代数入門問題集 [20070702]

3 環

断りのない限り、環は単位元をもつとは仮定しない。

1. 整域が有限集合であるならば、それは体であることを示せ。
2. 環 R の元 a が**べき等元**であるとは $a^2 = a$ となることである。単位元 1 をもつ環 R において a がべき等元であるならば $1 - a$ もべき等元であることを示せ。
3. 環 R の元 a が**べき零元**であるとは、ある自然数 n に対して $a^n = 0$ となることである。単位元 1 をもつ環 R において a がべき零元であるならば $1 - a$ は正則元であることを示せ。
4. R を環とし a, b は R のべき零元で $ab = ba$ を満たすものとする。このとき $a + b$ もべき零元であることを示せ。
5. R を環とし 任意の $a \in R$ に対して $a^2 = a$ が成り立つとする。このとき、任意の $a \in R$ に対して $2a = 0$ であることを示せ。(このような環を**ブール環**という。)
6. 有理整数環 $\mathbb{Z}$ の剰余環 $\mathbb{Z}/12\mathbb{Z}$ の正則元、零因子、べき零元をそれぞれ求めよ。
7. 有理整数環 $\mathbb{Z}$ の剰余環 $\mathbb{Z}/6\mathbb{Z}$ を考える。$a + 6\mathbb{Z}$ を $\overline{a}$ と書くことにする。
   (1) $S = \{\overline{0}, \overline{2}, \overline{4}\}$ は $\mathbb{Z}/6\mathbb{Z}$ の部分環であることを確認せよ。
   (2) S が単位元をもつかどうかを調べよ。
8. n を自然数とし有理整数環 $\mathbb{Z}$ の剰余環 $\mathbb{Z}/n\mathbb{Z}$ を考える。
   (1) $\mathbb{Z}/n\mathbb{Z}$ の零因子を決定せよ。
   (2) $\mathbb{Z}/n\mathbb{Z}$ の正則元を決定せよ。
   (3) $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ を $f(a + n\mathbb{Z}) = a + m\mathbb{Z}$ で定めたい。f が写像になるための m, n に関する必要十分条件を求めよ。
   (4) (3) の写像 $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ が定義されているとする。このとき $f((a+n\mathbb{Z})+(b+n\mathbb{Z})) = f(a+n\mathbb{Z})+f(b+n\mathbb{Z})$, $f((a + n\mathbb{Z})(b + n\mathbb{Z})) = f(a + n\mathbb{Z})f(b + n\mathbb{Z})$ が成り立つことを確認せよ。
   (5) $n = \ell m$ で ℓ と m が互いに素であるとする。このとき写像 $g : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ を $g(a + n\mathbb{Z}) = (a + \ell\mathbb{Z}, a + m\mathbb{Z})$ で定めれば、これは全単射であることを示せ。(これを**中国剰余定理**という)。
   (6) $\mathbb{Z}/n\mathbb{Z}$ の正則元の個数を $\varphi(n)$ と書く。$n = \ell m$ で ℓ と m が互いに素であるならば $\varphi(n) = \varphi(\ell)\varphi(m)$ が成り立つことを示せ。(φ を**オイラー関数**という。)
   (7) 素数 p と自然数 a に対して $\varphi(p^a)$ を求めよ。
   (8) $n = \sum_{m|n} \varphi(m)$ が成り立つことを示せ。
9. 1357 と 2468 の最大公約数を求めよ。
10. $28x + 15y = 1$ となる整数の組 (x, y) を求めよ。
11. 15 で割ると 1 余り、28 で割ると 9 余る最小の自然数を求めよ。
12. 自然数 m, n に対して、その最大公約数を d、最小公倍数を ℓ とする。このとき $mn = d\ell$ であることを示せ。
13. p を素数とするとき、p で割り切れない任意の自然数 a に対して $a^{p-1} \equiv 1 \pmod{p}$ が成り立つことを示せ。(これを**ファルマーの小定理**という)。
14. n を自然数とするとき、n と互いに素な自然数 a に対して $a^{\varphi(n)} \equiv 1 \pmod{n}$ が成り立つことを示せ。ただし $\varphi(n)$ はオイラー関数とする。
15. p を素数とするとき $(p-1)! \equiv -1 \pmod{p}$ であることを示せ。(これを**ウィルソンの定理**という)。
16. R を可換環とし $r \in R$ とする。$(r) = \{ar \mid a \in R\}$ とおくと、これは R のイデアルであることを示せ。(このようなイデアルを**単項イデアル**という。)
17. すべてのイデアルが単項イデアルである整域を**単項イデアル整域**という。有理整数環 $\mathbb{Z}$ は単項イデアル整域であることを示せ。

