群論問題集

箱星

2024 年 8 月 28 日

1　群論の基礎

問 1. ある群において $ghg^{-1} = h^{-1}$ をみたす元 g, h がある。$(gh)^2 = g^2$ を示せ。

解答.　$ghg^{-1} = h^{-1}$ に左から h、右から g をかけると $hgh = g$ となり、左から g をかけて $(gh)^2 = g^2$ を得る。 □

問 2. G は $g^{1028} = 1, g^{550} = 1$ をみたす元 g によって生成される非自明な巡回群である。G の位数を求めよ。

解答.　$\gcd(1028, 550) = 2$ であるから、$1028m + 550n = 2$ をみたす整数 m, n が存在する。$g^2 = g^{1028m+550n} = 1$ より、G の位数は 2 である。 □

問 3. G を群とする。G から G への写像 $g \mapsto g^{-1}$ が準同型であることと G がアーベル群であることは同値であることを示せ。

解答.　$\varphi\colon G \to G$ を $\varphi(g) = g^{-1}$ をみたす写像とする。φ が準同型のとき、$gh = \varphi(g^{-1})\varphi(h^{-1}) = \varphi(g^{-1}h^{-1}) = (g^{-1}h^{-1})^{-1} = hg$ となるので、アーベルである。逆に G がアーベル群のとき、$\varphi(gh) = h^{-1}g^{-1} = g^{-1}h^{-1} = \varphi(g)\varphi(h)$ なので φ は準同型である。 □

問 4. H, K を部分群とするとき、HK が部分群であることと $HK = KH$ は同値であることを示せ。

解答.　H, K は部分群なので $H = H^{-1}, K = K^{-1}$ をみたす。HK が部分群のとき、$HK = (HK)^{-1} = K^{-1}H^{-1} = KH$ となる。逆に $HK = KH$ のとき、$h_1, h_2 \in H, k_1, k_2 \in K$ に対して $h_1k_1h_2k_2 \in HKHK = HHKK = HK$ となる。また $h \in H, k \in K$ に対し $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$ となる。よって HK は部分群である。 □

問 5. G を群とする。

(a) G がアーベル群ならば、有限位数の元からなる部分集合 H は部分群であることを示せ。

(b) 非アーベル群 G および有限位数の元 $x, y \in G$ であって xy が無限位数となるような例を挙げよ。

解答.　(a) $x, y \in H$ とすると、$x^m = y^n = 1$ となる自然数 m, n が存在する。$(xy)^{mn} = x^{mn}y^{mn} = (x^m)^n(y^n)^m = 1, (x^{-1})^m = 1$ なので、$xy, x^{-1} \in H$ である。よって H は部分群である。

(b) 無限二面体群 $\langle x, y \mid x^2 = y^2 = 1\rangle$ が例である。

□

問 6. 次を証明または反証せよ：群がアーベルであることと部分群がすべて正規であることは同値である。

解答. 正しくない。G を位数 8 の四元数群 $\{\pm 1, \pm i, \pm j, \pm k\}$ とすると、非自明な部分群は $\{\pm 1\}, \{\pm 1, \pm i\}, \{\pm 1, \pm j\}, \{\pm 1, \pm k\}$ の 4 つである。位数 4 の部分群は指数 2 なので正規部分群である。ゆえに G の部分群はすべて正規であるが、G はアーベルでない。 □

問 7. G を巡回群とする。G の部分群は巡回群であることを示せ。

解答. H を巡回群 G の部分群とする。自明な群は巡回群なので、H は非自明な群としてよい。ある $a \in G$ が存在して、H の任意の元はある $n \in \mathbb{Z}_{\geq 0}$ を用いて a^n と表せる。H の非自明な元について、n の最小値を m とする。H の元 b を任意にとり、$b = a^n$ と表す。n を m で割り $n = qm + r$ $(0 \leq r < m)$ とすると

$$b = a^n = (a^m)^q a^r$$

となるので

$$a^r = ((a^m)^q)^{-1} b$$

となる。$a^m \in H, b \in H$ より、$a^r \in H$ となる。ここで $r \neq 0$ とすると m の最小性に反するので、$r = 0$ である。よって

