東大数理 院試過去問解答
専門科目 (代数)

nabla *

2024 年 12 月 9 日

目 次

*Twitter:@nabla_delta

はじめに

東大数理科学研究科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．

2020 年度 (令和 2 年度)

問 2

以下の問に答えよ.

(1) 体 K 上の 2 変数多項式環 $K[X,Y]$ の極大イデアルは 2 つの元で生成されることを示せ.

(2) 有理整数環 $\mathbb{Z}$ 上の 2 変数多項式環 $\mathbb{Z}[X,Y]$ の極大イデアルは 3 つの元で生成されることを示せ.

解答. 京大数学系 2005 年度専門問 1 の解答を参照. □

2019 年度 (平成 31 年度)

問 2

a, b, c を 1 以上の整数とする．このとき多項式 $X^a + Y^b + Z^c \in \mathbb{C}[X, Y, Z]$ は既約であることを示せ．

解答. $\mathbb{C}[X, Y, Z] = \mathbb{C}[Y, Z][X]$ で $\mathbb{C}[Y, Z]$ は UFD だから，$\mathbb{C}[Y, Z]$ の素元 f であって $Y^b + Z^c \in (f), Y^b + Z^c \notin (f^2)$ となるものが存在すれば，Eisenstein の既約判定法により $X^a + Y^b + Z^c$ は既約となる．よって f の存在を示せば良い．

$Y^b + Z^c \in \mathbb{C}[Y, Z] = \mathbb{C}[Z][Y]$ は Y についての次数が $b \geq 1$ だから単元ではない．よってある素元 f で割り切れる．今 f^2 で割り切れるとすると Y による偏微分 bY^{b-1} も f で割り切れるから，$(Y^b + Z^c) - \frac{Y}{b} \cdot bY^{b-1} = Z^c$ も f で割り切れる．これより $f = sZ^r\,(s \in \mathbb{C}, r \leq c)$ とおけるが，これは明らかに $Y^b + Z^c$ を割らないから矛盾．従ってこの f が条件を満たすから示された． □

2015 年度 (平成 27 年度)

問 2

$S = k[t]$ を体 k 上の一変数多項式環，K を S の商体とする．S の部分環 R を次のように定める：

$$R = k[t^4, t^{10}, t^{13}].$$

(1) $I = \{x \in K\,;\, xS \subset R\}$ とおいたとき，I は R と S, 両方のイデアルであることを示せ．
(2) I の R のイデアルとしての生成系のうち，生成元の個数が最小のものを 1 つ求めよ．

解答. (1) 任意の $x, y \in I, z \in R$ に対し

$$(x+y)S \subset xS + yS \subset R + R \subset R, \qquad zxS \in xS \subset R$$

なので，I は R のイデアルである．S のイデアルであることも同様．

(2) $x \in I$ は $x = x \cdot 1 \in xS \subset R$ を満たすから $I \subset R$ である．また $i \geq 0$ に対し

$$t^{20+4i} = (t^4)^{5+i}, \quad t^{21+4i} = (t^4)^{2+i} \cdot t^{13}, \quad t^{22+4i} = (t^4)^{3+i} \cdot t^{10}, \quad t^{23+4i} = (t^4)^i \cdot t^{10} \cdot t^{13}$$

は全て R の元であるから，$A = \{0, 4, 8, 10, 12, 13, 14, 17, 18\}$ とおくと $R = \bigoplus_{i \in A} kt^i \oplus t^{20}k[t]$ である．今 $f \in I$ の最低次の項を at^i とすると，任意の $j \geq 0$ に対し $t^j f \in fS \subset R$ となることから $i \geq 20$, すなわち $f \in t^{20}k[t]$ が必要．逆にこの時 $fS \subset t^{20}k[t] \subset R$ である．よって

$$\begin{aligned} I = t^{20}k[t] &= t^{20}k[t^4] + t^{21}k[t^4] + t^{22}k[t^4] + t^{23}k[t^4] \\ &\subset t^{20}R + t^{21}R + t^{22}R + t^{23}R \end{aligned}$$

であり，逆の包含は明らかだから $I = t^{20}R + t^{21}R + t^{22}R + t^{23}R$ である．従って I の R のイデアルとしての生成系として $t^{20}, t^{21}, t^{22}, t^{23}$ が取れる．

生成元が f_1, f_2, f_3 の 3 個であったとする．上の議論から $\deg f_i \geq 20$ であるから，生成系を取り直して f_i の最低次の項を t^{d_i} $(20 \leq d_1 < d_2 < d_3)$ として良い．R の定数でない元の次数の最小値は 4 であるから，$t^{20}, t^{21}, t^{22}, t^{23} \in I$ のうち少なくとも一つは I の元ではない．これは矛盾． □

2014 年度 (平成 26 年度)

問 2

可換環 $A = \mathbb{R}[x,y]/(x^2+y^2)$ の極大イデアルを全て求めよ.

解答. $I = (x^2+y^2)$ とおく. A の極大イデアルは I を含む $\mathbb{R}[x,y]$ の極大イデアル J を用いて $\mathfrak{m} = J/I$ と書ける. $A/\mathfrak{m} \cong \mathbb{R}[x,y]/J$ は体であり, しかも有限生成 $\mathbb{R}$ 代数だから, Zariski の補題よりこれは $\mathbb{R}$ の有限次代数拡大である. 従って $\mathbb{R}$ または $\mathbb{C}$ に同型.[1] 自然な射影 $\mathbb{R}[x,y] \to \mathbb{R}[x,y]/J$ を π, 単射 $\mathbb{R}[x,y]/J \to \mathbb{C}$ を ι とし, $\varphi = \iota \circ \pi$ とおく. ι は単射だから $\operatorname{Ker}\varphi = J$. 一方 x, y (の $\mathbb{R}[x,y]/J$ における同値類) の ι による像をそれぞれ a, b とおくと, φ は $x \mapsto a, y \mapsto b$ なる $\mathbb{R}$ 準同型だから

$$J = \operatorname{Ker}\varphi = ((x-a)\mathbb{C}[x,y] + (y-b)\mathbb{C}[x,y]) \cap \mathbb{R}[x,y]$$

である. また $I \subset J$ より $a^2+b^2 = 0$ なので $b = \pm ia$.

- $a = 0$ の時 : $b = 0$ より $J = (x,y)$.
- $a \in \mathbb{R}, a \neq 0$ の時 : $b = ia$ なら, $(y-ia)$ は $y = ia$ で 0 となる元全体だが, $\mathbb{R}[x,y]$ との共通部分では $y = \overline{ia} = -ia$ でも 0 になるから

$$(y-ia)\mathbb{C}[x,y] \cap \mathbb{R}[x,y] = (y-ia)(y+ia)\mathbb{R}[x,y] = (y^2+a^2)\mathbb{R}[x,y].$$

また $(x-a)\mathbb{C}[x,y] \cap \mathbb{R}[x,y] = (x-a)\mathbb{R}[x,y]$ だから $J = (x-a, y^2+a^2)$. $b = -ia$ についても同様.

- $a \in i\mathbb{R}, a \neq 0$ の時 : $b \in \mathbb{R}, b \neq 0$ だから, 上と同様に $J = (x^2+b^2, y-b)$.
- $\operatorname{Re} a, \operatorname{Im} a \neq 0$ の時 : $\operatorname{Re} a = \alpha, \operatorname{Im} a = \beta$ とおくと $b = \pm(-\beta + i\alpha)$ である. 上の議論と同様に

$$(x-a)\mathbb{C}[x,y] \cap \mathbb{R}[x,y] = (x-a)(x-\overline{a})\mathbb{R}[x,y] = ((x-\alpha)^2+\beta^2)\mathbb{R}[x,y],$$
$$(y-b)\mathbb{C}[x,y] \cap \mathbb{R}[x,y] = (y-b)(y-\overline{b})\mathbb{R}[x,y] = ((y \pm \beta)^2+\alpha^2)\mathbb{R}[x,y]$$

だから, 必要があれば β を $-\beta$ で置き換えて $J = ((x-\alpha)^2+\beta^2, (y-\beta)^2+\alpha^2)$.

以上から答えは

$$(x,y)/I, \quad (x-a, y^2+a^2)/I, \quad (x^2+a^2, y-a)/I,$$
$$((x-\alpha)^2+\beta^2, (y-\beta)^2+\alpha^2)/I.$$

ただし $a, \alpha, \beta \in \mathbb{R} \setminus \{0\}$. □

[1] $\mathbb{R} \subset K \subset \mathbb{C}$ なる $\mathbb{C}$ の部分体 K があれば $[\mathbb{C} : \mathbb{R}] = 2$ からわかる.

2012 年度 (平成 24 年度)

問 2

a を複素数とし，複素数体 $\mathbb{C}$ 上の可換代数

$$A = \mathbb{C}[x, y]/(xy, y(y-a))$$

を考える．

(1) A の極大イデアルを全て求めよ．

(2) A の各極大イデアル $\mathfrak{m}$ に対して $\dim_{\mathbb{C}} \mathfrak{m}/\mathfrak{m}^2$ を計算せよ．

(3) A の 0 でない冪零元を全て求めよ．

解答. (1) $I = (xy, y(y-a))$ とおく．A の極大イデアルは，I を含む $\mathbb{C}[x, y]$ の極大イデアル J を用いて J/I と書ける．また Hilbert の零点定理の弱形から $J = (x-c, y-d)\,(c, d \in \mathbb{C})$ と書ける．$I \subset J$ より $cd = d(d-a) = 0$ である．$d \neq 0$ なら $c = 0, d = a$. $d = 0$ なら $xy = (x-c)f + y^2 g$ となる $f, g \in \mathbb{C}[x, y]$ が取れる．よって $(x-c)f \in (y)$ より $f = yf'$ とおけて $x = (x-c)f' + yg$. $y = 0$ として $x = (x-c)f'(x, 0)$ だから $c = 0$. 以上から $J = (x, y), (x, y-a)$ なので，答えは

$$\mathfrak{m}_1 = (x, y)/I, \quad \mathfrak{m}_2 = (x, y-a)/I.$$

(2) • $\mathfrak{m}_1$: $\mathfrak{m}_1^2 = (x^2, xy, y^2)/I = (x^2, ay)/I$ より

$$\dim_{\mathbb{C}} \mathfrak{m}_1/\mathfrak{m}_1^2 = \dim_{\mathbb{C}}(x, y)/(x^2, ay) = \begin{cases} \dim_{\mathbb{C}}(x, y)/(x^2) = 2 & (a = 0) \\ \dim_{\mathbb{C}}(x)/(x^2) = 1 & (a \neq 0). \end{cases}$$

• $\mathfrak{m}_2$: $a = 0$ の時は $\dim_{\mathbb{C}} \mathfrak{m}_2/\mathfrak{m}_2^2 = 2$. $a \neq 0$ の時は

$$\mathfrak{m}_2^2 = (x^2, x(y-a), (y-a)^2)/I = (x^2, -ax, -a(y-a))/I = (x, y-a)/I = \mathfrak{m}_2$$

より $\dim_{\mathbb{C}} \mathfrak{m}_2/\mathfrak{m}_2^2 = 0$.

(3) A の元は $f(x) + cy\,(f \in \mathbb{C}[x], c \in \mathbb{C})$ と書ける．これが冪零元であるとする．

$$\sqrt{0} \subset \mathfrak{m}_1 \cap \mathfrak{m}_2 = \begin{cases} (x, y)/I & (a = 0) \\ (x)/I & (a \neq 0) \end{cases}$$

より $f(x) = xg(x)$ とおける．

• $a = 0$ の時：ある $n \geq 2$ に対し $0 = (xg + cy)^n = (xg)^n$ だから $g = 0$. よって零でない冪零元は $cy\,(c \in \mathbb{C}^\times)$.

• $a \neq 0$ の時：$c = 0$ であり，この時 xg が冪零元になるのは $g = 0$ の時のみ．よって零でない冪零元は存在しない． □

2011 年度 (平成 23 年度)

問 3

次の問に答えよ．

(1) 行列

$$A = \begin{pmatrix} 4 & 6 & 4 \\ 6 & 24 & 18 \\ 16 & 6 & 10 \\ 1 & 3 & 15 \end{pmatrix}$$

によって定められる自由加群の間の準同型 $L_A : \mathbb{Z}^3 \to \mathbb{Z}^4$ について，商加群 $\mathbb{Z}^4/\operatorname{Im} L_A$ の構造を決定せよ．

(2) M, N を有限生成自由加群とし，$M^* = \operatorname{Hom}(M, \mathbb{Z}), N^* = \operatorname{Hom}(N, \mathbb{Z})$ をそれぞれ双対加群とする．準同型 $f : M \to N$ に対し，準同型 $f^* : N^* \to M^*$ を $(f^*\varphi)(m) = \varphi(f(m))\,(\varphi \in N^*, m \in M)$ によって定める．f が単射であるとき，次が同値であることを示せ．

(i) $N/f(M)$ は自由加群である．

(ii) f^* は全射である．

解答． (1) A に基本変形をすると

$$A \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \\ 0 & 0 & 0 \end{pmatrix}$$

となるから

$$\begin{aligned} \mathbb{Z}^4/\operatorname{Im} L_A &\cong \mathbb{Z}^4/(\mathbb{Z} \oplus 2\mathbb{Z} \oplus 6\mathbb{Z}) \\ &\cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}. \end{aligned}$$

(2) M の基底を $a_1, \ldots, a_m$, N の基底を $b_1, \ldots, b_n$ とする．f は単射だから $m \leq n$ である．これらの基底に関する f の表現行列の転置を A とおく．$P \in M_m(\mathbb{Z})^\times, Q \in M_n(\mathbb{Z})^\times$ と $e_1, \ldots, e_m \in \mathbb{Z}_{\geq 0}$ が存在して

$$QAP = \begin{pmatrix} e_1 & & \\ & \ddots & \\ & & e_m \\ & 0_{(n-m)\times m} & \end{pmatrix}$$

と書ける．ここで $0_{(n-m)\times m}$ は $(n-m) \times m$ の零行列．また f の単射性から任意の i について $e_i > 0$ である．この時

$$N/f(M) \cong \mathbb{Z}^n/(e_1\mathbb{Z} \oplus \cdots \oplus e_m\mathbb{Z}) \cong \mathbb{Z}^{n-m} \oplus \bigoplus_{i=1}^{m} \mathbb{Z}/e_i\mathbb{Z}$$

だから，(i) は $e_1 = \cdots = e_m = 1$ と同値．

a_i, b_i の双対基底をそれぞれ a_i^*, b_i^* とおく．これらの基底に関する f^* の表現行列の転置は ${}^tA$ だから，上と同様に $\operatorname{Im} f^* \cong e_1\mathbb{Z} \oplus \cdots \oplus e_m\mathbb{Z}$ となる．よって (ii) は $e_1 = \cdots = e_m = 1$ と同値．

以上で示された． □

2010 年度 (平成 22 年度)

問 4

4 次対称群を S_4 と書き，正整数 k に対して $GL_k(\mathbb{C})$ で k 次複素一般線形群を表す．以下の問に答えよ．

(1) S_4 は $GL_4(\mathbb{C})$ のある部分群と同型であることを示せ．

(2) S_4 は $GL_3(\mathbb{C})$ のある部分群と同型であることを示せ．

(3) S_4 と同型になる $GL_2(\mathbb{C})$ の部分群は存在しないことを示せ．

解答. (2) $\mathbb{R}^3$ に正四面体 $ABCD$ を，その中心が原点 O となるように置く．頂点 A, B, C, D にそれぞれ $1, 2, 3, 4$ を割り当てて S_4 を $1, 2, 3, 4$ の置換と見る．$(1\ 2) \in S_4$ は，辺 AB の中点と辺 CD を含む平面に関する反転だから，その表現行列 $\rho((1\ 2))$ は $GL_3(\mathbb{R})$ の元である．同様に任意の互換 $a, b \in S_4$ に対し $\rho(a), \rho(b) \in GL_3(\mathbb{R})$ が定まり，$\rho(ab) = \rho(a)\rho(b)$ が成り立つ．S_4 は互換で生成されるから，単射準同型 $\rho : S_4 \to GL_3(\mathbb{R})$ が得られる．よって S_4 は $GL_3(\mathbb{R})\,(\subset GL_3(\mathbb{C}))$ の部分群 $\operatorname{Im}\rho$ と同型．

(1) (2) の ρ に対し準同型写像 $\rho' : S_4 \to GL_4(\mathbb{C})$ を $\sigma \mapsto \operatorname{diag}(\rho(\sigma), 1)$ と定めれば良い．

(3) $GL_2(\mathbb{C})$ の部分群 G と同型写像 $\rho : S_4 \to G$ が存在したとする．$a = (1\ 2), b = (3\ 4) \in S_4$ とおく．$\rho(a)^2 = \rho(a^2) = \rho(e) = I$ より $\rho(a)$ の固有値は ± 1 で，しかも対角化可能である．よって共役を考えれば $\rho(a)$ は $\pm I, \operatorname{diag}(1, -1), \operatorname{diag}(-1, 1)$ のいずれかである．$a \notin Z(S_4)$ より $\rho(a) \notin Z(G)$ なので $\pm I$ は不適．$\rho(b)$ についても同様．また $ab = ba$ より $\rho(a)\rho(b) = \rho(b)\rho(a)$ なので，$\rho(a), \rho(b)$ は同時対角化可能である．これと $\rho(a) \neq \rho(b)$ より，共役を考えて $\rho(a) = \operatorname{diag}(1, -1), \rho(b) = \operatorname{diag}(-1, 1)$ とできる．ところが $\rho(ab) = \rho(a)\rho(b) = -I \in Z(G)$ なので $ab \in Z(S_4)$ となって矛盾． □