18. R を整域とする。$a, b \in R$ に対して $(a) = (b)$ であることと、ある正則元 e が存在して $b = ae$ となることは同値であることを示せ。(このとき a と b は**同伴**であるという。)

19. R を環とし I, J を R のイデアルとする。$\{ij \mid i \in I,\ j \in J\}$ は R のイデアルとは限らない。このような例を具体的に一つ構成せよ。

20. R を環とし I, J を R のイデアルとする。$\{ij \mid i \in I,\ j \in J\}$ の元の有限個の和の全体を IJ と書く。このとき IJ は R のイデアルであることを示せ。

21. $\mathbb{C}$ 上 2 次全行列環 $M_2(\mathbb{C})$ の部分集合で以下のようなものを考える。

$$R = \begin{pmatrix} \mathbb{R} & \mathbb{C} \\ 0 & \mathbb{R} \end{pmatrix} = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \;\middle|\; a \in \mathbb{R},\ b \in \mathbb{C},\ c \in \mathbb{R} \right\}$$

以下では同様の記号を用いる。

(1) R は $M_2(\mathbb{C})$ の部分環であることを示せ。

(2) 以下の集合が $M_2(\mathbb{C})$ の部分環であるかどうかを判定せよ。

$$\begin{pmatrix} \mathbb{Q} & \mathbb{R} \\ 0 & \mathbb{Q} \end{pmatrix}, \begin{pmatrix} \mathbb{Q} & 0 \\ \mathbb{R} & \mathbb{R} \end{pmatrix}, \begin{pmatrix} \mathbb{R} & \mathbb{Q} \\ 0 & \mathbb{R} \end{pmatrix}, \begin{pmatrix} \mathbb{R} & \mathbb{R} \\ \mathbb{R} & 0 \end{pmatrix}, \begin{pmatrix} \mathbb{R} & \mathbb{Q} \\ \mathbb{Q} & \mathbb{R} \end{pmatrix}, \begin{pmatrix} \mathbb{R} & 0 \\ \mathbb{C} & \mathbb{Q} \end{pmatrix}$$

22. 実数 a, b, c, d に対して

$$M(a,b,c,d) = \begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix}$$

とおき、$\mathbb{H} = \{M(a,b,c,d) \mid a, b, c, d \in \mathbb{R}\}$ とする。

(1) $\mathbb{H}$ は全行列環 $M_4(\mathbb{R})$ の非可換な部分環であることを示せ。

(2) $M(a,b,c,d)M(a,-b,-c,-d)$ を計算せよ。

(3) $\mathbb{H}$ は斜体であることを示せ。($\mathbb{H}$ を**ハミルトンの四元数体**という。)

23. 全行列環 $M_4(\mathbb{C})$ の元 A を

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

とおく。

(1) A^2, A^3, $\cdots$ を求めよ。

(2) $R = \{a_0E + a_1A + a_2A^2 + a_3A^3 \mid a_0, a_1, a_2, a_3 \in \mathbb{C}\}$ とおくと R は $M_4(\mathbb{C})$ の可換な部分環であることを示せ。ただし E は単位行列とする。

(3) R の正則元、べき零元を決定せよ。

24. R を環とし $Z(R) = \{r \in R \mid$ 任意の $a \in R$ に対して $ar = ra\}$ とおく。このとき $Z(R)$ は R の部分環であることを示せ。($Z(R)$ を R の**中心**という。)

25. R を $\mathbb{C}$ 上 2 次全行列環 $M_2(\mathbb{C})$ とする。また E_{ij} で (i,j)-成分のみが 1 で他の成分がすべて 0 である R の元を表すことにする。

(1) E_{ij} で生成される R の右イデアル、すなわち $E_{ij}R$ を求めよ。

(2) E_{ij} で生成される R の左イデアル、すなわち RE_{ij} を求めよ。

(3) E_{ij} で生成される R の (両側) イデアル、すなわち $RE_{ij}R$ を求めよ。

(4) R のイデアルは 0 と R 以外にないことを示せ。(0 と自分自身以外にイデアルをもたない環を**単純環**という。)

26. K を体 (例えば $\mathbb{C}$) とする。K 上 n 次全行列環 $M_n(K)$ は単純環であることを示せ。

27. R を単位元 1 をもつ環とし、I をそのイデアルとする。このとき $1 \in I$ であることと $R = I$ であることは同値である。これを証明せよ。

28. R を環とし I, J を R の右イデアルとする。

(1) $I \cap J$ は I と J の両方に含まれる右イデアルで、そのような右イデアルのうち最大のものであることを示せ。

(2) $I + J = \{i + j \mid i \in I,\ j \in J\}$ は I と J の両方を含む右イデアルで、そのような右イデアルのうち最小のものであることを示せ。

