(2013/12/12)

問題 1 $|G:H|=m$, $|G:K|=n$ とする．

$$|G:H\cap K|=|G:H||H:H\cap K|=|G:K||K:H\cap K|$$

より，$|G:H\cap K|$ は m と n の倍数で，m と n は互いに素であるから mn の倍数である．一方，$|K:H\cap K|\leqq|G:H|=m$ より，

$$|G:H\cap K|=n|K:H\cap K|\leqq mn$$

であるから $|G:H\cap K|=mn$ となり，また $|K:H\cap K|=m$ もわかる．$a_1,\ldots,a_m$ を K の部分群 $H\cap K$ による右剰余類の代表元とすると，$i\neq j$ なら $a_ia_j^{-1}\notin H\cap K$ であるが，$a_ia_j^{-1}\in K$ より $a_ia_j^{-1}\notin H$ すなわち $Ha_i\neq Ha_j$ となる．したがって $G=Ha_1+\cdots+Ha_m$ となる．特に $G=HK$ である．

問題 2 $G=\mathbf{Q}$ または $G=\mathbf{R}$ とし，演算は “+” で表す．いずれの場合も，任意の $x\in G$ と任意の正の整数 n について $x=ny$ となる $y\in G$ が存在する．実際，有理数あるいは実数として $y=\dfrac{x}{n}$ とすればよい．$H\subset G$ を有限指数の部分群とする．G は加群であるから剰余加群 G/H が定義され，仮定から有限加群となる．G/H の位数を n とすると，系 8.5 により G/H の元の位数はすべて n の約数であるから，G の任意の元 y について $ny\in H$ となる．したがって，最初に述べたことから任意の $x\in G$ は H に含まれる．すなわち，$H=G$ であり，H は真部分群ではない．

問題 3 $G=\mathbf{C}^\sharp$ とする．任意の元 $z\in\mathbf{C}^\sharp$ は $r>0$ と $0\leqq\theta<2\pi$ により $z=r(\cos\theta+i\sin\theta)$ と表される．任意の正の整数 n に対して，$w=r^{1/n}(\cos(\theta/n)+i\sin(\theta/n))$ と置けばド・モアブルの定理により $z=w^n$ となる．$H\subset G$ を有限指数の部分群とし，剰余群 G/H の位数を n とする．G の任意の元 z について $z=w^n$ となる $w\in G$ が存在するので，$z\in H$ となる．したがって，$H=G$ であり真部分群ではない．

$G=\mathbf{R}^+$ の場合も $z\in G$ に対して $w=z^{1/n}$ をとれば $z=w^n$ であるから，同様に指数有限の真部分群は存在しない．$H\subset\mathbf{R}^\sharp$ を指数有限の部分群とする．$|\mathbf{R}^+:\mathbf{R}^+\cap H|\leqq|R^\sharp:H|$ であるから，$\mathbf{R}^+\cap H$ は $\mathbf{R}^+$ の指数有限の部分群であるが，先に述べたように $\mathbf{R}^+\cap H=\mathbf{R}^+$ すなわち $\mathbf{R}^+\subset H$ しかあり得ない．

$H = \mathbf{R}^+$ であれば $\mathbf{R}^\sharp = \mathbf{R}^+ \cup \mathbf{R}^+(-1)$ より指数 2 の部分群である．$H \neq \mathbf{R}^+$ であれば，指数は 2 より少ないので 1 となり真部分群ではない．

問題 4 G が 2 面体群 D_n に同型という結論なので n は 3 以上の整数という仮定を補っておく．ab で生成される G の部分群 H は仮定から位数 n の巡回群である．H に含まれる位数 2 の元は n が偶数のときの $(ab)^{n/2}$ だけだから，$a, b \in H$ とすれば，n が偶数で $a = b = (ab)^{n/2}$ となる．しかし，この場合 $ab = (ab)^{n/2}(ab)^{n/2} = (ab)^n = 1$ となり矛盾する．したがって，G の位数は n の倍数で $2n$ 以上である．$o(a) = o(b) = 2$ の仮定から $a^{-1} = a, b^{-1} = b$ である．$c = ab$ と置けば $c^{-1} = b^{-1}a^{-1} = ba$ であるから，$ca = aba = ac^{-1} = ac^{n-1}$ となる．仮定から G の元はすべて a, b の積の形になるが，$b = (aa)b = a(ab) = ac$ であるから a, c の積にも書ける．この積で a の左に c があれば $ca = ac^{n-1}$ の関係式で入れ換えることにより，G の元はすべて $a^i c^j$ に形になる．$a^2 = c^n = 1$ より $i = 0, 1$ かつ $j = 0, \ldots, n-1$ とできるので G の位数は $2n$ 以下となり，位数が $2n$ 以上であったことと合わせて位数が $2n$ であることがわかる．すなわち，$G = \{1, c, c^2, \ldots, c^{n-1}, a, ac, ac^2, \ldots, ac^{n-1}\}$ である．p. 35 の 2 面体群の生成元 τ, σ について，$a \mapsto \tau$, $c \mapsto \sigma$ と対応させれば乗積表も同じであることがわかるので，G は 2 面体群 D_n に同型である．