2009 年度 (平成 21 年度)

問 2

k を体，$k[x,y,z,w]$ を k 上の 4 変数多項式環とする．$I=(xz-y^2, yw-z^2, xw-yz)$ を $k[x,y,z,w]$ のイデアルとし，$R=k[x,y,z,w]/I$ とおく．

(1) R_x および R_w を簡単な形で表わせ．ただし $R_f\,(f\in R)$ で R の乗法系 $\{f^n\}$（n は 0 以上の整数）による局所化を表す．

(2) R は整域であることを示せ．

(3) R の商体において $R=R_x\cap R_w$ が成り立つことを示せ．

解答． (2) 全射な環準同型 $\varphi: k[x,y,z,w]\to R':=k[s^3,s^2t,st^2,t^3]$ を $x\mapsto s^3, y\mapsto s^2t, z\mapsto st^2, w\mapsto t^3$ で定める．$I\subset \mathrm{Ker}\,\varphi$ であるから φ は R から R' への準同型とみなせる．任意の $f\in R$ は $f=g_0(x,z,w)+g_1(x)y$ と書ける．これが $\mathrm{Ker}\,\varphi$ の元とすると $g_0(s^3,st^2,t^3)+g_1(s^3)s^2t=0$ である．左辺第 1 項は t^1 の項を含まないから $g_1\equiv 0$. ここで $z^3-xw^2=-z(yw-z^2)-w(xw-yz)\in I$ より $g_0(x,z,w)=h_0(x,w)+h_1(x,w)z+h_2(x,w)z^2$ と書けるから

$$0=g_0(s^3,st^2,t^3)=h_0(s^3,t^3)+h_1(s^3,t^3)st^3+h_2(s^3,t^3)(st^3)^2.$$

s の次数から $h_0=h_1=h_2\equiv 0$ となるので $g_1\equiv 0$. よって $f\equiv 0$ なので $\mathrm{Ker}\,\varphi\subset I$. 従って準同型定理より $R\cong k[s^3,s^2t,st^2,t^3]$ となり，これは整域である．

(1) (2) より

$$R_x\cong k[s^3,s^2t,st^2,t^3]_{s^3}=k[s^3,s^2t,st^2,t^3,s^{-3}]=k[t/s](s^3),$$
$$R_w\cong k[s^3,s^2t,st^2,t^3]_{t^3}=k[s^3,s^2t,st^2,t^3,t^{-3}]=k[s/t](t^3).$$

(3)

$$k[s^3,s^2t,st^2,t^3,s^{-3}]\cap k[s^3,s^2t,st^2,t^3,t^{-3}]=k[s^3,s^2t,st^2,t^3]$$

だから，φ で引き戻して $R_x\cap R_w=R$ を得る． □

問 3

整数 λ, μ に対して，連立漸化式

$$\begin{cases} a_{n+1} = \lambda a_n + b_n \\ b_{n+1} = a_n + \mu b_n \qquad n = 1, 2, \dots \\ a_1 = 0, b_1 = 1 \end{cases}$$

を考える．2 ではない素数 p を固定し，$(\lambda - \mu)^2 + 4$ は p で割り切れないと仮定する．

(1) 全ての正の整数 n に対して

$$p \mid a_{n+p^2-1} - a_n \quad \text{かつ} \quad p \mid b_{n+p^2-1} - b_n$$

が成り立つことを示せ．

(2) $\lambda = 2, \mu = 1$ とする．全ての正の整数 n に対して

$$p \mid a_{n+p-1} - a_n \quad \text{かつ} \quad p \mid b_{n+p-1} - b_n$$

が成り立つような 13 以下の奇素数 p を全て求めよ．

解答. (1) 自然な射影 $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ による a_n, b_n の像をそれぞれ c_n, d_n とし，以下 $\mathbb{F}_p$ の代数閉包 $\overline{\mathbb{F}_p}$ 上で考える．$c_{n+p^2-1} = c_n, d_{n+p^2-1} = d_n$ を示せば良い．$A = \begin{pmatrix} \lambda & 1 \\ 1 & \mu \end{pmatrix} \in M_2(\mathbb{F}_p)$ とおくと

$$\begin{pmatrix} c_{n+k} \\ d_{n+k} \end{pmatrix} = A \begin{pmatrix} c_{n+k-1} \\ d_{n+k-1} \end{pmatrix} = \cdots = A^k \begin{pmatrix} c_n \\ d_n \end{pmatrix} \tag{$*$}$$

である．A の固有多項式は $t^2 - (\lambda + \mu)t + \lambda\mu - 1$ で判別式は $D = (\lambda - \mu)^2 + 4 \neq 0$ だから，A は相異なる固有値を持つ．よって A の Jordan 標準形は対角行列である．また固有値は $\mathbb{F}_{p^2}$ の元だから $A^{p^2} = A$.

- $\lambda\mu \neq 1$ の時：A は正則だから $A^{p^2-1} = I$. よって $(*)$ より $c_{n+p^2-1} = c_n, d_{n+p^2-1} = d_n$ となる．
- $\lambda = \mu = 1$ の時：帰納的に $a_n = b_n = 2^{n-2}\,(n \geq 2)$ である．$p \neq 2$ だから，$n \geq 2$ に対し $c_{n+p^2-1} = 2^{n-2} \cdot (2^{p-1})^{p+1} = 2^{n-2} = c_n$ となる．d_n も同様．
- $\lambda = \mu = -1$ の時：帰納的に $a_n = (-1)^n 2^{n-2}, b_n = (-1)^{n+1} 2^{n-2}\,(n \geq 2)$ となる．$p^2 - 1$ が偶数であることに注意すると，$\lambda = \mu = 1$ の時と同様に $n \geq 2$ に対し $c_{n+p^2-1} = c_n, d_{n+p^2-1} = d_n$ となる．

(2) $\lambda\mu \neq 1$ だから，条件を満たすことは $A^p = A$, すなわち A の全ての固有値が $\mathbb{F}_p$ の元であることと同値．これは $D = 5$ が $\bmod p$ の平方剰余であることと同値．仮定から $p \neq 5$ である．また明らかに $p \neq 3$. $p > 5$ の時は Euler の規準と平方剰余の相互法則より

$$\left(\frac{5}{p}\right) = (-1)^{\frac{5-1}{2}\frac{p-1}{2}} \left(\frac{p}{5}\right) = \left(\frac{p}{5}\right) \equiv p^{(5-1)/2} = p^2 \pmod 5$$

だから，これが 1 となるのは $p \equiv \pm 1 \bmod 5$ の時．よって答えは $p = 11$ のみ．

(補足) $\lambda = \mu = \pm 1$ の時 $a_{p^2} - a_1$ は 2 のべき乗なので p で割り切れない． □

2008 年度 (平成 20 年度)

問 2

1 変数多項式環 $\mathbb{C}[T]$ の部分環 $\{f \in \mathbb{C}[T] \mid f(0) = f(1)\}$ を A とおく．$S = T^2 - T$ で生成される A の部分環 $\mathbb{C}[S]$ を B とおく．

(1) A は B 加群として自由加群であることを示し，その階数を求めよ．

(2) $\mathbb{C}$ 上の 2 変数多項式環 $\mathbb{C}[X, Y]$ のイデアル I であって剰余環 $\mathbb{C}[X, Y]/I$ が A と同型となるようなものを 1 つ求め，それを最小個数の生成元を用いて表わせ．

(3) 商群 $A\left[\frac{1}{S}\right]^{\times} \Big/ B\left[\frac{1}{S}\right]^{\times}$ の生成系で，要素の個数が最小のものを 1 組求めよ．ただし可換環 R に対し，$R^{\times}$ は R の乗法群を表すものとする．

解答. (1)

$$A = \{c + T(T-1)f(T)\,;\, c \in \mathbb{C}, f \in \mathbb{C}[T]\} = \{c + Sf(T)\,;\, c \in \mathbb{C}, f \in \mathbb{C}[T]\}$$

である．ここで任意に $f(T) \in \mathbb{C}[T]$ を取ると，$f(T) = f_1(T) + Sf_2(T) + \cdots + S^k f_{k+1}(T)$ となる $f_j \in \mathbb{C}[T], \deg f_j \leq 1$ が帰納的に（一意に）定まる．よって

$$\begin{aligned} A &= \{c + Sf_1(T) + S^2 f_2(T) + \cdots + S^k f_k(T)\,;\, c \in \mathbb{C}, \deg f_j \leq 1\} \\ &= \{g_0(S) + g_1(S)T\,;\, g_0, g_1 \in B\} = B \oplus TB \end{aligned}$$

は階数 2 の自由 B-加群．

(2) [2] 環準同型 $\varphi : \mathbb{C}[X, Y] \to \mathbb{C}[T]$ を $X \mapsto 4T(T-1), Y \mapsto 4T(T-1)(2T-1)$ で定める．明らかに $\operatorname{Im}\varphi \subset A$. また $\varphi(X/4) = S, \varphi((X+Y)/8) = ST$ だから逆の包含も成り立つ．$\operatorname{Ker}\varphi$ を求める．

$$\varphi(X^2(X+1)) = (4T(T-1))^2(2T-1)^2 = \varphi(Y^2)$$

より $I := (Y^2 - X^3 - X^2) \subset \operatorname{Ker}\varphi$ である．逆に $f \in \operatorname{Ker}\varphi$ として，f を $Y^2 - X^3 - X^2$ で割った余りを $f_1(X)Y + f_0(X)\,(f_0, f_1 \in \mathbb{C}[X])$ とおくと

$$f_1(4T(T-1)) \cdot 4T(T-1)(2T-1) + f_0(4T(T-1)) = 0.$$

左辺第 1 項，第 2 項の次数はそれぞれ奇数，偶数だから $f_1 = f_0 = 0$. よって $f \in I$ である．従って準同型定理より $\mathbb{C}[X, Y]/I \cong A$.

(3) 1996 年度問 1 と同様にして

$$\begin{aligned} B[1/S]^{\times} &= \mathbb{C}[S, 1/S]^{\times} = \{cS^k\,;\, c \in \mathbb{C}^{\times}, k \in \mathbb{Z}\}, \\ A[1/S]^{\times} &= \{cT^j(T-1)^k\,;\, c \in \mathbb{C}^{\times}, j, k \in \mathbb{Z}\} = \{cT^j S^k\,;\, c \in \mathbb{C}^{\times}, j, k \in \mathbb{Z}\} \end{aligned}$$

だから，$A[1/S]^{\times}/B[1/S]^{\times}$ は T の同値類 $\overline{T}$ で生成される． □

[2] 京大数理研平成 14 年度専門問 3 と同様.

2007 年度 (平成 19 年度)

問 2

R を可換環 $\mathbb{Z}[x,y]/(x^2+y^2)$ とする．以下の問に答えよ．

(1) $\mathfrak{p}$ を $\#(R/\mathfrak{p})$ が有限になるような R の素イデアルとする．（ここで $\#(R/\mathfrak{p})$ は環 $R/\mathfrak{p}$ の元の個数を表す．）このとき $\#(R/\mathfrak{p})$ としてとりうる値を全て求めよ．

(2) $\mathfrak{m}$ を R の極大イデアルとするとき，$R/\mathfrak{m}$ は有限体であることを示せ．

解答. (1) $R/\mathfrak{p}$ は有限整域だから有限体である．よって位数は p を素数として p^k とおける．$k=1$ の時は，$x^2+y^2 \in (p,x,y)$ であるから $\mathfrak{p}=(p,x,y)/(x^2+y^2)$ とすると

$$R/\mathfrak{p} \cong \mathbb{Z}[x,y]/(p,x,y) \cong \mathbb{F}_p.$$

これは位数 p の整域だから $\mathfrak{p}$ は条件を満たす．もし $k \geq 2$ なら，定数でない $f \in R/\mathfrak{p}$ が存在して $f^{p^k}=f$ が成り立つ．ところが両辺の定数でない最低次を比べると $f \equiv 0$ となって矛盾する．以上から答えは任意の素数.

(2) $\mathfrak{m}$ は x^2+y^2 を含む $\mathbb{Z}[x,y]$ の極大イデアル I を用いて $\mathfrak{m}=I/(x^2+y^2)$ と書ける．$R/\mathfrak{m} \cong \mathbb{Z}[x,y]/I$ を R' とおく．$I \cap \mathbb{Z}$ は $\mathbb{Z}$ のイデアルだから $\{0\}$ または $p\mathbb{Z}$（p は素数）である．x,y の R' における剰余類をそれぞれ $\overline{x},\overline{y}$ とおく．

• $I \cap \mathbb{Z} = p\mathbb{Z}$ の時：$R' \cong \mathbb{F}_p[\overline{x},\overline{y}]$ は体であり，さらに有限生成 $\mathbb{F}_p$ 代数だから，Zariski の補題より $\mathbb{F}_p$ の有限次拡大である．従って R' は有限体.

• $I \cap \mathbb{Z} = \{0\}$ の時：R' は $\mathbb{Z}$ を含む体だから $\mathbb{Q}$ も含む．よって $\mathbb{Q}[\overline{x},\overline{y}] \subset R'$ となるが，逆の包含も成り立つから $R'=\mathbb{Q}[\overline{x},\overline{y}]$ となる．R' は体かつ $\mathbb{Q}$-代数として有限生成だから，Zariski の補題より $\mathbb{Q}$ の有限次拡大である．従って $\overline{x},\overline{y}$ の $\mathbb{Q}$ 上 monic な最小多項式が存在する．それらをそれぞれ $f(t),g(t) \in \mathbb{Q}[t]$ とおき，$f(t),g(t)$ の係数の分母の最小公倍数を $d>0$ とすると，

$$R'=\mathbb{Z}[\overline{x},\overline{y}] \subset \mathbb{Z}[1/d][\overline{x},\overline{y}] \subset \mathbb{Q}[\overline{x},\overline{y}]=R'$$

より $R'=\mathbb{Z}[1/d][\overline{x},\overline{y}]$ である．一方 $f(t),g(t)$ は $\mathbb{Z}[1/d]$ 係数の monic な多項式だから，$\overline{x},\overline{y}$ は $\mathbb{Z}[1/d]$ 上整，すなわち R' は $\mathbb{Z}[1/d]$ 上整となる．これと R' が体であることから $\mathbb{Z}[1/d]$ も体になる．よって $\mathbb{Q} \subset \mathbb{Z}[1/d]$ となるが，$d<q$ なる素数 q に対し $1/q \notin \mathbb{Z}[1/d]$ だから矛盾.

以上で示された. □

2006 年度 (平成 18 年度)

問 1

$K = \mathbb{R}(T)$ を実数体上の 1 変数有理関数体とし，$n \geq 3$ を自然数とする．L を K 上の多項式 $X^n - T$ の最小分解体とする．

(1) 拡大次数 $[L : K]$ を求めよ．

(2) $n = 4$ とする．中間体 $K \subset M \subset L$ で，$[M : K] = 4$ であるものを全て求めよ．それぞれの M について，K 上の Galois 拡大であるかどうか判定せよ．

解答. (1) $\zeta = e^{2\pi i/n}$ とおくと $X^n - T$ の根は $\zeta^k T^{1/n}\,(k = 0, 1, \ldots, n-1)$ だから $L = K(\zeta, T^{1/n})$. $n \geq 3$ より $\zeta \notin \mathbb{R}$ なので,

$$[L : K] = [L : K(T^{1/n})][K(T^{1/n}) : K] = n\varphi(n).$$

ここで φ は Euler 関数.