$$b = (a^m)^q$$

となる。したがって、H は a^m により生成される巡回群である。 □

問 8. G を群とする。以下の各条件から、G がアーベル群であることが導かれるか。

(a) $f(a, b) = ab$ で定義される関数 $f\colon G \times G \to G$ は群準同型である。

(b) G は G/H が巡回群になるような正規部分群 H をもつ。

(c) G は G/H が巡回群かつ任意の $g \in G, h \in H$ に対して $gh = hg$ となるような正規部分群 H をもつ。

解答. (a) $f((1, x)(y, 1)) = f(y, x) = yx, f(1, x)f(y, 1) = xy$ より $xy = yx$ となるので、アーベル群である。

(b) $G = S_5, H = A_5$ のとき、$G/H \cong C_2$ は巡回群であるが、G はアーベル群でない。

(c) $g_1, g_2 \in G$ とする。G/H の生成元を xH とすると、$g_1 = (xH)^{m_1}, g_2 = (xH)^{m_2}$ と表せる。これより $g_1 = x^{m_1} h_1, g_2 = x^{m_2} h_2$ $(h_1, h_2 \in H)$ と表せる。$g_1 g_2 = x^{m_1} h_1 x^{m_2} h_2 = x^{m_1} x^{m_2} h_1 h_2 = x^{m_2} x^{m_1} h_2 h_1 = x^{m_2} h_2 x^{m_1} h_1 = g_2 g_1$ となる。よって G はアーベル群である。

□

問 9. $\mathbb{F}$ を体とする。G を乗法群 $\mathbb{F} \setminus \{0\}$ の有限部分群とする。このとき G は巡回群であることを示せ。

解答. G は有限アーベル群である。$|G| = n$ とし、G は巡回群でないとすると、有限アーベル群の構造定理より、任意の $x \in G$ に対し $x^d = 1$ をみたす $d < n$ が存在する。これより $x^d = 1$ の $\mathbb{F}$ における解の個数は n となるが、これは高々 d 個の解しか持たない。よって矛盾である。 □

問 10. H を G の部分群とする。$H \times G$ の部分群

$$L = \{(h, h) \mid h \in H\}$$

を考える。L が $H \times G$ の正規部分群であることと、H が G の中心に含まれることは同値であることを示せ。

解答. $(x,x) \in L$ と $(h,g) \in H \times G$ に対して、$(h,g)(x,x)(h,g)^{-1} = (hxh^{-1}, gxg^{-1})$ である。よって L が $H \times G$ の正規部分群であることと、任意の $g \in G, h, x \in H$ に対して $hxh^{-1} = gxg^{-1}$ となることは同値である。特に h を単位元とすることで、L が $H \times G$ の正規部分群ならば任意の $g \in G, x \in H$ に対して $gx = xg$、すなわち H が G の中心に含まれることがわかる。逆に H が G の中心に含まれるとき $hxh^{-1} = gxg^{-1} = x$ である。 □

問 11. x は奇数位数の群 G の元で、逆元と共役であるとする。このとき $x = e$ であることを示せ。

解答. x, y が共役であるとき、x^{-1}, y も共役であることから、x, y^{-1} も共役となる。よって x, y, x^{-1}, y^{-1} は同じ共役類 C に属する。C のすべての元 g について $g \neq g^{-1}$ とすると、C は偶数位数である。G は奇数位数で、共役類の大きさは位数の約数なので、ある C の元 g について $g = g^{-1}$ となる。このとき $g^2 = e$ となるが、G は奇数位数なので $g = e$ である。単位元を含む共役類は単位元のみからなるので、$x = e$ である。 □

2 有限群の構造

問 1. p をある有限群の位数を割り切る最小の素数とする。このとき指数 p の部分群は正規であることを示せ。

解答. G を H の指数 p の部分群とする。剰余類の置換作用により群準同型 $G \to S_p$ を得る。この準同型の核を N とすると、$N \leq H$ となる。$|H| = k|N|$ とおくと、$|G/N| = pk$ となる。G/N は S_p の部分群と同型なので、pk は $p!$ を割り切る。ゆえに k は $(p-1)!$ を割り切るので、k の素因数は $p-1$ 以下である。一方 k は $|H|$ を割り切るので $|G|$ も割り切る。$|G|$ の最小の素因数は p なので k の素因数は p 以上である。よって $k = 1$ となり、$H = N$ は正規である。 □

