代数入門問題集 [20070702]

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) $aH \cap bH \neq \phi$

    (H の右剰余類の場合も同様に成り立つ。)

13. 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。

14. 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。

15. 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。

16. 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。)

17. 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))

18. $A = \{1, 2, \cdots, n\}$ 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。

19. $n \geq 3$ 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。

20. 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。

21. (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 $|G| = [G : H]|H|$ 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。

22. 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。)

23. 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。

24. 位数 3 の群の乗法表を書け。

25. 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。

26. 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。

27. 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。

28. 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。

29. 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。

30. 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。

31. 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。

32. 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。

33. 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。

34. (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。

35. 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。

36. 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) $f(1_G) = 1_H$, $f(g^{-1}) = f(g)$ $(g \in G)$ 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。

37. 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。)

38. 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。)

39. H を群 G の正規部分群とする。G の H による剰余類の集合 G/H に積 $(g_1H)(g_2H) = (g_1g_2)H$ が矛盾なく定義されることを示せ。

40. 位数 8 の二面体群 $G = D_8$ を考え、問 19 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。

41. 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。

42. 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。

43. 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。

代数入門問題集・解答例と解説 [20070702]

2 群

1. (1) 省略。

   (教科書、講義ノートを見てください。このとき, 「単位元の存在」と「逆元の存在」を逆にかいてはいけません。)

   (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.

   (線型代数学でのベクトル空間の公理や、微分積分学での実数の性質を確認してみてください。足し算で群になっています。実数の場合さらに強く、体になっています。)

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。$m = qn + r$ $(q, r \in \mathbb{Z},\ 0 \le r < n)$ 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, $g^ig^j = g^{i+j} = g^jg^i$ 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 $q,\ r$ $(0 \le r < k)$ 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、同値なものもあります。)

    (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「$x - y \in H$」です。)

    (3) 任意の $x,\ y \in H$ に対して、$x - y \in H$ を満たすような $\mathbb{Z}$ の部分集合 H を考えてみてください。必ず $n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\}$ $(n \in \mathbb{Z})$ の形になるはずです。

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. (1) $x,\ y \in C_G(a),\ s \in S$ 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。

14. 問 13 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。

15. (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。

16. $Z(G) = C_G(G)$ 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。

17. (1) $\det M = \det N = 1$ ならば $\det(MN) = (\det M)(\det N) = 1$ である。また $\det = 1$ 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 ${}^t(ST)(ST) = {}^tS{}^tTTS = E$ 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。

18. (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), $\sigma_2 = (1\ 2\ 3)$, $\sigma_3 = (1\ 3\ 2)$, $\sigma_4 = (2\ 3)$, $\sigma_5 = (1\ 3)$, $\sigma_6 = (1\ 2)$

19. (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

20. (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。

(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。)

21. (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。

22.
- [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。

23. $|G| = p$ 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。

24. 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

25.
- 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。

26. 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。

27. 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。

28. $H \cup K = G$ 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。

29. 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。

30. (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 13 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 19 の記号を用いると) $\{1\}$, $\{s^2\}$, $\{s,\ s^3\}$, $\{t,\ s^2t\}$, $\{st,\ s^3t\}$

31. $a \in G$ 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。

32. 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 30 (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

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

    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。

33. 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。

34. 問 30 (3), (4) と問 33 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

35. $h \in H$, $k \in K$ 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。

36. (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 $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = 1_H 1_H{}^{-1} = 1_H$ 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 $f(gag^{-1}) = f(g)f(a)f(g^{-1}) = f(g)1_H f(g)^{-1} = 1_H$ 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。

37. 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。

38. $G = \{1,a\}$, $H = \{1,b\}$ 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)	$(a,1)$	$(1,b)$	$(1,1)$

39. 積が矛盾なく定義されることを示すには $g_1H = g_1'H$, $g_2H = g_2'H$ と仮定したときに $(g_1g_2)H = (g_1'g_2')H$ となることをいえばよい。$g_1H = g_1'H$, $g_2H = g_2'H$ と仮定する。ある $h, h' \in H$ が存在して $g_1' = g_1h$, $g_2' = g_2h'$ である。H は G の正規部分群だから、$hg_2 = g_2h''$ となる $h'' \in H$ が存在する。よって

$$g_1'g_2' = g_1hg_2h' = g_1g_2h''h' \in (g_1g_2)H$$

となるので $(g_1'g_2')H$ $(g_1g_2)H$ である。

40. (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 38 参照) と本質的に同じであることが分かる。)

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

42. G を位数 p^2 の群とする。問 32 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 23 よりこれは巡回群である。よって問 41 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。

43. $|\mathbb{Q} : H| = n < \infty$ 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。