資料 03-1

$\boxed{\text{問題2-2}}$ 以下の$\mathbb{Z}$係数多項式たちが$\mathbb{Q}$上の既約多項式になることを示せ.

(1) x^3+2x-2.

(2) $x^4+10x^3+15x^2+35x+55$.

(3) 正の整数 n に対する x^n-14.

(4) 素数 p に対する $x^{p-1}+x^{p-2}+\cdots+x+1$.

例: $x+1$, x^2+x+1, $x^4+x^3+x^2+x+1$, $x^6+x^5+\cdots+x+1$, ...

$\boxed{\text{記号}}$ $a|b \iff a$ で b は割り切れる $\iff a$ は b の約数 $\iff b$ は a の倍数

$a|b$ の否定を $a\nmid b$ と書く.

$\boxed{\text{例}}$ $2\nmid 1$, $2\nmid 3$, $2|0$, $2|2$, $2|4$, $2|6$, ...

$\boxed{\text{Eisensteinの判定法(}\mathbb{Z}\text{係数の多項式の場合)}}$

$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$, $a_i\in\mathbb{Z}$ のとき, 素数 p について,

$p\nmid a_n$, $p|a_{n-1}$, ..., $p|a_1$, $p|a_0$, $p^2\nmid a_0$ $\Rightarrow$ $f(x)$ は $\mathbb{Q}$ 上既約.

Gaussの補題を使う.

$\boxed{\text{解答例}}$ (1), (2), (3) では Eisenstein の判定法を直接使える.

(1) x^3+2x-2.　　2|0 の 0 は x^2 の係数

$2\nmid 1$, $2\mid 0$, $2\mid 2$, $2\mid -2$, $2^2\nmid -2$ と Eisenstein の判定法より, これは $\mathbb{Q}$ 上既約.

(2) $x^4+10x^3+15x^2+35x+55$.

$5\nmid 1$, $5\mid 10$, $5\mid 15$, $5\mid 35$, $5\mid 55$, $5^2\nmid 55$ と Eisenstein の判定法より, これは $\mathbb{Q}$ 上既約.

(3) 正の整数 n に対する x^n-14.　　p として, 2, 7 がとれる. どちらでもよい.

$7\nmid 1$, $7\mid 0$, …, $7\mid 0$, $7\mid -14$, $7^2\nmid -14$ と Eisenstein の判定法より, これは $\mathbb{Q}$ 上既約.

この次の(4)には直接に Eisenstein の判定法を使えない.

任意の $a\in\mathbb{Q}$ と $f(x)\in\mathbb{Q}[x]$ について,

$$f(x)\text{ は }\mathbb{Q}\text{ 上既約} \iff f(x+a)\text{ は }\mathbb{Q}\text{ 上既約}$$

を使う.

$$\left(\because\quad f(x)=g(x)h(x) \iff f(x+a)=g(x+a)h(x+a)\right)$$

(4) 素数 p に対する $x^{p-1}+x^{p-2}+\cdots+x+1$. これを $\varphi_p(x)$ と書く.

$\varphi_2(x)=x+1$ は1次なので $\mathbb{Q}$ 上既約.

$\varphi_3(x)=x^2+x+1=\dfrac{x^3-1}{x-1}$ より,

問題: $\varphi_5(x)$, $\varphi_7(x)$ について同様の計算をノートに書いてみよ.

$$\varphi_3(x+1)=\frac{(x+1)^3-1}{x}=\frac{x^3+3x^2+3x+1-1}{x}=x^2+3x+3.$$

$3\nmid 1$, $3\mid 3$, $3\mid 3$, $3^2\nmid 3$ と Eisenstein の判定法より, $\varphi_3(x+1)$ は $\mathbb{Q}$ 上既約で, $\varphi_3(x)$ も $\mathbb{Q}$ 上既約.

