Contents

1

1.1

(1)

1. $\forall A = (a_{ij}), B = (b_{ij}), C = (c_{ij}) \in M_n(\mathbb{R}), (A+B)+C = (a_{ij}+b_{ij})+(c_{ij}) = a_{ij}+(b_{ij}+c_{ij}) = A+(B+C)$
2. $\forall A \in M_n(\mathbb{R}), A+0 = 0+A = A$
3. $\forall A = (a_{ij}) \in M_n(\mathbb{R}), (a_{ij})+(-a_{ij}) = 0$ から逆元も存在
4. $\forall A, B \in M_n(\mathbb{R}), A+B = (a_{ij}+b_{ij}) = (b_{ij}+a_{ij}) = B+A$
5. $\forall A \in M_n(\mathbb{R}), AE = EA = A$
6. $\forall A, B, C \in M_n(\mathbb{R}), A(B+C) = \sum_{k=1}^{n} a_{ik}b_{kj} + \sum_{k=1}^{n} a_{ik}c_{kj} = AB+BC$
   $(A+B)C = \sum_{k=1}^{n} a_{ik}c_{kj} + \sum_{k=1}^{n} b_{ik}c_{kj} = AC+BC$
7. $\forall A, B, C \in M_n(\mathbb{R}), (AB)C = \sum_{k=1}^{n}\left(\sum_{l=1}^{n} a_{il}b_{lk}\right)c_{kj} = \sum_{l=1}^{n} a_{il}\left(\sum_{k=1}^{n} b_{lk}c_{kj}\right) = A(BC)$

(2)

$\forall A, B \in M_n(\mathbb{R}), AB \neq BA$ から，$M_n(\mathbb{R})$ は可換環ではない

1.2

1. $\forall f, g, h, ((f+g)+h)(x) = (f+g)(x)+h(x) = f(x)+g(x)+h(x) = f(x)+(g+h)(x) = (f+(g+h))(x)$
2. $\forall f, (f+0)(x) = f(x) = (0+f)(x)$
3. $\forall f, (f-f)(x) = 0 = (-f+f)(x)$
4. $\forall f, g, (f+g)(x) = f(x)+g(x) = g(x)+f(x) = (g+f)(x)$
5. $\forall f, (f1)(x) = f(x) = (1f)(x)$
6. $\forall f, g, h, (f(g+h))(x) = f(x)(g+h)(x) = (fg)(x)+(fh)(x)$
   $((f+g)h)(x) = (f+g)(x)h(x) = (fh)(x)+(gh)(x)$
7. $\forall f, g, h, ((fg)h)(x) = f(x)g(x)h(x) = (f(gh))(x)$

1.3

$M_n(\mathbb{R})$ は可換環ではないから，体ではない
$\forall \mathbb{Z} \ni a \neq \pm 1, \frac{1}{a} \notin \mathbb{Z}$ から，体ではない
$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ は体である

1.4

$\mathbb{Q}\left[\sqrt{2}\right]$ は可換環であるから，$\forall\left(a+b\sqrt{2}\right)\in\mathbb{Q}\left[\sqrt{2}\right]\setminus\{0\},\left(a+b\sqrt{2}\right)$ は可逆元であることを示せばいい

$a+b\sqrt{2}\neq 0$ から $\dfrac{1}{a+b\sqrt{2}}=\dfrac{a-b\sqrt{2}}{a^2-2b^2}=\dfrac{a}{a^2-2b^2}-\dfrac{b}{a^2-2b^2}\sqrt{2}$ で，$\dfrac{a}{a^2-2b^2},-\dfrac{b}{a^2-2b^2}\in\mathbb{Q}$ から，$\dfrac{1}{a+b\sqrt{2}}\in\mathbb{Q}\left[\sqrt{2}\right]$ かつ $\left(a+b\sqrt{2}\right)\dfrac{1}{a+b\sqrt{2}}=\dfrac{1}{a+b\sqrt{2}}\left(a+b\sqrt{2}\right)=1$

よって，$\mathbb{Q}\left[\sqrt{2}\right]$ は体である

2

2.1

(1)

$R=\mathbb{Z}\left[\sqrt{2}\right]=\left\{a+b\sqrt{2}:a,b\in\mathbb{Z}\right\}$ と定義するから，$a+b\sqrt{2},c+d\sqrt{2}\in R$ に対して

$$\left(a+b\sqrt{2}\right)+\left(c+d\sqrt{2}\right)=(a+c)+(b+d)\sqrt{2}\in R \tag{1}$$

$$\left(a+b\sqrt{2}\right)\left(c+d\sqrt{2}\right)=(ac+2bd)+(ad+bc)\sqrt{2}\in R \tag{2}$$

$\mathbb{Z}$ の単位元は 1 であるから，$1=1+0\sqrt{2}\in R$ は R の単位元である．以上より，R は $\mathbb{R}$ の部分環である

(2)

$\forall a+b\sqrt{2},c+d\sqrt{2}\in R$ に対し，$\left(a+b\sqrt{2}\right)\left(c+d\sqrt{2}\right)=0$ と仮定すると
$(ac+2bd)+(ad+bc)\sqrt{2}=0$ となり，$\begin{cases}ac+2bd=0\\ad+bc=0\end{cases}$
すると，$a+b\sqrt{2}\neq 0$ なら，$c+d\sqrt{2}=0$ から，R の零因子は 0 のみである．よって，R は整域である

2.2

$\forall\overline{i},\overline{j}\in\mathbb{Z}/n\mathbb{Z},\overline{i}\cdot\overline{j}=(i+m\mathbb{Z})(j+n\mathbb{Z})=ij+(in+mj+mn)\mathbb{Z}=\overline{ij}$
また，$\overline{j}\cdot\overline{i}=(j+n\mathbb{Z})(i+m\mathbb{Z})=ji+(jm+ni+mn)\mathbb{Z}=\overline{ji}$
よって，$\overline{i}\cdot\overline{j}=\overline{j}\cdot\overline{i}$ が成り立つから，可換環である．
また，$\mathbb{Z}/6\mathbb{Z}$ に対して，$\overline{2},\overline{3}\in\mathbb{Z}/6\mathbb{Z}$ で，$\overline{2}\cdot\overline{3}=\overline{6}=\overline{0}$ となるから，$\overline{2},\overline{3}$ は零因子である．よって，整域ではない

2.3

(1)

$u\in R$ が単元であるから，$\exists v\in R,s.t.uv=1$ が成り立ち，R が可換環であるより，$vu=1$ である．よって，$uv=vu=1$
u を零因子とすると，$\exists v'\in R,s.t.uv'=0$ が成り立つ．また，R が可換環であるから，$v'u=0$ である．よって，$uv'=v'u=0$ が成り立つ．$v'\in R\backslash\{0\}$ だから，$u=0$ である．これは単元の定義に反する．よって，u は零因子ではない

(2)

R を体とすると，R の任意の非零元は単元であり，(1) より零因子ではない．よって，R は整域である

(3)

R は整域であるから，任意の非零元は零因子ではない．$\forall a,b\in R,0\neq c\in R,ac=bc$ なら両辺に c の逆元 c^{-1} をかけて，$a=acc^{-1}=bcc^{-1}=b$ が成り立つ．よって，$a=b$ で，簡約律が成り立つ

2.4

$\overline{1} \in R$ を $f(x) = x^4 + \overline{3}x^3 + \overline{2}x + \overline{4}$ に代入すると，$f\left(\overline{1}\right) = \overline{1} + \overline{3} + \overline{2} + \overline{4} = \overline{10} = \overline{0}$ であるから，$\overline{1}$ は根であり，$\left(x - \overline{1}\right)$ は $f(x)$ の因子である．簡約すると，$f(x) = \left(x - \overline{1}\right)\left(x^3 + \overline{4}x^2 + \overline{4}x + \overline{1}\right)$ となる，$\overline{1}$ を $x^3 + \overline{4}x^2 + \overline{4}x + \overline{1}$ に代入すると，$\overline{0}$ になるから，$f(x) = \left(x - \overline{1}\right)^2\left(x^2 + \overline{4}\right)$．また，$\overline{4} = \overline{-1}$ から，$f(x) = \left(x - \overline{1}\right)^3\left(x + \overline{1}\right)$

2.5

R が整域であるから，R の任意の非零元は零因子ではない．$R[x]^\times$ は多項式環 $R[x]$ の単元全体の集合であるから，$\forall u(x), v(x) \in R[x]^\times, u(x)v(x) = v(x)u(x) = 1$
$0 = \deg 1 = \deg(u(x)v(x)) = \deg(u(x)) + \deg(v(x))$ かつ $\deg(u(x)), \deg(v(x)) \geq 0$ であるから，$\deg(u(x)) = \deg(v(x)) = 0$ である．だから，$u(x), v(x)$ は定数多項式で，$u(x) := a_0, v(x) := b_0$ とおくと，$a_0, b_0 \in R$. また，$u(x), v(x)$ は単元であるから，$a_0b_0 = b_0a_0 = 1$ で，a_0, b_0 も R の単元である．a_0, b_0 の任意性より，$R[x]^\times = R^\times$

2.6

(1)

$R = \mathbb{Z}/2\mathbb{Z}$ は $\overline{0}$ と $\overline{1}$ だけであるから，それぞれ代入すると $\begin{cases} f^*\left(\overline{0}\right) = \overline{0}^2 + \overline{0} \\ f^*\left(\overline{1}\right) = \overline{1}^2 + \overline{1} = \overline{0} \end{cases}$ から，$\forall a \in R, f(a) = 0$ である

(2)

$h(x) := f(x) - g(x) \in R[x]$ とする．$f(x) \neq g(x)$ であるから，$h(x) \neq 0$．また，零でない多項式 h は $\deg h$ 以下個の根しか存在しないから，$\deg h = d$ とすると，$h(x) = 0$ となる x は高々 d 個である．R は無限集合であるから，$\exists a \in R, s.t. h(a) \neq 0$ である．よって，$h^* \neq 0$ で，$f^* \neq g^*$ である

