

(2011/6/16)

問 21.1 (i) (1) I, J を左イデアルとする. $I \cap J$ は R の部分加群で, 任意の $r \in R$ と $a \in I \cap J$ について, $a \in I$ より $ra \in I$ で $a \in J$ より $ra \in J$ であるから $ra \in I \cap J$ がわかり $I \cap J$ は R の左イデアルとなる. I と J に含まれる左イデアルは当然 $I \cap J$ に含まれるので, $I \cap J$ はそのような左イデアルの中で最大である. 同様に I, J が右イデアルの場合には, $I \cap J$ は I と J に含まれる最大の右イデアルとなる. I, J が両側イデアルであれば, $I \cap J$ は右イデアルかつ左イデアルであるから両側イデアルである. また当然, 両方に含まれる両側イデアルで最大となる.

(2) I, J を左イデアルとする. 部分加群の和は部分加群なので, $I + J$ は R の部分加群である. また, R の部分加群 K が I と J を含めば $I + J \subset K$ であるから, $I + J$ は I と J を含む最小の部分加群である. $r \in R$ と $a \in I, b \in J$ について $r(a + b) = ra + rb \in I + J$ より, $I + J$ は R の左イデアルである. 同様に, I, J が右イデアルであれば $I + J$ はこれらを含む最小の右イデアルであり, I, J が両側イデアルであれば $I + J$ は最小の両側イデアルとなる.

(ii) $I \cap J$ は (i), (1) により両側イデアルである. $a_1, \dots, a_n \in I, b_1, \dots, b_n \in J$ とすると, 各 i について $a_i b_i \in I \cap J$ であるから $a_1 b_1 + \dots + a_n b_n \in I \cap J$ となり, $IJ \subset I \cap J$ がわかる. IJ は定義より和について閉じており, また $a_1, \dots, a_n \in I$ なら $-a_1, \dots, -a_n \in I$ であるから, $x = a_1 b_1 + \dots + a_n b_n \in IJ$ なら $-x = (-a_1) b_1 + \dots + (-a_n) b_n \in IJ$ である. また, 任意の $r \in R$ について $ra_i \in I$ ($i = 1, \dots, n$) より $r(a_1 b_1 + \dots + a_n b_n) = (ra_1) b_1 + \dots + (ra_n) b_n \in IJ$ となる. 同様に $(a_1 b_1 + \dots + a_n b_n) r \in IJ$ も成り立つので IJ は R の両側イデアルである.

問 21.2 $I = R$ であれば $1 \in R = I$ となる. また, $1 \in I$ であれば I が左イデアルであることから, 任意の $r \in R$ について $r = r1 \in I$ となり, $I = R$ がわかる.

問 21.4 R は整域なので可換環である. $b = au$ となる元 u があれば, 任意の $r \in R$ について $rb = rua \in (a)$ となり $(b) \subset (a)$ がわかる. この u が正則元であれば両辺に u^{-1} を乗じて, $a = bu^{-1}$ であるから $(a) \subset (b)$ もわかる.

次に, $(a) = (b)$ とする. $a = 0$ なら $(a) = \{0\}$ であるから, $b = 0$ となり $u = 1$ が条件を満たす. $a \neq 0$ とする. $b \in (a)$ より $b = au$ となる $u \in R$ が存在し,

$a \in (b)$ より $a = bv$ となる $v \in R$ が存在する. このとき, $a = bv = auv$ だから $a(uv - 1) = 0$ となる. R が整域で $a \neq 0$ であるから $uv = 1$ となり, u は正則元である.

問 21.7 $\alpha = x + y\sqrt{-1}$ について $\bar{\alpha} = x - y\sqrt{-1}$ と置く. $N(\alpha) = x^2 + y^2 = \alpha\bar{\alpha}$ であるから, $N(\alpha) = 1$ であれば $\bar{\alpha}$ が α の逆元である. また, α を正則元とすると, $\alpha\beta = 1$ となる $\beta \in \mathbf{Z}[\sqrt{-1}]$ が存在するが, $1 = N(\alpha\beta) = N(\alpha)N(\beta)$ で $N(\alpha), N(\beta)$ は正の整数なので $N(\alpha) = N(\beta) = 1$ となる. $x^2 + y^2 = 1$ となる整数の組 (x, y) は $(1, 0), (-1, 0), (0, 1), (0, -1)$ の 4 つなので $\{\pm 1, \pm\sqrt{-1}\}$ が $\mathbf{Z}[\sqrt{-1}]$ の単数群となる.

