，次の (i), (ii) を証明せよ．

(i) $f(0) \notin \mathfrak{m}$ ならば，$u \in R$ または $u^{-1} \in \mathfrak{m}$ が成り立つ．

(ii) k が無限体ならば，$u \in R$ または $u^{-1} \in \mathfrak{m}$ が成り立つ．

解答. (i) 仮定から $f(0) \in R \setminus \mathfrak{m} = R^\times$. これと $f(u) = 0$ より $u \neq 0$ である．よって $f(0)^{-1}u^{-d}f(u) = 0$（ただし $d = \deg f$）だから，$u^{-1} \in K$ は monic な多項式 $f(0)^{-1}x^d f(x^{-1}) \in R[x]$ の根である．これと R が整閉整域であることより $u^{-1} \in R$. 従って $u^{-1} \in R^\times$ なら $u \in R$ が成り立ち，$u^{-1} \notin R^\times$ なら $u^{-1} \in R \setminus R^\times = \mathfrak{m}$ が成り立つ．

(ii) 射影 $R \to k$ による $f(x) \in R[x], x \in R$ の像をそれぞれ $\overline{f}(x), \overline{x}$ と書く．$\overline{f}(x) \in k[x]$ は 0 でない多項式で $|k| = \infty$ だから，$\overline{f}(\overline{a}) \neq 0$ となる $a \in R$ が存在する.[4] すなわち $f(a) \notin \mathfrak{m}$. よって $g(x) = f(x + a) \in R[x]$ とおけば $g(u - a) = f(u) = 0, g(0) = f(a) \notin \mathfrak{m}$ だから，(i) より $u - a \in R$ または $(u - a)^{-1} \in \mathfrak{m}$. 前者の時は $u = (u - a) + a \in R$. 後者の時は $b = (u - a)^{-1}$ とおくと，$(u - a)b = 1$ より $ub = 1 + ab \in R^\times$. よって $u^{-1} = b(1 + ab)^{-1} \in \mathfrak{m}$. □

[4] 例えば数学系平成 5 年度数学 I 問 1 を参照.

問 2

有限群 G が次の二条件 (A), (B) をみたすとき，G の指標表を求めよ．

(A) G は指数 2 の部分群 H を含み，H の指標表は

	C_1	C_2	C_3
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

である．ただし，H の共役類を C_1, C_2, C_3 とし，H の既約指標を χ_1, χ_2, χ_3 とする．

(B) G の指標値はすべて有理数である．

解答. $H = S_3, |G| = 12$. https://people.maths.bris.ac.uk/~matyd/GroupNames/index.html □

平成 20 年度 (2007 年 8 月実施)

問 1

T, X は n 次元複素ベクトル空間 V の可逆な線形変換で $TXT = X^{-1}$ をみたし，T の最小多項式の次数が 2 であるとする．このとき，部分ベクトル空間の列

$$\{0\} = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_l = V$$

で，各 $1 \leq i \leq l$ に対し

$$TV_i \subseteq V_i, \quad XV_i \subseteq V_i, \quad \dim V_i/V_{i-1} \leq 2$$

をみたすものが存在することを示せ．

解答. X の Jordan 標準形を $\mathrm{diag}(J(\lambda_1, n_1), \ldots, J(\lambda_i, n_i))\,(\lambda_j \neq 0)$ とし，広義固有空間の元 v_{jk} を $Xv_{j1} = \lambda_j x_{j1}, Xv_{jk} = \lambda v_{jk} + v_{j,k-1}\,(2 \leq k \leq n_j)$ とする．また仮定から $T^2 - aT + bI = 0$ なる $a, b \in \mathbb{C}, b \neq 0$ が存在するから $XTX = T^{-1} = \frac{1}{b}(aI - T)$ である．よって $Xv_{j1}, Tv_{j1} \in \langle v_{j1}, Tv_{j1} \rangle$,

$$X(Tv_{j1}) = \frac{1}{\lambda_j b}(aI - T)v_{j1} \in \langle v_{j1}, Tv_{j1} \rangle ,$$
$$T(Tv_{j1}) = (aT - bI)v_{j1} \in \langle v_{j1}, Tv_{j1} \rangle .$$

また $2 \leq k \leq n_j$ に対して $Xv_{jk}, Tv_{jk}, T(Tv_{jk}) \in \langle v_{jk}, Tv_{jk}, v_{j,k-1} \rangle$.

$$XT(\lambda_j v_{jk} + v_{j,k-1}) = XTXv_{jk} = \frac{1}{b}(aI - T)v_{jk} \in \langle v_{jk}, Tv_{jk} \rangle$$

と $\lambda_j \neq 0$ より帰納的に $XTv_{jk} \in \langle v_{j1}, Tv_{j1}, \ldots, v_{jk}, Tv_{jk} \rangle$ である．以上から $v_{11}, \ldots, v_{1,n_1}, \ldots, v_{i,n_i}$ を改めて $v_1, \ldots, v_n$ と書いて $V_j = \langle v_1, Tv_1, \ldots, v_j, Tv_j \rangle$ とおけば，$XV_j \subset V_j, TV_j \subset V_j, \dim V_j/V_{j-1} \leq 2$ を満たす．また $\langle v_1, \ldots, v_n \rangle = \mathbb{C}^n$ だから，$V_\ell = V$ となる $\ell \leq i$ が存在する． □

問 2

K を体とし，L を K の 3 次拡大体とする．α, β を L の元でいずれも K に属さないものとする．このとき，

$$\beta = \frac{a\alpha + b}{c\alpha + d} \quad \text{かつ} \quad ad - bc \neq 0$$

をみたす $(a, b, c, d) \in K^4$ が存在し，K のスカラー倍を除いて一意的に定まることを示せ．

解答． $K(\alpha)$ は L の部分体だから $3 = [L : K] = [L : K(\alpha)][K(\alpha) : K]$. また $\alpha \notin K$ より $[K(\alpha) : K] > 1$ だから $[L : K(\alpha)] = 1, [K(\alpha) : K] = 3$. よって $L = K(\alpha)$ であり，α の K 上最小多項式を $f(X) \in K[X]$ とすると $\deg f = 3$ である．この時 $\beta \in L \setminus K = K(\alpha) \setminus K$ より $p, q, r \in K$ が存在して $\beta = p\alpha^2 + q\alpha + r$ と書ける．$f(X) = (cX + d)(pX^2 + qX + r) - (aX + b)$ と割り算すると $a, b, c, d \in K, (c, d) \neq (0, 0)$ であり，$0 = f(\alpha) = (c\alpha + d)\beta - (a\alpha + b)$ である．$\alpha \notin K$ より $c\alpha + d \neq 0$ なので $\beta = \dfrac{a\alpha + b}{c\alpha + d}$ を得る．$ad - bc = 0$ であったとすると，$\operatorname{rank} \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \leq 1$ と $(c, d) \neq (0, 0)$ より $(a, b) = \lambda(c, d)$ なる $\lambda \in K$ が存在する．よって $\beta = \lambda \in K$ となり矛盾する．

今 $\beta = \dfrac{a'\alpha + b'}{c'\alpha + d'}$ となる $(a', b', c', d') \in K^4$ が存在したとすると，

$$g(X) = (aX + b)(c'X + d') - (a'X + b')(cX + d) \in K[X]$$

は $g(\alpha) = 0$ を満たす．よって f は g を割り切るが，$\deg f = 3 > \deg g$ より $g \equiv 0$ が従う．よって

$$\begin{cases} ac' - a'c = 0 \\ ad' + bc' - a'd - b'c = 0. \\ bd' - b'd = 0 \end{cases}$$

$ad - bc \neq 0$ より $(a, c), (b, d) \neq (0, 0)$ だから，第 1 式と第 3 式より $\lambda_1, \lambda_2 \in K$ があって $(a', c') = \lambda_1(a, c), (b', d') = \lambda_2(b, d)$ と書ける．これを第 2 式に代入すると

$$0 = \lambda_2 ad + \lambda_1 bc - \lambda_1 ad - \lambda_2 bc = (\lambda_2 - \lambda_1)(ad - bc)$$

だから $\lambda_1 = \lambda_2$, すなわち $(a', b', c', d') = \lambda_1(a, b, c, d)$ となる． □

問 3

m, n を互いに素な正整数とし，$f(x,y) \in \mathbb{C}[x,y]$ を二変数 n 次斉次多項式とする．環

$$R = \mathbb{C}[x,y,z]/(z^m - f(x,y))$$

に対し，次の問に答えよ．

(1) R は整域であることを示せ．

(2) R の可逆元全体のなす集合 $R^\times$ は $\mathbb{C} \setminus \{0\}$ に一致することを示せ．

（ヒント：$z^m - f(x,y)$ は重み付き斉次多項式と考えられる．）

解答．(1) $I := (z^m - f(x,y))$ が素イデアルであることを示せば良い．それには $z^m - f(x,y)$ が既約であることを示せば十分．可約とすると，定数でない $p, q \in \mathbb{C}[x,y,z]$ があって $p(x,y,z)q(x,y,z) = z^m - f(x,y)$ と書ける．$\deg_z p = 0$ とすると両辺の z^m の係数を比較して p が定数となる．$\deg_z q$ についても同様なので，$\deg_z p, \deg_z q \geq 1$ である．f は 0 でないから，$f(x_0, y_0) \neq 0$ となる $(x_0, y_0) \in \mathbb{C}^2$ が存在する．f は斉次だから，(x_0, y_0) を適当に定数倍して $f(x_0, y_0) = 1$ と出来る．この時 t を不定元として

$$p(tx_0, ty_0, z)q(tx_0, ty_0, z) = z^m - f(tx_0, ty_0) = z^m - t^n$$

となる．よって $z^m - t^n \in \mathbb{C}[z,t]$ が既約であることが示せれば矛盾となる．これを示そう．準同型 $\varphi : \mathbb{C}[z,t] \to \mathbb{C}[s]$ を $\varphi(z) = s^n, \varphi(t) = s^m$ で定める．

$$g = (z^m - t^n)g_1(z,t) + \sum_{j=0}^{m-1} \sum_{k \geq 0} g_{jk} t^k z^j \in \operatorname{Ker} \varphi$$

とすると $0 = \sum_{j=0}^{m-1} \sum_{k \geq 0} g_{jk} s^{jn+km}$. 今 $(j,k), (j',k')$ が $0 \leq j, j' \leq m-1, jn + km = j'n + k'm$ を満たすとすると，$(j - j')n = (k' - k)m$ で $(m,n) = 1$ より $m | (j - j')$. よって $j = j'$, 従って $k = k'$. ゆえに $g_{jk} = 0$ となるから $g = (z^m - t^n)g_1(z,t)$. よって $\operatorname{Ker} \varphi \subset (z^m - t^n)$. 逆の包含は明らかだから，準同型定理より

$$\mathbb{C}[z,t]/(z^m - t^n) \cong \operatorname{Im} \varphi = \mathbb{C}[s^n, s^m].$$

この右辺は整域だから $(z^m - t^n)$ は素イデアル．よって $z^m - t^n$ は $\mathbb{C}[z,t]$ の素元．$\mathbb{C}[z,t]$ は整域だから $z^m - t^n$ は既約である．

(2) $A = \mathbb{C}[x,y,z]$ とおき，x, y, z の重みをそれぞれ m, m, n とする．重みが k の斉次多項式の全体を A_k とおくと，$A = \bigoplus_{k \geq 0} A_k$ は次数付き環となる．さらに $z^m - f(x,y) \in A_{mn}$ だから，$R = A/I = \bigoplus_{k \geq 0} A_k/(I \cap A_k)$ を得る．従って $R^\times \subset A_0/(I \cap A_0) = \mathbb{C} \setminus \{0\}$. 逆の包含は明らかだから示された． □

平成 19 年度 (2006 年 8 月実施)

問 1

$\mathbb{Q}$ の 4 次巡回拡大体 K であって，$i^2 = -1$ をみたす元 i を含むものは存在するか？存在する場合は例を挙げ，存在しない場合はその証明を与えよ．

解答. 存在しない．そのような K が存在したとすると $\mathrm{Gal}(K/\mathbb{Q}) = \mathbb{Z}/4\mathbb{Z}$. この部分群は $\mathbb{Z}/2\mathbb{Z}$ のみだから，K は唯一つの部分体 L を持つ．また $\mathbb{Z}/4\mathbb{Z} \rhd \mathbb{Z}/2\mathbb{Z}$ なので，$L/\mathbb{Q}$ は Galois 拡大である．一方 $\mathbb{Q}(i)$ は K の真部分体だから $L = \mathbb{Q}(i)$ を得る．$\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ を $\sigma(i) = -i$ で定める．$\mathbb{R} \subsetneq K$ より $\langle\sigma\rangle \cong \mathbb{Z}/2\mathbb{Z}$ であるから，これは $\mathrm{Gal}(K/\mathbb{Q})$ の唯一の部分群である．よって Galois の基本定理より $\mathbb{Q}(i) = K^{\langle\sigma\rangle} = K \cap \mathbb{R}$ となるが，$i \notin K \cap \mathbb{R}$ なので矛盾． □

問 2

p は素数とする．不定元 T に関する $\mathbb{Z}$ 係数多項式 $f(T)=\sum_{j\geq 0}c_jT^j$ に対して

$$f'(T)=\sum_{j\geq 1}jc_jT^{j-1}$$

と定め，非負整数 N に対して f_N は，$f(T)$ に $p\mathbb{Z}$ の元を代入することによって定まる写像

$$f_N : p\mathbb{Z}\to \mathbb{Z}/p^N\mathbb{Z}$$

を表すとする．$f'(T)\neq 0$ として以下の問に答えよ．

(i) $f_N(t)\neq 0\in\mathbb{Z}/p^N\mathbb{Z}$, $f'_N(t)\neq 0\in\mathbb{Z}/p^N\mathbb{Z}$ となる $t\in p\mathbb{Z}$ と非負整数 N が存在することを示せ．