問 2. p を素数とする。

(a) $n \geq 1$ に対して、位数 p^n の群は非自明な中心をもつことを示せ。

(b) (a) を用いて、位数 p^2 の群はすべてアーベル群であることを示せ。

解答. (a) 類等式より、$p^n = |Z(G)| + pm$ となる $(m \in \mathbb{Z}^+)$。これより $|Z(G)|$ は p の倍数なので、中心は非自明である。

(b) 中心の位数は p または p^2 である。位数が p であるとする。このとき $G/Z(G)$ の位数は p なので、巡回群である。これより G がアーベル群であることを示すことができる。これは中心の位数が p であることと矛盾する。従って中心の位数は p^2 なのでアーベル群である。

□

問 3. 位数 8128 の単純群は存在しないことを示せ。

解答. $8128 = 64 \times 127$ であり、127 は素数である。シロー 127 部分群はただ 1 つなので、これは正規部分群である。よって位数 8128 の単純群は存在しない。 □

問 4. この問題の目標は位数 35 の群を同型を除いて分類することである。

(a) 位数 35 のアーベル群を同型を除いてすべて求めよ。

(b) 位数 35 の群はすべてアーベル群であることを示せ。

解答. （a）有限アーベル群の基本定理より、$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ のみ。

（b）G を位数 35 の群、H をシロー 5 部分群、K をシロー 7 部分群とする。シローの定理より H の共役の個数は 7 の約数で 5 で割った余りが 1 なので、1 個である。ゆえに H は G の正規部分群である。同様に K も G の正規部分群である。$H \cap K$ は H, K の部分群なので、位数は $\gcd(5, 7) = 1$ である。HK は部分群で位数は 35 なので $G = HK$ となる。以上より

$$G = HK \cong H \times K = \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$$

はアーベル群である。

□

問 5. 位数 143 の群は巡回群であることを示せ。

解答. G を位数 143 の群、H をシロー 11 部分群、K をシロー 13 部分群とする。シローの定理より H の共役の個数は 13 の約数で 11 で割った余りが 1 なので、1 個である。ゆえに H は G の正規部分群である。同様に K も G の正規部分群である。$H \cap K$ は H, K の部分群なので、位数は $\gcd(11, 13) = 1$ である。HK は部分群で位数は 143 なので $G = HK$ となる。以上より

$$G = HK \cong H \times K = \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z} \cong \mathbb{Z}/143\mathbb{Z}$$

は巡回群である。 □

問 6. G を位数 24 の群とする。G のどのシロー部分群も正規でないとする。このとき G は対称群 S_4 と同型であることを示せ。

解答. シロー 3 部分群の個数は 8 の約数で 3 で割った余りが 1 なので、1 または 4 である。1 個のときシロー 3 部分群は正規になるので、4 個である。共役作用を考えると準同型 $\varphi\colon G \to S_4$ を得る。シロー部分群は互いに共役なので、φ は全射である[1)]。位数が等しいので φ は同型である。 □

問 7. 位数 30 の単純群は存在しないことを示せ。

解答. シロー 3 部分群の個数は $1, 10$、シロー 5 部分群の個数は $1, 6$ である。位数 30 の単純群があるとすると、シロー 3 部分群の個数は 10、シロー 5 部分群の個数は 6 となる。このとき、位数 3 の元は $2 \times 10 = 20$ 個、位数 5 の元は $4 \times 6 = 24$ 個ある。$20 + 24 > 30$ なので矛盾。よって位数 30 の単純群は存在しない。 □

問 8. ちょうど 2 つの共役類をもつ有限群を分類せよ。

解答. $|G|$ が 2 つの異なる素数 p, q で割り切れるとすると、G には位数 p, q の元が存在する。これらは共役でないので、G は少なくとも 3 つの共役類をもつことになる。よって G は p 群である。ゆえに中心は非自明で、各元は共役類をなすことより、$G = Z(G)$ は位数 2 である。よって位数 2 の巡回群のみが条件を満たす。 □