問 21.8 R は $K[x]$ 上の y を変数とする多項式環と考えられるし, また $K[y]$ 上の x を変数とする多項式環とも考えられる. ある 2 変数多項式 f により $Rx + Ry = (f)$ とする. $x \in (f)$ であるが, x の y についての次数は 0 であるから f も y について 0 次である. また, $y \in (f)$ であるが, y の x についての次数は 0 であるから f も x について 0 次である. したがって, f は x についても y についても 0 次であり 0 でない定数となる. しかし $Rx + Ry$ の元の定数項は必ず 0 なので f を含まず矛盾する. したがって, $Rx + Ry$ は単項イデアルではない.

問 21.9 (i) $(m) \subset (n)$ なら $m \in (n)$ なので, ある $l \in \mathbf{Z}$ について $m = ln$ となる. したがって $n|m$ である. 逆に, $n|m$ ならある $l \in \mathbf{Z}$ について $m = ln$ であるから, 任意の $r \in \mathbf{Z}$ について $rm = rln \in (n)$ であり, $(m) \subset (n)$ となる. 後半は $m = 0$ または $n = 0$ の場合は明らかで, それ以外は前半を使って $(m) = (n) \Leftrightarrow n|m$ かつ $m|n \Leftrightarrow m = \pm n$ となる. また, この部分は \mathbf{Z} の正則元が ± 1 であることにより, 問 21.4 の解からも示される.

(ii) 最大公約数や最小公倍数という言葉は通常は正の整数だけに用いるので, ここの m, n, d, l はすべて正の整数としておく. $(m) + (n) = (d)$ なら $(m) \subset (d)$ かつ $(n) \subset (d)$ なので d は m と n の約数で, さらに正の整数 e が m, n の約数であれば $(m) \subset (e)$ かつ $(n) \subset (e)$ で $(d) = (m) + (n) \subset (e)$ となり, e は d の約数となる. したがって d は m, n の最大公約数となる. l については, $(m) \cap (n) = (l)$ より $l \in (m) \cap (n)$ であるから l は m と n の倍数である. r が m と n の倍数であれば $r \in (m) \cap (n) = (l)$ となり, r は l の倍数となる. したがって, l は m と n の最小公倍数である.

問 21.11 $G = \langle a \rangle$ で $f \in \text{Aut } G$ とすると, f により定まるある整数 $0 \leq e(f) < n$ について $f(a) = a^{e(f)}$ となる.

$$a = f^{-1}(f(a)) = f^{-1}(a^{e(f)}) = f^{-1}(a)^{e(f)} = a^{e(f^{-1})e(f)}$$

となるので $e(f^{-1})e(f) \equiv 1 \pmod{n}$ である. したがって, 任意の f について $e(f)$ の \mathbf{Z}_n での類 $\overline{e(f)}$ は $U(\mathbf{Z})$ に含まれる. よって, $\text{Aut } G$ から $U(\mathbf{Z}_n)$ への対応 $f \mapsto \overline{e(f)}$ が得られる. f は $e(f)$ で決まるので, この対応は単射である. さらに,

$$a^{e(gf)} = (gf)(a) = g(f(a)) = g(a^{e(f)}) = a^{e(g)e(f)}$$

より, $\overline{e(gf)} = \overline{e(g)e(f)}$ であり, これは群の準同型となる. また, 整数 $0 \leq e < n$ の類 \bar{e} が $U(\mathbf{Z})$ に含まれれば, $ee' \equiv 1 \pmod{n}$ となる整数 $0 \leq e' < n$ が存在する. a^e の位数は n の約数であるが, $(a^e)^m = 1$ なら $1 = (a^{em})^{e'} = a^{(ee'-1)m} a^m = a^m$ となり, a^e の位数も n である. したがって, $\langle a^e \rangle$ は位数 n の巡回群となる. よって, $a \mapsto a^e$ となる G の自己同型が存在するので, この対応の全射性もわかる. したがって, この対応は同型となる.