29. S を既約分数で表したときに分母が奇数となる有理数全体の集合とする。ただし整数 a は $a/1$ として S の元であるとする。

(1) S は $\mathbb{Q}$ の部分環であることを示せ。

(2) S のイデアルをすべて決定せよ。

(3) S は単項イデアル整域 (問 17 参照) であることを示せ。

30. A を (加法を演算とする) アーベル群とする。写像 $f : A \to A$ で、任意の $a, b \in A$ に対して $f(a + b) = f(a) + f(b)$ となるものを A の**自己準同型**といい、その全体の集合を $\mathrm{End}(A)$ と書く。

(1) $f, g \in \mathrm{End}(A)$ に対して

$$(f + g)(a) = f(a) + g(a), \quad (fg)(a) = f(g(a))$$

で、$\mathrm{End}(A)$ に矛盾なく和と積が定まることを示せ。

(2) $\mathrm{End}(A)$ は単位元をもつ環になることを示せ。(これを A の**自己準同型環**という。)

代数入門問題集・解答例と解説 [20070702]

3 環

1. R を整域とし $|R| < \infty$ とする。R の 0 でない任意の元が正則であることを示せばよい。$0 \neq a \in R$ とする。$f : R \to R$ を $f(r) = ar$ で定める。R が整域なので f は単射である。$|R| < \infty$ なので f は全単射となる。よって $1 = f(b) = ab$ となる $b \in R$ が存在し、R は体である。

2. $(1-a)^2 = 1 - 2a + a^2 = 1 - a$ である。

3. $a^n = 0$ とする。このとき

$$(1-a)(1+a+a^2+\cdots+a^{n-1}) = (1+a+a^2+\cdots+a^{n-1})(1-a) = 1-a^n = 1$$

であるから $1-a$ は正則元である。

4. $a^m = 0$, $b^n = 0$ $(m, n \in \mathbb{N})$ とする。このとき $ab = ba$ より

$$(a+b)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} a^i b^{m+n-i}$$

である。右辺の各項について、$i \geq m$ ならば $a^i = 0$ であり、$i < m$ ならば $m+n-i \geq n$ より $b^{m+n-i} = 0$ である。よってこの和は 0 となり $a+b$ はべき零である。

5. $2a = (2a)^2 = 4a^2 = 4a$ であるから、$2a = 0$ である。

6. $a + 12\mathbb{Z}$ を $\overline{a}$ と書くことにする。正則元は $\{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$、零因子は $\{\overline{0}, \overline{2}, \overline{3}, \overline{4}, \overline{6}, \overline{8}, \overline{9}, \overline{10}\}$、べき零元は $\{\overline{0}, \overline{6}\}$ である。

7. (1) $a, b \in S$ に対して $a - b \in S$, $ab \in S$ が確認できるので部分環である。
   (2) $\overline{04} = \overline{0}$, $\overline{24} = \overline{2}$, $\overline{44} = \overline{4}$ より、$\overline{4}$ が単位元であることが分かる。($\mathbb{Z}/6\mathbb{Z}$ の単位元とは一致しない。)

8. (1) $a + n\mathbb{Z}$ を考える。$\gcd(a, n) = d$ とする。$d > 1$ ならば $a = a'd$, $n = n'd$ とおけば $(a+n\mathbb{Z})(n'+n\mathbb{Z}) = an' + n\mathbb{Z} = a'n + n\mathbb{Z} = 0 + n\mathbb{Z}$ であるから a は零因子である。$d = 1$ のとき $b \in \mathbb{Z}$ に対して $ab + n\mathbb{Z} = 0 + n\mathbb{Z}$ であるならば $ab \in n\mathbb{Z}$ であり、$b \in n\mathbb{Z}$ である。これは $a + n\mathbb{Z}$ が $\mathbb{Z}/n\mathbb{Z}$ で零因子でないことを意味する。
   よって $a + n\mathbb{Z}$ が $\mathbb{Z}/n\mathbb{Z}$ の零因子であるための必要十分条件は $\gcd(a, n) > 1$ となることである。
   (2) 零因子は正則ではないので $\gcd(a, n) = 1$ とする。このとき $ax + bn = 1$ となる整数の組 (x, y) が存在する。これは $b + n\mathbb{Z}$ が $a + n\mathbb{Z}$ の逆元であることを意味し、したがって $a + n\mathbb{Z}$ は正則元である。よって $a + n\mathbb{Z}$ が $\mathbb{Z}/n\mathbb{Z}$ の正則元であるための必要十分条件は $\gcd(a, n) = 1$ となることである。
   (3) 次の同値な言いかえを考える。

