環論演習 1

問 1.

(1) 環 $\boldsymbol{Z}/7\boldsymbol{Z}$, $\boldsymbol{Z}/8\boldsymbol{Z}$ の単数を求めよ。

(2) 環 R の元 x が，ある正整数 n に対し，$x^n = 0$ を充たすとき，ベキ零という。
x がベキ零ならば $1 + x$ は単数であることを示せ。

問 2.
例 12 の環 $R = \boldsymbol{Z} + \boldsymbol{Z}\varepsilon$ に対し，単数の全体 $R^\times$ を求めよ。

解答

問 1.

(1) $\boldsymbol{Z}/7\boldsymbol{Z}$ について
$\overline{2} \cdot \overline{4} = \overline{8} = \overline{1}$ であるから $\overline{2}$, $\overline{4}$ は単数である。同様に,
$\overline{3} \cdot \overline{5} = \overline{15} = \overline{1}$ であるから $\overline{3}$, $\overline{5}$ は単数であり,
$\overline{6} \cdot \overline{6} = \overline{36} = \overline{1}$ であるから $\overline{6}$ もまた単数である。単位元 $\overline{1}$ はもちろん単数。
したがって，$\boldsymbol{Z}/7\boldsymbol{Z}$ の単数は $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{5}$, $\overline{6}$ である。

$\boldsymbol{Z}/8\boldsymbol{Z}$ について
$\overline{2} \cdot \overline{4} = \overline{8} = \overline{0}$ より，$\overline{2}$, $\overline{4}$ は零因子なので単数ではない。
$\overline{3} \cdot \overline{3} = \overline{9} = \overline{1}$ であるから，$\overline{3}$ は単数である。
$\overline{5} \cdot \overline{5} = \overline{25} = \overline{1}$ であるから，$\overline{5}$ は単数である。
$\overline{6} \cdot \overline{4} = \overline{24} = \overline{0}$ より，$\overline{6}$ は零因子なので単数ではない。
$\overline{7} \cdot \overline{7} = \overline{49} = \overline{1}$ より，$\overline{7}$ は単数である。以上から,
$\boldsymbol{Z}/8\boldsymbol{Z}$ の単数は $\overline{1}$, $\overline{3}$, $\overline{5}$, $\overline{7}$ である。

(2) **(証明)** x がベキ零ならば，$x^n = 0$ をみたすような $n \in \boldsymbol{N}$ が存在する。このとき，$m \geq n$ なる任意の $m \in \boldsymbol{N}$ に対して $x^m = 0$ であるから，そのような m を奇数としてとれば,

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

である。したがって，$1 + x$ は単数である。

□

問 2.
R の単位元は 1 である。実際任意に R の元 $a+b\varepsilon$ $(a,b\in \boldsymbol{Z})$ をとれば,
$(a+b\varepsilon)(c+d\epsilon)=a+b\varepsilon \Longleftrightarrow ac=a,\ ad+bc=b \Longleftrightarrow c=1,\ d=0$
である。$a+b\epsilon\in R$ $(a,b\in \boldsymbol{Z})$ を単数とし，$c+d\varepsilon$ $(c.d\in \boldsymbol{Z})$ をその逆元とすると，
$ab+(ad+bc)\varepsilon=1$ であるから，$ac=1$ かつ $ad+bc=0$ である。今，$a,b,c,d\in \boldsymbol{Z}$ であるから，$ac=1$ より $a=\pm 1$ となる。逆に，$a+b\varepsilon$ は $a=\pm 1$ ならば，$a-b\varepsilon$ を逆元にもつような単数であることがわかるから，$R^{\times}=\{a+b\varepsilon \mid a=\pm 1,\ b\in \boldsymbol{Z}\}$ である。

環論演習 2

問 1.

(1) 教科書 問題 2.1，問 2

「$f(x) \in R[x],\ a \in R$ とする。このとき，$f(x)$ が既約 $\Leftrightarrow f(x+a)$ が既約」を示せ。

(2) (1) を利用し，素数 p に対して，

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

が $\boldsymbol{Z}[x]$ の多項式として既約であることを示せ。

問 2.
$f(x) \in \boldsymbol{Q}[x]$ は次数 3 の多項式とする。
命題 「$f(x)$ が $\boldsymbol{Q}$ の中に根を持たないならば，$f(x)$ は既約」
を証明せよ。次に，この命題の逆を書き，証明せよ。

解答

問 1.
(証明)
対偶をとり,「$f(x)$ が可約 $\Leftrightarrow f(x+a)$ が可約」であることを示す。
$f(x)$ が既約でないとすれば，$f(x) = g(x)h(x)$ となるような，$g(x), h(x) \in R[x]$
（ただし $\deg(g(x)), \deg(h(x)) \geq 1$）が存在する。このとき，$f(x+a) = g(x+a)h(x+a)$
であり，$g(x+a),\ h(x+a)$ はいずれも次数 1 以上であるから $f(x+a)$ は可約である。
逆に，$f(x+a)$ が可約ならば上の結果から，$f(x+a+(-a)) = f(x)$ は可約である。

□

問 2.

(証明)
3 次の多項式 $f(x)$ が可約であるとし，$f(x) = g(x)h(x)$ であるとすれば，$g(x),\ h(x)$ の
いずれかの次数は 1 でなくてはならない。それを $g(x) = x - a\ \ (a \in \boldsymbol{Q})$ とすれば，$f(x)$
は a を根に持つ。したがって，$f(x)$ が $\boldsymbol{Q}$ の中に根を持たないならば，$f(x)$ は既約
である。

□

逆 :「$f(x)$ が既約ならば $f(x)$ は $\boldsymbol{Q}$ の中に根を持たない」

(証明)
もし $f(x)$ が $\boldsymbol{Q}$ の中に根 a をもてば $f(x)$ は $x-a$ で割り切れるから，$f(x) = (x-a)g(x)$
と表せる。今，$f(x)$ の次数は 3 であるから，$\deg g(x) = 2$ であり，$f(x)$ は可約である。

□

環論演習 3

問 1.

(1) 体 K のイデアルはゼロイデアル $0(=(0))$ と K 自身 $K(=(1))$ の 2 つのみであることを示せ。逆に，可換環 R がゼロイデアルと R 自身の 2 つしかイデアルを持たないならば R は体であることを示せ。

(2) 環 $\boldsymbol{Z}[x]$ の中で，$(2)\cap(x)=(2x)$ であることを示せ。

問 2.

(1) a,b は整数とするとき，$(*)\cdots(a)\subset(b)\Leftrightarrow b|a$ を証明せよ。$(*)$ を用いて次を示せ：

(1.1) $(12)+(36)\subset(6)$　　(1.2) $(24)\subset(6)\cap(8)$

(2) 計算により (1.1), (1.2) の逆の包含関係 $\supset$ を示し，

$(12)+(30)=(6)$　　$(24)=(6)\cap(8)$

を証明せよ。

解答

問 1.

(1) **(証明)**

$\mathfrak{a}$ を 0 でない K のイデアルとすると，$\mathfrak{a}$ は 0 でない K の元 a を含むから，イデアルの定義により $1=a^{-1}a\in\mathfrak{a}$ である。よって任意の K の元 x に対して，$x=x1\in\mathfrak{a}$ となり $K\subset\mathfrak{a}$ である。したがって，$\mathfrak{a}=K$ であるから，体 K のイデアルは 0 と K 自身の 2 つである。

逆に可換環 R が 0 と K 自身の 2 つしかイデアルをもたないとする。このとき，任意の 0 でない R の元 a に対し，a で生成されるイデアル $(a)=Ra$ はゼロイデアルではないから，仮定によりこれは R 自身となる。したがって，$Ra=R$ であるから，$ba=1$ となるような R の元 b が存在するので，a は単数。今，a は任意の 0 でない R の元であったから，R は体である。

□

(2) **(証明)**

$(2)\cap(x)\supset(2x)$ であること。

$(2x)$ の任意の元は $2x\cdot f(x)$　$(f(x)\in\boldsymbol{Z}[x])$ と表せるから，$2x\cdot f(x)\in(2)$ かつ $2x\cdot f(x)\in(x)$ である。

$(2) \cap (x) \subset (2x)$ であること。

$f(x) \in (2) \cap (x)$ とし，$f(x) = a_0 + a_1 x + \cdots + a_m x^m$ $(a_0, \ldots, a_m \in \boldsymbol{Z})$ とおく。このとき，$f(x) \in (2)$ より，$a_0, \ldots, a_m \in 2\boldsymbol{Z}$ であり $f(x) \in (x)$ より，$a_0 = 0$ である。したがって，$a_i = 2a_i'$ とおけば，$f(x) = 2a_1' x + \cdots + 2a_m' x^m = 2x(a_1' + \cdots + a_m' x^{m-1})$ であるから $f(x) \in (2x)$ である。

□

問 2.