(ii) 次の性質 $(*)$ をみたす $c\in\mathbb{Z}$ と非負整数 m が存在することを示せ．

$(*)$ 任意の非負整数 $N\geq m$ に対して，集合

$$\{x\in\mathbb{Z}/p^N\mathbb{Z}\,|\,x\equiv c \bmod p^m\}$$

は f_N の像に含まれる．

解答. (i) $f'(T)\neq 0$ より f, f' はゼロでない多項式だから，$\{t\in p\mathbb{Z};\, f(t)=0$ または $f'(t)=0\}$ は有限集合である．よって $f(t)\neq 0, f'(t)\neq 0$ となる $t\in p\mathbb{Z}$ が存在するから，十分大きい N を取れば $f_N(t)\neq 0, f'_N(t)\neq 0$ となる．

(ii) t を (i) のものとする．$d=\deg f$ とおくと

$$f(T)=f(t)+a_1p^{e_1}(T-t)+\cdots+a_dp^{e_d}(T-t)^d$$

と書ける．ただし $a_i=0$ または $a_i,e_i\in\mathbb{N}, (a_i,p)=1$ である．仮定から $a_1,a_d\neq 0$ である．$a_i\neq 0$ となる任意の $i\geq 2$ に対し $e_1+j<e_i+ij$ となるように $j\geq 1$ を取る．($d=1$ の時は $j=1$ とする.) この時 $c=f(t), m=e_1+j$ が条件を満たすことを示す．任意に $N\geq m, k\in\mathbb{Z}$ を取る．$x=x_0+x_1p+\cdots+x_{N-m-1}p^{N-m-1}\,(0\leq x_i<p)$ とおけば

$$\begin{aligned} f(t+p^jx)-f(t) &= a_1p^{e_1+j}x+\sum_{i=2}^{d}a_ip^{e_i+ij}x^i \\ &= a_1x_0p^m+\sum_{i=1}^{N-m-1}(a_1x_i+(x_0,\ldots,x_{i-1}\text{ の多項式}))p^{m+i} \end{aligned}$$

である．ただし最後の等号は j の取り方による．$(a_1,p)=1$ だから，これが $\equiv kp^m \bmod p^N$ となるように帰納的に x_i を定めることができる．よって $f_N(t+p^jx)=c+kp^m$ となるから示された． □

問 3

2 変数多項式環 $\mathbb{C}[x,y]$ の中で $f(x,0)$ が定数となる多項式 $f(x,y)$ 全体のなす部分環を R とする．また，x と $y-b(b\in\mathbb{C})$ で生成される $\mathbb{C}[x,y]$ のイデアルを $\mathfrak{m}_b$ とおく．

(i) R のイデアル $\mathfrak{m}_1\cap R$ は二つの元で生成されることを示せ．

(ii) R のイデアル $\mathfrak{m}_0\cap R$ は有限生成でないことを示せ．

解答． (i) $f=xg(x,y)+(y-1)h(x,y)\in\mathfrak{m}_1$ を取る．$g=\sum_{j\geq 0}g_j(x)y^j, h=\sum_{j\geq 0}h_j(x)y^j\in\mathbb{C}[x,y]$ とおく．$f\in R$ となる時 $xg(x,0)-h(x,0)=xg_0(x)-h_0(x)$ は定数だから，それを c として

$$\begin{aligned} f &= x\sum_{j\geq 0}g_j(x)y^j+(y-1)\left(xg_0(x)-c+\sum_{j\geq 1}h_j(x)y^j\right)\\ &= xy\left(g_0(x)+g_1(x)+\sum_{j\geq 2}g_j(x)y^{j-1}\right)+(y-1)\left(-c+\sum_{j\geq 1}h_j(x)y^j\right)\end{aligned}$$

と書ける．第 2 項は $(y-1)$ に入り，$i,j\geq 0$ に対し

$$x^{i+1}y^{j+1}=xy\cdot x^iy^{j+1}-(y-1)x^{i+1}y^{j+1}\in(xy,y-1)$$

だから $f\in(xy,y-1)$. よって $\mathfrak{m}_1\cap R\subset(xy,y-1)$. 逆の包含は明らかだから

$$\mathfrak{m}_1\cap R=(xy,y-1).$$

これが単項イデアルだったとして生成元を $h(x,y)\in\mathbb{C}[x,y]$ とすると，$xy,y-1\in\mathfrak{m}_1\cap R$ より h は $xy,y-1$ の最大公約元 1 を割り切るから $h=1$. よって $\mathfrak{m}_1\cap R=R$ だから，$y\in R$ に対し $y=xg_1+(y-1)g_2$ となる $g_1,g_2\in R$ が存在する．ところが $y=1$ とすると $1=xg_1(x,1)$ となり矛盾．

(ii) $f=xg(x,y)+yh(x,y)\in\mathfrak{m}_0$ が R の元である時，$xg(x,0)=xg_0(x)$ は定数だから $g_0(x)=0$. よって

$$f=x\sum_{j\geq 1}g_j(x)y^j+y\sum_{j\geq 0}h_j(x)y^j\in(x^{i+1}y^{j+1},x^iy^{j+1}\,;\,i,j\geq 0).$$

さらに

$$x^{i+1}y^{j+1}=x^{i+1}y\cdot y^j,\quad x^iy^{j+1}=x^iy\cdot y^j\in(y,xy,x^2y,\dots)$$

なので $f\in(y,xy,x^2y,\dots)$. 逆に $(y,xy,x^2y,\dots)\subset\mathfrak{m}_0\cap R$ は明らかだから

$$\mathfrak{m}_0\cap R=(y,xy,x^2y,\dots).$$

これが有限生成であったとして，生成元を $f_1,\dots,f_m$ とおく．これらは $y,xy,\dots,x^ny$ で書けるとして良い．この時 $x^{n+1}y\in(y,xy,\dots,x^ny)$ だから $x^{n+1}y=\sum_{j=0}^n x^jy(c_j+yh_j(x,y))$ となる $c_j\in\mathbb{C},h_j\in\mathbb{C}[x,y]$ が存在するが，両辺を y で割って $y=0$ とすると $x^{n+1}=\sum_{j=0}^n c_jx^j$ となって矛盾． □

平成 18 年度 (2005 年 8 月実施)

問 1

集合 A, B に対して，$\mathrm{Map}(A, B)$ で A から B への写像全体のなす集合を表す．正整数 n に対して，$k[X_1, \ldots, X_n]$ を体 k 上の n 変数多項式環とする．$f \in k[X_1, \ldots, X_n]$ に対して，$\varphi(f) \in \mathrm{Map}(k^n, k)$ を

$$\varphi(f)(a_1, \ldots, a_n) = f(a_1, \ldots, a_n) \quad (a_1, \ldots, a_n \in k)$$

で定めることにより，写像 $\varphi : k[X_1, \ldots, X_n] \to \mathrm{Map}(k^n, k)$ を定義する．このとき，各 n に対して次の (i), (ii) の同値関係が成り立つことを証明せよ．

(i) φ が単射 $\iff$ k が無限体

(ii) φ が全射 $\iff$ k が有限体

解答. (i) $\Longrightarrow$: 対偶を示す．$\#k = q$ として $f = X_1^q, g = X_1 \in k[X_1, \ldots, X_n]$ とおくと，任意の $(a_1, \ldots, a_n) \in k^n$ に対し

$$\varphi(f)(a_1, \ldots, a_n) = a_1^q = a_1 = \varphi(g)(a_1, \ldots, a_n)$$

だから $\varphi(f) = \varphi(g)$. よって φ は単射でない．

$\Longleftarrow$: n についての帰納法で示す．φ は環準同型だから，$\varphi(f)$ が零写像ならば $f \equiv 0$ となることを示せば良い．$n = 1$ の時，$\varphi(f)$ が零写像となる $f = \sum_{j \geq 0} f_j X^j \in k[X]$ を取る．$\#k = \infty$ より相異なる $a_0, a_1, \ldots, a_d \in k$ が取れる．この時 $0 = \varphi(f)(a_i) = f(a_i)$ だから

$$\begin{pmatrix} 1 & a_0 & \cdots & a_0^d \\ \vdots & \vdots & & \vdots \\ 1 & a_d & \cdots & a_d^d \end{pmatrix} \begin{pmatrix} f_0 \\ \vdots \\ f_d \end{pmatrix} = 0$$

であるが，左辺の $d+1$ 次行列の行列式は $\prod_{i<j}(a_j - a_i) \neq 0$ なので $f_0 = \cdots = f_d = 0$. 従って φ は単射．$n - 1$ で正しいとする．$X' = (X_1, \ldots, X_{n-1}), a' = (a_1, \ldots, a_{n-1})$ とおく．$\varphi(f)$ が零写像となる $f = \sum_{j \geq 0} f_j(X') X_n^j \in k[X_1, \ldots, X_n]$ を取る．任意の $(a_1, \ldots, a_n) \in k^n$ に対し $0 = \varphi(f)(a', a_n) = \sum_{j=0}^d f_j(a') a_n^j$ であるから，$n = 1$ の時と同様に $f_j(a') = 0$. $f_j \in \mathrm{Map}(k^{n-1}, k)$ だから帰納法の仮定より $f_j = 0$. 従って φ は単射．

(ii) $\Longrightarrow$: 対偶を示す．$\#k = \infty$ とする．$X' = (X_1, \ldots, X_{n-1}), a' = (a_1, \ldots, a_{n-1})$ とおく．

$$f(X) = \begin{cases} 1 & (X_n = 0) \\ 0 & (X_n \neq 0) \end{cases} \in \mathrm{Map}(k^n, k)$$

を取る．$\varphi(g) = f$ となる $g = \sum_{j=0}^d g_j(X') X_n^j \in k[X_1, \ldots, X_n]$ が存在したとする．$\#k = \infty$ より相異なる $a_0, \ldots, a_d \in k \setminus \{0\}$ が取れる．任意の $a' \in k^n$ に対し $g(a', a_i) = \varphi(g)(a', a_i) = f(a', a_i) = 0$ だから

$$\begin{pmatrix} 1 & a_0 & \cdots & a_0^d \\ \vdots & \vdots & & \vdots \\ 1 & a_d & \cdots & a_d^d \end{pmatrix} \begin{pmatrix} g_0(a') \\ \vdots \\ g_d(a') \end{pmatrix} = 0.$$

左辺の $d+1$ 次行列の行列式は 0 でないから $g_0(a') = \cdots = g_d(a') = 0$. ところが $1 = f(a', 0) = \varphi(g)(a', 0) = g_0(a')$ なので矛盾．よって φ は全射でない．

$\Longleftarrow$: $\#k = q$ とし，k の元を $a_1, \ldots, a_q$ とおく．任意に $f \in \mathrm{Map}(k^n, k)$ を取る．この時任意の $(a_{i_1}, \ldots, a_{i_n}) \in k^n$ に対し $\sigma(i_1, \ldots, i_n)$ が存在して $f(a_{i_1}, \ldots, a_{i_n}) = a_{\sigma(i_1, \ldots, i_n)}$ と書ける．今

$$p_i(X) = \prod_{\substack{1 \leq l \leq q \\ l \neq i}} \frac{X - a_l}{a_i - a_l} \in k[X]$$

とおくと $p_i(a_i) = 1, p_i(X) = 0\,(X \neq a_i)$ だから，

$$p_{i_1,\ldots,i_n}(X_1,\ldots,X_n) = \prod_{j=1}^{n} p_{i_j}(X_j) \in k[X_1,\ldots,X_n]$$

は $(X_1,\ldots,X_n) = (a_{i_1},\ldots,a_{i_n})$ の時 1, それ以外の時 0 である．よって

$$g = \sum_{1\leq i_1,\ldots,i_n\leq q} a_{\sigma(i_1,\ldots,i_n)} p_{i_1,\ldots,i_n}(X_1,\ldots,X_n) \in k[X_1,\ldots,X_n]$$

とすれば，任意の $(a_{i_1},\ldots,a_{i_n}) \in k^n$ に対し

$$\varphi(g)(a_{i_1},\ldots,a_{i_n}) = g(a_{i_1},\ldots,a_{i_n}) = a_{\sigma(i_1,\ldots,i_n)} = f(a_{i_1},\ldots,a_{i_n})$$

だから $\varphi(g) = f$. 従って φ は全射．　□

問 2

2 変数多項式環 $\mathbb{C}[x,y]$ の部分環 A が単項的とは，A が単項式で生成されていることとする．1 でない単項式 $v=x^ay^b$ に対して，

$$\mathrm{slope}(v)=b/a\in[0,\infty]$$

とおく．単項的な部分環 $A\,(\mathbb{C}\subsetneq A)$ に対して，次の 2 条件が同値であることを示せ．

(a) A が $\mathbb{C}$ 上有限生成な環である．

(b) 順序集合 $[0,\infty]$ の部分集合 $\{\mathrm{slope}(v)\,|\,v$ は 1 でない A に属する単項式 $\}$ が最大値と最小値を持つ．

解答. $S=\{\mathrm{slope}(v)\,|\,v$ は 1 でない A に属する単項式 $\}$ とおく．

• (a) $\Longrightarrow$ (b)：A の生成元を $v_1,\dots,v_n$ とおく．$\mathrm{slope}(v_1)\le\cdots\le\mathrm{slope}(v_n)$ として良い．非負整数 a,b,c,d,p,q が $a/b\le p/q\le c/d$ を満たすとする．（ただし分母が 0 の時は ∞ とする．）この時

$$\frac{a+p}{b+q}-\frac{a}{b}=\frac{bp-aq}{b(b+q)}=\frac{q}{b+q}\left(\frac{p}{q}-\frac{a}{b}\right)\ge 0,$$
$$\frac{c}{d}-\frac{c+p}{d+q}=\frac{cq-dp}{d(d+q)}=\frac{q}{d+q}\left(\frac{c}{d}-\frac{p}{q}\right)\ge 0$$

だから，

$$\mathrm{slope}(v_i)\le\mathrm{slope}(v_iv_j)\le\mathrm{slope}(v_j).$$

これより帰納的に任意の $i_1\le\cdots\le i_k$ に対し

$$\mathrm{slope}(v_1)\le\mathrm{slope}(v_{i_1})\le\mathrm{slope}(v_{i_1}\cdots v_{i_k})\le\mathrm{slope}(v_{i_k})\le\mathrm{slope}(v_n)$$