   f は写像である。
   $\Leftrightarrow$ $a, b \in \mathbb{Z}$ に対して $a + n\mathbb{Z} = b + n\mathbb{Z}$ ならば $f(a + n\mathbb{Z}) = f(b + n\mathbb{Z})$。
   $\Leftrightarrow$ $a, b \in \mathbb{Z}$ に対して $a + n\mathbb{Z} = b + n\mathbb{Z}$ ならば $a + m\mathbb{Z} = b + m\mathbb{Z}$。
   $\Leftrightarrow$ $a, b \in \mathbb{Z}$ に対して $a - b \in n\mathbb{Z}$ ならば $a - b \in m\mathbb{Z}$。
   $\Leftrightarrow$ $\ell \in \mathbb{Z}$ に対して $\ell \in n\mathbb{Z}$ ならば $\ell \in m\mathbb{Z}$。
   $\Leftrightarrow$ n は m の約数である。

   よって f が写像であるための必要十分条件は n が m の約数であることである。
   (4) $f((a+n\mathbb{Z}) + (b+n\mathbb{Z})) = f((a+b)+n\mathbb{Z}) = (a+b) + m\mathbb{Z} = (a+m\mathbb{Z}) + (b+m\mathbb{Z}) = f(a+n\mathbb{Z}) + f(b+n\mathbb{Z})$ である。同様に $f((a+n\mathbb{Z})(b+n\mathbb{Z})) = f(ab+n\mathbb{Z}) = ab + m\mathbb{Z} = (a+m\mathbb{Z})(b+m\mathbb{Z}) = f(a+n\mathbb{Z})f(b+n\mathbb{Z})$ である。
   (5) $|\mathbb{Z}/n\mathbb{Z}| = n$, $|\mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}| = \ell m = n$ であるから g が単射であることを示せばよい。$g(a+n\mathbb{Z}) = g(a'+n\mathbb{Z})$ とすると $a + \ell\mathbb{Z} = a' + \ell\mathbb{Z}$ かつ $a + m\mathbb{Z} = a' + m\mathbb{Z}$ である。このとき $a - a'$ は ℓ と m の公倍数となるが ℓ と m は互いに素なので $\ell m = n$ の倍数となる。よって $a + n\mathbb{Z} = a' + n\mathbb{Z}$ であり、g は単射である。
   (6) $a \in \mathbb{Z}$ について、次の同値な言いかえができる。

   $a + n\mathbb{Z}$ は $\mathbb{Z}/n\mathbb{Z}$ の正則元である。
   $\Leftrightarrow$ $\gcd(a, n) = 1$
   $\Leftrightarrow$ $\gcd(a, \ell) = \gcd(a, m) = 1$
   $\Leftrightarrow$ $a + \ell\mathbb{Z}$ は $\mathbb{Z}/\ell\mathbb{Z}$ の正則元であり、$a + m\mathbb{Z}$ は $\mathbb{Z}/m\mathbb{Z}$ の正則元である。

これにより (4) の全単射で $\mathbb{Z}/n\mathbb{Z}$ の正則元と対応するのは、$\mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ の元で $\mathbb{Z}/\ell\mathbb{Z}$ の正則元と $\mathbb{Z}/m\mathbb{Z}$ の正則元を組み合わせたものであり、かつそのようなものに限る。したがってその個数について $\varphi(n) = \varphi(\ell)\varphi(m)$ が成り立つ。

(7) $0 \leq x < p^a$ なる x で p^a と互いに素でない数は p の倍数なので、その個数は p^{a-1} である。よって p^a と素なものの個数は $\varphi(p^a) = p^a - p^{a-1} = p(p^{a-1} - 1)$ である。

(8) $A = \{0, 1, \cdots, n-1\}$ とおく。また自然数 m に対して $A_m = \{x \in A \mid \gcd(x, n) = m\}$ とおく。任意の整数 x に対して $\gcd(x, n)$ は n の約数だから、A は

$$A = \bigcup_{m|n} A_m$$

と共通部分のない和に分解される。

$m \mid n$ とし $n = n'm$ とおく。m の倍数 x に対して $x = x'm$ とおくと、$\gcd(x, n) = m$ であることと $\gcd(x', n') = 1$ であることは同値である。よって A_m に含まれる元の数は $\{0, 1, \cdots, n/m - 1\}$ の元で $n' = n/m$ と互いに素なものの数、すなわち $\varphi(n/m)$ に等しい。

m が n の約数すべてを動けば n/m も n の約数すべてを動くことに注意すれば $n = \sum_{m|n} \varphi(m)$ が得られる。

9. **ユークリッドの互除法**による。

$$\begin{aligned} 2468 &= 1 \times 1357 + 1111 \\ 1357 &= 1 \times 1111 + 246 \\ 1111 &= 4 \times 246 + 127 \\ 246 &= 1 \times 127 + 119 \\ 127 &= 1 \times 119 + 8 \\ 119 &= 14 \times 8 + 7 \\ 8 &= 1 \times 7 + 1 \end{aligned}$$