(1) **(証明)**

$(a) \subset (b) \Rightarrow b|a$

(b) の任意の元は bx $(x \in \boldsymbol{Z})$ と表せる。今，$(a) \subset (b)$ より，$a \in (b)$ であるから，$a = bx$ となるような $x \in \boldsymbol{Z}$ が存在するので，$b|a$ である。

$(a) \subset (b) \Leftarrow b|a$

仮定から $b|a$ であるから $a = bk$ とおいておけば，任意の $ax \in (a)$ $(x \in \boldsymbol{Z})$ に対して，$ax = bkx \in (b)$ である。したがって，$(a) \subset (b)$ である。

以上から，$(*)$ が証明された。

$(12) + (30) \subset (6)$ であること。

$(*)$ より，$(12) \subset (6)$, $(30) \subset (6)$ である。$(12) + (30)$ は (12) と (30) を含む最小のイデアルであるから，$(12) + (30) \subset (6)$ である。

$(24) \subset (6) \cap (8)$ であること。

$(*)$ より，$(24) \subset (6)$, $(24) \subset (8)$ であるから，任意の $x \in (24)$ に対して $x \in (6)$ かつ $x \in (8)$ である。したがって，$x \in (6) \cap (8)$ より，$(24) \subset (6) \cap (8)$ である。

□

(2) **(証明)**

$(12) + (30) \supset (6)$ であること。

(6) の任意の元 $6x$ $(x \in \boldsymbol{Z})$ が，$12a + 30b$ $(a, b \in \boldsymbol{Z})$ の形に表せることを示せばよい。2 と 5 は互いに素であるから，$2s + 5t = 1$ となるような整数 s, t が存在する。したがって，$a = sx$, $b = tx$ とおけば，$6x = 6x(2s + 5t) = 12sx + 30tx = 12a + 30b$ となる。

$(24) \supset (6) \cap (8)$ であること。

任意の $x \in (6) \cap (8)$ に対して，$6|x$ かつ $8|x$ であるから，$24|x$ である。

□

環論演習 4

問 1.

(1) $\boldsymbol{Z}$ のイデアル (3) による剰余環 $\boldsymbol{Z}/(3) = \{\overline{0}, \overline{1}, \overline{2}\}$ において次の問に答えよ。

(1.1) x の方程式 $\overline{2}x + \overline{1} = \overline{0}$ を解け。

(1.2) x の方程式 $\overline{2}x^2 + x + \overline{1} = \overline{0}$ は $\boldsymbol{Z}/(3)$ に解を持つか調べよ。

(2) $\boldsymbol{Z}$ のイデアル (12) による剰余環 $\boldsymbol{Z}/(12) = \{\overline{0}, \overline{1}, \cdots, \overline{11}\}$ において次の問に答えよ。

(2.1) x の方程式 $x^2 = \overline{4}$ を解け。

(2.2) x の方程式 $\overline{4}x + \overline{1} = \overline{0}$ は $\boldsymbol{Z}/(12)$ に解を持つか調べよ。

問 2.

(1) 複素数体の部分環 $\boldsymbol{Z}[i] = \{a + bi : a, b \in \boldsymbol{Z}\}$ のイデアル $(1 + 3i)$ による剰余環 $R = \boldsymbol{Z}[i]/(1 + 3i)$ を考える。$\alpha \in \boldsymbol{Z}[i]$ を含む R の剰余類を $\overline{\alpha}$ と記す。

$1 + 3i \in (1 + 3i)$ より，$\overline{1 + 3i} = \overline{0}$。従って，$\overline{1} + \overline{3i} = \overline{0}$。$i$ をかけて，$\overline{i} - \overline{3} = \overline{0}$，即ち，$\overline{i} = \overline{3}$ である。このことから，$\overline{10} = \overline{0}$ を示せ。

(2) 環の準同型 $\varphi : \boldsymbol{Z} \longrightarrow R$ を $\varphi(n) = \overline{n}$ $(n \in \boldsymbol{Z})$ と定める。このとき，$\mathrm{Ker}\,\varphi = (10)$ を示せ。(実は φ は全射なので，準同型定理より $\boldsymbol{Z}/(10) \cong \boldsymbol{Z}[i]/)(1 + 3i)$ である。)

解答

問 1.

(1) (1.1) 次のような表をかけばよい。

x	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}x + \overline{1}$	$\overline{1}$	$\overline{3} = \overline{0}$	$\overline{5} = \overline{2}$

したがって，解は $x = \overline{1}$

(1.2) 上と同様に次のような表をかけばよい。

x	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}x^2 + x + \overline{1}$	$\overline{1}$	$\overline{4} = \overline{1}$	$\overline{11} = \overline{2}$

したがって，この方程式は $\boldsymbol{Z}/(3)$ の中に解を持たない。

(2) (2.1) これも (1) と同様すべて元を代入して表を作ればよい。

x	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$
x^2	$\overline{0}$	$\overline{1}$	$\overline{4}$	$\overline{9}$	$\overline{16}=\overline{4}$	$\overline{25}=\overline{1}$	$\overline{36}=\overline{0}$	$\overline{49}=\overline{1}$	$\overline{64}=\overline{4}$	$\overline{81}=\overline{9}$	$\overline{100}=\overline{4}$	$\overline{121}=\overline{1}$

したがって，この方程式の解は $x=\overline{2},\overline{4},\overline{8},\overline{10}$ である。

(2.2) これも表を作れば下のようになる。

x	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$
$\overline{4}x+\overline{1}$	$\overline{1}$	$\overline{5}$	$\overline{9}$	$\overline{13}=\overline{1}$	$\overline{17}=\overline{5}$	$\overline{21}=\overline{9}$	$\overline{1}$	$\overline{5}$	$\overline{9}$	$\overline{1}$	$\overline{5}$	$\overline{9}$

以上から，この方程式は $\boldsymbol{Z}/(12)$ の中に解を持たない。

問 2.

(1) **(証明)**

$\overline{i}=\overline{3}$ より，$\overline{i}\cdot\overline{i}=\overline{3}\cdot\overline{3}$ である。よって，$\overline{-1}=\overline{9}$ であるから，$\overline{10}=\overline{0}$

□

(2) **(証明)**

(1) の結果から，$\overline{10}=\overline{0}$ であるから，$n\in\boldsymbol{Z}$ に対し，$\varphi(10n)=\varphi(10)\varphi(n)=\overline{10}\cdot\overline{n}=\overline{0}$ なので，$(10)\subset\mathrm{Ker}\,\varphi$ であることはよいから，$\mathrm{Ker}\,\varphi\subset(10)$ を示せばよい。$n\in\mathrm{Ker}\,\varphi$，すなわち $\overline{n}=\overline{0}$ であるとすると，ある $\boldsymbol{Z}[i]$ の元 $a+bi$ $(a,b\in\boldsymbol{Z})$ が存在して，$n=(a+bi)(1+3i)$ となる。このとき，$n=(a-3b)+(3a+b)i$ であるから，虚部を比較して $3a+b=0$。よって $b=-3a$ であり，これより実部を比較すれば $n=a-3\cdot(-3a)=10a$ したがって，$n\in(10)$ である。ゆえに $\mathrm{Ker}\,\varphi\subset(10)$

□

環論演習 5

問 1.

複素数体 $\boldsymbol{C}$ 上の 1 変数多項式環 $R = \boldsymbol{C}[x]$ を考える。任意の複素数 $\lambda \in \boldsymbol{C}$ に対し $x - \lambda$ で生成された R のイデアル

$$\mathfrak{a}_\lambda = (x - \lambda) = \{(x - \lambda)f(x) : f(x) \in \boldsymbol{C}[x]\}$$

は R の極大イデアル，を示せ。

問 2.

