$\boxed{\text{問題 2-4}}$ $\omega^3=1$ と仮定し，$\alpha=\omega\sqrt[3]{7}$ とおき，写像 $\varphi:\mathbb{Q}[x]\to\mathbb{Q}[\alpha]$ を

$$\varphi(f(x))=f(\alpha)\quad(f\in\mathbb{Q}[x])$$

（補足：$\omega\in\mathbb{C}$）

と定める．以下で $\mathbb{Q}[\alpha]=\{f(\alpha)\mid f\in\mathbb{Q}[x]\}$ をみとめて使ってよい．以下を示せ．

(1) φ は全射環準同型でかつ $a\in\mathbb{Q}$ に対して $\varphi(a)=a$．

(2) $f(x)=x^3-7$ は $\mathbb{Q}$ 上の既約多項式である

(3) $\mathrm{Ker}\,\varphi=(x^3-7)\mathbb{Q}[x]$．これを (x^3-7) と書く．

(4) 環として，$\mathbb{Q}[x]/(x^3-7)\cong\mathbb{Q}[\alpha]$．

(5) $\mathbb{Q}[\alpha]$ は体になる．

$\boxed{\text{解答例}}$ (1) φ の定義より，$\varphi(a)=a$ $(a\in\mathbb{Q})$ は自明である．

$\mathbb{Q}[\alpha]=\{f(\alpha)\mid f\in\mathbb{Q}[x]\}$ より，$\varphi:\mathbb{Q}[x]\to\mathbb{Q}[\alpha]$ が全射であることがわかる．

φ が環の準同型であること，すなわち，φ が加法と乗法の単位元と乗法を保つことを示そう．

$f, g \in \mathbb{Q}[x]$ を任意にとる．$f = \sum_i a_i x^i$，$g = \sum_i b_i x^i$，$a_i, b_i \in \mathbb{Q}$ と書け，

$$\varphi(f+g) = \varphi\left(\sum_i (a_i+b_i)x^i\right) = \sum_i (a_i+b_i)\alpha^i = \sum_i a_i\alpha^i + \sum_i b_i\alpha^i = \varphi(f)+\varphi(g),$$

$\varphi(1) = 1$ （自明）．

$$\varphi(fg) = \varphi\left(\sum_k \left(\sum_{i+j=k} a_i b_j\right) x^k\right) = \sum_k \left(\sum_{i+j=k} a_i b_j\right)\alpha^k$$

$$= \left(\sum_i a_i \alpha^i\right)\left(\sum_j b_j \alpha^j\right) = \varphi(f)\varphi(g).$$

これで，φ が環の準同型であることも示された．

(2) $f(x) = x^3 - 7$ が $\mathbb{Q}$ 上既約であることを示そう．

$7 \nmid 1$, $7 \mid 0$, $7 \mid 0$, $7 \mid -7$, $7^2 \nmid -7$ なので Eisenstein の判定法より，$f(x)$ は $\mathbb{Q}$ 上既約である．

$\boxed{練習}$ x^3-7 が有理数係数の1次以上の2つの多項式の積に表されないことを高校生にもわかる方法で証明せよ．

$\square$

(3) $\mathrm{Ker}\,\varphi = (x^3-7)\mathbb{Q}[x]\ (=(x^3-7))$ を示そう.

$\mathrm{Ker}\,\varphi \supset (x^3-7)\mathbb{Q}[x]$ を示そう. $g \in (x^3-7)\mathbb{Q}[x]$ を任意にとる. $g(x)=(x^3-7)h(x)$, $h(x)\in\mathbb{Q}[x]$ と書け,

$\varphi(g) = (\alpha^3-7)h(\alpha) = (7-7)h(\alpha) = 0$. ($\alpha = \omega\sqrt[3]{7}$, $\omega^3=1$ より $\alpha^3=7$ となることを使った.)

$g\in\mathrm{Ker}\,\varphi$ を示せた. ゆえに, $\mathrm{Ker}\,\varphi \supset (x^3-7)\mathbb{Q}[x]$ が示された.

$\mathrm{Ker}\,\varphi \subset (x^3-7)\mathbb{Q}[x]$ を示そう. $g\in\mathrm{Ker}\,\varphi$ を任意にとる. このとき, $g(\alpha)=0$.

