代数入門問題集 [20120704]

1 二項演算、半群、モノイド

1. 集合 A の二項演算の定義を答えよ。
2. 集合 A がちょうど二つの要素をもつとする。A の二項演算はいくつあるか。
3. $A = \{a, b\}$ を $a \neq b$ なる集合とする。A の二項演算で、結合法則をみたすものを具体的に一つ構成せよ。
4. 以下のものは、半群、モノイド、群、そのいずれでもないか、最も適当なものをそれぞれ答えよ。
   (1) 集合 $\{0, 1\}$ で通常の加法を演算とするもの。
   (2) 集合 $\{0, 1\}$ で通常の乗法を演算とするもの。
   (3) 集合 $\{-1, 1\}$ で通常の乗法を演算とするもの。
   (4) 集合 $\{-1, 0, 1\}$ で通常の乗法を演算とするもの。
   (5) 実数を成分とする n 次正方行列の全体で通常の加法を演算とするもの。
   (6) 実数を成分とする n 次正方行列の全体で通常の乗法を演算とするもの。
   (7) 実数を成分とする n 次正則行列の全体で通常の乗法を演算とするもの。
5. 実数を成分とする n 次正方行列 $A = (a_{ij})$, $B = (b_{ij})$, $C = (c_{ij})$ について $(AB)C = A(BC)$ が成り立つことを示せ。
6. 複素数 $\alpha_1 = a_1 + b_1 i$, $\alpha_2 = a_2 + b_2 i$, $\alpha_3 = a_3 + b_3 i$ について $(\alpha_1\alpha_2)\alpha_3 = \alpha_1(\alpha_2\alpha_3)$ が成り立つことを示せ。ただし $a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{R}$ で i は虚数単位とする。
7. 直積集合 $\mathbb{R} \times \mathbb{R}$ に
$$(a, b)(c, d) = (ac, ad + bc)$$
で二項演算を定める。
   (1) これが結合法則を満たすことを示せ。(よってこれは半群である。)
   (2) 単位元を求めよ。(よってこれはモノイドである。)
   (3) 正則元を決定し、その逆元も求めよ。
8. 直積集合 $\mathbb{R} \times \mathbb{R}$ に
$$(a, b)(c, d) = (ac - bd, ad + bc)$$
で二項演算を定める。
   (1) これが結合法則を満たすことを示せ。
   (2) 単位元を求めよ。
   (3) 正則元を決定し、その逆元も求めよ。
9. 直積集合 $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$ に
$$\begin{aligned}(a, b, c) + (d, e, f) &= (a + d,\ b + e,\ c + f)\\ (a, b, c)(d, e, f) &= (ad,\ ae + bf,\ cf)\end{aligned}$$
で和と積を定める。
   (1) 積が結合法則を満たすことを示せ。
   (2) 積に関する単位元を求めよ。
   (3) 積に関する正則元を決定し、その逆元も求めよ。
   (4) 和と積が分配法則 $(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$, $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$ を満たすことを示せ。
10. A を空でない集合とし $a \in A$ を一つ固定する。任意の $x, y \in A$ に対して $xy = a$ として演算を定める。このとき、この演算は結合法則をみたすことを示せ。また A は単位元をもつかどうかを判定せよ。
11. A を空でない集合とする。任意の $x, y \in A$ に対して $xy = x$ として演算を定める。このとき、この演算は結合法則をみたすことを示せ。また A は単位元をもつかどうかを判定せよ。
12. $M_2(\mathbb{R})$ を実数を成分とする 2 次正方行列全体の集合とする。$P, Q \in M_2(\mathbb{R})$ に対して $[P, Q] = PQ - QP$ によって二項演算を定める。これが結合法則を満たさないことを示せ。

13. $|A| = 2$ なる可換半群を一つ具体的に構成せよ。また $|A| = 2$ なる非可換な半群を一つ具体的に構成せよ。

14. 半群であるがモノイドではないものの例を一つ挙げよ。

15. モノイドであるが群ではないものの例を一つ挙げよ。

16. モノイドの単位元はただ一つ存在することを示せ。

17. モノイドの正則元に対して、その逆元はただ一つ存在することを示せ。

18. M をモノイドとし、a を M の正則元とする。写像 $f : M \to M$ を $f(m) = am$ によって定めれば f は全単射であることを示せ。

19. $A = \{0, 1\}$ は通常の乗法によって半群になっている。このとき**演算表** (乗法表) を

	0	1
0	0	0
1	0	1

のように書く。$A = \{0, 1, -1\}$ も通常の乗法によって半群になっている。この半群の乗法表を書け。

20. A を半群とする。$e \in A$ が A の**左単位元**であるとは、「任意の $a \in A$ に対して $ea = a$」が成り立つこととする。また、$f \in A$ が A の**右単位元**であるとは、「任意の $a \in A$ に対して $af = a$」が成り立つこととする。左単位元は存在しないが、右単位元は存在するような例を構成せよ。

21. 半群 A が左単位元と右単位元をもつならば、A は単位元をもつことを示せ。

22. A を 1 を単位元とするモノイドとする。$a \in A$ に対して、$b \in A$ が a の **左逆元**であるとは、$ba = 1$ となることとする。また b が a の **右逆元**であるとは、$ab = 1$ となることとする。

    A を $\mathbb{N}$ から $\mathbb{N}$ への写像全体の集合とする。A は写像の合成を演算として、恒等写像 $id_{\mathbb{N}}$ を単位元とするモノイドになる。$f \in A$ を $f(a) = a + 1$ で定める。f は左逆元をもつが、右逆元をもたないことを示せ。また、$z \in \mathbb{N}$ に対して $g_z \in A$ を

$$g_z(a) = \begin{cases} a - 1 & (a \geq 2) \\ z & (a = 1) \end{cases}$$

    で定める。g_z は右逆元をもつが、左逆元をもたないことを示せ。

23. モノイド A の元 a が左逆元と右逆元をもつならば、a は逆元をもつことを示せ。

代数入門問題集 [20120704]

2 群

1. (1) 群の定義を書け。
   (2) 群の例を具体的にいくつか挙げよ。このとき、どんな集合に対して、どのような演算で群になっているか明記すること。

2. G を群とし $g \in G$ を一つ固定する。このとき以下の写像はすべて全単射であることを示せ。
   (1) $\alpha : G \to G$ $(\alpha(x) = xg)$
   (2) $\beta : G \to G$ $(\beta(x) = gx)$
   (3) $\gamma : G \to G$ $(\gamma(x) = g^{-1}xg)$
   (4) $\delta : G \to G$ $(\delta(x) = x^{-1})$

3. 群 G の元 x, y に対して $(xy)^{-1} = y^{-1}x^{-1}$ が成り立つことを示せ。

4. 群 G の任意の元 a に対して $a^2 = 1$ が成り立つならば、G はアーベル群になることを示せ。

5. A をモノイドとし、集合として有限集合であるとする。A において**左簡約法則**「$ab = ac$ ならば $b = c$」が成り立つならば A は群であることを示せ。(同様に**右簡約法則**「$ba = ca$ ならば $b = c$」も考えられる。右簡約法則、左簡約法則の両方が成り立つとき、単に**簡約法則**が成り立つという。)

6. モノイド A において左簡約法則「$ab = ac$ ならば $b = c$」が成り立っても A が群であるとは限らない。このような具体例を一つ挙げよ。

7. A を半群とし、集合として有限集合であるとする。A において簡約法則 (問 5 参照) が成り立つならば A は群であることを示せ。

8. x を群 G の有限位数の元とする。このとき x と $g^{-1}xg$ $(g \in G)$ は同じ位数をもつことを示せ。(x の位数とは、$x^n = 1$ となる最小の自然数 n である。このような n が存在するとき x は**有限位数**であるといい、そうでないときには**無限位数**であるという。)

9. x を群 G の位数 $n < \infty$ の元とする。このとき $x^m = 1$ となることと $m = n\ell$ となる $\ell \in \mathbb{Z}$ が存在することは同値である。これを証明せよ。

10. (1) 巡回群はアーベル群であることを示せ。
    (2) 巡回群の部分群は巡回群であることを示せ。
    (3) 加法群 $\mathbb{Z}$ の部分群は $n\mathbb{Z}$ の形に限られることを示せ。

11. (1) 群 G の部分集合 H が部分群であることの定義を書け。
    (2) 加法群 $\mathbb{Z}$ に対して、$2\mathbb{Z} = \{2a \mid a \in \mathbb{Z}\}$ は $\mathbb{Z}$ の部分群であることを示せ。ただし演算は通常の足し算とする。
    (3) 加法群 $\mathbb{Z}$ の部分群をできるだけたくさん挙げよ。

12. 群 G の部分群を H とする。 $a, b \in G$ に対して、次はすべて同値であることを示せ。
    (1) $aH = bH$
    (2) $a^{-1}b \in H$
    (3) $b \in aH$
    (4) $a \in bH$
    (5) $aH \cap bH \neq \phi$

    ($Ha = Hb$ など、左右を反対にしても同様のことが成り立つ。)

13. G を群、H をその部分群とする。$a^{-1}b \in H$ のときに $a \sim b$ として G 上の関係 $\sim$ を定義する。$\sim$ は同値関係であることを示せ。また a を含む同値類を集合の形で具体的に記述せよ。(この同値類を G の H による**左剰余類**という。同様に $ab^{-1} \in H$ で定めた同値関係による同値類を**右剰余類**という。)

14. G を群とする。$a \in G$ に対して $C_G(a) = \{g \in G \mid ga = ag\}$ を G における a の**中心化群**という。
    (1) $C_G(a)$ は G の部分群であることを示せ。

(2) $g, h \in G$ に対して $gag^{-1} = hah^{-1}$ であることと $gC_G(a) = hC_G(a)$ であることは同値であることを示せ。

15. 群 G とその部分集合 A に対して $C_G(A) = \bigcap_{a \in A} C_G(a)$ とおいて、これを G における A の**中心化群**という。$C_G(A)$ は G の部分群であることを示せ。

16. G を群、H をその部分群とする。$N_G(H) = \{g \in G \mid gHg^{-1} = H\}$ を G における H の**正規化群**という。

(1) $N_G(H)$ は G の部分群であることを示せ。

(2) $g, h \in G$ に対して $gHg^{-1} = hHh^{-1}$ であることと $gN_G(H) = hN_G(H)$ であることは同値であることを示せ。

17. 群 G に対して $Z(G) = \{x \in G \mid xg = gx \text{ for any } g \in G\}$ は G の部分群であることを示せ。($Z(G)$ を G の**中心**という。)

18. n を自然数とする。$GL_n(\mathbb{R})$ で実数を成分とする n 次正則行列全体の集合を表す。二つの正則行列の積、正則行列の逆行列、はまた正則行列なので、$GL_n(\mathbb{R})$ は積を演算として群になる。これを $\mathbb{R}$ 上 n 次**一般線形群** (general linear group) という。複素数体上でも同様に $GL_n(\mathbb{C})$ が定義される。以下の集合は $GL_n(\mathbb{R})$ または $GL_n(\mathbb{C})$ の部分群であることを示せ。ただし $\det M$ は行列 M の行列式、${}^tM$ は行列 M の転置行列、E は単位行列、$\overline{M}$ は行列 M のすべての成分を複素共役で置き換えた行列とする。

(1) $SL_n(\mathbb{R}) = \{M \in GL_n(\mathbb{R}) \mid \det M = 1\}$ ($\mathbb{R}$ 上 n 次**特殊線形群** (special linear group)。$\mathbb{C}$ 上でも同様である。)

(2) $O(n) = \{M \in GL_n(\mathbb{R}) \mid {}^tMM = E\}$ (n 次**直交群** (orthogonal group))

(3) $SO(n) = \{M \in O(n) \mid \det M = 1\}$

(4) $U(n) = \{M \in GL_n(\mathbb{C}) \mid {}^t\overline{M}M = E\}$ (n 次**ユニタリー群** (unitary group))

19. $A = \{1, 2, \cdots, n\}$ とする。A から A への全単射 を A 上の置換という。置換 σ を

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

と表すことにする。

(1) $n = 3$ とするとき A 上の置換を全て書け。

(2) 写像の合成で置換の積を定義すれば、A 上の置換全体の集合は群になる。これを n **次対称群**といい S_n と書く。S_3 の乗法表を作れ。
ヒント. 積は、例えば次のようになる。

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

(3) 置換 $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ は $1 \mapsto 2 \mapsto 3 \mapsto 1$ と 3 つの数を巡回的に移す置換である。このような置換を**巡回置換**といい、この場合 (1 2 3) と表す。任意の置換は共通の数を含まないいくつかの巡回置換の積として表すことができる。例えば

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 6 & 1 & 4 & 3 \end{pmatrix} = (1\ 5\ 4)(3\ 6)(2) = (1\ 5\ 4)(3\ 6)$$

である。一つの数だけの (2) は何も動かさないことを意味するので通常は省略される。$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 5 & 7 & 1 & 6 & 4 \end{pmatrix}$ をこのような巡回置換の積に表せ。

(4) (1) で求めた S_3 の元をすべて巡回置換として表せ。

20. $n \geq 3$ とする。S_n の二つの置換

$$s = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 2 & 3 & \cdots & n & 1 \end{pmatrix}, \quad t = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ n & n-1 & \cdots & 2 & 1 \end{pmatrix}$$

で生成される部分群を**二面体群**といい D_{2n} と書く。

(1) $s^n = 1$, $t^2 = 1$, $ts = s^{-1}t$ が成り立つことを確認せよ。

(2) D_{2n} の任意の元は s^it^j $(0 \leq i < n, 0 \leq j < 2)$ と一意的に表されることを示せ。これにより $|D_{2n}| = 2n$ であることが分かる。

(3) $n = 4$ として D_{2n} の乗法表を書け。

21. 行列 E, I, J, K を以下のように定める。

$$E = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},\ I = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix},\ J = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix},\ K = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}$$

$G = \{E,\ -E,\ I,\ -I,\ J,\ -J,\ K,\ -K\}$ とおく。

(1) G は通常の乗法で群になることを乗法表を書くことによって確認せよ。

(2) G は位数 8 の二面体群 D_8 と本質的に異なる群であることを説明せよ。

22. (1) 以下のものをそれぞれ集合として表し、その元の数を求めよ。

(i) $\mathbb{Z}/12\mathbb{Z}$

(ii) 加法群 $\mathbb{Z}/12\mathbb{Z}$ の部分群 $\langle\overline{4}\rangle$ (ここで $\overline{a} = a + 12\mathbb{Z}$ とする。)