可換環 R とそのイデアル $\mathfrak{a}$ が与えられている。このとき

剰余環 $R/\mathfrak{a}$ のイデアルは $\mathfrak{a}$ を含む R のイデアル $I(\supset \mathfrak{a})$ により，$I/\mathfrak{a}$ の形をしている。
(ただし，$I/\mathfrak{a} = \{\overline{a} : a \in I\}$)

$\because$) X を $R/\mathfrak{a}$ のイデアルとする。
$I = \{a \in R : \overline{a} \in X\}$ とおくと，I はイデアルの条件を充たすことが確かめられて，R のイデアルになる。そして，任意の $a \in \mathfrak{a}$ に対し，$R/\mathfrak{a}$ では $\overline{a} = \overline{0} \in X$ から $a \in I$。よって，$\mathfrak{a} \subset I$ である。従って，

$$I/\mathfrak{a} = \{\overline{a} : a \in I\} = \{\overline{a} : \overline{a} \in X\} = X. \quad \square$$

(1) 体 K 上の多項式環 $K[x]$ のイデアル $\mathfrak{a} = (f(x))$, $f(x) \in K[x]$ に対し，剰余環 $K[x]/\mathfrak{a}$ のイデアルは $g|f$ となる多項式 $g(x) \in K[x]$ により，$(g(x))/\mathfrak{a}$ の形をしていることを示せ。(上の事実を使う)

(2) $R = \boldsymbol{Q}[x]/(x^2 - x - 6)$ のイデアルをすべて求めよ。

解答

問 1.

(証明)
$\lambda \in \boldsymbol{C}$ を任意に一つとって固定する。このとき，$\Phi_\lambda : \boldsymbol{C}[x] \longrightarrow \boldsymbol{C}$ を $\Phi_\lambda(f(x)) = f(\lambda)$ (多項式に λ を代入する写像) によって定めると，Φ_λ は環準同型となる。また，Φ_λ は全射である。なぜなら任意の $c \in \boldsymbol{C}$ に対して，$f(x) \in \boldsymbol{C}[x]$ を定数多項式 $f(x) = c$ で定めれば $\Phi_\lambda(f(x)) = c$ である。したがって，準同型定理により $\boldsymbol{C}[x]/\mathrm{Ker}\,\Phi_\lambda \cong \boldsymbol{C}$ であるから，$\boldsymbol{C}[x]/\mathrm{Ker}\,\Phi_\lambda$ は体であるが，$\mathrm{Ker}\,\Phi_\lambda = (x - \lambda)$ であることを示せば主張は証明される。実際，

$$f(x) \in \mathrm{Ker}\,\Phi_\lambda \Longleftrightarrow f(\lambda) = 0$$
$$\Longleftrightarrow f(x) = (x - \lambda)g(x) \text{ となるような } g(x) \in \boldsymbol{C}[x] \text{ が存在する。}$$

であるから，$\mathrm{Ker}\,\Phi_\lambda = (x - \lambda)$ である。

□

問 2.

(1) **(証明)**

上の事実を用いれば，$K[x]/\mathfrak{a}$ のイデアルは $\mathfrak{a}$ を含む $K[x]$ のイデアル $I(\supset \mathfrak{a})$ により，$I/\mathfrak{a}$ の形をしている。また，$K[x]$ は単項イデアル整域（教科書 p.81 **定理 2.2.4**）であるから，この I はある $g(x) \in K[x]$ により，$I = (g(x))$ の形をしている。また，$\mathfrak{a} \subset (g(x))$ であるから，$f(x) \in (g(x))$ である。したがって，$f(x) = g(x)q(x)$ となるような $q(x) \in K[x]$ が存在するから，$g|f$ である。

□

(2) $x^2 - x - 6 = (x+2)(x-3)$ を割り切る多項式は，$1,\ x+2,\ x-3,\ x^2-x-6$ の 4 つである。(1) の結果から，R のイデアルは，

$$(1)/(x^2-x-6) = \boldsymbol{Q}[x]/(x^2-x-6) = R,\ \ (x+2)/(x^2-x-6)$$

$$(x-3)/(x^2-x-6),\ \ (x^2-x-6)/(x^2-x-6) = \{0\}$$

の 4 つである。

環論演習 6

問 1.

定理 2.2.7（極大イデアルの存在）の証明を真似て次を示せ。
可換環 R の積閉集合を S とする。このとき，$S \cap \mathfrak{p} = \emptyset$（空集合）となる素イデアル $\mathfrak{p}$ が存在する。
Hint; 1. $\mathcal{M}$ の替わりに $\mathcal{I} = \{I : I \text{ は } R \text{ のイデアルで } I \cap S = \emptyset \text{ を充たす}\}$ を考えよ。
2. イデアル $\mathfrak{p}$ が素イデアル，を証明するために，$a, b \in R,\ ab \in \mathfrak{p}$ とし，更に，$a \notin \mathfrak{p},\ b \notin \mathfrak{p}$ だったとして矛盾を出せ。

問 2.

(1) S を R の積閉集合とする．R のイデアル $\mathfrak{a}$ に対し，

$$S^{-1}\mathfrak{a} = \left\{ \frac{a}{s} : a \in \mathfrak{a},\ s \in S \right\}$$

とおくとき，$S^{-1}\mathfrak{a}$ は $S^{-1}R$ のイデアルであることを示せ。次に，

$$S^{-1}\mathfrak{a} = S^{-1}R \Leftrightarrow \mathfrak{a} \cap S \neq \emptyset$$

を示せ。

(2) 多項式環 $R = \boldsymbol{Q}[x, y]$ の積閉集合 $S = \{x^i y^j : i \geq 0,\ j \geq 0,\ i, j \in \boldsymbol{Z}\}$ とするとき，R のイデアル $\mathfrak{a} = (x^2 + y^2, (x + y)^2)$ に対し，$S^{-1}\mathfrak{a} = S^{-1}R$ を示せ。

解答

問 1.

(証明)
$\mathcal{I} = \{I : I \text{ は } R \text{ のイデアルで } I \cap S = \emptyset \text{ を充たす}\}$ とおくと，$0 \notin S$ より，$(0) \in \mathcal{I}$。したがって $\mathcal{I} \neq \emptyset$ である。そこで，$\mathcal{I}$ の任意の全順序部分集合 $\mathcal{J} = \{J_\lambda\}_{\lambda \in \Lambda}$ に対し，$\overline{\mathcal{J}} = \bigcup_{\lambda \in \Lambda} J_\lambda$ とすると，$\overline{\mathcal{J}}$ は R のイデアルである。なぜなら，$a, b \in \bigcup_{\lambda \in \Lambda} J_\lambda$ とすると，$a \in J_\lambda,\ b \in J_{\lambda'}$ となるような，$\lambda, \lambda' \in \Lambda$ が存在するが，$\mathcal{J}$ が全順序集合であるから，$\max\{J_\lambda, J_{\lambda'}\}$ を考えることができ（すなわち $J_\lambda \subset J_{\lambda'}$ または $J_\lambda \supset J_{\lambda'}$），今これを J_λ としておくと，$a, b \in J_\lambda$ である。ここで，$J_\lambda \in \mathcal{I}$ であるから J_λ は R のイデアルなので $a - b \in J_\lambda$ である。よって $a - b \in \overline{J}$, 任意の $r \in R$ に対して $ra \in J_\lambda$ であるから，$ra \in \overline{\mathcal{J}}$ でもあり $\overline{\mathcal{J}}$ は R のイデアルであることが示された。また，任意の $\lambda \in \Lambda$ に対し $J_\lambda \cap S = \emptyset$ であるから，$\overline{\mathcal{J}} \cap S = \left(\bigcup_{\lambda \in \Lambda} J_\lambda \right) \cap S = \emptyset$ でもあるから，$\overline{\mathcal{J}} \in \mathcal{I}$ である。$\overline{\mathcal{J}}$ が $\mathcal{J}$ の上界であることは明らか。以上から，$\mathcal{I}$ の任意の全順序部分集合が，$\mathcal{I}$ の

中に上界をもつことが示されたので，$\mathcal{I}$ は帰納的順序集合である。よって，ツォルンの補題により $\mathcal{I}$ には極大元 $\mathfrak{p}$ が存在する。この $\mathfrak{p}$ が素イデアルであることを示すために $a, b \in R,\ ab \in \mathfrak{p},\ a \notin \mathfrak{p},\ b \notin \mathfrak{p}$ とする。このとき，$\mathfrak{p} \subsetneq \mathfrak{p} + (a),\ \mathfrak{p} \subsetneq \mathfrak{p} + (b)$ であるから，$\mathfrak{p}$ の極大性により，$(\mathfrak{p} + (a)) \cap S,\ (\mathfrak{p} + (b)) \cap S$ はいずれも空でない。したがって，$x + ra,\ x' + r'b \in S$ となるような，$x, x' \in \mathfrak{p},\ r, r' \in R$ が存在し，S が積閉集合より，$(x + ra)(x' + r'b) = xx' + xr'b + x'ra + rr'ab \in S$ であるが，$x, x', ab \in \mathfrak{p}$ であるから，$\mathfrak{p}$ の元でもある。これは，$\mathfrak{p} \cap S = \emptyset$ であることに矛盾する。

□

問 2.