となるから，S は最小値 $\mathrm{slope}(v_1)$ と最大値 $\mathrm{slope}(v_n)$ を持つ．

• (b) $\Longrightarrow$ (a)：S の最小値，最大値を取る単項式をそれぞれ x^ay^b,x^cy^d として，$D=ad-bc$ とおく．

(1) $D=0$ の時：$|S|=1$ だから $A=\mathbb{C}[t^{n_1},t^{n_2},\dots]\,(t=x^py^q)$ とおける．よって $\mathbb{C}\subset A\subset\mathbb{C}[t]$ である．任意の monic な $f\in A\setminus\mathbb{C}$ に対し，$f(T)-f(t)\in A[T]$ は monic で $T=t$ を零点に持つから，t は A 上整である．従って $\mathbb{C}[t]$ は $\mathbb{C}$ 代数として有限生成かつ A 上整である．$\mathbb{C}$ は Noether 環なので，A も $\mathbb{C}$ 代数として有限生成となる．

(2) $D>0$ の時：$\mathrm{slope}(x^ay^b)\le\mathrm{slope}(x^py^q)\le\mathrm{slope}(x^cy^d)$ となる任意の $x^py^q\in A\setminus\{1\}$ に対し，$aq-bp,dp-cq\ge 0$ であることと

$$(x^ay^b)^{dp-cq}(x^cy^d)^{aq-bp}=(x^py^q)^{ad-bc}=(x^py^q)^D$$

より

$$\mathbb{C}\subset A\subset B:=\mathbb{C}[(x^ay^b)^{1/D},(x^cy^d)^{1/D}]$$

である．monic な $T^D-x^ay^b\in A[T]$ は $(x^ay^b)^{1/D}$ を零点に持つから，$(x^ay^b)^{1/D}$ は A 上整．$(x^cy^d)^{1/D}$ も同様．よって B は $\mathbb{C}$ 代数として有限生成かつ A 上整だから，A も $\mathbb{C}$ 代数として有限生成となる． □

平成 17 年度 (2004 年 8 月実施)

問 1

この問題では，環は単位元 1 を含む可換環で零環でないものを指す．また，環 A, B に対して，環準同型 $A \to B$ が与えられているとき，B を A 代数と呼ぶ．

環 A に対して，圏 $\mathcal{C}(A)$ を次のように定める．

- $\mathcal{C}(A)$ の対象は，A 代数，
- $\mathcal{C}(A)$ の対象 B, C に対し，射の集合 $\mathrm{Hom}_{\mathcal{C}(A)}(B, C)$ は，A 代数の準同型写像 $B \to C$ 全体．

今，2 つの環 A_1, A_2 と圏同値 $\Phi : \mathcal{C}(A_1) \xrightarrow{\sim} \mathcal{C}(A_2)$ が与えられたとする．(ただし,「圏同値」は「圏の同型」と考えてもよい.) B, C を $\mathcal{C}(A_1)$ の対象，$f \in \mathrm{Hom}_{\mathcal{C}(A_1)}(B, C)$ とするとき，次を示せ．

(i) f が 1 対 1 写像 (injection) ならば $\Phi(f)$ も 1 対 1 写像である．

(ii) f が上への写像 (surjection) ならば $\Phi(f)$ も上への写像である．

(iii) B が体ならば $\Phi(B)$ も体である．

(iv) B が整域ならば $\Phi(B)$ も整域である．

解答. Ψ を Φ の準逆とすると，自然同型 $\eta : \mathrm{id}_{\mathcal{C}(A_1)} \to \Psi \circ \Phi$ が存在し，次の図式は可換．

$$\begin{array}{ccc} B & \xrightarrow[\cong]{\eta_B} & \Psi\Phi(B) \\ \downarrow{\scriptstyle f} & \circlearrowright & \downarrow{\scriptstyle \Psi\Phi(f)} \\ C & \xrightarrow[\cong]{\eta_C} & \Psi\Phi(C) \end{array}$$

(i) 任意に $D \in \mathrm{Ob}(\mathcal{C}(A_2))$ を取る．$g, g' \in \mathrm{Hom}_{\mathcal{C}(A_2)}(D, \Phi(B))$ が $\Phi(f) \circ g = \Phi(f) \circ g'$ を満たすとする．このとき $\Psi\Phi(f) \circ \Psi(g) = \Psi\Phi(f) \circ \Psi(g')$ であることと $\Psi\Phi(f) = \eta_C \circ f \circ \eta_B^{-1}$ が単射であることから $\Psi(g) = \Psi(g')$. よって $g = \Phi\Psi(g) = \Phi\Psi(g') = g'$ となるから $\Phi(f)$ も単射である．

(ii) 任意に $D \in \mathrm{Ob}(\mathcal{C}(A_2))$ を取る．$g, g' \in \mathrm{Hom}_{\mathcal{C}(A_2)}(\Phi(C), D)$ が $g \circ \Phi(f) = g' \circ \Phi(f)$ を満たすとする．このとき $\Psi(g) \circ \Psi\Phi(f) = \Psi(g') \circ \Psi\Phi(f)$ であることと $\Psi\Phi(f)$ が全射であることから $\Psi(g) = \Psi(g')$. よって $g = \Phi\Psi(g) = \Phi\Psi(g') = g'$ となるから $\Phi(f)$ も全射である． □

問 2

p を素数とするとき，アーベル群 $(\mathbb{Z}/p\mathbb{Z}) \oplus (\mathbb{Z}/p^2\mathbb{Z})$ の自己同型群の位数を求めよ．

解答． $G = (\mathbb{Z}/p\mathbb{Z}) \oplus (\mathbb{Z}/p^2\mathbb{Z})$ とおく．$\psi \in \mathrm{Aut}(G)$ を取り，$\psi(1,0) = (a,b), \psi(0,1) = (c,d)$ とおく．$\psi(1,0), \psi(0,1)$ の位数はそれぞれ p, p^2 だから

$$(0,0) = \psi(p,0) = (0,pb), \qquad (0,0) \neq \psi(0,p) = (0,pd),$$

すなわち $p \mid b, p \nmid d$ が必要．また任意の $0 \leq k < p$ に対し $\psi(1,0) \neq \psi(0,kp)$, すなわち $(a,b) \neq (0,kpd)$ である．一方 $p \mid b, p \nmid d$ より $b \equiv kpd \bmod p^2$ となる $0 \leq k < p$ が存在するから，$p \nmid a$ が必要．逆にこれらが成り立つなら ψ は同型となることを示す．

$$S = \{\psi(0,k)\,;\, 0 \leq k < p^2\} = \{(kc,kd)\,;\, 0 \leq k < p^2\}$$

とおくと，$p \nmid d$ より $\#S = p^2$. 今 $\psi(1,0) \in S$ とすると $(a,b) = (kc,kd)$ となる k が存在するが，b,d の仮定から $p \mid k$ だから $p \mid a$ となり矛盾する．よって $\psi(1,0) \notin S$ だから $\#\operatorname{Im}\psi > \#S = p^2$ である．一方 $\#\operatorname{Im}\psi = \#(G/\operatorname{Ker}\psi) = \#G/\#\operatorname{Ker}\psi$ より $\#\operatorname{Im}\psi \mid \#G = p^3$ なので $\#\operatorname{Im}\psi = p^3$. よって ψ は全射．さらに G は有限群だから ψ は単射となり，結局 ψ は同型である．a,b,c,d の選び方はそれぞれ $p-1, p, p, p^2-p$ 通りだから

$$\#\operatorname{Aut}(G) = (p-1)\cdot p \cdot p \cdot (p^2-p) = p^3(p-1)^2.$$

□

問 3

次の (i), (ii), (iii) に答えよ．

(i) R を整域とし，K をその商体とする．f を R の 0 でない元とし，K の部分環で R と $\frac{1}{f}$ で生成されるものを $R[\frac{1}{f}]$ とかく．R 代数の同型

$$R\left[\frac{1}{f}\right] \cong R[x]/(xf-1)$$

を示せ．

(ii) 複素数係数の，0 でない一変数多項式 $f(t)$ に対して，$\mathbb{C}$ 代数 $\mathbb{C}[t][\frac{1}{f}]$ の可逆元全体のなす群の構造を求めよ．

(iii) $\mathbb{C}$ 代数の同型

$$\mathbb{C}[x]\left[\frac{1}{x(x-1)}\right] \cong \mathbb{C}[y]\left[\frac{1}{f(y)}\right]$$

が存在するような y の 0 でない多項式 $f(y)$ を全て求めよ．

解答. (i) R 代数の全射準同型 $\varphi : R[x] \to R[\frac{1}{f}]$ を $\varphi(x) = \frac{1}{f}$ で定める．$g = \sum_{i=0}^{d} g_i x^i \in \operatorname{Ker}\varphi$ とすると $f^d g = \sum_{i=0}^{d} g_j f^{d-i}(fx)^i$ だから $f^d g = h(fx)$ なる $h \in R[x]$ が存在する．この時 $h(1) = f^d g(\frac{1}{f}) = f^d \varphi(g) = 0$ だから $h(x) = (x-1)h_1(x)\,(h_1(x) \in R[x])$ と書ける．よって $f^d g = h(fx) = (xf-1)h_1(fx) \in (xf-1)$ なので

$$g(x) = g(x)(xf-(xf-1))^d = g(x)(x^d f^d + a(x)(xf-1)) \in (xf-1).$$

ここで $a(x) \in R[x]$. 従って $\operatorname{Ker}\varphi \subset (xf-1)$. 逆の包含は明らかなので，準同型定理により示された．

(ii) f の因数分解を $f = c\prod_{j=1}^{d}(t-c_j)^{e_j}$ とする．$\varphi \in \mathbb{C}[t][\frac{1}{f}]$ が可逆元であるとする．$\varphi = g/h\,(g,h \in \mathbb{C}[t])$ と既約分数で表すと，h は f のべきを割り切る．よって h の零点は f の零点である．$\varphi^{-1} = h/g$ だから g についても同様．今 g,h は共通因数を持たないから $\varphi = c'\prod_{j=1}^{d}(t-c_j)^{k_j}\,(c' \neq 0, k_j \in \mathbb{Z})$ と書ける．従って可逆元のなす群は $\mathbb{C}^\times \times \mathbb{Z}^d$ に同型．

(iii) 同型 $\mathbb{C}[x][\frac{1}{x(x-1)}] \cong \mathbb{C}[y][\frac{1}{f(y)}]$ が存在したとすると，可逆元のなす群も同型だから (ii) より

$$f(y) = c(y-a)^n(y-b)^m \quad (a,b \in \mathbb{C}, a \neq b, c \in \mathbb{C}\setminus\{0\}, n,m \in \mathbb{N}_{\geq 1}) \tag{$*$}$$

であることが必要．逆に f がこの形であるとする．$n \geq m$ として良い．同型写像 $y \mapsto (b-a)x+a$ により

$$\begin{aligned}\mathbb{C}[y]\left[\frac{1}{f(y)}\right] &\cong \mathbb{C}[(b-a)x+a]\left[\frac{1}{c(b-a)^{n+m}x^n(x-1)^m}\right]\\ &\cong \mathbb{C}[x]\left[\frac{1}{x^n(x-1)^m}\right] = \mathbb{C}[x]\left[\frac{1}{x(x-1)}\right]\end{aligned}$$

である．ただし最後の等号は，$\frac{1}{x^n(x-1)^m} = \frac{(x-1)^{n-m}}{(x(x-1))^n}$ により $\subset$ が，$\frac{1}{x(x-1)} = \frac{x^{n-1}(x-1)^{m-1}}{x^n(x-1)^m}$ により $\supset$ が成り立つことによる．よって答えは $(*)$ の形のもの全て． □

平成 16 年度 (2003 年 8 月実施)

問 1

G は群とし，H はその真部分群とする．このとき，G の部分集合

$$X_H = \bigcup_{g \in G} gHg^{-1}$$

について，次の (i), (ii) に答えよ．

(i) G が有限群のとき，X_H は G 全体にならないことを証明せよ．

(ii) G が複素 2 次正則行列全体のなす群 $GL_2(\mathbb{C})$ のとき，$X_H = G$ となる真部分群 H を一つ求めよ．

解答. (i) $S = \{gHg^{-1}\,;\, g \in G\}$ とおく．この時

$$xHx^{-1} = yHy^{-1} \Longleftrightarrow y^{-1}xH(y^{-1}x)^{-1} = H \Longleftrightarrow y^{-1}x \in N_G(H)$$

だから，写像 $G/N_G(H) \to S, gN_G(H) \mapsto gHg^{-1}$ は全単射である．これと $N_G(H) \rhd H$ より

$$|S| = |G/N_G(H)| \leq |G/H| = (G : H).$$

$|S| = n$ とおくと $S = \{g_1Hg_1^{-1}, \ldots, g_nHg_n^{-1}\}$ となる $g_1, \ldots, g_n \in G$ が取れる．この時任意の i に対し $e \in g_iHg_i^{-1}$ だから

$$\begin{aligned} |X_H| = \left| \bigcup_{i=1}^{n} g_iHg_i^{-1} \right| &\leq \sum_{i=1}^{n} (|g_iHg_i^{-1}| - 1) + 1 = n(|H| - 1) + 1 \\ &\leq (G : H)(|H| - 1) + 1 = |G| - (G : H) + 1 < |G|. \end{aligned}$$

よって $X_H \neq G$.