問 22.1 行列の成分に a, b があるので単射性は明らかである. 等式

$$(a + b\sqrt{-1})(c + d\sqrt{-1}) = ac - bd + (ad + bc)\sqrt{-1}$$

の右辺は行列の積の計算

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac - bd & ad + bc \\ -ad - bc & ac - bd \end{pmatrix}$$

の右辺に対応するので, この対応の準同型性もわかる.

問 23.8 この問題は例題 23.7 の証明の「イデアル」をすべて「左イデアル」に書き換えれば解答となる. なお, 右イデアルの場合の同様の主張は「イデアル」をすべて「右イデアル」に書き換えた上に, “ $ra \in J_\lambda \subset J$ ” の部分を “ $ar \in J_\lambda \subset J$ ” に書き換えれば証明となる.

問 24.5 $i = 1, \dots, n$ について $I_1 \cdots I_i = I_1 \cap I_2 \cap \cdots \cap I_i$ を数学的帰納法で示す. $i = 1$ なら $I_1 = I_1$ となり正しい. $i = k < n$ で正しいと仮定して $i = k + 1$ の

場合を示す. 各 $j = 1, \dots, k$ について I_j と I_{k+1} とは互いに素なので $x_j \in I_j$ と $y_j \in I_{k+1}$ が存在して $x_j + y_j = 1$ となる. このとき

$$1 - x_1 x_2 \cdots x_k = (x_1 + y_1)(x_2 + y_2) \cdots (x_k + y_k) - x_1 x_2 \cdots x_k \in I_{k+1}$$

であることが $y_1, \dots, y_k \in I_{k+1}$ に注意すればわかるので, $I_1 \cdots I_k$ と I_{k+1} は互いに素である. したがって

$$I_1 \cdots I_{k+1} = (I_1 \cdots I_k) \cap I_{k+1}$$

であり, 帰納法の仮定 $I_1 \cdots I_k = I_1 \cap \cdots \cap I_k$ を使えば右辺は $I_1 \cap I_2 \cap \cdots \cap I_{k+1}$ に等しい. よって $i = k + 1$ の場合も正しい.

問 25.2 反射律: $(a, s) \sim (a, s)$ であることは $t = 1$ とすればよい.

対称律: $(a, s) \sim (a', s')$ であれば $t \in S$ があつて $(as' - a's)t = 0$ となるので, $(a's - as')t = -(as' - a's)t = 0$ であり $(a', s') \sim (a, s)$ となる.

推移律: $(a, s) \sim (b, t)$ であれば $x \in S$ があつて $(at - bs)x = 0$ となる. また, $(b, t) \sim (c, u)$ であれば $y \in S$ があつて $(bu - ct)y = 0$ となる. このとき, $txy \in S$ で $(au - cs)txy = (at - bs)xuy + (bu - ct)ysx = 0$ であるから $(a, s) \sim (c, u)$ となる.

問 25.3 $(a, s) \sim (a', s')$ かつ $(b, t) \sim (b', t')$ のとき $(ab, st) \sim (a'b', s't')$ であることを示せばよい. 仮定から $(as' - a's)x = 0$ および $(bt' - b't)y$ となる $x, y \in S$ が存在する. このとき, $xy \in S$ で $(abs't' - a'b'st)xy = (as' - a's)xbt'y + (bt' - b't)ya'sx = 0$ であるから $(ab, st) \sim (a'b', s't')$ である.

問 25.4 結合法則: $((a/s)(b/t))(c/u) = (ab/st)(c/u) = abc/stu$ と $(a/s)((b/t)(c/u)) = (a/s)(bc/tu) = abc/stu$ の右辺が等しいので成り立つ.

分配法則: $(a/s)((b/t) + (c/u)) = (a/s)((bu + ct)/tu) = (abu + act)/stu$ と $(a/s)(b/t) + (a/s)(c/u) = (ab/st) + (ac/su) = (absu + acst)/s^2tu = (abu + act)/stu$ より成り立つ.