(1) **(証明)**

$\frac{a}{s},\ \frac{b}{s'} \in S^{-1}\mathfrak{a}$ とすると，$\frac{a}{s} - \frac{b}{s'} = \frac{s'a - sb}{ss'}$ であり，$a, b \in \mathfrak{a}$ より，$s'a - sb \in \mathfrak{a}$ $ss' \in S$ である。よって，$\frac{a}{s} - \frac{b}{s'} \in S^{-1}\mathfrak{a}$。また，$\frac{a}{s} \in S^{-1}\mathfrak{a},\ \frac{r}{s'} \in S^{-1}R$ ならば，$\frac{a}{s} \cdot \frac{r}{s'} = \frac{ar}{ss'}$ であり，$ar \in \mathfrak{a},\ ss' \in S$ であるから　$\frac{a}{s} \cdot \frac{r}{s'} \in S^{-1}\mathfrak{a}$ である。以上から $S^{-1}\mathfrak{a}$ は $S^{-1}R$ のイデアルである。次に，

$$S^{-1}\mathfrak{a} = S^{-1}R \Leftrightarrow \mathfrak{a} \cap S \neq \emptyset$$

を示す。

$S^{-1}\mathfrak{a} = S^{-1}R$ とすると，$\frac{a}{s} = 1$ となるような，$a \in \mathfrak{a},\ s \in S$ が存在する。このとき，$s'a = s's$ となるような $s' \in S$ が存在するが，$s'a \in \mathfrak{a},\ s's \in S$ より，$\mathfrak{a} \cap S \neq \emptyset$ である。逆に，$\mathfrak{a} \cap S \neq \emptyset$ とすると，$S^{-1}R$ のイデアル $S^{-1}\mathfrak{a}$ に単数が存在することになる。したがって，$S^{-1}\mathfrak{a} = S^{-1}R$ である。

□

(2) **(証明)**

$\frac{1}{2}((x + y)^2 - (x^2 + y^2)) = xy \in S$ であるが，$(x + y)^2,\ x^2 + y^2 \in \mathfrak{a}$ より，$xy \in \mathfrak{a}$ でもある。したがって，$\mathfrak{a} \cap S \neq \emptyset$ であるから，(1) の結果より，$S^{-1}\mathfrak{a} = S^{-1}R$

□

環論演習 7

問 1.

$\boldsymbol{Z}$ のイデアル $\mathfrak{a} = (6) = 6\boldsymbol{Z} = \{6z : z \in \boldsymbol{Z}\}$ とする。$S = 1 + \mathfrak{a} = \{1 + 6z : z \in \boldsymbol{Z}\}$ とおく。

(1) S は積閉集合を示せ。

(2) $\boldsymbol{Z}$ の S による商環 $S^{-1}\boldsymbol{Z}$ の中に，$\frac{1}{2}, \frac{1}{3}$ はあるか（即ち，$2, 3$ の逆元はあるか）？また，$\frac{1}{35}$ はあるか？

問 2.

$\boldsymbol{Z}$ の積閉集合 $S = \{6^n : n = 0, 1, 2, 3, \cdots\}$ による商環 $\boldsymbol{Z}_S$ を考える。

(1) $\boldsymbol{Z}_S$ に $\frac{1}{2}, \frac{1}{3}$ はあるか？また，$\frac{1}{5}$ はあるか？

(2) $a \in \boldsymbol{Z}$ に対し，$\boldsymbol{Z}_S$ のイデアル

$$a\boldsymbol{Z}_S := \{a \cdot \frac{z}{6^n} : z \in \boldsymbol{Z}, n = 0, 1, 2, 3, \cdots\}$$

とする。このとき，$28\boldsymbol{Z}_S = 7\boldsymbol{Z}_S$ を示せ。また，$7\boldsymbol{Z}_S$ は $\boldsymbol{Z}_S$ の素イデアルを示せ。

解答

問 1.

(1) **(証明)**
$1 + 6z, 1 + 6z' \in S$ とすると，$(1 + 6z)(1 + 6z') = 1 + 6(z + z' + 6zz') \in S$ であり，$1 \in S$ である。

□

(2) $2 \cdot \frac{a}{s} = \frac{1}{1}$ をみたすような $\frac{a}{s} \in S^{-1}\boldsymbol{Z}$ が存在したとすれば，ある $s' \in S$ があって，$2as' = ss'$ となってなくてはいけないが，左辺は偶数，右辺は S の元で奇数であるから矛盾する。したがって，2 は単数ではない。同様に 3 についても単数でないことがわかる。また，$-35 = -36 + 1 \in S$ であるから，$\frac{1}{-35} \in S^{-1}\boldsymbol{Z}$ である。
したがって，$\frac{-1}{-35} \in S^{-1}\boldsymbol{Z}$ であり，$35 \cdot \frac{-1}{-35} = 1$ であるから，35 は単数である。

問 2.

(1) $\dfrac{3}{6}, \dfrac{2}{6} \in \boldsymbol{Z}_S$ であり，$2 \cdot \dfrac{3}{6} = 1,\ 3 \cdot \dfrac{2}{6} = 1$ であるから，2 も 3 も単数である。また，$5 \cdot \dfrac{a}{s} = \dfrac{1}{1}$ となるような $\dfrac{a}{s} \in \boldsymbol{Z}$ が存在したとすると，$s' \in S$ があって $5as' = ss'$ となっていなくてはいけない。ところが，右辺は 6 のベキであるから，5 を素因数として含まないので矛盾する。したがって，5 に逆元はない。

(2) **(証明)**

任意の $28 \cdot \dfrac{z}{6^n} \in 28\boldsymbol{Z}_S$ に対して，$\dfrac{28z}{6^n} = 7 \cdot \dfrac{4z}{6^n} \in 7\boldsymbol{Z}_S$ であるから，$28\boldsymbol{Z}_S \subset 7\boldsymbol{Z}_S$ である。また，任意の $7 \cdot \dfrac{z}{6^n} \in 7\boldsymbol{Z}_S$ に対して，$\dfrac{7z}{6^n} = \dfrac{7z \cdot 6^2}{6^{n+2}} = 28 \cdot \dfrac{9z}{6^{n+2}} \in 28\boldsymbol{Z}_S$ であるから，$7\boldsymbol{Z}_S \subset 28\boldsymbol{Z}_S$ である。以上から，$28\boldsymbol{Z}_S = 7\boldsymbol{Z}_S$

また，$\dfrac{a}{6^m}, \dfrac{b}{6^n} \in \boldsymbol{Z}_S\ \ (a, b \in \boldsymbol{Z},\ m, n = 0, 1, \cdots)$ とし，$\dfrac{ab}{6^{m+n}} \in 7\boldsymbol{Z}_S$ とする。このとき，$6^\ell ab \in 7\boldsymbol{Z}\ \ (\ell = 0, 1, \cdots)$ であるから，7 は素数より $a \in 7\boldsymbol{Z}$ または $b \in 7\boldsymbol{Z}$ である。したがって，$\dfrac{a}{6^m} \in 7\boldsymbol{Z}_S$ または，$\dfrac{b}{6^n} \in 7\boldsymbol{Z}_S$ である。また，$\dfrac{1}{6} \notin 7\boldsymbol{Z}_S$ であることは容易にわかるから，$7\boldsymbol{Z}_S$ は $\boldsymbol{Z}_S$ の真のイデアルである。以上から $7\boldsymbol{Z}_S$ は素イデアルである。

□

環論演習 8

問 1.