(iii) 加法群 $\mathbb{Z}/12\mathbb{Z}$ の部分群 $\langle\overline{4}\rangle$ によるすべての剰余類

(2) G を有限群とし H をその部分群とする。任意の $a \in G$ に対して $|aH| = |H|$ であることを示せ。また、異なる左剰余類の数を $|G : H|$ と書くとき $|G| = |G : H| \cdot |H|$ であることを示せ。

(3) 有限群 G の元の位数は G の位数の約数であることを示せ。

(4) G を位数 n の有限群とするとき、 G の任意の元 a に対して $a^n = 1$ が成り立つことを示せ。

23. G を群とし H, K をその部分群とする。$a, b \in G$ に対して、ある $h \in H$ と $k \in K$ が存在して $b = hak$ となるとき $a \sim b$ として G 上の関係 $\sim$ を定義する。このとき $\sim$ は同値関係であることを示せ。(この同値関係による同値類を (H, K)-**両側剰余類**という。)

24. G を素数位数の有限群とする。このとき G は巡回群であることを示せ。

25. 位数 3 の群の乗法表を書け。

26. G を有限群とし H, K をその部分群とする。$HK = \{hk \mid h \in H,\ k \in K\}$ とおく。このとき HK が G の部分群であることと $HK = KH$ が成り立つことは同値であることを示せ。

27. G を有限群とし H, K をその部分群とする。$|HK| = |H| \cdot |K|/|H \cap K|$ を示せ。

28. 群 G とその二つの部分群 H, K で HK が G の部分群ではない例を具体的に示せ。

29. 群 G とその二つの真部分群 H, K に対して $H \cup K \subsetneq G$ を示せ。

30. 群 G の部分群 H が**正規部分群**であるとは、任意の $g \in G$ に対して $gH = Hg$ が成り立つこととである。群 G の部分群 H で $|G : H| = 2$ であるものは G の正規部分群であることを示せ。

31. N を群 G の正規部分群とする。G の N による左剰余類の集合 G/N に

$$(g_1N)(g_2N) = (g_1g_2)N$$

で演算を定めることを考える。

(1) この演算が矛盾なく定義されることをを示せ。

(2) この演算によって G/N が群になることを示せ。(この群を G の N による**剰余群**という。)

32. 群 G に以下のように関係 $\sim$ を定義する。$a, b \in G$ に対して $a \sim b$ であるとは、ある $g \in G$ が存在して $b = gag^{-1}$ となることとする。

(1) G 上の関係 $\sim$ は同値関係であることを示せ。

(2) $a \sim b$ であるとき a と b は G で**共役**であるといい、共役による同値類を**共役類**という。G が有限群であるとき $a \in G$ を含む共役類に含まれる元の数は $|G : C_G(a)|$ であることを示せ。

(3) 3 次対称群 S_3 の共役類を求めよ。

(4) 位数 8 の二面体群 D_8 の共役類を求めよ。

33. 群 G のある共役類が一つの元しか含まないとき、その元は G の中心 $Z(G)$ に含まれることを示せ。また、中心の元 a に対して、a を含む共役類は a のみからなることを示せ。

34. p を素数とする。位数が p-べきの有限群を p-**群**という。p-群の中心は自明でない、すなわち $\{1\}$ ではない、ことを示せ。

35. 群 G の正規部分群は、いくつかの共役類の和集合であることを示せ。逆に、群 G のいくつかの共役類の和が G の部分群であるならば、それは正規部分群であることを示せ。

36. (1) 3 次対称群 S_3 の正規部分群をすべて求めよ。
    (2) 位数 8 の二面体群 D_8 の正規部分群をすべて求めよ。

37. H, K を群 G の正規部分群とし、$H \cap K = \{1\}$ とする。このとき H の元と K の元は可換になることを示せ。

38. G, H を群とする。写像 $f : G \to H$ について、$f(ab) = f(a)f(b)$ が任意の $a, b \in G$ に対して成り立つとき f を**準同形写像**、または簡単に**準同型**、という。$f : G \to H$ は準同型であるとする。
    (1) $f(1_G) = 1_H$ であることを示せ。
    (2) 任意の $a \in G$ に対して $f(a^{-1}) = f(a)^{-1}$ であることを示せ。
    (3) $\mathrm{Ker}(f) = \{a \in G \mid f(a) = 1_H\}$ とおくと $\mathrm{Ker}(f)$ は G の正規部分群であることを示せ。($\mathrm{Ker}(f)$ を f の**核**という。)
    (4) $f(G) = \{f(a) \mid a \in G\}$ は H の部分群であることを示せ。
    (5) 準同型 $f : G \to H$ が単射であることと $\mathrm{Ker}(f) = \{1_G\}$ であることは同値であることを示せ。

39. G, H を群とし $f : G \to H$ は準同型写像であるとする。$K = \mathrm{Ker}(f)$ とする。また N を G の正規部分群とする。
    (1) 剰余群 G/N を考える (問 31 参照)。$\bar{f} : G/N \to H$ ($\bar{f}(gN) = f(g)$) が矛盾なく定義できるための必要十分条件は $N \subset K$ であることを示せ。
    (2) $N \subset K$ のとき $\bar{f}$ も準同型であることを示せ。

40. G, H を群とし $f : G \to H$ は準同型写像であるとする。$K = \mathrm{Ker}(f)$ とする。
    (1) 剰余群 G/K を考える (問 31 参照)。$\bar{f} : G/K \to f(G)$ ($\bar{f}(gK) = f(g)$) が矛盾なく定義でき、また準同型であることを示せ。
    (2) $\bar{f}$ は全単射であることを示せ。

41. G, H を群とする。集合としての直積 $G \times H$ に $(g, h)(g', h') = (gg', hh')$ によって積を定義する。このとき $G \times H$ はこの演算によって群になることを示せ。(群 $G \times H$ を群の**直積**という。三つ以上の群についても同様に直積を考えることができる。また群が加法的に書かれているときには、これを群の**直和**と呼び $G \oplus H$ と表す。)

42. G, H を共に位数 2 の巡回群とする。直積 $G \times H$ の乗法表を書け。(この群を**クラインの四元群**という。)

43. 位数 8 の二面体群 $G = D_8$ を考え、問 20 の記号を用いる。$H = \langle s^2 \rangle$ とする。
    (1) H は G の正規部分群であることを示せ。
    (2) H による G の左剰余類分解を求めよ。
    (3) 剰余群 G/H の乗法表を書け。

44. G を群とする。G の中心 $Z(G)$ による剰余群 $G/Z(G)$ が巡回群であるならば G はアーベル群であることを示せ。

45. p を素数とする。位数 p^2 の有限群はアーベル群であることを示せ。

46. 有理数全体の集合 $\mathbb{Q}$ を加法群と見る。$\mathbb{Q}$ の部分群 H に対して $|\mathbb{Q} : H| < \infty$ であるならば $\mathbb{Q} = H$ であることを示せ。

47. G を群、H を G の部分群とする。
    (1) $g \in G$ に対して gHg^{-1} も G の部分群であることを示せ。(これを H と **共役な部分群**という。)
    (2) H と 共役な部分群は $|G : N_G(H)|$ 個あることを示せ。

48. 位数 4 の有限群を決定せよ。

49. X を集合、G を群とする。写像 $G \times X \to X$ ($(g, x) \mapsto gx$) が
    - 任意の $x \in X$ に対して $1_G x = x$、
    - 任意の $g, h \in G$, $x \in X$ に対して $(gh)x = g(hx)$

    をみたすとき G は X に**作用する**という。
    以下、G は X に作用しているものとする。

(1) $gx = y$ ならば $g^{-1}y = x$ であることを示せ。

(2) ある $g \in G$ が存在して $gx = y$ となるとき $x \sim y$ と定めて、X 上の関係 $\sim$ を定義する。$\sim$ は同値関係であることを示せ。

(3) $x \in X$ に対して $G_x = \{g \in G \mid gx = x\}$ と定め、これを x の**安定部分群**と呼ぶ。G_x が G の部分群であることを示せ。

(4) (2) の同値関係による同値類を X の G-**軌道**という。$|X| < \infty$ とするとき $x \in X$ を含む G-軌道に含まれる元の数は $|G : G_x|$ であることを示せ。

50. 3 次元ユークリッド空間内の正多面体の自己同型群の位数を求めよう。3 次元ユークリッド空間内の正多面体は、正 4 面体、正 6 面体、正 8 面体、正 12 面体、正 20 面体、の 5 つある。これらを、それ自身に移すような変換全体のなす集合は、合成を演算として群になる。その群を**自己同型群**とよぶ。$n = 4, 6, 8, 12, 20$、それぞれに対して正 n 面体の自己同型群の位数を求めよ。

51. S を集合、G を群とする。$\mathrm{Map}(S, G)$ で S から G への写像全体のなす集合を表すことにする。$f, g \in \mathrm{Map}(S, G)$ に対して

$$(fg)(s) = f(s)g(s) \quad (s \in S)$$

によって $\mathrm{Map}(S, G)$ に積を定める。このとき $\mathrm{Map}(S, G)$ は群になる。この群の単位元を求めよ。

代数入門問題集 [20120704]

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. 単位元をもつ環 R の左零因子は正則元ではないことを示せ。(右零因子でも同様である。)
2. 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。
3. 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。
4. 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。
5. 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。
6. 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。)
7. 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。
8. 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。
9. 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 $g : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ 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。
10. $a, b \in \mathbb{N}$ とし $a = bq + r$ $(q, r \in \mathbb{N} \cup \{0\},\ 0 \leq r < b)$ とする。このとき $\gcd(a, b) = gcd(b, q)$ であることを示せ。
11. $a, b \in \mathbb{N}$ とする。$a_0 = a$, $a_1 = b$ とし、帰納的に $a_i = a_{i+1}q_{i+1} + a_{i+2}$ $(q_{i+1}, a_{i+2} \in \mathbb{N} \cup \{0\},\ 0 \leq a_{i+2} < a_{i+1})$ によって a_i を定める。このとき、数列 $\{a_i\}$ は 0 にならない限り狭義単調減少列であるから、ある n が存在して $a_n \neq 0$, $a_{n+1} = 0$ となる。$\gcd(a, b) = a_n$ を証明せよ (この方法で最大公約数を求める方法を**ユークリッドの互除法**という。)。
12. 1357 と 2468 の最大公約数を求めよ。
13. $a, b \in \mathbb{N}$ とする。$ax + by = \gcd(a, b)$ となる $x, y \in \mathbb{Z}$ が存在することを示せ。
14. $28x + 15y = 1$ となる整数の組 (x, y) を求めよ。
15. 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。
16. 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。
17. 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)。

18. 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。

19. 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)。

20. 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。)

21. 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。

22. 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。)

23. 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。

24. 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。

25. $\mathbb{C}$ 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。

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

26. 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。)

27. 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。

28. 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。)

29. 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。)

30. 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。

31. 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。

32. 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。

33. $a, b \in \mathbb{N}$ とし $d = \gcd(a, b)$ とする。$\mathbb{Z}$ のイデアル (a), (b) に対して $(a) + (b) = (d)$ が成り立つことを示せ。

34. 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 21 参照) であることを示せ。

35. 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。)

36. R を環、I をそのイデアルとする。

(1) $a, b \in R$ に対して、$a - b \in I$ のときに $a \sim b$ として R 上の関係 $\sim$ を定める。この関係が同値関係であることを示せ。(このとき通常は $a \equiv b \pmod{I}$ と記述される。)

(2) $a \in R$ を含む $\sim$ による同値類を $a + I$ とかくことにする。$a + I$ を集合の形で具体的に記述せよ。

(3) $\sim$ による同値類全体の集合を R/I と表す。$a + I, b + I \in R/I$ に対して

$$(a + I) + (b + I) = (a + b) + I, \quad (a + I)(b + I) = ab + I$$

で加法と乗法が矛盾なく定義できることを示せ。

(4) R/I は (3) の演算で環になることを示せ。(これを R の I による**剰余環**という。)

37. R_1, R_2 を単位元をもつ環とする。集合としての直積 $R_1 \times R_2$ に以下のように加法と乗法を定める。

$$(r_1, r_2) + (s_1, s_2) = (r_1 + s_1, r_2 + s_2), \quad (r_1, r_2)(s_1, s_2) = (r_1 s_1, r_2 s_2)$$

このとき、この演算によって $R_1 \times R_2$ は環になる。これを R_1 と R_2 の**直和**といい $R_1 \oplus R_2$ と書く。

(1) $R_1 \oplus R_2$ の零元と (乗法に関する) 単位元を求めよ。

(2) $R_1 \oplus R_2$ の正則元と左 (右) 零因子を R_1, R_2 の正則元と左 (右) 零因子を用いて決定せよ。

38. R を環とし $a \in R$ とする。$C = \{x \in R \mid ax = xa\}$ とおくと C は R の部分環になることを示せ。

39. R を環とし $a \in R$ とする。$A = \{x \in R \mid ax = 0\}$ とおくと A は R の右イデアルになることを示せ。

代数入門問題集 [20120704]

4 多項式環、体

1. 標数 $p>0$ の体 F の任意の二元 a,b に対して $(a+b)^p=a^p+b^p$ が成り立つことを示せ。
2. F を標数 $p>0$ の有限体とする。写像 $f:F\to F$ $(f(a)=a^p)$ は全単射であることを示せ。
3. 元数が 4 の有限体 $\mathbb{F}_4$ を構成し、その加法と乗法に関する演算表を書け。
4. K を体とし $f(x)$ $(\neq 0)$ を n 次の K 係数多項式とする。このとき $f(a)=0$ となる $a\in K$ は高々 n 個であることを示せ。($f(a)=0$ となる $a\in K$ を $f(x)$ の**根**という。)
5. K を体とし、$f(x)$ を K 係数多項式とする。$f(x)=\sum_{i=0}^{n}a_ix^i$ に対して $f'(x)=\sum_{i=1}^{n}ia_ix^{i-1}$ とおいて、これを $f(x)$ の**形式的な微分**という。
   (1) 多項式の形式的な微分についても、積の微分に関する公式 $(fg)'=f'g+fg'$ は成り立つことを示せ。
   (2) $f(x)$ が重根 a をもつことと $f(a)=f'(a)=0$ となることが同値であることを示せ。ただし a が $f(x)$ の重根であるとは、多項式 $g(x)$ が存在して $f(x)=(x-a)^2g(x)$ と書けることとする。
6. K を体とする。写像 $f:K\to K$ が**多項式写像**であるとは、ある K 係数多項式 F が存在して、任意の $a\in K$ に対して $f(a)=F(a)$ となることとする。K が有限体であるとき、任意の写像 $f:K\to K$ は多項式写像であることを示せ。
7. 体 K 上の二つの多項式で、多項式としては異なり、等しい多項式写像を定めるものを具体的に一つ答えよ。
8. $\sqrt{2}+\sqrt{3}$ を根にもつ次数最小で最高次係数が 1 の有理数係数多項式を求めよ。
9. $\mathbb{Q}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}\}$ とおく。$\mathbb{Q}[\sqrt{2}]$ は通常の演算で体であることを示せ。
10. R を整域とし R の部分集合 S は
    - $1\in S$, $0\notin S$
    - $a,b\in S$ ならば $ab\in S$