問題 5 (i) $\sigma \in A \setminus \{1\}$ として $\sigma \notin C_A(I)$ を示せばよい．$\sigma \neq 1$ であるから，ある $a \in G$ について $a^\sigma \neq a$ である．$a^\sigma a^{-1} \neq 1$ で $Z(G) = 1$ であるから，ある $x \in G$ について $a^\sigma a^{-1} x \neq x a^\sigma a^{-1}$ となる．この不等式の左から $(a^\sigma)^{-1}$ を，右から a を掛けると，不等式 $a^{-1}xa \neq (a^\sigma)^{-1} x a^\sigma$ を得る．σ は同型なので $x = y^\sigma$ となる $y \in G$ が存在する．このとき

$$y^{\sigma\iota(a)} = x^{\iota(a)} = a^{-1}xa \neq (a^\sigma)^{-1} x a^\sigma = (a^\sigma)^{-1} y^\sigma a^\sigma = (a^{-1}ya)^\sigma = y^{\iota(a)\sigma}$$

であるから，$\sigma\iota(a) \neq \iota(a)\sigma$ がわかる．σ は I の元 $\iota(a)$ と可換でないので $C_A(I)$ に含まれない．

(ii) $Z(G) = 1$ の場合は $g \mapsto \iota(g)$ の対応は単射で，この対応により G を $A = \operatorname{Aut} G$ の正規部分群と同一視できる．実際，$a \in A$ と $g \in G$ について，G の自己同型 $a^{-1}\iota(g)a$ は，任意の $x \in G$ に対して

$$x^{a^{-1}\iota(g)a} = (x^{a^{-1}})^{\iota(g)a} = (g^{-1}x^{a^{-1}}g)^a = (g^a)^{-1} x g^a = x^{\iota(g^a)}$$

であることから，$a^{-1}\iota(g)a = \iota(g^a)$ であり，上記の同一視により G の自己同型 a は A での a による内部自己同型の正規部分群 G への制限に等しい．(i) より $Z(A) = 1$ であるから，さらに A は $B = \mathrm{Aut}\, A$ の正規部分群とみなすことができる．$b \in B$ による A の自己同型は b による B の内部自己同型の制限であるから，G が A の特性部分群であるという仮定により G も B の正規部分群となる．対応 $b \mapsto \iota(b)|G$ は B から A への準同型であるが，先に見たように，この準同型の A への制限は恒等写像である．したがって，この対応が単射であることを示せば $B = A$ となる．$b \in B$ が $\iota(b) = 1$ を満たすとする．すなわち b は G のすべての元と可換である．$b \neq 1$ とすると，$a \in A$ が存在して $b^{-1}ab \neq a$ となる．$a^{-1}b^{-1}ab \in A \setminus \{1\}$ であるから，ある $g \in G$ について $(a^{-1}b^{-1}ab)g \neq g(a^{-1}b^{-1}ab)$ となる．$gb = bg$ を使って

$$a^{-1}b^{-1}ag = (a^{-1}b^{-1}agb)b^{-1} = (a^{-1}b^{-1}abg)b^{-1} \neq (ga^{-1}b^{-1}ab)b^{-1} = ga^{-1}b^{-1}a$$

を得るので，この両端の左から a, 右から a^{-1} を掛けて，不等式 $b^{-1}aga^{-1} \neq aga^{-1}b^{-1}$ を得るが，$aga^{-1} \in G$ は b と可換であるから矛盾する．したがって，$b = 1$ であり $B = A$ がわかる．