(1) v は体 K の付値とするとき，$v(a^{-n}) = -nv(a)$ を示せ。ただし，$n \geq 0,\ a \in K$。

(2) 有理数体 $\boldsymbol{Q}$ の p 進付値 v は付値の条件 (2)，(3) を充たすことを示せ。

付値の条件 (2)　$v(\alpha\beta) = v(\alpha) + v(\beta)$

付値の条件 (3)　$v(\alpha + \beta) \geq \min\{v(\alpha), v(\beta)\}$

問 2.

$p = 5$ のとき，即ち 5 進付値を考える。このとき付値環は

$$\boldsymbol{Z}_{(5)} = \left\{ \frac{a}{b} : 5 \text{ は } b \text{ を割らない},\ a, b \in \boldsymbol{Z} \right\},$$

付値イデアルは

$$\boldsymbol{Z}_{(5)} \text{での } 5 \text{ の倍数全体 } 5\boldsymbol{Z}_{(5)} = \left\{ 5 \cdot \frac{a}{b} : \frac{a}{b} \in \boldsymbol{Z}_{(5)} \right\}$$

である。定理 2.3.5(3) を用いてイデアル $\mathfrak{a} = 200\boldsymbol{Z}_{(5)}$ を含む $\boldsymbol{Z}_{(5)}$ のイデアルをすべて求めよ。

解答

問 1.

(1) **(証明)**

$v(1) = v(1 \cdot 1) = v(1) + v(1) = 2v(1)$ であるから，$v(1) = 0$ である。したがって，$n = 0$ のときは正しい。$0 = v(1) = v(a \cdot a^{-1}) = v(a) + v(a^{-1})$ であるから，$v(a^{-1}) = -v(a)$ である。したがって，$v(a^{-n}) = \overbrace{v(a^{-1}) + \cdots + v(a^{-1})}^{n \text{ 個}} = -nv(a)$ である。

□

(2) **(証明)**

α, β のどちらかが 0 ならば，主張は明らかであるから，$\alpha \neq 0,\ \beta \neq 0$ とする。

$\alpha, \beta \in \boldsymbol{Q}$ とし，$\alpha = ap^m$, $\beta = bp^n$ $(a, b$ は分母，分子がいずれも p で割り切れないような分数，$m, n \in \boldsymbol{Z})$ と表しておくと，$v(\alpha) = m$, $v(\beta) = n$ である。このとき，$\alpha\beta = abp^{m+n}$ であり，a, b のとり方から，ab は分母，分子がいずれも p で割り切れないような分数である。したがって，$v(\alpha\beta) = m + n = v(\alpha) + v(\beta)$ である。次に (3) についてだが，$m \leq n$ としてかまわない。このとき，$a = \dfrac{y_1}{x_1}$, $b = \dfrac{y_2}{x_2}$ と表せば，

$$\alpha + \beta = (a + bp^{n-m})p^m = \left(\frac{y_1}{x_1} + \frac{y_2}{x_2}p^{n-m}\right)p^m = \left(\frac{x_2y_1 + x_1y_2p^{m-n}}{x_1x_2}\right)p^m$$

であるが，a, b のとり方から，x_1, x_2 はいずれも p で割り切れない。よって，x_1x_2 は p で割り切れず，さらに $m - n \geq 0$ であることから，$v(\alpha + \beta) \geq m = \min\{v(\alpha), v(\beta)\}$

□

問 2.

$\mathfrak{a}$ の任意の元 $200 \cdot \dfrac{a}{b}$ $\left(\dfrac{a}{b} \in \boldsymbol{Z}_{(5)}\right)$ に対して，$200 \cdot \dfrac{a}{b} = 25 \cdot \dfrac{8a}{b} \in 25\boldsymbol{Z}_{(5)}$ であり，

$25\boldsymbol{Z}_{(5)}$ の任意の元 $25 \cdot \dfrac{c}{d}$ $\left(\dfrac{c}{d} \in \boldsymbol{Z}_{(5)}\right)$ に対し，$25 \cdot \dfrac{c}{d} = 200 \cdot \dfrac{c}{8d} \in \mathfrak{a}$ であるから，

$\mathfrak{a} \subset 25\boldsymbol{Z}_{(5)}$ かつ $\mathfrak{a} \supset 25\boldsymbol{Z}_{(5)}$。よって，$\mathfrak{a} = 25\boldsymbol{Z}_{(5)}$ である。定理 2.3.5(3) から，$\boldsymbol{Z}_{(5)}$ の真のイデアルはすべて付値イデアルのベキであり，$(5\boldsymbol{Z}_{(5)})^2 = 25\boldsymbol{Z}_{(5)} = \mathfrak{a}$ である。

よって，$\mathfrak{a}$ を含むような $\boldsymbol{Z}_{(5)}$ のイデアルは，$\boldsymbol{Z}_{(5)}$ 自身，$5\boldsymbol{Z}_{(5)}$, $\mathfrak{a}$ の 3 つである。

環論演習 9

問 1.

R は domain（整域）とする。$a, b \in R$ に対し，

「$c \in R$ が a と b の最小公倍数となる必要十分条件は $(c) = (a) \cap (b)$」

を示せ。

問 2.

R は問 1. と同じとする。R の元 a と b の最小公倍数を c とする。問 1. より $(c) = (a) \cap (b)$ であるから，$(ab) \subset (a) \cap (b) = (c)$ である。従って，$ab = cd$ となる $d \in R$ がある。このとき，d は a と b の最大公約数であることを示せ。

解答

問 1.

(証明)

c が a と b の最小公倍数であるとする。このとき，$c = xa,\ c = yb$ となるような $x, y \in R$ が存在する。したがって，任意の (c) の元 $rc\ \ (r \in R)$ に対して $rc = rxa \in (a)$ かつ $rc = ryb \in (b)$ であるから，$rc \in (a) \cap (b)$。よって，$(c) \subset (a) \cap (b)$ である。また，任意に $s \in (a) \cap (b)$ をとれば，$s = r_1 a = r_2 b$ となるような，$r_1, r_2 \in R$ が存在するから，s は a, b の公倍数である。よって，s は c で割り切れるので，$s = r_3 c$ となる $r_3 \in R$ が存在するから，$s \in (c)$ である。よって $(c) \supset (a) \cap (b)$ であり，$(c) = (a) \cap (b)$ である。逆に，$(c) = (a) \cap (b)$ であるとする。このとき，$c \in (a) \cap (b)$ であるから，c は a, b の公倍数である。したがって，a, b の公倍数が c' がすべて c で割り切れることを示せばよい。c' は a, b の公倍数であるから，$c' = r_1 a = r_2 b$ となるような，$r_1, r_2 \in R$ が存在するので，$c' \in (a) \cap (b)$ である。今，$(a) \cap (b) = (c)$ であるから，$c' \in (c)$ なので，$c' = r_3 c$ となるような $r_3 \in R$ が存在するから，c' は c で割り切れる。したがって，c は a, b の最小公倍数である。

□

問 2.

(証明)

d' が a と b の公約数ならば，$d' | d$ であることを示せばよい。$a = r_1 d',\ b = r_2 d'\ \ (r_1, r_2 \in R)$ とおく。このとき，$r_1 r_2 d'$ は a, b の公倍数であるから，$r_1 r_2 d'$ は最小公倍数 c で割り

切れる。そこで，$r_1 r_2 d' = sc$ とおけば，$cd = ab = d' \cdot r_1 r_2 d' = d' sc$ となる。R は整域であるから，$d = d's$ となり，$d' | d$ である。

□

環論演習 10

問 1.