(2) $[L : K] = 4\varphi(4) = 8, \zeta = i$ である．$S = T^{1/4}$ とおく．$\sigma, \tau \in \mathrm{Gal}(L/K)$ を

$$\sigma : (S, i) \mapsto (-iS, i), \qquad \tau : (S, i) \mapsto (S, -i)$$

で定める．この時 $\sigma^4 = \tau^2 = \mathrm{id}_L$ であり，また $\sigma\tau : (S, i) \mapsto (-iS, -i)$ より $(\sigma\tau)^2 = \mathrm{id}_L$ なので $\langle \sigma, \tau \rangle \cong D_4$ である．位数の比較から，これが $\mathrm{Gal}(L/K)$ である．M に対応する $\mathrm{Gal}(L/K)$ の部分群の位数は $[M : K] = 2$ である．京大数学系 1993 年度専門問 1 と同様に，D_4 の位数 2 の部分群は $H := \langle \sigma^2 \rangle, H_j := \langle \sigma^j \tau \rangle\ (j = 0, 1, 2, 3)$ の 5 個．$\sigma^2 : (S, i) \mapsto (-S, i), \sigma^j\tau : (S, i) \mapsto ((-i)^j S, -i)$ より

$$K(S) \subset L^{H_0}, \quad K((1-i)S) \subset L^{H_1},$$
$$K(iS) \subset L^{H_2}, \quad K((1+i)S) \subset L^{H_3}, \quad K(S^2, i) \subset L^H$$

である．左辺の部分体を順に $M_j\,(j = 0, 1, \ldots, 4)$ とおく．$[L : K]$ の計算と同様に $[M_4 : K] = 4$ なので $L^H = K(S^2, i)$. また K 上既約な $X^4 + T$ は $\frac{1 \pm i}{\sqrt{2}} S$ を根に持つから $[M_1 : K] = [M_3 : K] = 4$. よって $L^{H_1} = K((1-i)S), L^{H_3} = K((1+i)S)$. 同様に $L^{H_0} = K(S), L^{H_2} = K(iS)$.

$$(\sigma^j)^{-1}\sigma^2\sigma^j = \sigma^2, \quad (\sigma^j\tau)^{-1}\sigma^2(\sigma^j\tau) = \tau\sigma^2\tau = (\tau\sigma\tau)^2 = \sigma^{-2} = \sigma^2$$

より $H \lhd D_4$ である．また $\sigma^{-1}(\sigma^j\tau)\sigma = \sigma^{j-1}\sigma^{-1}\tau = \sigma^{j-2}\tau \notin \langle \sigma^j\tau \rangle$ より H_j は D_4 の正規部分群ではない．以上から K の 4 次拡大体は $M_0, M_1, \ldots, M_4$ の 5 個で，そのうち K 上 Galois 拡大のものは M_4 のみ. □

問 2

体 K 上の 1 変数多項式環 $K[X]$ を考える．$K[X]$ の部分環 R が K を含むとき，R は $K[X]$ の有限個の元 $f_1, f_2, \ldots, f_n$ によって K 上生成される部分環であること，すなわち $R = K[f_1, f_2, \ldots, f_n]$ であることを示せ．

解答． $K \subset R \subset K[X]$ である．任意の monic な $f \in R \setminus K$ に対し，$f(T) - f(X) \in R[T]$ は monic で $T = X$ を零点に持つから，X は R 上整である．よって $K[X]$ は K 代数として有限生成かつ R 上整である．K は Noether 環なので，R も K 代数として有限生成となる． □

問 4

$GL_2(\mathbb{C})$ を可逆な 2×2 複素行列全体のなす群とする．$\mathbb{C}$ 上の 2 変数多項式環 $\mathbb{C}[x,y]$ への $X=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in GL_2(\mathbb{C})$ の作用を

$$(R_X f)(x,y)=f(ax+by,cx+dy)\qquad (f(x,y)\in\mathbb{C}[x,y])$$

によって定義する．2×2 行列 A,B を

$$A=\begin{pmatrix}-\frac{1}{2} & -\frac{\sqrt{3}}{2}\\ \frac{\sqrt{3}}{2} & -\frac{1}{2}\end{pmatrix},\quad B=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$$

とするとき，以下の問に答えよ．

(1) A,B によって生成される $GL_2(\mathbb{C})$ の部分群の位数を求めよ．

(2) 3 次斉次多項式全体 $P_3\subset\mathbb{C}[x,y]$ を，R_A,R_B の作用についての不変かつ既約な部分空間の直和として表わせ．

ここで不変な部分空間 W とは

$$R_AW\subset W,\qquad R_BW\subset W$$

をみたす部分空間である．さらに不変な部分空間 W が既約であるとは，$W\neq\{0\}$ であり，W に含まれる不変な部分空間が $\{0\}$ と W に限られることをいう．

解答. (1) A,B は $\mathbb{R}^2$（xy 平面）に自然に左から作用する．A による作用は原点を中心とした $2\pi/3$ 回転，B による作用は x 軸に関する対称移動だから，A,B で生成される群は 2 面体群 D_3 に同型．よって答えは 6.

(2) P_3 の基底は $\{x^3,x^2y,xy^2,y^3\}$ であり，

$$\begin{pmatrix}R_A(x^3)\\ R_A(xy^2)\\ R_A(y^3)\\ R_A(x^2y)\end{pmatrix}=\underbrace{\frac{1}{8}\begin{pmatrix}-1 & -9 & -3\sqrt{3} & -3\sqrt{3}\\ -3 & 5 & -\sqrt{3} & -\sqrt{3}\\ 3\sqrt{3} & 3\sqrt{3} & -1 & -9\\ \sqrt{3} & \sqrt{3} & -3 & 5\end{pmatrix}}_{=:X}\begin{pmatrix}x^3\\ xy^2\\ y^3\\ x^2y\end{pmatrix}$$

である.[3] X の左上の 2×2 行列を Y, 左下の 2×2 行列を Z とおくと

$$\begin{aligned}|X-\lambda I|&=\begin{vmatrix}Y-\lambda I & -Z\\ Z & Y-\lambda I\end{vmatrix}=|(Y-\lambda I)+iZ||(Y-\lambda I)-iZ|\\ &=(\lambda^2-(4-4\sqrt{3}i)\lambda+(-32-32\sqrt{3}i))(\lambda^2-(4+4\sqrt{3}i)\lambda+(-32+32\sqrt{3}i))\\ &=(\lambda-8)^2(\lambda-(-4+4\sqrt{3}i))(\lambda-(-4-4\sqrt{3}i))\end{aligned}$$

だから，$\frac{1}{8}X$ の固有値は $1,1,(-1\pm\sqrt{3}i)/2$, 対応する固有ベクトルはそれぞれ

$${}^t(1,-1,0,0),\quad {}^t(0,0,1,-1),\quad {}^t(3i,i,3,1),\quad {}^t(-3i,-i,3,1).$$

すなわち R_A の固有ベクトルは

$$f_1=x^3-xy^2,\quad f_2=y^3-x^2y,\quad f_3=(3x^3+xy^2)i+(3y^3+x^2y),\quad f_4=-(3x^3+xy^2)i+(3y^3+x^2y)$$

である．$\langle f_1\rangle,\langle f_2\rangle$ はそれぞれ R_B でも不変で 1 次元だから，不変かつ既約な部分空間である．$\langle f_3\rangle,\langle f_4\rangle$ はそれぞれ R_B で不変ではないが，$\langle f_3,f_4\rangle$ は R_B で不変で既約である．よって

$$\begin{aligned}P_3&=\langle f_1\rangle\oplus\langle f_2\rangle\oplus\langle f_3,f_4\rangle\\ &=\langle x(x^2-y^2)\rangle\oplus\langle y(x^2-y^2)\rangle\oplus\langle x(3x^2+y^2),y(3y^2+x^2)\rangle.\end{aligned}$$

□

[3] 固有多項式の計算のため，基底の並べ方を変えてある．

2005 年度 (平成 17 年度)

問 1

p を奇素数とし，$GL_2(\mathbb{F}_p)$ を p 元体 $\mathbb{F}_p$ の元を成分に持つ可逆な 2×2 行列全体のなす群とする．$M \in GL_2(\mathbb{F}_p)$ について，行列式 $\det M$ が乗法群 $\mathbb{F}_p^\times$ の生成元ならば，M の位数は p と素であることを示せ．

解答. 対偶を示す．M の位数が p の倍数であるとする．M の Jordan 標準形は $\left(\begin{smallmatrix}\alpha & 0\\ 0 & \beta\end{smallmatrix}\right), \left(\begin{smallmatrix}\alpha & 1\\ 0 & \alpha\end{smallmatrix}\right)$ のいずれかである．M の固有多項式は $\mathbb{F}_p$ 係数 2 次多項式なので $\alpha, \beta \in \mathbb{F}_{p^2} \setminus \{0\}$ である．$\left(\begin{smallmatrix}\alpha & 0\\ 0 & \beta\end{smallmatrix}\right)$ とすると $\alpha + \beta = \operatorname{tr} M \in \mathbb{F}_p$ なので，$\alpha, \beta \in \mathbb{F}_p$ であるか $\alpha, \beta \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ である．前者の場合は M の位数は $p-1$ の約数となり矛盾．後者の場合も M の位数は p^2-1 の約数となり矛盾．よって M の Jordan 標準形は $\left(\begin{smallmatrix}\alpha & 1\\ 0 & \alpha\end{smallmatrix}\right)$ である．$2\alpha = \operatorname{tr} M \in \mathbb{F}_p$ と p が奇数であることから $\alpha \in \mathbb{F}_p$ なので，

$$(\det M)^{(p-1)/2} = (\alpha^2)^{(p-1)/2} = \alpha^{p-1} = 1.$$

従って $\det M$ は $\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$ の生成元ではない． □

2004 年度 (平成 16 年度)

問 1

有限次元線形空間 A, B, C, D の次元をそれぞれ a, b, c, d とし，線形写像 $g : B \to C$ の階数を r とする．線形写像

$$F : \mathrm{Hom}(A, B) \otimes \mathrm{Hom}(C, D) \to \mathrm{Hom}(A, D)$$

を $F(f \otimes h) = hgf$ で定めたとき，F の階数を求めよ．

解答. A, B, C, D は K 上のベクトル空間とし，基底を適当に取る．これらの基底について，$\mathrm{Hom}(A, B)$ の元を $b \times a$ の行列とみなす．他も同様．仮定から $p \in GL_c(K), q \in GL_b(K)$ が存在して $p^{-1}gq^{-1} = \widetilde{g} := \mathrm{diag}(I_r, 0_{(c-r)\times(b-r)})$ となる．ここで F の定義において g を $\widetilde{g}$ で置き換えた線形写像を $\widetilde{F}$ とし，$\mathrm{Hom}(A, B) \otimes \mathrm{Hom}(C, D)$ の同型写像 G を $G(f \otimes h) = qf \otimes hp$ で定める．この時

$$(\widetilde{F} \circ G)(f \otimes h) = \widetilde{F}(qf \otimes hp) = hp\widetilde{g}qf = hgf = F(f \otimes h)$$

より $F = \widetilde{F} \circ G$ だから，$\mathrm{rank}\, F = \mathrm{rank}(\widetilde{F} \circ G) = \mathrm{rank}\, \widetilde{F}$ である．よって $g = \widetilde{g}$ として良い．$r = 0$ の時は F は零写像である．$r \geq 1$ の時は，$M(b, a), M(d, c), M(d, a)$ の行列単位をそれぞれ $E_{ij}, E'_{ij}, E''_{ij}$ とすると

$$F(E_{1j} \otimes E'_{i1}) = E'_{i1} \begin{pmatrix} I_r & \\ & 0_{(c-r)\times(b-r)} \end{pmatrix} E_{1j} = E''_{ij}$$

だから F は全射.

以上から

$$\mathrm{rank}\, F = \begin{cases} 0 & (r = 0), \\ ad & (r > 0). \end{cases}$$

□

問 2

n を自然数とし，$L = \mathbb{C}(T_1, \ldots, T_n)$ を n 変数有理関数体とする．$\mathbb{C}$ 上の L の自己同型 σ を

$$\sigma(T_i) = T_{i+1} \quad (i = 1, \ldots, n-1),$$
$$\sigma(T_n) = T_1$$

で定める．$K = \{f \in L\,;\, \sigma(f) = f\}$ を不変部分体とする．

(1) 拡大次数 $[L : K]$ を求めよ．

(2) L の線形部分空間 $\bigoplus_{i=1}^{n} \mathbb{C}T_i$ を σ の作用に関する固有空間に分解せよ．

(3) 多項式 $f_1, \ldots, f_n \in \mathbb{C}[T_1, \ldots, T_n]$ で $K = \mathbb{C}(f_1, \ldots, f_n)$ となるようなものを一組与えよ．

(4) $n = 6$ のとき L と K の中間体を全て求めよ．

解答. (1) $\#\langle\sigma\rangle = n$ であるから Artin の定理より $[L : K] = n$.

(2) $\{T_1, \ldots, T_n\}$ に関する σ の表現行列は

$$\begin{pmatrix} & & 1 \\ & I_{n-1} & \\ & & \end{pmatrix}$$

である．この行列の固有多項式は $\lambda^n - 1$ だから，$\zeta = e^{2\pi i/n}$ とおくと固有値は $\zeta^k\,(k = 1, 2, \ldots, n)$. 固有ベクトルは $(1, \zeta^{-k}, \zeta^{-2k}, \ldots, \zeta^{-(n-1)k})$ だから，

$$X_k = T_1 + \zeta^{-k}T_2 + \zeta^{-2k}T_3 + \cdots + \zeta^{-(n-1)k}T_n$$

とおけば固有空間への分解は $\bigoplus_{k=1}^{n} \mathbb{C}T_k = \bigoplus_{k=1}^{n} \mathbb{C}X_k$.

(3) $(X_1, \ldots, X_n) = (T_1, \ldots, T_n)A\,(A \in GL_n(\mathbb{C}))$ と書けるから $L = \mathbb{C}(X_1, \ldots, X_n)$ である．(2) より $\sigma(X_k) = \zeta^k X_k$ なので $\sigma(X_1^{n-k}X_k) = X_1^{n-k}X_k$. よって

$$f_k = X_1^{n-k}X_k \in \mathbb{C}[X_1, \ldots, X_n] = \mathbb{C}[T_1, \ldots, T_n] \quad (k = 1, \ldots, n)$$

とおけば $K' := \mathbb{C}(f_1, \ldots, f_n) \subset K$ である．また $K'(X_1) = \mathbb{C}(X_1, \ldots, X_n) = L$ であり，$g(x) := x^n - f_1 \in K'[x]$ は $x = X_1$ を根に持つから

$$[L : K'] \leq n = [L : K] \leq [L : K'].$$

よって $K = K'$ なので，上の f_k たちが求めるものである．

(4) Artin の定理より L/K は Galois 拡大で $G := \mathrm{Gal}(L/K) = \langle\sigma\rangle \cong \mathbb{Z}/6\mathbb{Z}$ である．$[L : K] = n$ より X_1 の K 上最小多項式は g であるから，X_1 の K-共役元は $\zeta^j X_1\,(j = 0, 1, \ldots, 5)$. G の生成元は $\sigma : X_1 \mapsto \zeta X_1$ で，部分群は $\langle\sigma^2\rangle, \langle\sigma^3\rangle$ の 2 つである．よって L/K の中間体は

$$L^{\langle\sigma^2\rangle} = K(X_1^3), \qquad L^{\langle\sigma^3\rangle} = K(X_1^2)$$

の 2 つ． □

問 4

p を 3 以上の素数とする．単位元をもつ可換環 A の可逆元のなす群 $A^\times$ は，位数 p^2 の巡回群にはならないことを証明せよ．

解答． $A^\times \cong \mathbb{Z}/p^2\mathbb{Z}$ となる A が存在したとする．$|A^\times| = p^2$ は奇数だから $-1 \in A^\times$ の位数も奇数．よって $-1 = 1$ だから A の標数は 2 である．$A^\times$ の生成元を g とし，環準同型 $\varphi : \mathbb{F}_2[x] \to A$ を $x \mapsto g$ で定める．$\operatorname{Ker}\varphi$ は $\mathbb{F}_2[x]$ のイデアルなので，一つの $f \in \mathbb{F}_2[x]$ で生成される．$f_0(x) = x^{p^2} - 1$ とおくと $(f_0) \subset \operatorname{Ker}\varphi$ であるから f_0 は f で割り切れる．また $f_0'(x) = p^2 x^{p^2-1} \neq 0\,(x \in A \setminus \{0\})$ だから f_0 は重根を持たない．よって f も重根を持たないから，$\mathbb{F}_2$ 上で既約かつどの二つも互いに素な多項式 $f_1, \ldots, f_n$ があって $f = f_1 \cdots f_n$ とおける．従って準同型定理と中国剰余定理から

$$\begin{aligned}\operatorname{Im}\varphi &\cong \mathbb{F}_2[x]/(f_1 \cdots f_n) \\ &\cong \mathbb{F}_2[x]/(f_1) \times \cdots \times \mathbb{F}_2[x]/(f_n) \\ &\cong \mathbb{F}_{2^{d_1}} \times \cdots \times \mathbb{F}_{2^{d_n}}.\end{aligned}$$

ただし $d_i = \deg f_i$ とおいた．$x \notin \operatorname{Ker}\varphi$ であること，また g の位数は $p^2 > 1$ だから $x - 1 \notin \operatorname{Ker}\varphi$ であることから $d_i \geq 2$ である．

ここで $(\operatorname{Im}\varphi)^\times = A^\times$ を示す．$\operatorname{Im}\varphi \subset A$ より $(\operatorname{Im}\varphi)^\times \subset A^\times$ である．逆に $u \in A^\times$ なら $v \in A^\times$ が存在して $uv = 1$ となる．$\varphi|_{R^\times} : R^\times \to A^\times$ は全射だから，$u', v' \in R^\times$ であって $\varphi(u') = u, \varphi(v') = v$ となるものが存在する．この時 $1 = uv = \varphi(u')\varphi(v')$ だから $u = \varphi(u') \in (\operatorname{Im}\varphi)^\times$. よって $A^\times \subset (\operatorname{Im}\varphi)^\times$ となるから示された．

