代数数理工学 基本演習 略解

問題 1. (1) 明らかに, $(x \wedge y) \preceq x$, $(x \wedge z) \preceq x$ が成立. 一方, $(x \wedge y) \preceq y \preceq (y \vee z)$, $(x \wedge z) \preceq z \preceq (y \vee z)$ も成立. したがって, $(x \wedge y) \vee (x \wedge z) \preceq x \wedge (y \vee z)$ を得る.

(2) 明らかに, $(x \vee y) \succeq x$, $(x \vee z) \succeq x$ が成立. 一方, $(x \vee y) \succeq y \succeq (y \wedge z)$, $(x \vee z) \succeq z \succeq (y \wedge z)$ も成立. したがって, $(x \vee y) \wedge (x \vee z) \succeq x \vee (y \wedge z)$ を得る.

(3) 定義から, $x \preceq (x \vee y)$, $(y \wedge z) \preceq z$ は明らか. また, $(y \wedge z) \preceq y \preceq (x \vee y)$ も成立. したがって, $x \preceq z$ ならば, $x \vee (y \wedge z) \preceq (x \vee y) \wedge z$ を得る.

問題 2. 「$x \preceq z \Rightarrow x \vee (y \wedge z) = (x \vee y) \wedge z$」を示せばよい. 分配律より, $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$. ここで, $x \preceq z$ ならば, 右辺に $x \vee z = z$ を適用して, $x \vee (y \wedge z) = (x \vee y) \wedge z$ を得る.

問題 3. (1) 24.

(2) 置換 $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$ が生成する巡回群.

(3) 置換 $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ と $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ が生成する 2 面体群.

(4) 回転運動によって, 立方体の対角線 4 本が置換される. 逆に対角線の置換を定めると, 立方体の回転の仕方が定まる.

問題 4. (1) $\frac{1}{24}(k^8 + 17k^4 + 6k^2)$ 通り.

(2) $\frac{1}{24}(k^6 + 3k^4 + 12k^3 + 8k^2)$ 通り.

(3) $\frac{1}{24}(k^{12} + 6k^7 + 3k^6 + 8k^4 + 6k^3)$ 通り.

問題 5. 有限整域 K の 0 でない任意の元 a に対して, $\sigma(x) = ax$ とすると, σ は $K \backslash \{0\}$ 上の置換となる. したがって, $ab = 1$ となる $b \in K \backslash \{0\}$, すなわち a の乗法逆元が存在する.

問題 6. 任意の元 $a + b\sqrt{-1} \in \mathbf{Z}[\sqrt{-1}]$ に対して, $\varphi(a + b\sqrt{-1}) = a^2 + b^2$ とする.

問題 7. イデアル I に関して, $\varphi(a)$ が最小となる $a \in I \backslash \{0\}$ を考える. 任意の $b \in I$ に対して, $a|b$ でないなら, $b = qa + r$, $\varphi(r) < \varphi(a)$ を満たす $q, r \in R$ が存在する. このとき, $r \in I$ となり, a の選び方に矛盾する.

問題 8. イデアル $J = \{g(x, y) \mid g(0, 0) = 0\}$ は, 単項イデアルでない.

問題 9. (1) 素元 $r \in R$ に対して, $r = st$ ならば, $r|s$ または $r|t$. 仮に, $r|s$ とすると, $s = qr$ となる $q \in R$ が存在する. その結果, $r = qrt$ が成立し, $r(qt - 1) = 0$ を得る. さらに, R が整域であることから, $qt = 1$ となり, t は可逆元. 同様に, $r|t$ とすると, s が可逆元. したがって, r は既約元.

(2) $(a+b\sqrt{-5})(c+d\sqrt{-5}) = 2$ とならば, $(a^2+5b^2)(c^2+5d^2) = 4$ が成立し, $b = d = 0$ を得る. さらに, $a = \pm 1$ または $c = \pm 1$ となることから, 2 は既約元. しかし, $(1+\sqrt{-5})(1-\sqrt{-5}) = 6$ に対して $2|6$ となることから, 2 は素元でない.

問題 10. 整数行列 A, B, C の単因子標準形は以下の通り.

$$A \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}, \qquad B \sim \begin{pmatrix} 2 & 0 & 0 \\ 0 & 12 & 0 \end{pmatrix}, \qquad C \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 6 \end{pmatrix}.$$

問題 11. $x^4 - 10x^2 + 1$.

問題 12. (1) 準同型であることは, 簡単に確かめられる. 任意の $a+b\sqrt{2}$ に対して, $f(x) = a+bx$ とすると, $\varphi(f(X)) = a+b\sqrt{2}$ が成立. したがって, φ は全射準同型.

(2) $\operatorname{Ker}\varphi = \{f(X) \mid f(\sqrt{2}) = 0\}$.

(3) 任意の $f(X), g(X) \in \operatorname{Ker}\varphi$ に対し, $f(\sqrt{2}) = g(\sqrt{2}) = 0$ より, $f(\sqrt{2})+g(\sqrt{2}) = 0$ となり, $f(X)+g(X) \in \operatorname{Ker}\varphi$. また, 任意の $f(X) \in \operatorname{Ker}\varphi$ と $g(X) \in \mathbf{Q}[X]$ に対し, $g(\sqrt{2})f(\sqrt{2}) = 0$ となるため, $g(X)f(X) \in \operatorname{Ker}\varphi$. ゆえに, $\operatorname{Ker}\varphi$ はイデアル.