(ii)

$$H = \left\{ \begin{pmatrix} \lambda_1 & \mu \\ & \lambda_2 \end{pmatrix} ;\, \lambda_1, \lambda_2 \in \mathbb{C}^\times, \mu \in \mathbb{C} \right\} \subsetneq G$$

とすれば良い．実際，任意の $x, y \in H$ に対し xy^{-1} は対角成分が 0 でない上三角行列だから $xy^{-1} \in H$. すなわち H は G の真部分群である．また，H は任意の正則な Jordan 標準形を含むから，任意の $g \in G$ に対し $p \in G$ があって $p^{-1}gp \in H$. よって $g \in pHp^{-1} \subset X_H$ となり $G \subset X_H$. □

問 2

p は素数とし，$\mathbb{Z}/p^2\mathbb{Z}$ 係数の 1 変数多項式環 $A=(\mathbb{Z}/p^2\mathbb{Z})[T]$ に対して，写像 $\delta : A \to A$ を

$$\delta\Big(\sum_{j\geq 0} c_j T^j\Big) = \sum_{j\geq 0} j c_j T^{j-1}$$

で定める．

(i) $f, g \in A$ に対して

$$\delta(fg) = \delta(f)g + f\delta(g)$$

が成立することを示せ．

(ii) $B = \mathrm{Ker}\,\delta$ が A の部分環であることを示し，剰余環 A/pA における B の像を求めよ．

(iii) B のイデアル $I = (pA) \cap B$ の極小生成系を一つ求めよ．

解答． (i) δ は $\mathbb{Z}/p^2\mathbb{Z}$-線形だから $f = aT^j, g = bT^k$ の時に示せば良い．

$$\delta(f)g + f\delta(g) = ajT^{j-1}\cdot bT^k + aT^j \cdot bkT^{k-1} = ab(j+k)T^{j+k-1} = \delta(abT^{j+k}) = \delta(fg).$$

(ii) 任意の $a, b \in \mathbb{Z}/p^2\mathbb{Z}, f, g \in B$ に対し

$$\begin{cases} \delta(af+bg) = a\delta(f) + b\delta(g) = a\cdot 0 + b\cdot 0 = 0, \\ \delta(fg) = \delta(f)g + f\delta(g) = 0\cdot g + f\cdot 0 = 0 \end{cases}$$

だから $af+bg, fg \in B$. よって B は A の部分環である．$f = \sum_{j\geq 0} c_j T^j \in A$ が $f \in B$ を満たすことは，任意の $j \geq 0$ に対し $p^2 \mid jc_j$ となることと同値だから，$j \in p^2\mathbb{Z}$ の時 c_j は任意，$j \in p\mathbb{Z} \setminus p^2\mathbb{Z}$ の時 $p \mid c_j$, $j \notin p\mathbb{Z}$ の時 $c_j = 0$. よって

$$B = \left\{ f = \sum_{k\geq 0} c_{p^2k} T^{p^2k} + \sum_{k\geq 0, p\nmid k} p c_{pk} T^{pk} \in A \right\}$$

なので，これの A/pA における像は $(\mathbb{Z}/p^2\mathbb{Z})[T^{p^2}]$.

(iii) $f \in I$ は B の元であって A/pA における像が 0 となるものだから，(ii) より

$$f = \sum_{k\geq 0} p c_{pk} T^{pk} = \sum_{j\geq 0}\sum_{k=0}^{p-1} p c_{p(pj+k)} (T^{p^2})^j T^{pk} \in (p, pT^p, \ldots, pT^{(p-1)p}).$$

逆に $(p, pT^p, \ldots, pT^{(p-1)p}) \subset I$ は明らかだから $I = (p, pT^p, \ldots, pT^{(p-1)p})$ である．これが極小生成系でないとすると，ある $0 \leq i \leq p-1$ に対し $g_j(T) = g_{j1}(T) + g_{j2}(T) \in B$ $(g_{j1} \in (\mathbb{Z}/p^2\mathbb{Z})[T^{p^2}], g_{j2} \in p(\mathbb{Z}/p^2\mathbb{Z})[T^p])$ が存在して

$$pT^{ip} = \sum_{\substack{0\leq j\leq p-1 \\ j\neq i}} pT^{jp} g_j(T) = \sum_{\substack{0\leq j\leq p-1 \\ j\neq i}} pT^{jp} g_{j1}(T)$$

と書ける．左辺は T のベキが $ip \bmod p^2$ の項だが，右辺は T のベキが $ip \bmod p^2$ の項を含まないから矛盾．よって $p, pT^p, \ldots, pT^{(p-1)p}$ は I の極小生成系である． □

問 3

整数 $n \geq 2$ に対して $e_n = \exp(\frac{2\pi\sqrt{-1}}{n})$ とおき，複素 2 次元空間 $\mathbb{C}^2$ の自己同型 φ, ψ を以下の式で定める．

$$\begin{aligned} \varphi : &\quad (a,b) \longmapsto (e_n a, e_n^{-1} b) \\ \psi : &\quad (a,b) \longmapsto (b,a). \end{aligned}$$

また，$\mathbb{C}^2$ 上の複素数値多項式関数 $f = f(x,y) : \mathbb{C}^2 \to \mathbb{C}$ 全体のなす $\mathbb{C}$ 上の環を $\mathbb{C}[x,y]$ で表す．このとき，φ と ψ が生成する $\mathbb{C}^2$ の自己同型群 G の元 γ に対して，

$$R_\gamma = \{f \in \mathbb{C}[x,y] \,|\, f \circ \gamma = f\}$$

とおき，この部分環の $\mathbb{C}$ 上の生成元について考える．

(i) R_φ は 3 つの元で生成されることを示し，そのような 3 つの元の組を一つ求めよ．

(ii) 共通部分 $R_\varphi \cap R_\psi$ は 2 つの元で生成されることを示し，そのような元の対 $g(x,y), h(x,y)$ を一つ求めよ．

(iii) (ii) で求めた $g(x,y), h(x,y)$ は次の性質 $(*)$ をみたすことを示せ．

$(*)$ $\mathbb{C}^2$ の点の対 $(a_1,b_1), (a_2,b_2)$ で $g(a_1,b_1) = g(a_2,b_2), h(a_1,b_1) = h(a_2,b_2)$ をみたすものに対して $(a_1,b_1) = \gamma(a_2,b_2)$ となるような G の元 γ が存在する．

解答. (i) $f = \sum c_{jk} x^j y^k \in \mathbb{C}[x,y]$ に対し

$$f \circ \varphi = \sum c_{jk} (e_n x)^j (e_n^{-1} y)^k = \sum c_{jk} e_n^{j-k} x^j y^k$$

だから，$f \in R_\varphi$ となることと $c_{jk} = 0\,(n \nmid (j-k))$ は同値．よって $f \in R_\varphi$ は

$$\begin{aligned} f &= \sum (c_{jk} x^{nj+k} y^k + c'_{jk} x^k y^{nj+k}) \\ &= \sum (c_{jk} (x^n)^j + c'_{jk} (y^n)^j)(xy)^k \in \mathbb{C}[x^n, xy, y^n]. \end{aligned}$$

一方 x^n, xy, y^n が R_φ で不変なことは明らかなので $R_\varphi = \mathbb{C}[x^n, xy, y^n]$. 生成元は x^n, xy, y^n.

(ii)

$$f \circ \psi = \sum c_{jk} y^j x^k = \sum c_{kj} x^j y^k$$

だから，$f \in R_\psi$ となることと $c_{jk} = c_{kj}$ は同値．よって $f \in R_\psi$ は

$$\begin{aligned} f &= \sum_{j \geq 0} c_j x^j y^j + \sum_{j<k} c_{jk} (x^j y^k + x^k y^j) \\ &= \sum_{j \geq 0} c_j (xy)^j + \sum_{j<k} c_{jk} (xy)^j (x^{k-j} + y^{k-j}) \in \mathbb{C}[x+y, xy]. \end{aligned}$$

一方 $x+y, xy$ が R_ψ で不変なことは明らかなので $R_\psi = \mathbb{C}[x+y, xy]$. 従って

$$R_\varphi \cap R_\psi = \mathbb{C}[x^n, xy, y^n] \cap \mathbb{C}[x+y, xy] = \mathbb{C}[x^n + y^n, xy]$$

だから $g(x,y) = x^n + y^n, h(x,y) = xy$.

(iii) $g(a_1,b_1) = g(a_2,b_2), h(a_1,b_1) = h(a_2,b_2)$ とすると $a_1^n + b_1^n = a_2^n + b_2^n, a_1 b_1 = a_2 b_2$ である．

• $a_1 b_1 a_2 b_2 = 0$ の時 : 対称性から $a_1 = 0$ として良い．第 2 式より $a_2 = 0$ または $b_2 = 0$ である．$a_2 = 0$ の時，第 1 式より $b_2 = e_n^k b_1\,(k \in \mathbb{Z})$ と書けるので，

$$(a_1, b_1) = (0, e_n^{-k} b_2) = \varphi^k(0, b_2) = \varphi^k(a_2, b_2).$$

よって $\gamma = \varphi^k$ とすれば良い．$b_2 = 0$ の時，$b_1 = e_n^k a_2\,(k \in \mathbb{Z})$ と書けるので，

$$(a_1, b_1) = (0, e_n^k a_2) = \psi(e_n^k a_2, 0) = \psi\varphi^k(a_2, 0) = \psi\varphi^k(a_2, b_2).$$

よって $\gamma = \psi\varphi^k$ とすれば良い.

• $a_1b_1a_2b_2 \neq 0$ の時：第 2 式より $\frac{a_1}{a_2} = \frac{b_2}{b_1} = \lambda \neq 0$ とおけるから $a_2 = \lambda^{-1}a_1, b_2 = \lambda b_1$. 第 1 式に代入して整理すると $(\lambda^n - 1)(\lambda^{-n}a_1^n - b_1^n) = 0$ である．$\lambda^n = 1$ の時，$\lambda = e_n^k\,(k \in \mathbb{Z})$ と書けるので，

$$(a_1, b_1) = (e_n^k a_2, e_n^{-k} b_2) = \varphi^k(a_2, b_2).$$

よって $\gamma = \varphi^k$ とすれば良い．$\lambda^n \neq 1$ の時，$a_1 = e_n^k \lambda b_1 = e_n^k b_2\,(k \in \mathbb{Z})$ と書けるので，$b_1 = \frac{a_2 b_2}{a_1} = e_n^{-k} a_2$. よって

$$(a_1, b_1) = (e_n^k b_2, e_n^{-k} a_2) = \varphi^k(b_2, a_2) = \varphi^k\psi(a_2, b_2)$$

だから，$\gamma = \varphi^k\psi$ とすれば良い． □

平成 15 年度 (2002 年 8 月実施)

問 1

$\mathbb{C}$ の元 $i = \sqrt{-1}$ と $\sqrt{3}$ を $\mathbb{Q}$ に添加して得られる体 $K = \mathbb{Q}(i, \sqrt{3})$ を考える．K の元 α で，$\alpha^4 = -3$ を満たすものは存在しないことを示せ．

解答． $f(X) = (X^2+1)(X^2-3) \in \mathbb{Q}[X]$ とおく．f は $\mathbb{Q}$ 上分離的．また f の根は $\pm i, \pm\sqrt{3}$ だから K は f の $\mathbb{Q}$ 上最小分解体である．よって $K/\mathbb{Q}$ は正規拡大だから Galois 拡大．拡大次数は $\deg f = 4$ である．K の $\mathbb{Q}$ 上の自己同型 σ, τ を

$$\sigma : \begin{cases} i & \mapsto & -i \\ \sqrt{3} & \mapsto & \sqrt{3} \end{cases} \qquad \tau : \begin{cases} i & \mapsto & i \\ \sqrt{3} & \mapsto & -\sqrt{3} \end{cases}$$

で定めると $\sigma^2 = \tau^2 = 1, \sigma\tau = \tau\sigma$ であり $\langle \sigma, \tau \rangle \subset \mathrm{Gal}(K/\mathbb{Q})$. $\langle \sigma, \tau \rangle$ の元は $\sigma^i \tau^j$ $(0 \le i, j \le 1)$ と書けるから $\#\langle \sigma, \tau \rangle = 4 = \#\mathrm{Gal}(K/\mathbb{Q})$. よって $\mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma, \tau \rangle \cong (\mathbb{Z}/2\mathbb{Z})^2$.

今 $\alpha \in K$ で $\alpha^4 = -3$ となるものがあったとする．$g(X) = X^4 + 3 \in \mathbb{Q}[X]$ は $g(\alpha) = 0$ を満たし，Eisenstein の既約判定法 $(p = 3)$ より $\mathbb{Q}$ 上既約．よって g は α の $\mathbb{Q}$ 上最小多項式である．α の $\mathbb{Q}$ 共役元は $\pm\alpha, \pm\alpha i$ で，$K/\mathbb{Q}$ は正規拡大だから，これらは K に入る．よって α の $\mathbb{Q}$ 上最小分解体 $L := \mathbb{Q}(\alpha, i)$ は K の部分体となり，さらに $L/\mathbb{Q}$ は Galois 拡大で，その拡大次数は $\deg g = 4$ となる．g は $\mathbb{Q}$ 上既約だから $\mu \in \mathrm{Gal}(L/\mathbb{Q})$ で $\mu(\alpha) = -\alpha i, \mu(i) = i$ となるものが存在する．$\mu^2(\alpha) = -\alpha, \mu^3(\alpha) = \alpha i, \mu^4(\alpha) = \alpha$ だから μ の位数は 4. 従って $\mathrm{Gal}(L/\mathbb{Q}) = \langle \sigma \rangle \cong \mathbb{Z}/4\mathbb{Z}$. ところが $[K : \mathbb{Q}] = 4 = [L : \mathbb{Q}]$ だから $K = L$. 従って $\mathrm{Gal}(K/\mathbb{Q}) = \mathrm{Gal}(L/\mathbb{Q})$ となるから，これは矛盾． □

問 2

$\mathbb{C}[x]$ は複素 1 変数多項式環とする．この環の中で $\mathbb{C}$ 上 x^2 と x^3 で生成される部分環を R とする．また，R に属さない多項式 $f(x) \in \mathbb{C}[x]$ をとり，$f(x)$ で生成される $\mathbb{C}[x]$ のイデアルを I とする．このとき，共通部分 $I \cap R$ は R のイデアルとして 2 個の元で生成されることを示せ．また，1 個の元では生成されないことを証明せよ．