(1) $\boldsymbol{Z}[x]$ の多項式

$$f(x) = 102x^8 + 78x^7 + 84x^6 + 48x^5 + 66x^2 + 72x + 54$$

を $f(x) = ag(x),\ a \in \boldsymbol{Z},\ g(x)$ は原始的，と表せ。ただし，a は素因数分解せよ。

(2) $R = \boldsymbol{Q}[x]$ とする。$R[y]$ の多項式

$$f(y) = x^3y^4 - \frac{5}{2}x^2y^4 + xy^4 + x^2y^3 + x^3y^2 - \frac{5}{2}xy^3 - \frac{7}{2}x^2y^2 + x^3 + y^3 + \frac{7}{2}xy^2 - \frac{3}{2}x^2 - y - 2 - \frac{3}{2}x + 1$$

を $f(y) = ag(y),\ a \in \boldsymbol{Q}[x],\ g(y)$ は原始的，と表せ。ただし，a は因数分解せよ。

問 2.

(1) $\boldsymbol{Z}[x]$ の多項式

$$f(x) = 144x^3 + 432x^2 + 72x + 216$$

を素元分解せよ。

(2) $R = \boldsymbol{Q}[x]$ とする。$R[y]$ の多項式

$$f(y) = x^6y + x^3y^2 - x^5 - x^4y - x^2y - xy^2 + x^3 + y$$

を $f(y) = ag(y),\ a \in \boldsymbol{Q}[x],\ g(y)$ は原始的，と表し，$f(y)$ を素元分解（因数分解）せよ。

解答

問 1.

(1) 各係数の最大公約数は 6 である。したがって，

$$f(x) = 2 \cdot 3 \cdot (17x^8 + 13x^7 + 14x^6 + 8x^5 + 11x^2 + 12x + 9)$$

(2)

$$f(y) = \frac{1}{2}\{(2x^3 - 5x^2 + 2x)y^4 + (2x^2 - 5x + 2)y^3 + (2x^3 - 7x^2 + 7x - 2)y^2 + (2x^3 - 3x^2 - 3x + 2)\}$$

である。各係数について

$$2x^3-5x^2+2x=x(2x-1)(x-2)$$
$$2x^2-5x+2=(2x-1)(x-2)$$
$$2x^3-7x^2+7x-2=(x-2)(2x^2-3x+1)=(x-2)(2x-1)(x-1)$$
$$2x^3-3x^2-3x+2=(x+1)(2x^2-5x+2)=(x+1)(2x-1)(x-2)$$

であるから，$f(x)=\dfrac{1}{2}(2x-1)(x-2)\{xy^4+y^3+(x-1)y^2+(x+1)\}$

問 2.

(1) $f(x)=72(2x^3+6x^2+x+3)=2^3\cdot 3^2\cdot(x+3)(2x^2+1)$
であり，$2x^2+1$ は既約な原始多項式であるから，これでよい。

(2) $f(y)=(x^3-x)y^2+(x^6-x^4-x^2+1)y-(x^5-x^3)$ であり，各係数は

$$x^3-x=x(x+1)(x-1)$$
$$x^6-x^4-x^2+1=x^4(x^2-1)-(x^2-1)=(x^2-1)(x^4-1)=(x+1)^2(x-1)^2(x^2+1)$$
$$x^5-x^3=x^3(x^2-1)=x^3(x+1)(x-1)$$

であるから，
$f(y)=(x+1)(x-1)\{xy^2+(x+1)(x-1)(x^2+1)y-x^3\}=(x+1)(x-1)(y+x^3)(xy-1)$

環論演習 11

問 1.

R は可換環，S を R の積閉集合とする。R の S による商環 $S^{-1}R$ のイデアルは全て次の $(*)$ の様に表されることは証明されている：

$$(*)\quad S^{-1}\mathfrak{a} = \left\{ \frac{a}{s} : a \in \mathfrak{a},\ s \in S \right\}\quad (\mathfrak{a} \text{ は } R \text{ のイデアル})$$

この事実を用いて $(**)$ を示せ。

$$(**)\quad R \text{ がネータ環ならば} S^{-1}R \text{ もネータ環である.}$$

問 2.

$\boldsymbol{Z}[x]$ の部分環 R を

$$R = \boldsymbol{Z}[2x, 2x^2, 2x^3, \cdots]$$

とする。即ち，多項式 $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \boldsymbol{Z}[x]$ について，

$$f(x) \in R \Longleftrightarrow a_1, \cdots, a_n \text{は } 2 \text{ の倍数 } (a_0 \text{はどの整数でもよい})$$

R の部分集合 $\mathfrak{a}$ を

$$\mathfrak{a} = \{ a_n x^n + \cdots + a_1 x : n \geq 1,\ a_1, \cdots, a_n \text{は } 2 \text{ の倍数} \}$$

とおく。このとき

(1) $\mathfrak{a}$ は R のイデアルを示せ。

(2) $\mathfrak{a}$ は有限生成でないことを示せ（従って R はネータ環ではない。）

解答

問 1.

(証明)

$S^{-1}R$ の任意のイデアルの無限上昇列を

$$S^{-1}\mathfrak{a}_0 \subset S^{-1}\mathfrak{a}_1 \subset \cdots \subset S^{-1}\mathfrak{a}_n \subset \cdots$$

を考える。(上の $(*)$ からこのような形をしている) このとき，各 $i \leq 0$ に対し，$\mathfrak{a}_i \subset \mathfrak{a}_{i+1}$ である。なぜなら，$\mathfrak{a}_i$ の任意の元 a に対し，$\dfrac{a}{1} \in S^{-1}\mathfrak{a}_i$ であるから，$\dfrac{a}{1} \in S^{-1}\mathfrak{a}_{i+1}$ でもあり，$a \in \mathfrak{a}_{i+1}$ である。したがって，R のイデアルの無限上昇列

$$\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \cdots \subset \mathfrak{a}_n \subset \cdots$$

が得られるが，R がネータ環であることから，ある $n \in \boldsymbol{Z}$ が存在して，$\mathfrak{a}_n = \mathfrak{a}_{n+1} = \cdots$ となる。したがって，このとき $S^{-1}\mathfrak{a}_n = S^{-1}\mathfrak{a}_{n+1} = \cdots$ であるから，$S^{-1}R$ はネータ環である。

□

問 2.

(1) **(証明)**

$f(x), g(x) \in \mathfrak{a}$ ならば，$f(x), g(x)$ の定数項は 0 であるから $f(x) - g(x)$ の定数項も 0 である。したがって，$f(x) - g(x) \in \mathfrak{a}$ である。また，任意の $h(x) \in R$ に対して，$h(x)f(x)$ の定数項も 0 であるから，$h(x)f(x) \in \mathfrak{a}$。よって，$\mathfrak{a}$ は R のイデアル。

□

(2) **(証明)**

$\mathfrak{a}$ が有限生成であると仮定し，$\mathfrak{a} = (f_1(x), \cdots, f_n(x))$ とおく。このとき，各生成元の次数の中で最大のものを m とおくと，任意の $g(x) \in R$ に対して $g(x)f_i(x)$ の $m+1$ 次の係数は 4 の倍数である。したがって $2x^{m+1} \in \mathfrak{a}$ であるが，

$$2x^{m+1} = g_1(x)f_1(x) + \cdots + g_n(x)f_n(x)$$

とおけば，$g_1(x)f_1(x) + \cdots + g_n(x)f_n(x)$ の $m+1$ 次の係数は 4 の倍数であるから 2 にはなり得ないので矛盾。よって $\mathfrak{a}$ は有限生成ではない。

□

環論演習 12

問 1.

p, q が相異なる素数のとき，$\boldsymbol{Z}$ のイデアル (p^2)，(pq) に対して

$$\sqrt{(p^2)} = (p), \quad \sqrt{(pq} = (pq)$$

を示せ。

問 2.

p が素数のとき，$\boldsymbol{Z}$ のイデアル (p^2) について次の問に答えよ。

(1) $\boldsymbol{Z}$ のイデアル $\mathfrak{a}$ が $\mathfrak{a} \supset (p^2)$ ならば $\mathfrak{a} = \boldsymbol{Z}$ または $\mathfrak{a} = (p^2)$ または $\mathfrak{a} = (p)$ を示せ。

(2) (p^2) は既約なイデアル，を示せ。

解答

問 1.