    を満たすものとする。このとき S を R の**積閉集合**という。直積集合 $S\times R$ に $sr'=s'r$ のときに $(s,r)\sim(s',r')$ として関係 $\sim$ を定める。
    (1) $\sim$ は同値関係であることを示せ。
    (2) (s,r) を含む $\sim$ による同値類を r/s と書くことにする。また同値類全体の集合を $S^{-1}R$ と書く。$S^{-1}R$ に加法と乗法を
    $$r/s+r'/s'=(rs'+r's)/(ss'),\quad (r/s)(r'/s')=(rr')/(ss')$$
    によって定めることができることを示せ。
    (3) 上の演算が、加法に関する交換法則、結合法則、乗法に関する結合法則、分配法則を満たすことを示せ。
    (4) 以上より $S^{-1}R$ は環の構造をもつ。これを R の S による**商環**という。特に S として $R-\{0\}$ をとれば、これは積閉集合である。このときの商環 $S^{-1}R$ は体であることを示せ。(この体を整域 R の**商体**という。)
    (5) $R=\mathbb{Z}$ のとき、その商体は何かを考えよ。
11. (1) 整域 R 上の一変数多項式環 $R[x]$ はまた整域であることを示せ。
    (2) 整域 R 上の n 変数多項式環 $R[x_1,x_2,\cdots,x_n]$ は整域であることを示せ。
12. K を体とする。
    (1) K 上の一変数多項式環 $K[x]$ は単項イデアル整域 (§3 問 21 参照) であることを示せ。
    (2) $f(x),g(x)\in K[x]$ に対して $(f(x),g(x))=\{f(x)a(x)+g(x)b(x)\mid a(x),b(x)\in K[x]\}$ とおくと、$(f(x),g(x))$ は $K[x]$ のイデアルであることを示せ。
    (3) (1), (2) より、$f(x),g(x)\in K[x]-\{0\}$ に対して $(f(x),g(x))=(h(x))$ となる $h(x)\in K[x]$ が存在する。最高次係数で割って $h(x)$ の最高次係数は 1 であると仮定してよい。このとき $h(x)$ を $f(x)$ と $g(x)$ の**最大公約元**といい、$\gcd(f,g)$ と書くことにする。$f(x)=g(x)q(x)+r(x)$, $\deg r(x)<\deg f(x)$ とするとき $\gcd(f,g)=\gcd(g,r)$ であることを示せ。
13. K を体とする。$f(x)\in K[x]$ を既約な多項式とする。このとき $K[x]/(f(x))$ は体であることを示せ。

14. $\mathbb{Q}[x]/(x^2-2)$ は本質的に $\mathbb{Q}[\sqrt{2}]$ (問 9 参照) と同じ体であることを示せ。(本質的に同じ体であるとは、集合としての全単射で、和と積を保つものが存在することをいうこととする。このとき二つの体は**同型**であるという。)

15. $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ (元数 2 の有限体) とする。

    (1) $\mathbb{F}_2$ 上の既約な 2 次多項式 $f(x)$ を見付けよ。

    (2) $\mathbb{F}_2[x]/(f(x))$ は本質的に問 3 の体 $\mathbb{F}_4$ と同じ体であることを示せ。

16. $f(x) = x^6 - 1$ を $\mathbb{Z}[x]$ で既約多項式の積に分解せよ。

17. (1) $K = \mathbb{Z}/5\mathbb{Z}$ とする。$f(x) = x^5 - 1$ を $K[x]$ で既約多項式の積に分解せよ。

    (2) p を素数とし $K = \mathbb{Z}/p\mathbb{Z}$ とする。$f(x) = x^p - 1$ を $K[x]$ で既約多項式の積に分解せよ。

18. $a_1, a_2, \cdots, a_n$ を相異なる実数とし、$b_1, b_2, \cdots, b_n$ を (異なるとは限らない) 実数とする。

    (1) $f_k(a_i) = \delta_{ki}$ となる $f_k(x) \in \mathbb{R}[x]$ を各 k に対して一つ求めよ。

    (2) 任意の i について $f(a_i) = b_i$ となる $f(x) \in \mathbb{R}[x]$ を求めよ。

19. $F = \mathbb{Z}/7\mathbb{Z}$ とすると、これは体である。多項式環 $F[x]$ で $f(x) = 2x^4 + x^2 + 1$ を $g(x) = 3x^2 + 1$ で割った商と余りを求めよ。

20. $f(x) = x^2 + x + 1$, $g(x) = x - 1$ とする。剰余環 $\mathbb{Q}[x]/f(x)\mathbb{Q}[x]$ において $\overline{g(x)} = g(x) + f(x)\mathbb{Q}[x]$ の逆元を求めよ。

21. $K = \mathbb{Z}/7\mathbb{Z}$ とする。$f(x) = x^3 + 2$, $g(x) = x^2 + 3$ とする。剰余環 $K[x]/f(x)K[x]$ において $\overline{g(x)} = g(x) + f(x)K[x]$ の逆元を求めよ。

22. K を体とし $|K| > n$ とする。二つの $f(x), g(x) \in K[x]$ について、$\deg f(x) \leq n$, $\deg g(x) \leq n$ とし、更に $f(x) \neq g(x)$ とする。このとき $f^* \neq g^*$ であることを示せ。

代数入門問題集・解答例と解説 [20120704]

1 二項演算、半群、モノイド

1. A の二項演算とは、写像 $A \times A \to A$ のことである。

2. 一般に、有限集合 X, Y について $|X| = m$, $|Y| = n$ とすると、X から Y への写像は n^m 個ある。$|A \times A| = 4$, $|A| = 2$ であるから、二項演算は $2^4 = 16$ 個ある。

3. 例えば以下のようなものがある。

   (1) 任意の $x, y \in A$ に対して $f(x, y) = a$ であるもの。

   (2) $f(a, a) = f(a, b) = a$, $f(b, a) = f(b, b) = b$ で定まるもの。

   (3) $f(a, a) = f(a, b) = f(b, a) = a$, $f(b, b) = b$ で定まるもの。

   (4) $f(a, a) = f(b, b) = a$, $f(a, b) = f(b, a) = b$ で定まるもの。

4. (1) いずれでもない (2) モノイド (3) 群 (4) モノイド (5) 群 (6) モノイド (7) 群

5. AB の (i, j)-成分は $\sum_{k=1}^{n} a_{ik} b_{kj}$ である。$(AB)C$, $A(BC)$ の (i, j)-成分はそれぞれ

$$\begin{aligned} ((AB)C)_{ij} &= \sum_{k=1}^{n} (AB)_{ik} c_{kj} = \sum_{k=1}^{n} \sum_{\ell=1}^{n} (a_{i\ell} b_{\ell k}) c_{kj} \\ (A(BC))_{ij} &= \sum_{p=1}^{n} a_{ip} (BC)_{pj} = \sum_{p=1}^{n} \sum_{q=1}^{n} a_{ip} (b_{pq} c_{qj}) \end{aligned}$$

   であるから、これらは等しい。

   (二つの行列が等しいことの定義は、すべての対応する成分が等しいことである。)

6. 直接計算することによって

$$\begin{aligned} (\alpha_1 \alpha_2)\alpha_3 &= ((a_1 + b_1 i)(a_2 + b_2 i))(a_3 + b_3 i) = ((a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2) i)(a_3 + b_3 i) \\ &= ((a_1 a_2 - b_1 b_2) a_3 - (a_1 b_2 + b_1 a_2) b_3) + ((a_1 a_2 - b_1 b_2) b_3 + (a_1 b_2 + b_1 a_2) a_3) i \\ &= (a_1 a_2 a_3 - b_1 b_2 a_3 - a_1 b_2 b_3 - b_1 a_2 b_3) + (a_1 a_2 b_3 - b_1 b_2 b_3 + a_1 b_2 a_3 + b_1 a_2 a_3) i \\ \alpha_1(\alpha_2 \alpha_3) &= (a_1 + b_1 i)((a_2 + b_2 i)(a_3 + b_3 i)) = (a_1 + b_1 i)((a_2 a_3 - b_2 b_3) + (a_2 b_3 + b_2 a_3) i) \\ &= (a_1 (a_2 a_3 - b_2 b_3) - b_1 (a_2 b_3 + b_2 a_3)) + (a_1 (a_2 b_3 + b_2 a_3) + b_1 (a_2 a_3 - b_2 b_3)) i \\ &= (a_1 a_2 a_3 - a_1 b_2 b_3 - b_1 a_2 b_3 - b_1 b_2 a_3) + (a_1 a_2 b_3 + a_1 b_2 a_3 + b_1 a_2 a_3 - b_1 b_2 b_3) i \end{aligned}$$

   となるから、この二つの値は等しい。

7. (1) $((a, b)(c, d))(e, f) = (ac, ad + bc)(e, f) = (ace, acf + (ad + bc)e) = (ace, acf + ade + bce)$ である。また $(a, b)((c, d)(e, f)) = (a, b)(ce, cf + de) = (ace, a(cf + de) + bce) = (ace, acf + ade + bce)$ である。よって $((a, b)(c, d))(e, f) = (a, b)((c, d)(e, f))$ であり、結合法則が成り立つ。

   (2) $(1, 0)(a, b) = (a, b)(1, 0) = (a, b)$ となるので $(1, 0)$ が単位元である。

   (3) (a, b) について、$a = 0$ ならば $(0, b)(c, d) = (0, bc) \neq (1, 0)$ であるから (a, b) は正則元ではない。$a \neq 0$ とする。このとき $(a, b)(a^{-1}, -b/a^2) = (a^{-1}, -b/a^2)(a, b) = (1, 0)$ が成り立つ。よって (a, b) が正則元となるための必要十分条件は $a \neq 0$ で、そのときの逆元は $(a^{-1}, -b/a^2)$ である。

   これは (a, b) を多項式 $a + bx$ と見て、2 次以上の項を無視したものと本質的に同じものである。

8. (1) 省略。

   ($((a, b)(c, d))(e, f) = (a, b)((c, d)(e, f))$ を計算によって確かめればよい。実は問 6 と本質的に同じである。)

   (2) $(1, 0)(a, b) = (a, b)(1, 0) = (a, b)$ となるので $(1, 0)$ が単位元である。

   (3) $(a, b) = (0, 0)$ は零元なので正則元ではない。$(a, b) \neq (0, 0)$ と仮定する。$(a, b)(a/(a^2 + b^2), -b/(a^2 + b^2)) = (a/(a^2 + b^2), -b/(a^2 + b^2))(a, b) = (1, 0)$ が成り立つ。よって (a, b) が正則元となるための必要十分条件は $(a, b) \neq (0, 0)$ で、そのときの逆元は $(a/(a^2 + b^2), -b/(a^2 + b^2))$ である。

9. (1) 省略。

(2) $(1,0,1)$ が単位元である。

(3) (a,b,c) が正則元になるための必要条件として $a \neq 0$, $c \neq 0$ がすぐに分かる。$a \neq 0$, $c \neq 0$ と仮定する。このとき $(a,b,c)(1/a,\ -b/ac,\ 1/c) = (1/a,\ -b/ac,\ 1/c)(a,b,c) = (1,0,1)$ が確認できる。よって (a,b,c) が正則となるための必要十分条件は $a \neq 0$ かつ $c \neq 0$ であることで、このとき逆元は $(1/a,\ -b/ac,\ 1/c)$ である。

(4) 計算によって確かめるだけなので省略する。

これは (a,b,c) を行列 $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ と見たものと本質的に同じものである。

10. 任意の $x,y,z \in A$ に対して
$$(xy)z = az = a, \quad x(yz) = xa = a$$
なので、この演算は結合法則をみたす。

$|A| = 1$ ならば a は単位元である。

$|A| > 1$ とする。単位元 e が存在すると仮定する。このとき $ee = e$ であるが、演算の定義より $ee = a$ である。よって $e = a$ となる。$|A| > 1$ より $x \in A - \{a\}$ が存在する。このとき a が単位元であるから $ax = x$ であるが、演算の定義より $ax = a$ である。これは $x \neq a$ に矛盾する。よって $|A| > 1$ のときは単位元は存在しない。

11. 任意の $x,y,z \in A$ に対して
$$(xy)z = xz = x, \quad x(yz) = xy = x$$
なので、この演算は結合法則をみたす。

$|A| = 1$ ならば $A = \{a\}$ として、a は A の単位元である。

$|A| > 1$ とする。単位元 e が存在すると仮定する。$|A| > 1$ より $x \in A - \{e\}$ が存在する。このとき演算の定義から $ex = e$ であるが、e が単位元であることから $ex = x$ である。これは $x \neq e$ に矛盾する。よって $|A| > 1$ のときは単位元は存在しない。

12. E_{ij} で (i,j)-成分が 1 で、他の成分がすべて 0 である 2 次正方行列を表すことにする。このとき
$$[[E_{11},E_{11}],E_{12}] = 0, \quad [E_{11},[E_{11},E_{12}]] = E_{12}$$
となり、結合法則は成り立たない。

(結合法則が成り立たないことを示すには、成り立たないような例を一つ挙げればよい。)

13. $A = \{a,b\}$ とする。任意の $x,y \in A$ に対して $xy = a$ で定まるものは可換半群である。$aa = ab = a$, $ba = bb = b$ で定まるものは非可換半群である。

14. 例えば、$2\mathbb{Z} = \{2a \mid a \in \mathbb{Z}\}$ で演算として乗法を考えたもの。

15. 例えば、$\mathbb{Z}$ で演算として乗法を考えたもの。

16. e, e' を共に単位元とする。このとき $e = ee' = e'$ であるから $e = e'$ である。よって単位元はただ一つである。

17. e を単位元とする。a をモノイドの正則元とし b, b' を共に a の逆元とする。このとき $b = b1 = b(ab') = (ba)b' = 1b' = b'$ であるから $b = b'$ である。よって a の逆元はただ一つである。

18. (単射であること) $f(m) = f(m')$ とする。$am = am'$ である。a は正則元なので、逆元 a^{-1} が存在する。a^{-1} を $am = am'$ に左からかければ $m = m'$ となる。よって f は単射である。

(全射であること) $m \in M$ とする。このとき $f(a^{-1}m) = a(a^{-1}m) = m$ となるので f は全射である。

[**別解**] $g : M \to M$ を $g(m) = a^{-1}m$ で定める。このとき $fg = gf = \mathrm{id}_M$ となるので f は全単射である。

19.