3

3.1

$a+n\mathbb{Z}=a'+n\mathbb{Z}$ かつ $b+n\mathbb{Z}=b'+n\mathbb{Z}$ と仮定すると，$a=a'+nk, b=b'+nl, (k,l\in\mathbb{Z})$ であり，$ab=(a'+nk)(b'+nl)=a'b'+(a'nl+b'nk)+kln^2$ であるから，$ab-a'b'=(a'nl+b'nk)+kln^2=n(a'l+b'k+kln)$ となり，$n\mid(ab-a'b')$ となる．よって，$ab\equiv a'b' \pmod n$ で，$ab+n\mathbb{Z}=a'b'+n\mathbb{Z}$．したがって，$(a+n\mathbb{Z})(b+n\mathbb{Z})=ab+n\mathbb{Z}$．よって，well-defined である

3.2

(1)

$\overline{1}:\overline{1}\cdot\overline{1}=\overline{1}, \forall\overline{k}\in\mathbb{Z}/12\mathbb{Z}, \overline{1}\cdot\overline{k}\neq\overline{0}$ から，逆元は $\overline{1}$ で，零因子ではない
$\overline{2}:2\mid 12$ であるから，逆元は存在しないが，$\overline{2}\cdot\overline{6}=\overline{12}=\overline{0}$ となるから，$\overline{2}$ は零因子である
$\overline{3}:3\mid 12$ であるから，逆元は存在しないが，$\overline{3}\cdot\overline{4}=\overline{12}=\overline{0}$ となるから，$\overline{3}$ は零因子である
$\overline{4}:4\mid 12$ であるから，逆元は存在しないが，$\overline{4}\cdot\overline{3}=\overline{12}=\overline{0}$ となるから，$\overline{4}$ は零因子である
$\overline{5}:\overline{5}\cdot\overline{5}=\overline{25}=\overline{1}$ から，逆元は $\overline{5}$ で，零因子ではない
$\overline{6}:6\mid 12$ であるから，逆元は存在しないが，$\overline{6}\cdot\overline{2}=\overline{12}=\overline{0}$ となるから，$\overline{6}$ は零因子である
$\overline{7}:\overline{7}\cdot\overline{7}=\overline{49}=\overline{1}$ から，逆元は $\overline{7}$ で，零因子ではない
$\overline{8}:4\mid 12$ であるから，逆元は存在しないが，$\overline{8}\cdot\overline{3}=\overline{24}=\overline{0}$ となるから，$\overline{8}$ は零因子である
$\overline{9}:3\mid 12$ であるから，逆元は存在しないが，$\overline{9}\cdot\overline{4}=\overline{36}=\overline{0}$ となるから，$\overline{9}$ は零因子である
$\overline{10}:2\mid 12$ であるから，逆元は存在しないが，$\overline{10}\cdot\overline{6}=\overline{60}=\overline{0}$ となるから，$\overline{10}$ は零因子である
$\overline{11}:\overline{11}\cdot\overline{11}=\overline{121}=\overline{1}$ から，逆元は $\overline{11}$ で，零因子ではない

(2)

$\overline{3}\cdot\overline{x}=\overline{0}$ であるから，$3x=12k, k\in\mathbb{Z}$．また，$0\leq x<12$ であるから，$x=0,4,8$

3.3

$\overline{33}\cdot\overline{a}=\overline{1}$ とすると，$33a=124b+1$ である．拡張ユークリッドの互除法により

$$\begin{pmatrix}1&0&33\\0&1&124\end{pmatrix}\to\begin{pmatrix}1&0&33\\-3&1&25\end{pmatrix} \tag{3}$$

$$\to\begin{pmatrix}-3&1&25\\4&-1&8\end{pmatrix} \tag{4}$$

$$\to\begin{pmatrix}4&-1&8\\-15&4&1\end{pmatrix} \tag{5}$$

よって，$a=-15$ であり，$\overline{a}=\overline{-15}=\overline{124-15}=\overline{109}$ である

3.4

単元は $\mathbb{Z}/n\mathbb{Z}$ の n と互いに素な剰余類であるから,$\phi(24)=8$ より,単元は $\{\overline{1},\overline{5},\overline{7},\overline{11},\overline{13},\overline{17},\overline{19},\overline{23}\}$ である

3.5

(1)

n が素数であるとき，$\forall k \in \mathbb{Z}/n\mathbb{Z}, \gcd(k,n) = 1$ で，整域になる
自分自身が逆元になる $\iff \forall \overline{a} \in \mathbb{Z}/n\mathbb{Z}, \overline{a}^2 = \overline{1} \iff \overline{a}^2 - \overline{1} = 0 \iff \left(\overline{a} - \overline{1}\right)\left(\overline{a} + \overline{1}\right) = 0$
よって，$\begin{cases} \overline{a} - \overline{1} = 0 \\ \overline{a} + \overline{1} = 0 \end{cases} \implies \overline{a} = \overline{1}$ または $\overline{n-1}$ である

(2)

n は素数でないとき，$\mathbb{Z}/n\mathbb{Z}$ は必ず整域となるとは限らないから，$\overline{0}$ 以外の零因子が存在する．
例として，$n = 6$ で，$\overline{2} \cdot \overline{3} = \overline{0}$ である．よって，$\overline{2}, \overline{3}$ は自分自身が逆元ではない

3.6

(1)

f_a は単射で，R は有限個の元を持つから，全射でもある．よって，f_a は全単射である．よって $\exists x \in R, s.t. f_a(x) = 1$ となる．言い換えれば，$ax = 1$ で，$x = a^{-1}$ は a の逆元である．なお，R は可換環であるので，$xa = 1$ も成り立つ．よって，a は単元である

(2)

零元自体は零因子であるから，以下は $a \in R \backslash \{0\}$ を考える．a が零因子でないと仮定すると，$ax = ay \implies a(x-y) = 0 \implies x - y = 0 \implies x = y$ となるから，f_a は単射である
逆に a が単元でないなら，$f_a = ax = 1$ の解は存在しないから，f_a は全射でない．また，R は有限集合であるから，単射でもない．よって，$x \neq y$ で，$ax = ay$ より，a は零因子である

3.7

(1)

R は整域で，$a \neq 0$ であるから，$\exists a^{-1}, s.t. aa^{-1} = a^{-1}a = 1$ が成り立つ．$f_a(x) = f_a(x)$ とすると，$ax = ay$ となり，$a(x-y) = 0$ となる．R は整域なので，a は零因子ではないから，$x = y$.
よって，$f_a(x)$ は単射である

(2)

R は整域なので，$\forall a \in R \backslash \{0\}, a$ は零因子ではない．また，(1) より f_a は単射であり，R は有限集合であるから，f_a は全単射である．よって $\forall a \in R \backslash \{0\}, \exists x \in R, s.t. f_a(x) = ax = 1$ で，$x = a^{-1}$ は a の逆元である．よって，R は体である

4

4.1

$\forall \overline{a}, \overline{b} \in n\mathbb{Z}, \overline{a} + \overline{b} = \overline{a+b} \in n\mathbb{Z}$
$\forall \overline{a} \in n\mathbb{Z}, k \in \mathbb{Z}, k\overline{a} = \overline{ka} \in n\mathbb{Z}, \overline{a}k = \overline{ak} \in n\mathbb{Z}$ から，$n\mathbb{Z}$ は $\mathbb{Z}$ の両側イデアルである

4.2

$\forall \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{R}), \forall \begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix}, \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix} = \begin{bmatrix} ax & 0 \\ cx & 0 \end{bmatrix} \in I$ で
$\forall \begin{bmatrix} x_1 & 0 \\ y_1 & 0 \end{bmatrix}, \begin{bmatrix} x_2 & 0 \\ y_2 & 0 \end{bmatrix} \in I, \begin{bmatrix} x_1 & 0 \\ y_1 & 0 \end{bmatrix} \begin{bmatrix} x_2 & 0 \\ y_2 & 0 \end{bmatrix} = \begin{bmatrix} x_1x_2 & 0 \\ y_1x_2 & 0 \end{bmatrix} \in I$
よって，I は $M_2(\mathbb{R})$ の左イデアルである
$\forall \begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix} \in I, \forall \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in R, \begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} ax & bx \\ ay & by \end{bmatrix}$ であるから，bx, by 必ず 0 になることは限らない．よって，I は $M_2(\mathbb{R})$ の右イデアルではない

4.3

$I = 10\mathbb{Z}, J = 15\mathbb{Z}$ であるから，$I \cap J = \{x \in \mathbb{Z} : x \in 10\mathbb{Z}, x \in 15\mathbb{Z}\} = \{x \in \mathbb{Z} : 10 \mid x, 15 \mid x\} = \{x \in \mathbb{Z} : 30 \mid x\} = 30\mathbb{Z}$ であるから，$d = 30$
$I + J = \{10a + 15b : a, b \in \mathbb{Z}\} = \{5(2a + 3b) : a, b \in \mathbb{Z}\} = 5\mathbb{Z}$ であるから，$d = 5$
$IJ = \{ab : 10 \mid a, 15 \mid b\} = \{150ab : a, b \in \mathbb{Z}\} = 150\mathbb{Z}$ であるから，$d = 150$

4.4

(1)

$1 \in I$ とすると，$\forall r \in R, r = r \cdot 1 \in I$（イデアルだから）よって，$R \subset I$ である．また，$I \subset R$ であるから，$I = R$ である
$I = R$ とすると，I は R のイデアルであるから，$1_R \in I$

(2)

単元 $u \in I$ とすると，$\exists u^{-1} \in R, s.t. uu^{-1} = u^{-1}u = 1_R$ が成り立つ．また，I はイデアルであるから，$u \in I, u^{-1} \in R$ に対して，$uu^{-1} = u^{-1}u = 1 \in I$．(1) より，$I = R$ である