(iii) G は非可換単純群であるから正規部分群 $Z(G)$ は G ではあり得ず，$Z(G) = \{1\}$ となる．したがって，この問題の (i) と (ii) がこの G について使える．$\sigma : A \to A$ を A の任意の外部自己同型とする．$\sigma(G) \neq G$ と仮定して矛盾を導く．G は A の正規部分群で σ は同型であるから，$\sigma(G)$ も A の正規部分群となる．特に $G \subset A = N_A(\sigma(G))$ である．$G \subset \sigma(G)$ であれば $\sigma^{-1}(G)$ が G の正規部分群となり，G の単純性から，これはあり得ない．$H = G \cap \sigma(G)$ と置く．H は A の正規部分群と G の交わりであるから G の正規部分群である．G は単純群であるから $G \cap \sigma(G) = H = \{1\}$ である．$h \in \sigma(G) \setminus \{1\}$ をとれば，$h \notin G$ より h は G の外部自己同型を引き起こす．特に $g \in G$ で $h^{-1}gh \neq g$ となる元が存在する．このとき $1 \neq g^{-1}h^{-1}gh \in G \cap \sigma(G) = \{1\}$ となり矛盾する．したがって，常に $\sigma(G) = G$ であり，G は A の特性部分群である．よって (ii) より $B = A$ がわかる．

問題 7 $M = \{(x, g) \in X \times G \mid x^g = x\}$ と置く．各 $x \in X$ に対して $(x, g) \in M$ は g が安定部分群 G_x に含まれることを意味している．軌道 x^G の各元 y について，G_y は G_x と共役であるから $(y, g) \in M$ となる g の数は G_x の位数にひとしい．x^G の元の数は $|G : G_x|$ であるから，$\{(y, g) \in M \mid y \in x^G\}$ の元の

数は $|G_x||G:G_x| = |G|$ となる．これは X のすべての G 軌道について成り立つので，M の元の総数は $|\operatorname{Orb}(X,G)||G|$ となる．

同じ M を次は各 $g \in G$ について数える．g を 1 つ定めると $(x,g) \in M$ は $x \in \operatorname{fix}(g)$ を意味するので，M の元の総数は $|\operatorname{fix}(g)|$ をすべての $g \in G$ について足し合わせた $\sum_{g\in G} |\operatorname{fix}(g)|$ となる．したがって，等式

$$|\operatorname{Orb}(X,G)||G| = \sum_{g\in G} |\operatorname{fix}(g)|$$

が得られ，両辺を $|G|$ で割れば問題の等式が得られる．

問題 8 $\sigma \in S_n$ の型が $1^{r_1}2^{r_2}\cdots n^{r_n}$ とする．σ を同じ文字を含まない巡回置換の積に表したとき，長さ l の巡回置換は r_l 個現れる．ここに現れる $r_l l$ 個の文字のみの置換 τ で σ を不変とするもの，すなわち $\tau^{-1}\sigma\tau = \sigma$ であるものの全体を H_l とする．各巡回置換に現れる文字のその巡回置換による置換の繰り返しは全部で l^{r_l} 個ある．また，r_l 個の巡回置換の置換は $r_l!$ 通りある．したがって，H_l の元はは全部で $l^{r_l}r_l!$ 個となる．これが $l = 1,\ldots,n$ について成り立ち，これですべての文字の置換を考えることになるので，$C_{S_n}(\sigma) = H_1\times\cdots\times H_n$ であり，その位数は各群の位数の積 $1^{r_1}2^{r_2}\cdots n^{r_n}(r_1!)(r_2!)\cdots(r_n!)$ となる．σ と共役な元の数は $|S_n|/|C_{S_n}(\sigma)|$ で $|S_n| = n!$ であるから，これは $n!/1^{r_1}2^{r_2}\cdots n^{r_n}(r_1!)(r_2!)\cdots(r_n!)$ に等しい．

問題 9 S_5 の単位元 1 以外の元の型は $(1,2)$, $(1,2,3)$, $(1,2,3,5)$, $(1,2,3,4,5)$, $(1,2)(3,4)$, $(1,2,3)(4,5)$ であるから，偶置換からなる部分群 A_5 に含まれる単位元以外の元の型は $(1,2,3)$, $(1,2)(3,4)$, $(1,2,3,4,5)$ の 3 通りである．