よって最大公約数は 1 である。

10. ユークリッドの互除法を行う。

$$\begin{aligned} 28 &= 1 \times 15 + 13 \\ 15 &= 1 \times 13 + 2 \\ 13 &= 6 \times 2 + 1 \end{aligned}$$

それぞれ書き換えると

$$\begin{aligned} 13 &= 28 - 1 \times 15 \\ 2 &= 15 - 1 \times 13 = 15 - 1 \times (28 - 1 \times 15) = -1 \times 28 + 2 \times 15 \\ 1 &= 13 - 6 \times 2 = (28 - 1 \times 15) - 6 \times (-1 \times 28 + 2 \times 15) = 7 \times 28 - 13 \times 15 \end{aligned}$$

よって $(x, y) = (7, -13)$ が条件を満たす。

11. 121

(28n + 9 を n を動かして順に 15 で割ってみる。)

12. m, n の素因数分解を、それぞれ

$$\begin{aligned} m &= {p_1}^{e_1} \cdots {p_r}^{e_r} \\ n &= {p_1}^{f_1} \cdots {p_r}^{f_r} \end{aligned}$$

とする。ただし、一方にしか現れない素数については、その指数を 0 として、他方にも補っておく。このとき

$$\begin{aligned} d &= {p_1}^{\min\{e_1, f_1\}} \cdots p_r^{\min\{e_r, f_r\}} \\ \ell &= {p_1}^{\max\{e_1, f_1\}} \cdots p_r^{\max\{e_r, f_r\}} \end{aligned}$$

である。したがって $mn = d\ell$ が成り立つ。

13. p が素数ならば $\mathbb{Z}/p\mathbb{Z}$ は体である。よって、その単数群は $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/p\mathbb{Z} - \{\overline{0}\}$ でその位数は $p - 1$ である。したがって $\overline{a} \neq \overline{0}$ ならば $\overline{a}^{p-1} = \overline{1}$ が成り立ち、これは $a^{p-1} \equiv 1 \pmod{p}$ が成り立つことを意味する。

14. $\mathbb{Z}/n\mathbb{Z}$ の単数群の位数は $\varphi(n)$ なので、問 13 と同様に n と互いに素な自然数 a に対して $a^{\varphi(n)} \equiv 1 \pmod{n}$ が成り立つ。

15. $p = 2$ のときは明らかなので $p > 2$ とする。p が素数なので $\mathbb{Z}/p\mathbb{Z}$ は体である。その単数群は $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/p\mathbb{Z} - \{\overline{0}\}$ で $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$ に対して $\overline{a}\overline{b} = \overline{1}$ となる $\overline{b}$ がただ一つ定まる。§?? 問 ?? より $\overline{a} = \overline{b}$、すなわち $\overline{a}^2 = \overline{1}$ となるのは $\overline{1}$, $\overline{-1}$ のみである。よって $(\mathbb{Z}/p\mathbb{Z})^\times$ の元すべての積は $\overline{-1}$ となり、これは $(p-1)! \equiv -1 \pmod{p}$ を意味する。

16. R は可換環なので (r) がイデアルであることをいうには

- $i, j \in (r)$ ならば $i - j \in (r)$
- $i \in (r)$, $x \in R$ ならば $xi \in (r)$

を示せばよい。

$i, j \in (r)$ とする。ある $a, b \in R$ があって $i = ar$, $j = br$ である。このとき $i - j = ar - br = (a-b)r \in (r)$ となる。

$i \in (r)$, $x \in R$ とする。ある $a \in R$ があって $i = ar$ である。このとき $xi = x(ar) = (xa)r \in (r)$ である。

よって (r) は R のイデアルである。

17. I を $\mathbb{Z}$ のイデアルとする。$I = 0 (= \{0\})$ ならば $I = 0\mathbb{Z}$ で、これは単項イデアルなので $I \neq 0$ とする。このとき I は 0 でない元 a を含む。$a \in I$ ならば $-a \in I$ でもあるので、$a > 0$ としてよい。すなわち I は正の整数、すなわち自然数を含む。自然数は整列集合なので、I に含まれる自然数のうち、最小なものが存在する。これを n とおく。$I = (n)$ であることを示す。任意の $a \in \mathbb{Z}$ に対して $an \in I$ なので $(n) \subset I$ が成り立つ。$m \in I$ とする。

$$m = nq + r, \quad 0 \leq r < n$$

なる整数 q, r が存在する。このとき $m \in I$, $nq \in I$ より $r = m - nq \in I$ であり、n の最小性より $r = 0$ である。よって $m \in (n)$ となり $I \subset (n)$ である。以上より $I = (n)$ が成り立ち、任意のイデアルは単項イデアルであることが分かる。