(証明)

$\sqrt{(p^2)} = (p)$ であること：
任意の $pm \in (p)$ $(m \in \boldsymbol{Z})$ に対して，$(pm)^2 = p^2m^2 \in (p^2)$ であるから，$pm \in \sqrt{(p^2)}$ である。よって，$\sqrt{(p^2)} \supset (p)$
また，$x \in \sqrt{(p^2)}$ ならば，ある $k \in \boldsymbol{Z}$ が存在し，$x^k \in (p^2)$ となるから，$p^2 \mid x^k$ であり，p は素数であるから，$p \mid x$ でなければならない。したがって，$x \in (p)$ であるから，$\sqrt{(p^2)} \subset (p)$
以上から，$\sqrt{(p^2)} = (p)$ である。

$\sqrt{(pq)} = (pq)$ であること：
$\sqrt{(pq)} \supset (pq)$ であることは明らかなので，$\sqrt{(pq)} \subset (pq)$ であることを示せばよい。
$x \in \sqrt{(pq)}$ ならば，ある $m \in \boldsymbol{Z}$ が存在し，$x^m \in (pq)$ となるから，このとき $pq \mid x^m$ である。今，p, q は相異なる素数であるから，$pq \mid x$ でなければならない。したがって，$x \in (pq)$ であり，$\sqrt{(pq)} \subset (pq)$

□

問 2.

(1) **(証明)**

$\boldsymbol{Z}$ は単項イデアル整域であるから，$\mathfrak{a} = (m)$ $(m \in \boldsymbol{Z})$ と表しておく。p.92 の補題 2.4.1 より，$(m) \supset (p^2) \Leftrightarrow m \mid p^2$ であるから，m は $1, p, p^2$ のいずれかである。したがって，$m = 1$ のとき，$\mathfrak{a} = (m) = \boldsymbol{Z}$，$m = p$ のとき，$\mathfrak{a} = (p)$，$m = p^2$ のとき，$\mathfrak{a} = (p^2)$ である。

□

(2) **(証明)**

$1 \notin (p^2)$ であるから，$(p^2) \subsetneq \boldsymbol{Z}$ であることはよい。また，(1) の結果から (p^2) を真に含む $\boldsymbol{Z}$ のイデアルは $\boldsymbol{Z}$ と (p) しかなく，$(p) \cap (p) = (p)$, $(p) \cap \boldsymbol{Z} = (p)$, $\boldsymbol{Z} \cap \boldsymbol{Z} = \boldsymbol{Z}$ であるから，(p^2) は既約なイデアルである。

□

環論演習 13

問 1.

R を環とし，$e \in R$ は $e^2 = e$ をみたすとする。$e \neq 0, 1$ ならば，e は零因子であることを示せ。

問 2.

R を可換環とし，$x \in R$ とする。このとき，

$$\ell(x) := \{\, r \in R \mid rx = \{0\} \,\}$$

は R のイデアルであることを示せ。

問 3.

(1) $\boldsymbol{Z}/45\boldsymbol{Z}$ のイデアルをすべて求めよ。

(2) $\boldsymbol{Z}/45\boldsymbol{Z}$ の素イデアルはどれか。

解答

問 1.

(証明)

$e \neq 0, 1$ であるから，$1 - e \neq 0, 1$ である。ところが，$0 = e - e^2 = e(1 - e) = (1 - e)e$ であるから，e は零因子である。

□

問 2.

(証明)
$a, b \in \ell(x)$ とする。このとき，$(a - b)x = ax - bx = 0 - 0 = 0$ であるから，$a - b \in \ell(x)$
また，任意の $r \in R$ に対し，$(ra)x = r(ax) = r0 = 0$ であるから，$ra \in \ell(x)$
以上から，$\ell(x)$ は R のイデアルである。

□

問 3.

(1) $\boldsymbol{Z}/45\boldsymbol{Z}$ のイデアルは $45\boldsymbol{Z}$ を含む $\boldsymbol{Z}$ のイデアル $\mathfrak{a} = m\boldsymbol{Z}$ $(m \in \boldsymbol{Z})$ によって，$m\boldsymbol{Z}/45\boldsymbol{Z}$ の形をしている (環論演習 5 の (2) 参照)。したがって，$45\boldsymbol{Z}$ を含む $\boldsymbol{Z}$ のイデアルをすべて求めれば良いが，p.92 の補題 2.4.1 より，$(m) \supset (45) \Leftrightarrow m \mid 45$ であるから，45 の約数を調べればよい。したがって，45 の約数は $1, 3, 5, 9, 15, 45$ であるから，$\boldsymbol{Z}/45\boldsymbol{Z}$ のすべてのイデアルは，$\boldsymbol{Z}/45\boldsymbol{Z}$, $3\boldsymbol{Z}/45\boldsymbol{Z}$, $5\boldsymbol{Z}/45\boldsymbol{Z}$, $9\boldsymbol{Z}/45\boldsymbol{Z}$, $15\boldsymbol{Z}/45\boldsymbol{Z}$, $\{0\}$ である。

(2) 極大イデアルは素イデアルであるから，$3\boldsymbol{Z}/45\boldsymbol{Z}$, $5\boldsymbol{Z}/45\boldsymbol{Z}$ は素イデアルである。また，$\overline{a} = a+45\boldsymbol{Z}$ $(a \in \boldsymbol{Z})$ と表すことにすると，$\overline{3} \notin 9\boldsymbol{Z}/45\boldsymbol{Z}$ であるが，$\overline{3}\cdot\overline{3} = \overline{9} \in 9\boldsymbol{Z}/45\boldsymbol{Z}$ であるから，$9\boldsymbol{Z}/45\boldsymbol{Z}$ は素イデアルではない。さらに，$\overline{5}, \overline{3} \notin 15\boldsymbol{Z}/45\boldsymbol{Z}$ であるが，$\overline{3}\cdot\overline{5} = \overline{15} \in 15\boldsymbol{Z}/45\boldsymbol{Z}$ であるから，$15\boldsymbol{Z}/45\boldsymbol{Z}$ も素イデアルではない。同様に，$\overline{5}, \overline{9} \neq \overline{0}$ であるが，$\overline{9}\cdot\overline{5} = \overline{0}$ であるから，$45\boldsymbol{Z}/45\boldsymbol{Z} = \{0\}$ も素イデアルではない。以上から，素イデアルは $3\boldsymbol{Z}/45\boldsymbol{Z}$, $5\boldsymbol{Z}/45\boldsymbol{Z}$ である。

(別解)

$(\boldsymbol{Z}/45\boldsymbol{Z})/(m\boldsymbol{Z}/45\boldsymbol{Z}) \cong \boldsymbol{Z}/m\boldsymbol{Z}$ $(m = 1, 3, 5, 9, 15, 45)$ であるから，$m\boldsymbol{Z}/45\boldsymbol{Z}$ が素イデアルであることと $\boldsymbol{Z}/m\boldsymbol{Z}$ が整域であることと同値である。それはさらに，$m\boldsymbol{Z}$ が素イデアルであることと同値なのだから，$\boldsymbol{Z}/45\boldsymbol{Z}$ の素イデアルは $3\boldsymbol{Z}/45\boldsymbol{Z}$, $5\boldsymbol{Z}/45\boldsymbol{Z}$ である。

環論演習 14

問 1.

環準同型 $\varphi : \boldsymbol{R}[x] \longrightarrow \boldsymbol{C}$ を $\varphi(f(x)) = f(i)$ $(i = \sqrt{-1})$ によって定める。次の問に答えよ。

(1) φ は全射であることを示せ。

(2) $\ker\varphi$ を求めよ。

(3) $\boldsymbol{C}$ はある $\boldsymbol{R}[x]$ の剰余環と同型であることを示せ。

問 2.

R を可換環とし，$a_1, \cdots, a_n \in R$ とする。このとき，

$$(a_1, \cdots, a_n) = \{\, a_1r_1 + \cdots + a_nr_n \mid r_1, \cdots, r_n \in R \,\}$$

であることを示せ。

解答

問 1.