(3)

a が単元であるとすると，$\exists a^{-1} \in R, s.t. aa^{-1} = a^{-1}a = 1_R$ が成り立つ．また，$1 = a^{-1}a = aa^{-1} \in (a)$ だから，(1) より，$(a) = R$
$(a) = R$ とすると，$1_R \in (a)$ であるから，$\exists r \in R, s.t. 1_R = ar = ra$ が成り立つ．よって，a は単元である

4.5

$\forall r_1, r_2 \in A_R(I), \forall x \in I, r_1x = r_2x = 0 \Longrightarrow (r_1 - r_2)x = 0 \Longrightarrow r_1 - r_2 \in A_R(I)$
$\forall a \in R, \forall r \in A_R(I), (ar)x = a(rx) = 0 \Longrightarrow ar \in A_R(I)$
$\forall b \in R, \forall r' \in A_R(I), (r'b)x = r'(bx)$ で，I は R の左イデアルであるから，$bx = 0$．よって $r'(bx) = 0$ で，$r'b \in A_R(I)$ である
以上より，$A_R(I)$ は R の両側イデアルである

4.6

(1)

$I = (\overline{3}) = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$ だから，R/I の代表元は $[\overline{0}], [\overline{1}], [\overline{2}]$ である

(2)

加法表：

$$\begin{cases} [\overline{0}] + [\overline{0}] = [\overline{0}] \\ [\overline{0}] + [\overline{1}] = [\overline{1}] \\ [\overline{0}] + [\overline{2}] = [\overline{2}] \end{cases}, \begin{cases} [\overline{1}] + [\overline{0}] = [\overline{1}] \\ [\overline{1}] + [\overline{1}] = [\overline{2}] \\ [\overline{1}] + [\overline{2}] = [\overline{0}] \end{cases}, \begin{cases} [\overline{2}] + [\overline{0}] = [\overline{2}] \\ [\overline{2}] + [\overline{1}] = [\overline{0}] \\ [\overline{2}] + [\overline{2}] = [\overline{1}] \end{cases}$$

乗法表：

$$\begin{cases} [\overline{0}] \cdot [\overline{0}] = [\overline{0}] \\ [\overline{0}] \cdot [\overline{1}] = [\overline{0}] \\ [\overline{0}] \cdot [\overline{2}] = [\overline{0}] \end{cases}, \begin{cases} [\overline{1}] \cdot [\overline{0}] = [\overline{0}] \\ [\overline{1}] \cdot [\overline{1}] = [\overline{1}] \\ [\overline{1}] \cdot [\overline{2}] = [\overline{2}] \end{cases}, \begin{cases} [\overline{2}] \cdot [\overline{0}] = [\overline{0}] \\ [\overline{2}] \cdot [\overline{1}] = [\overline{2}] \\ [\overline{2}] \cdot [\overline{2}] = [\overline{1}] \end{cases}$$

4.7

$x^2 \equiv -1$ であるから

$$\begin{aligned} \overline{3x^4 + 2x^3 + 4x^2 - 1} &= \overline{3\left(x^2\right)^2 + 2x\left(x^2\right) + 4x^2 - 1} && (6) \\ &= \overline{3 \cdot (-1)^2 + 2x \cdot (-1) + 4 \cdot (-1) - 1} && (7) \\ &= \overline{3 - 2x - 4 - 1} && (8) \\ &= \overline{-2x - 2} && (9) \end{aligned}$$

から，次数が一番小さい $f(x)$ は $-2x - 2$

5

5.1

(1)

$\forall a_i, b_i \in \mathbb{Q}, A = a_1 + b_1\sqrt{2}, B = a_2 + b_2\sqrt{2}$

$$\phi(A+B) = \phi\left(a_1 + b_1\sqrt{2} + a_2 + b_2\sqrt{2}\right) \tag{10}$$
$$= \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ 2(b_1 + b_2) & a_1 + a_2 \end{bmatrix} \tag{11}$$
$$\phi(A) + \phi(B) = \begin{bmatrix} a_1 & b_1 \\ 2b_1 & a_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ 2b_2 & a_2 \end{bmatrix} \tag{12}$$
$$= \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ 2(b_1 + b_2) & a_1 + a_2 \end{bmatrix} \tag{13}$$
$$\phi(AB) = \phi\left(a_1a_2 + 2b_1b_2 + (a_1b_2 + a_2b_1)\sqrt{2}\right) \tag{14}$$
$$= \begin{bmatrix} a_1a_2 + 2b_1b_2 & a_1b_2 + a_2b_1 \\ 2(a_1b_2 + a_2b_1) & a_1a_2 + 2b_1b_2 \end{bmatrix} \tag{15}$$
$$\phi(A)\phi(B) = \begin{bmatrix} a_1 & b_1 \\ 2b_1 & a_1 \end{bmatrix}\begin{bmatrix} a_2 & b_2 \\ 2b_2 & a_2 \end{bmatrix} \tag{16}$$
$$= \begin{bmatrix} a_1a_2 + 2b_1b_2 & a_1b_2 + a_2b_1 \\ 2(a_1b_2 + a_2b_1) & a_1a_2 + 2b_1b_2 \end{bmatrix} \tag{17}$$
$$\phi(1) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = 1_R \tag{18}$$

以上，ϕ は準同型である

(2)

$\forall \begin{bmatrix} a & b \\ 2b & a \end{bmatrix} \in R, a, b \in \mathbb{Q}$ であるから $q \in \mathbb{Q}\left[\sqrt{2}\right]$ により定義できるから，ϕ は前者である
$\begin{bmatrix} a & b \\ 2b & a \end{bmatrix} = \begin{bmatrix} a' & b' \\ 2b' & a' \end{bmatrix}$ の $(1,1)$ 成分と $(1,2)$ 成分を比較すると，$a = a', b = b'$ であるから，ϕ は単射である．よって，ϕ は同型である

5.2

(1)

$\phi\left(x^2 - 2\right) = \left(\sqrt{2}\right)^2 - 2 = 0$ から，$x^2 - 2 \in \mathrm{Ker}\phi \Longleftrightarrow \left(x^2 - 2\right) \subset \mathrm{Ker}\phi$
逆に，$\forall f(x) \in \mathbb{Q}[x]$ を取り，$f\left(\sqrt{2}\right) = 0$．また $\mathbb{Q}[x]$ は整域であるから，$\left(x^2 - 2\right)$ で割ると $f(x) = \left(x^2 - 2\right)q(x) + r(x)$ と表せる．$\deg r(x) < 2$ から，$f\left(\sqrt{2}\right) = s + t\sqrt{2}$ と表し，$s + t\sqrt{2} = 0$ であるから，$s = t = 0$. よって，$f(x) = \left(x^2 - 2\right)q(x)$,i.e. $f(x) \in \left(x^2 - 2\right)$ から $\mathrm{Ker}\phi \subset \left(x^2 - 2\right)$
以上，$\mathrm{Ker}\phi = \left(x^2 - 2\right)$

(2)

$\mathrm{Im}\phi = \mathbb{Q}\left[\sqrt{2}\right], \mathrm{Ker}\phi = \left(x^2 - 2\right)$ であるから，環の準同型定理より，$\mathbb{Q}[x]/\mathbb{Q}\left[\sqrt{2}\right]$

5.3

$\phi : \mathbb{Z} \to \mathbb{Z}$ を環準同型とすると，$\phi(1) = 1$ であり，$\phi(n) = ((n-1)+1) = \phi(n-1) + \phi(1) = \phi(n-1) + 1$ であるから，帰納的に，$\phi(n) = n$

5.4

$\psi : \mathbb{R} \to \mathbb{C}$ の環準同型が存在すると仮定すると，ψ は全単射で，$\mathrm{Ker}\psi = \{0\}$ である．すると，$0 = \psi(0) = \psi\left(1 + i^2\right) = \psi^2(i) + \psi(1) = \psi^2(i) + 1$．よって，$\psi^2(i) = -1$ で，$\psi(i) = \sqrt{-1} = i$ であるが，$i \notin \mathbb{R}$ より，この環準同型は存在しない

5.5

(1)

I は R の両側イデアルであるから，$\begin{cases} \forall a, b \in I, a + b \in I \\ \forall a \in I, r \in R, ra, ar \in I \end{cases}$

ϕ は環準同型であるから，$\begin{cases} \phi(I) \ni \phi(a+b) = \phi(a) + \phi(b) \\ \phi(I) \ni \phi(ra) = \phi(r)\phi(a) \\ \phi(I) \ni \phi(ar) = \phi(a)\phi(r) \end{cases}$

よって，$\phi(I)$ は R' の両側イデアルである

(2)

I' は R の両側イデアルであるから，$\begin{cases} \forall a', b' \in I', a' + b' \in I' \\ \forall a' \in I', r \in R', ra', a'r \in I' \end{cases}$

ϕ は環準同型であるから，$\begin{cases} \phi^{-1}(I') \ni \phi^{-1}(a'+b') = \phi^{-1}(a') + \phi^{-1}(b') \\ \phi^{-1}(I') \ni \phi^{-1}(ra') = \phi^{-1}(r)\phi^{-1}(a') \\ \phi^{-1}(I') \ni \phi^{-1}(a'r) = \phi^{-1}(a')\phi^{-1}(r) \end{cases}$

よって，$\phi^{-1}(I')$ は R の両側イデアルである

(3)

R の加法と乗法をそれぞれ $\oplus, \otimes$ とし，S は R の部分環であるから，$\forall s_1, s_2 \in S, s_1 \oplus s_2 \in S, s_1 \otimes s_2 \in S$ が成り立ち，$1_R \in S$ である．ϕ は環準同型であるから，$\phi(s_1 \oplus s_2) = \phi(s_1) \oplus' \phi(s_2), \phi(s_1 \otimes s_2) = \phi(s_1) \otimes' \phi(s_2)$ が成り立つ．また，$\phi(1_R) = 1_{R'}$ であるから，$\phi(S)$ は R' の部分環である

