「環と加群の基礎」演習問題解答

大阿久 俊則

1 環

1.1 環の定義と例

問題 1.1 (1) $\frac{1}{2} \in R$ であるが $\frac{1}{2}\frac{1}{2} = \frac{1}{4}$ は R に属さないから R は $\mathbb{C}$ の部分環ではない.

(2) R の元は非負整数 n と整数 k によって $\frac{k}{10^n}$ と表される．$m, l \in \mathbb{Z}$, $m \geq 0$ のとき,

$$\frac{k}{10^n} \pm \frac{l}{10^m} = \frac{k \cdot 10^m \pm l \cdot 10^n}{10^{n+m}}, \qquad \frac{k}{10^n}\frac{l}{10^m} = \frac{kl}{10^{m+n}}$$

であるから，R の 2 つの元の和，差，積はまた R に属する．また，$0, 1 \in R$．よって R は $\mathbb{C}$ の部分環である.

問題 1.2 R を $\mathbb{C}$ の部分環とする．$0, 1 \in R$ である．任意の自然数 n が R に属することを n についての帰納法で示そう．$n = 1$ は R に属する．$n \geq 2$ として $n - 1 \in R$ と仮定すると，R が環であることから，$n = (n-1) + 1 \in R$ となる．以上により非負整数はすべて R に属することがわかった．さらに R が環であることから，任意の $n \in \mathbb{N}$ に対して $-n \in R$ でなければならないから，R はすべての整数を含む．以上により $\mathbb{Z} \subset R$ が示された.

問題 1.3 (1) 可換環の条件 (1)–(8) を確かめればよい．($\mathbb{Z}$ が環であることは証明せずに用いてよい.）加法の単位元は $(0,0)$, 乗法の単位元は $(1,1)$, (a,b) の加法についての逆元は $(-a,-b)$ である.

(2) $(1,0)(0,1) = (0,0)$ より $\mathbb{Z}^2$ は整域ではない.

(3) (a,b) が $\mathbb{Z}^2$ の可逆元とすると，ある整数 c, d があって $(a,b)(c,d) = (1,1)$ すなわち $ac = 1$ かつ $bd = 1$ が成立する．a, b, c, d は整数だから $a = \pm 1$, $b = \pm 1$ でなければならない．よって (a,b) は $(1,1)$, $(1,-1)$, $(-1,1)$, $(-1,-1)$ のいずれかである．これらがすべて可逆元であることもわかるので，$\mathbb{Z}^2$ の可逆元はこの 4 つである.

問題 1.4 $\mathbb{Q}[\sqrt{-1}]$ が $\mathbb{C}$ の部分環であることは例 1.2 と同様に示せる．$a, b \in \mathbb{Q}$ について $a + bi \neq 0$ すなわち $(a,b) \neq (0,0)$ とする．このとき $(a+bi)(c+di) = 1$ を満たす $c, d \in \mathbb{Q}$ が存在することを示せばよい．$(a+bi)(a-bi) = a^2 + b^2 > 0$ より $c = \frac{a}{a^2+b^2}$, $d = -\frac{b}{a^2+b^2}$ とおけば $(a+bi)(c+di) = 1$ が成立することがわかる．以上により $\mathbb{Q}[\sqrt{-1}]$ は体であることが示された.

問題 1.5 $a, b \in \mathbb{Z}$ として $a+bi$ が $\mathbb{Z}[\sqrt{-1}]$ の単元とすると，$(a+bi)(c+di)=1$ を満たす $c, d \in \mathbb{Z}$ が存在する．両辺の絶対値の 2 乗をとると

$$1 = |a+bi|^2|c+di|^2 = (a^2+b^2)(c^2+d^2)$$

ここで a^2+b^2 と c^2+d^2 は非負整数であるから $a^2+b^2 = c^2+d^2 = 1$ でなければならない．これから (a, b) は $(1,0), (-1,0), (0,1), (0,-1)$ のいずれかであることがわかる．これらに対応する $\mathbb{Z}[\sqrt{-1}]$ の元 $1, -1, i, -i$ はいずれも単元であることがわかる（たとえば $i(-i)=1$）ので，これらが $\mathbb{Z}[\sqrt{-1}]$ の単元のすべてである．

問題 1.6 (1) $R \subset \mathbb{Q}$ は定義より明らか．$0 = \dfrac{0}{2^0} \in R$, $1 = \dfrac{1}{2^0} \in R$ である．$n, m \in \mathbb{Z}$, $k, l \in \mathbb{N} \cup \{0\}$ とすると，

$$\frac{n}{2^k} + \frac{m}{2^l} = \frac{2^l n + m 2^k}{2^{k+l}} \in R, \quad -\frac{n}{2^k} = \frac{-n}{2^k} \in R, \quad \frac{n}{2^k}\frac{m}{2^l} = \frac{nm}{2^{k+l}} \in R$$

が成立するから R は $\mathbb{Q}$ の部分環である．$\dfrac{1}{2}$ は R の元であるが，$\mathbb{Z}$ には属さない．また，$\dfrac{1}{3}$ は $\mathbb{Q}$ の元であるが R には属さない．従って $\mathbb{Z} \subsetneqq R \subsetneqq \mathbb{Q}$ である．

(2) R の単元（可逆元）の全体は $U := \{\pm 2^k \mid k \in \mathbb{Z}\}$ であることを示す．$k \in \mathbb{Z}$ に対して $\pm 2^k, \pm 2^{-k} \in R$ かつ $(\pm 2^k)(\pm 2^{-k}) = 1$ より $\pm 2^k$ は R の単元である．次に $\dfrac{n}{2^k}$ $(n, k \in \mathbb{Z},\ k \geq 0)$ が R の単元であると仮定すると，$l \geq 0$ かつ $\dfrac{n}{2^k}\dfrac{m}{2^l} = 1$ を満たす整数 m, l が存在する．このとき $nm = 2^{k+l}$ であるから，ある非負整数 p, q によって $n = \pm 2^p$, $m = \pm 2^q$ と表される（素因数分解の一意性より）．よって $\dfrac{n}{2^k} = \pm\dfrac{2^p}{2^k} = \pm 2^{p-k}$ は U に属する．

問題 1.7 (1) $R \subset \mathbb{Q}$ は定義より明らか．$0 = \dfrac{0}{1} \in R$, $1 = \dfrac{1}{1} \in R$ である．n, n' を整数，m, m' を正の奇数とすると，mm' も奇数であるから，

$$\frac{n}{m} + \frac{n'}{m'} = \frac{nm' + n'm}{mm'} \in R, \quad -\frac{n}{m} = \frac{-n}{m} \in R, \quad \frac{n}{m}\frac{n'}{m'} = \frac{nn'}{mm'} \in R$$

が成立するから R は $\mathbb{Q}$ の部分環である．$\dfrac{1}{3}$ は R の元であるが，$\mathbb{Z}$ には属さない．また，$\dfrac{1}{2}$ は $\mathbb{Q}$ の元であるが R には属さない．従って $\mathbb{Z} \subsetneqq R \subsetneqq \mathbb{Q}$ である．

(2) R の単元（可逆元）の全体は $U := \left\{ \dfrac{n}{m} \mid n, m \text{ は奇数}, m > 0 \right\}$ であることを示す．m, n が奇数ならば $\dfrac{n}{m}$ と $\dfrac{m}{n}$ は共に R の元であり，積は 1 だから $\dfrac{n}{m}$ は単元である．よって U のすべての元は単元である．逆に $\dfrac{n}{m}$ が単元とすると，整数 n' と正の奇数 m' が存在して $\dfrac{n}{m}\dfrac{n'}{m'} = 1$，すなわち $nn' = mm'$ が成立する． mm' は奇数だかから n と n' も奇数でなければならない．よって $\dfrac{n}{m}$ は U に属する．以上により U が R の単元の全体であることが示された．

1.2 環準同型

問題 1.8 環準同型は 1 を 1 にうつすから f_n が環準同型であるためには $n = f_n(1) = 1$ でなければならない．f_1 は恒等写像だから環準同型である．よって f_n が環準同型であるための必要十分条件は $n = 1$ である．

