代数学 I 期末試験予告問題 + 解答例

担当：大矢 浩徳 (OYA Hironori)*

- 代数学 I の成績は中間試験 40 %，期末試験 40 %，レポート 20 %の配分で付けられる．出席等は考慮されない．(『2019 年度代数学 I 履修上の注意』参照.)
- 期末試験の問題は大問が計 5 つで，

  問 1：計算問題 (20 点)

  問 2, 3：レポート課題および中間試験の類題(40 点)

  問 4：予告問題 (30 点)

  問 5：その他 (32 点)

  である．問 1 の計算問題に関しては別プリント『代数学 I 計算練習ドリル 2』で練習すること．問 2 のレポート課題および中間試験の類題はこれまで全 12 回のレポート課題と中間試験の問題から数字や群をのみを少し変えたものが出題される．ただし，あくまで類題なので解答例を数字ごと丸暗記してくることは無意味である．本プリントは問 4 の予告問題に対応する．本プリントの問 1〜3 の中から 1 問が期末試験の問 4 としてそのまま出題される．

  なお，上の配点だと満点が 122 点になるが，100 点を超えたかどうかに関わらず得点に $\times 0.4$ をしたものが成績に反映される．このため，上では期末試験の成績への寄与を「全体の 40 %」としたが，実際には満点であった場合，48.8 点分が期末試験から得られることになる．

以下では n 次 2 面体群を $D_n = \{e, \sigma, \sigma^2, \ldots, \sigma^{n-1}, \tau, \sigma\tau, \sigma^2\tau, \ldots, \sigma^{n-1}\tau\}$(ただし $\sigma^n = e, \tau^2 = e, \tau\sigma = \sigma^{-1}\tau$) とする．

問題 1

G を位数 18 の群とする．

$$X := \{\{g_1, g_2, g_3\} \subset G \mid g_1, g_2, g_3 \text{は相異なる } G \text{ の 3 元 }\}$$

としたとき，

$$G \times X \to X, (g, \{g_1, g_2, g_3\}) \mapsto \{gg_1, gg_2, gg_3\}$$

は X 上の G の作用を定める (このことは証明しなくて良い)．このとき，以下の問に答えよ．

(1) X の元の個数を求めよ．解答は答えのみで良い．

(2) 任意の $\{g_1, g_2, g_3\} \in X$ に対し，その固定部分群 $G_{\{g_1,g_2,g_3\}}$ の位数は 3 以下であることを証明せよ．

(3) X 上の G の作用は元の個数が 6 である G-軌道を少なくとも 1 つ持つことを証明せよ．

(4) G は位数 3 の部分群を少なくとも 1 つ持つことを証明せよ．

(5) 9 次 2 面体群 D_9 の位数 3 の部分群を具体的に挙げよ．解答は答えのみで良い．

* *e-mail* : hoya@shibaura-it.ac.jp

問題 1 解答例.

(1) $|X| = {}_{18}\mathrm{C}_3 = \dfrac{18 \cdot 17 \cdot 16}{3 \cdot 2 \cdot 1} = 816.$ □

(2) $G_{\{g_1,g_2,g_3\}} = \{g \in G \mid \{gg_1, gg_2, gg_3\} = \{g_1, g_2, g_3\}\}$ であるので，各 $g \in G_{\{g_1,g_2,g_3\}}$ に対してある $i \in \{1,2,3\}$ が定まり，$gg_1 = g_i$，つまり $g = g_i g_1^{-1}$. よって，

$$G_{\{g_1,g_2,g_3\}} \subset \{g_i g_1^{-1} \mid i = 1,2,3\}.$$

これより，$|G_{\{g_1,g_2,g_3\}}| \leq 3.$ □

(3) 各 $\{g_1, g_2, g_3\} \in X$ に対し，

$$|G.\{g_1, g_2, g_3\}| = \frac{|G|}{|G_{\{g_1,g_2,g_3\}}|}$$

が成立する. (2) より，$|G_{\{g_1,g_2,g_3\}}| \leq 3$ であり，Lagrange の定理よりこの値は $|G| = 18$ の約数であることから，$|G_{\{g_1,g_2,g_3\}}|$ は $1, 2, 3$ のいずれか. よって，$|G.\{g_1, g_2, g_3\}|$ は，$18, 9, 6$ のいずれか.