(4)

R' の加法と乗法をそれぞれ $\oplus', \otimes'$ とし，S' は R' の部分環であるから，$\forall s'_1, s'_2 \in S', s'_1 \oplus' s'_2 \in S', s'_1 \otimes' s'_2 \in S'$ が成り立ち，$1_{R'} \in S'$ である．ϕ は環準同型であるから，$\phi^{-1}(s'_1 \oplus' s'_2) = \phi^{-1}(s'_1) \oplus \phi^{-1}(s'_2), \phi^{-1}(s'_1 \otimes' s'_2) = \phi^{-1}(s'_1) \otimes \phi^{-1}(s'_2)$ が成り立つ．また，$\phi^{-1}(1_{R'}) = 1_R$ であるから，$\phi^{-1}(S')$ は R の部分環である

5.6

S は R の部分環であるから，$\begin{cases} \forall s_1, s_2 \in S, s_1 + s_2 \in S \\ \forall s_1, s_2 \in S, s_1 s_2 \in S \\ 1_R \in S \end{cases}$

また，I は R の両側イデアルであるから，$\begin{cases} \forall a, b \in I, a + b \in I \\ \forall a \in I, r \in R, ra, ar \in I \end{cases}$

$\forall p \in (S + I), q \in (S + I),$ $\begin{cases} p := a_1 + x_1 & a_1 \in S, x_1 \in I \\ q := a_2 + x_2 & a_2 \in S, x_2 \in I \end{cases}$ とする

$p + q = a_1 + x_1 + a_2 + x_2 = (a_1 + a_2) + (x_1 + x_2),$ $\begin{cases} a_1 + a_2 \in S \\ x_1 + x_2 \in I \end{cases} \implies p + q \in (S + I)$

$pq = (a_1 + x_1)(a_2 + x_2) = a_1 a_2 + a_1 x_2 + x_1 a_2 + x_1 x_2,$ $\begin{cases} a_1 a_2 \in S \\ a_1 x_2 \in I \\ x_1 a_2 \in I \\ x_1 x_2 \in I \end{cases} \implies pq \in (S + I)$

$1_R \in S \implies 1_R \in (S + I)$
以上より，$(S + I)$ は R の部分環である

6

6.1

(1)

$(a,b)+(c,d)=(a+c,b+d),(a,b)\cdot(c,d)=(ac,bd)$

(2)

$R=\left\{\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} : a,b\in\mathbb{Z}\right\}\subset M_2(\mathbb{R})$ とする

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}+\begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}=\begin{bmatrix} a+c & 0 \\ 0 & b+d \end{bmatrix} \tag{19}$$

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}\begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}=\begin{bmatrix} ac & 0 \\ 0 & bd \end{bmatrix} \tag{20}$$

また，$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\in R$ から R は $M_2(\mathbb{R})$ の部分環である

$\phi(a,b)=\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ で定めると

$$\phi((a,b)+(c,d))=\phi(a+c,b+d)=\begin{bmatrix} a+c & 0 \\ 0 & b+d \end{bmatrix}=\phi(a,b)+\phi(c,d) \tag{21}$$

$$\phi((a,b)\cdot(c,d))=\phi(ac,bd)=\begin{bmatrix} ac & 0 \\ 0 & bd \end{bmatrix}=\phi(a,b)\cdot\phi(c,d) \tag{22}$$

なお，$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ は (a,b) で唯一的に表せるから，ϕ は全射であり，$\phi(a,b)=\phi(a',b')$ とすると，$a=a',b=b'$ であるから，ϕ は単射である．よって，ϕ は全単射である．以上，$\mathbb{R}\times\mathbb{R}\cong R$

6.2

$180=2^2\cdot3^2\cdot5$ から，$\mathbb{Z}/180\mathbb{Z}\cong\mathbb{Z}/36\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$

6.3

(1)

$\begin{cases} x_1\equiv0 \pmod{5\mathbb{Z}} \\ x_1\equiv1 \pmod{7\mathbb{Z}} \end{cases}\Longrightarrow x_1=35k,k\in\mathbb{Z}$ とおき，$x_1\equiv1 \pmod{4\mathbb{Z}}$ から，$35k\equiv3k\equiv1 \pmod{4\mathbb{Z}}$ となる．よって，$k=3$ であり，$x_1=105$ である

$\begin{cases} x_2\equiv0 \pmod{4\mathbb{Z}} \\ x_2\equiv0 \pmod{7\mathbb{Z}} \end{cases}\Longrightarrow x_2=28l,l\in\mathbb{Z}$ とおき，$x_2\equiv1 \pmod{5\mathbb{Z}}$ から．$28l\equiv3l \pmod{5\mathbb{Z}}$ となる．よって，$l=2$ であり，$x_2=56$ である

$\begin{cases} x_3\equiv0 \pmod{4\mathbb{Z}} \\ x_3\equiv0 \pmod{5\mathbb{Z}} \end{cases}\Longrightarrow x_3=20m,m\in\mathbb{Z}$ とおき，$x_3\equiv1 \pmod{7\mathbb{Z}}$ から，$20m\equiv6m\equiv1 \pmod{7\mathbb{Z}}$ となる．よって，$m=6$ であり，$x_3=120$ である

(2)

$$x \equiv (x_1a_1 + x_2a_2 + x_3a_3) \equiv \begin{cases} x_1a_1 & (\mathrm{mod}\ 4\mathbb{Z}) \\ x_2a_2 & (\mathrm{mod}\ 5\mathbb{Z}) \\ x_3a_3 & (\mathrm{mod}\ 7\mathbb{Z}) \end{cases}$$

ここで $x_1 \equiv 1\ (\mathrm{mod}\ 4\mathbb{Z}), x_2 \equiv 1\ (\mathrm{mod}\ 5\mathbb{Z}), x_3 \equiv 1\ (\mathrm{mod}\ 7\mathbb{Z})$ であるから,$x \equiv \begin{cases} a_1 & (\mathrm{mod}\ 4\mathbb{Z}) \\ a_2 & (\mathrm{mod}\ 5\mathbb{Z}) \\ a_3 & (\mathrm{mod}\ 7\mathbb{Z}) \end{cases}$

(3)

$a_1 = 2, a_2 = 1, a_3 = 3$ のとき，$x = 2x_1 + x_2 + 3x_3$ であり，(1) より $x_1 = 105, x_2 = 56, x_3 = 120$ を代入すると
$x = 2 \cdots 105 + 56 + 3 \cdots 120 = 210 + 56 + 360 = 626 \equiv 66\ (\mathrm{mod}\ 140)$ から，$x = 66$

6.4

(1)

$I = \left(x^2\right), J = \left((1-x)^2\right)$ は $\mathbb{C}[x]$ のイデアルであるとき，$I = x^2\mathbb{C}[x], J = (1-x)^2\mathbb{C}[x]$ となるから，$IJ = \left\{x^2(1-x)^2 f(x) : f(x) \in \mathbb{C}[x]\right\} = \left(x^2(1-x)^2\right)$

(2)

$IJ = \left\{x^2(1-x)^2 f(x) : f(x) \in \mathbb{C}[x]\right\} = \left(x^2(1-x)^2\right) = I \cap J$ から，I と J が互いに素であればいい
$f(x), g(x) \in \mathbb{C}[x]$ とおき，$x^2 f(x) + (1-x)^2 g(x) = 1$ に対して，$x = 0$ のとき，$\forall f(x) \in \mathbb{C}[x], g(x) = 1$ とすれば解は常に存在する．同様に $x = 1$ のとき，$f(x) = 1, \forall g(x) \in \mathbb{C}[x]$ とすれば解は常に存在する．それ以外の場合，$x^2 \neq 0, (1-x)^2 \neq 0$ だから，$f(x) = \dfrac{1}{2x^2}, g(x) = \dfrac{1}{2(1-x)^2}$ とおけば，$x^2 f(x) + (1-x)^2 g(x) = 1$ は常に解があるので，I と J は互いに素である．よって，$\mathbb{C}[x] / \left(x^2(1-x)^2\right) \cong \mathbb{C}[x] / \left(x^2\right) \times \mathbb{C}[x] / \left((1-x)^2\right)$

7

7.1

(1)

$(\Longrightarrow)$
$n\mathbb{Z}$ が素イデアルとすると，$\mathbb{Z}/n\mathbb{Z}$ は整域である．したがって，n は素数または 0 である
$\mathbb{Z}/n\mathbb{Z}$ を整域とすると，$\forall a,b\in\mathbb{Z}/n\mathbb{Z},ab=0$ ならば，零因子は 0 のみである．もし n は素数でないと仮定すると，$\exists u,v\in\mathbb{Z},s.t.n=uv$ で，$\overline{u},\overline{v}\in\mathbb{Z}/n\mathbb{Z}$，$\overline{uv}=\overline{u}\overline{v}=\overline{0}$ から，共に零因子になるので，矛盾する
n は正の整数だから，$n\neq 0$ で，素数である
$(\Longleftarrow)$
n が素数であるとすると，$\mathbb{Z}/n\mathbb{Z}$ は聖域になるから，$n\mathbb{Z}$ は素イデアルである

(2)

$(\Longrightarrow)$
$n\mathbb{Z}$ を極大イデアルとすると，$\mathbb{Z}/n\mathbb{Z}$ が体になり，整域にもなる（なぜなら $n\mathbb{Z}\ni a,b\neq 0,ab=0$ で，両辺に左から a^{-1} をかけると，$b=0$ となり，零因子は 0 のみである）．すると $n\mathbb{Z}$ は素イデアルである
$(\Longleftarrow)$
$n\mathbb{Z}$ が素イデアルであると仮定すると，$\mathbb{Z}/n\mathbb{Z}$ は整域である．また，(1) より，n は素数であるから，$\mathbb{Z}/n\mathbb{Z}$ は体になる．よって，$n\mathbb{Z}$ は極大イデアルである

(3)