解答. $R = \{c + x^2 h(x)\,;\, c \in \mathbb{C}, h \in \mathbb{C}[x]\}$ である．また I は $\mathbb{C}[x]$ のイデアルだから $f = f_0 + x + x^2 f_2(x)\,(f_0 \in \mathbb{C}, f_2 \in \mathbb{C}[x])$ とおける．$fg \in I$ を取る．$g = g_0 + g_1 x + x^2 g_2(x)\,(g_0, g_1 \in \mathbb{C}, g_2 \in \mathbb{C}[x])$ とおくと，$fg \in R$ であることは fg の x の係数 $f_0 g_1 + g_0$ が 0 であることと同値だから

$$\begin{aligned} I \cap R &= \{f(-f_0 g_1 + g_1 x + x^2 g_2)\,;\, g_1 \in \mathbb{C}, g_2 \in \mathbb{C}[x]\} \\ &= \left\{ g_1 f(-f_0 + x) + \sum_{j \geq 0} g_{2,j} f x^{j+2} \right\}. \end{aligned}$$

ここで $fx^2 \in (f(-f_0 + x), fx^2), fx^{k+1} = f(-f_0 + x)x^k + fx^k \cdot f_0$ より帰納的に任意の $k \geq 2$ に対し $fx^k \in (f(-f_0 + x), fx^2)$ だから $I \cap R \subset (f(-f_0 + x), fx^2)$. 逆の包含は明らかだから

$$I \cap R = (f(-f_0 + x), fx^2).$$

これが単項イデアルであったとして，生成元を $h \in \mathbb{C}[x] \setminus \{0\}$ とする．

- $f_0 \neq 0$ の時：$f(-f_0 + x), fx^2 \in I \cap R$ より h は $f(-f_0 + x), fx^2$ を割り切る．よって h は $f_0^2 f = fx^2 - f(-f_0 + x)(f_0 + x)$ を割り切るから $(f) \subset (h) = I \cap R$. これは $f \notin R$ に矛盾．
- $f_0 = 0$ の時：$xf = hh_1, x^2 f = hh_2\,(h_1, h_2 \in R)$ と書けるから $hh_2 = xhh_1$. よって $xh_1 = h_2 \in R$ だから h_1 の定数項は 0. 従って $h_1 = x^2 h_1'\,(h_1' \in \mathbb{C}[x])$ と書ける．この時 $f = xhh_1'$ だから $(h) = (fx, fx^2) = (x^2 hh_1', x^3 hh_1') \subset x^2 h\mathbb{C}[x]$. よって $h \in x^2 h\mathbb{C}[x]$ となって矛盾． □

平成 14 年度 (2001 年 8 月実施)

問 1

整数 $n \geq 1$ に対して，1 の原始 n 乗根を

$$\zeta_n = e^{\frac{2\pi\sqrt{-1}}{n}} \in \mathbb{C}$$

と書く．このとき，

(i) ζ_n を有理数体 $\mathbb{Q}$ に添加して得られる体 $\mathbb{Q}(\zeta_n)$ が，$\mathbb{Q}$ の有限次アーベル拡大になることを示せ．

(ii) 体 $\mathbb{Q}(\zeta_n)$ の元 x で $x^3 = 5$ を満たすものがないことを示せ．

解答. (i) $K = \mathbb{Q}(\zeta_n)$ とおく．$f(X) = X^n - 1 \in \mathbb{Q}[X]$ とおくとこれは $\mathbb{Q}$ 上分離的．根は $1, \zeta_n, \ldots, \zeta_n^{n-1}$ だから K は f の $\mathbb{Q}$ 上最小分解体．よって $K/\mathbb{Q}$ は正規拡大なので有限次 Galois 拡大．$\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ に対し $\sigma(\zeta_n)$ は 1 の原始 n 乗根だから，$i(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^\times$ があって $\sigma(\zeta_n) = \zeta_n^{i(\sigma)}$ と書ける．任意の $\sigma, \tau \in \mathrm{Gal}(K/\mathbb{Q})$ に対し

$$\begin{aligned}\sigma\tau(\zeta_n) &= \sigma(\zeta_n^{i(\tau)}) = \sigma(\zeta_n)^{i(\tau)} = (\zeta_n^{i(\sigma)})^{i(\tau)} \\ &= (\zeta_n^{i(\tau)})^{i(\sigma)} = \tau(\zeta_n)^{i(\sigma)} = \tau(\zeta_n^{i(\sigma)}) = \tau\sigma(\zeta_n)\end{aligned}$$

だから $\sigma\tau = \tau\sigma$. よって $\mathrm{Gal}(K/\mathbb{Q})$ は Abel 群であり，位数は $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$ で有限.

(ii) (i) より $G := \mathrm{Gal}(K/\mathbb{Q})$ は有限 Abel 群なので，任意の G の部分群は正規かつ Abel．よって $K/\mathbb{Q}$ の中間拡大は全て Abel 拡大．今 $x^3 = 5$ なる $x \in K$ が存在したとする．$f(X) = X^3 - 5 \in \mathbb{Q}[X]$ は Eisenstein の既約判定法 ($p = 5$) により $\mathbb{Q}$ 上既約．また $f(x) = 0$ だから f は x の Q 上最小多項式である．$K/\mathbb{Q}$ は Galois 拡大だから，x の $\mathbb{Q}$ 共役元 $x, \zeta_3 x, \zeta_3^2 x$ は K の元．よって x の $\mathbb{Q}$ 上最小分解体 $L := \mathbb{Q}(x, \zeta_3) = \mathbb{Q}(a, \zeta_3)\,(a = 5^{1/3})$ は K の部分体となるから，$L/\mathbb{Q}$ は Abel 拡大となる．今 $\sigma, \tau \in \mathrm{Gal}(L/\mathbb{Q})$ を

$$\sigma : \begin{cases} a & \mapsto & a \\ \zeta_3 & \mapsto & \zeta_3^2 \end{cases} \qquad \tau : \begin{cases} a & \mapsto & a\zeta_3 \\ \zeta_3 & \mapsto & \zeta_3 \end{cases}$$

で定めると $\sigma^2 = \tau^3 = 1, \sigma^{-1}\tau\sigma = \tau^2$ であり，$\langle \sigma, \tau \rangle \subset \mathrm{Gal}(L/\mathbb{Q})$. ところが左辺の位数は 6, 右辺の位数は $[L : \mathbb{Q}] = [L : \mathbb{Q}(a)][\mathbb{Q}(a) : \mathbb{Q}] = 2 \cdot 3 = 6$ だから，包含は等号が成立し

$$\mathrm{Gal}(L/\mathbb{Q}) = \langle \sigma, \tau | \sigma^2 = \tau^3 = 1, \sigma^{-1}\tau\sigma = \tau^2 \rangle .$$

これは Abel 群でないから矛盾. □

問 2

素数 $p>2$ に対して，p 個の元からなる有限体を，$\mathbb{F}_p$ と書く．なお，$\mathbb{F}_p$ の元を成分とする，行列式が 1 となる 2×2 行列全体が,（掛け算に関して）成す行列群を

$$SL_2(\mathbb{F}_p)=\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}\,;\,a,b,c,d\in\mathbb{F}_p,\det\begin{pmatrix}a & b\\ c & d\end{pmatrix}=1\right\}$$

と表す．以下では，位数 2 の巡回群への準同型

$$\varphi : SL_2(\mathbb{F}_p)\to\mathbb{Z}/2\mathbb{Z}$$

が与えられたとして，その核 $K=\mathrm{Ker}(\varphi)$ について考える．

(i) K は必ず部分群

$$U=\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in SL_2(\mathbb{F}_p)\,;\,a=d=1,c=0\right\}\subseteq SL_2(\mathbb{F}_p)$$

とそのすべての $SL_2(\mathbb{F}_p)$ 共役を含むことを示せ．

(ii) 任意の $(x,y)\in\mathbb{F}_p\times\mathbb{F}_p$（ただし，$(x,y)\neq(0,0)$ とする）に対して，

$$T\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}x\\y\end{pmatrix}$$

を満たす $T\in K$ が存在することを示せ．

(iii) K は必ず $SL_2(\mathbb{F}_p)$ 全体となることを示せ．

解答． (i) $\varphi(I)=\varphi(I^2)=2\varphi(I)=0$ だから

$$\varphi\left(\begin{pmatrix}1 & b\\ & 1\end{pmatrix}\right)=p\varphi\left(\begin{pmatrix}1 & b\\ & 1\end{pmatrix}\right)=\varphi\left(\begin{pmatrix}1 & b\\ & 1\end{pmatrix}^p\right)=\varphi\left(\begin{pmatrix}1 & bp\\ & 1\end{pmatrix}\right)=\varphi(I)=0.$$

よって $U\subset K$. また任意の $x\in U,g\in SL_2(\mathbb{F}_p)$ に対し $\varphi(g^{-1}xg)=-\varphi(g)+\varphi(x)+\varphi(g)=0$ だから $g^{-1}Ug\subset K$.

(ii) $T=\left(\begin{smallmatrix}x & b\\ y & d\end{smallmatrix}\right)$ とおける．

• $y=0$ の時：

• $y\neq 0$ の時：(i) より $T=gug^{-1}$ となる $b,d\in\mathbb{F}_p,u\in U,g\in SL_2(\mathbb{F}_p)$ が存在することを示せば良い．この両辺の $\mathrm{tr},\det$ を取ると $x+d=2,dx-by=1$. よって $d=2-x,b=-(x-1)^2y^{-1}$ だから

$$T=\begin{pmatrix}x & -(x-1)^2y^{-1}\\ y & 2-x\end{pmatrix}.$$

ここで $v_1=\left(\begin{smallmatrix}x-1\\ y\end{smallmatrix}\right),v_2=\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$ とおくと $Tv_1=v_1,Tv_2=v_1+v_2$ だから，

$$T(v_1,-y^{-1}v_2)=(v_1,-y^{-1}v_1-y^{-1}v_2)=(v_1,-y^{-1}v_2)\begin{pmatrix}1 & -y^{-1}\\ & 1\end{pmatrix}.$$

$\det(v_1,-y^{-1}v_2)=1$ であるから示された．

(iii) $SL_2(\mathbb{F}_p)\subset K$ を示せば良い．任意に $g=\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)\in SL_2(\mathbb{F}_p)$ を取る．$\left(\begin{smallmatrix}a\\c\end{smallmatrix}\right)\neq 0$ だから，(ii) より $T\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)=\left(\begin{smallmatrix}a\\c\end{smallmatrix}\right)$ となる $T\in K$ が存在する．$\left(\begin{smallmatrix}b'\\d'\end{smallmatrix}\right)=T^{-1}\left(\begin{smallmatrix}b\\d\end{smallmatrix}\right)$ とおくと $g=T\left(\begin{smallmatrix}1 & b'\\ & d'\end{smallmatrix}\right)$. 両辺の det を取ると $d'=1$ だから，$g=Tu\,(u\in U)$. よって $\varphi(g)=\varphi(T)+\varphi(u)=0$ だから $g\in K$. □

問 3

方程式 $y^2 = x^2 - x^3$ に関連する，次の各問に答えよ．

(i) 多項式 $f, g \in \mathbb{R}[t]$ であって，写像

$$\alpha(t) = (f(t), g(t)) : \mathbb{R} \to \mathbb{R}^2$$

が次の 3 条件を全て満たす f, g を 1 組求めよ．

(1) $\alpha(1) = \alpha(-1) = (0, 0)$,

(2) 任意の $t \in \mathbb{R}$ に対して，$g(t)^2 = f(t)^2 - f(t)^3$,

(3) $x \neq 0, y^2 = x^2 - x^3$ を満たす任意の $(x, y) \in \mathbb{R}^2$ に対して $\alpha^{-1}(x, y)$ がちょうど 1 点からなる．

(ii) 一変数多項式環の部分環 $A = \{h \in \mathbb{R}[t]\,;\, h(1) = h(-1)\}$ に対して，環としての同型写像

$$\mathbb{R}[x, y]/(y^2 - x^2 + x^3) \to A$$

を 1 つ求めよ．

解答. (i) $f(t) = 1-t^2, g(t) = t(1-t^2)$ が条件を満たすことを示す．(1), (2) は明らか．$x \neq 0, y^2 = x^3 - x^2$ なる $(x, y) \in \mathbb{R}^2$ を任意に取る．この時 $\alpha(s) = \alpha(t) = (x, y)$ となる s, t が存在したとすると

$$\begin{cases} 1 - s^2 = 1 - t^2 = x \\ s(1 - s^2) = t(1 - t^2) = y. \end{cases}$$

よって $sx = tx = y$ となるから $s = y/x = t$. 従って (3) も満たす．

(ii) $h \in A$ は，$c \in \mathbb{R}$ が存在して $h(t) - c$ が $t = \pm 1$ を零点に持つから

$$A = \{(1 - t^2)h(t) + c\,;\, h(t) \in \mathbb{R}[t], c \in \mathbb{R}\}.$$

環準同型 $\varphi : \mathbb{R}[x, y] \to \mathbb{R}[t]$ を $\varphi(x) = 1 - t^2, \varphi(y) = t(1 - t^2)$ で定める．$\operatorname{Im}\varphi \subset A$ は明らか．また任意の $(1 - t^2)h(t) + c \in A$ に対し $h_0, h_1 \in \mathbb{R}[t]$ が一意に存在して $h(t) = h_0(t^2) + th_1(t^2)$ と書ける．そこで $f = yh_1(1 - x) + xh_0(1 - x) + c$ とおけば

$$\varphi(f)(t) = t(1 - t^2)h_1(t^2) + (1 - t^2)h_0(t^2) + c = (1 - t^2)h(t) + c$$

だから $A \subset \operatorname{Im}\varphi$. また $f \in \operatorname{Ker}\varphi$ を $y^2 - x^2 + x^3$ で割った余りを $yf_1(x) + f_0(x)$ とすると $t(1 - t^2)f_1(1 - t^2) + f_0(1 - t^2) = 0$ であるが，左辺第 1 項，第 2 項の次数はそれぞれ奇数，偶数だから $f_1(x) = f_0(x) = 0$. よって $\operatorname{Ker}\varphi \subset (y^2 - x^2 + x^3)$. 逆の包含は明らか．従って準同型定理より示すべき同型が得られる． □