$\mathrm{Ker}\,\varphi$ に含まれる 0 でない多項式で次数が最小でモニックなもの (最高次の係数が 1 のもの) が存在する. それの 1 つを $f_0(x)\in\mathrm{Ker}\,\varphi$ と書く.

$f(x)=x^3-7\in\mathrm{Ker}\,\varphi$ は $f(x)=f_0(x)q(x)+r(x)$, $q, r\in\mathbb{Q}[x]$, $\deg r < \deg f_0$

と書ける. このとき, $0 = f(\alpha) = \underbrace{f_0(\alpha)}_{=0}q(\alpha)+r(\alpha) = r(\alpha) = \varphi(r)$ より, $r\in\mathrm{Ker}\,\varphi$

となり, f_0 は $\mathrm{Ker}\,\varphi$ に含まれる 0 でない多項式の中で最低次のものなので,

$r(x)=0$ となり, $f(x)=f_0(x)q(x)$ となる. もしも $\deg f_0 < \deg f$ だとすると,

f が $\mathbb{Q}$ 上既約であることに反するので, $\deg f_0 = \deg f$ となり, $f_0 = f$ となる

ことがわかる (f_0 をモニックにとっていたことを使っている).

以上によって，$f(x)=x^3-7$ は Kerφ に含まれる多項式の中で最低次のものになっていることがわかった．

⇔ αを代入すると0になる

（注意 これは，$f(\alpha)=0$ と $f(x)$ が $\mathbb{Q}$ 上既約であることのみを使って示されているので，もっと一般の場合にも同様のことが言える．）

前ページの議論を任意にとってあった $g \in \mathrm{Ker}\,\varphi$ についてくりかえそう．

$g(x)=f(x)q(x)+r(x)$，$q, r \in \mathbb{Q}[x]$，$\deg r < \deg f$ と書ける．

このとき，$0=\varphi(g)=\underbrace{f(\alpha)}_{=0}q(\alpha)+r(\alpha)=r(\alpha)=\varphi(r)$ となり，$r \in \mathrm{Ker}\,\varphi$ となる．

f は Kerφ に含まれる0でない多項式の中で最低次のものなので，$r=0$．

したがって，$g(x)=f(x)q(x) \in f(x)\mathbb{Q}[x]=(x^3-7)\mathbb{Q}[x]$．

これで，$\mathrm{Ker}\,\varphi \subset (x^3-7)\mathbb{Q}[x]$ も示された．

以上によって，$\mathrm{Ker}\,\varphi=(x^3-7)\mathbb{Q}[x]$．

（注意 $g(\alpha)=0$ をみたす0でない $g \in \mathbb{Q}[x]$ の中で最低次（かつモニック）なものを α の最小多項式と呼ぶ．）

(4) 環として, $\mathbb{Q}[x]/(x^3-7) \cong \mathbb{Q}[\alpha]$ という同型が得られることを示そう.

$\varphi: \mathbb{Q}[x] \to \mathbb{Q}[\alpha],\ f \mapsto f(\alpha)$ に環の準同型定理を使うと, φ が全射で

$\mathrm{Ker}\,\varphi = (x^3-7)\ (= (x^3-7)\mathbb{Q}[x])$ であることより, 環の同型写像

$$\overline{\varphi}: \mathbb{Q}[x]/(x^3-7) \xrightarrow{\sim} \mathbb{Q}[\alpha],\quad \underbrace{f+(x^3-7)}_{} \mapsto f(\alpha)$$

が得られる

$f \bmod x^3-7$ と書くことも多い.

(5) $\mathbb{Q}[\alpha]$ は体になることを示そう.

(4) より, $\mathbb{Q}[x]/(x^3-7)$ が体になることを示せば十分である.

一般に PID の A と $0 \neq p \in A$ について,

p は A の既約元 $\Leftrightarrow$ $(p) = pA$ は A の極大イデアル $\Leftrightarrow$ $A/(p)$ は体.

そして, $f(x) = x^3-7$ は $\mathbb{Q}$ 上の既約多項式なので, $\mathbb{Q}[x]$ の既約元であり,

$\mathbb{Q}[x]/(x^3-7)$ は体になる

(注意 既約多項式は体を作るために使える!)

$\square$