問題 1.9 (1) f が単射であると仮定する．f は環準同型だから $f(0_R) = 0_{R'}$ である．よって $a \in R$ について $f(a) = 0_{R'}$ ならば f が単射であることから $a = 0_R$ でなければならない．よって $\{a \in R \mid f(a) = 0_{R'}\} = \{0_R\}$ である．

(2) $\{a \in R \mid f(a) = 0_{R'}\} = \{0_R\}$ を仮定して f が単射であることを示す．$a, b \in R$ について $f(a) = f(b)$ と仮定すると，$f(a - b) = f(a) - f(b) = 0_{R'}$ であるから，仮定より $a - b = 0_R$ すなわち $a = b$ となるから f は単射である．

問題 1.10 $f(1_R) = 1_{R'}$ より $f^{-1}(1_{R'}) = 1_R$ である．また任意の $a', b' \in R'$ に対して $a = f^{-1}(a'), b = f^{-1}(b')$ とおくと，f が環準同型であることから

$$f(a + b) = f(a) + f(b) = a' + b', \quad f(ab) = f(a)f(b) = a'b'$$

よって

$$f^{-1}(a' + b') = a + b = f^{-1}(a') + f^{-1}(b'), \quad f^{-1}(a'b') = ab = f^{-1}(a')f^{-1}(b')$$

以上により $f^{-1} : R' \to R$ は環準同型である．さらに f が全単射だから f^{-1} も全単射である．よって f^{-1} は環同型である．

問題 1.11 $f : \mathbb{Z} \to \mathbb{Z}$ を環準同型とする．任意の自然数 n について $f(n) = n$ が成立することを n についての帰納法で示す．準同型の定義より $f(1) = 1$ であるから $n = 1$ のときは成立する．$n \geq 2$ として $f(n - 1) = n - 1$ と仮定すると $f(n) = f((n - 1) + 1) = f(n-1) + f(1) = (n-1) + 1 = n$ が成立する．よって示された．$f(0) = 0$ である．また n が自然数のとき $0 = f(0) = f(n) + f(-n)$ より $f(-n) = -f(n) = -n$ も成立する．以上により任意の整数 n について $f(n) = n$ であることが示されたから f は恒等写像である．

問題 1.12 $f : \mathbb{Q} \to \mathbb{Q}$ を環準同型とすると，前問と同じ論法により，任意の整数 n について $f(n) = n$ であることがわかる．$p \in \mathbb{Z}, q \in \mathbb{N}$ とすると，

$$qf\left(\frac{p}{q}\right) = f(q)f\left(\frac{p}{q}\right) = f\left(q\frac{p}{q}\right) = f(p) = p$$

であるから，$f\left(\dfrac{p}{q}\right) = \dfrac{p}{q}$ が成立する．従って f は恒等写像である．

問題 1.13 $f : \mathbb{Z} \to \mathbb{Z}^2$ を環準同型とする．$\mathbb{Z}$ の加法の単位元は $(0, 0)$ であるから，$f(0) = (0, 0)$ である．また，$\mathbb{Z}^2$ の乗法の単位元は $(1, 1)$ であるから，$f(1) = (1, 1)$ でなければならない．数学的帰納法により，任意の非負整数 n について $f(n) = (n, n)$ が成立することを示そう．$n = 0, 1$ のときは示された．$f(n) = (n, n)$ を仮定すると

$$f(n + 1) = f(n) + f(1) = (n, n) + (1, 1) = (n + 1, n + 1)$$

が成立する．よって上の主張は示された．このとき $f(-n) = -f(n) = -(n,n) = (-n,-n)$ であるから，任意の整数 n について $f(n) = (n,n)$ が成立する．任意の $n, m \in \mathbb{Z}$ に対して

$$f(n+m) = (n+m, n+m) = (n,n) + (m,m) = f(n) + f(m),$$
$$f(nm) = (nm, nm) = (n,n)(m,m) = f(n)f(m), \qquad f(1) = (1,1)$$

が成立するから，f は環準同型である．以上により $\mathbb{Z}$ から $\mathbb{Z}^2$ への環準同型はこの f のみであることがわかった．

問題 1.14 (1) $a = f((1,0)), b = f((0,1))$ とおく．数学的帰納法により，任意の自然数 n について $f((n,0)) = na$, $f((0,n)) = nb$ が成立することがわかる．これは $n = 0$ のときも成立する．また $f((-n,0)) = f(-(n,0)) = -f(n,0) = -na$, 同様に $g((0,-n)) = -nb$ より，任意の整数 m, n について

$$f((m,n)) = f((m,0) + (0,n)) = f((m,0)) + f((0,n)) = ma + nb$$

が成立する．

(2) f が環準同型であることから

$$a^2 = f((1,0))^2 = f((1,0)^2) = f((1,0)) = a, \quad b^2 = f((0,1))^2 = f((0,1)^2) = f((0,1)) = b$$

が成立する．従って a と b は 0 または 1 である．また，

$$1 = f((1,1)) = a + b$$

より $(a,b) = (1,0)$ または $(a,b) = (0,1)$ である．$(a,b) = (1,0)$ のときは，$f((m,n)) = m$ であり，これが環準同型であること容易にわかる．$(a,b) = (0,1)$ のときは，$f((m,n)) = n$ であり，これも環準同型である．

問題 1.15 (1) $i^2 + 1 = 0$ と f が環準同型であることから，

$$0 = f(0) = f(i^2+1) = f(i)^2 + f(1) = f(i)^2 + 1 = (f(i) - i)(f(i) + i)$$

よって $f(i) = i$ または $f(i) = -i$ である．

(2) $f(i) = i$ ならば任意の $a, b \in \mathbb{R}$ に対して

$$f(a+bi) = f(a) + f(b)f(i) = a + bf(i) = a + bi$$

であるから f は恒等写像である．$f(i) = -i$ ならば任意の $a, b \in \mathbb{R}$ に対して

$$f(a+bi) = f(a) + f(b)f(i) = a + bf(i) = a - bi$$

となる（複素数にその共役複素数を対応させる写像）．いずれの場合にも f が全単射であることは明らか（逆写像は $f^{-1} = f$）だから f が環準同型であることを示せばよい．

$f(i) = i$ の場合は $f = \mathrm{id}_{\mathbb{C}}$ が環準同型であることは明らかである．$f(i) = -i$ の場合に f が環準同型であることを示す．f の定義より $f(1) = 1$ が成立する．$a, b, c, d \in \mathbb{R}$ に対して

$$\begin{aligned}
&f((a+bi)+(c+di)) = f((a+c)+(b+d)i) = a+c-(b+d)i \\
&= (a-bi)+(c-di) = f(a+bi)+f(a+bi), \\
&f((a+bi)(c+di)) = f((ac-bd)+(ad+bc)i) = ac-bd-(ad+bc)i \\
&= (a-bi)(c-di) = f(a+bi)f(c+di)
\end{aligned}$$

が成立する．以上により f はいずれの場合にも環同型である．

1.3 多項式環

問題 1.16 $f = (x^2+3x-1)g - 4$

問題 1.17 f を x^3-1 で割り算した余りを $r(x)$, 商を $q(x)$ とおくと，

$$f(x) = (x^3-1)q(x) + r(x) = (x-1)(x^2+x+1)q(x) + r(x)$$

ここで $r(x)$ は高々2次式であるから，$r(x)$ を x^2+x+1 で割り算すると

$$r(x) = c(x^2+x+1) + ax + b \quad (\exists a, b, c \in \mathbb{Q})$$

という形になる．これを前式に代入して

$$f(x) = \{(x-1)q(x)+c\}(x^2+x+1) + ax + b$$

を得る．従って f を x^2+x+1 で割った余りが $ax+b$ であるから，$a = 1$, $b = 2$ である．一方剰余定理により

$$6 = f(1) = r(1) = 3c + a + b = 3c + 3$$

よって $c = 1$. 以上により

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

問題 1.18 $f(x)$ を $(x-a)(x-b)$ で割り算して

$$f(x) = q(x)(x-a)(x-b) + Ax + B \qquad (q(x) \in K[x], \quad A, B \in K)$$

とする．ここで x に a, b を代入すると仮定より

$$Aa + B = f(a) = 0, \qquad Ab + B = f(b) = 0$$

辺々引き算して $A(a-b) = 0$. これと $a \neq b$ より $A = B = 0$ となる．従って $f(x)$ は $(x-a)(x-b)$ で割り切れる．