問 25.5 $(s/1)(1/s) = (s/s) = (1/1)$ である.

問 25.6 $S^{-1}R$ の零元は $0/1$ であるから, $a \in R$ について $a/1 = 0 = 0/1$ となることは, $(a1 - 01)s = sa = 0$ となる $s \in S$ が存在することと同値である. した

がって $\text{Ker } \phi_S = \{a \in R \mid at = 0, \exists t \in S\}$ となる. ここで S の元がすべて零因子でなければ $at = 0$ は $a = 0$ を意味する. したがって $\text{Ker } \phi_S = \{0\}$ である.

問 25.10 $a/s \in I$ とすれば, $(s/1)(a/s) = sa/s = a/1 \in I$ であり $a/1 \in \phi_S(R) \cap I$ となる. 任意の I の元が $a/s = (1/s)(a/1) \in (\phi_S(R) \cap I)(S^{-1}R)$ となるので, $I \subset (\phi_S(R) \cap I)(S^{-1}R)$ がわかる.

逆は, $\phi_S(R) \cap I \subset I$ で I が $S^{-1}R$ のイデアルであることから, $(\phi_S(R) \cap I)(S^{-1}R) \subset I$ がわかる.

問 25.14 (i) は問 25.10 において $R = \mathbf{Z}$ および $S = R \setminus (p)$ とおけばよい.

(ii) $\{0\}$ でないイデアル I について $I \cap \mathbf{Z} = (n)$ ($n > 0$) とする. $n = p^e m$ で $(n, m) = 1$ とすると, $m \in S$ であるから $p^e = (1/m)n \in I$ となり, $p^e \in (n)$ すなわち $p^e = n$ がわかる. したがって $I = (p^e)$ である.

(追加) (i) $I \cap \mathbf{Z}$ が \mathbf{Z} のイデアルあることは明らかである. これについては, 一般に $f: R \rightarrow S$ を環の準同型とすると, $I \subset S$ が左イデアルであれば $f^{-1}(I)$ は R の左イデアル, $I \subset S$ が右イデアルであれば $f^{-1}(I)$ は R の右イデアル, $I \subset S$ が両側イデアルであれば $f^{-1}(I)$ は R の両側イデアルとなる. R が S の部分環とすれば, 埋め込み写像 $R \rightarrow S$ は準同型であるから, S の左, 右, 両側イデアルと R の交わりは, それぞれ R の左, 右, 両側イデアルとなる. 特に R, S が可換環であれば S のイデアル I と R の交わりは R のイデアルである.

\mathbf{Z} は単項イデアル整域であるから, ある整数 n について $I \cap \mathbf{Z} = (n)$ となる. $n \in I$ だから $n\mathbf{Z}_{(p)} \subset I$ は成り立つ. $x = a/b$ ($a \in \mathbf{Z}, b \in \mathbf{Z} \setminus p\mathbf{Z}$) を $\mathbf{Z}_{(p)}$ の元とする. $a = bx \in I \cap \mathbf{Z} = (n)$ より $x = a(1/b) \in n\mathbf{Z}_{(p)}$ となる. よって $n\mathbf{Z}_{(p)} = I$ が成り立つ.

(ii) $\mathbf{Z}_{(p)}$ の任意のイデアルは (i) によりある整数 n について $I = n\mathbf{Z}_{(p)}$ となる. $n = 0$ であれば $I = \{0\}$ である. $n = mp^e$ ($(m, p) = 1$) と書けば, $m \in \mathbf{Z} \setminus p\mathbf{Z}$ より m は $\mathbf{Z}_{(p)}$ の正則元となる. したがって $I = n\mathbf{Z}_{(p)} = p^e\mathbf{Z}_{(p)}$ となる. $e = 0$ であれば $I = \mathbf{Z}_{(p)}$ である.