	0	1	−1
0	0	0	0
1	0	1	−1
−1	0	−1	1

20. [**解答例 1**] $A = \{x,y\}$ に以下のように演算を定義する。

	x	y
x	x	x
y	y	y

このとき、この演算は結合法則をみたしている (問 11 参照)。また x, y は共に右単位元で、左単位元は存在しない。

この例から右 (左) 単位元は、存在したとしても一意的ではないことが分かる。

[**解答例 2**] $A = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$ とおいて、行列の通常の積を演算とすれば、これは半群となる。任意に $r \in \mathbb{R}$ を取って固定する。任意の $a, b \in \mathbb{R}$ に対して $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ r & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$ であるから $\begin{pmatrix} 1 & 0 \\ r & 0 \end{pmatrix}$ は右単位元である。任意の $c, d \in \mathbb{R}$ に対して $\begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ であるから、左単位元は存在しない。

21. e を左単位元、f を右単位元とする。e が左単位元であるから $ef = f$ である。また f が右単位元であるから $ef = e$ である。よって $e = f$ で、これは A の単位元である。

22. h が f の右逆元であるとすると $fh = f \circ h = id_S$ である。しかし f は全射ではないので、これは矛盾である。よって f は右逆元をもたない。

    k が g_z の左逆元であるとすると $kg_z = k \circ g_z = id_S$ である。しかし g_z は単射ではないので、これは矛盾である。よって g_z は左逆元をもたない。

    すぐに分かるように $g_z f = id_S$ が成り立ち、よって g_z は f の左逆元、f は g_z の右逆元である。

    これによって左 (右) 逆元は、存在しても一意的ではないことも分かる。

23. g を a の左逆元、h を a の右逆元とする。$ga = ah = 1$ である。このとき $g = g1 = g(ah) = (ga)h = 1h = h$ である。よって g は a の逆元である。

代数入門問題集・解答例と解説 [20120704]

2 群

1. (1) 省略。

   (2) (i) $(\mathbb{N},\ +)$

   (ii) $(\mathbb{Q}-\{0\},\ \times)$

   (iii) $(M_n(\mathbb{R}),\ +)$ ($M_n(\mathbb{R})$ は実数を成分とする n 次正方行列全体)

   (iv) $(GL_n(\mathbb{R}),\ \times)$ ($GL_n(\mathbb{R})$ は実数を成分とする n 次の正則行列全体)

   (v) $(\mathbb{R}^n,\ +)$ (ベクトル空間)

   (vi) 連続函数全体の集合 (足し算) など

2. (1) $\alpha(x)=\alpha(y)$ とすると $xg=yg$ なので、両辺に右から g^{-1} をかけて $x=y$ となる。よって α は単射である。$z\in G$ に対して $\alpha(zg^{-1})=zg^{-1}g=z$ であるから α は全射である。

   [**別解**] $\alpha' : G\to G$ を $\alpha'(x)=xg^{-1}$ で定める。このとき、任意の $x\in G$ に対して $\alpha\alpha'(x)=\alpha(xg^{-1})=(xg^{-1})g=x$ である。同様に $\alpha'\alpha(x)=\alpha'(xg)=(xg)g^{-1}=x$ である。よって $\alpha\alpha'=\alpha'\alpha=\mathrm{id}_G$ が成り立ち、α は全単射である。

   (2) (1) と同様なので省略する。

   (3) $\gamma' : G\to G$ を $\gamma'(x)=gxg^{-1}$ で定める。このとき $\gamma\gamma'=\gamma'\gamma=\mathrm{id}_G$ が確かめられ γ は全単射である。

   (4) $\delta(x)=\delta(y)$ とする。$x^{-1}=y^{-1}$ である。この式に、右から x を、左から y をかければ $y=x$ となる。よって δ は単射である。任意の $x\in G$ に対して $xx^{-1}=x^{-1}x=1$ より $(x^{-1})^{-1}=x$ が成り立つので $\gamma(x^{-1})=x$ となり、γ は全射である。

   [**別解**] 任意の $x\in G$ に対して $(x^{-1})^{-1}=x$ が成り立つ。これは $\gamma\gamma=\mathrm{id}_G$ を意味し、よって γ は全単射である。

3. $xy\in G$ だから、 $(xy)(xy)^{-1}=1$ 両辺の左から x^{-1} をかけて $y(xy)^{-1}=x^{-1}$ さらに、両辺の左からに y^{-1} をかけて $(xy)^{-1}=y^{-1}x^{-1}$ となる。

4. $a,b\in G$ とする。仮定より $a^2=1, b^2=1, (ab)^2=1$ だから $a^{-1}=a, b^{-1}=b, (ab)^{-1}=ab$ である。一方 $(ab)^{-1}=b^{-1}a^{-1}=ba$ よって $ab=ba$ ゆえに G はアーベル群である。

5. 任意の $a\in A$ が逆元をもつことを示せばよい。$a\in A$ とする。写像 $f : A\to A$ を $f(x)=ax$ で定める。左簡約法則は f が単射であることを意味する。A は有限集合なので f は全単射となる。特に $1\in A$ に対して $1=f(b)=ab$ となる $b\in A$ が存在する。このとき $a1=a=1a=(ab)a=a(ba)$ となるので、左簡約法則により $ba=1$ も成り立つ。よって b は a の逆元である。

6. 例えば、自然数全体の集合 $\mathbb{N}$ で、演算として乗法を考えたもの。

7. $a\in A$ に対して、写像 $L_a : A\to A$ を $L_a(x)=ax$ で、写像 $R_a : A\to A$ を $R_a(x)=xa$ で定める。左簡約法則、右簡約法則はそれぞれ L_a, R_a が単射であることを意味している。$|A|<\infty$ なので、これらは共に全単射である。

   $a\in A$ とする。L_a が全単射であるから $a=L_a(b)=ab$ となる $b\in A$ が存在する。この b が A の単位元であることを示す。

   $c\in A$ とする。R_a が全射であることにより $c=R_a(d)=da$ となる $d\in A$ が存在する。このとき

   $$cb=(da)b=d(ab)=da=c$$

   が成り立つ。よって b は A の右単位元である。特に $bb=b$ が成り立つ。L_b が全射であることにより $c=L_b(f)=bf$ となる $f\in A$ が存在する。このとき

   $$bc=b(bf)=(bb)f=bf=c$$

   である。よって b は A の左単位元である。以上より b は A の単位元である。

   これで A がモノイドであることが分かった。問 5 により A は群である。

8. 一般に $(g^{-1}xg)^n=\overbrace{(g^{-1}xg)\cdots(g^{-1}xg)}^{n}=g^{-1}x^ng$ が成り立つ。$x^n=1$ ならば $(g^{-1}xg)^n=g^{-1}x^ng=g^{-1}g=1$ である。また $(g^{-1}xg)^n=1$ ならば $g^{-1}x^ng=1$ となるので、左から g を、右から g^{-1} をかければ $x^n=1$ である。よって $x^n=1$ であることと $(g^{-1}xg)^n=1$ であることは同値であり、よってその位数は一致する。

9. $m = n\ell$ $(\ell \in \mathbb{Z})$ であるならば $x^m = (x^n)^\ell = 1^\ell = 1$ である。

   $x^m = 1$ とする。$m = qn + r$ $(q, r \in \mathbb{Z},\ 0 \leq r < n)$ と一意的に書くことができる。このとき

   $$1 = x^m = (x^n)^q x^r = x^r$$

   である。位数 n の最小性より $r = 0$ である。すなわち $m = qn$ $(q \in Z)$ となる。

10. (1) G を巡回群とする。このとき適当な生成元 g が存在して、$G = \langle g \rangle$ とかける。よって G の任意の元は $g^i,\ g^j$ $(i, j \in \mathbb{Z})$ とかけて, $g^i g^j = g^{i+j} = g^j g^i$ となるから、G はアーベル群である。

    (2) 巡回群 $\langle g \rangle$ の部分群を H とする。H の任意の元は $\langle g \rangle$ の元でもあるから、g^i とかける。$g^i \in H$ となる最小の自然数 i を k とおくと、$g^k \in H$ であって、H は群だから $\langle g^k \rangle$ は H の部分群である。逆に、任意の H の元 g^j に対して,「割り算の原理 (剰余の定理)」より、適当な整数 $q,\ r$ $(0 \leq r < k)$ が存在して、$j = kq + r$ となる。このとき, $g^r = g^{j-kq} \in H$ であるが、k の最小性により、$r = 0$ となる。ゆえに、$g^j = g^{kq} = (g^k)^q \in \langle g^k \rangle$ であるから、$\langle g^k \rangle = H$ となるよって H は巡回群である。

    (3) 加法群 $\mathbb{Z}$ は 1 を生成元とする巡回群なので、部分群は $n\mathbb{Z}$ の形に限られることは (2) の証明より分かる。

11. (1) H が G の演算で群となっているとき、H は G の部分群であるという。

    (この他、「任意の H の元 $x,\ y$ に対して，$xy^{-1} \in H$ となる」など、同値なものもある。)

    (2) 任意の $x,\ y \in 2\mathbb{Z}$ に対して、適当な整数 $m,\ n$ が存在して、$x = 2m,\ y = 2n$ となる。このとき、$x - y = 2m - 2n = 2(m - n)$ だから、$x - y \in 2\mathbb{Z}$ である。ゆえに $2\mathbb{Z}$ は $\mathbb{Z}$ の部分群である。

    ($xy^{-1} \in H$ を「足し算 (加法)」の形で書くと「$x - y \in H$」である。)

    (3) $n\mathbb{Z}$ $(n \in \mathbb{N})$ はすべて $\mathbb{Z}$ の部分群である。逆に $\mathbb{Z}$ の部分群はこの形のものと $\{0\}$ に限る。

12. (1) $\Rightarrow$ (2) : $b \in bH = aH$ である。よって、ある $h \in H$ があって $b = ah$ だから $a^{-1}b = h \in H$ となる。

    (2) $\Rightarrow$ (3) : $a^{-1}b \in H$ とすると、ある $h \in H$ があって $a^{-1}b = h$ よって $b = ah \in aH$ である。

    (3) $\Rightarrow$ (4) : $b \in aH$ とすると、ある $h \in H$ があって $b = ah$ となる。よって $a = bh^{-1} \in bH$ である。

    (4) $\Rightarrow$ (5) : $a \in bH$ とすると $a \in aH$ だから $a \in aH \cap bH$ である。ゆえに $aH \cap bH \neq \phi$ である。

    (5) $\Rightarrow$ (1) : 条件より $x \in aH \cap bH$ が存在する。このとき $x \in aH$ より $x = ah$ となる $h \in H$ が存在し、$x \in bH$ より $x = bh'$ となる $h' \in H$ が存在する。$a = xh^{-1} = bh'h^{-1}$ である。

    $c \in aH$ とする。ある $h'' \in H$ に対して $c = ah''$ となる。このとき $c = bh'h^{-1}h''$, $h'h^{-1}h'' \in H$ となるので $c \in bH$ である。よって $aH \subset bH$ が成り立つ。同様に $aH \supset bH$ も成り立ち $aH = bH$ となる。

13. - $a \in G$ に対して $a^{-1}a = 1 \in H$ であるから $a \sim a$ である。
    - $a \sim b$ とする。$a^{-1}b \in H$ である。このとき $b^{-1}a = (a^{-1}b)^{-1} \in H$ となり $b \sim a$ である。
    - $a \sim b,\ b \sim c$ とする。$a^{-1}b \in H,\ b^{-1}c \in H$ である。このとき $a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$ であるから $a \sim c$ である。

    以上より $\sim$ は同値関係である。

    a を含む同値類は $aH = \{ah \mid h \in H\}$ である。

14. (1) $x,\ y \in C_G(a)$ に対して、$(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy)$ より $xy \in C_G(a)$ である。また $xa = ax$ の両辺に両側から x^{-1} をかければ $ax^{-1} = x^{-1}a$ となるので $x^{-1} \in C_G(a)$ である。よって $C_G(a)$ は G の部分群である。

    (2) $gag^{-1} = hah^{-1}$ と仮定する。このとき $a = g^{-1}hah^{-1}h = (g^{-1}h)a(g^{-1}h)^{-1}$ であるから $g^{-1}h \in C_G(a)$ である。よって $gC_G(a) = hC_G(a)$ が成り立つ。

    $gC_G(a) = hC_G(a)$ と仮定する。ある $\ell \in C_G(a)$ が存在して $h = g\ell$ となる。このとき

    $$hah^{-1} = (g\ell)a(g\ell)^{-1} = g\ell a\ell^{-1}g^{-1} = ga\ell\ell^{-1}g^{-1} = gag^{-1}$$

    である。

15. 問 14 より $C_G(a)$ は部分群であり、部分群の共通部分はまた部分群である。よって $C_G(A)$ は G の部分群である。

16. (1) $x,\ y \in N_G(H)$ に対して $(xy)H(xy)^{-1} = xyHy^{-1}x^{-1} = xHx^{-1} = H$ であるから $xy \in N_G(S)$ である。また $xHx^{-1} = H$ の両辺に左から x^{-1}、右から x をかければ $H = x^{-1}Hx = x^{-1}H(x^{-1})^{-1}$ となるので $x^{-1} \in N_G(H)$ となる。