問 9. ちょうど 3 つの共役類をもつ有限群を分類せよ。

解答. $\{1\}$ は共役類である。アーベル群で条件を満たすものは位数 3 のもののみなので、以下非アーベルとする。シローの定理により、位数の素因数は 1 つまたは 2 つである。

---

1) 違くない？

位数が p^n のとき、中心 Z は非自明であり、非アーベルより $|Z| \leq 2$ である。よって $|Z| = 2$ で $p = 2$ である。また $G \setminus Z$ は共役類である。このとき G/Z は 2 つの共役類しかないので位数 2 である。よって G の位数は 4 となり、非アーベルであることと矛盾する。

位数が $p^m q^n$ ($p < q$ は素数) のとき、G の元の位数は $1, p, q$ の 3 つのみであり、同じ位数なら互いに共役となる。シロー部分群 S_p, S_q を考える。S_p の中心の元 $c \neq 1$ をとると、c の中心化群 $Z(c)$ は S_p を含むので、c の共役の数は $[G : Z(c)] = q^s$ $(s \leq n)$ となる。同様に S_q の中心の元 $d \neq 1$ をとると、d の共役の数は p^t $(t \leq m)$ となる。$1 + p^t + q^s = p^m q^n$ であるから、$p^t = p^m = 2, q^s = q^n = 3$ に限られる。位数 6 の非アーベル群は 3 次対称群のみであり、これは条件を満たす。

したがって、求める群は位数 3 の巡回群、3 次対称群のいずれかである。 □

問 10. p, q, r を $p < q < r$ をみたす素数とし、G を位数 pqr の群とする。このとき G は正規 Sylow 部分群を持つことを示せ。

解答. シロー x 部分群の個数を N_x とする。G は正規シロー部分群をもたないとすると、$N_p \mid qr, N_q \mid pr, N_r \mid pq$ より $N_p \geq q, N_q \geq p, N_r \geq p$ である。また $N_r \equiv 1 \pmod r$ かつ $p < q < r$ より $N_r = pq$ である。位数 p, q, r の元の個数はそれぞれ $N_p(p-1), N_q(q-1), N_r(r-1)$ である。位数に関する不等式

$$pqr \geq N_p(p-1) + N_q(q-1) + N_r(r-1) \geq q(p-1) + p(q-1) + pq(r-1)$$

より

$$(p-1)(q-1) \leq 1$$

となるが、これをみたす素数 $p < q$ は存在しない。よって G は正規シロー部分群をもつ。 □

3 対称群

問 1. S_n の位数 d の元の例をあげよ。存在しない場合はその理由を記せ。

(a) $n = 10, d = 30$

(b) $n = 11, d = 33$

解答. (a) $(1,2)(3,4,5)(6,7,8,9,10)$ の位数は $2, 3, 5$ の最小公倍数なので 30 である。

(b) 長さ 33 のサイクルか、長さ 3 のサイクルと長さ 11 のサイクルをもたなければならないが、$n = 11$ なのでこれは不可能である。

□

問 2. S_n を $\{1, 2, \ldots, n\}$ の置換群とする。次の元の例をあげるか、存在しない理由を述べよ。

(a) S_{13} における位数 40 の元

(b) S_{16} における位数 34 の元

証明. (a) $x = (1,2,3,4,5)(6,7,8,9,10,11,12,13) \in S_{13}$ とする。$x^n = 1$ は、n が 5 の倍数かつ 8 の倍数であることと同値なので、x の位数は 40 である。

(b) 元の位数は群の位数の約数であるが、34 は $16!$ の約数でないので、S_{16} に位数 34 の元は存在しない。

□

問 3. Q_8 を四元数群とする。$f\colon Q_8 \to S_n$ が単射準同型ならば、$n \geq 8$ であることを示せ。

解答. 単射準同型 $Q_8 \to S_7$ が存在したと仮定し、Q_8 の元を置換と同一視する。$i^2 = j^2 = k^2 = -1$ は位数 2 の偶置換なので、型は $(2,2)$ である。また $i = jk$ より i, j, k は偶置換であり、2 乗して型 $(2,2)$ になるので型は $(4,2)$ である。-1 に対応する置換を $(a_1, a_2)(a_3, a_4)$ とおくと、i, j, k の長さ 4 の巡回置換は (a_1, a_3, a_2, a_4) または (a_1, a_4, a_2, a_3) のいずれかであり、長さ 2 の巡回置換は a_1, a_2, a_3, a_4 以外からなる。しかし $i = jk$ をみたさないので、これは矛盾である。 □