18.
- 正則元 e が存在して $b = ae$ であるとする。このとき $b = ae \in (a)$ であり、よって任意の $x \in R$ に対して $bx \in (a)$ である。よって $(b) \subset (a)$ が成り立つ。e が正則なので $a = be^{-1}$ に同様の議論を行えば $(a) \subset (b)$ が成り立つ。よってこのとき $(a) = (b)$ である。
- $(a) = (b)$ とする。$a \in (b)$, $b \in (a)$ となるので、ある $x, y \in R$ が存在して $a = bx$, $b = ay$ となる。$a = 0$ と $b = 0$ は同値であり、このとき $b = a1$ となる。よって $a \neq 0$, $b \neq 0$ とする。このとき $a = bx = axy$ なので $a(1 - xy)$ である。$a \neq 0$ で R が整域なので $1 - xy = 0$、すなわち $xy = 1$ である。したがって $a = bx$ で x は正則元でである。

19. K を体 (例えば複素数体 $\mathbb{C}$) とし、4 変数多項式環 $R = K[x, y, z, u]$ を考える。R の元で、定数項が 0 であるものの全体の集合を I とすれば、これは R のイデアルである。$M = \{ij \mid i,\ j \in I\}$ とする。このとき x, y, z, $u \in I$ であるから xy, $zu \in M$ である。しかし $xy + zu$ は積に分解することはできず、よって $xy + zu \notin M$ である。したがって M は R のイデアルではない。

20. $x, y \in IJ$ とすると

$$x = \sum_{\alpha \in A} i_\alpha j_\alpha, \quad y = \sum_{\beta \in B} i_\beta j_\beta$$

$(|A| < \infty, |B| < \infty, i_\alpha, i_\beta \in I, j_\alpha, j_\beta \in J)$ と書くことができる。このとき $x - y$ はやはり $\{ij \mid i \in I,\ j \in J\}$ の元の有限個の和になるので IJ に含まれる。

$x \in IJ$, $r \in R$ とする。$x = \sum_{\alpha \in A} i_\alpha j_\alpha$ $(|A| < \infty, i_\alpha \in I, j_\alpha \in J)$ と書くことができる。このとき

$$rx = \sum_{\alpha \in A} (ri_\alpha) j_\alpha, \quad xr = \sum_{\alpha \in A} i_\alpha (j_\alpha r)$$

であり $ri_\alpha \in I$, $j_\alpha r \in J$ であるから、rx, xr はやはり IJ に含まれる。

よって IJ は R のイデアルである。

21. (1) $x = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$, $y = \begin{pmatrix} d & e \\ 0 & f \end{pmatrix} \in R$ とする。$a, c, d, f \in \mathbb{R}$, $b, e \in \mathbb{C}$ である。このとき

$$x - y = \begin{pmatrix} a-d & b-e \\ 0 & c-f \end{pmatrix}, \quad xy = \begin{pmatrix} ad & ae+bf \\ 0 & cf \end{pmatrix}$$

である。$a-d$, $c-f$, ad, $cf \in \mathbb{R}$ であり、他の成分は $\mathbb{C}$ に入るから $x-y$, $xy \in R$ である。よって R は $M_2(\mathbb{C})$ の部分環である。

(2) 順番に ○○××××○。

22. (1) $M(a,b,c,d)-M(a',b',c',d')=M(a-a',b-b',c-c',d-d')\in\mathbb{H}$ である。また $M(a,b,c,d)M(a',b',c',d')=M(aa'-bb'-cc'-dd',\ ab'+ba'+cd'-dc',\ ac'-bd'+ca'+db',\ ad'+bc'-cb'+da')\in\mathbb{H}$ である。よって $\mathbb{H}$ は $M_4(\mathbb{R})$ の部分環である。$M(1,0,0,0)$ が単位元、$M(0,0,0,0)$ が零元であることもすぐに分かる。

(2) $M(a,b,c,d)M(a,-b,-c,-d)=(a^2+b^2+c^2+d^2)M(1,0,0,0)$

(3) $M(a,b,c,d)\neq M(0,0,0,0)$ のとき $a^2+b^2+c^2+d^2\neq 0$ で、(2) より $M(a,b,c,d)(M(a,-b,-c,-d)/(a^2+b^2+c^2+d^2)=M(1,0,0,0)$ となる。よって $\mathbb{H}$ の 0 でない元は正則元となり $\mathbb{H}$ は斜体である。