(2) $gHg^{-1} = hHh^{-1}$ と仮定する。このとき $H = h^{-1}gHg^{-1}h = (h^{-1}g)H(h^{-1}g)^{-1}$ となるので $h^{-1}g \in N_G(H)$ である。よって $gN_G(H) = hN_G(H)$ である。
$gN_G(H) = hN_G(H)$ と仮定する。ある $\ell \in N_G(H)$ が存在して $h = g\ell$ となる。このとき

$$hHh^{-1} = (g\ell)H(g\ell)^{-1} = g\ell H\ell^{-1}g^{-1} = gHg^{-1}$$

が成り立つ。

17. $Z(G) = C_G(G)$ なので中心化群が部分群であることから中心も部分群である。

18. (1) $\det M = \det N = 1$ ならば $\det(MN) = (\det M)(\det N) = 1$ である。また $\det M = 1$ ならば $\det M^{-1} = (\det M)^{-1} = 1$ である。
(2) $S, T \in O(n)$ とする。このとき ${}^t(ST)(ST) = {}^tT{}^tSST = E$ なので $ST \in O(n)$ である。また ${}^tSS = E$ より $({}^tS)^{-1} = {}^t(S^{-1})$ に注意して、${}^t(S^{-1})(S^{-1}) = E$ となる。よって $S^{-1} \in O(n)$ である。
(3) $SO(n) = SL_n(\mathbb{R}) \cap O(n)$ なので、これは部分群である。
(4) (2) とほぼ同様なので省略する。

19. (1) $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $\sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $\sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$
(2) 記号を簡単にするため、上記 σ_i を単に i と書くことにすると乗法表は以下の通りである。

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	3	1	6	4	5
3	3	1	2	5	6	4
4	4	5	6	1	2	3
5	5	6	4	3	1	2
6	6	4	5	2	3	1

(3) (1 2 3 5)(4 7)
(4) $\sigma_1 = ()$ (単位元は通常このように表される), $\sigma_2 = (1\ 2\ 3)$, $\sigma_3 = (1\ 3\ 2)$, $\sigma_4 = (2\ 3)$, $\sigma_5 = (1\ 3)$, $\sigma_6 = (1\ 2)$

20. (1) $s^n = t^2 = 1$ は定義より明らかである。

$$\begin{aligned} ts &= \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ n & n-1 & \cdots & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 2 & 3 & \cdots & n & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ n-1 & n-2 & \cdots & 1 & n \end{pmatrix} \\ s^{-1}t &= \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ n & 1 & \cdots & n-2 & n-1 \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ n & n-1 & \cdots & 2 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ n-1 & n-2 & \cdots & 1 & n \end{pmatrix} \end{aligned}$$

であるから $ts = s^{-1}t$ も分かる。
(2) (1) の関係より、s, s^{-1}, t, t^{-1} の有限個の積は s^it^j $(i, j \in \mathbb{Z})$ の形に書けることが分かる。また $s^n = t^2 = 1$ より $0 \le i < n$, $0 \le j < 2$ としてよいことも分かる。よって一意性を示せばよい。$0 \le i < n$ に対して

$$s^i(1) = 1 + i, \qquad s^i(2) = \begin{cases} 2+i & (0 \le i \le n-2) \\ 1 & (i = n-1) \end{cases}$$

$$s^it(1) = \begin{cases} n & (i = 0) \\ i & (1 \le i < n), \end{cases} \qquad s^it(2) = \begin{cases} n+i-1 & (0 \le i \le 1) \\ i-1 & (2 \le i < n-1) \end{cases}$$

なので s^it^j $(0 \le i < n, 0 \le j < 2)$ はすべて異なる。

(3) 乗法表は以下の通りである。

	1	s	s^2	s^3	t	st	s^2t	s^3t
1	1	s	s^2	s^3	t	st	s^2t	s^3t
s	s	s^2	s^3	1	st	s^2t	s^3t	t
s^2	s^2	s^3	1	s	s^2t	s^3t	t	st
s^3	s^3	1	s	s^2	s^3t	t	st	s^2t
t	t	s^3t	s^2t	st	1	s^3	s^2	s
st	st	t	s^3t	s^2t	s	1	s^3	s^2
s^2t	s^2t	st	t	s^3t	s^2	s	1	s^3
s^3t	s^3t	s^2t	st	t	s^3	s^2	s	1

21. (1) 乗法表は以下の通りである。

	E	$-E$	I	$-I$	J	$-J$	K	$-K$
E	E	$-E$	I	$-I$	J	$-J$	K	$-K$
$-E$	$-E$	E	$-I$	I	$-J$	J	$-K$	K
I	I	$-I$	$-E$	E	K	$-K$	$-J$	J
$-I$	$-I$	I	E	$-E$	$-K$	K	J	$-J$
J	J	$-J$	$-K$	K	$-E$	E	I	$-I$
$-J$	$-J$	J	K	$-K$	E	$-E$	$-I$	I
K	K	$-K$	J	$-J$	$-I$	I	$-E$	E
$-K$	$-K$	K	$-J$	J	I	$-I$	E	$-E$

(2) D_8 は位数 2 の元を 5 つもつが G は 1 つしかもたない。よってこれらは異なるものである。

(この G を**四元数群**といい、Q_8 という記号で書かれることが多い。)

22. (1) (i) $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}\}$。元数は 12。
(ii) $\{\overline{0}, \overline{4}, \overline{8}\}$。元数は 3。
(iii) $\{\langle\overline{4}\rangle, 1+\langle\overline{4}\rangle, 2+\langle\overline{4}\rangle, 3+\langle\overline{4}\rangle\}$。元数は 4。

(2)
- $a \in G$ とし、写像 $f : H \to aH$ $(f(h) = ah)$ が全単射であることを示す。全射は aH の定義より明らかである。また $f(h) = f(h')$ とすると $ah = ah'$ であるから、左から a^{-1} をかければ $h = h'$ となる。よって f は単射である。以上より f は全単射であり $|H| = |aH|$ が成り立つ。
- $[G : H] = n$ とする。G 左剰余類分解して表すと、$G = a_1H \cup \cdots \cup a_nH$ (共通部分のない和集合) となり $|G| = |a_1H| + \cdots + |a_nH|$ である。ここで $|a_iH| = |H|$ がすべての i について成り立つので $|G| = n|H|$ である。

(3) $a \in G$ とする。a によって生成される巡回部分群 $\langle a\rangle$ の位数が a の約数である。(2) により部分群の位数は $|G|$ の約数になるので a の位数も $|G|$ の約数である。

(4) a の位数を m とすると (3) より m は群 G の位数 $n = |G|$ の約数である。$n = m\ell$ と書くことが出来て、このとき $a^n = (a^m)^\ell = 1^\ell = 1$ である。

23.
- [対称律] $a \in G$ に対して $a = 1a1$ $(1 \in H, 1 \in K)$ となるので $a \sim a$ である。
- [反射律] $a \sim b$ とする。ある $h \in H$ と $k \in K$ が存在して $b = hak$ である。このとき $a = h^{-1}bk^{-1}$, $h^{-1} \in H$, $k^{-1} \in K$ であるから $b \sim a$ である。
- [推移律] $a \sim b$, $b \sim c$ とする。ある $h, h' \in H$ と $k, k' \in K$ が存在して $b = hak$, $c = h'bk'$ である。このとき $c = h'hakk'$ で $h'h \in H$, $kk' \in K$ なので $a \sim c$ である。

24. $|G| = p$ とし $1 \neq a \in G$ とする。a の生成する巡回部分群 $\langle a\rangle$ の位数は $|G|$ の約数だから 1 または p である。$a \neq 1$ と仮定しているので $\langle a\rangle$ の位数は p、すなわち a の位数は p となる。したがって $G = \langle a\rangle$ となり G は巡回群である。

25. G を位数 3 の群とすれば、G は巡回群であるから $G = \{1, a, a^2\}$ と書くことができる。乗法表は以下の通りである。

	1	a	a^2
1	1	a	a^2
a	a	a^2	1
a^2	a^2	1	a

26. • HK が G の部分群であるとする。$h \in H$, $k \in K$ とする。このとき $h^{-1} \in H$, $k^{-1} \in K$ であり、$h^{-1}k^{-1} \in HK$ である。HK は G の部分群だから $kh = (h^{-1}k^{-1})^{-1} \in HK$ となる。よって $KH \subset HK$ である。
また $(hk)^{-1} \in HK$ なので、ある $h' \in H$, $k' \in K$ が存在して $(hk)^{-1} = h'k'$ である。このとき $hk = (h'k')^{-1} = k'^{-1}h'^{-1} \in KH$ であるから $HK \subset KH$ である。
よって $HK = KH$ である。

• $HK = KH$ と仮定する。$h, h' \in H$, $k, k' \in K$ として $(hk)(h'k')^{-1} \in HK$ であることを示す。$HK = KH$ なので、ある $h'' \in H$, $k'' \in K$ が存在して $kk'^{-1}h'^{-1} = h''k''$ である。よって

$$(hk)(h'k')^{-1} = hkh'^{-1}h'^{-1} = hh''k'' \in HK$$

が成り立ち、したがって HK は G の部分群である。

27. 写像 $f : H \times K \to HK$ を $f(h,k) = hk$ で定める。任意の $x \in HK$ に対して $|f^{-1}(x)| = |H \cap K|$ であることを示す。これがいえれば $|HK| = |H| \cdot |K|/|H \cap K|$ は成り立つ。

$x \in HK$ とし $hk = x$ なる $h \in H, k \in K$ を一組固定して考える。$S = \{(h\ell, \ell^{-1}k) \mid \ell \in H \cap K\}$ とおけば $S \subset f^{-1}(x)$, $|S| = |H \cap K|$ であることはすぐに分かる。よって $S \supset f^{-1}(x)$ を示せばよい。$h' \in H$, $k' \in K$, $h'k' = x = hk$ とする。このとき $h^{-1}h' = kk'^{-1} \in H \cap K$ である。$h' = hkk'^{-1}$, $k' = h'^{-1}hk = (h^{-1}h')^{-1}k = (kk'^{-1})^{-1}k$ であり $kk'^{-1} \in H \cap K$ であるから $(h', k') \in S$ である。したがって $S \supset f^{-1}(x)$ がいえて、主張は成り立つ。

28. 例えば、3 次対称群 S_3 を G とし、$H = \langle (1\ 2) \rangle$, $K = \langle (1\ 3) \rangle$ とする。

29. $H \cup K = G$ と仮定する。H, K は真の部分群だから、ある a, $b \in G$ が存在して、$a \notin H$, $b \notin K$ である。このとき、仮定より $a \in K$, $b \in H$, $ab \in H \cup K$ である。$ab \in H$ ならば $b \in H$ より $a = (ab)b^{-1} \in H$ となり矛盾である。同様に $ab \in K$ ならば $a \in K$ より $b = (ba)a^{-1} \in K$ となり矛盾である。よって $H \cup K \subsetneq G$ である。

30. G の H による右剰余類は二つなので $G = H \cup (G - H)$ が剰余類分解となる。よって $a \notin H$ に対して $Ha = G - H$ である。同様のことが左剰余類分解についても成り立つので、$a \notin H$ に対して $aH = G - H$ である。よって任意の $g \in G$ に対して $gH = Hg$ が成り立ち、H は G の正規部分群である。

31. (1) $g_1N = g_1'N$, $g_2N = g_2'N$ とする。ある $n_1, n_2 \in N$ が存在して $g_1' = g_1n_1$, $g_2' = g_2n_2$ である。また $Ng_2 = g_2N$ が成り立っているので、ある $n_3 \in N$ が存在して $n_1g_2 = g_2n_3$ である。よって

$$g_1'g_2' = g_1n_1g_2n_2 = g_1g_2n_3n_2$$

が成り立ち $n_3n_2 \in N$ であるから $(g_1'g_2')N = (g_1g_2)N$ である。よって、この演算は矛盾なく定義できる。

(2) 結合法則は明らかに成り立つ。また 1_GN は単位元となる。また $gN \in G/N$ に対して $g^{-1}N$ がその逆元である。以上より G/N は群である。

32. (1) • $a \in G$ について $a = 1a1^{-1}$ なので $a \sim a$ である。
• $a \sim b$ とする。ある $g \in G$ があって $b = gag^{-1}$ である。このとき $a = g^{-1}b(g^{-1})^{-1}$ であるから $b \sim a$ である。
• $a \sim b$, $b \sim c$ とする。ある $g, h \in G$ があって $b = gag^{-1}$, $c = hbh^{-1}$ である。このとき $c = hgag^{-1}h^{-1} = (hg)a(hg)^{-1}$ であるから $a \sim c$ である。

(2) $a \in G$ を含む共役類は $C = \{b \in G \mid a \sim b\} = \{gag^{-1} \mid g \in G\}$ である。写像 $f : G \to C$ を $f(g) = gag^{-1}$ で定める。問 14 により、任意の $b \in C$ に対して $|f^{-1}(b)| = |C_G(a)|$ となり、よって $|C| = |G : C_G(a)|$ である。

(3) $\{()\}$, $\{(1\ 2), (1\ 3), (2\ 3)\}$, $\{(1\ 2\ 3), (1\ 3\ 2)\}$

(4) (問 20 の記号を用いると) $\{1\}$, $\{s^2\}$, $\{s,\ s^3\}$, $\{t,\ s^2t\}$, $\{st,\ s^3t\}$

33. $a \in G$ を含む共役類は $C = \{b \in G \mid a \sim b\} = \{gag^{-1} \mid g \in G\}$ である。$|C| = 1$ ということは、任意の $g \in G$ に対して $gag^{-1} = a$ であるということである。このとき $ga = ag$ が任意の $g \in G$ について成り立つから、a は G の中心に入る。

逆に中心の元 a に対しては $gag^{-1} = a$ が任意の $g \in G$ について成り立つから $C = \{a\}$ である。

34. G の共役類を $C_1, C_2, \cdots, C_k$ とする。これは共通部分のない和なので $|G| = \sum_{i=1}^{k} |C_i|$ である。C_i の代表元を a_i とすると、問 32 (2) によって $|C_i| = |G : C_G(a_i)|$ であり、特に $|C_i|$ は $|G|$ の約数である。今、$|G|$ は p-べきと仮定しているので $|C_i|$ も p-べきである。また 1_G は G の中心の元なので、1_G を含む共役類は $\{1_G\}$ である。$C_1 = \{1_G\}$ とおくと

$$|G| = 1 + \sum_{i=2}^{k} |C_i|$$

(このような式を**類等式**という) で、$|G|$, $|C_i|$ は p-べきである。よって、$2 \le i \le k$ なるある i について $|C_i| = 1$ でなければならず、このとき C_i は中心に含まれる。