1.4 イデアル

問題 1.19 (1) $1 \in I$ であるから，I がイデアルならば $-1 \in I$ でなければならないが，これは I の定義に反する．よって I は R のイデアルでない．

(2) $1 \in I$ であるが $2 = 1 + 1$ は I に属さないから I はイデアルでない．

(3) $f = a_n x^n + \cdots + a_1 x + a_0$, $g = b_m x^n + \cdots + b_1 x + b_0$ $(a_i, b_j \in \mathbb{Z})$ とおく．($i > n$ のとき $a_i = 0$, $j > m$ のとき $b_j = 0$ とする．）もし $f, g \in I$ ならば $a_i \in 2\mathbb{Z}$, $b_j \in 2\mathbb{Z}$ より $a_i + b_i \in 2\mathbb{Z}$ だから

$$f + g = \sum_{i=0}^{\max\{n,m\}} (a_i + b_i) x^i \in I$$

となる．また $f \in I$ と仮定して $fg = c_{n+m} x^{n+m} + \cdots c_1 x + c_0$ とおくと

$$c_k = \sum_{i=0}^{k} a_k b_{k-i} \in 2\mathbb{Z}$$

であるから $fg \in I$ である．以上により I は R のイデアルであることが示された．

(4) $f, g \in I$ とすると $(f+g)(1) = f(1) + g(1) \in 2\mathbb{Z}$ より $f + g \in I$ である．$f \in I$, $g \in R$ とすると $(fg)(1) = f(1)g(1) \in 2\mathbb{Z}$ より $fg \in I$. よって I は R のイデアルである．

(5) $f, g \in I$ とすると $(f+g)(\sqrt{2}) = f(\sqrt{2}) + g(\sqrt{2}) = 0$ より $f + g \in I$. $f \in I$, $g \in R$ とすると $(fg)(\sqrt{2}) = f(\sqrt{2})g(\sqrt{2}) = 0$ より $fg \in I$. よって I は R のイデアルである．

問題 1.20 $0 \in I$, $0 \in J$ より $0 = 0 + 0 \in I + J$ である．$I + J$ の任意の 2 つの元は $a + b$, $c + d$ $(a, c \in I,\ b, d \in J)$ と表せる．このとき $a + c \in I$, $b + d \in I$ より $(a + b) + (c + d) = (a + c) + (b + d)$ は $I + J$ に属する．また，任意の $r \in R$ に対して $ra \in I$, $rb \in J$ より $r(a + b) = ra + rb$ は $I + J$ に属する．以上により $I + J$ は R のイデアルである．

$0 \in I \cap J$ である．$a, b \in I \cap J$, $c \in R$ のとき $a + b \in I$ かつ $a + b \in J$ より $a + b \in I \cap J$. また $ca \in I$ かつ $ca \in J$ より $ca \in I \cap J$. 以上により $I \cap J$ は R のイデアルである．

問題 1.21 $0 \in R'$ かつ $0 \in I$ より $0 \in I \cap R'$ である．$a, b \in I \cap R'$, $c \in R'$ とすると，I がイデアルであることから $a + b$ と ca は I に属する．また，R' が部分環であることから $a + b$ と ca は R' に属する．よって $a + b$ と ca は $I \cap R'$ に属するから $I \cap R'$ は R' のイデアルである．

問題 1.22 (1) $f(0_R) = 0_{R'} \in I'$ より $0_R \in f^{-1}(I')$ である．$a, b \in f^{-1}(I')$ かつ $c \in R$ とすると $f(a + b) = f(a) + f(b) \in I'$, $f(ca) = f(c)f(a) \in I'$ より $a + b$ と ca は $f^{-1}(I')$ に属する．よって $f^{-1}(I')$ は R のイデアルである．

(2) $a', b' \in f(I)$, $c \in R'$ とする．$f(a) = a'$, $f(b) = b'$ を満たす $a, b \in I$ が存在する．I はイデアルだから $a + b \in I$．よって

$$a' + b' = f(a) + f(b) = f(a + b) \in f(I)$$

が成立する．また f は全射だから $f(c) = c'$ となる $c \in R$ が存在する．$c'a' = f(c)f(a) = f(ca)$ であり $ca \in I$ だから $c'a' \in f(I)$ である．以上により $f(I)$ は R' のイデアルである．

(3) たとえば $f : \mathbb{Z} \to \mathbb{Q}$ を埋め込み写像，すなわち $f(a) = a$ $(\forall a \in \mathbb{Z})$ として $I = 2\mathbb{Z}$ とおく．このとき I は $\mathbb{Z}$ のイデアルであるが，$f(I) = 2\mathbb{Z}$ は $\mathbb{Q}$ のイデアルではない．実際 $1/2 \in \mathbb{Q}$ かつ $2 \in f(I)$ であるが $(1/2)2 = 1 \notin 2\mathbb{Z}$ である．

問題 1.23 I を K のイデアルとする．I が 0 以外の K の元 a を含めば，$1 = a^{-1}a \in I$ より $I = K$ である．よって K のイデアルは $\{0\}$ と K のみである．

(2) $a \in R$ かつ $a \neq 0$ とする．$I := Ra$ は $a \neq 0$ を含むから仮定より $I = R$ である．特に $1 \in I$ であるから，$1 = ca$ を満たす $c \in R$ が存在する．よって a は R の単元であるから，R は体である．

問題 1.24 問題訂正: $R \neq \{0_R\}$，すなわち $1_R \neq 0_R$ と仮定する．

解答: $\operatorname{Ker} f$ は K のイデアルである．K は体であるから前問より $\operatorname{Ker} f = \{0_K\}$ または $\operatorname{Ker} f = K$ が成立する．$f(1_K) = 1_R \neq 0_R$ より $1_K \notin \operatorname{Ker} f$ であるから $\operatorname{Ker} f = \{0_K\}$ である．よって問題 1.9 より f は単射である．

問題 1.25 (1) $(a, b) \in I$ とすると $(a, 0) = (1, 0)(a, b) \in I$, $(0, b) = (0, 1)(a, b) \in I$ となる．

(2) $a, b \in I_1$ とすると $(a, 0) \in I$ かつ $(b, 0) \in I$ であるから $(a+b, 0) = (a, 0)+(b, 0) \in I$. よって $a + b \in I_1$ である．また，任意の $c \in Z$ に対して，$(ca, 0) = (c, 0)(a, 0) \in I$ より $ca \in I_1$ となる．以上により I_1 は $\mathbb{Z}$ のイデアルであることが示された．I_2 についても同様.

(3) $a \in I_1, b \in I_2$ とすると，I_1 と I_2 の定義より $(a, b) = (a, 0) + (0, b) \in I$ となる．よって $I_1 \times I_2 \subset I$ である．逆に $(a, b) \in I$ とすると (1) より $a \in I_1$ かつ $b \in I_2$ であるから，$I \subset I_1 \times I_2$ である．以上により $I = I_1 \times I_2$ が示された.

1.5 剰余環と環準同型定理

問題 1.26 単元は $\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}$ である．（乗法の演算表で $\overline{1}$ が現れる行または列に対応する第 1 列あるいは第 1 行の元が単元である.）

和	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{6}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$

積	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{1}$	$\overline{3}$	$\overline{5}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{2}$	$\overline{5}$	$\overline{1}$	$\overline{4}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{1}$	$\overline{5}$	$\overline{2}$	$\overline{6}$	$\overline{3}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

問題 1.27

和	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{6}$	$\overline{6}$	$\overline{7}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{7}$	$\overline{7}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$

積	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{1}$	$\overline{4}$	$\overline{7}$	$\overline{2}$	$\overline{5}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{2}$	$\overline{7}$	$\overline{4}$	$\overline{1}$	$\overline{6}$	$\overline{3}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{7}$	$\overline{0}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

(2) 乗法の演算表より単元は $\overline{1}$, $\overline{3}$, $\overline{5}$, $\overline{7}$. (3) 乗法の演算表より零因子は $\overline{2}$ と $\overline{4}$.