巡回置換 $(1,2,3)$ と S_5 で共役な元の数は $5!/(3\cdot 2!) = 20$ である．これらの元はある $\sigma \in S_5$ により $\sigma^{-1}(1,2,3)\sigma$ と書けるが，$(4,5)$ が $(1,2,3)$ と可換で $(1,2,3) = (4,5)^{-1}(1,2,3)(4,5)$ であることから σ が奇置換の場合も

$$\sigma^{-1}(1,2,3)\sigma = \sigma^{-1}(4,5)^{-1}(1,2,3)(4,5)\sigma = ((4,5)\sigma)^{-1}(1,2,3)((4,5)\sigma)$$

となり，A_5 でも共役となる．$(1,2)(3,4)$ と共役な元の数は $5!/(2^2\cdot 2!) = 15$ である．$(1,2)(3,4)$ が互換 $(1,2)$ と可換であることから，これらも同じ議論で A_5 内でも共役であることがわかる．$\tau = (1,2,3,4,5)$ と共役な元の数は $5!/5 = 24$ である．中心化群 $Z_{S_5}(\tau)$ は位数 5 の巡回群で A_5 が指数 2 の正規部分群であることから $Z_{S_5}(\tau)\cap A_5 = Z_{S_5}(\tau)$ すなわち $Z_{A_5}(\tau) = Z_{S_5}(\tau)$ がわかる．した

がって，$Z_{A_5}(\tau)$ の指数は 12 で，S_5 の共役類の 24 個の元は A_5 では 12 個の元からなる 2 つの共役類に分かれる．結局，類等式は

$$|A_5| = 1 + 20 + 15 + 12 + 12$$

となる．

N が A_5 の正規部分群であれば，N は $\{1\}$ といくつかの共役類の和集合となる．位数は $5!/2 = 60$ の約数であるから，1 でも 60 でもなければ，$2, 3, 4, 5, 6, 10, 12, 15, 20, 30$ のいずれかであるが，これらの数はいずれも 1 と類等式の項である $20, 15, 12, 12$ のうちいくつかの和にはならない．したがって A_5 は単純群である．

問題 10 群 G の位数が p^2 とする．このとき，定理 13.3 により中心 $Z(G)$ は $\{1\}$ ではない．$Z(G)$ の位数は p^2 の約数で 1 ではないから p または p^2 である．p^2 なら $G = Z(G)$ で G がアーベル群となるので，位数が p として矛盾を導けばよい．位数が p なら $G \neq Z(G)$ であるから，元 $x \in G \setminus Z(G)$ をとる．中心化群 $C_G(x)$ は G の中心 $Z(G)$ とそれに含まれない x を含むので，位数は p^2 で $C_G(x) = G$ となる．ところが，これは $x \in Z(G)$ を意味するので，x の取り方に矛盾する．したがって G はアーベル群である．

問題 11 素数 p を $|H|$ の任意の約数とするとき，p が $|G : H|$ の約数でないことを示せばよい．$|G| = p^c q$ で $(p, q) = 1$ とする．H の p シロー部分群の 1 つを Q とすると，Q は G の p 部分群であるから，定理 13.5, (1) により Q を含む G の p シロー部分群 P が存在する．p が $|H|$ の約数なので $Q \neq \{1\}$ であり，元 $h \in Q \setminus \{1\}$ をとることができる．また，P は $\{1\}$ でない p 群であるから，定理 13.3 により $Z(P) \neq \{1\}$ であり，$x \in Z(P) \setminus \{1\}$ をとることができる．$h, x \in P$ で x は中心の元なので $hx = xh$ であり，$x \in C_G(h) \subset H$ となる．$x \in Z(P)$ かつ $x \in H$ なので $P \subset C_G(x) \subset H$ となる．$|G : H||H : P| = |G : P| = q$ であるから，p は $|G : H|$ の約数でない．

問題 12 (i) n 次元数ベクトル空間 $\mathbf{F}_q^n$ の 1 次独立な横ベクトル $\mathbf{a}_1, \ldots, \mathbf{a}_n$ をとって

$$A = \begin{bmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_n \end{bmatrix}$$