35. H を G の正規部分群とする。$h \in H$ に対して、その共役がすべて H に含まれることを示せばよい。$g \in G$ とすると、H が正規部分群であることから $ghg^- \in gHg^{-1} = H$ が成り立つ。

群 G のいくつかの共役類の和が G の部分群 H であるとする。$a \in H$ ならば a の共役はすべて H に含まれる。すなわち $a \in H$, $g \in G$ ならば $gag^{-1} \in H$ である。これは H が G の正規部分群であることを意味する。

36. 問 32 (3), (4) と問 35 を用いればよい。

(1) $\{()\}$, $\{(), (1\ 2\ 3), (1\ 3\ 2)\}$, S_3

(2) $\{1\}$, $\{1, s^2\}$, $\{1, s, s^2, s^3\}$, $\{1, s^2, t, s^2t\}$, $\{1, s^2, st, s^3t\}$, D_8

37. $h \in H$, $k \in K$ とする。$hk \in Hk = kH$ であるから、$hk = kh'$ となる $h' \in H$ が存在する。また $hk = hK = Kh$ であるから $hk = k'h$ となる $k' \in K$ が存在する。このとき $kh' = k'h$ より $h'h^{-1} = k^{-1}k' \in H \cap K = \{1\}$ である。よって $h' = h$, $k' = k$ となり、$hk = kh$ が成り立つ。

38. (1) $f(1_G) = f(1_G1_G) = f(1_G)f(1_G)$ である。両辺に右から $f(1_G)^{-1}$ をかけて $1_H = f(1_G)$ となる。

(2) $a \in G$ とする。$1_H = f(1_G) = f(aa^{-1}) = f(a)f(a^{-1})$ であり、同様に $1_H = f(a^{-1})f(a)$ である。よって $f(a^{-1}) = f(a)^{-1}$ である。

(3) $a, b \in \mathrm{Ker}(f)$ とする。このとき $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = 1_H1_H{}^{-1} = 1_H$ となるので $ab^{-1} \in \mathrm{Ker}(f)$ である。よって $\mathrm{Ker}(f)$ は G の部分群である。

$a \in \mathrm{Ker}(f)$, $g \in G$ とする。このとき $f(gag^{-1}) = f(g)f(a)f(g^{-1}) = f(g)1_Hf(g)^{-1} = 1_H$ なので $gag^{-1} \in \mathrm{Ker}(f)$ である。したがって $\mathrm{Ker}(f)$ は G の正規部分群である。

(4) $x, y \in f(G)$ とする。ある $a, b \in G$ が存在して $f(a) = x$, $f(b) = y$ である。このとき $xy^{-1} = f(a)f(b)^{-1} = f(ab^{-1}) \in f(G)$ であるから $f(G)$ は H の部分群である。

(5)
- f が単射であるとする。$f(1_G) = 1_H$ であるから、$f(a) = 1_H$ となる $a \in G$ は 1_G だけであり、よって $\mathrm{Ker}(f) = \{1_G\}$ である。
- $\mathrm{Ker}(f) = \{1_G\}$ と仮定する。$f(a) = f(b)$ とすると $1_H = f(b)f(b)^{-1} = f(a)f(b^{-1}) = f(ab^{-1})$ となる。よって $ab^{-1} \in \mathrm{Ker}(f) = \{1_G\}$、すなわち $ab^{-1} = 1_G$ となり $a = b$ である。したがって f は単射である。

39. (1)
- $\bar{f}$ が定義できるとする。任意の $n \in N$ に対して $1N = nN$ であるから $f(1) = \bar{f}(1N) = \bar{f}(nN) = f(n)$ である。よって $n \in K$ であり、$N \subset K$ となる。
- $N \subset K$ とする。$a, b \in G$ に対して $aN = bN$ とする。このとき $a = bn$ となる $n \in N$ が存在する。よって $f(a) = f(bn) = f(b)f(n) = f(b)$ となり、$\bar{f}$ は矛盾なく定義できる。

(2) $\bar{f}((aN)(bN)) = \bar{f}((ab)N) = f(ab) = f(a)f(b) = \bar{f}(aN)\bar{f}(bN)$ である。

40. (1) $a \in G$ に対して $f(a) \in f(G)$ であるから、問 39 より $\bar{f}$ は矛盾なく定義でき、準同型である。

(2) 全射であることは明らかであるから、単射であることを示す。$\bar{f}(aK) = \bar{f}(bK)$ とする。$f(a) = f(b)$ である。問 38 (2) より $1 = f(a)f(b)^{-1} = f(a)f(b^{-1}) = f(ab^{-1})$ である。よって $ab^{-1} \in K$ となり $aK = bK$ である。したがって $\bar{f}$ は単射である。

41. G, H を群、$(g, h), (g', h'), (g'', h'') \in G \times H$ とする。

- (結合法則) $((g, h)(g', h'))(g'', h'') = (gg', hh')(g'', h'') = ((gg')g'', (hh')h'') = (g(g'g''), h(h'h'')) = (g, h)(g'g'', h'h'') = (g, h)((g', h')(g'', h''))$ である。
- (単位元の存在) $(g, h)(1_G, 1_H) = (1_G, 1_H)(g, h) = (g, h)$ である。よって、$(1_G, 1_H)$ が単位元である。
- (逆元の存在) $(g, h)(g^{-1}, h^{-1}) = (gg^{-1}, hh^{-1}) = (1_G, 1_H)$, $(g^{-1}, h^{-1})(g, h) = (g^{-1}g, h^{-1}h) = (1_G, 1_H)$ である。よって、(g, h) の逆元は (g^{-1}, h^{-1}) である。

以上より $G \times H$ は $(g, h)(g', h') = (gg', hh')$ の演算によって群になる。

42. $G = \{1, a\}$, $H = \{1, b\}$ とすると $G \times H = \{(1, 1), (1, b), (a, 1), (a, b)\}$ で乗法表は以下のようになる。

	$(1,1)$	$(1,b)$	$(a,1)$	(a,b)
$(1,1)$	$(1,1)$	$(1,b)$	$(a,1)$	(a,b)
$(1,b)$	$(1,b)$	$(1,1)$	(a,b)	$(a,1)$
$(a,1)$	$(a,1)$	(a,b)	$(1,1)$	$(1,b)$
(a,b)	(a,b)	$(a,1)$	$(1,b)$	$(1,1)$

43. (1) $H = \{1, s^2\}$ である。任意の $g \in G$ に対して $g1g^{-1}1$, $gs^2g^{-1} = s^2$ が成り立つ (すなわち $1, s^2$ は G の中心に含まれる) ので H は G の正規部分群である。

(2) $1H = \{1, s^2\}$, $sH = \{s, s^3\}$, $tH = \{t, s^2t\}$, $stH = \{st, s^3t\}$

(3) ($1H$ は通常 H と書かれるが、左剰余類であることをはっきりさせるため $1H$ と書くことにする。)

	$1H$	sH	tH	stH
$1H$	$1H$	sH	tH	stH
sH	sH	$1H$	stH	tH
tH	tH	stH	$1H$	sH
stH	stH	tH	sH	$1H$

(この乗法表はクラインの四元群 (問 42 参照) と本質的に同じであることが分かる。)

44. $G/Z(G) = \langle aZ(G)\rangle$ とする。このとき G の任意の元は $a^i z$ ($i \in \mathbb{Z}$, $z \in Z(G)$) と書くことが出来る。$a^i z$ と $a^j z'$ について $(a^i z)(a^j z') = (a^j z')(a^i z)$ が簡単に分かるので G はアーベル群である。

45. G を位数 p^2 の群とする。問 34 より $Z(G) \neq \{1\}$ である。$Z(G)$ は G の部分群だから、その位数は p^2 または p である。$|Z(G)| = p^2$ ならば $G = Z(G)$ で、中心の定義より G はアーベル群である。$|Z(G)| = p$ とすると $|G/Z(G)| = p$ で、問 24 よりこれは巡回群である。よって問 44 より G は巡回群になるが、このとき $G = Z(G)$ なので、これは矛盾である。

46. $|\mathbb{Q} : H| = n < \infty$ とする。剰余群 $\mathbb{Q}/H$ は位数 n の有限群なので、任意の $a \in \mathbb{Q}$ に対して $na \in H$ となる。$r \in Q$ とすると $r/n \in \mathbb{Q}$ で $r = n(r/n)$ なので $r \in H$ である。よって $\mathbb{Q} = H$ である。

47. (1) $h, h' \in H$ に対して $(ghg^{-1})^{-1}(gh'g^{-1}) = gh^{-1}g^{-1}gh'g^{-1} = gh^{-1}h'g^{-1} \in gHg^{-1}$ であるから gHg^{-1} は G の部分群である。

    (2) 問 16 (2) より、H の異なる共役と $N_G(H)$ による剰余類は一対一に対応する。]

48. 有限群の元の位数は、その群の位数の約数であるから 1, 2, 4 のいずれかである。位数 1 の元は単位元に限る。位数 4 の元が存在すれば、その群は巡回群である。

    単位元以外のすべての元の位数が 2 であると仮定する。よってすべての元 g について $g^{-1} = g$ が成り立つ。$G = \{1, a, b, c\}$ とし、その演算表を考えれば

	1	a	b	c
1	1	a	b	c
a	a	1		
b	b		1	
c	c			1

    となるが、群の演算表の各行各列には、同じ要素が現れないことから

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

    でなければならない。これはクラインの四元群 (問 42 参照) と同じものである。

    よって位数 4 の群は (1) 巡回群、(2) クラインの四元群、のいずれかである。

49. (1) $gx = y$ とする。このとき $x = 1x = (g^{-1}g)x = g^{-1}(gx) = g^{-1}y$ である。

    (2)
    - 任意の $x \in X$ に対して $1_G x = x$ より $x \sim x$ である。
    - $x \sim y$ とする。ある $g \in G$ があって $y = gx$ である。このとき (1) より $g^{-1}y = x$ であるから $y \sim x$ である。
    - $x \sim y$, $y \sim z$ とする。$gx = y$, $hy = z$ となる $g, h \in G$ が存在する。このとき $z = hy = h(gx) = (hg)x$ なので $x \sim z$ である。

    以上より $\sim$ は同値関係である。

    (3) $g, h \in G_x$ とする。$gx = x, hx = x$ であり、(1) より $h^{-1}x = x$ も成り立つ。よって $(gh^{-1})x = g(h^{-1}x) = gx = x$ となり $gh^{-1} \in G_x$ である。したがって G_x は G の部分群である。

    (4) 「$gx = hx \iff gG_x = hG_x$」を示す。

    $\Rightarrow$) $gx = hx$ とする。このとき $(h^{-1}g)x = h^{-1}(gx) = h^{-1}(hx) = (h^{-1}h)x = 1x = x$ となり、$h^{-1}g \in G_x$ である。よって $gG_x = hG_x$ である (問 12 参照)。

    $\Leftarrow$) $gG_x = hG_x$ とする。$h \in gG_x$ であるから、ある $k \in G_x$ が存在して $h = gk$ である。このとき $hx = (gk)x = g(kx) = gx$ である。

これによって x を含む G-軌道 $\{gx \mid g \in G\}$ と G の G_x による左剰余類全体の集合 G/G_x の間に全単射があることが分かり、G-軌道に含まれる元の数は $|G : G_x|$ である。

50. まず、頂点や辺に関する基本的な情報を考える。

面の数 (n)	面の形 (正 m 角形)	頂点の数 (p)	一つの頂点から出る辺の数 (q)
4	3	4	3
6	4	8	3
8	3	6	4
12	5	20	3
20	3	12	5

正 n 面体の頂点の集合全体を X、自己同型群を G とする。自然に G は X に作用し、X 全体が一つの G-軌道になっている。$x \in X$ とすると、問 49 (4) より $|X| = |G : G_x| = |G|/|G_x|$ である。ここで G_x は頂点 x を動かさない変換全体なので、回転と裏返しで、丁度 $2q$ 個の元からなることが分かる。したがって $|G| = |G_x| \cdot |X| = 2pq$ である。まとめると以下の通りである。

n	4	6	8	12	20
$\lvert G\rvert$	24	48	48	120	120

正方形の各面の中心に頂点を取って結ぶと正 8 面体が得られる。逆に正 8 面体の各面の中心に頂点を取れば正方形が得られる。したがって正方形を正方形に移す変換は正 8 面体を正 8 面体に移す。すなわち正方形の自己同型群は正 8 面体の自己同型群と一致する。このような関係を**双対**という。正 12 面体の双対は正 20 面体で、正 4 面体は自己双対的である (双対も正 4 面体ということ)。

51. $f : S \to G$ を、任意の $s \in S$ に対して $f(s) = 1_G$ で定めれば、f が $\mathrm{Map}(S, G)$ の単位元であることが簡単に確かめられる。

代数入門問題集・解答例と解説 [20120704]

3 環

1. $a \in R$ を左零因子であると仮定する。ある $0 \neq b \in R$ があって $ab = 0$ である。更に a は正則元であるとする。$a^{-1} \in R$ が存在する。このとき $0 = a^{-1}0 = a^{-1}ab = 1b = b$ となり $b \neq 0$ に矛盾する。したがって a は正則元ではない。

2. 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。

3. $(1-a)^2 = 1 - 2a + a^2 = 1 - a$ である。

4. $a^n = 0$ 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。

5. $a^m = 0$, $b^n = 0$ $(m, n \in \mathbb{N})$ 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。

6. $2a = (2a)^2 = 4a^2 = 4a$ であるから、$2a = 0$ である。

7. $a + 12\mathbb{Z}$ 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。

8. (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) $\overline{0} \cdot \overline{4} = \overline{0}$, $\overline{2} \cdot \overline{4} = \overline{2}$, $\overline{4} \cdot \overline{4} = \overline{4}$ 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。)

9. (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。
   - $d = 1$ とする。ある $x, y \in \mathbb{Z}$ があって $ax + ny = 1$ である。よって $(a+n\mathbb{Z})(x+n\mathbb{Z}) = 1 + n\mathbb{Z}$ となり $a + n\mathbb{Z}$ は正則元である。正則元は零因子ではないので $a + n\mathbb{Z}$ は零因子ではない。