$0\mathbb{Z}=\{0\}$ に対して，$\forall z\in\mathbb{Z},0z=z0=0\in 0\mathbb{Z}$ であるから，イデアルである．また，$\forall a,b\in\mathbb{Z},ab\in 0\mathbb{Z}$ とすると，$ab=0$ で，少なくとも一方が 0 であるから，a または b は $0\mathbb{Z}$ に属している．よって，$0\mathbb{Z}$ は素イデアルである

7.2

(1)

$\mathbb{R}[x]\ni f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$ に対して，$\phi(f(x))=f(0)=a_0$ をみたす写像 ϕ を考える．$\forall f,g\in\mathbb{R}[x],\phi(f(x)+g(x))=f(0)+g(0)=\phi(f(x))+\phi(g(x)),\phi(f(x)g(x))=f(0)g(0)=\phi(f(x))\phi(g(x))$ ので，ϕ は環準同型である
$\mathrm{Ker}\phi=\{f(x)\in\mathbb{R}[x]:\phi(f(x))=0\}=\{f(x)\in\mathbb{R}[x]:f(0)=0\}$ だから，$a_0=0$ で，$f(x)=a_1x+a_2x^2+\cdots+a_nx^n\ni(x)$ で，$\mathrm{Ker}\phi=(x)$．また，$\mathrm{Im}\phi=\{\phi(f(x)):f(x)\in\mathbb{R}[x]\}$ から，$\phi(f(x))=f(0)=a_0$ より，$\mathrm{Im}\phi=\mathbb{R}$
以上，準同型定理より，$\mathbb{R}/(x)\cong\mathbb{R}$ であるから，体である．よって，(x) は極大イデアルである

(2)

$\left(x^2-1\right)$ が極大イデアルであることと仮定すると，$\left(x^2-1\right)$ を含むイデアルは $\left(x^2-1\right)$ と $\mathbb{R}[x]$ しかないが，$x^2-1=(x-1)(x+1)$ であるから，$(x-1)\ni f(x)\not\ni\left(x^2-1\right)$ を満たす $f(x)$ が存在するから，$\left(x^2-1\right)\subsetneq(x-1)$ で，$(x-1)$ も $\mathbb{R}[x]$ のイデアルだから，$\left(x^2-1\right)$ の極大と矛盾する．よって，$\left(x^2-1\right)$ は極大イデアルでない

(3)

(1) と同様に,写像 $\psi : \mathbb{R}[x] \to \mathbb{R}[i]$ を $\psi(f(x)) = f(i)$ と定める.$\forall f, g \in \mathbb{R}[x], \psi(f(x) + g(x)) = f(i) + g(i) = \psi(f(x))\psi(g(x))$ から，ψ は準同型である
$\mathrm{Ker}\psi = \{f(x) \in \mathbb{R}[x] : \psi(f(x)) = 0\} = \{f(x) \in \mathbb{R}[x] : f(i) = 0\} = \left(x^2 - 1\right)$ で，$\mathrm{Im}\psi = \{\psi(f(x)) \in \mathbb{R}[i] : f(x) \in \mathbb{R}[x]\} = \{f(i) : f(x) \in \mathbb{R}[x]\} = \mathbb{R}[i] = \mathbb{C}$ であるから，準同型定理より，$\mathbb{R}[x] / \left(x^2 + 1\right) \cong \mathbb{C}$ であり，$\mathbb{C}$ は体であるから，$\mathbb{R}[x] / \left(x^2 - 1\right)$ も体となり，$\left(x^2 + 1\right)$ は極大イデアルである

7.3

(1)

(x) は $\mathbf{Z}[x]$ の素イデアル $\iff$ $\mathbb{Z}[x] / (x)$ は整域であるから，写像 $\phi : \mathbb{Z}[x] \to \mathbb{Z}$ を $\phi(f(x)) = f(0) = a_0$ とすると，$\forall f, g \in \mathbb{Z}[x], \phi(f(x) + g(x)) = \phi(a_0 + b_0 + (a_1 + b_1)x + \cdots) = a_0 + b_0 = f(0) + g(0) = \phi(f(x)) + \phi(g(x))$ であり，$\phi(f(x)g(x)) = \phi(a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots) = a_0b_0 = \phi(f(x))\phi(g(x))$ から，ϕ は準同型である
$\mathrm{Ker}\phi = \{f(x) \in \mathbb{Z}[x] : \phi(f(x)) = 0\} = \{f(x) \in \mathbb{Z}[x] : f(0) = 0\}$ だから，$a_0 = 0$ で，$f(x) = a_1x + a_2x^2 + \cdots + a_nx^n \ni (x)$ から，$\mathrm{Ker}\phi = (x)$．また，$\mathrm{Im}\phi = \{\phi(f(x)) : f(x) \in \mathbb{Z}[x]\} = \{a_0 \in \mathbb{Z} : f(x) \in \mathbb{Z}[x]\} = \mathbb{Z}$ であるから，準同型定理より，$\mathbb{Z}[x] / (x) \cong \mathbb{Z}$ から，$\mathbb{Z}[x] / (x)$ は整域である．よって，(x) は素イデアルである
なお，$\mathbb{Z}$ は体ではないから，$\mathbb{Z}[x] / (x)$ も体ではない．よって，(x) は極大イデアルではない

(2)

$(2, x) = \{g(x) \cdot 2 + h(x) \cdot x : g(x), h(x) \in \mathbb{Z}[x]\}$ とする.$\forall f(x) \in (2, x), f(x) = g(x) \cdot 2 + h(x) \cdot x$ で,$x = 0$ を代入すると,$f(0) = 2g(0)$ となる.$g(0) \in \mathbb{Z}$ だから,$f(0) \in 2\mathbb{Z}$.逆に,$f(0) \in 2\mathbb{Z}$ とすると,$\forall k \in \mathbb{Z}, f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + 2k = \left(a_nx^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1\right)x + 2k$ とかけるから,$g(x) = k, h(x) = a_nx^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1$ とすれば,$f(x) = g(x) \cdot 2 + h(x) \cdot x$ となり，$f(x) \in (2, x)$
また，$\forall f(x) \in (x), f(0) = 0 \in 2\mathbb{Z} \implies f(x) \in (2, x)$ であり，$g(x) = k \in \mathbb{Z}$ とすれば，$2g(x) + xh(x) = a_nx^n + \cdots + a_1x + 2k$ であるから，$2g(x) + xh(x) \notin (x)$ になる．$(x) \subsetneq (2, x)$
$\forall f(x) \in (2, x), f(x) = 2g(x) + xh(x) = a_nx^n + \cdots + a_1x + 2k$ であるから，$f(x) \in \mathbb{Z}[x]$ が，$f'(x) = a_nx^n + \cdots + a_1x + 2k + 1$ とすれば，$\mathbb{Z}[x] \ni f'(x) \notin (2, x)$．よって，$(2, x) \subsetneq \mathbb{Z}[x]$

(3)

$(2, x)$ は極大イデアル $\iff$ $\mathbb{Z}[x] / (2, x)$ は体であるから，写像 $\psi : \mathbb{Z}[x] \to \mathbb{Z}/2\mathbb{Z}$ を $\psi(f(x)) := \overline{f(0)} = \begin{cases} 0 & f(0) \equiv 0 \pmod 2 \\ 1 & f(0) \equiv 1 \pmod 2 \end{cases}$ と定める．すると，$\forall f, g \in \mathbb{Z}[x]$

$$\begin{aligned}
\psi(f(x) + g(x)) &= \psi(a_nx^n + \cdots + a_1x + a_0 + b_mx^m + \cdots + b_1x + b_0) && (23)\\
&= \overline{a_0 + b_0} = \overline{a_0} + \overline{b_0} && (24)\\
&= \psi(f(x)) + \psi(g(x)) && (25)\\
\psi(f(x)g(x)) &= \psi((a_nx^n + \cdots + a_1x + a_0)(b_mx^m + \cdots + b_1x + b_0)) && (26)\\
&= \overline{a_0b_0} = \overline{a_0} \cdot \overline{b_0} && (27)\\
&= \psi(f(x))\psi(g(x)) && (28)
\end{aligned}$$

であるから，ψ は準同型である

$$\begin{aligned}
\mathrm{Ker}\psi &= \left\{f(x) \in \mathbb{Z}[x] : \psi(f(x)) = \overline{0}\right\} && (29)\\
&= \left\{f(x) = 2\left(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n\right) + x\left(b_0 + b_1x + b_2x^2 + \cdots + b_mx^m\right)\right\} && (30)\\
&= (2, x) && (31)\\
\mathrm{Im}\psi &= \{\psi(f(x)) : f(x) \in \mathbb{Z}[x]\} && (32)\\
&= \left\{\overline{0}, \overline{1}\right\} = \mathbb{Z}/2\mathbb{Z} && (33)
\end{aligned}$$

から，準同型定理より，$\mathbb{Z}[x]/(2, x) \cong \mathbb{Z}/2\mathbb{Z}$ で，$\mathbb{Z}/2\mathbb{Z}$ は体であるから，$\mathbb{Z}[x]/(2, x)$ も体で，$(2, x)$ は極大イデアルである

7.4

(1)

$$\begin{aligned}
I &= \left(2, \sqrt{10}\right) && (34)\\
&= \left\{2\left(a + b\sqrt{10}\right) + \sqrt{10}\left(c + d\sqrt{10}\right) : a, b, c, d \in \mathbb{Z}\right\} && (35)\\
&= \left\{2(a + 5d) + \sqrt{10}(2b + c) : a, b, c, d \in \mathbb{Z}\right\} && (36)\\
&= \left\{2a + b\sqrt{10} : a, b \in \mathbb{Z}\right\} && (37)
\end{aligned}$$

(2)