(1) **(証明)**

任意の $a + bi \in \boldsymbol{C}$ $(a, b \in \boldsymbol{R})$ に対し，$f(x) = a + bx$ とおけば，$\varphi(f(x)) = a + bi$ であるから φ は全射である。

□

(2) $\varphi(x^2+1) = 0$ であるから，$\ker\varphi \supset (x^2+1)$ である。なぜなら，任意の $(x^2+1)f(x) \in (x^2+1)$ に対して，φ は環準同型であるから，$\varphi((x^2+1)f(x)) = \varphi(x^2+1)\varphi(f(x)) = 0$

逆に，$f(x) \in \ker\varphi$ ならば，$f(i) = 0$ であるから，因数定理により $f(x)$ は x^2+1 で割り切れる。したがって，$\ker\varphi \subset (x^2+1)$ である。よって，$\ker\varphi = (x^2+1)$

(3) **(証明)**

準同型定理より，$\boldsymbol{R}[x]/\ker\varphi \cong \mathrm{Im}\,\varphi$ であるが，(1), (2) より，$\mathrm{Im}\,\varphi = \boldsymbol{C}$，$\ker\varphi = (x^2+1)$ であるから，

$$\boldsymbol{R}[x]/(x^2+1) \cong \boldsymbol{C}$$

□

問 2.

(証明)
$I = \{\, a_1r_1 + \cdots + a_nr_n \mid r_1, \cdots, r_n \in R \,\}$ とおく。このとき任意の $a_1r_1 + \cdots + a_nr_n$, $a_1s_1 + \cdots + a_ns_n \in I \ \ (r_i, s_i \in R)$ に対し,

$$(a_1r_1 + \cdots + a_nr_n) - (a_1s_1 + \cdots + a_ns_n) = a_1(r_1 - s_1) + \cdots + a_n(r_n - s_n) \in I$$

また，任意の $r \in R$ に対し，$r(a_1r_1 + \cdots + a_nr_n) = a_1r_1r + \cdots + a_nr_nr \in I$ であるから，I は R のイデアルである。また，任意の $i = 0, 1, \cdots, n$ に対し，$a_i = a_i \cdot 1 \in I$ より，I は $a_1, \cdots, a_n$ を含む R のイデアルである。したがって，$(a_1, \cdots, a_n)$ とは，$a_1, \cdots, a_n$ をすべて含むような R のイデアルで最小のものであったから，$(a_1, \cdots, a_n) \subset I$ である。逆に，任意の $a_1r_1 + \cdots + a_nr_n \in I \ \ (r_1, \cdots, r_n \in R)$ に対し，$a_i \in (a_1, \cdots, a_n)$ より，イデアルの定義から $a_ir_i \in (a_1, \cdots, a_n)$ であり $a_1r_1 + \cdots + a_nr_n \in (a_1, \cdots, a_n)$ である。したがって，$(a_1, \cdots, a_n) \supset I$ であり，$(a_1, \cdots, a_n) = I$ が示された。

□

環論演習 15

問 1.

整数を成分に持つ 2 次の正方行列の全体 $M_2(\mathbb{Z})$ は行列の和と積に関して環である。$M_2(\mathbb{Z})$ の部分集合

$$R = \left\{ \begin{pmatrix} a & 2b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{Z} \right\}$$

は $M_2(\mathbb{Z})$ の部分環であることを示せ。また，R は整域かどうか調べよ。

問 2.

$\mathbb{Z}$ のイデアル (2),(6) および $\mathbb{Q}[x]$ のイデアル $(x), (x^2), (x^2+1)$ について答えよ。

(1) 極大イデアルはどれか。

(2) $6x^2$ を含むイデアルはどれか。

(3) 剰余環 $\mathbb{Z}/(6)$ と $\mathbb{Q}[x]/(x^2)$ は整域でないことを示せ。

問 3.

整数環 $\mathbb{Z}$ の積閉集合 $S = \{1, 3, 3^2, \cdots\}$ とする。$\mathbb{Z}$ の素イデアル $\mathfrak{p} = (2)$ とする。このとき，$S^{-1}\mathbb{Z} \subset \mathbb{Z}_{\mathfrak{p}}$ を示せ。

問 4.

$\mathbb{Z}[x]$ の元 $3x^2 - 18x + 24$ と $5x^2 - 20$ の最大公約数，最小公倍数を求めよ。

問 5.

素数 p に対し，$\mathbb{Z}$ のイデアル (p^3) の根基 $\sqrt{(p^3)}$ を求めよ。

解答

問 1.

(証明)

$\begin{pmatrix} a & 2b \\ 0 & a \end{pmatrix}, \begin{pmatrix} a' & 2b' \\ 0 & a' \end{pmatrix} \in R$ ならば,

$$\begin{pmatrix} a & 2b \\ 0 & a \end{pmatrix} - \begin{pmatrix} a' & 2b' \\ 0 & a' \end{pmatrix} = \begin{pmatrix} a-a' & 2(b-b') \\ 0 & a-a' \end{pmatrix} \in R$$

$$\begin{pmatrix} a & 2b \\ 0 & a \end{pmatrix} \begin{pmatrix} a' & 2b' \\ 0 & a' \end{pmatrix} = \begin{pmatrix} aa' & 2(ab'+a'b) \\ 0 & aa' \end{pmatrix} \in R$$

また,

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in R$$

以上から，R は $M_2(\mathbb{Z})$ の部分環である。

□

また，$\begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} \in R$ であるが,

$$\begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} = O$$

であるから，R は整域ではない。

問 2.

(1) $\mathbb{Z}$ に対しては素数を，$\mathbb{Q}[x]$ に対しては既約な多項式を見つければよいのだから，極大イデアルは (2), (x), (x^2+1) である。

(2) $6x^2 = 6x \cdot x = 6 \cdot x^2$ であるから，$6x^2 \in (x)$, $6x^2 \in (x^2)$ である。$x^2+1 \nmid 6x^2$ であるから，$6x^2 \notin (x^2+1)$ である。

(3) **(証明)**

$3+(6),\ 2+(6) \in \mathbb{Z}/(6)$ であり，$3+(6), 2+(6) \neq (6)$ であるが，$(3+(6))(2+(6)) = 6+(6) = (6)$ より，$\mathbb{Z}/(6)$ は整域ではない。

また，$x+(x^2) \in \mathbb{Q}[x]/(x^2)$ で，$x+(x^2) \neq (x^2)$ であるが，$(x+(x^2))(x+(x^2)) = x^2+(x^2) = (x^2)$ より，$\mathbb{Q}[x]/(x^2)$ は整域ではない。

□

(別証)

R を環 I を R のイデアルとすると，R/I が整域 $\Leftrightarrow$ I は素イデアル

$\mathbb{Z},\ \mathbb{Q}[x]$ は単項イデアル整域であるから，素イデアル $\Leftrightarrow$ 極大イデアルなので

(1) の結果から，$\mathbb{Z}/(6),\ \mathbb{Q}[x]/(x^2)$ はいずれも整域ではない。

問 3.

(証明)

$\mathbb{Z}-\mathfrak{p}$ は奇数全体の集合，すなわち $1+2\boldsymbol{Z}$ であるから，$S \subset \mathbb{Z}-\mathfrak{p}$ である。よって $S^{-1}\mathbb{Z} = \{\, \frac{a}{s} \mid a \in \mathbb{Z},\ s \in S \,\}$, $\mathbb{Z}_{\mathfrak{p}} = \{\, \frac{a}{s} \mid a \in \mathbb{Z},\ s \in 1+2\mathbb{Z} \,\}$ であるから，$S^{-1}\mathbb{Z} \subset \mathbb{Z}_{\mathfrak{p}}$ である。

□

問 4.

それぞれを素元分解すると，$3(x-2)(x-4),\ 5(x+2)(x-2)$ であるから，最大公約数は $x-2$，最小公倍数は $3\cdot 5(x-2)(x-4)(x+2)$ である。

問 5.

任意の $pm \in (p)$ $(m \in \mathbb{Z})$ に対し，$(pm)^3 \in (p^3)$ であるから，$\sqrt{(p^3)} \supset (p)$ である。
また，任意の $x \in \sqrt{(p^3)}$ に対し，ある $k \in \mathbb{Z}$ が存在して，$x^k \in (p^3)$ となるが，
このとき $p^3 \mid x^k$ であり p が素数であることから，$p \mid x$ である。したがって，$x \in (p)$ であり，$\sqrt{(p^3)} \subset (p)$ である。以上から，$\sqrt{(p^3)} = (p)$