問 26.2 (i) $a|b$ とはある元 $c \in R$ について $b = ac$ となることである. $c = wp_1^{q_1} \cdots p_s^{q_s}$ とする. ここで $s \geq r$ で p_{r+1}, \dots, p_s も既約元とする. このとき, 等式 $b = ac$

から

$$vp_1^{f_1} \cdots p_s^{f_s} = uwp_1^{e_1+g_1} \cdots p_s^{e_s+g_s}$$

となる. ここで $e_{r+1} = \cdots = e_s = f_{r+1} = \cdots = f_s = 0$ としている. R が一意分解環であることから $f_i = e_i + g_i$ が $i = 1, \dots, s$ について成り立つ. e_i, f_i, g_i はすべて 0 以上の整数であるから $f_i \geq e_i$ がすべての i について成り立つ. なお, $f_{r+1} = \cdots = f_s = 0$ であるから $g_{r+1} = \cdots = g_s = 0$ となる.

逆に $f_i \geq e_i$ ($1 \leq i \leq r$) とすると, $c = u^{-1}vp_1^{f_1-e_1} \cdots p_r^{f_r-e_r}$ は R の元で $b = ac$ となっている. したがって $a|b$ である.

(ii) すべての i について $d_i \leq e_i, f_i$ となるので, (i) より $x = p_1^{d_1} \cdots p_r^{d_r}$ は a と b の約元である. $c = wp_1^{g_1} \cdots p_s^{g_s}$ を a と b の約元とすると, $s = r$ で $g_i \leq d_i$ ($i = 1, \dots, r$) でなければならず, (i) より c が x の約元であることがわかる. したがって x は a, b の最大公約元である.

すべての i について $e_i, f_i \leq m_i$ となるので, (i) より $y = p_1^{m_1} \cdots p_r^{m_r}$ は a と b の倍元である. $c = wp_1^{g_1} \cdots p_s^{g_s}$ を a と b の倍元とすると, $i = 1, \dots, r$ について $m_i \leq g_i$ でなければならず, (i) より c が y の倍元であることがわかる. したがって y は a, b の最小公倍元である.

問 26.7 (i) (1) \Rightarrow (2) $Ra_1 + \cdots + Ra_n = (d)$ とする. このとき $a_1, \dots, a_n \in (d)$ であるから d はこれらの公約元である. $e \in R$ が a_1, \dots, a_n の公約元とすると $(d) = Ra_1 + \cdots + Ra_n \subset (e)$ となる. したがって $d \in (e)$ であり, ある $f \in R$ について $d = ef$ となる. したがって d は a_1, \dots, a_n の最大公約元である.

(2) \Rightarrow (1) d が a_1, \dots, a_n の最大公約元であると仮定する. R は単項イデアル整域であるから, ある $e \in R$ について $Ra_1 + \cdots + Ra_n = (e)$ となる. (i) より e も a_1, \dots, a_n の最大公約元であるから, d と e は同伴で $Ra_1 + \cdots + Ra_n = (e) = (d)$ となる.

(ii) $f(x)$ と $g(x)$ を $K[x]$ の元とすると, $q(x) \in K[x]$ と $\deg r(x) < \deg g(x)$ を満たす $r(x) \in K[x]$ により

$$f(x) = q(x)g(x) + r(x) \tag{*}$$

と一意に書ける (定理 6.1). 一意性から明らかのように, $g(x)$ が $f(x)$ の約元となるための必要十分条件は $r(x) = 0$ となることである. また L を K

を含む体とすると, $K[x] \subset L[x]$ であるからこの表示 (*) は $L[x]$ での表示と見ることもできる. したがって $L[x]$ において $g(x)$ が $f(x)$ の約元である条件も同じ $r(x) = 0$ であり, $K[x]$ で約元であることと $L[x]$ で約元であることは同値である. 最後の主張は $L[x]$ において $f(x)$ が $g(x)$ で割り切れれば $K[x]$ の元としても割り切れるので, 商である $h(x)$ は $K[x]$ の元である. 注意として, $K[x]$ に含まれる多項式が $K[x]$ で既約であることと $L[x]$ で既約であることは一般には同値でない. 例として $x^2 + 1$ は $\mathbf{R}[x]$ では既約だが $\mathbf{C}[x]$ では $x^2 + 1 = (x - i)(x + i)$ と因数分解される.