I が素イデアル $\iff$ R/I が整域であるから

写像 $\phi : R \to \mathbb{Z}/2\mathbb{Z}$ を $\phi\left(a + b\sqrt{10}\right) = \begin{cases} \overline{0} & a \equiv 0 \pmod 2 \\ \overline{1} & a \equiv 1 \pmod 2 \end{cases}$ と定める．すると $\forall a, b, c, d \in \mathbb{Z}$

$$\begin{aligned}
\phi\left(\left(a + b\sqrt{10}\right) + \left(c + d\sqrt{10}\right)\right) &= \phi\left((a + c) + (b + d)\sqrt{10}\right) && (38)\\
&= \overline{a + c} = \overline{a} + \overline{c} && (39)\\
&= \phi\left(a + b\sqrt{10}\right) + \phi\left(c + d\sqrt{10}\right) && (40)\\
\phi\left(\left(a + b\sqrt{10}\right)\left(c + d\sqrt{10}\right)\right) &= \phi\left((ac + 10bd) + (ad + bc)\sqrt{10}\right) && (41)\\
&= \overline{ac + 10bd} = \overline{a} \cdot \overline{c} \qquad 10bd \equiv 0 \pmod 2 && (42)\\
&= \phi\left(a + b\sqrt{10}\right)\phi\left(c + d\sqrt{10}\right) && (43)
\end{aligned}$$

よって，ϕ は準同型である

$$\begin{aligned}
\mathrm{Ker}\phi &= \left\{a + b\sqrt{10} \in R : \phi\left(a + b\sqrt{10}\right) = \overline{0}\right\} && (44)\\
&= \left\{a + b\sqrt{10} \in R : a \equiv 0 \pmod 2\right\} && (45)\\
&= \left\{2k + b\sqrt{10} : k, b \in \mathbb{Z}\right\} = I && (46)\\
\mathrm{Im}\phi &= \left\{\phi\left(a + b\sqrt{10}\right) : a, b \in \mathbb{Z}\right\} && (47)\\
&= \left\{\overline{0}, \overline{1}\right\} = \mathbb{Z}/2\mathbb{Z} && (48)
\end{aligned}$$

から，準同型より，$R/I \cong \mathbb{Z}/2\mathbb{Z}$ である．$\mathbb{Z}/2\mathbb{Z}$ は整域であるから，R/I も整域であり，I は素イデアルである

7.5

$I \cap J$ は素イデアルではない $\iff \forall a, b \in R, (ab \in I \cap J \Longrightarrow a \in I \cap J \vee b \in I \cap J)$ で，対偶から考えると，$\exists a, b \in R, s.t. (a \notin I \cap J \wedge b \notin I \cap J \Longrightarrow ab \in I \cap J)$ を証明すればいい
I, J はイデアルであるから，$a \in I$ に対して，$\forall b \in R, ab \in I$．同様に，$b \in J, ab \in J$．よって，$ab \in I \cap J$．ここで，$I \nsubseteq J$ かつ $J \nsubseteq I$ であるから，$a \in I \setminus (I \cap J), b \in J \setminus (I \cap J)$ が存在する．
よって，$I \cap J$ は素イデアルではない

8

8.1

(1)

$b|a$ とすると，$\exists c \in R, s.t. a = bc$ であるから，$(a) \ni x = ra = rbc = (rc)\, b$ であるから，$(a) \subseteq (b)$.
逆に $(a) \subseteq (b)$ とすると，$a \in (a) \subseteq (b) \Longrightarrow a \in \{tb : t \in R\}$ となるから，$\exists t \in R, s, t. a = bt$ で，$b|a$ である．以上，$b|a \iff (a) \subseteq (b)$

(2)

$a \approx b$ とすると，$\exists u \in R^{\times}, s.t. a = bu$ で，$b|a$. また，R は整域であるから，$\exists u^{-1} \in R^{\times}, s.t. u^{-1}u = uu^{-1} = 1$
$a = bu$ の両辺に右から u^{-1} をかけると，$au^{-1} = b$ だから，$a|b$
(1) より，$(a) \subseteq (b)$ かつ $(b) \subseteq (a)$ で，$(a) = (b)$
逆に，$(a) = (b)$ とすると，$(a) \subseteq (b)$ かつ $(b) \subseteq (a)$ で，(1) より，$b|a$ かつ $a|b$ である．これは $\exists c, d \in R, s.t. a = bc, b = ad \Longrightarrow a = (ad)\, c = a\, (dc) \Longrightarrow dc = 1$ よって，$a \approx b$

8.2

$u \in \mathbb{Z}^{\times}$ であるから，$uu^{-1} = u^{-1}u = 1$ で，$u = \pm 1$．すると，$a \approx b$ となる $b \in \mathbb{Z}$ は $b = \pm a$．また，$a = 0$ のとき，$b = \pm a = 0$

8.3

(1)

$u = a + b\sqrt{-5}$ の逆元 $v = c + d\sqrt{-5}$ と定義すると，$uv = \left(a + b\sqrt{-5}\right)\left(c + d\sqrt{-5}\right) = 1$
よって，$\begin{cases} ac - 5bd = 1 \\ ad + bc = 0 \end{cases}$

1. $b = 0$ のとき，$\begin{cases} ac = 1 \\ ad = 0 \end{cases}$ で，$a, b, c, d \in \mathbb{Z}$ であるから，$a = \pm 1, c = \mp 1, b = d = 0$
2. $b \neq 0$ のとき，$c = -\dfrac{ad}{b}$ で，$-d\left(\dfrac{a^2}{b} + 5b\right) = 1$ となり，$d \neq 0$．また，$c \in \mathbb{Z}$ から，$b = \pm 1$ となる．すると $\left|\dfrac{a^2}{b} + 5b\right| \geq 5$ となるから，$-d\left(\dfrac{a^2}{b} + 5b\right) = 1$ をみたす $d \in \mathbb{Z}$ は存在しない

よって，$b = d = 0, a = \pm 1, c = \mp 1$．つまり，$\mathbb{Z}\left[\sqrt{-5}\right]$ のすべての単元は ± 1 である

(2)

$u, v \in \mathbb{Z}\left[\sqrt{-5}\right], uv = 3$ とすると，$\begin{cases} ac - 5bd = 3 \\ ad + bc = 0 \end{cases}$
(1) の討論より，$b = 0$ の場合しか成り立てないから，$b = d = 0, \begin{cases} a = \pm 1 \\ c = \pm 3 \end{cases}$ または $\begin{cases} a = \pm 3 \\ c = \pm 1 \end{cases}$.
言い換えれば，u, v の中で必ず一方が単元 ± 1 である．よって，3 は既約元である

(3)

$u, v \in \mathbb{Z}\left[\sqrt{-5}\right], uv = 2+\sqrt{-5}$ とすると, $\begin{cases} ac-5bd=2 \\ ad+bc=1 \end{cases} \Longrightarrow c-2d = \pm(5d+2c)$ で，$a = b\dfrac{5d+2c}{c-2d}$ を考えると，$a=3b$ となり，$LHS = 3RHS$ で矛盾する．よって，$2+\sqrt{-5}$ は既約元である．$2-\sqrt{-5}$ も同じ考えであるから略

(4)

$3\cdot 3 = 9 = \left(2+\sqrt{-5}\right)\left(2-\sqrt{-5}\right)$ であるから，$9 \in (3)$ であるが，$2+\sqrt{-5} \notin (3), 2-\sqrt{-5} \notin (3)$ から，素イデアルの定義より，(3) は素イデアルではない

(5)

$9 \in \mathbb{Z}\left[\sqrt{-5}\right]$ で，(2)(3) より，既約分解は $3\cdot 3$ または $\left(2+\sqrt{-5}\right)\left(2-\sqrt{-5}\right)$ である．すると，R は UFD であるなら，$3 \approx \left(2\pm\sqrt{-5}\right)$ をみたせばいいが，(1) より，単元は ± 1 しかないから，$\left(2\pm\sqrt{-5}\right)\cdot(\pm 1) \neq 3$ より，$3 \not\approx \left(2\pm\sqrt{-5}\right)$ である．よって，R は UFD ではない

(6)

(2)(3) より，$3\cdot 3 = 9 = \left(2+\sqrt{-5}\right)\left(2-\sqrt{-5}\right)$

8.4

(1)

$u = a+bi$ と逆元 $v = c+di$ を定義すると，$uv = 1$ となり，$\begin{cases} ac-bd=1 \\ ad+bc=0 \end{cases}$

1. $b=0$ のとき，$\begin{cases} ac=1 \\ ad=0 \end{cases} \Longrightarrow a = \pm 1, c = \pm 1, b = d = 0$
2. $b \neq 0$ のとき，$c = -\dfrac{ad}{b}$ で，$-d\left(\dfrac{a^2}{b}+b\right) = 1$ となり，$d \neq 0$

   また，$c \in \mathbb{Z}$ から，$b = \pm 1$ となる．また，$\left|\dfrac{a^2}{b}+b\right|$ は $a \neq 0$ のとき 1 より大きいであるから，$a = c = 0$

以上，$u = \pm 1$ または $\pm i$

(2)

$2 = (a+bi)(c+di)$ とすると $4 = |2|^2 = |a+bi|^2 |c+di|^2 = \left(a^2+b^2\right)\left(c^2+d^2\right) = \begin{cases} 1\cdot 4 \\ 2\cdot 2 \\ 4\cdot 1 \end{cases}$

1. $a^2+b^2 = 1$ のとき，$(a,b) = (\pm 1, 0), (0, \pm i)$ で，単元である
2. $a^2+b^2 = 2$ のとき，$a, b, c, d = \pm 1$ で，$2 = (1+i)(1-i)$ で，$1+i, 1-i \notin \mathbb{R}^\times$ より既約元ではない

(3)

$3=(a+bi)(c+di)$ とすると，$9=\left(a^2+b^2\right)\left(c^2+d^2\right)=\begin{cases}1\cdot 9\\3\cdot 3\\9\cdot 1\end{cases}$