   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 (1) の証明の後半から $a + n\mathbb{Z}$ 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) 「f が写像になる $\iff$ m は n の約数である」を示す。
   - $\Rightarrow$) f を写像とする。$n + n\mathbb{Z} = 0 + n\mathbb{Z}$ なので $n + m\mathbb{Z} = f(n + n\mathbb{Z}) = f(0 + n\mathbb{Z}) = 0 + m\mathbb{Z}$ である。したがって $n \in m\mathbb{Z}$ となり $m \mid n$ である。
   - $\Leftarrow$) $m \mid n$ とする。$n = m\ell$ となる $\ell \in \mathbb{N}$ が存在する。$a + n\mathbb{Z} = b + n\mathbb{Z}$ と仮定する。ある $k \in \mathbb{Z}$ が存在して $a - b = nk$ となる。このとき $a - b = nk = m(\ell k)$ となるので $a + m\mathbb{Z} = b + m\mathbb{Z}$ である。よって f は定義される。

   以上より f が写像になるための必要十分条件は $m \mid n$ 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) $\ell \mid n$, $m \mid n$ であるから (3) と同じようにして f が定義されることが確認できる。$|\mathbb{Z}/n\mathbb{Z}| = n$, $|\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}| = \ell m = n$ 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) $U(\mathbb{Z}/n\mathbb{Z})$ を $\mathbb{Z}/n\mathbb{Z}$ の単数群、すなわち正則元全体の集合、とする。(5) の全単射 $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ を考える。$\ell \mid n$, $m \mid n$ であるから $n\mathbb{Z} \subset \ell\mathbb{Z}$, $n\mathbb{Z} \subset m\mathbb{Z}$ であることに注意する。

- $a+n\mathbb{Z} \in U(\mathbb{Z}/n\mathbb{Z})$ とする。ある $b+n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ があって $1+n\mathbb{Z} = (a+n\mathbb{Z})(b+n\mathbb{Z}) = ab+n\mathbb{Z}$ である。すなわち $1-ab \in n\mathbb{Z}$ である。このとき $1-ab \in n\mathbb{Z} \subset \ell\mathbb{Z}$ なので $b+\ell\mathbb{Z}$ は $\mathbb{Z}/\ell\mathbb{Z}$ における $a+\ell\mathbb{Z}$ の逆元であり、よって $b+\ell\mathbb{Z}$ は $\mathbb{Z}/\ell\mathbb{Z}$ の正則元である。同様にして $b+m\mathbb{Z}$ は $\mathbb{Z}/m\mathbb{Z}$ の正則元である。よって $f(U(\mathbb{Z}/n\mathbb{Z}) \subset U(\mathbb{Z}/\ell\mathbb{Z}) \times U(\mathbb{Z}/m\mathbb{Z})$ である。
- $f(a+n\mathbb{Z}) \in U(\mathbb{Z}/\ell\mathbb{Z}) \times U(\mathbb{Z}/m\mathbb{Z})$ とする。$a+\ell\mathbb{Z} \in U(\mathbb{Z}/\ell\mathbb{Z})$ かつ $a+m\mathbb{Z} \in U(\mathbb{Z}/m\mathbb{Z})$ である。ある $b, c \in \mathbb{Z}$ があって $ab+\ell\mathbb{Z} = 1+\ell\mathbb{Z}$, $ac+m\mathbb{Z} = 1+m\mathbb{Z}$ となる。f が全単射であることから、$d \in \mathbb{Z}$ が存在し、$f(d+n\mathbb{Z}) = (b+\ell\mathbb{Z}, c+m\mathbb{Z})$ となる。すなわち $d+\ell\mathbb{Z} = b+\ell\mathbb{Z}$, $d+m\mathbb{Z} = c+m\mathbb{Z}$ である。このとき

$$f(ad+n\mathbb{Z}) = (db+\ell\mathbb{Z}, dc+m\mathbb{Z}) = (ab+\ell\mathbb{Z}, ac+m\mathbb{Z}) = (1+\ell\mathbb{Z}, 1+m\mathbb{Z}) = f(1+n\mathbb{Z})$$

となる。f が全単射なので $ad+n\mathbb{Z} = 1+n\mathbb{Z}$ となり、$d+n\mathbb{Z}$ は $a+n\mathbb{Z}$ の逆元となる。したがって $a+n\mathbb{Z} \in U(\mathbb{Z}/n\mathbb{Z})$ である。よって $f(U(\mathbb{Z}/n\mathbb{Z}) \supset U(\mathbb{Z}/\ell\mathbb{Z}) \times U(\mathbb{Z}/m\mathbb{Z})$ である。

よって $f(\mathbb{Z}/n\mathbb{Z}) = U(\mathbb{Z}/\ell\mathbb{Z}) \times U(\mathbb{Z}/m\mathbb{Z})$ が成り立ち、f が全単射であることからその個数について $\varphi(n) = \varphi(\ell)\varphi(m)$ 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。

10. $d = \gcd(a,b)$, $d' = \gcd(b,r)$ とおく。$d \mid b$, $d \mid a-bq = r$ なので d は b, r の公約数であり $d \mid d'$ となる。また $d' \mid b$, $d' \mid bq+r = a$ なので d' は a, b の公約数であり $d' \mid d$ である。よって $d = d'$ である。

11. 問 10 より $\gcd(a,b) = \gcd(a_0, a_1) = \gcd(a_1, a_2) = \cdots = \gcd(a_n, a_{n+1}) = \gcd(a_n, 0) = a_n$ である。

12. **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。

13. 問 11 のように a_i, q_i, n を定める。$a_n = \gcd(a,b)$ である。$a_n = 1a_n + 0a_{n+1}$ である。

$a_n = a_i x_i + a_{i+1} y_i$ なる $x_i, y_i \in \mathbb{Z}$ が存在するとき $a_n = a_{i-1}x_{i-1} + a_i y_{i-1}$ なる $x_{i-1}, y_{i-1} \in \mathbb{Z}$ が存在することを示せば、これを繰り返して x_0, y_0 が条件を満たすことが分かる。

$a_{i+1} = a_{i-1} - a_i q_i$ であるから

$$a_n = a_i x_i + a_{i+1} y_i = a_i x_i + (a_{i-1} - a_i q_i) y_i = a_{i-1} y_i + a_i (x_i - q_i y_i)$$

となる。よって $x_{i-1} = y_i$, $y_{i-1} = x_i - q_i y_i$ とすればよい。

14. 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。

15. 121

    ($28n + 9$ を n を動かして順に 15 で割ってみる。)

16. 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。

17. 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。

18. $\mathbb{Z}/n\mathbb{Z}$ の単数群の位数は $\varphi(n)$ なので、問 17 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。

19. $p = 2$ 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。§4 問 4 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。

20. 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。

21. 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。

22. - 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。

23. 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。

24. $x, y \in IJ$ 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。

25. (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 ○○××××○。

26. (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。

27. (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。)

28. $s, t \in Z(R)$ 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。

29. (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。

30. 問 29 (4) と同様である。

31. $I = R$ 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。

32. (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。

33. 定義により $(a) + (b) = \{ax + by \mid x, y \in \mathbb{Z}\}$ である。これに含まれる数が d の倍数であることは明らかなので $(a) + (b) \subset (d)$ である。逆を示すには $d \in (a) + (b)$ を示せば十分である。しかしこれは問 13 に他ならない。

34. (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。

35. (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。

36. (1)
- $a \in R$ に対して $a - a = 0 \in I$ なので $a \sim a$ である。
- $a \sim b$ とする。このとき $a - b \in I$ であるから $b - a = -(a-b) \in I$ となり $b \sim a$ である。
- $a \sim b,\ b \sim c$ とする。$a - b \in I,\ b - c \in I$ である。よって $a - c = (a-b) + (b-c) \in I$ である。

以上より $\sim$ は同値関係である。

(2) $a + I = \{a + i \mid i \in I\}$

(3) $a + I = a' + I,\ b + I = b' + I$ とする。ある $i, j \in I$ があって $a' = a + i,\ b' = b + j$ とかける。このとき

$$\begin{aligned}(a' + b') - (a + b) &= (a' - a) + (b' - b) = i + j \in I\\ a'b' - ab &= (ab + aj + ib + ij) - ab = aj + ib + ij \in I\end{aligned}$$

であるから $(a' + b') + I = (a + b) + I,\ a'b' + I = ab + I$ が成り立ち、和、積、共に矛盾なく定義できる。

(4) 省略。(加法群であること、積に関して結合法則が成り立つこと、分配法則が成り立つこと、を確認すればよい。いずれも易しい。)

37. (1) $(0_{R_1}, 0_{R_2})$ が零元で $(1_{R_1}, 1_{R_2})$ が単位元である。

(2)
- (a, b) を R の正則元とし、(c, d) をその逆元とする。このとき $(1,1) = (a,b)(c,d) = (ac, bd),\ (1,1) = (c,d)(a,b) = (ca, db)$ であるから、$ac = ca = 1,\ bd = db = 1$ となり、$a,\ b$ はそれぞれ $R_1,\ R_2$ の正則元である。

  逆に $a,\ b$ をそれぞれ $R_1,\ R_2$ の正則元とすれば、(a^{-1}, b^{-1}) は (a, b) の逆元となり (a, b) は正則である。

  したがって $U(R_1 \oplus R_2) = \{(a, b) \mid a \in U(R_1),\ b \in U(R_2)\}$ である。

- $(a,b) \neq (0,0)$ を R の左零因子とする。ある $(c,d) \neq (0,0)$ があって $(0,0) = (a,b)(c,d) = (ac,bd)$ である。$(c,d) \neq (0,0)$ なので $c \neq 0$ または $d \neq 0$ である。$c \neq 0$ ならば a は 0 または左零因子である。$d \neq 0$ ならば b は 0 または左零因子である。したがって (a,b) が左零因子であるための必要十分条件は「$(a,b) \neq (0,0)$ であって、「a が左零因子または 0」、または 「b が左零因子または 0」」となることである。

38.
- $a0 = 0a = 0$ より $0 \in C$ となり、$C \neq \emptyset$ である。
- $x, y \in C$ とする。$a(x+y) = ax + ay = xa + ya = (x+y)a$ より $x+y \in C$ である。
- $x, y \in C$ とする。$a(xy) = (ax)y = (ax)y = (xa)y = x(ay) = x(ya) = (xy)a$ より $xy \in C$ である。

以上より C は R の部分環である。

39.
- $a0 = 0$ より $0 \in A$ となり、$A \neq \emptyset$ である。
- $x, y \in A$ とすると $a(x+y) = ax + ay = 0$ より $x+y \in A$ である。
- $x \in A$, $r \in R$ とする。$a(xr) = (ax)r = 0r = 0$ なので $ax \in A$ である。

以上より A は R の右イデアルである。

代数入門問題集・解答例と解説 [20120704]

4 多項式環、体

1. $(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}$ であるが、$i \neq 0,\ p$ のとき $p \mid \binom{p}{i}$ なので主張が成り立つ。

2. $f(a) = f(b)$ とする。$a^p - b^p = 0$ である。

   - $p = 2$ ならば $a^2 - b^2 = a^2 + b^2 = (a+b)^2 = (a-b)^2$ である。
   - $p \neq 2$ ならば p は奇数なので $a^p - b^p = a^p + (-b)^p = (a-b)^p$ である。

   よっていずれの場合も $0 = (a-b)^p$ となる。F は体なので $a - b = 0$、すなわち $a = b$ となる。よって f は単射である。$|F| < \infty$ なので F から F への単射 f は全単射である。

3. $\mathbb{F}_4$ は $\mathbb{F}_2$ 上 2 次元ベクトル空間の構造をもつので、その基底を $1,\ \alpha$ とする。このとき $\mathbb{F}_4 = \{0,\ 1,\ \alpha,\ 1+\alpha\}$ である。また $\mathbb{F}_4$ の乗法群 $\mathbb{F}_4 - \{0\}$ は位数 3 の群になるので、それは巡回群である。以上より、以下の演算表を得る。

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

$\times$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

   (一般に有限体 $\mathbb{F}_q$ の乗法群 $\mathbb{F}_q - \{0\}$ は素数位数でなくても巡回群になる。)

4. 次数に関する帰納法で示す。次数が 0 すなわち $f(x)$ が 0 でない定数ならば根はないので、主張は正しい。$f(x)$ を 1 次以上の次数の多項式とする。$f(x)$ が根をもたなければ主張は成り立つので、$f(x)$ は根 a をもつとする。因数定理により $f(x) = (x-a)g(x)$ と書けて $g(x)$ の次数は $n-1$ である。$b \neq a$ がやはり $f(x)$ の根であるとすると、$0 = f(b) = (b-a)g(b)$ である。$b - a \neq 0$ と K が体、よって整域であることにより $g(b) = 0$ である。したがって $f(x)$ の根は a であるか、または $g(x)$ の根である。帰納法の仮定により $g(x)$ の根は高々 $n-1$ 個なので、$f(x)$ の根は高々 n 個である。

   ($a \in K$ が多項式 $f(x)$ の根であることと $f(x) = (x-a)g(x)$ となる多項式 $g(x)$ が存在することは同値である。これを**因数定理**という。)

5. (1) 形式的な微分が和とスカラー倍を保つこと、すなわち $(f+g)' = f' + g',\ (af)' = af'\ (a \in K)$ となること、は計算によってすぐに確かめることができる。
   単項式の積 $x^n = x^m x^{n-m}$ について示す。$(x^n)' = nx^{n-1}$ であり、また $(x^m)'x^{n-m} + x^m(x^{n-m})' = mx^{n-1} + (n-m)x^{n-1} = nx^{n-1}$ なので、この場合には $(x^n)' = (x^m)'x^{n-m} + x^m(x^{n-m})'$ は成り立つ。
   一般の場合を考える。$f(x) = \sum_{i=0}^{m} a_i x^i,\ g(x) = \sum_{j=0}^{n} b_j x^j$ とする。

$$\begin{aligned}(f(x)g(x))' &= \sum_{i=0}^{m}\sum_{j=0}^{n} a_i b_j (x^{i+j})' = \sum_{i=0}^{m}\sum_{j=0}^{n} a_i b_j ((x^i)'(x^j) + (x^i)(x^j)' \\ &= \sum_{i=0}^{m}\sum_{j=0}^{n} a_i b_j (x^i)'(x^j) + \sum_{i=0}^{m}\sum_{j=0}^{n} a_i b_j (x^i)(x^j)' = f'(x)g(x) + f(x)g'(x)\end{aligned}$$

   が成り立つ。

   (2) a が $f(x)$ の重根であるとすると $f(x) = (x-a)^2 g(x)$ と書ける。このとき $f'(x) = 2(x-a)g(x) + (x-a)^2 g'(x)$ なので $f(a) = f'(a) = 0$ である。
   $f(a) = f'(a) = 0$ と仮定する。因数定理より $f(x) = (x-a)g(x)$ と書ける。$f'(x) = g(x) + (x-a)g'(x)$ より $0 = f'(a) = g(a)$ である。よって因数定理より $g(x) = (x-a)h(x)$ と書くことができ、a は $f(x)$ の重根である。