(4) 素イデアルであることを示す. 実際, $f(X)g(X) \in \operatorname{Ker}\varphi$ は $f(\sqrt{2})g(\sqrt{2}) = 0$ を意味する. 以下の問題 13 (1) の解答と同様にして, $f(\sqrt{2}) = 0$ または $g(\sqrt{2}) = 0$ を得る. すなわち, $f(X) \in \operatorname{Ker}\varphi$ または $g(X) \in \operatorname{Ker}\varphi$ となる. したがって, $\operatorname{Ker}\varphi$ は素イデアル.

(5) 多項式環 $\mathbf{Q}[X]$ は単項イデアル整域であり, 任意の素イデアルが極大イデアル. したがって, $\operatorname{Ker}\varphi$ は極大イデアル.

(6) $\mathbf{Q}[X]$ における同値関係 $\sim$ は, $f(X)-g(X) \in \operatorname{Ker}\varphi$ のときに $f(X) \sim g(X)$ とすることで定められる. $f(X)$ の同値類 $[f(X)]$ に対して, $\bar{\varphi}([f(X)]) = f(\sqrt{2})$ とすることで, $\bar{\varphi}$ を定める. このとき, $f(X) \sim g(X)$ ならば, $f(\sqrt{2}) = g(\sqrt{2})$ が成立するので, $\bar{\varphi}$ は代表元の取り方によらず, 値が定まる写像となる (well-defined). さらに, $\bar{\varphi}$ が準同型であることは, 簡単に確かめられる.

(7) $f(\sqrt{2}) = g(\sqrt{2})$ のときに, $h(X) = f(X) - g(X)$ とすれば, $h(\sqrt{2}) = 0$, すなわち $h(X) \in \operatorname{Ker}\varphi$ であり, $f(X) \sim g(X)$ を得る. したがって, $\bar{\varphi}$ は単射. 一方で φ が全射であることから, $\bar{\varphi}$ が全射であることも明らか. ゆえに $\bar{\varphi}$ は同型写像である.

(8) $\operatorname{Ker}\varphi$ が極大イデアルであることから, $\mathbf{Q}[\sqrt{2}] \simeq \mathbf{Q}[X]/\operatorname{Ker}\varphi$ が体であることが導かれる. あるいは, $\mathbf{Q}[\sqrt{2}]\backslash\{0\}$ の任意の元 $a+b\sqrt{2}$ に対して, $\dfrac{a}{a^2-2b^2} - \dfrac{b}{a^2-2b^2}\sqrt{2}$ が乗法逆元となることからも $\mathbf{Q}[\sqrt{2}]$ が体であることが示される.

問題 13. (1) $(a+b\sqrt{2})(c+d\sqrt{2}) = 0$ とすると, $ac+2bd = 0$ と $ad+bc = 0$ が成立し, $d(a^2-2b^2) = 0$ となる. すなわち, $d = 0$ または $a^2 = 2b^2$ を得る. ここで,

$d = 0$ の場合, $ac = 0$ と $bc = 0$ が成立するので, $c = 0$ または $a = b = 0$ となる. 一方, $a^2 = 2b^2$ の場合, $a = b = 0$ となる. 以上より, いずれの場合にも $a = b = 0$ または $c = d = 0$ であり, 零因子は存在しない.

(2) $(\sqrt{2}-1)(1+\sqrt{2}) = 1$ より, $1+\sqrt{2}$ は可逆元.

(3) 任意の自然数 k に対して, $(1+\sqrt{2})^k$ は可逆元. したがって, 可逆元が無限にある.

(4) $\mathbf{Q}[\sqrt{2}]$.

問題 14. 自然数 n を m で割った商を q, 剰余を r とする. このとき,

$$\begin{aligned} x^n - 1 &= x^{mq}x^r - 1 \\ &= \{(x^m-1)(1+x^m+\cdots+x^{(q-1)m})+1\}x^r - 1 \\ &= (x^m-1)(1+x^m+\cdots+x^{(q-1)m})+x^r-1 \end{aligned}$$

すなわち, $x^n - 1$ を $x^m - 1$ で割った剰余が $x^r - 1$ となる. ここで, $r = 0$ のとき, かつそのときに限り, $x^r - 1 = 0$ となることに注意する.

問題 15. 多項式 $f(x+1) = \dfrac{(x+1)^p - 1}{x} = \displaystyle\sum_{k=1}^{p} \binom{p}{k} x^{k-1}$ に Eisenstein の既約判定法を適用する. まず, $k = 1, \ldots, p-1$ に対しては, $\binom{p}{k}$ が p の倍数. また, $k = p$ に対して, $\binom{p}{k} = 1$ は p の倍数でない. さらに, $k = 1$ に対して, $\binom{p}{k} = p$ は, p^2 の倍数でない. したがって, $f(x+1)$ は $\mathbf{Q}$ 上の既約多項式であり, $f(x)$ も $\mathbf{Q}[x]$ で既約.

問題 16. 不定方程式 $31x + 23y = 1$ を Euclid の互除法を用いて解くと, $x = 3$, $y = -4$ を得る. 有限体 GF(31) においては, $-4 = 27$. したがって, 23 の乗法逆元は 27.