問 4. (a) S_6 における位数 2 の元の共役類をすべて求めよ。
(b) A_6 についても同様のことを行え。

解答. (a) S_6 の共役類は 6 の分割と一対一対応する。位数 2 の元の共役類は、最大値が 2 である分割と一対一対応する。よって、位数 2 の元の共役類は、$(2, 1^4), (2^2, 1^2), (2^3)$ の 3 つである。

(b) 上のうち偶置換からなる共役類は $(2^2, 1^2)$ のみである。ここで $(2^2, 1^2)$ の 2 つの置換が A_n でも共役であることを示す。(a_1, a_2, a_3, a_4) を (b_1, b_2, b_3, b_4) または (b_2, b_1, b_3, b_4) に移すことを考えると、この 2 つは互換 1 つ分だけ異なるのでどちらかは偶置換である。偶置換である方を π とすると $(a_1, a_2)(a_3, a_4)$ の π による共役は $(b_1, b_2)(b_3, b_4)$ となり、A_n で共役である。よって A_6 における位数 2 の元の共役類は $(2^2, 1^2)$ である。

□

問 5. 対称群 S_3 の自己同型群を求めよ。

解答. 内部自己同型群は $S_3/Z(S_3) = S_3$ である。$(1,2), (2,3)$ は S_3 の生成元である。S_3 に位数 2 の元は 3 つあるので、生成元の自己同型による行先の決め方は高々 6 通りである。よって自己同型は高々 6 個だが、内部自己同型が 6 個なので、これらは一致する。よって S_3 の自己同型群は S_3 と同型である。 □

問 6. 交代群 A_5 は単純であることを示せ。A_4 は可解であることを示せ。

解答. A_5 の共役類の位数は $1, 12, 12, 15, 20$ である。N が A_5 の正規部分群であるとき、N は $\{1\}$ を含む共役類の和として表せる。ゆえに N の位数は 1 を含む $1, 12, 12, 15, 20$ の部分和であって、かつ 60 の約数である。このようなものは $1, 60$ しかないので、N は自明な部分群である。よって A_5 は単純である。

A_4 は $\{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ という正規部分群をもち、これはアーベル群である。よって A_4 は可解である。 □

問 7. S_4 は $(1234), (1243)$ で生成されることを示せ。

解答. $(1234)(1243)^2 = (13)$ となり、$(13)^{(1243)} = (12)$ となる。(12) の (1234) による共役を考えると、$(12), (23), (34)$ が得られる。S_4 はこれらの元で生成されるので、$(1234), (1243)$ により生成される。 □

問 8. 5 次交代群は位数 20 の部分群をもたないことを示せ。

解答. 位数 20 の部分群 H が存在したとする。A_5 は H による剰余類に作用する。H の指数は 3 なので、この作用により準同型 $\varphi\colon A_5 \to S_3$ が得られる。A_5 は単純群かつ $\operatorname{Ker}\varphi \neq A_5$ より、$\operatorname{Ker}\varphi$ は

単位群である。これより φ は単射となるが、$|A_5| > |S_3|$ と矛盾。よって位数 20 の部分群は存在しない。 $\square$

問 9. G が S_n の部分群で $G \cap A_n = \{e\}$ をみたすならば $|G| \leq 2$ であることを示せ。

解答. G の 2 つの奇置換 π, ρ に対し、$\pi^2, \pi\rho \in A_n$ なので、$\pi^2 = e = \pi\rho$ となる。よって $\pi = \rho$ となるので、G の奇置換は高々 1 つ。偶置換は e のみなので、$|G| \leq 2$ である。 $\square$

4 行列群

問 1. $\mathrm{SL}_2(\mathbb{F}_5)$ の 5 シロー部分群の個数を求めよ。

解答. $\mathrm{SL}_2(\mathbb{F}_5)$ の位数は 120 である。対角成分が 1 である上三角行列のなす群は位数 5 なので、5 シロー部分群である。同様に下三角行列を考えることで、5 シロー部分群が 2 個以上あることがわかる。シローの定理より、5 シロー部分群の個数は 24 の約数であって 5 で割って 1 余るものなので、6 である。 $\square$