6. K の元数を q とする。K から K への写像は q^q 個ある。一方で、$q-1$ 次以下の多項式も q^q 個あるので、これらがすべて写像として異なることをいえばよい。

   $f(x), g(x)$ を $q-1$ 次以下の多項式とし、K から K への写像として等しいと仮定する。このとき $h(x) = f(x) - g(x)$ も $q-1$ 次以下の多項式であって、K の任意の元が $h(x)$ の根になる。$h(x) \neq 0$ ならば、問 4 によってその根の数は高々 $q-1$ 個であり、これは矛盾である。よって $h(x) = 0$、すなわち $f(x) = g(x)$ となる。

   (多項式 $x^q - x$ は K のすべての元を根にもち、写像としては 0 と等しくなる。)

7. (問 6 参照。) $K = \mathbb{Z}/2\mathbb{Z}$ とする。このとき $f(x) = x^2 + x$ は多項式としては 0 ではないが $f(0) = 0^2 + 0 = 0$, $f(1) = 1^2 + 1 = 0$ であり、0 と同じ多項式写像を与える。

8. $a = \sqrt{2} + \sqrt{3}$ とおく。
$$a^2 = 5 + 2\sqrt{6}, \quad a^3 = 11\sqrt{2} + 9\sqrt{3}, \quad a^4 = 49 + 20\sqrt{6}$$
である。ここで $\{1, a\}$, $\{1, a, a^2\}$,$\{1, a, a^2, a^3\}$ はいずれも $\mathbb{Q}$ 上一次独立であることが簡単に分かり、したがって a は 3 次以下の多項式の根にはならない。4 次式については $a^4 - 10a^2 + 1 = 0$ が成り立つことが分かるので、求める多項式は $x^4 - 10x^2 + 1$ である。

($x^4 - 10x^2 + 1 = 0$ の根は $\pm\sqrt{2} \pm \sqrt{3}$ である。)

9. $\mathbb{Q}[\sqrt{2}]$ が通常の和、差、積で閉じていること、すなわち $\mathbb{C}$ の部分環であることは明らかである。したがって $0 \neq x = a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ が逆元をもつことを示せばよい。もちろん x は $\mathbb{C}$ では逆元をもち、それは
$$x^{-1} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}$$
である。よって x^{-1} も $\mathbb{Q}[\sqrt{2}]$ の元であり、したがって $\mathbb{Q}[\sqrt{2}]$ は体である。

(同様にして、一般に $\mathbb{Q}[\sqrt{m}] = \{a + b\sqrt{m} \mid a, b \in \mathbb{Q}\}$ $(m \in \mathbb{Z})$ も体であることが分かる。)

10. (1) 対称律、反射律は明らかである。推移律を示す。$(s, r) \sim (s', r')$ かつ $(s', r') \sim (s'', r'')$ と仮定する。このとき $sr' = s'r$, $s'r'' = s''r'$ である。したがって $ss'r'' = ss''r' = s's''r$ である。ここで $s' \in S$ より $s' \neq 0$ で、かつ R が整域なので $sr'' = s''r$ となる。よって $(s, r) \sim (s'', r'')$ が成り立つ。

(2) $(r, s) \sim (a, b)$, $(r', s') \sim (a', b')$ と仮定する。仮定より $rb = sa$, $r'b' = s'a'$ が成り立っている。したがって
$$(rs' + r's)bb' = rs'bb' + r'sbb' = ss'ab' + ss'a'b = ss'(ab' + a'b)$$
となり $(rs' + r's, ss') \sim (ab' + a'b, bb')$ が成り立つ。よって和は矛盾なく定義される。また $rr'bb' = ss'aa'$ より $(rr', ss') \sim (aa', bb')$ であり、積も矛盾なく定義される。

(3)
- [加法に関する交換法則、結合法則] 加法についての交換法則が成り立つことはすぐに分かる。$(r/s + r'/s') + r''/s'' = (rs' + r's)/ss' + r''/s'' = (rs's'' + r'ss'' + r''ss')/ss's''$ であり $r/s + (r'/s' + r''/s'') = r/s + (r's'' + r''s')/s's'' = (rs's'' + r'ss'' + r''ss')/ss's''$ であるから結合法則は成り立つ。
- [乗法に関する結合法則] $(r/s \cdot r'/s') \cdot r''/s'' = (rr')/(ss') \cdot r''/s'' = (rr'r'')/(ss's'') = (r/s) \cdot (r'r''/s's'') = r/s \cdot (r'/s' \cdot r''/s'')$ であるから結合法則は成り立つ。
- [分配法則] $(r/s + r'/s') \cdot r''/s'' = (rs' + r's)/ss' \cdot r''/s'' = (rr''s' + r'r''s)/ss's'' = rr''s'/ss's'' + r'r''s/ss's''$ ここで R が整域で $s \neq 0$, $s' \neq 0$ であるから $(r/s + r'/s') \cdot r''/s'' = rr''/ss'' + r'r''/s's'' = r/s \cdot r''/s'' + r'/s' \cdot r''/s''$ となる。

(4) $S^{-1}R$ の零元は $0/1$ であり、単位元は $1/1$ であることに注意しておく。$r/s \in S^{-1}R - \{0\}$ とすると $0 \neq r \in R$, $0 \neq s \in R$ である。よって $s/r \in S^{-1}R$ となり $(r/s)(s/r) = 1_{S^{-1}R}$ となる。したがって 0 でない任意の元が正則元となり $S^{-1}R$ は体である。

(5) $\mathbb{Z}$ の商体は有理数体 $\mathbb{Q}$ である。

11. (1) $f(x) = \sum_{i=0}^{m} a_i x^i$, $g(x) = \sum_{j=0}^{n} b_j x^j$ とし、$f(x) \neq 0$, $g(x) \neq 0$ と仮定する。係数が 0 である項を略して $a_m \neq 0$, $b_n \neq 0$ と仮定してよい。このとき $f(x)g(x) = \sum_{k=0}^{m+n} \sum_{i+j=k} a_i b_j x^k$ であり、特に x^{m+n} の係数は $a_m b_n$ である。$a_m \neq 0$, $b_n \neq 0$ で R が整域であることにより $a_m b_n \neq 0$ である。よって $f(x)g(x) \neq 0$ である。

(2) n に関する帰納法で示す。$n = 1$ のときは (1) である。$n > 1$ とする。$R[x_1, x_2, \cdots, x_n]$ は $R[x_1, x_2, \cdots, x_{n-1}]$ 上一変数多項式環 $R[x_1, x_2, \cdots, x_{n-1}][x_n]$ と見ることができる。帰納法の仮定から $R[x_1, x_2, \cdots, x_{n-1}]$ は整域であるから (1) より $R[x_1, x_2, \cdots, x_n]$ も整域である。

12. (1) I を $K[x]$ の 0 でないイデアルとする。I の 0 でない元で、次数最小のものを $f(x)$ とする。($f(x)$ は一意的ではないが、その一つをとり固定する。)
$g(x) \in I$ とする。多項式の割り算を考えれば
$$g(x) = q(x)f(x) + r(x), \quad \deg(r(x)) < \deg(f(x))$$
となる $q(x)$, $r(x) \in K[x]$ が存在する。ここで $r(x) = g(x) - q(x)f(x) \in I$ となるので、$f(x)$ の次数の最小性から $r(x) = 0$ である。したがって $g(x) \in f(x)K[x]$ である。よって $I \subset f(x)K[x]$ となる。一方で $f(x) \in I$ なので $f(x)K[x] \subset I$ は明らかに成り立ち $I = f(x)K[x]$ となる。したがって I は単項イデアルである。
問 11 より $K[x]$ は整域なので $K[x]$ は単項イデアル整域である。

(2) $\alpha(x), \beta(x) \in (f(x), g(x))$, $h(x) \in K[x]$ とする。$\alpha(x) = f(x)a(x) + g(x)b(x)$, $\beta(x) = f(x)a'(x) + g(x)b'(x)$ となる $a(x),\ a'(x),\ b(x),\ b'(x) \in K[x]$ が存在する。このとき

$$\begin{aligned} \alpha(x) - \beta(x) &= f(x)(a(x) - a'(x)) + g(x)(b(x) - b'(x)) \in (f(x), g(x)) \\ h(x)\alpha(x) &= f(x)(h(x)a(x)) + g(x)(h(x)b(x)) \in (f(x), g(x)) \end{aligned}$$

であるから $(f(x), g(x))$ は $K[x]$ のイデアルである。

(3) (1) よりイデアルの次数最小の元はスカラー倍を除いて一意的に定まるので $(f(x), g(x)) = (g(x), r(x))$ を示せば十分である。$f(x) = g(x)q(x) + r(x) \in (g(x), r(x))$, $g(x) \in (g(x), r(x))$ であるから $(f(x), g(x)) \subset (g(x), r(x))$ が成り立つ。また $g(x) \in (f(x), g(x))$, $r(x) = f(x) - q(x)g(x) \in (f(x), g(x))$ より $(f(x), g(x)) \supset (g(x), r(x))$ が成り立つ。よって $(f(x), g(x)) = (g(x), r(x))$ である。

13. $g(x) \in K[x]$ に対して $g(x) + (f(x)) \in K[x]/(f(x))$ を $\overline{g(x)}$ と書くことにする。$\overline{g(x)} \neq 0$、すなわち $g(x) \notin (f(x))$ とする。このとき $\overline{g(x)}$ が逆元をもつことを示せばよい。$f(x)$ を割り切る多項式は 1 と $f(x)$ 自身しかないので、問 12 によって $\gcd(f(x), g(x)) = 1$ である。よって、やはり問 12 によって $f(x)a(x) + g(x)b(x) = 1$ となる $a(x), b(x) \in K[x]$ が存在する。このとき $\overline{g(x)b(x)} = \overline{1}$ となり、$\overline{b(x)}$ が $\overline{g(x)}$ の逆元である。

14. 自然な全射 $\mathbb{Q}[x] \to \mathbb{Q}[x]/(x^2 - 2)$ による $f(x) \in \mathbb{Q}[x]$ の像を $\overline{f(x)}$ と書くことにする。$\overline{x^2} = \overline{2}$ に注意すれば、任意の $\overline{f(x)} \in \mathbb{Q}[x]$ は $\overline{a + bx}$ $(a, b \in \mathbb{Q})$ と一意的に表されることが分かる。このとき $\Gamma : \mathbb{Q}[x]/(x^2 - 2) \to \mathbb{Q}[\sqrt{2}]$ を $\Gamma(\overline{a + bx}) = a + b\sqrt{2}$ と定めれば、これは全単射である。Γ が和を保存することはすぐに分かる。また

$$\begin{aligned} \Gamma((\overline{a + bx})(\overline{c + dx})) &= \Gamma((ac + 2bd) + (ad + bc)x) = (ac + 2bd) + (ad + bc)\sqrt{2} \\ &= (a + b\sqrt{2})(c + d\sqrt{2}) = \Gamma(\overline{a + bx})\Gamma(\overline{c + dx}) \end{aligned}$$

となり、積を保存することも分かる。

15. (1) $x^2 + x + 1$ は既約である。(既約でないならば 0 または 1 を根にもたなくてはならない。)

(2) $\mathbb{F}_2[x]/(f(x)) = \{\overline{0},\ \overline{1},\ \overline{x},\ \overline{1 + x}\}$ である。加法、乗法の演算表を書けば問 3 の体と同じになることが分かる。(実際、問 3 の解答例にある α は $\alpha^2 + \alpha + 1$ を満たしている。)

16. $f(x) = (x^3 + 1)(x^3 - 1) = (x + 1)(x - 1)(x^2 + x + 1)(x^2 - x + 1)$ である。

17. (1) 因数定理を繰り返し用いることによって $f(x) = (x - 1)^5$ となる。

(2) (1) より $f(x) = (x - 1)^p$ であることが予想されるが、実際に展開すれば、これが正しいことが確認できる。

18. (1) $g_k(x) = \prod_{j \neq k}(x - a_j)$ とすれば、$i \neq k$ に対して $g_k(a_i) = 0$ である。したがって

$$f_k(x) = \frac{\prod_{j \neq k}(x - a_j)}{\prod_{j \neq k}(a_k - a_j)}$$

とおけば、これは $f_k(a_i) = \delta_{ki}$ をみたしている。

(2) (1) を用いて $f(x) = \sum_{k=1}^{n} b_k f_k(x)$ とすればよい。

19. 商は $3x^2$ で、余りは 4 である。

20. (一般にはユークリッドの互除法による。) $f(x) = (x + 2)g(x) + 3$ より

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

である。これを $f(x)\mathbb{Q}[x]$ を法としてみれば $\overline{g(x)}^{-1} = \overline{-\frac{1}{3}(x + 2)}$ である。

21. まずユークリッドの互除法を行う。

$$\begin{aligned} x^3 + 2 &= x(x^2 + 3) + (4x + 2) \\ x^2 + 3 &= 2x(4x + 2) + (3x + 3) \\ 4x + 2 &= 6(3x + 3) + 5 \end{aligned}$$

これをもとに 5 を $f(x)$ と $g(x)$ で表す。

$$\begin{aligned} 5 &= (4x + 2) - 6(3x + 3) = (4x + 2) + (3x + 3) \\ &= (4x + 2) + ((x^2 + 3) - 2x(4x + 2)) = (x^2 + 3) + (1 - 2x)(4x + 2) \\ &= (x^2 + 3) + (1 - 2x)((x^3 + 2) - x(x^2 + 3)) = (1 - x + 2x^2)(x^2 + 3) + (1 - 2x)(x^3 + 2) \end{aligned}$$

$5^{-1} = 3$ を両辺にかけて

$$1 = (x + 3)f(x) + (6x^2 + 4x + 3)g(x)$$

である。よって $\overline{g(x)}^{-1} = \overline{6x^2 + 4x + 3}$ である。

22. $h(x) = f(x) - g(x)$ とおく。仮定から $\deg h(x) \leq n$ である。したがって $h(x)$ は高々 n 個の解をもつ。$|K| > n$ より、ある $a \in K$ があって $h(a) \neq 0$ である。したがって $f(a) \neq g(a)$ であり $f^* \neq g^*$ である。