問題 1.28 (1) 省略
(2) 単元は $\overline{1}$, $\overline{5}$, $\overline{7}$, $\overline{11}$ である．$\overline{2}, \ldots, \overline{11}$ との積が $\overline{1}$ となるような元があるかどうか調べればよい．実は，単元は 12 と互いに素な自然数の同値類となる（問題 1.37）．
(3) 零因子は $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{6}$, $\overline{8}$, $\overline{9}$, $\overline{10}$.

問題 1.29 (1) $g = x^2 + x + 1$ とおく．$f \in R[x]$ を g で割った余りは $ax + b$ $(a, b \in R)$ と表せる．f の $R/R[x]f$ における同値類を $[f]$ とすると，このとき $[f] = [ax + b] = a[x] + b$ が成立する．($f - (ax + b)$ は g で割り切れるから $R[x]f$ に属するので.）また $a', b' \in R$ に対して $[a'x + b'] = [ax + b]$ とすると，$(a - a')x + (b - b')$ が g で割り切れることになるが，g の次数は 2 だから，これは $a = a'$ かつ $b = b'$ と同値である．以上により

$$S = R/Rg = \{[ax + b] \mid a, b \in R\} = \{[\overline{0}], [\overline{1}], [x], [x + \overline{1}]\}$$

となる．よって元の個数は 4 である．

(2) S における和は $[ax + b] + [a'x + b'] = [(a + a')x + (b + b')]$ で定義される．また，$(ax + b)(a'x + b')$ を g で割った余りを $cx + d$ とすれば $[ax + b][a'x + b'] = [cx + d]$ である．たとえば $[x][x + \overline{1}] = [x^2 + x] = [(x^2 + x + \overline{1}) + \overline{1}] = [\overline{1}]$. なお，$[\overline{0}]$ が S の加法に関する単位元，$[\overline{1}]$ が乗法に関する単位元である．

和	$[\overline{0}]$	$[\overline{1}]$	$[x]$	$[x + \overline{1}]$
$[\overline{0}]$	$[\overline{0}]$	$[\overline{1}]$	$[x]$	$[x + \overline{1}]$
$[\overline{1}]$	$[\overline{1}]$	$[\overline{0}]$	$[x + \overline{1}]$	$[x]$
$[x]$	$[x]$	$[x + \overline{1}]$	$[\overline{0}]$	$[\overline{1}]$
$[x + \overline{1}]$	$[x + \overline{1}]$	$[x]$	$[\overline{1}]$	$[\overline{0}]$

積	$[\overline{0}]$	$[\overline{1}]$	$[x]$	$[x + \overline{1}]$
$[\overline{0}]$	$[\overline{0}]$	$[\overline{0}]$	$[\overline{0}]$	$[\overline{0}]$
$[\overline{1}]$	$[\overline{0}]$	$[\overline{1}]$	$[x]$	$[x + \overline{1}]$
$[x]$	$[\overline{0}]$	$[x]$	$[x + \overline{1}]$	$[\overline{1}]$
$[x + \overline{1}]$	$[\overline{0}]$	$[x + \overline{1}]$	$[\overline{1}]$	$[x]$

問題 1.30 (1) $\alpha = a + bi$ $(a, b \in \mathbb{R})$ を任意の複素数とする．$f(x) = bx + a \in \mathbb{R}[x]$ とおけば $\rho(f) = bi + a = \alpha$ となるから ρ は全射である．

(2) 商を $q(x) \in \mathbb{R}[x]$ とすると $f(x) = q(x)(x^2 + 1) + ax + b$. 両辺に $x = i$ を代入して $f(i) = ai + b$.

(3) $x^2 + 1$ は $x = i$ を代入すると 0 になるから $\mathrm{Ker}\,\rho$ に属する．$\mathrm{Ker}\,\rho$ はイデアルだから $\mathbb{R}[x](x^2 + 1) \subset \mathrm{Ker}\,\rho$ が成立する．$f \in \mathrm{Ker}\,\rho$ として f を $x^2 + 1$ で割った余りを $ax + b$

$(a, b \in \mathbb{R})$ とすると，(2) より $ai + b = f(i) = \rho(f) = 0$，よって $a = b = 0$ となるから $f(x) = q(x)(x^2 + 1)$ は　$\mathbb{R}[x](x^2 + 1)$ に属する．

(4) (2) と環準同型定理より $\mathbb{R}[x]/\mathrm{Ker}\,\rho \cong \mathbb{C}$.

問題 1.31 a を R の零因子とすると $a \neq 0$ であり，$ab = 0$ かつ $b \neq 0$ を満たす $b \in R$ が存在する．一方，a が単元でもあると仮定すると，$au = 1$ を満たす $u \in R$ が存在する．このとき

$$b = 1b = (au)b = (ab)u = 0u = 0$$

となり $b \neq 0$ に矛盾する．従って a は単元ではない．

問題 1.32 (a, b) を R の零因子とする．$(a, b) \neq (0, 0)$ であり，$(a, b)(c, d) = (0, 0)$ かつ $(c, d) \neq (0, 0)$ を満たす $c, d \in \mathbb{Z}$ が存在する．このとき，$ac = bd = 0$ より $a \neq 0$ かつ $b \neq 0$ ならば $c = d = 0$ となり矛盾なので a と b のどちらか一方（のみ）が 0 である．$a \neq 0$ ならば $(a, 0)(0, 1) = (0, 0)$ より $(a, 0)$ は零因子である．$b \neq 0$ ならば $(0, b)(1, 0) = (0, 0)$ より $(0, b)$ は零因子である．以上により R の零因子は $(a, 0)$ および $(0, a)$ (a は 0 でない定数）である．

1.6　ユークリッド整域と単項イデアル整域

問題 1.33 ユークリッド整域 $\mathbb{Z}$ において命題 1.6 とユークリッドの互除法を用いる．(1.6 節の時点ではまだ素元分解の一意性を示していないし，素元分解と最大公約元の関係については授業で触れなかったので，素因数分解よりもユークリッドの互除法で最大公約数を求める方が（論理的には）よい.)

(1) $24 = 15 + 9$, $15 = 9 + 6$, $9 = 6 + 3$, $6 = 2 \times 3$ より 24 と 9 の最大公約数は 3 であるから，命題 1.6 により $24\mathbb{Z} + 15\mathbb{Z} = 3\mathbb{Z}$.

(2) $2520 = 2014 + 506$, $2014 = 3 \times 506 + 496$, $506 = 496 + 10$, $496 = 49 \times 10 + 6$, $10 = 6 + 4$, $6 = 4 + 2$, $4 = 2 \times 2$ より 2520 と 2014 の最大公約数は 2 であるから，$2014\mathbb{Z} + 2520\mathbb{Z} = 2\mathbb{Z}$.

(3) まず 3 つのうち 2 つのイデアルの和を求める．$16 = 15 + 1$ より 16 と 15 の最大公約数は 1 であるから，$15\mathbb{Z} + 36\mathbb{Z} + 16\mathbb{Z} = \mathbb{Z} + 36\mathbb{Z} = \mathbb{Z}$. あるいは，$15\mathbb{Z} + 36\mathbb{Z} = 3\mathbb{Z}$ と $3\mathbb{Z} + 16\mathbb{Z} = \mathbb{Z}$ を示してもよい.

問題 1.34 ユークリッド整域 $\mathbb{Q}[x]$ において命題 1.6 とユークリッドの互除法を用いる．$\mathbb{Q}[x]$ の単元は $\mathbb{Q}$ の 0 でない元（を 0 次多項式とみなしたもの）の全体であることに注意する.