23. (1)
$$A^2=\begin{pmatrix}0&0&1&0\\0&0&0&1\\0&0&0&0\\0&0&0&0\end{pmatrix},\quad A^3=\begin{pmatrix}0&0&0&1\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix},\quad A^\ell=0\quad(\ell\geq 4)$$

(2) 和で閉じていることは明らかである。また (1) より積でも閉じている。積の可換性もすぐに分かる。

(3)
- Step 1. 「$x=a_1A+a_2A^2+a_3A^3$ はべき零である」ことを示す。
  $x^4=0$ であることがすぐに分かる。
- Step 2. 「$a_0\neq 0$ のとき $x=a_0E+a_1A+a_2A^2+a_3A^3$ は正則である」ことを示す。
  $x=a_0(E+y)$ とかくと y はべき零で $y^4=0$ である。$z={a_0}^{-1}(E-y+y^2-y^3)$ とおけば $xz=zx=E-y^4=E$ であるから z が x の逆元となり、x は正則である。

べき零元は正則でなく、正則元はべき零元ではないので、
- $a_0E+a_1A+a_2A^2+a_3A^3$ が正則であるための必要十分条件は $a_0\neq 0$
- $a_0E+a_1A+a_2A^2+a_3A^3$ がべき零であるための必要十分条件は $a_0=0$

である。

(任意の自然数 n に対して、この問題と同様の方法で $M_n(\mathbb{C})$ の部分環が定義される。)

24. $s,t\in Z(R)$ とする。このとき、任意の $a\in R$ に対して $a(s-t)=as-at=sa-ta=(s-t)a$, $a(st)=(as)t=(sa)t=s(at)=s(ta)=(st)a$ であるから、$s-t,\ st\in Z(R)$ である。よって $Z(R)$ は R の部分環である。

25. (1)
$$E_{11}\begin{pmatrix}a&b\\c&d\end{pmatrix}=\begin{pmatrix}a&b\\0&0\end{pmatrix}$$
であるから
$$E_{11}R=\left\{\begin{pmatrix}a&b\\0&0\end{pmatrix}\,\middle|\,a,b\in\mathbb{C}\right\}$$
である。同様にして
$$E_{12}R=\left\{\begin{pmatrix}a&b\\0&0\end{pmatrix}\,\middle|\,a,b\in\mathbb{C}\right\},\quad E_{21}R=E_{22}R=\left\{\begin{pmatrix}0&0\\c&d\end{pmatrix}\,\middle|\,c,d\in\mathbb{C}\right\}$$
である。

(2) (1) と同様に計算すれば
$$RE_{11}=RE_{21}=\left\{\begin{pmatrix}a&0\\c&0\end{pmatrix}\,\middle|\,a,c\in\mathbb{C}\right\},\quad RE_{12}=RE_{22}=\left\{\begin{pmatrix}0&b\\0&d\end{pmatrix}\,\middle|\,b,d\in\mathbb{C}\right\}$$
である。

(3) 任意の $1\leq k,\ell\leq 2$ に対して
$$E_{k\ell}=E_{ki}E_{ij}E_{j\ell}\in RE_{ij}R$$
となるので $RE_{ij}R=R$ である。

(4) I を R の 0 でないイデアルとする。$0\neq A=(a_{ij})\in I$ とすると、ある a_{ij} は 0 ではない。このとき、任意の $1\leq k,\ell\leq 2$ に対して
$$E_{k\ell}={a_{ij}}^{-1}E_{ki}AE_{j\ell}\in I$$
なので $I=R$ である。

26. 問 25 (4) と同様である。

27. $I = R$ ならば $1 \in I$ であることは明らかである。$1 \in I$ とする。このとき、任意の $r \in R$ に対して $r = r1 \in I$ であるから $R \subset I$ である。$I \subset R$ は明らかなので $I = R$ である。

28. (1) 示すべきことは
    - $I \cap J$ が I と J の両方に含まれること、
    - $I \cap J$ が右イデアルであること、
    - K が I と J の両方に含まれる右イデアルであるならば $K \subset I \cap J$ であること

    の三つである。$I \cap J$ が I と J の両方に含まれることは明らかなので、残りの二つを示す。
    $x, y \in I \cap J$, $r \in R$ とする。I が右イデアルであるから $x - y \in I$, $xr \in I$ である。また J が右イデアルであるから $x - y \in J$, $xr \in J$ である。したがって $x - y \in I \cap J$, $xr \in I \cap J$ となり $I \cap J$ は右イデアルである。
    K を I と J の両方に含まれる右イデアルとする。$K \subset I$ かつ $K \subset J$ なので $K \subset I \cap J$ である。