$a^2+b^2=1, c^2+d^2=9$ とすると,$\begin{cases}a=\pm 1\\b=0\end{cases}$ または $\begin{cases}a=0\\b=\pm 1\end{cases}$ で,$3=(\pm 1)(c+di)=(\pm 1)(\pm 3)$ または $3=(\pm i)(c+di)=(\pm i)(\mp 3i)$ しか分解できない．$\pm 1, \pm i$ は単元であるから，3 は既約元である

9

9.1

(1)

$\gamma = a + b\sqrt{-2}, \gamma' = p + q\sqrt{-2}$ とすると，仮定より，$\begin{cases} |p-a| \leq \dfrac{1}{2} \\ |q-b| \leq \dfrac{1}{2} \end{cases}$ ．すると

$$N\left(\gamma' - \gamma\right) = N\left((p-a) + (q-b)\sqrt{-2}\right) \tag{49}$$
$$= (p-a)^2 + 2(q-b)^2 \tag{50}$$
$$\leq \frac{1}{4} + 2 \cdot \frac{1}{4} = \frac{3}{4} < 1 \tag{51}$$

(2)

$R = \mathbb{Z}\left[\sqrt{-2}\right]$ がユークリッド整域であるなら，$\forall \alpha, \beta \in R, \exists q, r \in R, s.t. \alpha = \beta q + r$ で，$r = 0$ または $N(r) < N(\beta)$ である．$\mathbb{Q}\left[\sqrt{-2}\right]$ で $\dfrac{\alpha}{\beta}$ を考えると，$\dfrac{\alpha}{\beta} = u + v\sqrt{-2} \quad (u, v \in \mathbb{Q})$ が書け，(1) より，$\exists m, n \in \mathbb{Z}, s.t. |u-m| < \dfrac{1}{2}, |v-n| < \dfrac{1}{2}$ から，$q = m + n\sqrt{-2}$ とおき，$r = \alpha - \beta q$ となり，$r = 0$ または $N(r) < N(\beta)$ をみたせばいい

$$N(r) = N\left(\beta\left(\frac{\alpha}{\beta} - q\right)\right) \tag{52}$$
$$= N(\beta) N\left(\frac{\alpha}{\beta} - q\right) \tag{53}$$
$$= N(\beta)\left(N\left[(u-m) + (v-n)\sqrt{-2}\right]\right) \tag{54}$$
$$= N(\beta)\left((u-m)^2 + 2(v-n)^2\right) \tag{55}$$
$$< N(\beta)\left(\frac{1}{4} + 2 \cdot \frac{1}{4}\right) \tag{56}$$
$$= \frac{3}{4} N(\beta) < N(\beta) \tag{57}$$

よって，$R = \mathbb{Z}\left[\sqrt{-2}\right]$ はユークリッド整域である

9.2

$\omega = \dfrac{-1 + \sqrt{-3}}{2}$ は $x^2 + x + 1 = 0$ の解であり，$\overline{\omega} = \omega^2$ なので

$$N(a + b\omega) = (a + b\omega)\left(a + b\omega^2\right) \tag{58}$$
$$= a^2 + ab\left(\omega + \omega^2\right) + b^2\omega^3 \tag{59}$$
$$= a^2 - ab + b^2 \tag{60}$$

と $N(a + b\omega) = a^2 - ab + b^2$ と定義する（$\mathbb{Q}[\omega]$ 上）
$\forall \alpha, \beta \in R := \mathbb{Z}[\omega], \exists q, r \in R, s.t. \alpha = \beta q + r$ で，$r = 0$ または $N(r) < N(\beta)$ を示す
$\dfrac{\alpha}{\beta} = u + v\omega \quad (u, v \in \mathbb{Q})$ とすると，$\exists m, n \in \mathbb{Z}, s.t. |u-m| < \dfrac{1}{2}, |v-n| < \dfrac{1}{2}$ から，$q := m + n\omega$

とおき，$r=\alpha-\beta q$ となり，$r=0$ または $N(r)<N(\beta)$ をみたせばいい

$$N(r)=N\left(\beta\left(\frac{\alpha}{\beta}-q\right)\right) \tag{61}$$

$$=N(\beta)N\left(\frac{\alpha}{\beta}-q\right) \tag{62}$$

ここで，$\epsilon_x:=x-m,\epsilon_y:=y-n$ とすると

$$N(r)=N(\beta)N\left(\frac{\alpha}{\beta}-q\right) \tag{63}$$

$$=N(\beta)N(\epsilon_x+\epsilon_y\omega) \tag{64}$$

$$=N(\beta)\left(\epsilon_x^2-\epsilon_x\epsilon_y+\epsilon_y^2\right) \tag{65}$$

$$<N(\beta)\left(\frac{1}{4}+\frac{1}{4}+\frac{1}{4}\right) \tag{66}$$

$$=\frac{3}{4}N(\beta)<N(\beta) \tag{67}$$

9.3

F を体とすると，$\forall a\in F,\exists a^{-1}\in F,s.t.aa^{-1}=a^{-1}a=1$ であるから．$\forall a,b\in F,q:=b^{-1}a$ とすれば，$a=bb^{-1}a=b\left(b^{-1}a\right)=bq\quad(+0)$ であるから，写像 $N(x)=1$ とすればいい

9.4

(1)

$(a,b)=(d)$ とすると，$(a)\subset(a,b),(b)\subset(a,b)$ であるから，$(a)\subset(d),(b)\subset(d)$ となり，$d|a,d|b$ である．よって，d は a,b の公約元である．c も a,b の公約元であると仮定すると，$(a)\subseteq(c)$ かつ $(b)\subseteq(c)$ である．すると，$(d)=(a,b)\subseteq(c)$ となるから，$c|d$ である．以上より，d は a,b の最大公約元である

(2)

$(a)\cap(b)=(m)$ とすると，$(m)\subseteq(a)$ かつ $(m)\subseteq(b)$ となり，m は a,b の公倍元である．n も a,b の公倍元であると仮定すると，$(n)\subseteq(a)$ かつ $(n)\subseteq(b)$ である．すると，$(n)\subseteq(a)\cap(b)=(m)$ から，$m|n$ となる．よって，m は a,b の最小公倍元である

(3)

d は a,b の最大公約元であるから，$\exists x,y\in R,s.t.d=xa+yb$ で，両辺に m をかけると，$dm=xam+ybm$ となる．また，m は a,b の最小公倍元であるから，$\exists s,t\in R,s.t.m=sa=tb$ で

$$dm=xam+ybm \tag{68}$$

$$=xa(tb)+yb(sa) \tag{69}$$

$$=xtab+ysab=(xt+ys)ab \tag{70}$$

から，$ab|dm$ で，$(dm)\subseteq(ab)$
逆に，d は a,b の最大公約元であるから，$d|a,d|b$ で，$\dfrac{ab}{d}$ は a,b の公倍元であり，m は a,b の最小公倍元であるから，$m|\dfrac{ab}{d}$ で，$\exists k\in R,s.t.\dfrac{ab}{d}=mk$ となる．両辺に d をかけると，$ab=dmk$ で，$dm|ab$ があるから，$(ab)\subseteq(dm)$
以上より，$(ab)=(dm)$

9.5

$(2,x)$ が単項イデアルであると仮定すると，$\exists f(x) \in \mathbb{Z}[x], s.t.\ (2,x) = (f(x))$
$2 \in (2,x) = (f(x))$ より，$f(x) | 2$ で，$f(x) \in \{\pm 1, \pm 2\}$
同様に，$x \in (2,x) = (f(x))$ から，$f(x) | x$ が成り立つ．しかし，$\pm 2 \nmid x$ であるから，$f(x) \in \{\pm 1\}$ となるが，$f(x) = \pm 1$ とすると，$(f(x)) = \mathbb{Z}([x])$ で，$2f(x) + xg(x) \in (2,x)$ の定数項は必ず偶数であるが，$\mathbb{Z}[x]$ の中に定数項が奇数である多項式が存在するので，矛盾する．よって，$(2,x)$ は単項イデアルではない

9.6

$$\begin{pmatrix} x^4+2x^3+5x+2 \\ x^4+x^3-3x^2+4x+2 \end{pmatrix} \to \begin{pmatrix} x^3+3x^2+x \\ x^4+x^3-3x^2+4x+2 \end{pmatrix} \tag{71}$$

$$\to \begin{pmatrix} x^3+3x^2+x \\ 2x^2+6x+2 \end{pmatrix} \tag{72}$$

$$\to \begin{pmatrix} x^2+3x+1 \\ 0 \end{pmatrix} \tag{73}$$

から，最大公約元は x^2+3x+1

10

10.1

包含写像 $\phi : \mathbb{Z} \to \mathbb{Q}$ を $\phi(x) = x$ と定めると，ϕ は明らかに単射である．また，$\forall a, b, c, d \in \mathbb{Z}, b, d \neq 0, x = \dfrac{a}{b} + \dfrac{c}{d}\sqrt{2} \in \mathbb{Q}\left[\sqrt{2}\right]$ で

$$x = \frac{a}{b} + \frac{c}{d}\sqrt{2} \tag{74}$$

$$= \frac{ad + bc\sqrt{2}}{bd} \tag{75}$$

$$= \phi\left(ad + bc\sqrt{2}\right)\phi(bd)^{-1} \tag{76}$$

から，$\mathbb{Q}\left[\sqrt{2}\right]$ は $\mathbb{Z}\left[\sqrt{2}\right]$ の商体である

10.2

$\phi : K \to K$ を $\phi(x) = x$ と定めると，ϕ は明らかに単射である．また，$x = \phi(x) = \phi(x)\phi(1)^{-1}$ であることを注意すると，K の商体は K 自身である

10.3

(1)