問 2. $\mathrm{SL}_2(\mathbb{R})$ を行列式が 1 の実数係数 2×2 行列の群とする。

$$\sigma = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

とする。${}^t g$ を $g \in \mathrm{SL}_2(\mathbb{R})$ の転置とする。

(a) $g \in \mathrm{SL}_2(\mathbb{R})$ に対し $\sigma g \sigma^{-1} = {}^t g^{-1}$ を示せ。

(b) 任意の $g \in \mathrm{SL}_2(\mathbb{R})$ に対して $\tau g \tau^{-1} = {}^t g$ となるような $\tau \in \mathrm{SL}_2(\mathbb{R})$ が存在しないのはなぜか。$\tau g \tau^{-1} = g^{-1}$ となる τ は存在するか。

解答. (a) 直接計算すればわかる。

(b) $g, h \in \mathrm{SL}_2(\mathbb{R})$ に対し、$\tau g \tau^{-1} = {}^t g, \tau h \tau^{-1} = {}^t h, \tau g h \tau^{-1} = {}^t(gh)$ となる。よって

$${}^t g {}^t h = \tau g \tau^{-1} \tau h \tau^{-1} = \tau g h \tau^{-1} = {}^t(gh)$$

となるが、${}^t(gh) = {}^t h {}^t g$ なので、これは成り立たない。同様に、$\tau g \tau^{-1} = g^{-1}$ となる τ も存在しない。

$\square$

問 3. S_4 は $\mathrm{GL}_2(\mathbb{F}_3)/Z(\mathrm{GL}_2(\mathbb{F}_3))$ と同型であることを示せ。

解答. まず $Z(\mathrm{GL}_2(\mathbb{F}_3))$ はスカラー行列からなり、位数は 2 である。$\mathbb{F}_3^2$ の 1 次元部分空間は

$$\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \rangle, \langle \begin{pmatrix} 0 \\ 1 \end{pmatrix} \rangle, \langle \begin{pmatrix} 1 \\ 1 \end{pmatrix} \rangle, \langle \begin{pmatrix} 1 \\ -1 \end{pmatrix} \rangle$$

の 4 つあり、$\mathrm{GL}_2(\mathbb{F}_3)$ が作用するので準同型 $\mathrm{GL}_2(\mathbb{F}_3) \to S_4$ を得る。核はスカラー行列からなるので、単射準同型 $\mathrm{GL}_2(\mathbb{F}_3)/Z(\mathrm{GL}_2(\mathbb{F}_3)) \to S_4$ を得る。位数が等しいので同型である。 $\square$

問 4. $\mathrm{GL}_3(\mathbb{F}_q)$ の位数を求めよ。

解答. 3 次元ベクトル空間 $\mathbb{F}_q^3$ の基底の数に等しいので

$$(q^3 - 1)(q^3 - q)(q^3 - q^2)$$

である。 $\square$

問 5. G を $\mathrm{SL}_n(\mathbb{Z})$ の有限部分群とする。G の位数は

$$\frac{1}{2}(3^n-1)(3^n-3)\cdots(3^n-3^{n-1})$$

を割り切ることを示せ。ヒント：modulo 3 を用いる。

解答. $\mathrm{SL}_n(\mathbb{Z}) \to \mathrm{SL}_n(\mathbb{F}_3)$ を $a_{ij} \mapsto a_{ij} \bmod 3$ により定めるとこれは群準同型となる。定義域を G に制限することで準同型 $\varphi\colon G \to \mathrm{SL}_n(\mathbb{F}_3)$ を得る。$|G| = |\operatorname{Ker}\varphi| \cdot |\operatorname{Im}\varphi|$ であり、$\operatorname{Im}\varphi$ は $\mathrm{SL}_n(\mathbb{F}_3)$ の部分群なので、位数 $|\operatorname{Im}\varphi|$ は $|\mathrm{SL}_n(\mathbb{F}_3)| = \frac{1}{2}(3^n-1)(3^n-3)\cdots(3^n-3^{n-1})$ の約数。よって $|G|$ はこの値の約数である。 $\square$