とおけば $GL(n,\mathbf{F}_q)$ の元が得られる．また逆に，$GL(n,\mathbf{F}_q)$ の任意の元はこのようにして得られる．

$\mathbf{a}_1$ から順に取り方の数を計算する．$\mathbf{a}_1$ の取り方は 0 でないベクトルとして q^n-1 通りの取り方ができる．$\mathbf{a}_2$ の取り方は $\mathbf{a}_1$ の定数倍でなければよいので q^n-q 通りある．$\mathbf{a}_3$ の取り方は $\mathbf{a}_1,\mathbf{a}_2$ で生成される 2 次元部分ベクトル空間に入らないベクトルならよいので，p^n-p^2 通りある．以下同様に，$\mathbf{a}_1,\dots\mathbf{a}_i$ まで取ったとすると，$\mathbf{a}_{i+1}$ はこれらで生成される i 次元の部分ベクトル空間に入らないベクトルをとればよいので，全部で p^n-p^i 通りある．したがって，$\mathbf{a}_1,\dots\mathbf{a}_n$ の取り方の数はこれらの積

$$(q^n-1)(q^n-q)\cdots(q^n-q^{n-1})=q^{n(n-1)/2}(q^n-1)(q^{n-1}-1)\cdots(q-1)$$

となる．

$\det A=d$ であれば $\mathbf{a}_n$ を $(1/d)\mathbf{a}_n$ で置き換えた行列 A' が $\det A'=1$ をみたす．逆に，$\det A=1$ であれば第 n 行を 0 でない $d\in\mathbf{F}_q$ について d 倍すれば，行列式が d となる $GL(n,\mathbf{F}_q)$ の元が得られる．これらの対応は 1 対 1 であるから，行列式が d となる $GL(n,\mathbf{F}_q)$ の元の個数はすべての $d\in\mathbf{F}_q\setminus\{0\}$ について等しい．行列式が 1 となる $GL(n,\mathbf{F}_q)$ の元全体が $SL(n,\mathbf{F}_q)$ であるから，その元の数は $GL(n,\mathbf{F}_q)$ の位数を $\mathbf{F}_q\setminus\{0\}$ の元の数で割った

$$(q^n-1)(q^n-q)\cdots(q^n-q^{n-1})/(q-1)=q^{n(n-1)/2}(q^n-1)(q^{n-1}-1)\cdots(q^2-1)$$

となる．

(ii) $GL(n,\mathbf{F}_q)$ の位数についての (i) の結果から，シロー p 部分群の位数は $q^{n(n-1)/2}=p^{en(n-1)/2}$ である．一方，ここに書かれた行列の $*$ の部分の成分の数が $n(n-1)/2$ であるから，部分群 P の位数も $q^{n(n-1)/2}=p^{en(n-1)/2}$ となる．したがって，P は $GL(n,\mathbf{F}_q)$ のシロー p 部分群である．

問題 13 (i) H_11 は K_1/H_1 の単位元で H_21 は K_2/H_2 の単位元であり，また ϕ は群の同型であるから $\phi(H_11)=H_21$ となる．したがって $1\in H$ であり，H は空ではない．$(x_1,x_2),(y_1,y_2)\in H$ とする．このとき $\phi(H_1x_1y_1)=\phi(H_1x_1)\phi(H_1y_1)=(H_2x_2)(H_2y_2)=H_2x_2y_2$ となり，積 $(x_1,x_2)(y_1,y_2)=(x_1y_1,x_2y_2)$ も H に含まれる．また，$(x_1,x_2)\in H$ とすると，(x_1^{-1},x_2^{-1}) がその逆元で，$\phi(H_1x_1^{-1})=\phi((H_1x_1)^{-1})=(H_2x_2)^{-1}=H_2x_2^{-1}$ となり，H に含まれることがわかる．したがって，H は G の部分群である．