$\varphi_p(x)=\dfrac{x^p-1}{x-1}$ より,

$$\varphi_p(x+1)=\frac{(x+1)^p-1}{x}=\frac{\sum_{k=0}^{p}\binom{p}{k}x^k-1}{x}=\sum_{k=1}^{p}\binom{p}{k}x^{k-1}=\binom{p}{p}x^{p-1}+\binom{p}{p-1}x^{p-2}+\cdots+\binom{p}{2}x+\binom{p}{1}.$$

$$\binom{p}{p}=1,\ \underbrace{\binom{p}{p-1}=p,\ \ldots,\ \binom{p}{k}=\frac{p(p-1)\cdots(p-k+1)}{k!},\ \ldots,\ \binom{p}{2}=\frac{p(p-1)}{2},\ \binom{p}{1}=p}_{p\text{ で割り切れるが }p^2\text{ で割り切れない}}.$$

$\leftarrow$ $1\leqq k\leqq p-1$

ゆえに, Eisenstein の判定法より, $\varphi_p(x+1)$ は $\mathbb{Q}$ 上既約で, $\varphi_p(x)$ も $\mathbb{Q}$ 上既約である. □

$\boxed{\text{注意}}$ 素数 p について，$x^{p-1}+x^{p-2}+\cdots+x+1$ は $\mathbb{Q}$ 上既約になるが，

$m,n\in\mathbb{Z}$，$m,n\geqq 2$ のとき，$x^{mn-1}+x^{mn-2}+\cdots+x+1$ は $\mathbb{Q}$ 上既約でない．

なぜならば，

$(x^m)^n$

$$x^{mn-1}+x^{mn-2}+\cdots+x+1=\frac{x^{mn}-1}{x-1}=\frac{x^m-1}{x-1}\,\frac{x^{mn}-1}{x^m-1}$$

$$=(x^{m-1}+x^{m-2}+\cdots+x+1)(x^{m(n-1)}+x^{m(n-2)}+\cdots+x^m+1).$$

たとえば

$$x^3+x^2+x+1=\frac{x^4-1}{x-1}=\frac{x^2-1}{x-1}\,\frac{x^4-1}{x^2-1}=(x+1)(x^2+1)$$

$$x^5+x^4+x^3+x^2+x+1$$

$(x^2+1)^2-x^2=x^4+x^2+1$

$$=\frac{x^2-1}{x-1}\,\frac{x^6-1}{x^2-1}=(x+1)(x^4+x^2+1)=(x+1)(x^2+x+1)(x^2-x+1)$$

$$=\frac{x^3-1}{x-1}\,\frac{x^6-1}{x^3-1}=(x^2+x+1)(x^3+1)=(x^2+x+1)(x+1)(x^2-x+1)$$

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

$\square$

x^n-1 を割り切る $\mathbb{Q}$ 上既約な多項式を円分多項式と呼ぶ．

問題 2-3 R は可換環であるとし，$p\in R$ であるとする．

modulo p での reduction の話

"mod p"

$a\in R$ の R/pR での像を $\bar{a}$ と書き，写像 $\varphi: R[x]\to (R/pR)[x]$ を

$$\varphi\left(\sum_i a_i x^i\right) = \sum_i \bar{a}_i x^i \quad (a_i\in R)$$

と定める．以下を示せ．

pR を任意のイデアル I に一般化できる．

(1) φ は環の準同型写像である．

(2) φ は全射である．

(3) $\operatorname{Ker}\varphi = pR[x]$ ← p で生成される $R[x]$ のイデアル ← $IR[x] =$ (I で生成される $R[x]$ のイデアル) に一般化可能

(4) 環の同型写像 $\bar{\varphi}: R[x]/pR[x] \xrightarrow{\sim} (R/pR)[x],\ (f \bmod p)\mapsto \varphi(f)$ が得られる．

注意 $pR[x]$ も pR も (p) と書かれることがある．分脈によって区別せよ：

$$R[x]/(p) \xrightarrow{\sim} (R/(p))[x],\ (f \bmod p)\mapsto \varphi(f).$$

互いに異なることに注意

□

解答例 (1) φ が加法と 1 と乗法を保つことを示せばよい．

任意に $f, g\in R[x]$ をとる．f, g は次のように表される：

$$f = \sum_i a_i x^i,\quad g = \sum_i b_i x^i,\quad a_i, b_i\in R.$$

有限和，有限個を除いて $a_i = b_i = 0$.