問 26.10 等式 $f(x) = g(x)h(x)$ に補題 26.9 を適用すると $I(f) \approx I(g)I(h)$ となる. $f(x) \in R[x]$ より $I(f) \in R$ で $g(x)$ は原始的なので $I(g) \approx 1$ である. したがって $I(f) \approx I(h) \in R$ となり $h(x)$ は $R[x]$ の元である.

問 27.5 M が U を基底とする R 自由加群とする. 各 $u \in U$ について 1 つの元 u の R 自由性から, $ru = 0 \Rightarrow r = 0$ となる. したがって, 対応 $r \mapsto ru$ は単射で R 加群の同型 $R \simeq Ru$ が得られる. U が基底であることから $M = \sum_{u \in U} Ru$ であるが, M の元 x が $x = a_1u_1 + \cdots + a_nu_n = b_1u_1 + \cdots + b_nu_n$ と 2 通りに表されたとすると

$$(a_1 - b_1)u_1 + \cdots + (a_n - b_n)u_n = x - x = 0$$

となり, R 自由性から $a_i = b_i$, ($i = 1, \dots, n$) となる. したがって $M = \bigoplus_{u \in U} Ru$ である.

逆を示す. $\{u_1, \dots, u_n\}$ を U の有限部分集合とする. $r_1u_1 + \cdots + r_nu_n = 0$ とすると, 各 i について $r_iu_i \in Ru_i$ であって, 仮定から $M = \bigoplus_{u \in U} Ru$ であるからすべての i について $r_iu_i = 0$ となる. さらに $r \mapsto ru_i$ は単射であるから $r_i = 0$ となる. $M = \sum_{u \in U} Ru$ であることは $M = \bigoplus_{u \in U} Ru$ であることの条件の 1 つなので成り立つ. したがって M は U を基底とする R 自由加群である.

問 27.8 (i) $V = Ku$ として $W \subset V$ を $\{0\}$ でない K 部分加群とする. $x \in W$ を 0 でない元とする. このとき $x \in Ku$ よりある $a \in K$ について $x = au$ となる. $x \neq 0$ より $a \neq 0$ だから a^{-1} が存在し, $u = a^{-1}x \in W$ となる. これから $V = Ku \subset W$ となり $W = V$ がわかる. したがって V は単純である.

(ii) ある $i \leq r$ について $u_i \in Ku_1 + \cdots + Ku_{i-1}$ であれば $u_i = a_1u_1 + \cdots +$

$a_{i-1}u_{i-1}$ すなわち $a_1u_1 + \cdots + a_{i-1}u_{i-1} - u_i = 0$ となり u_1, \dots, u_r は線形独立でない。これで (\Rightarrow) がわかる。

(\Leftarrow) を示す。 u_1, \dots, u_r が線形独立でないとする。すべてが 0 ではないある $a_1, \dots, a_r \in K$ について $a_1u_1 + \cdots + a_ru_r = 0$ となる。ここで $a_i \neq 0$ となる最大の i をとり、等式 $a_iu_i = -a_1u_1 - \cdots - a_{i-1}u_{i-1}$ の両辺を a_i で割って

$$u_i = a_i^{-1}(-a_1u_1 - \cdots - a_{i-1}u_{i-1}) = (-a_i^{-1}a_1)u_1 + \cdots + (-a_i^{-1}a_{i-1})u_{i-1}$$

となり、右辺は $Ku_1 + \cdots + Ku_{i-1}$ に含まれる。

問 27.10 $f + g$ が R 準同型であることは

$$\begin{aligned} (x + y)(f + g) &= (x + y)f + (x + y)g = xf + yf + xg + yg \\ &= xf + xg + yf + yg = x(f + g) + y(f + g) \end{aligned}$$

と

$$(ax)(f + g) = (ax)f + (ax)g = a(xf) + a(xg) = a(xf + xg) = a(x(f + g))$$

からわかる。 $\text{Hom}_R(M, N)$ が加法群となることを示す。

可換性：任意の $f, g \in \text{Hom}_R(M, N)$ と $x \in M$ について

$$x(f + g) = xf + xg = xg + xf = x(g + f)$$

より $f + g = g + f$ が成り立つ。

結合法則： $f, g, h \in \text{Hom}_R(M, N)$ と $x \in M$ について

$$\begin{aligned} x((f + g) + h) &= x(f + g) + xh = (xf + xg) + xh = xf + (xg + xh) \\ &= xf + x(g + h) = x(f + (g + h)) \end{aligned}$$