(1) $x^3 + 1 = x(x^2 - 1) + x + 1$,　$x^2 - 1 = (x - 1)(x + 1)$ より $x^3 + 1$ と $x^2 - 1$ の最大公約元は $x + 1$ であるから $\mathbb{Q}[x](x^2 - 1) + \mathbb{Q}[x](x^3 + 1) = \mathbb{Q}[x](x + 1)$

(2)

$$x^4 + 2x^3 + x^2 - 1 = (x^4 + x^2 + 1) + 2x^3 - 2, \quad x^4 + x^2 + 1 = x(x^3 - 1) + x^2 + x + 1,$$
$$x^3 - 1 = (x - 1)(x^2 + x + 1).$$

ここで $2x^3-2=2(x^3-1)$ で 2 は $\mathbb{Q}[x]$ の単元だから, $2x^3-2$ を x^3-1 で置き換えて割り算した. よって $x^4+2x^3+x^2-1$ と x^4+x^2+1 の最大公約元は x^2+x+1 であるから,

$$\mathbb{Q}[x](x^4+x^2+1)+\mathbb{Q}[x](x^4+2x^3+x^2-1)=\mathbb{Q}[x](x^2+x+1)$$

問題 1.35 両辺を 9 で割って $442a+384b=1$ を満たす整数 a,b を求めればよい.

$$442=385+57,\quad 385=6\times 57+43,\quad 57=43+14,\quad 43=3\times 14+1$$

より

$$\begin{aligned}1&=43-3\times 14=43-3\times(57-43)=-3\times 57+4\times 43\\&=-3\times 57+4\times(385-6\times 57)=4\times 385-27\times 57\\&=4\times 385-27\times(442-385)=-27\times 442+31\times 385\end{aligned}$$

よって $a=-27$, $b=31$. （題意を満たす a,b の組は他にも無数にあるが，これが絶対値最小になる．また，3978 と 3465 に直接ユークリッドの互除法を適用してもよい.）

問題 1.36

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

より（多項式は定数で割り切れるので最後の割り算は実行しなくてよい）

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

問題 1.37 (1) $kl+qn=1$ をみたす整数 l,q が存在すれば, $\mathbb{Z}/n\mathbb{Z}$ において $\overline{kl}=\overline{1}$ が成立するから $\overline{k}$ は単元である. 逆に $\overline{k}$ が単元ならば $\overline{kl}=\overline{1}$ をみたす $l\in\mathbb{Z}$ が存在する. このとき $kl-1$ は n の倍数だから $kl-1=-qn$ すなわち $kl+qn=1$ をみたす $q\in\mathbb{Z}$ が存在する.

(2) $kl+qn=1$ をみたす $k,l\in\mathbb{Z}$ が存在することと k,l が互いに素であることは同値であるから (1) とあわせて結論を得る.

(3) $\mathbb{Z}/15\mathbb{Z}$ の単元の個数は, 0 から 15 までの整数のうち 16 と互いに素なもの $1,3,5,7,9,11,13,15$ の個数 8 である.

(4) $\mathbb{Z}/30\mathbb{Z}$ の単元の個数は, 0 から 19 までの整数のうち 30 と互いに素なもの $1,7,11,13,17,19,23,29$ の個数 8 である.

問題 1.38 (1) $e=a'b'd=b'(a'd)=b'a\in Ra$, $e=a'(b'd)=a'b\in Rb$ より e は $Ra\cap Rb$ に属するから $Re\subset Ra\cap Rb$ が従う.

(2) $Ra+Rb=Rd$ より $ua+vb=d$ を満たす $u,v\in R$ が存在する. これと $a=a'd$, $b=b'd$ より $(ua'+vb')d=d$ すなわち $(ua'+vb'-1)d=0$ を得る. R は整域だから $ua'+vb'=1$ が成立する.

(3) $c\in Ra\cap Rb$ より $c=qa=rb$ を満たす $q,r\in R$ が存在する. このとき

$$c=c(ua'+vb')=cua'+cvb'=rbua'+qavb'=rb'dua'+qa'dvb'=(ru+qv)a'b'd=(ru+qv)e$$

(4) (3) より $Ra\cap Rb\subset Re$ であるから (1) とあわせて $Ra\cap Rb=Re$ が示された.

問題 1.39 36 と 54 の最大公約数は 18 であり $36 = 2 \cdot 18$, $54 = 3 \cdot 18$ であるから, 前問の e は $e = 2 \cdot 3 \cdot 18 = 108$ である. 従って前問より $36\mathbb{Z} \cap 54\mathbb{Z} = 108\mathbb{Z}$ である.

問題 1.40 I が単項イデアルと仮定すると, ある $f \in \mathbb{Z}[x]$ によって $I = \mathbb{Z}[x]f$ となる. 2 は I に属するから $2 = q(x)f(x)$ を満たす $q(x) \in \mathbb{Z}[x]$ が存在する. よって $f(x) = d$ は 0 以外の整数であり 2 の約数だから $f(x) = \pm 1$ または $f(x) = \pm 2$ である.

(1) $f = \pm 1$ とすると, $1 \in I$ より $1 = 2a(x) + xb(x)$ となる $a(x), b(x) \in R[x]$ が存在する. $x = 0$ を代入すると $1 = 2a(0)$ は偶数となり矛盾である.

(2) $f = \pm 2$ とすると, $I \ni x = 2b(x)$ を満たす $b(x) \in \mathbb{Z}[x]$ が存在することになるが, 両辺の x の係数を比較すると 1 = 偶数となり矛盾である.

以上により I は単項イデアルではないことが示された.

問題 1.41 (1) I を R のイデアルとすると, $I \cap \mathbb{Z}$ は $\mathbb{Z}$ のイデアルであり, $\mathbb{Z}$ は PID だから, ある非負整数 m によって $I \cap R = \mathbb{Z}m$ となる. このとき $I = Rm$ が成立することを示そう. $m \in I$ より $Rm \subset I$ がわかる. $n, k \in \mathbb{Z}$, $k \geq 0$ として $\dfrac{n}{2^k} \in I$ とすると $n = 2^k \dfrac{n}{2^k} \in I \cap \mathbb{Z}$ であるから, ある整数 q があって $n = qm$ となる. 従って $\dfrac{n}{2^k} = \dfrac{q}{2^k} m \in Rm$ である. 以上により $I = Rm$ が示された.

(2) m, n を非負整数とするとき $Rm = Rn$ となるための必要十分条件は R の単元 u が存在して $n = um$ となることである. R の単元 u はある整数 k によって $u = \pm 2^k$ と表されるから, $Rm = Rn$ であるための必要十分条件は $m/n = 2^k$ となるような整数 k が存在することである. 以上により R の相異なるイデアルは $R0 = \{0\}$ と Rm (m は正の奇数) である. (m を素因数分解して 2 のべき乗を除いたもので置き換えればよい.)

問題 1.42 (1) 前問の (1) と同様に示せる.

(2) 自然数 m, n に対して $Rm = Rn$ となるための条件は m/n が R の単元, すなわち m/n を約分したとき分母と分子が奇数となることである. 従って m を素因数分解したとき 2 以外の素数のべき乗は省いても Rm は変らないから, R の相異なるイデアルは $R0 = \{0\}$ と $R2^k$ ($k = 0, 1, 2, \dots$) である.

1.7 素イデアルと極大イデアル

問題 1.43 (1) 任意の $c \in \mathbb{Z}$ に対して $I := \mathbb{Z}[x](x - c)$ は $\mathbb{Z}[x]$ の素イデアルであることを示せ.

(2) $J = \mathbb{Z}[x]x + \mathbb{Z}[x]2$ は $\mathbb{Z}[x]$ の極大イデアルであることを示せ.

(3) 任意の $c \in \mathbb{Z}$ と任意の素数 p に対して $J = \mathbb{Z}[x](x - c) + \mathbb{Z}[x]p$ は $\mathbb{Z}[x]$ の極大イデアルであることを示せ.

