

代数学 I 演習問題 (7)

環と言ったら必ず乗法単位元を持つ環を意味するとする. また環とその部分環の乗法単位元は一致するものとし, 準同型写像は乗法単位元を乗法単位元に写すもののみを考える.

1. $F(X), G(X) \in \mathbb{Z}[X]$ で, $G(X)$ の最高次の係数が 1 であるものとする. $F(X) = G(X)H(X)$ となる $H(X) \in \mathbb{Q}[X]$ が存在すれば, $H(X) \in \mathbb{Z}[X]$ であることを証明せよ.
2. $\mathbb{Z}[X] \cap (X^2 + 1)\mathbb{Q}[X] = (X^2 + 1)\mathbb{Z}[X]$ が成り立つことを証明せよ.
3. (a) $x \in \mathbb{Z}[i]$ に対し, 「 $x \in \mathbb{Z}[i]^\times \iff |x| = 1$ 」であることを証明せよ.
(b) $x \in \mathbb{Z}[i]$ に対し, $|x|^2$ が素数ならば x は $\mathbb{Z}[i]$ の既約元であることを証明せよ.
(c) 3 は $\mathbb{Z}[i]$ の既約元であることを証明せよ.
(d) 5 は $\mathbb{Z}[i]$ の既約元でないことを証明せよ.
(e) $\mathbb{Z}[i]/(3)$ の掛け算の表を作れ. (余裕があれば $\mathbb{Z}[i]/(5)$ の掛け算の表も.)
注意. $\mathbb{Z}[i]$ が P.I.D. であることを証明できる. よって (c) より (3) は $\mathbb{Z}[i]$ の極大イデアルなので, $\mathbb{Z}[i]/(3)$ は体である. (e) の表を見てそのことを実感せよ.
4. (a) ユークリッドの互除法を用いて $(37, 59) = 1$ を証明せよ.
(b) $37x + 59y = 1$ なる $x, y \in \mathbb{Z}$ を一組求めよ.
(c) 体 $\mathbb{Z}/59\mathbb{Z}$ における $37 + 59\mathbb{Z}$ の乗法逆元を求めよ. (注意: 59 は素数である.)
5. $\mathbb{Q}(\sqrt[3]{2}) := \{a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 \mid a, b, c \in \mathbb{Q}\}$ とおく.
(a) $\mathbb{Q}(\sqrt[3]{2})$ は $\mathbb{R}$ の部分環であることを証明せよ.
(b) $f: \mathbb{Q}[X] \rightarrow \mathbb{Q}(\sqrt[3]{2})$ を $f(F(X)) = F(\sqrt[3]{2})$ ($F(X) \in \mathbb{Q}[X]$) で定義する. f が全射であること, $(X^3 - 2) \subset \text{Ker}(f) \subsetneq \mathbb{Q}[X]$ であることを証明せよ. (f が準同型写像であることは認めてよい.)
(c) $X^3 - 2$ は $\mathbb{Q}$ 上既約であることを証明せよ.
(d) $\text{Ker}(f) = (X^3 - 2)$ を証明せよ.
(e) $\mathbb{Q}[X]/(X^3 - 2) \cong \mathbb{Q}(\sqrt[3]{2})$ を証明せよ.
(f) (c), (e) より $\mathbb{Q}(\sqrt[3]{2})$ は体であることがわかるので, $1/(1 + \sqrt[3]{2}) \in \mathbb{Q}(\sqrt[3]{2})$ が成立する. よって $1/(1 + \sqrt[3]{2}) = a + b\sqrt[3]{2} + c\sqrt[3]{2}^2$ となる $a, b, c \in \mathbb{Q}$ が存在する. このような $a, b, c \in \mathbb{Q}$ を求めよ.
6. (a) $a, b, c \in \mathbb{Q}$ に対し, 「 $a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 = 0 \implies a = b = c = 0$ 」が成り立つことを証明せよ.
ヒント: $a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 = 0 \implies a + bX + cX^2 \in \text{Ker}(f)$, f は…

- (b) $\{a + b\sqrt[3]{2} \mid a, b \in \mathbb{Q}\}$ は実数の加法, 乗法に関し環でないことを証明せよ.
7. $F(X) := X^3 + X^2 - 2X - 1 \in \mathbb{Z}[X]$ が $\mathbb{Q}$ 上既約であることを,
- (a) $F(X)$ が $\mathbb{Q}$ に根を持たないことを示すことにより証明せよ ;
- (b) アイゼンシュタインの定理を用いることにより証明せよ.
8. k を自然数とする. $X^4 - kX^2 + 1 \in \mathbb{Z}[X]$ が $\mathbb{Q}$ 上既約であるための k に関する必要十分条件を求めよ.
9. K を体とする. $F(X) \in K[X]$ に対し, 「 $F(X)$ が K に根を持つ $\iff \exists G(X) \in K[X]$ s.t. $\deg(G(X)) = 1, G(X) \mid F(X)$ 」を証明せよ.
10. (a) $F(X) \in \mathbb{C}[X]$ に対し, 「 $F(X)$ が $\mathbb{C}$ 上既約 $\iff \deg(F(X)) = 1$ 」が成り立つことを証明せよ. (ヒント. $\mathbb{C}$ の基本定理を使う.)
- (b) $F(X) \in \mathbb{R}[X]$ に対し, 「 $\deg(F(X)) \geq 3$ ならば $F(X)$ は $\mathbb{R}$ 上可約」を証明せよ. (ヒント. $F(X)$ が虚数根を持てば, その共役も…)
11. p を素数とする. $a, b \in \mathbb{Z}$ に対し, $(a + b)^p \equiv a^p + b^p \pmod{p}$ が成り立つことを証明せよ.
12. p を素数とし, $K := \mathbb{Z}/p\mathbb{Z}$ とおく. (K は体であった.) $f(a) = a^p$ ($a \in K$) で定義される写像 $f: K \rightarrow K$ は同型写像であることを証明せよ.
13. $z \in \mathbb{C}$ とする. z を根とする $F(X) \in \mathbb{Q}[X] - \{0\}$ で, $\deg(F(X)) \geq 2$ かつ $F(X)$ が $\mathbb{Q}$ 上既約であるようなものが存在すれば, $z \notin \mathbb{Q}$ であることを証明せよ.
14. p を素数, n を 2 以上の自然数とする. この時 $\sqrt[n]{p} \notin \mathbb{Q}$ であることを証明せよ.
注意. この問題から $\sqrt{2} \notin \mathbb{Q}$ がわかる.
15. $2X + 2 \in \mathbb{Z}[X]$ は $\mathbb{Z}[X]$ の既約元でないことを証明せよ.
16. $(2 + 4\mathbb{Z})X + (1 + 4\mathbb{Z}) \in (\mathbb{Z}/4\mathbb{Z})[X]$ は $(\mathbb{Z}/4\mathbb{Z})[X]$ の既約元でないことを証明せよ.
17. G を有限群, a を G の元とする. $(\#G, n) = 1$ なる $n \in \mathbb{Z}$ に対し $a^n = e_G$ (e_G は G の単位元) が成り立っていれば, $a = e_G$ である. このことを証明せよ.
18. p を $p \equiv 2 \pmod{3}$ なる素数とする. $f(a) = a^3$ ($a \in (\mathbb{Z}/p\mathbb{Z})^\times$) で定義される写像 $f: (\mathbb{Z}/p\mathbb{Z})^\times \rightarrow (\mathbb{Z}/p\mathbb{Z})^\times$ は (群の) 同型写像であることを証明せよ.