平成 13 年度 (2000 年 8 月実施)

問 1

$f(x)$ を $\mathbb{Q}$ 上の奇数次既約多項式とする．今，方程式 $f(x)=0$ の $\mathbb{C}$ における根 α を 1 つとったとき，$\mathbb{Q}(\alpha)$ が $\mathbb{Q}$ 上の Galois 拡大になったとする．このとき，$f(x)=0$ のすべての根は実根であることを示せ．

解答. f が $\mathbb{Q}$ 上既約だから，f は α の $\mathbb{Q}$ 上最小多項式である．よって $\#\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) = [\mathbb{Q}(\alpha):\mathbb{Q}] = \deg f$ は奇数である．$\sigma:\mathbb{C}\to\mathbb{C}$ を複素共役 $\sigma(z)=\bar{z}$ とする．$f\in\mathbb{Q}[x]$ は σ で不変だから，f の根の集合も σ で不変である．これと $\sigma|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$ より $\sigma\in\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ となる．f の根に実根でないものがあるとすると，$\mathbb{Q}(\alpha)/\mathbb{Q}$ が Galois 拡大であることから $\mathbb{R}\subsetneq\mathbb{Q}(\alpha)$. よって σ の位数は 2 であるから，$\#\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ が奇数であることに矛盾． □

問 2

$n, d \geq 1$ とする．変数 $x = (x_1, \ldots, x_n)$ についての実係数の d 次多項式 $f(x)$ が与えられたとし，変数 $y_i = (y_{i1}, \ldots, y_{in})\,(i = 1, \ldots, d)$ を導入する．$x, y_1, \ldots, y_d$ についての多項式

$$F(x, y_1, \ldots, y_d) = \sum_{a_1=0}^{1} \cdots \sum_{a_d=0}^{1} (-1)^{d-(a_1+\cdots+a_d)} f(x + a_1 y_1 + \cdots a_d y_d)$$

を定義する．例えば，$d = 1, 2$ の場合には，

$$F = f(x + y_1) - f(x) \qquad (d = 1)$$
$$F = f(x + y_1 + y_2) - f(x + y_1) - f(x + y_2) + f(x) \qquad (d = 2)$$

である．

以下を示せ．

(i) $F(x, y_1, \ldots, y_d)$ は（0 でない）d 次斉次式である．

(ii) $F(x, y_1, \ldots, y_d)$ は x によらない．

(iii) $F(x, y_1, \ldots, y_d)$ は各 i に対して他の変数をパラメータと見て $y_i = (y_{i1}, \ldots . y_{in})$ だけの多項式と考えると，(0 でない）1 次斉次式である．

解答． (i) $\alpha = (\alpha_1, \ldots . \alpha_n) \in \mathbb{N}_0^n$ に対し $|\alpha| = \alpha_1 + \cdots + \alpha_n, x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ などと定める．$|\alpha| < d$ ならば

$$\sum_{a_i \in \{0,1\}} (-1)^{d-(a_1+\cdots+a_d)} (x + a_1 y_1 + \cdots + a_d y_d)^\alpha = 0 \qquad (*)$$

となることを d についての帰納法で示す．$d = 1$ の時は $\alpha = 0$ だから左辺は $\sum_{a_1=0}^{1} (-1)^{1-a_1} = 0$ となり正しい．$d - 1$ で正しいとする．$|\alpha| < d$ となる任意の $\alpha \in \mathbb{N}_0^n$ を取る．$e_1 = (1, 0, \ldots, 0)$ とおくと

$$\begin{aligned}
&\frac{\partial}{\partial y_{1j}} \sum_{a_i} (-1)^{d-(a_1+\cdots+a_d)} (x + a_1 y_1 + \cdots + a_d y_d)^\alpha \\
=&\sum_{a_i} (-1)^{d-(a_1+\cdots+a_d)} a_1 \alpha_j (x + a_1 y_1 + \cdots + a_d y_d)^{\alpha - e_1} \\
=&\alpha_j \sum_{a_i\ (i \neq 1)} (-1)^{d-1-(a_2+\cdots+a_d)} (x + y_1 + a_2 y_2 + \cdots + a_d y_d)^{\alpha - e_1} = 0.
\end{aligned}$$

最後の等号は，$(x + y_1 + a_2 y_2 + \cdots + a_d y_d)^{\alpha - e_1}$ の次数が $|\alpha| - 1 < d - 1$ で，$x + y_1$ を一つの変数と見ると帰納法の仮定が使えることによる．y_{kj} についての微分も同様だから，$(*)$ の左辺は $y_1, \ldots, y_d$ によらない．$y_1 = \cdots = y_d = 0$ とすると $(*)$ の左辺は

$$\sum_{a_i} (-1)^{d-(a_1+\cdots+a_d)} x^\alpha = \prod_{i=1}^{d} \sum_{a_i=0}^{1} (-1)^{1-a_i} x^\alpha = \prod_{i=1}^{d} 0 \cdot x^\alpha = 0$$

だから d でも正しい．これで示せた．これより $f(x) = \sum_{m=0}^{d} \sum_{|\alpha|=m} f_\alpha x^\alpha$ に対し

$$F = \sum_{|\alpha|=d} f_\alpha \sum_{a_i} (-1)^{d-(a_1+\cdots+a_d)} (x + a_1 y_1 + \cdots + a_d y_d)^\alpha$$

であるから F は d 次斉次．

(ii) (i) と同様に e_j を定めると

$$\frac{\partial F}{\partial x_j} = \sum_{|\alpha|=d} f_\alpha \sum_{a_i} (-1)^{d-(a_1+\cdots+a_d)} \alpha_j (x + a_1 y_1 + \cdots + a_d y_d)^{\alpha - e_j} = 0$$

である．最後の等号は $|\alpha - e_j| = |\alpha| - 1 = d - 1$ と $(*)$ による．よって F は x によらない．

(iii) (i) より $f(x)=x^\alpha\,(|\alpha|=d)$ の場合に示せば良い．(ii) より

$$
\begin{aligned}
F=&\sum_{a_i}(-1)^{d-(a_1+\cdots+a_d)}(a_1y_1+\cdots+a_dy_d)^\alpha=\sum_{a_i}(-1)^{d-(a_1+\cdots+a_d)}\prod_{j=1}^{n}(a_1y_{1j}+\cdots+a_dy_{dj})^{\alpha_j}\\
=&\sum_{a_i}(-1)^{d-(a_1+\cdots+a_d)}\prod_{j=1}^{n}\sum_{k_j=0}^{\alpha_j}\binom{\alpha_j}{k_j}(a_1y_{1j})^{k_j}(a_2y_{2j}+\cdots+a_dy_{dj})^{\alpha_j-k_j}\\
=&\sum_{a_i}(-1)^{d-(a_1+\cdots+a_d)}\sum_{0\le k_j\le\alpha_j}\prod_{j=1}^{n}\binom{\alpha_j}{k_j}(a_1y_{1j})^{k_j}(a_2y_{2j}+\cdots+a_dy_{dj})^{\alpha_j-k_j}\\
=&\sum_{0\le k_j\le\alpha_j}\prod_{j=1}^{n}\binom{\alpha_j}{k_j}\underbrace{\sum_{a_1=0}^{1}(-1)^{1-a_1}\prod_{j=1}^{n}(a_1y_{1j})^{k_j}}_{(1)}\\
&\times\underbrace{\sum_{a_i\,(i\neq1)}(-1)^{d-1-(a_2+\cdots+a_d)}\prod_{j=1}^{n}(a_2y_{2j}+\cdots+a_dy_{dj})^{\alpha_j-k_j}}_{(2)}
\end{aligned}
$$

である．$k_1=\cdots=k_n=0$ なら (1) は 0 に等しく，$k_1+\cdots+k_n>1$ なら $(*)$ で $x=0$ とした式から (2) は 0 に等しい．よって $k_1+\cdots+k_n=1$ の項のみ残る．$k_1=1,k_2=\cdots=k_n=0$ の項は

$$
\begin{aligned}
&\alpha_1\sum_{a_1=0}^{1}(-1)^{1-a_1}a_1y_{11}\cdot\sum_{a_i\,(i\neq1)}(-1)^{d-1-(a_2+\cdots+a_d)}\prod_{j=1}^{n}(a_2y_{2j}+\cdots+a_dy_{dj})^{\alpha_j-k_j}\\
=&\alpha_1y_{11}\times(y_2,\ldots,y_d\text{ の多項式})
\end{aligned}
$$

である．他も同様なので

$$F=\sum_{j=1}^{n}\alpha_jy_{1j}\times(y_2,\ldots,y_d\text{ の多項式}).$$

これは y_1 のみの多項式と見ると 1 次斉次．他の y_j についても同様． □

問 3A

複素 $2n-1$ 次元射影空間 $\mathbb{P}^{2n-1}$ とその斉次座標 $(x_0 : \cdots : x_{2n-1})$ を考える．今，2 つの $n-1$ 次元線形部分空間 $L_1, L_2 \subseteq \mathbb{P}^{2n-1}$ が交わらない（$L_1 \cap L_2 = \emptyset$）と仮定する．このとき，ある正則対称行列 $B \in GL(2n, \mathbb{C})$, ${}^tB = B$ が存在して

$$\left\{ (x_0 : \cdots : x_{2n-1}) \in \mathbb{P}^{2n-1} ; (x_0, \ldots, x_{2n-1}) B \begin{pmatrix} x_0 \\ \vdots \\ x_{2n-1} \end{pmatrix} = 0 \right\}$$

が $L_1 \cup L_2$ を含むことを示せ．

解答. 座標は縦ベクトルで書くことにする．L_1, L_2 は，$v_1, \ldots, v_{2n} \in \mathbb{C}^{2n}$ を用いて

$$L_1 = \{[x_1 v_1 + \cdots + x_n v_n] \in \mathbb{P}^{2n-1} ; (x_1, \ldots, x_n) \in \mathbb{C}^n \setminus (0, \ldots, 0)\},$$
$$L_2 = \{[x_{n+1} v_{n+1} + \cdots + x_{2n} v_{2n}] \in \mathbb{P}^{2n-1} ; (x_{n+1}, \ldots, x_{2n}) \in \mathbb{C}^n \setminus (0, \ldots, 0)\}$$

と書ける．ただし $\operatorname{rank}(v_1, \ldots, v_n) = \operatorname{rank}(v_{n+1}, \ldots, v_{2n}) = n$. また，[ ] で $\mathbb{C}^{2n}$ の点を $\mathbb{P}^{2n-1}$ の斉次座標とみなしている．$v_1, \ldots, v_n$ が張る $\mathbb{C}^{2n}$ の線形部分空間を L_1' とおく．L_2' も同様に定める．$L_1 \cap L_2 = \emptyset$ だから $L_1' \cap L_2' = \{0\}$. よって

$$\dim(L_1' \cup L_2') = \dim L_1' + \dim L_2' - \dim(L_1' \cap L_2') = 2n$$

なので $v_1, \ldots, v_{2n}$ は $\mathbb{C}$ 上一次独立．従ってこれらは $\mathbb{C}^{2n}$ の基底となるので，$P(v_1, \ldots, v_{2n}) = I_{2n}$ となる $P \in GL(2n, \mathbb{C})$ が一意に存在する．この時 Pv_i は基本列ベクトル e_i である．ここで

$$B = {}^tP \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix} P$$

とおくと，これは正則対称行列である．また，任意の $1 \le i, j \le n$ に対し

$${}^t v_i B v_j = {}^t v_i {}^t P \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix} P v_j = {}^t e_i \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix} e_j = 0$$

だから，任意の $v \in L_1$ に対し ${}^t v B v = 0$. 同様に任意の $n+1 \le i, j \le 2n$ に対し ${}^t v_i B v_j = 0$ だから，任意の $v \in L_2$ に対し ${}^t v B v = 0$. これで示された． □

問 3B

複素 n 変数形式的べき級数環 $R = \mathbb{C}[\![x_1, \ldots, x_n]\!]$ 上の有限生成加群 M, N を考える．もし $M \otimes_R N$ が R 加群として R と同型ならば，M および N も R と同型になることを示せ．

解答． R は局所環だから唯一つの極大イデアル $\mathfrak{m}$ を持つ．剰余体を $k = R/\mathfrak{m}$ とおく．

$$\begin{aligned}(M/\mathfrak{m}M) \otimes_k (N/\mathfrak{m}N) &\cong (k \otimes_R M) \otimes_k (k \otimes_R N) \cong ((k \otimes_R M) \otimes_k k) \otimes_R N \\ &\cong (k \otimes_R M) \otimes_R N \cong k \otimes_R (M \otimes_R N) \cong k \otimes_R R \cong k\end{aligned}$$

であるから，$\dim_k M/\mathfrak{m}M = d_1, \dim_k N/\mathfrak{m}N = d_2$ とおいて両辺の $\dim_k$ を比較すると $d_1 d_2 = 1$. よって $d_1 = d_2 = 1$. $a \in M$ を $M/\mathfrak{m}M$ の生成元とすると，中山の補題より a は M の生成元となるから $M = aR$. $\varphi : R \to aR$ を $\varphi(x) = ax$ で定めるとこれは全射．よって R のイデアル $\mathrm{Ker}\,\varphi$ を I_1 とおくと $M = aR \cong R/I_1$. 同様に R のイデアル I_2 が存在して $N \cong R/I_2$. 従って

$$R \cong M \otimes_R N \cong (R/I_1) \otimes_R (R/I_2) \cong R/(I_1 + I_2)$$

なので $I_1 + I_2 = 0$. よって $I_1 = I_2 = 0$ なので $M \cong N \cong R$. □

平成 12 年度 (1999 年 8 月実施)

問 1

ω を $\mathbb{C}$ における 1 の原始 3 乗根 $e^{2\pi\sqrt{-1}/3}$ とし，不定元 t によって生成される $\mathbb{Q}(\omega)$ 上の一変数有理関数体を L とする：$L=\mathbb{Q}(\omega)(t)$. さらに，L の部分体 $\mathbb{Q}(t^3)$ を K とおく．

(i) L が K 上の Galois 拡大であることを示せ．

(ii) 拡大 L/K の Galois 群 $\mathrm{Gal}(L/K)$ が，有限体 $\mathbb{F}_3(=\mathbb{Z}/3\mathbb{Z})$ 上の 2 次正方可逆行列のなす群

$$\left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \middle| \, a \neq 0 \right\}$$

と同型であることを示せ．

解答. (i) $f(X)=X^3-t^3\in K[X]$ とおくと，これは K 上既約で $f(t)=0$ だから t の K 上最小多項式．また K 上分離的．t の K 共役元は $t,\omega t,\omega^2 t$ だから，f の K 上最小分解体は $K(t,\omega)=\mathbb{Q}(\omega,t)=L$. よって L/K は正規拡大だから Galois 拡大．拡大次数は $[L:K]=[L:\mathbb{Q}(t)][\mathbb{Q}(t):K]=2\cdot 3=6$.