1.8 素元分解整域

問題 1.41 素数 $2, 3, 5, \ldots$ で順番に割ってみると，$96577 = 13 \times 17 \times 19 \times 23$ となることがわかる．ここで 13, 17, 19, 23 は素数，すなわち $\mathbb{Z}$ における既約元 (± 1 と異なる 2 つの整数の積では表せない）であることが容易にわかる．$\mathbb{Z}$ は PID（単項イデアル整域）だから定理 1.3 により UFD（一意分解整域）であり，UFD では既約元と素元は一致する（命題 1.13）から，13, 17, 19, 23 は $\mathbb{Z}$ の素元である（または例 1.25 より）．したがって上の式は 96577 の $\mathbb{Z}$ における素元分解である．

問題 1.42 $x^4 + x^2 + 1 = x^4 + 2x^2 + 1 - x^2 = (x^2 + 1) - x^2 = (x^2 + x + 1)(x^2 - x + 1)$. ここで 2 次方程式の解の公式より $x^2 \pm x + 1 = 0$ を満たす有理数 x はないことがわかるから， $x^2 \pm x + 1$ は $\mathbb{Q}[x]$ において 1 次式では割り切れない（因数定理）．従って $\mathbb{Q}[x]$ の既約元である．$\mathbb{Q}[x]$ は PID だから UFD であり，UFD では既約元と素元は一致するから，$x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1)$ は $\mathbb{Q}[x]$ における素元分解である．

解の公式により $\mathbb{C}[x]$ においては $x^2 \pm x + 1 = \left(x - \dfrac{\mp 1 + \sqrt{3}i}{2}\right)\left(x - \dfrac{\mp 1 - \sqrt{3}i}{2}\right)$ と分解できる．1 次式は単元（0 でない定数多項式）でない 2 つの元の積では表せないから $\mathbb{C}[x]$ の既約元である．$\mathbb{C}[x]$ は PID 従って UFD なので既約元は素元である．以上により

$$x^4 + x^2 + 1 = \left(x - \frac{1 + \sqrt{3}i}{2}\right)\left(x - \frac{1 + \sqrt{3}i}{2}\right)\left(x - \frac{-1 + \sqrt{3}i}{2}\right)\left(x - \frac{-1 + \sqrt{3}i}{2}\right)$$

は $\mathbb{C}[x]$ における素元分解である．

2 環上の加群

2.1 加群の定義と例

問題 2.1 (1) $0 \in N_1$ かつ $0 \in N_2$ より $0 = 0 + 0 \in N_1 + N_2$. $u_1, v_1 \in N_1$, $u_2, v_2 \in N_2$ とすると，$(u_1 + u_2) + (v_1 + v_2) = (u_1 + v_1) + (u_2 + v_2) \in N_1 + N_2$. また，任意の $a \in R$ に対して $a(u_1 + u_2) = au_1 + au_2 \in N_1 + N_2$ であるから $N_1 + N_2$ は M の部分 R 加群である．

(2) $0 \in N_1$ かつ $0 \in N_2$ より $0 \in N_1 \cap N_2$. $u, v \in N_1 \cap N_2$, $a \in R$ とすると，$u, v \in N_1$ で N_1 は M の部分 R 加群だから $u + v \in N_1$ かつ $au \in N_1$ である．同様に $u + v \in N_2$ かつ $au \in N_2$ も成立する．よって $N_1 \cap N_2$ は M の部分 R 加群である．

(3) $N := Ru_1 + \cdots + Ru_m$ とおく．$0 = 0u_1 + \cdots + 0u_m \in N$. N の 2 つの元 u と v は，ある $a_i, b_i \in R$ $(i = 1, \ldots, m)$ によって

$$u = a_1u_1 + \cdots + a_mu_m, \qquad v = b_1u_1 + \cdots + b_mu_m$$

と表されるから，任意の $a \in R$ に対して，

$$u + v = (a_1 + b_1)u_1 + \cdots + (a_m + b_m)u_m \in N, \qquad au = (aa_1)u_1 + \cdots + (aa_m)u_m \in N$$

よって N は M の部分 R 加群である．

問題 2.2 $\mathrm{Ker}\, f$ が M の部分 R 加群であることを示す．$f(0) = 0$ より $0 \in \mathrm{Ker}\, f$ である．$u, v \in \mathrm{Ker}\, f$ かつ $a \in R$ とすると，f が R 準同型であることから，

$$f(u+v) = f(u) + f(v) = 0_N + 0_N = 0_N, \qquad f(au) = af(u) = a0_N = 0_N$$

よって $u+v \in \mathrm{Ker}\, f$ かつ $au \in \mathrm{Ker}\, f$ であるから $\mathrm{Ker}\, f$ は M の部分 R 加群である．

$\mathrm{Im}\, f$ が N の部分 R 加群であることを示す．$0 = f(0) \in \mathrm{Im}\, f$ である．$u', v' \in \mathrm{Im}\, f$ とすると，ある $u, v \in M$ が存在して $u' = f(u)$, $v' = f(v)$ となる．このとき任意の $a \in R$ に対して

$$u' + v' = f(u) + f(v) = f(u+v) \in \mathrm{Im}\, f, \qquad au' = af(u) = f(au) \in \mathrm{Im}\, f$$

であるから $\mathrm{Im}\, f$ は N の部分 R 加群である．

問題 2.3 (1) f が単射なら $f(u) = 0_N$ を満たす $u \in M$ は 0_M のみである．逆に $\mathrm{Ker}\, f = \{0_M\}$ と仮定して $u, v \in M$ かつ $f(u) = f(v)$ とすると $f(u-v) = f(u) - f(v) = 0_N$ であるから $u - v \in \mathrm{Ker}\, f$ であり仮定から $u - v = 0_M$，すなわち $u = v$ となる．よって f は単射である．

(2) $u', v' \in N$ に対して $u = f^{-1}(u')$, $v' = f^{-1}(v')$ とおくと f が R 準同型であることから任意の $a \in R$ に対して

$$f(u+v) = f(u) + f(v) = u' + v', \qquad f(au) = af(u) = au'$$

よって

$$f^{-1}(u'+v') = u + v = f^{-1}(u') + f^{-1}(v'), \quad f^{-1}(au') = au = af^{-1}(u')$$

が成立するから f^{-1} は R 準同型である．

問題 2.4 $u, v \in L$ かつ $a \in R$ とすると f と g が R 準同型であることから，

$$(g \circ f)(u+v) = g(f(u+v)) = g(f(u) + f(v)) = g(f(u)) + g(f(v)) = (g \circ f)(u) + (g \circ f)(v)$$
$$(g \circ f)(au) = g(f(au)) = g(af(u)) = ag(f(u)) = a(g \circ f)(u)$$

よって $g \circ f$ は R 準同型である．

問題 2.5 (1) $a, b, k \in \mathbb{Z}$ に対して $f_n(a+b) = n(a+b) = na + nb = f_n(a) + f_n(b)$, $f_n(ka) = n(ka) = k(na) = kf_n(a)$ であるから f_n は $\mathbb{Z}$ 準同型である．

(2) $\mathrm{Im}\, f_n = \{na \mid a \in \mathbb{Z}\} = n\mathbb{Z}$ である．また $\mathrm{Ker}\, f_n = \{a \in \mathbb{Z} \mid na = 0\}$ は $n \neq 0$ ならば $\{0\}$, $n = 0$ ならば $\mathbb{Z}$ である．

(3) f_n が全射，すなわち $n\mathbb{Z} = \mathbb{Z}$ ならば $na = 1$ を満たす $a \in \mathbb{Z}$ があるから n は単元，すなわち $n = \pm 1$ でなければならない．よって f_n が全単射ならば $n = \pm 1$ である．逆に $n = \pm 1$ ならば $n\mathbb{Z} = \mathbb{Z}$ であるから f_n は全射であり，$n \neq 0$ より f_n は単射．よって f_n は全単射である．

(4) $n = f(1)$ とおくと f が $\mathbb{Z}$ 準同型であることから，任意の $k \in \mathbb{Z}$ に対して $f(k) = f(k1) = kf(1) = kn = f_n(k)$. よって $f = f_n$ である．

(5) f_n が環準同型ならば $1 = f_n(1) = n$ でなければならない．f_1 は恒等写像であるから $\mathbb{Z}$ 準同型である．よって求める条件は $n = 1$ である．

2.2 自由加群と有限生成加群

問題 2.10 (1) $0+0+0=0$ より $(0,0,0)\in M_3$ である．$(u_1,u_2,u_3),(v_1,v_2,v_3)\in M_3$, $k\in\mathbb{Z}$ とすると，

$$(u_1+v_1)+(u_2+v_2)+(u_3+v_3)=(u_1+u_2+u_3)+(v_1+v_2+v_3)=0,$$
$$ku_1+ku_2+ku_3=k(u_1+u_2+u_3)=0$$

より $(u_1,u_2,u_3)+(v_1,v_2,v_3)\in M_3$ かつ $k(u_1,u_2,u_3)\in M_3$ となる．以上により，M_3 は $\mathbb{Z}^3$ の部分 $\mathbb{Z}$ 加群である．