以上から

$$\begin{aligned}A^\times &\cong (\mathbb{F}_{2^{d_1}} \times \cdots \times \mathbb{F}_{2^{d_n}})^\times \cong \mathbb{F}_{2^{d_1}}^\times \times \cdots \times \mathbb{F}_{2^{d_n}}^\times \\ &\cong \mathbb{Z}/(2^{d_1} - 1)\mathbb{Z} \times \cdots \times \mathbb{Z}/(2^{d_n} - 1)\mathbb{Z}\end{aligned}$$

だから，位数を比較して $p^2 = (2^{d_1} - 1) \cdots (2^{d_n} - 1)$. これより $n \leq 2$ である．$\bmod 4$ で見ると，$d_i \geq 2$ より $1 \equiv (-1)^n$ なので $n = 2$. この時 $2^{d_i} - 1 > 1$ より $2^{d_1} - 1 = 2^{d_2} - 1 = p$ であるが，$A^\times \cong (\mathbb{Z}/p\mathbb{Z})^2 \ncong \mathbb{Z}/p^2\mathbb{Z}$ となって矛盾． □

(補足) 単位元を持つ可換環 R の乗法群 $R^\times$ の位数としてありうるものは全て決定されているらしい．[4]

[4] https://www.jstor.org/stable/10.4169/amer.math.monthly.124.10.960

1999 年度 (平成 11 年度)

問 2

$A = \mathbb{Z}[X]$ を有理整数環上の 1 変数多項式環とする．A の異なる素イデアル $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ で

$$\{0\} \neq \mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \mathfrak{p}_3$$

を満たすものは存在しない（すなわち，A のクルル次元は 2 以下である）ことを証明せよ．

解答. $\mathfrak{p}_1$ を A の零でない素イデアルとする．$\mathfrak{p}_1$ の次数が最小の既約元 f を取る．

• $\deg f = 0$ の時：f は素数であるから，それを p とする．$\mathfrak{p}_1 \subset \mathfrak{p}_2$ なる A の素イデアル $\mathfrak{p}_2$ を取ると，$\mathfrak{p}_2/\mathfrak{p}_1$ は $A/\mathfrak{p}_1 \cong \mathbb{F}_p[X]$ の素イデアルである．$\mathbb{F}_p$ は体ゆえ $\mathbb{F}_p[X]$ は PID なので，$\mathbb{F}_p$ 上の既約多項式 $\overline{g}(X) \in \mathbb{F}_p[X]$ が存在して $\mathfrak{p}_2/\mathfrak{p}_1 = (\overline{g})$ となる．自然な射影 $\mathbb{Z}[X] \to \mathbb{F}_p[X]$ を π とおくと，$\pi(g) = \overline{g}$ となる $g \in A$ が取れる．この時 $\mathfrak{p}_2 = (p, g)$ である．$A/\mathfrak{p}_2 \cong \mathbb{F}_p[X]/(\overline{g})$ は体だから，$A/\mathfrak{p}_2$ の真の素イデアル $\mathfrak{p}_3/\mathfrak{p}_2$ （すなわち $\mathfrak{p}_2 \subset \mathfrak{p}_3$ なる A の素イデアル $\mathfrak{p}_3$）は存在しない．

• $\deg f \geq 1$ の時：f は $\mathbb{Z}$ 上既約．$\mathfrak{p}_2$ を $\mathfrak{p}_1 \subset \mathfrak{p}_2$ なる A の素イデアルとする．$\mathfrak{p}_2 \setminus \mathfrak{p}_1$ の次数が最小の既約元 g を取る．$\deg g > 0$ であったとすると，割り算して $f = ag + b\,(\deg b < \deg g)$ となる $a, b \in \mathbb{Q}[X]$ が取れる．適当に整数倍すれば $cf = ag + b\,(\deg b < \deg g)$ となる $c \in \mathbb{Z}, a, b \in \mathbb{Z}[X]$ が取れる．この時 $b \in (f, g) \subset \mathfrak{p}_2$ だから，$b = b_1^{r_1} \cdots b_k^{r_k}$ と既約元の積で書いた時，$b_i \in \mathfrak{p}_2$ となる i が少なくとも一つ存在する．もし $b_i \in \mathfrak{p}_1$ なら，$ag = cf - b \in \mathfrak{p}_1$ より a の素因数で $\mathfrak{p}_1$ の元となるものが存在する．これは $\deg f$ の最小性に反するから $b_i \in \mathfrak{p}_2 \setminus \mathfrak{p}_1$ である．ところが $\deg b_i \leq \deg b < \deg g$ なので，$\deg g$ の最小性に反する．よって $\deg g = 0$, すなわち g は素数．それを p とおくと $\mathfrak{p}_2 = (f, p)$ である．あとは $\deg f = 0$ の場合と同様. □

問 4

$\mathbb{Z}$ を有理整数環，$\mathbb{Z}[X]$ を $\mathbb{Z}$ 係数一変数多項式環とし，$\mathbb{Z}[X]$ の単項イデアル (X^n)（ただし n は 2 以上の整数）による剰余環 $\mathbb{Z}[X]/(X^n)$ を考える．

(1) この剰余環の単数群（可逆元全体が乗法に関してなす群）は，有限生成アーベル群であることを示せ．

(2) その群の不変系を求めよ．つまり上の群を標準形

$$\mathbb{Z}^{\oplus r} \oplus \mathbb{Z}/e_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/e_s\mathbb{Z} \qquad (e_1 \mid e_2, e_2 \mid e_3, \dots)$$

と同型であるとしたとき，階数 r とねじれの不変量 $e_1, e_2, \dots, e_s$ を求めよ．

解答． X の $R := \mathbb{Z}[X]/(X^n)$ における同値類を x とおく．

(1) $R^\times$ が有限生成であることを示せば良い．$a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in R$ の逆元が $b_0 + b_1x + \cdots + b_{n-1}x^{n-1}$ とすると，積の定数項から $a_0 = \pm 1$ が必要．逆にこの時 x^i の係数から $a_0b_i + a_1b_{i-1} + \cdots + a_ib_0 = 1$ なので，$b_0, b_1, \dots, b_{n-1} \in \mathbb{Z}$ が帰納的に一意に定まる．よって

$$R^\times = \{\pm 1 + xf(x)\,;\, f \in \mathbb{Z}[x]\}$$

である．ここで $f_i(x) = 1 - x^i$ $(i = 1, 2, \dots, n-1)$ とおく．$(k-1)i < n \le ki$ なる $k \in \mathbb{Z}$ を取ると

$$(1 + x^i + x^{2i} + \cdots + x^{(k-1)i})f_i(x) = 1 - x^{ki} = 1$$

だから $f_i \in R^\times, f_i^{-1} = 1 + x^i + x^{2i} + \cdots + x^{(k-1)i}$ である．今任意に $f(x) = 1 + a_1x + \cdots + a_{n-1}x^{n-1} \in R^\times$ を取る．$a_1 > 0$ の時は $f_1^{a_1} f = 1 \bmod x^2$, $a_1 < 0$ の時は $f_1^{-|a_1|} f = 1 \bmod x^2$ となる．以下同様に続けると，$f_1^{c_1} \cdots f_{n-1}^{c_{n-1}} f = 1$ となる $c_1, \dots, c_{n-1} \in \mathbb{Z}$ が存在する．定数項が -1 の場合は $-1 \in R^\times$ をかければ上の議論がそのまま成り立つから，$-1, f_1, \dots, f_{n-1}$ は $R^\times$ の生成元である．

(2) $f_i^j = 1 + j(-x)^i \bmod x^{i+1}$ だから f_i は無限位数である．また $f_{i_1}^{c_{i_1}} \cdots f_{i_k}^{c_{i_k}} = 1$ となる $1 \le i_1 < \cdots < i_k < n$ と $c_{i_j} > 0$ が存在したとすると，$1 + c_1(-x)^{i_1} \equiv 1 \bmod x^{i_1+1}$ となって矛盾．よって $-1, f_1, \dots, f_{n-1}$ たちの間には（群としての）関係式は存在しない．従って

$$R^\times = \langle -1, f_1, \dots, f_{n-1} \rangle \cong \mathbb{Z}^{n-1} \times \mathbb{Z}/2\mathbb{Z}$$

なので $r = n - 1, s = 1, e_1 = 2$. □

1997 年度 (平成 9 年度)

問 4

p を素数，L を p 元体 $\mathbb{F}_p$ 上の一変数有理関数体 $\mathbb{F}_p(T)$ とする．$S \in L$ を

$$S = \sum_{k=1}^{p} T^{k(p-1)} = T^{p-1} + T^{2(p-1)} + \cdots + T^{p(p-1)}$$

とし，K を L の部分体 $\mathbb{F}_p(S)$ とする．

(1) L の K 上の拡大次数 $[L : K]$ を求めよ．

(2) L は K のガロア拡大であることを示せ．

(3) ガロア群 $\mathrm{Gal}(L/K)$ の位数 p の部分群はただ一つであることを示し，その部分群に対応する中間体を求めよ．

解答. (1)

$$\begin{aligned} S &= \frac{T^{p-1}(T^{p(p-1)} - 1)}{T^{p-1} - 1} = \frac{T^{p-1}(T^{p-1} - 1)^p}{T^{p-1} - 1} \\ &= T^{p-1}(T^{p-1} - 1)^{p-1} = (T^p - T)^{p-1} \end{aligned}$$

より $f(X) = (X^p - X)^{p-1} - S$ は T を根に持つ．f は S の 1 次式だから $K[X] = \mathbb{F}_p[X](S)$ において既約．よって f は T の K 上の最小多項式だから，$[L : K] = \deg f = p(p-1)$.

(2) 任意の $a \in \mathbb{F}_p^\times, b \in \mathbb{F}_p$ に対し

$$((aT + b)^p - (aT + b))^{p-1} = (aT^p + b - (aT + b))^{p-1} = (T^p - T)^{p-1} = S$$

だから $f(aT + b) = 0$. これと $|\mathbb{F}_p^\times \times \mathbb{F}_p| = (p-1)p = \deg f$ より $f(X)$ の根（すなわち T の L-共役元）は $aT + b$ で，これらは全て L の元だから L/K は正規かつ分離的．従って L/K は Galois 拡大．

(3) $G = \mathrm{Gal}(L/K)$ とおくと $|G| = \deg f = p(p-1)$ である．G の p-Sylow 部分群の個数を n とおくと，Sylow の定理より $n \equiv 1 \bmod p$ かつ $n \mid p(p-1)$. 第 1 式より $(n, p) = 1$ だから $n \mid (p-1)$. よって $n < p$ なので $n = 1$ である．その部分群を H とおく．$\{\sigma_b(T) = T + b;\, b \in \mathbb{F}_p\}$ は G の部分群で位数は p だから，これが H である．(2) の計算から $T^p - T \in L^H$ なので $\mathbb{F}_p(T^p - T) \subset L^H$. 一方 $S = (T^p - T)^{p-1}$ より

$$[L^H : K] = \frac{[L : K]}{[L : L^H]} = \frac{|G|}{|H|} = p - 1 = [\mathbb{F}_p(T^p - T) : K]$$

だから，$L^H = \mathbb{F}_p(T^p - T)$. □

1996 年度 (平成 8 年度)

問 1

単位元を持つ可換環の可逆元全体は積に関して群をなす．これをその環の単数群という．次の環の単数群を求めよ．

(1) $\mathbb{Z}[X]$

(2) $\mathbb{Z}\left[X, \dfrac{1}{X}, \dfrac{1}{1-X}\right]$

ただし，$\mathbb{Z}$ は有理整数環，X は不定元とする．

解答. (1) $f \in \mathbb{Z}[X]^\times$ とすると $g \in \mathbb{Z}[X]$ が存在して $fg = 1$ となる．両辺の次数を比較して $\deg f + \deg g = 0$ だから $\deg f = \deg g = 0$. よって $\mathbb{Z}[X]^\times = \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$.

(2) 環を R とおく．$f \in R^\times$ を $\frac{p(X)}{X^n(1-X)^m}$ $(p \in \mathbb{Z}[X], n, m \in \mathbb{Z}_{\geq 0})$ と既約分数で書く．$p(X)$ の最高次係数を a とすると，$\frac{X^n(1-X)^m}{p(X)} \in R$ より $a = \pm 1$ が必要．またこの分母の根としてあり得るのは $X = 0, 1$ のみだから，$f(X) = \pm X^i(1-X)^j$ $(i, j \in \mathbb{Z})$ と書けることが必要．逆にこの形の元が $R^\times$ の元であることは明らか．よって

$$R^\times = \{\pm X^i(1-X)^j \,;\, i, j \in \mathbb{Z}\} \cong \mathbb{Z}^2 \times \mathbb{Z}/2\mathbb{Z}.$$

□

問 2

整数 λ, μ に対し数列 $\{a_n\}$ を帰納的に

$$\begin{cases} a_1 = 1, a_2 = 1, \\ a_{n+2} = \lambda a_{n+1} + \mu a_n \end{cases}$$

と定める．

(1) 素数 p が $\lambda^2 + 4\mu$ の約数でないとき，任意の整数 $n \geq 1$ に対し p は $a_{n+p^2-1} - a_n$ の約数であることを示せ．

(2) $\lambda = 2, \mu = -4$ とする．5 以上の素数 p が，任意の整数 $n \geq 1$ に対し $a_{n+p-1} - a_n$ の約数であるための必要十分条件を求めよ．(p に対する合同式で表わせ．)

解答. (1) 自然な射影 $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ による a_n の像を b_n とし，以下 $\mathbb{F}_p$ の代数閉包 $\overline{\mathbb{F}_p}$ 上で考える．$b_{n+p^2-1} = b_n$ を示せば良い．$A = \begin{pmatrix} \lambda & \mu \\ 1 & 0 \end{pmatrix} \in M_2(\mathbb{F}_p)$ とおく．この時

$$\begin{pmatrix} b_{n+k} \\ b_{n+k-1} \end{pmatrix} = A \begin{pmatrix} b_{n+k-1} \\ b_{n+k-2} \end{pmatrix} = \cdots = A^k \begin{pmatrix} b_n \\ b_{n-1} \end{pmatrix} \tag{$*$}$$

である．A の固有多項式は $t^2 - \lambda t - \mu$ で判別式は $D = \lambda^2 + 4\mu \neq 0$ だから，相異なる固有値を持つ．よって A の Jordan 標準形は対角行列である．また固有値は $\mathbb{F}_{p^2}$ の元だから $A^{p^2} = A$ である．

- $\mu \neq 0$ の時：A は正則だから $A^{p^2-1} = I$. よって $(*)$ より $b_{n+p^2-1} = b_n$ となる．
- $\mu = 0$ の時：帰納的に $a_n = \lambda^{n-2}\,(n \geq 2)$ である．また仮定から $\lambda \neq 0$ だから，$n \geq 2$ に対し $b_{n+p^2-1} = \lambda^{n-2} \cdot (\lambda^{p-1})^{p+1} = \lambda^{n-2} = b_n$ となる．

(2) $\mu \neq 0$ だから，条件を満たすことは $A^p = A$ と同値．Jordan 標準形を考えれば，これは A の全ての固有値が $\mathbb{F}_p$ の元であること，すなわち $D = -12$ が mod$p$ の平方剰余であることと同値である．Euler の規準，平方剰余の相互法則より

$$\begin{aligned} \left(\frac{-12}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{2^2}{p}\right)\left(\frac{3}{p}\right) = (-1)^{(p-1)/2} \cdot 1 \cdot (-1)^{\frac{3-1}{2}\frac{p-1}{2}} \left(\frac{p}{3}\right) \\ &= \left(\frac{p}{3}\right) \equiv p^{(3-1)/2} = p \pmod 3 \end{aligned}$$

だから，答えは $p \equiv 1 \bmod 3$.

(補足) 2009 年度問 3 と同様に，$\mu = 0$ の時は $n = 1$ で成り立たない． □

問 3

X を変数とする多項式

$$f(X) = X^4 + 4X^3 + 3X^2 - 2X + 23$$

を考える．

(1) $f(X)$ の有理数体 $\mathbb{Q}$ 上の最小分解体を F とし，ガロア群 $\mathrm{Gal}(F/\mathbb{Q})$ の構造を求めよ．

(2) 任意の素数 p について，$f(X) \bmod p$ は体 $\mathbb{Z}/p\mathbb{Z}$ 上可約であることを示せ．

解答. (1)

$$\begin{aligned} f(X-1) &= (X^4 - 4X^3 + 6X^2 - 4X + 1) + 4(X^3 - 3X^2 + 3X - 1) \\ &\quad + 3(X^2 - 2X + 1) - 2(X - 1) + 23 \\ &= X^4 - 3X^2 + 25 = (X^2 + 5)^2 - 13X^2 \\ &= (X^2 + 5 + \sqrt{13}X)(X^2 + 5 - \sqrt{13}X) \end{aligned}$$

だから，$f(X) = 0$ の根は

$$1 + \frac{\pm\sqrt{13} \pm \sqrt{-7}}{2}$$

である．よって $F = \mathbb{Q}(\sqrt{13}, \sqrt{-7})$. また

$$[F : \mathbb{Q}] = [F : \mathbb{Q}(\sqrt{13})][\mathbb{Q}(\sqrt{13}) : \mathbb{Q}] = 2^2$$

である．ここで $\sigma, \tau \in \mathrm{Gal}(F/\mathbb{Q})$ を

$$\sigma : \sqrt{13} \mapsto -\sqrt{13}, \sqrt{-7} \mapsto \sqrt{-7}, \qquad \tau : \sqrt{13} \mapsto \sqrt{13}, \sqrt{-7} \mapsto -\sqrt{-7}$$

で定めると，$\sigma^2 = \tau^2 = \mathrm{id}_F, \sigma\tau = \tau\sigma$ だから $\#\langle\sigma, \tau\rangle = 2^2 = \#\mathrm{Gal}(F/\mathbb{Q})$. よって $\mathrm{Gal}(F/\mathbb{Q}) = \langle\sigma, \tau\rangle \cong (\mathbb{Z}/2\mathbb{Z})^2$.