であるから $(f + g) + h = f + (g + h)$ が成り立つ。

単位元の存在： M のすべての元を $0 \in N$ に対応させる写像を 0 と定義すれば、これは R 準同型で、任意の $f \in \text{Hom}_R(M, N)$ と $x \in M$ について

$$x(f + 0) = xf + x0 = xf + 0 = xf$$

より $f + 0 = f$ となり、 0 は単位元となる。

逆元の存在： $f \in \text{Hom}_R(M, N)$ に対して $-f$ を $x(-f) = -xf$ で定義する。
 $-f$ は R 準同型で、 $x(f + (-f)) = xf + x(-f) = xf + (-xf) = 0$ より
 $f + (-f) = 0$ となり、 $-f$ は f の逆元である。

以上で $\text{Hom}_R(M, N)$ が群となることがわかる。なお、 $f \in \text{Hom}_R(M, N)$ と
 $a \in R$ に対して $af : M \rightarrow N$ を $x(af) = a(xf)$ で定義しても、 $(bx)(af) =$
 $a((bx)f) = a(b(xf)) = (ab)(xf)$ および $b(x(af)) = b(a(xf)) = (ba)(xf)$ であ
ることから、一般には af は R 準同型にならない。したがって、 $\text{Hom}_R(M, N)$
は一般には R 加群ではない。ただし、 R が可換環の場合は af は R 準同型で
あり、 $\text{Hom}_R(M, N)$ は R 加群となる。

問 27.12 恒等写像 id_R が ${}_R R$ の単位元で $\phi(\text{id}_R) = 1\text{id}_R = 1 \in R$ である。 $\phi(f) =$
 $a, \phi(g) = b$ とする。 $1(f+g) = 1f+1g = a+b$ より $\phi(f+g) = a+b = \phi(f)+\phi(g)$
で、また $1(fg) = (1f)g = ag = (a1)g = a(1g) = ab$ より $\phi(fg) = ab =$
 $\phi(f)\phi(g)$ となるので ϕ は環準同型である。

問 28.2 (28.5) の左辺は

$$(u_i u_j) u_k = \left(\sum_{\nu} r_{ij\nu} u_{\nu} \right) u_k = \sum_{\nu} r_{ij\nu} u_{\nu} u_k = \sum_{\nu} \sum_l r_{ij\nu} r_{\nu kl} u_l$$

で、右辺は

$$u_i (u_j u_k) = u_i \left(\sum_{\nu} r_{jk\nu} u_{\nu} \right) = \sum_{\nu} r_{jk\nu} u_i u_{\nu} = \sum_{\nu} \sum_l r_{jk\nu} r_{i\nu l} u_l$$

であるから、これらが等しいのは各 l について u_l の係数が等しい場合、すな
わち等式

$$\sum_{\nu} r_{ij\nu} r_{\nu kl} = \sum_{\nu} r_{jk\nu} r_{i\nu l}$$

がすべての $1 \leq i, j, k, l \leq n$ について成り立つ場合である。

問 28.5 $1 - \sqrt{-1}i, 1 + \sqrt{-1}i$ はいずれも $Q_{\mathbf{C}}$ の 0 でない元であるが、積は

$$(1 - \sqrt{-1}i)(1 + \sqrt{-1}i) = 1 - (\sqrt{-1})^2 i^2 = 1 - (-1)(-1) = 0$$

となり、これらは零因子である。したがって $Q_{\mathbf{C}}$ は斜体ではない。

問 28.6 $Q_{\mathbf{R}}$ の元 $z = a + bi + cj + dk$ は

$$a + bi + cj + dk = a + bi + cj + dij = (a + bj) + (c + di)j \in \mathbf{C} + \mathbf{C}j$$