ここで元の個数が 6 の軌道が存在しないとすると，X を軌道分解したときに元の個数が 18 または 9 の軌道で軌道分解されるので，特に X の元の個数は 9 の倍数となる. しかし，(1) より X の元の個数は 816 で 9 の倍数ではない. これらより，元の個数が 6 である G-軌道が少なくとも 1 つ存在することがわかる.

(4) (3) より元の個数が 6 である G-軌道がとれるので，この軌道に含まれる元を $\{g_1, g_2, g_3\}$ とすると，

$$|G_{\{g_1,g_2,g_3\}}| = \frac{|G|}{|G.\{g_1, g_2, g_3\}|} = \frac{18}{6} = 3.$$

よって，この $G_{\{g_1,g_2,g_3\}}$ が位数 3 の G の部分群の例としてとれる.

(5) $\{e, \sigma^3, \sigma^6\}$ □

問題 1(1)–(4) 補足解説. 問題 3 補足解説を参照のこと. 問にある写像が群作用であることについては付録例 3 を参照のこと. □

問題 1(5) 補足解説. D_9 の位数 3 の部分群は以下の理由で $\{e, \sigma^3, \sigma^6\}$ のみである：

3 は素数なので位数 3 の群は必ず巡回群である. よって，D_9 の位数 3 の部分群は $\mathrm{ord}(g) = 3$ となる元 g を用いて $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$ と書かれるものとなる. ここで，D_9 の各元の位数を計算してみると，

$$\mathrm{ord}(e) = 1 \qquad \mathrm{ord}(\sigma) = \mathrm{ord}(\sigma^2) = \mathrm{ord}(\sigma^4) = \mathrm{ord}(\sigma^5) = \mathrm{ord}(\sigma^7) = \mathrm{ord}(\sigma^8) = 9$$
$$\mathrm{ord}(\sigma^3) = \mathrm{ord}(\sigma^6) = 3 \qquad \mathrm{ord}(\sigma^k\tau) = 2,\ k = 0, 1 \ldots, 9$$

となり，位数 3 の元は σ^3 と σ^6 のみである. このいずれの場合も $\langle \sigma^3 \rangle = \langle \sigma^6 \rangle = \{e, \sigma^3, \sigma^6\}$ となる. □

問題 2

G を位数 10 の群とする.

$$X := \{\{g_1, g_2, g_3, g_4, g_5\} \subset G \mid g_1, g_2, g_3, g_4, g_5 \text{は相異なる } G \text{ の 5 元 }\}$$

としたとき,

$$G \times X \to X, (g, \{g_1, g_2, g_3, g_4, g_5\}) \mapsto \{gg_1, gg_2, gg_3, gg_4, gg_5\}$$

は X 上の G の作用を定める (このことは証明しなくて良い). このとき, 以下の問に答えよ.

(1) X の元の個数を求めよ. 解答は答えのみで良い.
(2) 任意の $\{g_1, g_2, g_3, g_4, g_5\} \in X$ に対し, その固定部分群 $G_{\{g_1,g_2,g_3,g_4,g_5\}}$ の位数は 5 以下であることを証明せよ.
(3) X 上の G の作用は元の個数が 2 である G-軌道を少なくとも 1 つ持つことを証明せよ.
(4) G は位数 5 の部分群を少なくとも 1 つ持つことを証明せよ.
(5) G の位数 5 の部分群 (の 1 つ) を H とするとこれは正規部分群であることを証明せよ.

問題 2 解答例.

(1) $|X| = {}_{10}\mathrm{C}_5 = \dfrac{10 \cdot 9 \cdot 8 \cdot 7 \cdot 6}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 252.$ □