(2) $g(X) = f(X-1)$ とおく．$g(X) \bmod p$ が $\mathbb{F}_p$ 上可約であることを示せば良い．

- 13 が $\bmod p$ の平方剰余の時：$n^2 = 13 \bmod p$ となる $n \in \mathbb{F}_p$ が取れるから

$$g(X) = (X^2 + 5)^2 - 13X^2 = (X^2 + 5)^2 - n^2X^2 = (X^2 + 5 + nX)(X^2 + 5 - nX).$$

- -7 が $\bmod p$ の平方剰余の時：$g(X) = (X^2 - 5)^2 + 7X^2$ だから上と同様.
- 上記以外の時：$13 \cdot (-7) = -91$ は $\bmod p$ の平方剰余だから，$n^2 = -91 \bmod p$ となる $n \in \mathbb{F}_p$ が取れる．また $2 \in \mathbb{F}_p^\times$ だから

$$g(X) = \left(X^2 - \frac{3}{2}\right)^2 + \frac{91}{4} = \left(X^2 - \frac{3}{2}\right)^2 - \frac{n^2}{4} = \left(X^2 - \frac{3+n}{2}\right)\left(X^2 - \frac{3-n}{2}\right).$$

□

1995 年度 (平成 7 年度)

問 3

素体 $\mathbb{F}_p$ に成分をもつ

$$\begin{pmatrix} 1 & a & d & f \\ 0 & 1 & b & e \\ 0 & 0 & 1 & c \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

なる形の行列全てよりなり，行列の積を演算とする群を G とする．G から $\mathbb{F}_p$ の加法群への準同型写像を全て求めよ．

解答.

$$g_1 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad g_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad g_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

とおくと

$$g_1^{-1}g_2^{-1}g_1g_2 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad g_2^{-1}g_3^{-1}g_2g_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$(g_1^{-1}g_2^{-1}g_1g_2)^{-1}g_3^{-1}(g_1^{-1}g_2^{-1}g_1g_2)g_3 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

である．これら 7 個の行列は 4 次行列に左から掛けると行基本変形に対応する．一方 G の任意の元は，単位行列に行基本変形をすれば得られるから，g_1, g_2, g_3 は G の生成元である．$g_1^p = g_2^p = g_3^p = I$ であり，これ以外に g_i の間に関係式は存在しない（これは g_i が基本変形に対応することからわかる）ので，

$$G = \langle g_1, g_2, g_3 | g_1^p = g_2^p = g_3^p = I \rangle$$

である．準同型 $\varphi : G \to \mathbb{F}_p$ は $\varphi(g_i^p) = p\varphi(g_i) = 0 = \varphi(I)$ を満たすから，$i, j, k \in \mathbb{F}_p$ を任意に取り $g_1 \mapsto i, g_2 \mapsto j, g_3 \mapsto k$ から定まる p^3 個の写像が求めるものである． □

問 4

有限群 G の体 K 上の群環 $K[G]$ について次の問に答えよ.

(1) $K[G]$ の元 a を

$$a = \sum_{g \in G} a_g g \qquad (a_g \in K)$$

と表し，$K[G]$ の部分集合 A を

$$A = \left\{ a \in K[G] \,;\, \sum_{g \in G} a_g = 0 \right\}$$

と定義する．A は $K[G]$ の両側イデアルであることを示せ.

(2) $K[G] = A \oplus B$ なる $K[G]$ の左イデアル B を全て求めよ.

解答. (1) 任意の $a, b \in A$ に対し

$$a + b = \sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g, \qquad \sum_{g \in G} (a_g + b_g) = 0$$

だから $a + b \in A$. また任意の $x \in G$ に対し

$$xa = \sum_{g \in G} a_g xg = \sum_{x^{-1}h \in G} a_{x^{-1}h} h, \qquad \sum_{x^{-1}h \in G} a_{x^{-1}h} = \sum_{g \in G} a_g = 0$$

だから $xa \in A$. よって任意の $x' \in K[G]$ に対し $x'a \in A$ となるから，A は $K[G]$ の左イデアルである．右イデアルであることも同様.

(2) B の生成元 $\sum_{g \in G} a_g g$ を任意に取ると，

$$B \ni \left(\sum_{h \in G} h \right) \left(\sum_{g \in G} a_g g \right) = \sum_{g \in G} a_g \left(\sum_{h \in G} hg \right) = \sum_{g \in G} a_g \left(\sum_{h \in G} h \right)$$

である．ただし最後の等号は，$g \in G$ を固定した時写像 $G \to G, h \mapsto hg$ が全単射であることによる．$A \oplus B = K[G]$ より $\sum_{g \in G} a_g \neq 0$ だから $\sum_{h \in G} h \in B$. よって $I := (\sum_{g \in G} g) \subset B$ である．一方，任意に $x \in K[G]$ を取ると

$$x = \sum_{g \in G} x_g g = \sum_{g \in G} \left(x_g - \frac{1}{|G|} \sum_{h \in G} x_h \right) g + \sum_{g \in G} \left(\frac{1}{|G|} \sum_{h \in G} x_h \right) g \in A \oplus I$$

だから $K[G] \subset A \oplus I$. 従って

$$A \oplus I \subset A \oplus B = K[G] \subset A \oplus I$$

なので，答えは

$$B = I = \left(\sum_{g \in G} g \right)$$

のみ. □

1994 年度 (平成 6 年度)

問 3

8 個の元からなる有限体 $\mathbb{F}_8$ 上の方程式

$$y^2 + y = x^7 + x^3$$

の解 (x, y) の個数を求めよ.

解答. $x = 0$ の時は $y^2+y = 0$ だから $y = 0, 1$. 以下 $x \neq 0$ とする. $\mathbb{F}_2$ 上の既約多項式 $t^3+t+1 \in \mathbb{F}_2[t]$ の根の一つを α とすれば $\mathbb{F}_8 \cong \mathbb{F}_2[\alpha]/(\alpha^3+\alpha+1)$ である. $x = x_0+x_1\alpha+x_2\alpha^2, y = y_0+y_1\alpha+y_2\alpha^2$ $(x_i, y_i \in \mathbb{F}_2)$ とおくと, $\alpha^4 = \alpha \cdot \alpha^3 = \alpha(-\alpha - 1) = \alpha^2 + \alpha$ であることから

$$x^2 = x_0^2 + x_1^2\alpha^2 + x_2^2\alpha^4 = x_0 + x_2\alpha + (x_1 + x_2)\alpha^2.$$

よって

$$\begin{aligned}
y^2 + y &= (y_0 + y_2\alpha + (y_1 + y_2)\alpha^2) + (y_0 + y_1\alpha + y_2\alpha^2) \\
&= (y_1 + y_2)\alpha + y_1\alpha^2, \\
x^7 + x^3 &= 1 + (x_0 + x_2\alpha + (x_1 + x_2)\alpha^2)(x_0 + x_1\alpha + x_2\alpha^2) \\
&= 1 + x_0^2 + (x_0x_1 + x_0x_2)\alpha + (x_0x_2 + x_1x_2 + (x_1 + x_2)x_0)\alpha^2 \\
&\quad + (x_2^2 + (x_1 + x_2)x_1)\alpha^3 + (x_1 + x_2)x_2\alpha^4 \\
&= 1 + x_0 + x_2 + (x_1 + x_2)x_1 + (\alpha, \alpha^2 \text{ の項}).
\end{aligned}$$

従って x_1, x_2 を任意に一組決めると, 方程式の $\alpha^0, \alpha^1, \alpha^2$ の係数を比較して x_0, y_1, y_2 が一意に定まる. (この時 $(x_0, x_1, x_2) \neq (0, 0, 0)$ だから $x \neq 0$ である.) また y_0 は任意だから解は $2^3 = 8$ 個.

以上から答えは $2 + 8 = 10$. □

実施年度不明 1

問 1

k を可換体とする．乗法群 $k^\times = k - \{0\}$ が有限生成の群なら，k は有限体であることを示せ．

解答. k の標数が 0 であるとすると，$k^\times$ は $\mathbb{Q}^\times$ を含む．$k^\times$ は有限生成だから，その部分群 $\mathbb{Q}^\times$ も有限生成となる[5] が，$\mathbb{Q}^\times$ は無限個の素数で生成されるから矛盾．よって k の標数は $p > 0$. もし $\mathbb{F}_p$ 上超越的な $x \in k^\times$ が存在すれば，$k^\times$ の部分群 $\mathbb{F}_p(x)^\times$ は有限生成となる．ところが $\mathbb{F}_p[x]$ は既約多項式を無限個含むから，上と同様に矛盾．従って任意の $x \in k^\times$ は $\mathbb{F}_p$ 上代数的であるから，$k^\times$ の生成元は $g_1, \ldots, g_n \, (g_i \in \mathbb{F}_{p^{k_i}})$ とおける．この時十分大きい N が存在して $k^\times \subset \mathbb{F}_{p^N}$ となるから示された． □

[5] https://math.stackexchange.com/questions/137287/ を参照.

実施年度不明 2

問 2

(i) ちょうど 4 個の共役類を持つ有限群の同型類は有限個しかないことを示せ.
(ii) そのような有限群のうち，位数が 3 の倍数でないものの同型類を全て求めよ.

解答. (i) 群 G の位数を N とし，共役類を $O_i\,(i=1,\dots,4)$ とおく．O_i の代表元を x_i（ただし $x_4=1$）とし，$|O_1|\geq|O_2|\geq|O_3|$ としておく．$Z_G(x_i)=\{g\in G;\, x_ig=gx_i\}$ を x_i の中心化群とし，$|Z_G(x_i)|=n_i$ とおく．$|O_i|=[G:Z_G(x_i)]=N/n_i, n_4=N$ だから，類等式より

$$\frac{1}{n_1}+\frac{1}{n_2}+\frac{1}{n_3}+\frac{1}{N}=1$$

である．$n_1\leq n_2\leq n_3\leq N$ より $1\leq\frac{4}{n_1}$ なので $n_1=2,3,4$ である．n_1 を固定すると $1\leq\frac{1}{n_1}+\frac{3}{n_2}$ より $n_2\leq 3(1-\frac{1}{n_1})^{-1}$. 同様にして $n_3\leq 2(1-\frac{1}{n_1}-\frac{1}{n_2})^{-1}$ だから N の取りうる範囲は有限．ここで N を固定した時，任意に $g\in G$ を取ると全単射 $G\to G, x\mapsto gx$ は $N!$ 通りあり得るから，G に入る積は高々 $N\cdot N!$ 通り．よって G も有限個である．

(ii) • $n_1=4$ の時：$\frac{3}{4}=\frac{1}{n_2}+\frac{1}{n_3}+\frac{1}{N}\leq\frac{1}{4}+\frac{1}{4}+\frac{1}{4}=\frac{3}{4}$ だから $n_2=n_3=N=4$. よって G は位数が素数の平方だから Abel 群．従って $G\cong\mathbb{Z}/4\mathbb{Z},(\mathbb{Z}/2\mathbb{Z})^2$.

• $n_1=3$ の時：$n_2\leq\frac{9}{2}$ だから $n_2=3,4$ である．$n_2=4$ なら $n_3\leq\frac{24}{5}$ より $n_3=4$. この時 $N=6$ だから不適．$n_2=3$ なら $\frac{1}{n_3}+\frac{1}{N}=\frac{1}{3}$ より $(n_3-3)(N-3)=9$ だから $(n_3-3,N-3)=(1,9),(3,3)$. いずれも $3\mid N$ なので不適.

• $n_1=2$ の時：$n_2\leq 6$ である.

(a) $n_2=6$ の時：$\frac{1}{3}=\frac{1}{n_3}+\frac{1}{N}\leq\frac{1}{6}+\frac{1}{6}=\frac{1}{3}$ より $n_3=N=6$ となり不適.

(b) $n_2=5$ の時：$n_3\leq\frac{20}{3}$ より $n_3=5,6$ である．$\frac{1}{2}+\frac{1}{5}+\frac{1}{6}=\frac{13}{15}$ だから $n_3=6$ は不適で $n_3=5$. この時 $N=10$ で Sylow の定理より G は位数 5 の正規部分群 $H=\langle x\rangle$ を唯一つ持つ．$y\in G\setminus H$ は位数 2 だから，$K=\langle y\rangle$ とおくと $H\cap K=\{1\}, G=HK$ である．よって $\sigma: K\to\mathrm{Aut}(H)$ があって $G=H\rtimes_\sigma K$ となる．$\mathrm{Aut}(H)\cong(\mathbb{Z}/5\mathbb{Z})^\times\cong\mathbb{Z}/4\mathbb{Z}$ だから σ は $y\mapsto(x\mapsto x), y\mapsto(x\mapsto x^2)$ の 2 通りあるが，前者は $G\cong H\times K\cong\mathbb{Z}/10\mathbb{Z}$ で共役類が 10 個なので不適．後者は $G=\langle x,y\,|\,x^5=y^2=1, yxy=x^2\rangle\cong D_5$ となる.

(c) $n_2=4$ の時：$\frac{1}{n_3}+\frac{1}{N}=\frac{1}{4}$ より $(n_3-4)(N-4)=16$ だから $(n_3,N)=(5,20),(6,12),(8,8)$ である．$(6,12)$ は $3\mid N$ なので不適．$(8,8)$ の時は G の既約複素指標 $\chi_i\,(i=1,\dots,4)$ の次数を d_i とすると $\sum_{i=1}^4 d_i^2=|G|=8$ となるが，そのような d_i は存在しないから不適．$(5,20)$ の時は $|Z_G(x_3)|=5$ だが，Sylow の定理より G の Sylow-5 部分群は唯一つだから $G\rhd Z_G(x_3)$. よって $|G/Z_G(x_3)|=4$ だから $G/Z_G(x_3)$ は Abel 群であり，共役類の個数は 4 個．これは G の共役類の個数に等しいから矛盾.

(d) $n_2=3$ の時：$\frac{1}{n_3}+\frac{1}{N}=\frac{1}{6}$ より $(n_3-6)(N-6)=36$. $3\nmid N$ より $n_3-6=9,18,36$ となるが，いずれも $n_3>N$ なので不適.

以上から答えは $\mathbb{Z}/4\mathbb{Z},(\mathbb{Z}/2\mathbb{Z})^2, D_5$ の 3 個. □

問 4

k を標数が 2 と異なる可換体，a, b を 0 でない k の元とする．X を 3 次元射影空間内の 2 次曲面

$$\{(x : y : z : w) \in \mathbb{P}^3(k)\,;\, x^2 = y^2 + az^2 + bw^2\}$$

として，点 $(1 : 1 : 0 : 0)$ におけるこの 2 次曲面の接平面を H を考える．

(i) $\{p \in X\,;\, p \notin H\}$ から k^2 への全単射で，X の点の座標に関する有理式で表されるものを一つ与えよ．

(ii) k が位数 q の有限体のとき，集合 X の位数を求めよ．

解答. (i) $p_0 = (1 : 1 : 0 : 0)$ とし，$F(x, y, z, w) = x^2 - (y^2 + az^2 + bw^2)$ とおく．$(F_x, F_y, F_z, F_w)|_{p_0} = (2, -2, 0, 0)$ で k の標数は 2 でないから $H = \{x - y = 0\}$ である．$f : X \setminus H \to k^2$ を

$$(x : y : z : w) \mapsto \left(\frac{z}{x-y}, \frac{w}{x-y}\right)$$

で定める．任意に $(\alpha, \beta) \in k^2$ を取る．$(x : y : z : w) \in X \setminus H$ が $f(x : y : z : w) = (\alpha, \beta)$ を満たすとする．$z = \alpha(x - y), w = \beta(x - y)$ より $x^2 - y^2 = a\alpha^2(x - y)^2 + b\beta^2(x - y)^2$ だから $\frac{x+y}{x-y} = a\alpha^2 + b\beta^2$. よって $(a\alpha^2 + b\beta^2 - 1)x = (a\alpha^2 + b\beta^2 + 1)y$ であるが，k の標数が 2 でないから，x, y の係数が共に 0 になることはない．従って $(x : y : z : w) \in X \setminus H$ は一意に決まる．よって f は全単射であるから，これが求めるものである．

(ii) $X_0 = (X \cap H) \cap \{x = 0\}, X_1 = (X \cap H) \cap \{x \neq 0\}$ とおく．

$$\begin{aligned} X_0 &= \{(0 : 0 : z : w) \in \mathbb{P}^3(k)\,;\, az^2 + bw^2 = 0\} \\ &= \{(0 : 0 : z : 1) \in \mathbb{P}^3(k)\,;\, (az)^2 + ab = 0\}, \\ X_1 &= \{(1 : 1 : z : w) \in \mathbb{P}^3(k)\,;\, az^2 + bw^2 = 0\} \end{aligned}$$

である．

• $-ab$ が k の平方数でない時:$\#X_0 = 0$ である．$(1 : 1 : z : w) \in X_1$ が $z \neq 0$ であれば $(bw/z)^2 + ab = 0$ となるが，仮定から矛盾．よって $z = 0$ だから，$b \neq 0$ より $w = 0$. 従って $X_1 = \{(1 : 1 : 0 : 0)\}$ なので $\#X = q^2 + 0 + 1 = q^2 + 1$.