となる。また、 $\mathbf{C} + \mathbf{C}j$ の元 $(a + bj) + (c + di)j$ は $a + bi + cj + dk$ に等しいので、これが 0 となるのは $a + bj = c + di = 0$ の場合であり、 $Q_{\mathbf{R}} = \mathbf{C} \oplus \mathbf{C}j$ となることがわかる。

$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $i = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, $j = \begin{bmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{bmatrix}$, $k = \begin{bmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{bmatrix}$ とおけば、右の集合は $1, i, j, k$ を基底とする \mathbf{R} ベクトル空間で、等式 $i^2 = j^2 = k^2 = -1$, $ij = k, jk = i, ki = j, ji = -k, kj = -i, ik = -j$ が成り立つので、これは $Q_{\mathbf{R}}$ に同型な $M(2, \mathbf{C})$ の部分環である。

問 29.10 $I \subset S^{-1}R$ をイデアルとすると、 $I' = I \cap R$ は R のイデアルで $I'S^{-1}R = I$ である。ここで、自然な準同型 $\phi: R \rightarrow S^{-1}R$ が単射でない場合も、 $\phi^{-1}(I)$ を $I \cap R$ と書いている。 I_1, I_2, I_3, \dots を $S^{-1}R$ のイデアルの昇鎖 (あるいは降鎖) とすると、 I'_1, I'_2, I'_3, \dots は R の昇鎖 (あるいは降鎖) となり、 R がネーター環 (あるいはアルチン環) とすると、ある n について $I'_n = I'_{n+1} = I'_{n+2} = \dots$ となる。このとき、最初に注意したことから $I_n = I_{n+1} = I_{n+2} = \dots$ となるので、 $S^{-1}R$ はネーター環 (あるいはアルチン環) となる。

問 29.13 $K[x]$ のイデアルの列

$$K[x] \supset xK[x] \supset x^2K[x] \supset x^3K[x] \supset \dots$$

は降鎖で、すべての i について $x^i \in x^iK[x] \setminus x^{i+1}K[x]$ より $x^iK[x] \neq x^{i+1}K[x]$ であるから、 $K[x]$ はアルチン環ではない。

問 30.2 $\{v_1, \dots, v_n\}$ が F の基底であれば各 j について $u_j = \sum_k b_{jk}v_k$ と書ける。このとき等式

$$v_i = \sum_j a_{ij}u_j = \sum_j \sum_k a_{ij}b_{jk}v_k$$

と、 $\{v_1, \dots, v_n\}$ の 1 次独立性より各 i, k について $\sum_j a_{ij}b_{jk} = \delta_{ik}$ であり、 $[a_{ij}][b_{jk}] = I_n$ となる。両辺の行列式を考えると $\det[a_{ij}]\det[b_{jk}] = 1$ であるから、 $[a_{ij}]$ は正則行列である。

逆に、 $[a_{ij}]$ が正則行列であれば $[a_{ij}][b_{jk}] = I_n$ となる逆行列 $[b_{jk}]$ が存在する。このとき $[b_{ki}][a_{ij}] = I_n$ も成り立つので、

$$\sum_i b_{ki}v_i = \sum_i \sum_j b_{ki}a_{ij}u_j = u_k$$

となり, F は $\{v_1, \dots, v_n\}$ で生成される. また, $\sum_i c_i v_i = 0$ とすると, $0 = \sum_i c_i v_i = \sum_i \sum_j c_i a_{ij} u_j$ で $\{u_1, \dots, u_n\}$ が F の基底であるから, $\sum_i c_i a_{ij} = 0$ ($j = 1, \dots, n$) となる. これから $c_k = \sum_j b_{jk} (\sum_i c_i a_{ij}) = 0$ ($k = 1, \dots, n$) がわかり, $\{v_1, \dots, v_n\}$ の 1 次独立性も示される.

問 30.7 M にトーションがなければ定理 30.5 により M は $R \oplus \dots \oplus R$ の形となり R 自由である. 逆に M が自由加群であれば $R \oplus \dots \oplus R$ の形の加群で, M の 0 でない元はどれかの成分が 0 でなく, R が整域であることから 0 でない元をかけてもその成分は 0 にならない. したがって $T(M) = \{0\}$ である.