つづく

このとき,

$a \mapsto \bar{a}$ は環の準同型より

$$\varphi(f+g) = \varphi\left(\sum_i (a_i+b_i)x^i\right) = \sum_i (\overline{a_i+b_i})\,x^i = \sum_i (\bar{a}_i + \bar{b}_i)\,x^i$$

$1x^0 \overset{\varphi}{\mapsto} \bar{1}x^0$

$$= \sum_i \bar{a}_i x^i + \sum_i \bar{b}_i x^i = \varphi(f)+\varphi(g).$$

$\varphi(1) = \bar{1} = ((R/pR)[x]$ における乗法の単位元$)$.

ポイント

$$\varphi(fg) = \varphi\left(\sum_k\left(\sum_{i+j=k} a_i b_j\right)x^k\right) = \sum_k\left(\overline{\sum_{i+j=k} a_i b_j}\right)x^k = \sum_k\left(\sum_{i+j=k}\bar{a}_i\,\bar{b}_j\right)x^k$$

$$= \left(\sum_i \bar{a}_i x^i\right)\left(\sum_j \bar{b}_j x^j\right) = \varphi(f)\varphi(g).$$

$$\left(\sum_i a_i x^i\right)\left(\sum_j b_j x^j\right) = \sum_{i,j} a_i b_j x^{i+j} = \sum_k\left(\sum_{i+j=k} a_i b_j\right)x^k$$

これで $\varphi : R[x] \to (R/pR)[x]$ が環の準同型であることが示された.

(2) φ が全射であることを示そう.

$F \in (R/pR)[x]$ を任意にとる. $F = \sum_i \alpha_i x^i$ (有限和), $\alpha_i \in R/pR$ と書ける.

R/pR の元はすべて $\bar{a}$, $a \in R$ の形をしているので, $\alpha_i = \bar{a}_i$, $a_i \in R$ と書ける.

F が n 次のとき, $i > n$ ならば $a_i = 0$ としておく.

そのとき, $f = \sum_i a_i x^i$ によって, $f \in R[x]$ を作れ, $\varphi(f) = \sum_i \bar{a}_i x^i = \sum_i \alpha_i x^i = F$.

これで, φ の全射性を示せた.

(3) $\mathrm{Ker}\,\varphi = pR[x]$ を示そう.

$\mathrm{Ker}\,\varphi \supset pR[x]$ を示そう. 任意に $f \in pR[x]$ をとる $f = pg,\ g \in R[x]$ と書ける.

ゆえに, $\varphi(f) = \varphi(pg) = \varphi(p)\varphi(g) = \overline{p}\,\varphi(g) = \overline{0}\,\varphi(g) = \overline{0}$.

したがって, $f \in \mathrm{Ker}\,\varphi$. $\quad \overline{p} = \overline{0}$ in R/pR

これで, $\mathrm{Ker}\,\varphi \supset pR[x]$ が示された.

$\mathrm{Ker}\,\varphi \subset pR[x]$ を示そう. 任意に $f \in \mathrm{Ker}\,\varphi$ をとる. $\varphi(f) = \overline{0}$ が成立している.

$f = \sum_i a_i x^i$ と書ける. そのとき, $\varphi(f) = \sum_i \overline{a_i}\, x^i$.

これが $\overline{0}$ に等しいので, すべての i について, $\overline{a_i} = \overline{0}$ となる.