• $-ab$ が k の平方数の時:$\#X_0 = 2$ である．$-ab = c^2\ (c \in k)$ とおくと $a(az^2 + bw^2) = (az)^2 - (cw)^2 = (az + cw)(az - cw)$ だから

$$X_1 = \{(1 : 1 : z : w) \in \mathbb{P}^3(k)\,;\, az \pm cw = 0\}.$$

k の標数が 2 でないから，$az + cw = az - cw = 0$ となるのは $z = w = 0$ に限る．よって $\#X_1 = q + q - 1 = 2q - 1$ なので $\#X = q^2 + 2 + (2q - 1) = (q + 1)^2$.

ここで $-ab$ が k の平方数であること，すなわち $T^2 + ab = 0$ が k において根を持つことは，$k[T]$ において $T^q - T$ が $T^2 + ab$ で割り切れることと同値．$T^q - T = T((T^2)^{(q-1)/2} - 1)$ を $T^2 + ab$ で割った余りは $((-ab)^{(q-1)/2} - 1)T$ だから，

$$\#X = \begin{cases} (q+1)^2 & ((-ab)^{(q-1)/2} = 1) \\ q^2 + 1 & ((-ab)^{(q-1)/2} \neq 1). \end{cases}$$

□

(補足) q が素数なら，最後の議論は Legendre 記号を使うほうが楽.

実施年度不明 4

問 3

x^7-1 および x^5-1 を有限体 $\mathbb{F}_2$ 上の多項式環 $\mathbb{F}_2[x]$ の元と考えて既約多項式の積に分解せよ．

解答． • x^7-1：

$$\begin{aligned}\frac{x^7-1}{x-1} &= x^6+x^5+x^4+x^3+x^2+x+1\\ &= (x^3+1)^2+(x^3+1)x^2+(x^3+1)x+x^3\\ &= (x^3+1+x^2)(x^3+1+x)\end{aligned}$$

であり，x^3+x^2+1, x^3+x+1 は $x=0,1$ を根に持たないから $\mathbb{F}_2$ 上既約．従って

$$x^7-1=(x-1)(x^3+x^2+1)(x^3+x+1).$$

• x^5-1：$f(x)=x^4+x^3+x^2+x+1$ とおくと $x^5-1=(x-1)f(x)$ である．f は $x=0,1$ を根に持たないから，可約であるとすると既約な 2 次式 2 つの積になる．ところが $\mathbb{F}_2$ 上既約な 2 次式は x^2+x+1 のみであり $(x^2+x+1)^2=x^4+x^2+1\neq f$ だから，f は $\mathbb{F}_2$ 上既約．従って

$$x^5-1=(x-1)(x^4+x^3+x^2+x+1).$$

□

問 4

$f(x)=x^4+1$ とし，体 K について L を $f(x)$ の K 上の最小分解体とする．次の 2 つの場合に L/K のガロア群の構造を決定せよ．

(1) $K=\mathbb{F}_p$（有限体．p は素数）

(2) $K=\mathbb{Q}$（有理数体）

解答. (1) $p=2$ の時は $f(x)=(x+1)^4$ だから $L=K$. よって $\mathrm{Gal}(L/F)\cong\{1\}$. 以下 $p\geq 3$ とする．

• $8\mid(p-1)$ の時：$f(x)=0$ の根 a は $a^8=(-1)^2=1$ を満たすから $a^{p-1}=1$. よって $a\in\mathbb{F}_p$ なので $L=K$ となり，$\mathrm{Gal}(L/K)=\{1\}$.

• $8\nmid(p-1), 4\mid(p-1)$ の時：$(\frac{-1}{p})=(-1)^{(p-1)/2}=1$ より $n^2=-1$ となる $n\in\mathbb{F}_p$ が取れる．この時

$$f(x)=x^4-n^2=(x^2+n)(x^2-n).$$

よって $x^2-n=0$ の根の一つを a とすれば $f(x)=0$ の根は $\pm a,\pm an$ なので，$L=K(a)$. ここで p の仮定と $a^4=n^2=-1$ より $a^{p-1}=-1$ となる．これと $a\neq 0$ より $a\notin\mathbb{F}_p$ である．従って $[L:K]=2$ なので $\mathrm{Gal}(L/K)\cong\mathbb{Z}/2\mathbb{Z}$.

• $4\nmid(p-1)$ の時：-1 は $\mathrm{mod}p$ の平方非剰余であるから，± 2 のどちらか一方のみが $\mathrm{mod}p$ の平方剰余である．$n^2=2$ となる $n\in\mathbb{F}_p$ が存在したとする．$a^2=-2$ となる a を取る．$2\in\mathbb{F}_p^\times$ だから

$$\begin{aligned}f(x)&=(x^2+1)^2-2x^2=(x^2+1)^2-n^2x^2\\&=(x^2+1+nx)(x^2+1-nx)\\&=\left(\left(x+\frac{n}{2}\right)^2-\frac{a^2}{4}\right)\left(\left(x-\frac{n}{2}\right)^2-\frac{a^2}{4}\right).\end{aligned}$$

よって $f(x)=0$ の根は $(\pm n\pm a)/2$ なので $L=K(a)$. 従って $[L:K]=2$ なので $\mathrm{Gal}(L/K)\cong\mathbb{Z}/2\mathbb{Z}$. -2 が $\mathrm{mod}p$ の平方剰余の時も，$f(x)=(x^2-1)^2+2x^2$ より同様に $\mathrm{Gal}(L/K)\cong\mathbb{Z}/2\mathbb{Z}$.

以上をまとめると

$$\mathrm{Gal}(L/K)\cong\begin{cases}\{1\} & (p=2 \text{ または } p\equiv 1 \bmod 8)\\ \mathbb{Z}/2\mathbb{Z} & (\text{それ以外})\end{cases}$$

(2) $f(x)$ は 1 の原始 8 乗根 $\zeta=e^{2\pi i/8}$ の $\mathbb{Q}$ 上の最小多項式だから，$L=K(\zeta)$. よって

$$\mathrm{Gal}(L/K)\cong(\mathbb{Z}/8\mathbb{Z})^\times=\langle 3\rangle\times\langle 5\rangle\cong(\mathbb{Z}/2\mathbb{Z})^2.$$

□

1983 年度 (昭和 58 年度)

問 102

$f(x)$ は体 k 上で既約な最高次係数 1 の多項式で $f(x^2)$ が $f(x)$ で割り切れるものとする．$f(x) \neq 1, x$ のとき，

(i) $f(x) = 0$ の根は位数が奇数の 1 の冪根であることを示せ．

(ii) $k = \mathbb{Q}$（有理数体）のとき $f(x^4)$ はいくつの $\mathbb{Q}$ 上既約な多項式の積に分解するか．

(iii) $k = \mathbb{Q}$ のとき次数が 6 以下の $f(x)$ を全て求めよ．

解答. (i) a が $f(x)$ の根なら仮定より $f(a^2) = 0$ だから，a^2 も $f(x)$ の根である．同様にして a^{2^n} $(n = 1, 2, \dots)$ も $f(x)$ の根であるが，f は多項式だから，$a^{2^n} = a$ となる n が存在する．今 $f(x)$ は k 上既約だから $a \neq 0$ である．よって $a^{2^n - 1} = 1$.

(ii) 1 の原始 n 乗根を ζ_n とおき，$\Phi_n(x) = \prod_{(n,d)=1}(x - \zeta_n^d)$ を円分多項式とする．(i) より f はある ζ_n の $\mathbb{Q}$ 上最小多項式で割り切れるが，仮定から奇数 n が存在して $f(x) = \Phi_n(x)$ となる．ここで

$$\Phi_{2m}(x) = \begin{cases} \Phi_m(x^2) & (2 \mid m) \\ \Phi_m(x^2)/\Phi_m(x) & (2 \nmid m) \end{cases} \tag{$*$}$$

であるから，

$$f(x^4) = \Phi_n(x^4) = \Phi_n(x^2)\Phi_{2n}(x^2) = \Phi_n(x)\Phi_{2n}(x)\Phi_{4n}(x).$$

円分多項式は $\mathbb{Q}$ 上既約だから，答えは 3.

(iii) $n = 1$ の時は $f(x) = \Phi_1(x) = x - 1$ で，これは条件を満たす．以下 $n \geq 3$ とする．$\varphi(x)$ を Euler 関数とする．n の素因数分解を $\prod_j p_j^{e_j}$ とすると

$$6 \geq \deg \Phi_n = \varphi(n) = \prod_j p_j^{e_j - 1}(p_j - 1)$$

だから，n の素因数としてありうるのは $3, 5, 7$ のみである．$7 \mid n$ の時は $n = 7$ のみ．$7 \nmid n$ の時は $\varphi(3^a) = 3^{a-1} \cdot 2 \leq 6$ となるのは $3, 3^2$ の 2 つ．$\varphi(5^b) = 5^{b-1} \cdot 4 \leq 6$ となるのは 5 のみ．また $\varphi(3^a 5^b) = 3^{a-1} \cdot 2 \cdot 5^{b-1} \cdot 4 > 6$ だから，答えは

$$\begin{aligned} &\Phi_1(x) = x - 1, \quad \Phi_3(x) = x^2 + x + 1, \\ &\Phi_5(x) = x^4 + x^3 + x^2 + x + 1, \\ &\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \\ &\Phi_9(x) = \frac{x^9 - 1}{\Phi_1(x)\Phi_3(x)} = x^6 + x^3 + 1 \end{aligned}$$

の 5 個. □

(補足) $(*)$ は手元の教科書には書かれているものがなかったが，教科書によっては公式として扱われている[6] ので既知とした．$\Phi_n(x) = \prod_{d \mid n}(x^{n/d} - 1)^{\mu(d)}$ （μ は Möbius 関数）を使う証明や，$\Phi_m(x^2)$ の根に注目した証明がある．

[6] 例えば Lang, S. (2002). Algebra. Graduate Texts in Mathematics, vol 211. Springer, P280

1982 年度 (昭和 57 年度)

問 104

有理数体 $\mathbb{Q}$ 上代数的である 2 つの複素数 α, β に対して，2 変数多項式環 $\mathbb{Q}[x, y]$ のイデアル I を

$$I = \{f(x, y) \in \mathbb{Q}[x, y]\,;\, f(\alpha, \beta) = 0\}$$

で定義する．

(i) I は $\mathbb{Q}[x, y]$ の極大イデアルであるか？

(ii) p を素数とし

$$\alpha = e^{2\pi\sqrt{-1}/p}, \quad \beta = \sqrt{p}$$

とするとき，I の生成元を具体的に一組求めよ．その際生成元の個数を最小となるように取り，その最小性の証明も与えよ．

解答． (i) $I \subsetneq J$ となる $\mathbb{Q}[x, y]$ のイデアル J が存在したとする．$g(x, y) \in J \backslash I$ を取ると $a := g(\alpha, \beta) \neq 0$ だから，$g(x, y) - a \in I$. よって $a \in g(x, y) + I \subset J$ から $1 \in J$ なので $J = \mathbb{Q}[x, y]$. 従って I は $\mathbb{Q}[x, y]$ の極大イデアル．

(ii) $f(x) = x^{p-1} + \cdots + x + 1, g(x) = x^2 - p$ とおく．全射な環準同型 $\varphi : \mathbb{Q}[x, y] \to \mathbb{Q}[\alpha, \beta] = \mathbb{Q}(\alpha, \beta)$ を $x \mapsto \alpha, y \mapsto \beta$ で定める．$(f, g) \subset \operatorname{Ker}\varphi = I$ は明らか．$h(x, y) \in \mathbb{Q}[x, y]$ は

$$\sum_{j=0}^{p-1}\sum_{k=0}^{1} a_{jk}x^j y^k + h(x, y) \quad (h \in (f, g))$$

とおける．これが I の元とすると

$$\sum_{j=0}^{p-1}\sum_{k=0}^{1} a_{jk}\alpha^j \beta^k = 0.$$

今 $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\beta)][\mathbb{Q}(\beta) : \mathbb{Q}] = 2(p - 1)$ だから，$\alpha^j \beta^k\, (0 \leq j \leq p - 1, k = 0, 1)$ は $\mathbb{Q}$ 上一次独立．よって $a_{jk} = 0$ なので $h \in (f, g)$. 従って $I = (f, g)$ である．これが単項イデアルであったとして，生成元を h とおく．$f \in (h), g \in (h)$ で f, g は共通因子を持たないから $fg \mid h$. よって $h = fga\, (a \in \mathbb{Q}[x, y])$ とおける．$f \in I = (h) = (fga)$ だから $gab = 1$ となる $b \in \mathbb{Q}[x, y]$ が存在するが，g は定数でないから矛盾． □

1981 年度 (昭和 56 年度)

問 103

p を素数とする．p 進整数環 $\mathbb{Z}_p$ の（p 進位相に関する）コンパクト開集合全体の族 A から有理数体 $\mathbb{Q}$ の中への写像 μ が次の二つの条件を満たすものとする．

(i) $U, V \in A, U \cap V = \emptyset$ ならば $\mu(U \cup V) = \mu(U) + \mu(V)$.

(ii) $\mathbb{Q}$ 係数の一変数 k 次多項式 $F(t) \in \mathbb{Q}[t]\ (k \geq 1)$ が存在して，任意の自然数 N および $0 \leq a \leq p^N - 1$ なる任意の整数 a に対して

$$\mu(a + p^N \mathbb{Z}_p) = p^{N(k-1)} F\left(\frac{a}{p^N}\right)$$

と表される．

このとき $F(t+1) - F(t)$ は t^{k-1} の定数倍であることを示し，$\mu(\mathbb{Z}_p^\times)$ を F の特殊値を用いて表わせ．ただし $\mathbb{Z}_p^\times$ は $\mathbb{Z}_p$ の単数群である．

解答. 任意の $N \in \mathbb{N}$ と $0 \leq a \leq p^N - 1$ に対し

$$\begin{aligned} p^{N(k-1)} F\left(\frac{a}{p^N}\right) = \mu(a + p^N \mathbb{Z}_p) &= \sum_{j=0}^{p-1} \mu(a + jp^N + p^{N+1} \mathbb{Z}_p) \\ &= \sum_{j=0}^{p-1} p^{(N+1)(k-1)} F\left(\frac{a + jp^N}{p^{N+1}}\right) \end{aligned}$$

である．N と a を動かした時 a/p^N は相異なる $k+1$ 個以上の値を取り，$\deg F = k$ であるから，$t = a/p^N$ とおいた

$$F(t) = p^{k-1} \sum_{j=0}^{p-1} F\left(\frac{t+j}{p}\right) \tag{$*$}$$

は t についての恒等式である．よって

$$F(t+1) - F(t) = p^{k-1}\left(F\left(\frac{t+p}{p}\right) - F\left(\frac{t}{p}\right)\right) = p^{k-1}\left(F\left(\frac{t}{p} + 1\right) - F\left(\frac{t}{p}\right)\right).$$

ここで $\deg(F(t+1) - F(t)) = k - 1$ より $F(t+1) - F(t) = a_{k-1}t^{k-1} + \cdots + a_1 t + a_0$ とおけるから，代入して t^j の係数を比べると $a_j = p^{k-1-j} a_j$. よって $a_0 = \cdots = a_{k-2} = 0$ なので，$c \in \mathbb{Q}$ があって $F(t+1) - F(t) = ct^{k-1}$ と書ける．また

$$\mu(\mathbb{Z}_p^\times) = \sum_{j=1}^{p-1} \mu(j + p\mathbb{Z}_p) = \sum_{j=1}^{p-1} p^{k-1} F\left(\frac{j}{p}\right) = (1 - p^{k-1}) F(0)$$

である．ただし最後の等号は $(*)$ で $t = 0$ とした等式による． □

1980 年度 (昭和 55 年度)

問 101

p を奇素数とする．$\alpha = \tan\dfrac{2\pi}{p}$ は有理数体 $\mathbb{Q}$ 上で代数的であることを示せ．さらに $\mathbb{Q}$ に α を添加した体 $\mathbb{Q}(\alpha)$ は $\mathbb{Q}$ のガロア拡大体であることを示し，そのガロア群 $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ を記述せよ．

解答. $\zeta = e^{2\pi i/p}$ とおく．ζ, i は $\mathbb{Q}$ 上代数的だから

$$\alpha = \frac{\sin\frac{2\pi}{p}}{\cos\frac{2\pi}{p}} = \frac{\zeta - \zeta^{-1}}{i(\zeta + \zeta^{-1})} \in \mathbb{Q}(\zeta, i)$$