(ii) 同型を示すべき 2 次行列の群を G とおく．$\sigma\in\mathrm{Gal}(L/K)$ を取る．ω の K 共役元は ω,ω^2, t の K 共役元は $t,\omega t,\omega^2 t$ なので，$j(\sigma)\in\mathbb{F}_3^\times, k(\sigma)\in\mathbb{F}_3$ があって $\sigma(\omega)=\omega^{j(\sigma)}, \sigma(t)=\omega^{k(\sigma)}t$ と書ける．$\sigma,\tau\in\mathrm{Gal}(L/K)$ に対し

$$\begin{cases} \tau\sigma(\omega)=\tau(\omega^{j(\sigma)})=\tau(\omega)^{j(\sigma)}=\omega^{j(\tau)j(\sigma)} \\ \tau\sigma(t)=\tau(\omega^{k(\sigma)}t)=\tau(\omega)^{k(\sigma)}\omega^{k(\tau)}t=\omega^{j(\tau)k(\sigma)+k(\tau)}t \end{cases}$$

なので $j(\tau\sigma)=j(\tau)j(\sigma), k(\tau\sigma)=j(\tau)k(\sigma)+k(\tau)$. ここで $\Phi:\mathrm{Gal}(L/K)\to G$ を $\Phi(\sigma)=\left(\begin{smallmatrix} j(\sigma) & k(\sigma) \\ & 1 \end{smallmatrix}\right)$ で定義すると

$$\begin{aligned} \Phi(\tau)\Phi(\sigma) &= \begin{pmatrix} j(\tau) & k(\tau) \\ & 1 \end{pmatrix}\begin{pmatrix} j(\sigma) & k(\sigma) \\ & 1 \end{pmatrix} = \begin{pmatrix} j(\tau)j(\sigma) & j(\tau)k(\sigma)+k(\tau) \\ & 1 \end{pmatrix} \\ &= \begin{pmatrix} j(\tau\sigma) & k(\tau\sigma) \\ & 1 \end{pmatrix} = \Phi(\tau\sigma) \end{aligned}$$

だから Φ は準同型．さらに $\#G=2\cdot 3=6=[L:K]=\#\mathrm{Gal}(L/K)$ だから Φ は同型である．これで示された． □

問 2

a, b を整数とする．0 でない複素数 t の 4 次元アフィン空間への作用を

$$(x, y, z, u) \mapsto (tx, t^a y, t^b z, t^{-1} u)$$

により定める．そのとき，すべての t により不変な x, y, z, u の $\mathbb{C}$ 係数の多項式の全体を $A(a, b)$ とし，そのイデアル $I(a, b)$ を

$$\{f \in A(a, b) \mid f(0, 0, 0, 0) = 0\}$$

で定義する．

(i) 環 $A(1, -1)$ とイデアル $I(1, -1)$ を計算せよ．

(ii) $a, b \geq 0$ のとき，

$$\dim_{\mathbb{C}} I(a, b)/I(a, b)^2 = 3$$

を示せ．

(iii) $b = -2$ のとき，$\dim_{\mathbb{C}} I(a, b)/I(a, b)^2 = 4$ となる正の整数 a をすべて求めよ．

解答. $f = \sum f_{ijkl} x^i y^j z^k u^l \in \mathbb{C}[x, y, z, u]$ に対し問題の作用をさせると $\sum f_{ijkl} t^{i+aj+bk-l} x^i y^j z^k u^l$ となるから，$f \in A(a, b)$ となることは $f_{ijkl} = 0\,(i + aj + bk - l \neq 0)$ と同値．

(i) $i + j = k + l$ の $\mathbb{N}^4_{\geq 0}$ における解は $(1, 0, 1, 0), (1, 0, 0, 1), (0, 1, 1, 0), (0, 1, 0, 1)$ で張られるから，$A(1, -1)$ は xz, xu, yz, yu で生成される．よって

$$A(1, -1) = \mathbb{C}[xz, xu, yz, yu], \quad I(1, -1) = (xz, xu, yz, yu).$$

(ii) $i + aj + bk - l = 0$ の時 $x^i y^j z^k u^l = (xu)^i (yu^a)^j (zu^b)^k$ だから

$$A(a, b) = \mathbb{C}[xu, yu^a, zu^b], \quad I(a, b) = (xu, yu^a, zu^b).$$

よって $\dim_{\mathbb{C}} I(a, b)/I(a, b)^2 \leq 3$. 今 $c_1, c_2, c_3 \in \mathbb{C}$ が $c_1 xu + c_2 yu^a + c_3 zu^b \in I(a, b)^2$ を満たすとする．$y = z = 0$ とすると $c_1 xu \in (x^2 u^2)$ となるから $c_1 = 0$. 同様に $c_2 = c_3 = 0$ となるから xu, yu^a, zu^b は $\mathbb{C}$ 上一次独立．従って $\dim_{\mathbb{C}} I(a, b)/I(a, b)^2 \geq 3$ なので示された．

(iii) • $a = 2n + 1$ の時：$i + (2n + 1)j = 2k + l$ の $\mathbb{N}^4_{\geq 0}$ における解は

$$(2, 0, 1, 0), (1, 0, 0, 1), (0, 2, 2n + 1, 0), (0, 1, m, 2(n - m) + 1) \quad (m = 0, 1, \ldots, n)$$

で張られるから

$$A(a, b) = \mathbb{C}[x^2 z, xu, y^2 z^{2n+1}, yu^{2n+1}, yzu^{2n-1}, \ldots, yz^n u],$$
$$I(a, b) = (x^2 z, xu, y^2 z^{2n+1}, yu^{2n+1}, yzu^{2n-1}, \ldots, yz^n u).$$

ここで $c_0, \ldots, c_n, d_1, d_2, d_3 \in \mathbb{C}$ が

$$d_1 x^2 z + d_2 xu + d_3 y^2 z^{2n+1} + c_0 yu^{2n+1} + c_1 yzu^{2n-1} + \cdots + c_n yz^n u \in I(a, b)^2$$

を満たすとする．$y = u = 0$ として $d_1 x^2 z \in (x^4 z^2)$ だから $d_1 = 0$. 同様に $d_2 = d_3 = 0$. $x = 0$ として $y(c_0 u^{2n+1} + c_1 zu^{2n-1} + \cdots + c_n z^n u) \in y^2 \mathbb{C}[y, z, u]$ だから $c_0 = c_1 = \cdots = c_n = 0$. よって $x^2 z, xu, y^2 z^{2n+1}, yu^{2n+1}, yzu^{2n-1}, \ldots, yz^n u$ は $\mathbb{C}$ 上一次独立だから $\dim_{\mathbb{C}} I(a, b)/I(a, b)^2 = n + 4$.

• $a = 2n$ の時：$i + 2nj = 2k + l$ の $\mathbb{N}^4_{\geq 0}$ における解は

$$(2, 0, 1, 0), (1, 0, 0, 1), (0, 1, m, 2(n - m)) \quad (m = 0, 1, \ldots, n)$$

で張られるから

$$A(a, b) = \mathbb{C}[x^2 z, xu, yu^{2n}, yzu^{2n-2}, \ldots, yz^n],$$
$$I(a, b) = (x^2 z, xu, yu^{2n}, yzu^{2n-2}, \ldots, yz^n).$$

上と同様にして $x^2 z, xu, yu^{2n}, yzu^{2n-2}, \ldots, yz^n$ は $\mathbb{C}$ 上一次独立であるから $\dim_{\mathbb{C}} I(a, b)/I(a, b)^2 = n+3$.

以上から答えは $a = 1, 2$. □

問 3

$V_0, V_1, V_2, \cdots$ を有限次元複素ベクトル空間の列とし，その直和 $\bigoplus_{j=0}^{\infty} V_j$ を V とおく．線型写像 $f, g : V \to V$ が，任意の $j \geq 0$ に対して

$$f(V_j) \subset V_{j+1}, \quad g(V_j) \subset V_j$$

を満たすとする．任意の複素数 t に対して $f_t = f + tg$ とおき，P_t を自然な全射

$$P_t : V \to V/f_t(V)$$

とする．

(i) V の部分空間 $\bigoplus_{j=0}^{n} V_j$ を F_n とおく $(n = 0, 1, \cdots)$．そのとき，任意の t と任意の $n \geq 0$ に対して

$$\dim P_t(F_n) \leq \dim P_0(F_n)$$

が成り立つことを証明せよ．

(ii) 上記の不等式において等号の成り立たないような例を挙げよ．

解答. (i) $f(V_j) \subset V_{j+1}$ より

$$P_0(F_n) = V_0 \oplus \bigoplus_{j=1}^{n} (V_j/f(V_{j-1}))$$

だから

$$\dim P_0(F_n) = \dim V_0 + \sum_{j=1}^{n} (\dim V_j - \dim f(V_{j-1})).$$

同様に $g(V_j) \subset V_j$ より

$$P_t(F_n) = (V_0/g(V_0)) \oplus \bigoplus_{j=1}^{n} (V_j/(f(V_{j-1}) \cup g(V_j)))$$

だから

$$\dim P_t(F_n) = (\dim V_0 - \dim g(V_0)) + \sum_{j=1}^{n} (\dim V_j - \dim(f(V_{j-1}) \cup g(V_j))).$$

ここで $\dim g(V_0) \geq 0, \dim(f(V_{j-1}) \cup g(V_j)) \geq \dim f(V_{j-1})$ であるから $\dim P_t(F_n) \leq \dim P_0(F_n)$ が成り立つ．

(ii) $\dim V_j = 2$ とし，V_j の基底を x_{j1}, x_{j2} とする．$f(x_{jk}) = x_{j+1,1}, g(x_{jk}) = x_{j2}$ で f, g を定める．この時

$$g(V_0) = \mathbb{C}x_{02}, \quad f(V_{j-1}) \cup g(V_j) = \mathbb{C}x_{j1} \cup \mathbb{C}x_{j2} = \mathbb{C}x_{j1} \oplus \mathbb{C}x_{j2}, \quad f(V_{j-1}) = \mathbb{C}x_{j1}$$

だから，$\dim g(V_0) > 0$ および任意の $j \geq 1$ に対して $\dim(f(V_{j-1}) \cup g(V_j)) > \dim f(V_{j-1})$ となる．従って任意の $t \in \mathbb{C}^{\times}, n \geq 0$ に対して (i) の不等号で等号が成立しない． □

平成 11 年度 (1998 年 8 月実施)

問 1

複素 2 次正方行列全体のなす線型空間を $M_2(\mathbb{C})$ とし，$\det(X) = 1$ を満たす $X \in M_2(\mathbb{C})$ の全体のなす乗法群を $SL_2(\mathbb{C})$ とする．また，$\mathbb{C}$ の元をスカラー行列と同一視して $M_2(\mathbb{C})$ の元とみなす．

(i) $A \in SL_2(\mathbb{C})$ に対して，線型写像

$$\begin{array}{rccc} \mathrm{Ad}(A): & M_2(\mathbb{C}) & \longrightarrow & M_2(\mathbb{C}) \\ & \cup & & \cup \\ & X & \longmapsto & AXA^{-1} \end{array}$$

の跡（trace）を求めよ．

(ii) G を $SL_2(\mathbb{C})$ の有限部分群とする．このとき，$M_2(\mathbb{C})$ における次の二つの等式を示せ：

$$\text{(a)} \qquad \sum_{g\in G} \sigma = \begin{cases} 1 & (G = \{1\} \text{ のとき}), \\ 0 & (G \neq \{1\} \text{ のとき}), \end{cases}$$

$$\text{(b)} \qquad \sum_{g\in G} \sigma^2 = |G| \left(\frac{\dim_{\mathbb{C}} C(G)}{2} - 1 \right).$$

ここで，$|G|$ は G の元の個数を表す．また，

$$C(G) = \{X \in M_2(\mathbb{C}) \,|\, \text{任意の } \sigma \in G \text{ に対し } \sigma X = X\sigma\}$$

とする．

(iii) $SL_2(\mathbb{C})$ の有限部分群で巡回群でないものは -1 を含むことを示せ．

解答. (i) A の Jordan 標準形を D とすると $P \in GL_2(\mathbb{C})$ があって $P^{-1}AP = D$ と書ける．この時

$$\mathrm{Ad}(A)(X) = (PDP^{-1})X(PDP^{-1})^{-1} = P\mathrm{Ad}(D)(P^{-1}XP)P^{-1}$$

だから，$\mathrm{Ad}(A)(X) = \lambda X$ は $\mathrm{Ad}(D)(P^{-1}XP) = \lambda P^{-1}XP$ と同値．よって A は Jordan 標準形 $\left(\begin{smallmatrix} \alpha & \\ & \alpha^{-1} \end{smallmatrix}\right), \left(\begin{smallmatrix} \varepsilon & 1 \\ & \varepsilon \end{smallmatrix}\right)$ $(\alpha \in \mathbb{C}^\times, \varepsilon = \pm 1)$ であるとして良い．$X = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)$ とおく．

• $A = \left(\begin{smallmatrix} \alpha & \\ & \alpha^{-1} \end{smallmatrix}\right)$ の時：$\mathrm{Ad}(A)(X) = \left(\begin{smallmatrix} x & \alpha^2 y \\ \alpha^{-2} z & w \end{smallmatrix}\right)$ だから，$\mathrm{Ad}(A)(X) = \lambda X$ は

$$(1-\lambda)x = (\alpha^2 - \lambda)y = (\alpha^{-2} - \lambda)z = (1-\lambda)w = 0$$

と同値．$X \neq 0$ だから $\lambda = 1, 1, \alpha^2, \alpha^{-2}$ なので $\mathrm{tr}\,\mathrm{Ad}(A) = 2 + \alpha^2 + \alpha^{-2} = (\alpha + \alpha^{-1})^2 = (\mathrm{tr}\, A)^2$.

