中間試験 (代数学)

作成者：石川雅雄

平成 28 年 6 月 4 日

裏面に問題 5 があります.

問題 1. 整域 $R=\mathbb{Z}\left[\sqrt{-5}\right]$ が単項イデアル整域でないことを次の手順によって示す. 各問いに答えよ.

(1) 一般の整域 D において, $x\in D$ が素元であることの定義を述べよ. また, $x\in D$ が既約元であることの定義も述べよ.

(2) D が単項イデアル整域ならば, 既約元 $x\in D$ は素元であることを示せ.

(3) $x=a+b\sqrt{-5}\in R=\mathbb{Z}\left[\sqrt{-5}\right]$ $(a,b\in\mathbb{Z})$ に対して $\overline{x}=a-b\sqrt{-5}$ と定義する. このとき, $x,y\in R$ に対して, $\overline{xy}=\overline{x}\cdot\overline{y}$ となることを示せ. また, $N(x)=x\overline{x}=a^2+5b^2\in\mathbb{Z}$ と定義すると $N(xy)=N(x)N(y)$ を示せ. さらに R で $x|y$ ならば, $\mathbb{Z}$ で $N(x)|N(y)$ であることを示せ.

(4) $1+\sqrt{-5}$ も $1-\sqrt{-5}$ も R において 2 の倍元でないことを示せ.

(5) 2 は R の既約元であることを示せ.

(6) $2|\left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right)$ であることを利用して, 2 は既約元であるが素元ではない理由を書け. また, このことから, R が単項イデアル整域でないといえる理由を書け.

(7) $\left(2,1+\sqrt{-5}\right)$ は R の単項イデアルでないことを示せ.

問題 2. $R=\mathbb{Z}[i]$ が単項イデアル整域であることを, 次の手順で示せ. ただし, $i=\sqrt{-1}$ とする.

(1) ユークリッド整域の定義を述べよ.

(2) ユークリッド整域は, 単項イデアル整域であることを示せ.

(3) $x=a+bi\in R$ に対して $\overline{x}=a-bi$ をその共役複素数とする. $N(x)=x\overline{x}=a^2+b^2$ とおく. $x,y\in R$, $x\neq 0$ ならば $q,r\in R$ が存在して $y=xq+r$ かつ $N(r)\leq\frac{1}{2}N(x)$ とできることを示せ.

(4) $R=\mathbb{Z}[i]$ はユークリッド整域であることを示せ.

(5) $\mathbb{Z}[i]/(2+i)$ は体であることを示せ.

問題 3. $F=\mathbb{Q}$, $E=\mathbb{Q}\left(\sqrt{1+i}\right)$ とする. ただし, $i=\sqrt{-1}$ とする. 次の問いに答えよ.

(1) $\alpha=\sqrt{1+i}$ の $\mathbb{Q}$ 上の最小多項式 $f(X)$ を求めよ. また, $f(X)$ の既約性を示せ.

(2) $(1,\alpha,i,i\alpha)$ が E の $\mathbb{Q}$ 上のベクトル空間としての基底であることを示せ.

(3) (2) の基底の間の乗法の演算表を作れ.

(4) (1) で求めた $f(X)$ を $\mathbb{Q}(\alpha)$ 上で可能な限り因数分解せよ.

(5) $f(X)$ を $\mathbb{Q}\left(\alpha,\sqrt{N}\right)$ で因数分解するとき, 1 次式の積に分解するような最小の自然数 N を求めよ. また, そのときの因数分解を書け.

問題 4. 有限体 $\mathbb{F}_2$ 上の多項式 $f(X)=X^3+X+1\in\mathbb{F}_2[X]$ の根の 1 つを α とし, $E=\mathbb{Q}(\alpha)$ とする. 次の問いに答えよ.

(1) $f(X)$ は $\mathbb{F}_2$ 上既約多項式であることを示せ.

(2) $1,\alpha,\alpha^2$ は E の $\mathbb{F}_2$ 上の基底である理由を述べ, $[E:\mathbb{Q}]=3$ であることを示せ.

(3) E の元の数は $2^3=8$ である理由を述べ, これらの 8 個の元の間の乗算表を作れ.

(4) $f(X)$ は E 上で

$$f(X)=(X-\alpha)(X-\alpha^2)(X-\alpha^{2^2})$$

と因数分解することを示せ.

(5) E の自己同型写像全体の群 $\mathrm{Aut}_{\mathbb{Q}}(E)$ の位数を求めよ.

問題 5. 次の (i) か (ii) のどちらかを解け.

(i) $F = \mathbb{F}_2$ とし, $f(X) = X^2 + X + 1 \in F[X]$ の根の 1 つを α として $E = F(\alpha)$ とする. E 上の 2 次の特殊線型群 $G = \mathrm{SL}(2, E)$ は E の元を成分とする 2 次正方行列 A で $\det A = 1$ となるもの全体がなす群である. このとき, 次の問いに答えよ.

(1) $V = E^2$ を E を成分とする 2 次のベクトル全体のなすベクトル空間として, G の V への自然な作用を考える. すなわち, $A \in G$, $\boldsymbol{v} \in V$ に対して $A\boldsymbol{v} \in V$ は行列を掛ける作用である. このとき, $\boldsymbol{v}_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ の G による軌道 (orbit) は

$$V_0 = \{\boldsymbol{v} \in V \mid \boldsymbol{v} \neq 0\}$$

であることを示せ. よって, $|V_0| = 15$ となる理由を言え.

(2) G の (1) の作用による $\boldsymbol{v}_0$ の不変部分群 H を求めよ. これによって, $|H| = 4$ であることを示せ.

(3) H は クラインの四元群 $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$ と同型なことを示せ.

(4) E 上の 2 次の特殊線型群 G の位数は $|G| = 60$ となる理由を言え.

(5) $A \in G$ に対して, その固有多項式を $\gamma_A(X)$ と書くとき, 次の 4 つの場合しか起こらないことを示せ.

a) $\gamma_A(X) = X^2 + 1$

b) $\gamma_A(X) = X^2 + X + 1$

c) $\gamma_A(X) = X^2 + \alpha X + 1$

d) $\gamma_A(X) = X^2 + \alpha^2 X + 1$

(6) 上の a) の場合には, A は単位行列であるか, または A の位数は 2 であることを示せ.

(7) 上の b) の場合には, A の位数は 3 であることを示せ.

(8) 上の c) の場合に, $\gamma_A(X) = X^2 + \alpha X + 1$ の根の 1 つを β とおくと, $L = E(\beta) = \mathbb{F}_2(\alpha, \beta)$ において d) の固有多項式 $X^2 + \alpha^2 X + 1$ も一次式の積に分解することを示せ. また, このとき A の位数が 5 であることを示せ. d) の場合も同様に A の位数が 5 であることを示せ.

(ii) ζ を 1 の原始 7 乗根 $e^{\frac{2\pi i}{7}}$ とし,

$$A = \left\{a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4\zeta^4 + a_5\zeta^5 + a_6\zeta^6 \mid a_1, a_2, a_3, a_4, a_5, a_6 \in \{0, 1\}\right\}$$

を考える. このとき, $\mathbb{Q}(\alpha) = \mathbb{Q}(\zeta)$ となる $\alpha \in A$ の個数を求めよ. (平成 26 年度 京都大学大学院入試問題)