次に M_3 の基底を求める．$u_1+u_2+u_3=0$ より $u_3=-u_1-u_2$ だから，$(u_1,u_2,u_3)\in M_3$ ならば

$$(u_1,u_2,u_3)=(u_1,u_2,-u_1-u_2)=u_1(1,0,-1)+u_2(0,1,-1)$$

よって M_3 は $\mathbf{v}_1:=(1,0,-1)$ と $\mathbf{v}_2:=(0,1,-1)$ で生成される．$c_1,c_2\in\mathbb{Z}$ かつ $c_1\mathbf{v}_1+c_2\mathbf{v}_2=\mathbf{0}$ とすると，$(c_1,c_2,-c_1-c_2)=(0,0,0)$ より $c_1=c_2=0$ となる．よって $\mathbf{v}_1$ と $\mathbf{v}_2$ は 1 次独立でもあるから，M_3 の基底である．（基底は他にも無数にある．たとえば $(1,-1,0)$ と $(1,0,-1)$ も基底である．）

(2) **問題の訂正** $f(u_1,u_2,u_3)$ は正確には $f((u_1,u_2,u_3))$ と表すべきでした．

f が M_3 から M_3 への $\mathbb{Z}$ 準同型であることを示す．$(u_1,u_2,u_3),(v_1,v_2,v_3)\in M_3$，$k\in\mathbb{Z}$ とすると，$f((u_1,u_2,u_3))=(u_2,u_3,u_1)$ であり $u_2+u_3+u_1=0$ であるから f は M_3 から M_3 への写像である．

$$f((u_1,u_2,u_3)+(v_1,v_2,v_3))=f((u_1+v_1,u_2+v_2,u_3+v_3))=(u_2+v_2,u_3+v_3,u_1+v_1)$$
$$=(u_2,u_3,u_1)+(v_2,v_3,v_1)=f((u_1,u_2,u_3))+f((v_1,v_2,v_3)),$$
$$f(k(u_1,u_2,u_3))=f((ku_1,ku_2,ku_3))=(ku_2,ku_1,ku_3)=k(u_2,u_1,u_3)=kf((u_1,u_2,u_3))$$

よって f は $\mathbb{Z}$ 準同型である．

$f(\mathbf{v}_1)=(0,-1,1)=-\mathbf{v}_2$, $f(\mathbf{v}_2)=(1,-1,0)=\mathbf{v}_1-\mathbf{v}_2$ より $\mathbf{v}_1$ と $\mathbf{v}_2$ に関する f の行列表示は $A=\begin{pmatrix}0&1\\-1&-1\end{pmatrix}$ である．$\det A=1$ より A はユニモジュラー行列だから f は全単射である（プリント 33 ページの可換図式を参照）．

（別解） $f((u_1,u_2,u_3))=(u_2,u_3,u_1)=(0,0,0)$ ならば $(u_1,u_2,u_3)=(0,0,0)$ であるから f は単射．$(u_1,u_2,u_3)\in M_3$ に対して $f(u_3,u_1,u_2)=(u_1,u_2,u_3)$ であるから f は全射，よって全単射である．

2.5 単因子

問題 2.15

(1) $\begin{pmatrix}9 & 6 & 20\end{pmatrix} \to \begin{pmatrix}6 & 9 & 20\end{pmatrix} \to \begin{pmatrix}6 & 3 & 20\end{pmatrix} \to \begin{pmatrix}3 & 6 & 20\end{pmatrix} \to \begin{pmatrix}3 & 6 & 2\end{pmatrix} \to \begin{pmatrix}2 & 6 & 3\end{pmatrix}$
$\to \begin{pmatrix}2 & 6 & 1\end{pmatrix} \to \begin{pmatrix}1 & 6 & 2\end{pmatrix} \to \begin{pmatrix}1 & 0 & 0\end{pmatrix}$ よって単因子は 1.

(2) $\begin{pmatrix}4 & 0\\ 0 & 6\end{pmatrix} \to \begin{pmatrix}4 & -2\\ 0 & 6\end{pmatrix} \to \begin{pmatrix}-2 & 4\\ 6 & 0\end{pmatrix} \to \begin{pmatrix}-2 & 4\\ 0 & 12\end{pmatrix} \to \begin{pmatrix}-2 & 0\\ 0 & 12\end{pmatrix} \to \begin{pmatrix}2 & 0\\ 0 & 12\end{pmatrix}$
よって単因子は 2, 12.

(3) $\begin{pmatrix}3 & 5\\ 0 & 3\end{pmatrix} \to \begin{pmatrix}3 & 2\\ 0 & 3\end{pmatrix} \to \begin{pmatrix}2 & 3\\ 3 & 0\end{pmatrix} \to \begin{pmatrix}2 & 1\\ 3 & -3\end{pmatrix} \to \begin{pmatrix}1 & 2\\ -3 & 3\end{pmatrix} \to \begin{pmatrix}1 & 2\\ 0 & 9\end{pmatrix} \to \begin{pmatrix}1 & 0\\ 0 & 9\end{pmatrix}$
よって単因子は 1, 9.

(4) $\begin{pmatrix}36 & -24\\ -18 & 9\end{pmatrix} \to \begin{pmatrix}9 & -18\\ -24 & 36\end{pmatrix} \to \begin{pmatrix}9 & -18\\ -24 & 36\end{pmatrix} \to \begin{pmatrix}9 & -18\\ 3 & -18\end{pmatrix} \to \begin{pmatrix}3 & -18\\ 9 & -18\end{pmatrix}$
$\to \begin{pmatrix}3 & -18\\ 0 & 36\end{pmatrix} \to \begin{pmatrix}3 & 0\\ 0 & 36\end{pmatrix}$ よって単因子は 3, 36.

問題 2.17

(1) $\begin{pmatrix}x-1 & -1\\ 0 & x-2\end{pmatrix} \to \begin{pmatrix}-1 & x-1\\ x-2 & 0\end{pmatrix} \to \begin{pmatrix}-1 & x-1\\ 0 & (x-1)(x-2)\end{pmatrix} \to \begin{pmatrix}-1 & x-1\\ 0 & (x-1)(x-2)\end{pmatrix}$
$\to \begin{pmatrix}-1 & 0\\ 0 & (x-1)(x-2)\end{pmatrix} \to \begin{pmatrix}1 & 0\\ 0 & (x-1)(x-2)\end{pmatrix}$ よって単因子は 1, $(x-1)(x-2)$.

(2) $\begin{pmatrix}x-1 & -1\\ 0 & x-1\end{pmatrix} \to \begin{pmatrix}-1 & x-1\\ x-1 & 0\end{pmatrix} \to \begin{pmatrix}-1 & x-1\\ 0 & (x-1)^2\end{pmatrix} \to \begin{pmatrix}-1 & 0\\ 0 & (x-1)^2\end{pmatrix}$
$\to \begin{pmatrix}1 & 0\\ 0 & (x-1)^2\end{pmatrix}$ よって単因子は 1, $(x-1)^2$.

(3) $\begin{pmatrix}x-1 & 0\\ 0 & x-2\end{pmatrix} \to \begin{pmatrix}x-1 & -1\\ 0 & x-2\end{pmatrix}$
これは (1) と同じなので，単因子は 1, $(x-1)(x-2)$.