$0 = \dfrac{0}{1}, 1 = \dfrac{1}{1}, (p, 1) = 1$ であることを注意すると，$0, 1 \in \mathbb{Z}_{(p)}$
$\forall \dfrac{m}{n}, \dfrac{m'}{n'} \in \mathbb{Z}_{(p)}, (p, n) = (p, n') = 1$ で

$$\frac{m}{n} + \frac{m'}{n'} = \frac{mn' + m'n}{nn'} \in \mathbb{Z}_{(p)} \qquad \left(p, nn'\right) = 1 \tag{77}$$

$$\frac{m}{n} \cdot \frac{m'}{n'} = \frac{mm'}{nn'} \in \mathbb{Z}_{(p)} \qquad \left(p, nn'\right) = 1 \tag{78}$$

また，$\dfrac{m}{n} \in \mathbb{Z}_{(p)}$ の加法に関する逆元は $-\dfrac{m}{n} = \dfrac{-m}{n} \in \mathbb{Z}_{(p)}$ であり，$\dfrac{m}{n} \in \mathbb{Z}_{(p)}$ から，$(p, n) = 1$ より，$\dfrac{-m}{n} \in \mathbb{Z}_{(p)}$
以上より，$\mathbb{Z}_{(p)}$ は $\mathbb{Q}$ の部分環である

(2)

包含写像 $\phi : \mathbb{Z}_{(p)} \to \mathbb{Q}$ を $\phi(x) = x$ と定め，ϕ は明らかに単射で，$n = 1$ とすると，$(p, n) = 1$ で

$$\phi(a)(b)^{-1} = \frac{a}{1} \cdot \frac{1}{b} \tag{79}$$

$$= \frac{a}{b} \tag{80}$$

とかけるから，$\mathbb{Z}_{(p)}$ の商体は $\mathbb{Q}$ である

11

11.1

(1)

$$x^2+\overline{1}=x^2+\overline{0}x+\overline{1}=x^2+\overline{2}x+\overline{1}=\left(x+\overline{1}\right)\left(x+\overline{1}\right) \tag{81}$$

より，既約でない

(2)

$\overline{0},\overline{1},\overline{2}$ をそれぞれ代入すると，$\begin{cases}x^2+\overline{1}=\overline{1} & x=\overline{0}\\ x^2+\overline{1}=\overline{2} & x=\overline{1}\\ x^2+\overline{1}=\overline{2} & x=\overline{2}\end{cases}$ となり，$\overline{0}$ にならない
よって，$x^2+\overline{1}$ は $(\mathbb{Z}/3\mathbb{Z})[x]$ で既約である

(3)

$\overline{1}^3+\overline{2}=\overline{3}=\overline{0}$ であることを注意すると，$x^3+\overline{2}=\left(x-\overline{1}\right)\left(x^2+x+\overline{1}\right)$ と分解できるから，既約でない

11.2

$f(x)=x^3-x-2$ が $(\mathbb{Z}/5\mathbb{Z})[x]$ で可約であると仮定すると，$\exists a\in\mathbb{Z}/5\mathbb{Z},s.t.x=a$ は x^3-x-2 の根である．$\overline{0},\overline{1},\overline{2},\overline{3},\overline{4}$ をそれぞれ代入すると

$$\begin{cases}x^3-x-2=\overline{3} & x=\overline{0}\\ x^3-x-2=\overline{3} & x=\overline{1}\\ x^3-x-2=\overline{4} & x=\overline{2}\\ x^3-x-2=\overline{2} & x=\overline{3}\\ x^3-x-2=\overline{3} & x=\overline{4}\end{cases} \tag{82}$$

となるから，根が存在しない．よって，$f(x)=x^3-x-2$ は $(\mathbb{Z}/5\mathbb{Z})[x]$ で既約である

11.3

(1)

$f(x)=x^4-x-3$ が $g(x)=x+a,h(x)=x^3+bx^2+cx+d$ と分解できると仮定すると

$$f(x)=(x+a)\left(x^3+bx^2+cx+d\right) \tag{83}$$
$$=x^4+(a+b)x^3+(ab+c)x^2+(ac+d)x+ad \tag{84}$$
$$=x^4-x-3 \tag{85}$$

から，$\begin{cases} a+b=0 \\ ab+c=0 \\ ac+d=-1 \\ ad=-3 \end{cases}$ となり，$a \in \mathbb{Z}$ より，$a=\pm 1, \pm 3$

$\pm 1, \pm 3$ をそれぞれ代入すると

$$f(1)=-3 \tag{86}$$
$$f(-1)=-1 \tag{87}$$
$$f(3)=75 \tag{88}$$
$$f(-3)=81 \tag{89}$$

で，いずれも 0 にならないから，根が存在しない．よって，$f(x)$ は $\mathbb{Z}[x]$ で既約である

(2)

$f(x)=x^4-x-3$ が $g(x)=x^2+ax+b$ と $h(x)=x^2+cx+d$ と分解できると仮定すると

$$f(x)=\left(x^2+ax+b\right)\left(x^2+cx+d\right) \tag{90}$$
$$=x^4+(a+c)x^3+(ac+b+d)x^2+(ad+bc)x+bd \tag{91}$$
$$=x^4-x-3 \tag{92}$$

から，$\begin{cases} a+c=0 \\ ac+b+d=0 \\ ad+bc=-1 \\ bd=-3 \end{cases} \Longrightarrow (b,d)=(1,-3),(-1,3),(3,-1),(-3,1) \Longrightarrow b+d=\pm 2$

$\begin{cases} ac=-b-d=\mp 2 \\ a=-c \end{cases}$ より，$a^2=\pm 2$ となり，いずれも $a \in \mathbb{Z}$ を満たさない．よって，$f(x)$ は $\mathbb{Z}[x]$ で既約である

(3)

(1)(2) より，$f(x)$ は $\mathbb{Z}[x]$ で既約で，$\mathbb{Q}[x]$ は $\mathbb{Z}[x]$ の商体であるから，$f(x)$ は $\mathbb{Q}[x]$ でも既約である

11.4

$(\mathbb{Z}/2\mathbb{Z})[x]$ での 2 次多項式は $\begin{cases} x^2+\overline{0}x+\overline{0} \\ x^2+\overline{0}x+\overline{1} \\ x^2+\overline{1}x+\overline{0} \\ x^2+\overline{1}x+\overline{1} \end{cases}$ であり，$\mathbb{Z}/2\mathbb{Z}$ で根を持たないのは $x^2+\overline{1}x+\overline{1}$ だけであるから，既約であるものは $x^2+\overline{1}x+\overline{1}$ である

11.5

x^2+x+1 は $(\mathbb{Z}/2\mathbb{Z})[x]$ 上で既約で

$$\left(x^2+x+1\right)^2=x^4+2x^3+3x^2+2x+1 \tag{93}$$
$$\equiv x^4+x^2+1 \pmod 2 \tag{94}$$

であることを注意すると，$x^4+x^2+\overline{1}$ は $(\mathbb{Z}/2\mathbb{Z})[x]$ 上で既約ではない

11.6

(1)

$$f(x) = 3x^5 - 2x^4 + x^3 - 3x^2 - x + 5 \tag{95}$$
$$\equiv x^5 + x^3 + x^2 + x + 1 \qquad (\mathrm{mod}\ 2) \tag{96}$$

一次の因式に対して，$\overline{0}, \overline{1}$ は $f(x)$ の根でないから存在しない．また，二次の因式に対して，既約なものは $x^2 + x + 1$ だけであるが，$x^2 + x + 1$ で割った余りは x であり，0 ではないから，2 次（3 次）の因子も存在しない．以上，$f(x)$ は $(\mathbb{Z}/2\mathbb{Z})[x]$ 上で既約である

(2)

$(\mathbb{Z}/2\mathbb{Z})[x]$ は $\mathbb{Z}[x]$ の商体であり，$\mathbb{Q}[x]$ も $\mathbb{Z}[x]$ の商体であるから，$f(x)$ は $\mathbb{Q}[x]$ 上でも既約である

12

12.1

$3 \nmid 1, 3 \mid 3, 3 \mid -6, 3^2 = 9 \nmid 3$ から, Eisenstein の既約判定法により, $f(x) = x^4+3x^3-6x^2+3x+3$ は $\mathbb{Q}[x]$ で既約である

12.2

$f(x)$ が既約とし，$f(x+a)$ が可約であると仮定すると，$\exists g(x), h(x) \in \mathbb{Z}[x], s.t. f(x+a) = g(x)h(x)$ で，$f(x) := g(x-a)h(x-a)$ とかける．すると，$f(x)$ が既約であることより，$g(x-a)$ または $h(x-a)$ は ± 1 となり，$g(x)$ または $h(x)$ は ± 1 となる．よって，$f(x+a)$ は既約である
逆に，$f(x+a)$ が既約であるとし，$f(x) = g(x)h(x)$ とすると，$g(x+a)$ または $h(x+a)$ が ± 1 となり，$g(x)$ または $h(x)$ が ± 1 となる．よって，$f(x)$ は既約である

12.3

(1)

$x = y+1$ とおくと

$$x^4 + 1 = (y+1)^4 + 1 \tag{97}$$
$$= y^4 + 4y^3 + 6y^2 + 4y + 2 \tag{98}$$

となり，$p = 2$ とすれば，Eisenstein の既約判定法により，x^4+1 は $\mathbb{Q}[x]$ で既約である

(2)

(1) と同様に，$x = y+1$ とおくと

$$x^{p-1} + x^{p-2} + \cdots + x + 1 = (y+1)^{p-1} + (y+1)^{p-2} + \cdots + (y+1) + 1 \tag{99}$$
$$= \frac{(y+1)^p - 1}{(y+1) - 1} \tag{100}$$
$$= \frac{\displaystyle\sum_{k=0}^{p} \binom{p}{k} y^k - 1}{y} \tag{101}$$
$$= \sum_{k=1}^{p} \binom{p}{k} y^{k-1} \tag{102}$$
$$= \sum_{j=0}^{p-1} \binom{p}{j+1} y^j \tag{103}$$

で，Eisenstein の既約判定法により，$x^{p-1} + x^{p-2} + \cdots + x + 1$ は $\mathbb{Q}[x]$ で既約である

参考文献