も $\mathbb{Q}$ 上代数的である．

$K = \mathbb{Q}(\alpha), L = \mathbb{Q}(\zeta, i)$ とおくと K は L の部分体であり，$L/\mathbb{Q}$ は Galois 拡大で $[L:\mathbb{Q}] = 2(p-1)$ である.[7] ここで $\sigma_j, \tau \in G := \mathrm{Gal}(L/\mathbb{Q})\,(j = 1, 2, \ldots, p-1)$ を

$$\sigma_j : \zeta \mapsto \zeta^j, i \mapsto i, \qquad \tau : \zeta \mapsto \zeta, i \mapsto -i$$

で定める．$\tau^2 = \mathrm{id}_L, \sigma_j\tau = \tau\sigma_j$ だから，$\mathbb{F}_p^\times$ の生成元 k を取れば $\langle \sigma_k, \tau\rangle \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. 位数を比較してこれが G である．これは Abel 群だから，K に対応する G の部分群 H は G の正規部分群となる．従って $K/\mathbb{Q}$ も Galois 拡大である．α を固定する G の元を求める．

$$\sigma_j(\alpha) - \alpha = \frac{\zeta^j - \zeta^{-j}}{i(\zeta^j + \zeta^{-j})} - \frac{\zeta - \zeta^{-1}}{i(\zeta + \zeta^{-1})} = \frac{2(\zeta^{j-1} - \zeta^{-j+1})}{i(\zeta^j + \zeta^{-j})(\zeta + \zeta^{-1})}$$

が 0 となることは $\zeta^{2(j-1)} = 1$ と同値．p は奇数だから $j = 1$.

$$\tau\sigma_j(\alpha) - \alpha = \frac{\zeta^j - \zeta^{-j}}{-i(\zeta^j + \zeta^{-j})} - \frac{\zeta - \zeta^{-1}}{i(\zeta + \zeta^{-1})} = \frac{-2(\zeta^{j+1} - \zeta^{-j-1})}{i(\zeta^j + \zeta^{-j})(\zeta + \zeta^{-1})}$$

が 0 となることは $\zeta^{2(j+1)} = 1$ と同値．よって $j = p-1$. 以上から $H = \{\sigma_1 = \mathrm{id}_L, \tau\sigma_{p-1}\} \cong \mathbb{Z}/2\mathbb{Z}$ だから $|\mathrm{Gal}(K/\mathbb{Q})| = |G/H| = p-1$. また $\sigma_k H \in G/H$ の位数は $p-1$ だから $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/(p-1)\mathbb{Z}$. □

[7] 京大数理研平成 14 年度専門問 1 と同様に示せる．

問 105

複素数体 $\mathbb{C}$ 上の 3 変数多項式環 $\mathbb{C}[x,y,z]$ のイデアル I が 3 つの元

$$zx-y^2,\quad zy-x^6,\quad z^2-yx^5$$

で生成されているとき，以下の問に答えよ．

(i) I が $\mathbb{C}[x,y,z]$ の素イデアルであることを示せ．

(ii) $\mathbb{C}[x,y,z]$ の I による商環 $R=\mathbb{C}[x,y,z]/I$ の商体 K は $\mathbb{C}$ の純粋超越拡大体であることを示せ．

(iii) R 上整であるような K の元の全体のなす K の部分環（すなわち K 内の R の整閉包）を R' とする．R' と R を $\mathbb{C}$ 上のベクトル空間とみなして，商ベクトル空間 R'/R の $\mathbb{C}$ 上の次元を求めよ．

(iv) 環 R の自己同型であって $\mathbb{C}$ の各元を固定するものの全体のなす群 G を決定せよ．

解答. (i) 全射な環準同型 $\varphi:\mathbb{C}[x,y,z]\to\mathbb{C}[t^3,t^7,t^{11}]$ を $x\mapsto t^3, y\mapsto t^7, z\mapsto t^{11}$ で定めると $I\subset\operatorname{Ker}\varphi$ である．$\mathbb{C}[x,y,z]$ の元は $f=g(x,y)+cz+h(x,y,z)\,(g\in\mathbb{C}[x,y], h\in I, c\in\mathbb{C})$ と書ける．これが $\operatorname{Ker}\varphi$ の元とすると $g(t^3,t^7)+ct^{11}=0$ である．$3n+7m=11$ となる非負整数 n,m は存在しないから t^{11} の係数から $c=0$. また京大数理研平成 20 年度専門問 3(1) と同様の議論により $g\equiv 0$ がわかるから $f\in I$. よって $\operatorname{Ker}\varphi=I$ だから，準同型定理より $\mathbb{C}[x,y,z]/I\cong\mathbb{C}[t^3,t^7,t^{11}]$. この右辺は整域なので，$I$ は素イデアルである．

(ii) $R_1:=\mathbb{C}[t^3,t^7,t^{11}]$ の商体を K_1 とおく．$t^{-1}=(t^3)^2/t^7\in K_1$ だから $\mathbb{C}(t)\subset K_1$. また逆の包含は明らかだから $K_1=\mathbb{C}(t)$. よって $K\cong K_1=\mathbb{C}(t)$ だから示された．

(iii) K_1 内の R_1 の整閉包を R_1' とする．任意の $f\in R_1'$ は 共通因子を持たない $p,q\in\mathbb{C}[t]$ を用いて $f=p/q$ と書ける．また f はある $X^n+a_{n-1}X^{n-1}+\cdots+a_0\in R_1[X]$ の根である．もし $\deg q\geq 1$ なら，$X=f$ を代入して整理すると $p^n=-a_{n-1}p^{n-1}q-\cdots-a_0q^n$. 右辺は q の根で 0 になるから p もそうなるが，これは矛盾．よって $q\in\mathbb{C}$ だから $R_1'\subset\mathbb{C}[t]$. また $X^3-t^3\in R_1[X]$ は monic で $X=t$ を根に持つから $t\in R_1'$. 以上から $R_1'=\mathbb{C}[t]$ なので

$$R'/R\cong R_1'/R_1=\mathbb{C}[t]/\mathbb{C}[t^3,t^7,t^{11}].$$

ここで $k\geq 0$ に対し $t^{9+3k},t^{10+3k},t^{11+3k}\in\mathbb{C}[t^3,t^7,t^{11}]$ であるから，$\mathbb{C}[t]/\mathbb{C}[t^3,t^7,t^{11}]$ の $\mathbb{C}$ 上の基底は t,t^2,t^4,t^5,t^8 である．よって $\dim_{\mathbb{C}}R'/R=5$.

(iv) $G\cong\operatorname{Aut}_{\mathbb{C}}R_1$ である．$\sigma\in\operatorname{Aut}_{\mathbb{C}}R_1$ は $\operatorname{Aut}_{\mathbb{C}}R_1'$ に一意に拡張されるから，$\sigma(t)=at+b\,(a,b\in\mathbb{C}, a\neq 0)$ とおける．$(at+b)^3=\sigma(t)^3=\sigma(t^3)\in R_1$ より $b=0$ が必要．逆にこの時 $\sigma(t^k)=(at)^k\in R_1\,(k=3,7,11)$ であるから，$G\cong\operatorname{Aut}_{\mathbb{C}}R_1\cong\mathbb{C}^\times$ となる． □

1979 年度 (昭和 54 年度)

問 101

各自然数 n に対し，変数 x の整数係数多項式 $f_n(x)$ であって

$$f_n\left(\frac{x^2+1}{x}\right)=\frac{x^{2n}+1}{x^n}$$

を満たすものが一意的に存在することを示せ．そして

(i) 有理数係数多項式環 $\mathbb{Q}[x]$ における $f_n(x)$ の既約因子の個数を求めよ．特に $n=12,15$ のときにこの個数を求めよ．

(ii) $f_n(x)$ が $\mathbb{Q}[x]$ において既約となるような n の値を決定せよ．

解答. $f_1(x)=x$ であり，$x^2+x^{-2}=(x+x^{-1})^2-2$ より $f_2(x)=x^2-2$ である．また

$$x^{n+1}+x^{-(n+1)}=(x+x^{-1})(x^n+x^{-n})-(x^{n-1}+x^{-(n-1)})$$

であるから，$f_{n+1}(x)=xf_n(x)-f_{n-1}(x)$ により帰納的に f_n が一意に定まる．

$t=x+x^{-1},\zeta_n=e^{2\pi i/n}$ とおく．$\Phi_n(x)=\prod_{(n,d)=1}(x-\zeta_n^d)$ を円分多項式とし，$n=2^rm\,(2\nmid m)$ とすると

$$f_n(t)=x^{-n}\frac{x^{4n}-1}{x^{2n}-1}=x^{-n}\frac{\prod_{d|4n}\Phi_d(x)}{\prod_{d|2n}\Phi_d(x)}=x^{-n}\prod_{\substack{d|4n\\ d\nmid 2n}}\Phi_d(x)=x^{-n}\prod_{d|m}\Phi_{2^{r+2}d}(x)$$

である．また

$$\sum_{d|m}\deg\Phi_{2^{r+2}d}(x)=\sum_{d|m}\varphi(2^{r+2}d)=\sum_{d|m}2^{r+1}\varphi(d)=2^{r+1}m=2n$$

だから，

$$f_n(t)=\prod_{d|m}x^{-\varphi(2^{r+2}d)/2}\Phi_{2^{r+2}d}(x).$$

ここで $n\in\mathbb{N}$ に対し，$x^{-\varphi(4n)/2}\Phi_{4n}(x)$ が t の多項式であり，それは $\mathbb{Q}$ 上既約であることを示す．上で見たように $\deg\Phi_{4n}(x)=\varphi(4n)$ は偶数だから $2k$ とおける．また $(4n,d)=1$ なら $(4n,4n-d)=1$ だから，ζ_{4n}^d が $\Phi_{4n}(x)$ の根なら $\zeta_{4n}^{4n-d}=\zeta_{4n}^{-d}$ も $\Phi_{4n}(x)$ の根である．よって $\Phi_{4n}(x)$ の $x^j,x^{2k-j}\,(j=0,1,\dots,k)$ の係数は等しく，それらを c_j とおくと

$$\begin{aligned}x^{-k}\Phi_{4n}(x)&=x^{-k}(x^{2k}+c_1x^{2k-1}+\cdots+c_{k-1}x^{k+1}+c_kx^k+c_{k-1}x^{k-1}+\cdots+c_1x+1)\\&=(x^k+x^{-k})+\sum_{j=1}^{k-1}c_j(x^{k-j}+x^{-k+j})+c_k=f_k(t)+\sum_{j=1}^{k-1}c_jf_{k-j}(t)+c_k\end{aligned}$$

は t の多項式である．また $x^{-k}\Phi_{4n}(x)=g(t)h(t)$ と書けたとすると $\Phi_{4n}(x)=x^kg(t)h(t)$ であるが，右辺の次数から $\deg g+\deg h=k$ なので $\Phi_{4n}(x)=x^{\deg g}g(t)\cdot x^{\deg h}h(t)$. ところが $\Phi_{4n}(x)$ は $\mathbb{Q}$ 上既約なので $x^{\deg g}g(t),x^{\deg h}h(t)\in\mathbb{Q}[x]$ のどちらかは定数．よって $x^{-k}\Phi_{4n}(x)$ は $\mathbb{Q}$ 上既約である．

(i) 上の議論から，m の約数の個数，すなわち n の奇数の約数の個数である．$n=12=2^2\cdot3$ の時は 2. $n=15=3\cdot5$ の時は $2^2=4$.

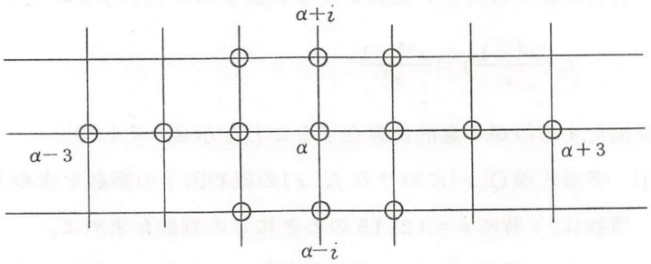
(ii) 奇数の約数を持たない n だから，$n=2^k\,(k=1,2,\dots)$. □

(補足) $x=e^{i\theta}$ とおくと $f_n(2\cos\theta)=2\cos n\theta$ だから，第一種 Chebyshev 多項式 $T_n(x)$ を用いて $f_n(x)=2T_n(x/2)$ と書ける．Chebyshev 多項式の既約因子については色々研究があるらしい.[8]

[8]例えば https://www.fq.math.ca/Papers1/52-4/DJGrubb4282014.pdf

問 103

$\mathbb{Z}$ を有理整数環，$i=\sqrt{-1}$ とし，ガウス整数環 $R=\mathbb{Z}[i]$ の元を複素平面内の格子点で表す．R の各元 α に対して下図の ◯ 印で表される 13 個の R の元の積を $P(\alpha)$ とおく．α が R の元全体を動くとき $P(\alpha)$ の R における最大公約数を求めよ．



解答. 求める最大公約数を d とおく．また $x+iy\in R$ に対し $N(x+iy)=x^2+y^2$ とおく．

$$P(2i)=(-13)(-8)(-5)(-10)(-2)i\cdot 2i\cdot 3i=2^6\cdot 3\cdot 5^2\cdot 13i,$$
$$P(5i)=(-34)(-29)(-26)(-37)(-17)4i\cdot 5i\cdot 6i=2^5\cdot 3\cdot 5\cdot 13\cdot 17^2\cdot 29\cdot 37i$$

であり，$17,29,37$ の（R における）因数は $P(2i)$ を割らないから，d は $2^5\cdot 3\cdot 5\cdot 13$ を割り切る．[9] $\alpha+j+ik\,(j,k\in\{0,\pm 1\})$ の 9 点には，実部と虚部がともに 3 の倍数の点があるから $P(\alpha)$ は 3 で割り切れる．

$R_1=(1+2i)R$ とおく．$P(\alpha)\in(1+2i)R$ を示す．それには R/R_1 の元として $P(\alpha)$ が 0 であることを示せば良い．R/R_1 の代表元は $0,1,1+i,2,2+i$ だから，α がこの 5 点の時を調べれば十分．$\alpha=0$ の時は明らか．$\alpha=1$ の時は $\alpha+1-i=-i(1+2i)\in R_1$. $\alpha=1+i$ の時は $\alpha+i=1+2i\in R_1$. $\alpha=2$ の時は $\alpha-i=-i(1+2i)\in R_1$. $\alpha=2+i$ の時は $\alpha-1+i=1+2i\in R_1$. よって示された．同様の議論で $P(\alpha)\in(1-2i)R$ がわかるから，$P(\alpha)$ は $(1+2i)(1-2i)=5$ で割り切れる．

同様に $R/(2+3i)R$ の代表元 12 個について調べれば，$P(\alpha)\in(2+3i)R$ がわかる．（$\mathbb{C}$ 上の $2+3i$ と $3-2i$ が張る格子上に，13 個の点のうち少なくとも一つが必ず存在することを見れば良い．以下の $1+i$ で割り切れる回数を調べるのも同様.）よって $P(\alpha)$ は $(2+3i)(2-3i)=13$ で割り切れる．

$2=-i(1+i)^2$ であるから，$P(\alpha)$ が $1+i$ で最低何回割り切れるか調べる．$\alpha=x+iy\in R$ が $(1+i)^2=-2i$ で割り切れることと，x,y が共に偶数であることは同値であることに注意する．

- x,y が共に奇数の時：$\alpha\pm 1\pm i$ は 2 回割り切れ, $\alpha,\alpha\pm 2$ は 1 回割り切れるから 11.
- x が奇数で y が偶数の時：$\alpha\pm 1,\alpha\pm 3$ は 2 回割り切れ, $\alpha\pm i$ は 1 回割り切れるから 10.
- x,y が共に偶数の時：$\alpha,\alpha\pm 2$ は 2 回割り切れ, $\alpha\pm 1\pm i$ は 1 回割り切れるから 10.
- x が偶数で y が奇数の時：$\alpha\pm 1,\alpha\pm 3$ は 1 回割り切れる．$\alpha=2n+(2m+1)i$ とおくと $\alpha-i=2(n+mi),\alpha+i=2(n+(m+1)i)$. $n-m$ が偶数なら $\alpha-i=2(m(1+i)+(n-m))$ は $1+i$ で 3 回割り切れ，$\alpha+i$ は 2 回割り切れる．$n-m$ が奇数の時も同様だから 9.