これは, $a_i \in pR$ と同値なので, $a_i = pb_i,\ b_i \in R$ と書ける.

ゆえに, $f = \sum_i p b_i x^i = p \sum_i b_i x^i \in pR[x]$.

これで, $\mathrm{Ker}\,\varphi \subset pR[x]$ が示された.

以上によって, $\mathrm{Ker}\,\varphi = pR[x]$ が示された.

(4) 環の同型写像 $\overline{\varphi}: R[x]/pR[x] \xrightarrow{\sim} (R/pR)[x]$, $(f \bmod p) \mapsto \varphi(f)$ が得られることを示す。

しかし、これは (1), (2), (3) に環の準同型定理を適用した結果に等しい。

<u>環の準同型定理</u>　環 A, B と環の準同型写像 $\varphi: A \to B$ について、次の環の同型写像が得られる：

$$\begin{array}{ccc} \overline{\varphi}: A/\mathrm{Ker}\,\varphi & \longrightarrow & \mathrm{Im}\,\varphi = \{\varphi(x) \mid x \in A\} \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ a + \mathrm{Ker}\,\varphi & \longmapsto & \varphi(a). \end{array}$$

これを $A = R[x]$, $B = (R/pR)[x]$, φ を問題のものとすると、ほしい結果が得られる。

$\square$

環の準同型定理の証明をきちんと理解しておくと、

他のことがらも理解しやすくなる。

そこに基本がつまっている！

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

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

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.

(補足: $\omega\in\mathbb{C}$)

$\mathbb{Q}[\alpha]=\left(\begin{array}{l}\mathbb{Q}\text{ と }\alpha\text{ を含む }\mathbb{C}\text{ の}\\ \text{最小の部分環}\end{array}\right)$

$=\{a+b\alpha+c\alpha^2\mid a,b,c\in\mathbb{Q}\}$

(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$\underbrace{\text{乗法の単位元}}_{=1}$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.

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. □

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

$\mathrm{Ker}\,\varphi$ は PID の $\mathbb{Q}[x]$ のイデアルになるので, ある $f_0(x) \in \mathrm{Ker}\,\varphi$ が存在して,
$\mathrm{Ker}\,\varphi = f_0(x)\mathbb{Q}[x]$ となる.

$f(x) \in \mathrm{Ker}\,\varphi$ なので, $f(x) = f_0(x)g(x)$, $g(x) \in \mathbb{Q}[x]$ と書ける.

$f(x)$ は $\mathbb{Q}$ 上既約なので, $\deg f_0(x) = 0$ または $\deg g(x) = 0$ となる.

もしも $\deg f_0(x) = 0$ ならば $f_0(x) = a \in \mathbb{Q}^\times$ となるので $f_0(\alpha) = a \neq 0$ となり,
$f_0(x) \in \mathrm{Ker}\,\varphi$ に矛盾する. ゆえに, $\deg g(x) = 0$ すなわち, $g(x) = c \in \mathbb{Q}^\times$ となる.
このとき, $f_0(x) = c^{-1}f(x)$ なので,

$$\mathrm{Ker}\,\varphi = f_0(x)\mathbb{Q}[x] = c^{-1}f(x)\mathbb{Q}[x] = f(x)\mathbb{Q}[x].$$

(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 $\iff$ $(p) = pA$ は A の極大イデアル $\iff$ $A/(p)$ 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！）

$\square$

(3)の証明の古いバージョンの記録

(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 $\underbrace{\mathrm{Ker}\,\varphi \text{に含まれる}}_{\Leftrightarrow\ \alpha\text{を代入すると}0\text{になる}}$ 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．

（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 $\mathrm{Ker}\,\varphi$ に含まれる 0 でない多項式の中で最低次のものなので，$r=0$．

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 $\mathbb{Q}$ 上の最小多項式と呼ぶ．上の f は $\sqrt[3]{7}$ の $\mathbb{Q}$ 上の最小多項式．）