2.6 剰余加群と準同型定理

問題 2.21 問題 2.15 の (1)–(4) の各々の行列を A とする．

(1) $\mathbb{Z}$ 準同型 $A : \mathbb{Z}^3 \to \mathbb{Z}$ の核と余核を求める．A の標準形は $B = \begin{pmatrix}1 & 0 & 0\end{pmatrix}$ であり，$B : \mathbb{Z}^3 \to \mathbb{Z}$ は $B\,{}^t(x_1, x_2, x_3) = x_1$ となる．よって

$$\operatorname{Ker} B = \{(0, x_2, x_3) \mid x_2, x_3 \in \mathbb{Z}\} = \{0\} \oplus \mathbb{Z} \oplus \mathbb{Z} \simeq \mathbb{Z}^2,$$
$$\operatorname{Coker} B = \mathbb{Z}/\{x_1 \mid x_1 \in \mathbb{Z}\} = \mathbb{Z}/\mathbb{Z} = \{0\}$$

（任意の $n \in \mathbb{Z}$ に対して $n - 0 = n \in \mathbb{Z}$ より剰余加群 $\mathbb{Z}/\mathbb{Z}$ において $\overline{n} = \overline{0}$ であるから，$\mathbb{Z}/\mathbb{Z} = \{\overline{0}\}$ となる．$\overline{0}$ は加群の零元なので 0 と表した.）命題 2.12 より $\mathbb{Z}$ 加群としての同型

$$\operatorname{Ker} A \simeq \operatorname{Ker} B \simeq \mathbb{Z}^2, \qquad \operatorname{Coker} A \simeq \operatorname{Coker} B \simeq \{0\}$$

を得る．

(2) $\mathbb{Z}$ 準同型 $A : \mathbb{Z}^2 \to \mathbb{Z}^2$ の核と余核を求める．A の標準形は $B = \begin{pmatrix} 2 & 0 \\ 0 & 12 \end{pmatrix}$ であり，$B : \mathbb{Z}^2 \to \mathbb{Z}^2$ は ${}^t(x_1, x_2) = {}^t(2x_1, 12x_2)$ で

$$\begin{aligned} &\operatorname{Ker} B = \{{}^t(x_1, x_2) \mid 2x_1 = 12x_2 = 0\} = \{{}^t(0, 0)\}, \\ &\operatorname{Coker} B = (\mathbb{Z} \oplus \mathbb{Z})/\{{}^t(2x_1, 12x_2) \mid x_1, x_2 \in \mathbb{Z}\} = (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/12\mathbb{Z}) \end{aligned}$$

となる．ここで 3 と 4 は $\mathbb{Z}$ において互いに素であるから，中国剰余定理により $\mathbb{Z}/12\mathbb{Z} \simeq (\mathbb{Z}/4\mathbb{Z}) \oplus (\mathbb{Z}/3\mathbb{Z})$ と直和分解できる．よって命題 2.12 より $\mathbb{Z}$ 加群としての同型

$$\operatorname{Ker} A \simeq \operatorname{Ker} B \simeq \{0\}, \qquad \operatorname{Coker} A \simeq \operatorname{Coker} B \simeq (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/4\mathbb{Z}) \oplus (\mathbb{Z}/3\mathbb{Z})$$

を得る.（直和の順番は任意.）

(3) $\mathbb{Z}$ 準同型 $A : \mathbb{Z}^2 \to \mathbb{Z}^2$ の核と余核を求める．A の標準形は $B = \begin{pmatrix} 1 & 0 \\ 0 & 9 \end{pmatrix}$ であり，$B : \mathbb{Z}^2 \to \mathbb{Z}^2$ は ${}^t(x_1, x_2) = {}^t(x_1, 9x_2)$ となる．

$$\begin{aligned} &\operatorname{Ker} B = \{{}^t(x_1, x_2) \mid x_1 = 9x_2 = 0\} = \{{}^t(0, 0)\}, \\ &\operatorname{Coker} B = (\mathbb{Z} \oplus \mathbb{Z})/\{{}^t(x_1, 9x_2) \mid x_1, x_2 \in \mathbb{Z}\} = (\mathbb{Z}/\mathbb{Z}) \oplus (\mathbb{Z}/9\mathbb{Z}) \simeq \mathbb{Z}/9\mathbb{Z} \end{aligned}$$

となる．よって命題 2.12 より $\mathbb{Z}$ 加群としての同型

$$\operatorname{Ker} A \simeq \operatorname{Ker} B \simeq \{0\}, \qquad \operatorname{Coker} A \simeq \operatorname{Coker} B \simeq \mathbb{Z}/9\mathbb{Z}$$

を得る．($\mathbb{Z}/9\mathbb{Z}$ は直和に分解できない．)

(4) $\mathbb{Z}$ 準同型 $A : \mathbb{Z}^2 \to \mathbb{Z}^2$ の核と余核を求める．A の標準形は $B = \begin{pmatrix} 3 & 0 \\ 0 & 36 \end{pmatrix}$ であり，$B : \mathbb{Z}^2 \to \mathbb{Z}^2$ は ${}^t(x_1, x_2) = {}^t(3x_1, 36x_2)$ であり，

$$\begin{aligned} &\operatorname{Ker} B = \{{}^t(x_1, x_2) \mid 3x_1 = 36x_2 = 0\} = \{{}^t(0, 0)\}, \\ &\operatorname{Coker} B = (\mathbb{Z} \oplus \mathbb{Z})/\{{}^t(3x_1, 36x_2) \mid x_1, x_2 \in \mathbb{Z}\} = (\mathbb{Z}/3\mathbb{Z}) \oplus (\mathbb{Z}/36\mathbb{Z}) \end{aligned}$$

となる．ここで中国剰余定理により $\mathbb{Z}/36\mathbb{Z} \simeq (\mathbb{Z}/4\mathbb{Z}) \oplus (\mathbb{Z}/9\mathbb{Z})$ と直和分解できるから，命題 2.12 より $\mathbb{Z}$ 加群としての同型

$$\operatorname{Ker} A \simeq \{0\}, \qquad \operatorname{Coker} A \simeq \operatorname{Coker} B \simeq (\mathbb{Z}/3\mathbb{Z}) \oplus (\mathbb{Z}/4\mathbb{Z}) \oplus (\mathbb{Z}/9\mathbb{Z})$$

を得る.（直和の順番は任意.）

問題 2.23 問題 2.17 の (1)–(3) の各々の行列を A とする．また $R = \mathbb{Q}[x]$ とおく．

(1) R準同型 $A : R^2 \to R^2$ の核と余核を求める．A の標準形は $B = \begin{pmatrix} 1 & 0 \\ 0 & (x-1)(x-2) \end{pmatrix}$ であり，$B : R^2 \to R^2$ は $B\,{}^t(u_1, u_2) = {}^t(u_1, (x-1)(x-2)u_2)$ であるから，

$$\begin{aligned} &\operatorname{Ker} B = \{{}^t(u_1, u_2) \in R^2 \mid u_1 = (x-1)(x-2)u_2 = 0\} = \{{}^t(0,0)\}, \\ &\operatorname{Coker} B = (R \oplus R)/\{{}^t(u_1, (x-1)(x-2)u_2) \mid u_1, u_2 \in R\} \\ &= (R/R) \oplus (R/R(x-1)(x-2)) \simeq R/R(x-1)(x-2) \end{aligned}$$

となる．ここで $x-1$ と $x-2$ は R において互いに素であるから，中国剰余定理により $R/R(x-1)(x-2) \simeq (R/R(x-1)) \oplus (R/R(x-2))$ と直和分解できるから，命題 2.12 より R 加群としての同型

$$\operatorname{Ker} A \simeq \{0\}, \qquad \operatorname{Coker} A \simeq \operatorname{Coker} B \simeq (R/R(x-1)) \oplus (R/R(x-2))$$

を得る．

(2) R 準同型 $A : R^2 \to R^2$ の核と余核を求める．A の標準形は $B = \begin{pmatrix} 1 & 0 \\ 0 & (x-1)^2 \end{pmatrix}$ であり，$B : R^2 \to R^2$ は $B\,{}^t(u_1, u_2) = {}^t(u_1, (x-1)^2 u_2)$ で

$$\begin{aligned} &\operatorname{Ker} B = \{{}^t(u_1, u_2) \in R^2 \mid u_1 = (x-1)^2 u_2 = 0\} = \{{}^t(0,0)\}, \\ &\operatorname{Coker} B = (\mathbb{Z} \oplus \mathbb{Z})/\{{}^t(u_1, (x-1)^2 u_2) \mid u_1, u_2 \in R\} \\ &= (R/R) \oplus (R/R(x-1)^2) \simeq R/R(x-1)^2 \end{aligned}$$

となる．命題 2.12 より R 加群としての同型

$$\operatorname{Ker} A \simeq \{0\}, \qquad \operatorname{Coker} A \simeq \operatorname{Coker} B \simeq R/R(x-1)^2$$

を得る．

(3) (1) と同じ．