以上から $P(\alpha)$ は $(1+i)^9$ で割り切れる．$\alpha=2+i$ の時

$$\alpha+i=2(1+i)=-i(1+i)^3,\quad \alpha-i=2=-i(1+i)^2,\quad \alpha+1=3+i=(1+i)(2-i),$$
$$\alpha-1=1+i,\quad \alpha+3=5+i=(1+i)(3-2i),\quad \alpha-3=-1+i=i(1+i)$$

であり，$2-i,3-2i$ は R の既約元だから，$P(2+i)$ は $1+i$ で丁度 9 回割り切れる．

以上から

$$d=(1+i)^9\cdot 3\cdot 5\cdot 13=2^4\cdot 3\cdot 5\cdot 13\cdot(1+i).$$

□

[9] $P(4),P(5),P(6),P(2i),P(3i),P(4i),P(5i)$ あたりを計算すれば予想がつく．

1978 年度 (昭和 53 年度)

問 101

A を有理数を成分とする m 行 n 列の行列とする．整数を成分とする n 次元列ベクトル全体のなす加群を $\mathbb{Z}^n$ とする．$\mathbb{Z}^n$ の部分加群 L_A を

$$L_A = \{v \in \mathbb{Z}^n \,;\, Av \in \mathbb{Z}^n\}$$

によって定める．このとき次の問に答えよ．

(i) 商加群 $\mathbb{Z}^n/L_A$ は有限群であることを示せ．

(ii)

$$A = \begin{pmatrix} \frac{1}{12} & \frac{1}{6} & \frac{1}{4} & \frac{1}{3} \\ \frac{1}{6} & \frac{7}{6} & \frac{1}{2} & \frac{3}{2} \\ \frac{1}{4} & \frac{4}{3} & \frac{3}{4} & \frac{11}{6} \end{pmatrix}$$

のとき，$\mathbb{Z}^4/L_A$ を巡回群の直積に分解せよ．

解答. (i) A の成分の分母たちの最小公倍数を ℓ とすると，$(\ell\mathbb{Z})^n \subset L_A$ であるから

$$|\mathbb{Z}^n/L_A| \leq |\mathbb{Z}^n/(\ell\mathbb{Z})^n| = \ell^n < \infty.$$

(ii) A に基本変形を施すと

$$A \to \begin{pmatrix} \frac{1}{12} & \frac{1}{6} & \frac{1}{4} & \frac{1}{3} \\ 0 & \frac{5}{6} & 0 & \frac{5}{6} \\ 0 & \frac{5}{6} & 0 & \frac{5}{6} \end{pmatrix} \to \begin{pmatrix} \frac{1}{12} & \frac{1}{6} & \frac{1}{4} & \frac{1}{3} \\ 0 & \frac{5}{6} & 0 & \frac{5}{6} \\ 0 & 0 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} \frac{1}{12} & 0 & 0 & 0 \\ 0 & \frac{5}{6} & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

となるから，

$$\mathbb{Z}^4/L_A \cong \mathbb{Z}^4/(12\mathbb{Z} \times 6\mathbb{Z} \times \mathbb{Z}^2) \cong \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}.$$

□

1977 年度 (昭和 52 年度)

問 101

F を可換体，$a \in F$ とし，$b = 1 + a^2$ は F の中に平方根を持たないとする．x に関する 4 次方程式 $x^4 - 2bx^2 + a^2b = 0$ の一根を F に付け加えて得られる体を K とするとき，

(i) K は F 上のガロア拡大であることを証明せよ．

(ii) K/F のガロア群を求めよ．

(iii) $K \supsetneq F' \supsetneq F$ となる体 F' を定めよ．

解答. (i) $f(x) = x^4 - 2bx^2 + a^2b$ とおくと

$$f(x) = x^4 - 2bx^2 + (b-1)b = (x^2 - b)^2 - b = (x^2 - b + \sqrt{b})(x^2 - b - \sqrt{b})$$

だから，f の根は $\pm\alpha, \pm\beta$ である．ただし $\alpha = \sqrt{b + \sqrt{b}}, \beta = \sqrt{b - \sqrt{b}}$. $\alpha \in K$ とすると $\sqrt{b} = \alpha^2 - b \in F$ だから $\beta = a\sqrt{b}/\alpha \in F$. よって K/F は正規．また仮定より $b \neq 0$ だから $\pm\alpha, \pm\beta$ は相異なる．よって K/F は分離的なので Galois 拡大である．他の場合も同様.

(ii) 仮定から $b \equiv 0 \bmod p, b \not\equiv 0 \bmod p^2$ となる素元 $p \in F$ が存在する．この時 $a \not\equiv 0 \bmod p$ だから，$a^2b \not\equiv 0 \bmod p^2$ である．F は UFD だから，Eisenstein の既約判定法により f は F 上既約である．これより $\#\mathrm{Gal}(K/F) = \deg f = 4$ であり，$\sigma \in \mathrm{Gal}(K/F)$ であって $\sigma(\alpha) = -\beta$ となるものが存在する．この時

$$\sigma(\sqrt{b}) = \sigma(\alpha^2 - b) = \sigma(\alpha)^2 - b = \beta^2 - b = -\sqrt{b}$$

より

$$\sigma(-\beta) = \sigma(-a\sqrt{b}/\alpha) = -a(-\sqrt{b})/(-\beta) = -\alpha,$$
$$\sigma(-\alpha) = \beta, \quad \sigma(\beta) = \alpha$$

なので σ の位数は 4. よって $\mathrm{Gal}(K/F) = \langle\sigma\rangle \cong \mathbb{Z}/4\mathbb{Z}$.

(iii) $\mathrm{Gal}(K/F)$ の部分群は $\langle\sigma^2\rangle \cong \mathbb{Z}/2\mathbb{Z}$ のみだから，F' はただ一つで $[F' : F] = 2$ である．一方仮定から K の部分体 $F(\sqrt{b})$ は F の 2 次拡大なので，$F' = F(\sqrt{b})$. □

問 102

次の表の空白部分を補って，それを指標表とする有限群 G が存在するかどうかを調べ，存在すればそれを生成元と基本関係で表わせ．ただし $C_n\,(1 \leq n \leq 5)$ は G の全ての相異なる共役類で C_1 は単位元の類，$\chi_n\,(1 \leq n \leq 5)$ は G の既約複素指標とし，$i = \sqrt{-1}$ である．

	C_1	C_2	C_3	C_4	C_5
χ_1					
χ_2	1	i			
χ_3					
χ_4					
χ_5					

解答. 表の上から i 行目，左から j 列目の数字を a_{ij} とする．（すなわち $a_{21} = 1, a_{22} = i.$）χ_1 は単位指標として良いから $a_{1j} = 1.$ また C_2 の代表元を x とすると，$a_{21} = 1$ より χ_2 は 1 次表現であり，$\chi_2(x) = i$ より $x^4 = 1.$ よって x の位数は 4 なので $x^2 \in C_3, x^3 \in C_4$ として良い．この時 $a_{2j} = \chi_2(x^j) = i^j\,(j = 2, 3, 4)$ である．$|C_2| = |C_3| = |C_4| = d_1, |C_5| = d_2$ とおく．$(\chi_1, \chi_2) = 0$ より $1 - d_1 + a_{25}d_2 = 0.$ これと $|a_{25}| = 1, d_1, d_2 \in \mathbb{N}$ より $a_{25} = \pm 1.$ もし $a_{25} = -1$ なら $d_1 + d_2 = 1$ となって不適．よって $a_{25} = 1, d_2 = d_1 - 1.$ χ_2 は 1 次表現ゆえ $\overline{\chi_2}, \chi_2^2$ も G の 1 次表現だから，それを χ_3, χ_4 とする．$d = d_1, a = a_{51}$ とおく．指標の第 2 直交関係から $a_{52} = a_{53} = a_{54} = 0, a_{55} = -4/a$ である．また $\mathbb{N} \ni \frac{|G|}{|C_5|} = 4 + \frac{4}{d-1}$ より d は $2, 3, 5$ のいずれかであるが，$|G|$ を 2 通りに数えると $4d = 4 + a^2$ となるから $d = 3$ は不適．$y \in C_5$ を取り，$H = \langle x \rangle, K = \langle y \rangle$ とおく．G は x, y で生成される．$d = 2$ なら $|G| = 8$ より $[G : H] = 2$ だから $G \rhd H.$ よって $y^{-1}xy \in C_2 \cap H = \{x\}$ なので G は Abel 群となるが，指標表のサイズは $5 < |G|$ なので矛盾．従って $d = 5$ なので $a = 4.$ 以上から G の指標表は以下となる．ただし C_i の下の数字は $|C_i|$ を表す．

	C_1	C_2	C_3	C_4	C_5
	1	5	5	5	4
χ_1	1	1	1	1	1
χ_2	1	i	-1	$-i$	1
χ_3	1	$-i$	-1	i	1
χ_4	1	-1	1	-1	1
χ_5	4	0	0	0	-1

x, y の関係式を求める．y^2 の位数は 5 だが，C_2, C_3, C_4 の元の位数はそれぞれ $4, 2, 4$ なので $y^2 \in C_5.$ また $G = HK$ だから $x^{-j}yx^j = y^2$ となる j が存在する．$j = 0$ は明らかに不適．$j = 1$ なら $x^{-1}yx = y^2.$ $j = 3$ なら x^{-1} を改めて x とおけば $j = 1$ の場合に帰着される．$j = 2$ なら $x^2yx^2 = y^2$ である．ここで G の Sylow 5-部分群の個数を n とすると，Sylow の定理より $n \equiv 1 \bmod 5, n \mid 20$ だから $n = 1.$ よって $G \rhd K$ なので $\sigma : H \to \mathrm{Aut}(K)$ が存在して $G = K \rtimes_\sigma H$ となる．$\sigma : x \mapsto (y \mapsto y^m)$ とすると $x^2yx^2 = y^{m^2}x^4 = y^{m^2}$ となるから $m^2 \equiv 2 \bmod 5.$ これは矛盾．以上から

$$G = \langle x, y \,|\, x^4 = y^5 = 1, x^{-1}yx = y^2 \rangle.$$

□

(補足) $G \cong \mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ は Frobenius 群というものらしい．
`https://people.maths.bris.ac.uk/~matyd/GroupNames/1/F5.html`

1976 年度 (昭和 51 年度)

問 101

共役類の個数が 3 であるような有限群を全て求めよ.

解答. 実施年度不明 2 問 2 と同じ記号を用いると

$$\frac{1}{n_1}+\frac{1}{n_2}+\frac{1}{N}=1$$

である. $n_1 \leq n_2 < N$ より $1 \leq \frac{1}{n_1}+\frac{1}{n_1}+\frac{1}{n_1}=\frac{3}{n_1}$ なので $n_1 = 2, 3$.

- $n_1 = 3$ の時 : $\frac{2}{3}=\frac{1}{n_2}+\frac{1}{N} \leq \frac{1}{3}+\frac{1}{3}=\frac{2}{3}$ だから $n_2 = N = 3$. よって $G \cong \mathbb{Z}/3\mathbb{Z}$.
- $n_1 = 2$ の時 : $\frac{1}{n_2}+\frac{1}{N}=\frac{1}{2}$ より $(n_2-2)(N-2)=4$ なので $(n_2, N) = (3,6), (4,4)$. 後者は G が Abel 群なので, 共役類は 4 個となって不適. 前者の時, 同様に G は非可換群なので $G \cong S_3$.

以上から $\mathbb{Z}/3\mathbb{Z}, S_3$ の 2 個. □

問 102

m を平方因子を含まない負の整数とし，$K=\mathbb{Q}(\sqrt{m}), R=\mathbb{Z}[\sqrt{m}]$ とする．
(i) $K\otimes_{\mathbb{Q}} K$ において，単位元を 2 個の冪等元 $(\neq 0)$ の和として表わせ．
(ii) 環 $R\otimes_{\mathbb{Z}} R$ の可逆元のつくる乗法群を求めよ．

解答．(i) $\otimes_{\mathbb{Q}}$ を $\otimes$ と書く．$x=1\otimes 1, y=\sqrt{m}\otimes\sqrt{m}$ とおく．$ax+by\in K\otimes K$ が零でない冪等元とすると，

$$ax+by=(ax+by)^2=(a^2+b^2m^2)x+2aby$$

より $a^2+b^2m^2=a, 2ab=b$ なので $(a,b)=(0,0),(1,0),(\frac{1}{2},\pm\frac{1}{2m})$. よって

$$u=\frac{1}{2}x+\frac{1}{2m}y,\quad v=\frac{1}{2}x-\frac{1}{2m}y$$

とおけば，これらは零でない冪等元であり，$u+v=1\otimes 1$ である．

(ii) $\otimes_{\mathbb{Z}}$ を $\otimes$ と書く．$x\otimes y\in R^\times$ の逆元が $z\otimes w$ であるとすると $1\otimes 1=(x\otimes y)(z\otimes w)=xz\otimes yw$ だから $(xz,yw)=\pm(1,1)$. よって $x,y\in R^\times$ が必要．逆にこの時 $x\otimes y\in(R\otimes R)^\times$ である．従って $(R\otimes R)^\times=R^\times\otimes R^\times$ であるから，$R^\times$ を求める．$K/\mathbb{Q}$ のノルム $N(a+b\sqrt{m})$ は $N(a+b\sqrt{m})=a^2-b^2m$ である．$a+b\sqrt{m}\in R^\times$ の逆元を $c+d\sqrt{m}$ とすると

$$\begin{aligned}1&=N(1)=N((a+b\sqrt{m})(c+d\sqrt{m}))\\&=N(a+b\sqrt{m})N(c+d\sqrt{m})=(a^2-b^2m)(c^2-d^2m)\end{aligned}$$

だから，$m<0$ とから $a^2-b^2m=1$ が必要．

- $m<-1$ の時：$(a,b)=(\pm1,0)$ であり，実際 $\pm1\in R^\times$ である．よって

$$(R\otimes R)^\times=\{(\pm1)\otimes(\pm1)\}=\{\pm1\otimes 1\}\cong\mathbb{Z}/2\mathbb{Z}.$$

- $m=-1$ の時：$(a,b)=(\pm1,0),(0,\pm1)$ であり，実際 $\pm1,\pm\sqrt{-1}\in R^\times$ である．よって

$$(R\otimes R)^\times=\{\pm1\otimes 1,\pm1\otimes\sqrt{-1},\pm\sqrt{-1}\otimes 1,\pm\sqrt{-1}\otimes\sqrt{-1}\}.$$

ここで $a=1\otimes\sqrt{-1}, b=\sqrt{-1}\otimes\sqrt{-1}$ とおけば $a^4=b^2=1\otimes 1$ であり，

$$\begin{aligned}&a^2=-1\otimes 1,\quad a^3=-1\otimes\sqrt{-1},\\&ab=-\sqrt{-1}\otimes 1,\quad a^2b=-\sqrt{-1}\otimes\sqrt{-1},\quad a^3b=\sqrt{-1}\otimes 1\end{aligned}$$

だから

$$\begin{aligned}(R\otimes R)^\times&=\{1\otimes 1,a^2,a,a^3,a^3b,ab,b,a^2b\}\\&\cong\langle a,b|a^4=b^2=1,ab=ba\rangle\cong\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}.\end{aligned}$$

□

問 104

p を素数，$\mathbb{Z}_p$ を p 進整数環とする．写像 $f : \mathbb{Z}_p \to \mathbb{Z}_p$ を

$$f(x) = x^p + p\sum_{n=0}^{\infty} a_n x^n$$

によって定義する．ただし，$\{a_n\}_{n=0}^{\infty}$ は $\mathbb{Z}_p$ における数列で $\lim_{n\to\infty} a_n = 0$ とする．このとき各 $b \in \mathbb{Z}_p$ に対して

$$\begin{cases} x \equiv b \pmod{p} \\ f(x) = x \end{cases}$$

を満たす $x \in \mathbb{Z}_p$ がただ一つ存在することを示せ．

解答. $b \in \{0, 1, \ldots, p-1\}$ として良い．$B = \{x \in \mathbb{Z}_p \,;\, |x-b|_p \le p^{-1}\}$ とおく．f は B から B への写像である．実際，任意の $x \in B$ を $x = b + pu\,(u \in \mathbb{Z}_p^{\times})$ と書くと $x^p - b = (b + p^p u^p) - b = p^p u^p$ だから

$$|f(x) - b|_p = \left| p^p u^p + p\sum_{n\ge 0} a_n x^n \right|_p \le \max\left\{ p^{-p}|u^p|_p, \max_{n\ge 0} p^{-1}|a_n|_p |x^n|_p \right\} \le p^{-1}$$

である．$\mathbb{Z}_p$ は $|\cdot|_p$ について完備だから，$f|_B : B \to B$ が縮小写像であることが示せれば，縮小写像の原理により f は B において不動点を一意に持つ．これを示そう．任意に $x, y \in \mathbb{Z}_p$ を取る．$x \equiv y \bmod p^k$ ならば，$x^n \equiv y^n \bmod p^k$ だから $|x^n - y^n|_p \le |x-y|_p$ である．特に $n = p, x \not\equiv y \bmod p^{k+1}$ の時は $x - y = p^k u\,(u \in \mathbb{Z}_p^{\times})$ とおくと

$$x^p = (y + p^k u)^p = y^p + \sum_{j=1}^{p} \binom{p}{j} y^{p-j} (p^k u)^j \equiv y^p \bmod p^{k+1}$$

だから $|x^p - y^p|_p \le p^{-(k+1)} = p^{-1}|x-y|_p$ である．これらより任意の $x, y \in B$ に対し

$$\begin{aligned} |f(x) - f(y)|_p &= \left| (x^p - y^p) + p\sum_{n\ge 0} a_n (x^n - y^n) \right|_p \\ &\le \max\left\{ |x^p - y^p|_p, \max_{n\ge 0} p^{-1}|a_n|_p |x^n - y^n|_p \right\} \\ &\le \max\left\{ p^{-1}|x-y|_p, \max_{n\ge 0} p^{-1}|a_n|_p |x-y|_p \right\} \\ &= p^{-1}|x-y|_p \end{aligned}$$

なので示された． □