(ii) $i = 1, 2$ について第 i 成分への射影 $p_i : G_1 \times G_2 \to G_i$ は準同型であるから，$K_1 = p_1(H)$ と $K_2 = p_2(H)$ は，それぞれ G_1 と G_2 の部分群である．G_1 と G_2 を G の部分群と考え，$H_i = H \cap G_i$ $(i = 1, 2)$ と置く．任意の $x_1 \in K_1$ に対して $x_2 \in K_2$ で $(x_1, x_2) \in H$ となるものが存在する．$y \in H_1$ とすると $(x_1, x_2)^{-1}(y, 1)(x_1, x_2) = (x_1^{-1}yx_1, 1)$ は H の元の積なので H の元で，しかも G_1 に含まれているので $x_1^{-1}yx_1 \in H_1$ となる．したがって H_1 は K_1 の正規部分群である．同様に H_2 が K_2 の正規部分群であることもわかる．$\phi : K_1/H_1 \to K_2/H_2$ を $(x_1, x_2) \in H$ のとき $\phi(H_1x_1) = H_2x_2$ で定義する．$(y_1, y_2) \in H$ で $H_1x_1 = H_1y_1$ とすると，$x_1^{-1}y_1 \in H_1$ で $((x_1^{-1}y_1)^{-1}, 1)(x_1, x_2)^{-1}(y_1, y_2) = (1, x_2^{-1}y_2) \in H$ となり，$x_2^{-1}y_2 \in H_2$ すなわち $H_2x_2 = H_2y_2$ がわかる．したがって，この写像の定義は $(x_1, x_2) \in H$ の選び方に依らない．$x_1, y_1 \in K_1$ に対しては $(x_1, x_2), (y_1, y_2) \in H$ となるように $x_2, y_2 \in K_2$ をとれば $(x_1y_1, x_2y_2) \in H$ であるから $\phi((H_1x_1)(H_1y_1)) = \phi(H_1x_1y_1) = H_2x_2y_2 = (H_2x_2)(H_2y_2) = \phi(H_1x_1)\phi(H_1y_1)$ となり，ϕ が準同型であることがわかる．同様に準同型 $\phi' : K_2/H_2 \to K_1/H_1$ を $(x_1, x_2) \in H$ のとき $\phi'(H_2x_2) = H_1x_1$ で定義すれば，ϕ' は ϕ の逆写像となっているので，ϕ が同型であることもわかる．定義から $(x_1, x_2) \in H$ であれば $\phi(H_1x_1) = H_2x_2$ である．また逆に $x_1 \in K_1, x_2 \in K_2$ で $\phi(H_1x_1) = H_2x_2$ とすると $(y_1, y_2) \in H$ が存在して $H_1x_1 = H_1y_1$ と $H_2x_2 = H_2y_2$ となる．このとき $(x_1, x_2) = (x_1y_1^{-1}, 1)(1, x_2y_2^{-1})(y_1, y_2) \in H_1H_2H = H$ である．したがって，H は (i) で定義したものに一致する．

(iii) K_1, K_2, H_1, H_2 を (ii) と同様に定義する．このとき，K_1/H_1 の位数は G_1 の約数で K_2/H_2 の位数は G_2 の約数であるから，これらは互いに素である．一方，同型 ϕ が存在することからこれらは等しいので，$H_1 = K_1$ かつ $H_2 = K_2$ の場合しかあり得ない．$H_1 \times H_2 \subset H \subset K_1 \times K_2$ であるから，$H = H_1 \times H_2$ がわかる．

問題 14 $m = o(a)$, $n = o(b)$ とする．この条件を満たすとして元 $ab \in \langle a \rangle \times \langle b \rangle$ の位数を調べる．$(ab)^i = a^ib^i$ であるから，これが単位元 1 となるのは $a^i = 1$ かつ $b^i = 1$ のときである．例題 7.5 により，これは $m|i$ かつ $n|i$ であることと同値である．条件 $(m, n) = 1$ より， これは $mn|i$ と同じで ab の位数は mn となる．群 $\langle a \rangle \times \langle b \rangle$ の位数も mn なので，この群は ab で生成される巡回群である．

つぎに，$\langle a\rangle \times \langle b\rangle$ が巡回群とする．$\langle a\rangle \times \langle b\rangle$ が無限巡回群とすると，a, b はその 1 でない元なので位数はいずれも無限大である．しかし，$a^s b^t \in \langle a\rangle \times \langle b\rangle$ をどのようにとっても，$(a^s b^t)^i = a^{is} b^{it}$ より $a = a^1 b^0$ または $b = a^0 b^1$ は部分群 $\langle a^s b^t\rangle$ に含まれない．したがって，$\langle a\rangle \times \langle b\rangle$ は無限巡回群ではあり得ない．$m = o(a), n = o(b)$ が $l = (m, n) > 1$ を満たすとする．このとき $0 \leqq i, j < l$ について $(a^{i(m/l)} b^{j(n/l)})^l = a^{im} b^{jn} = 1$ となり，$\langle a\rangle \times \langle b\rangle$ に $x^l = 1$ を満たす元が l^2 個以上あることがわかる．これは例題 9.8 に矛盾する．したがって $(m, n) = 1$ である．