• $A = \left(\begin{smallmatrix} \varepsilon & 1 \\ & \varepsilon \end{smallmatrix}\right)$ の時：

$$AX = \lambda XA \Longleftrightarrow \begin{pmatrix} \varepsilon x + z & \varepsilon y + w \\ \varepsilon z & \varepsilon w \end{pmatrix} = \lambda \begin{pmatrix} \varepsilon x & x + \varepsilon y \\ \varepsilon z & z + \varepsilon w \end{pmatrix}$$

$$\Longleftrightarrow \begin{pmatrix} \varepsilon(1-\lambda) & 0 & 1 & 0 \\ -\lambda & \varepsilon(1-\lambda) & 0 & 1 \\ 0 & 0 & \varepsilon(1-\lambda) & 0 \\ 0 & 0 & -\lambda & \varepsilon(1-\lambda) \end{pmatrix} \begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix} = 0$$

である．$X \neq 0$ より，この 4 次行列の行列式 $(1-\lambda)^4$ は 0 だから $\lambda = 1$. よって $\mathrm{tr}\,\mathrm{Ad}(A) = 4$.
いずれにしても $\mathrm{tr}\,\mathrm{Ad}(A) = (\mathrm{tr}\, A)^2$ である．

(ii) (a) $G = \{1\}$ の時は自明だから $G \neq \{1\}$ とする．$\left(\begin{smallmatrix} \varepsilon & 1 \\ & \varepsilon \end{smallmatrix}\right)$ の位数は無限だから，任意の G の元の Jordan 標準形は $\mathrm{diag}(\zeta, \zeta^{-1})$ である．また $G \neq \{1\}$ だから，1 を固有値に持たない $g \in G$ が存在する．この時写像 $G \to G, \sigma \mapsto g\sigma$ は全単射だから

$$g \sum_{\sigma\in G} \sigma = \sum_{\sigma\in G} g\sigma = \sum_{\sigma\in G} \sigma. \qquad \therefore (g-1) \sum_{\sigma\in G} \sigma = 0$$

これより $\sum_{\sigma\in G}\sigma = 0$.
(b) $G = \{1\}, \{\pm 1\}$ の時は $C(G) = M_2(\mathbb{C})$ だから $\dim_{\mathbb{C}} C(G) = 4$. よって示すべき式の両辺はともに $|G|$ となり正しい．$G \neq \{1\}, \{\pm 1\}$ とする．$g_0 = p\,\mathrm{diag}(\zeta, \zeta^{-1})p^{-1}$ $(\zeta \neq 0, \pm 1, p \in GL_2(\mathbb{C}))$ となる $g_0 \in G$ が存在する．この時

$$\mathbb{C} \subset C(G) \subset C(\langle g_0\rangle) = \{p\,\mathrm{diag}(x, w)p^{-1}\,;\, x, w \in \mathbb{C}\}$$

だから $\dim_{\mathbb{C}} C(G) = 1, 2$.
• $\dim_{\mathbb{C}} C(G) = 2$ の時 $C(G) = \{\mathrm{diag}(x, w)\,;\, x, w \in \mathbb{C}\}$ である．特に任意の $x \in \mathbb{C}^\times, g \in G$ に対し $\mathrm{Ad}(\mathrm{diag}(x, x^{-1}))(g) = g$ だから，(i) より g は対角行列となる．従って G は対角行列のなす有限群だから巡回群であり，生成元は $\mathrm{diag}(\zeta, \zeta^{-1})$ $(\zeta = e^{2\pi i/n})$ と書ける．$G \neq \{1\}, \{\pm 1\}$ より $n \geq 3$ なので，

$$\sum_{\sigma\in G}\sigma^2 = \sum_{k=1}^{n}\mathrm{diag}(\zeta^{2k}, \zeta^{-2k}) = 0.$$

• $\dim_{\mathbb{C}} C(G) = 1$ の時
(iii) G を $SL_2(\mathbb{C})$ の巡回群でない有限部分群とする．$SL_2(\mathbb{C})$ の元で位数 2 のものは（Jordan 標準形を考えれば）-1 のみであるから，$g \in G$ の位数が $2k$ ならば $-1 = g^k \in G$ となる．偶数位数の G の元が存在しないとする．この時 $|G|$ は奇数であり，写像 $G \ni g \mapsto g^2 \in G$ は単射である．実際，$g_1^2 = g_2^2$ $(g_1, g_2 \in G)$, $|G| = 2n-1$ とすると $g_1 = g_1 \cdot g_1^{2n-1} = (g_1^2)^n = (g_2^2)^n = g_2$ である．また $|G| < \infty$ だから，この写像は全射でもある．よって

$$\sum_{\sigma\in G}\sigma^2 = \sum_{\sigma\in G}\sigma = 0$$

なので $\dim_{\mathbb{C}} C(G) = 2$. この時 G は巡回群となって矛盾． □

問 2A

有理数係数の既約 3 次方程式の一つの実根 θ が有限個の有理数 $a_1, \ldots, a_n$ の実 3 乗根 $a_1^{1/3}, \ldots, a_n^{1/3}$ の有理数係数多項式として表されると仮定する．このとき，θ はある一つの有理数 a の実 3 乗根 $a^{1/3}$ の有理数係数多項式としても表されることを証明せよ．

解答. $n = 2$ で正しいなら，帰納的に任意の n で成り立つ．よって $n = 2$ の時に示せば良い．a_1, a_2 は $\mathbb{Q}$ の立方数でないとして良い．$K = \mathbb{Q}[a_1^{1/3}, a_2^{1/3}] = \mathbb{Q}(a_1^{1/3}, a_2^{1/3}), L = K(\omega)$ とおく．ただし $\omega = e^{2\pi i/3}$. L は K の $\mathbb{Q}$ 上の Galois 閉包であり $[L : \mathbb{Q}] = [L : K][K : \mathbb{Q}] = 2 \cdot 3^2$ である．$G = \mathrm{Gal}(L/\mathbb{Q})$ とおく．$\sigma_1, \sigma_2, \tau \in G$ を

$$\sigma_1 : \begin{cases} a_1^{1/3} & \mapsto & \omega a_1^{1/3} \\ a_2^{1/3} & \mapsto & a_2^{1/3} \\ \omega & \mapsto & \omega \end{cases} \qquad \sigma_2 : \begin{cases} a_1^{1/3} & \mapsto & a_1^{1/3} \\ a_2^{1/3} & \mapsto & \omega a_2^{1/3} \\ \omega & \mapsto & \omega \end{cases} \qquad \tau : \begin{cases} a_1^{1/3} & \mapsto & a_1^{1/3} \\ a_2^{1/3} & \mapsto & a_2^{1/3} \\ \omega & \mapsto & \omega^2 \end{cases}$$

で定める．$\sigma_1^3 = \sigma_2^3 = \tau^2 = 1, \sigma_1\sigma_2 = \sigma_2\sigma_1, (\sigma_1\tau)^2 = (\sigma_2\tau)^2 = 1$ だから，σ_1, σ_2, τ で生成される部分群は位数 18 である．一方 $\#G = [L : \mathbb{Q}] = 18$ だから，G は σ_1, σ_2, τ で生成される．$K = L^{\langle\tau\rangle}$ だから，K の部分体で $\mathbb{Q}$ 上 3 次拡大のものは，$\langle\tau\rangle$ を含む位数 6 の部分群による不変部分体である．位数 6 の群の 3-Sylow 部分群の個数 n_3 は $n_3 \equiv 1 \bmod 3, n_3 \mid 6$ を満たすから $n_3 = 1$. すなわち位数 3 の部分群は唯一つである．G の位数 3 の部分群は $\langle\sigma_1\rangle, \langle\sigma_2\rangle, \langle\sigma_1\sigma_2\rangle, \langle\sigma_1^2\sigma_2\rangle$ の 4 個だから，$\langle\tau\rangle$ を含む位数 6 の G の部分群は $\langle\sigma_1, \tau\rangle, \langle\sigma_2, \tau\rangle, \langle\sigma_1\sigma_2, \tau\rangle, \langle\sigma_1^2\sigma_2, \tau\rangle$ の 4 個である．よって K の部分体で $\mathbb{Q}$ 上 3 次拡大のものは

$$L^{\langle\sigma_1,\tau\rangle} = \mathbb{Q}(a_2^{1/3}), \quad L^{\langle\sigma_2,\tau\rangle} = \mathbb{Q}(a_1^{1/3}), \quad L^{\langle\sigma_1\sigma_2,\tau\rangle} = \mathbb{Q}((a_1^2 a_2)^{1/3}), \quad L^{\langle\sigma_1^2\sigma_2,\tau\rangle} = \mathbb{Q}((a_1 a_2)^{1/3})$$

で全て．仮定から $\theta \in K, [\mathbb{Q}(\theta) : \mathbb{Q}] = 3$ だから $\mathbb{Q}(\theta)$ はこのどれかに一致するが，いずれの場合も $a \in \mathbb{Q}$ があって $\mathbb{Q}(\theta) = \mathbb{Q}(a^{1/3})$ と書ける．よって $\theta \in \mathbb{Q}(\theta) = \mathbb{Q}(a^{1/3}) = \mathbb{Q}[a^{1/3}]$ となる． □

問 2B

$\mathbb{P}^1$ を 1 次元複素射影空間とし，$C(\mathbb{P}^1)$ を $\mathbb{P}^1$ の有理関数体とする．正則写像 $f : \mathbb{P}^1 \to \mathbb{P}^1$ で，f の誘導する体拡大 $f^* : C(\mathbb{P}^1) \to C(\mathbb{P}^1)$ が 4 次の Galois 拡大となるものについて，次の同値関係を考える：

$$f_1 \text{ と } f_2 \text{ が同値} \quad \Longleftrightarrow \quad \mathbb{P}^1 \text{ から } \mathbb{P}^1 \text{ への正則同型 } u, v \text{ があって，} f_2 = u \circ f_1 \circ v.$$

このとき，各同値類の代表元を求めよ．

解答. $C(\mathbb{P}^1) \cong \mathbb{C}(x)$ だから，体拡大 $\mathbb{C}(x)/\mathbb{C}(f)$ を考えれば良い．同値関係を $\sim$ と書く．$[\mathbb{C}(z) : \mathbb{C}(f)] = 4$ となる $f \in \mathbb{C}(z)$ は $f(z) = \frac{p(z)}{q(z)}, \max\{\deg p, \deg q\} = 4$ と書ける．必要があれば，定数を引いて逆数を考えることにより $\deg p = 4 > \deg q$ として良い．この f 全体の集合を S とおく．また $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{C})$ に対し $u_A(z) = \frac{az+b}{cz+d}$ とおく．$\mathrm{Gal}(\mathbb{C}(z)/\mathbb{C}(f))$ は $\mathbb{Z}/4\mathbb{Z}$ または $(\mathbb{Z}/2\mathbb{Z})^2$ である．

• $\mathbb{Z}/4\mathbb{Z}$ の時：$D = \mathrm{diag}(i, 1)$ とおくと Galois 群は $\langle D \rangle \cong \langle u_D \rangle$ に共役だから，$\mathrm{Gal}(\mathbb{C}(z)/\mathbb{C}(f))$ の元は $u_{PD^kP^{-1}} = u_P \circ u_{D^k} \circ u_P^{-1}$ $(P \in GL_2(\mathbb{C}), 0 \le k \le 3)$ と書ける．よって $f \in S$ は $f \circ u_P \circ u_{D^k} \circ u_P^{-1} = f$, すなわち $f \circ u_P \circ u_{D^k} = f \circ u_P$ を満たすから $f \circ u_P = az^4 + b$ $(a \neq 0)$ と書ける．さらに $g(z) = (z-b)/a$ とおけば $g \circ f \circ u_P = z^4$ だから $f \sim z^4$. ここで z の $\mathbb{C}(z^4)$ 上最小多項式は $T^4 - z^4$ だから，$\mathbb{C}(z^4)$-共役元は $\pm z, \pm iz$. これらは全て $\mathbb{C}(z)$ の元だから Galois 拡大になっている．従って代表元は z^4.

• $(\mathbb{Z}/2\mathbb{Z})^2$ の時：$R = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ とおくと Galois 群は $\langle D^2, R \rangle \cong \langle u_{D^2}, u_R \rangle$ に共役である．上と同様に $u_{D^{2j}} = (-1)^j z, u_{R^j} = z^{-j}$ $(j = 0, 1)$ で不変な S の元は

$$\frac{az^4 + bz^2 + a}{z^2} = a(z^2 + z^{-2}) + b \quad (a \neq 0)$$

と書ける．これは $z^2 + z^{-2}$ と同値だから $f \sim z^2 + z^{-2}$. ここで z の $\mathbb{C}(z^2 + z^{-2})$ 上最小多項式は $T^4 - (z^2 + z^{-2})T^2 + 1$ だから，$\mathbb{C}(z^2 + z^{-2})$-共役元は $\pm z, \pm z^{-1}$. これらは全て $\mathbb{C}(z)$ の元だから Galois 拡大になっている．従って代表元は $z^2 + z^{-2}$.

以上から答えは

$$z^4, \qquad z^2 + z^{-2}.$$

□