    (2) 示すべきことは
    - $I + J$ が I と J の両方を含むこと、
    - $I + J$ が右イデアルであること、
    - K が I と J の両方を含む右イデアルであるならば $K \supset I + J$ であること

    の三つである。
    任意の $i \in I$ に対して、$i = i + 0 \in I + J$ である。よって $I \subset I + J$ である。$J \subset I + J$ も同様に示される。
    $x, y \in I + J$, $r \in R$ とする。ある $i, i' \in I$, $j, j' \in J$ があって $x = i + j$, $y = i' + j'$ となる。このとき

$$x - y = (i + j) - (i' + j') = (i - i') + (j - j') \in I + J, \quad xr = (i + j)r = ir + jr \in I + J$$

    なので $I + J$ は R の右イデアルである。
    K を I と J の両方を含む右イデアルとする。$x \in I + J$ とすれば、ある $i \in I$, $j \in J$ があって $x = i + j$ である。このとき $i \in I \subset K$, $j \in J \subset K$ なので $x = i + j \in K$ である。よって $I + J \subset K$ が成り立つ。

29. (1) $a/b,\ c/d \in S$ (b, d は奇数) とする。このとき

$$a/b - c/d = (ad - bc)/bd, \quad (a/b)(c/d) = ac/bd$$

    で、いずれの場合も分母の bd は奇数である。これが既約分数であるとは限らないが、既約分数にしたときの分母は bd の約数であるから、やはり奇数である。よって、これらは S の元であり S は $\mathbb{Q}$ の部分環である。

    (2) $0 \neq x \in S$ に対して $\nu(x) = \max\{\ell \in \mathbb{N} \cup \{0\} \mid x/2^\ell \in S\}$ とおく。(x は S の元なので、分母の素因数に 2 を含まない。分子に素因数として 2 が何回現れるかを $\nu(x)$ とするのである。) I を 0 でない R のイデアルとする。$m = \min\{\nu(x) \mid x \in I - \{0\}\}$ とおく。I は 0 でないとしているから m は定まる。$I = 2^m S$ であることを示そう。
    定義により $I \subset 2^m S$ であることは明らかである。したがって $2^m \in I$ であることを示せばよい。m の定義から、ある $0 \neq x \in I$ があって $\nu(x) = m$ である。このとき $x = 2^m a/b$ (a, b は奇数) と書くことができる。ここで $b/a \in S$ となるので $2^m = x(b/a) \in I$ である。したがって $I = 2^m S$ であることが分かった。
    以上より S のイデアルは 0 と $2^m S$ $(m \in \mathbb{N} \cup \{0\})$ である。

    (3) (2) より明らかである。

30. (1) $f, g \in \mathrm{End}(A)$ のとき $f + g$, fg も $\mathrm{End}(A)$ の元、すなわち自己準同型であることを示せばよい。$a, b \in A$ に対して

$$\begin{aligned} (f + g)(a + b) &= f(a + b) + g(a + b) = f(a) + g(a) + f(b) + g(b) = (f + g)(a) + (f + g)(b) \\ (fg)(a + b) &= f(g(a + b)) = f(g(a) + g(b)) = f(g(a)) + f(g(b)) = (fg)(a) + (fg)(b) \end{aligned}$$

    であるから $f + g,\ fg \in \mathrm{End}(A)$ である。

    (2)
    - 加法について、結合法則を満たすことは簡単な計算で分かる。任意の $a \in A$ について $z(a) = 0$ として z を定めれば、これは自己準同型である。この z は加法に関する単位元になる。(通常はこれを 0 と書く。$0(a) = 0$ である。) 任意の $f \in \mathrm{End}(A)$ に対して $g(a) = -f(a)$ で g を定めれば、これはやはり自己準同型で、加法に関する f の逆元になる。(通常はこれを $-f$ と書く。$(-f)(a) = -f(a)$ である。) 以上より $\mathrm{End}(A)$ は加法についてアーベル群である。
    - 乗法について、写像の合成によって積が定義されているので、結合法則は成り立つ。また恒等写像は自己準同型で、これが乗法に関する単位元になる。したがって $\mathrm{End}(A)$ は乗法についてモノイドである。

- 分配法則を満たすことを確認する。$f, g, h \in \mathrm{End}(A)$ とする。任意の $a \in A$ に対して

$$\begin{aligned}(f(g+h))(a) &= f((g+h)(a)) = f(g(a)+h(a)) = f(g(a))+f(h(a)) \\ &= (fg)(a)+(fh)(a) = (fg+fh)(a)\end{aligned}$$

  である。よって $f(g+h) = fg+fh$ が成り立つ。$(f+g)h = fh+gh$ についても同様にして確かめることができる。

以上より $\mathrm{End}(A)$ は環になる。