(2) $G_{\{g_1,g_2,g_3,g_4,g_5\}} = \{g \in G \mid \{gg_1, gg_2, gg_3, gg_4, gg_5\} = \{g_1, g_2, g_3, g_4, g_5\}\}$ であるので, 各 $g \in G_{\{g_1,g_2,g_3,g_4,g_5\}}$ に対してある $i \in \{1, 2, 3, 4, 5\}$ が定まり, $gg_1 = g_i$, つまり $g = g_i g_1^{-1}$. よって,

$$G_{\{g_1,g_2,g_3,g_4,g_5\}} \subset \{g_i g_1^{-1} \mid i = 1, 2, 3, 4, 5\}.$$

これより, $|G_{\{g_1,g_2,g_3,g_4,g_5\}}| \leq 5$. □

(3) 各 $\{g_1, g_2, g_3, g_4, g_5\} \in X$ に対し,

$$|G.\{g_1, g_2, g_3, g_4, g_5\}| = \frac{|G|}{|G_{\{g_1,g_2,g_3,g_4,g_5\}}|}$$

が成立する. (2) より, $|G_{\{g_1,g_2,g_3,g_4,g_5\}}| \leq 5$ であり, Lagrange の定理よりこの値は $|G| = 10$ の約数であることから, $|G_{\{g_1,g_2,g_3,g_4,g_5\}}|$ は $1, 2, 5$ のいずれか. よって, $|G.\{g_1, g_2, g_3, g_4, g_5\}|$ は, $10, 5, 2$ のいずれか.

ここで元の個数が 2 の軌道が存在しないとすると, X を軌道分解したときに元の個数が 10 または 5 の軌道で軌道分解されるので, 特に X の元の個数は 5 の倍数となる. しかし, (1) より X の元の個数は 252 で 5 の倍数ではない. これらより, 元の個数が 2 である G-軌道が少なくとも 1 つ存在することがわかる.

(4) (3) より元の個数が 2 である G-軌道がとれるので, この軌道に含まれる元を $\{g_1, g_2, g_3, g_4, g_5\}$ とすると,

$$|G_{\{g_1,g_2,g_3,g_4,g_5\}}| = \frac{|G|}{|G.\{g_1, g_2, g_3, g_4, g_5\}|} = \frac{10}{2} = 5.$$

よって, この $G_{\{g_1,g_2,g_3,g_4,g_5\}}$ が位数 5 の G の部分群の例としてとれる.

(5) G における H の指数 $[G : H]$ は Lagrange の定理より,

$$[G : H] = \frac{|G|}{|H|} = \frac{10}{5} = 2$$

である. これより, $g_0 \notin H$ なる G の元を任意にとると, G の H による左・右剰余類への分解は

$$G = H \cup g_0 H = H \cup H g_0$$

となる. ここで, $H \cap g_0 H = H \cap H g_0 = \emptyset$ であるので, $g_0 H = G \setminus H = H g_0$ である. ($G \setminus H$ は商空間ではなく H の G における補集合の意味.)

よって，各 $g \in G$ に対して，

$$\begin{cases} g \in H \text{ のとき}, gH = H = Hg \\ g \notin H \text{ のとき}, gH = G \setminus H = Hg \end{cases}$$

となる．これより，任意の $g \in G$ に対して $gH = Hg$ となるので，H は G の正規部分群である． □

問題 2(1)–(4) 補足解説. 問題 3 補足解説を参照のこと．問にある写像が群作用であることについては付録例 3 を参照のこと． □

問題 2(5) 補足解説. この証明をよく見ると，H が正規部分群であることの本質的な理由は指数 $[G : H] = 2$ であることがわかる．つまり，指数が 2 の部分群に対しては，全く同様の証明でそれが正規部分群であることを示すことができる．命題の形でまとめておくと以下が成立する：

命題.

一般に群 G の指数 2 の部分群 H は正規部分群となる．

この事実は第 7 回レポート課題解答例でも解説されているので参照すること．

さて，問題の話に戻ると，問題 2 では位数が 10 の群 G において位数 5 の部分群が少なくとも 1 つ存在することを示した．そして実は位数 5 の部分群はただ一つしかないことが以下のように示される：

位数 5 の部分群がただ一つであることの証明：$H_1, H_2 \subset G$ を G の位数 5 の部分群であるとする．このとき $H_1 = H_2$ となることを示せばよい．いま H_1, H_2 の位数 5 は素数なので，$e \neq h_1 \in H_1, e \neq h_2 \in H_2$ とすると，

$$H_1 = \langle h_1 \rangle = \{h_1^i \mid i = 0, 1, 2, 3, 4\} \qquad H_2 = \langle h_2 \rangle = \{h_2^j \mid j = 0, 1, 2, 3, 4\}$$

となる．ここで，$h_1^i h_2^j, i, j \in \{0, 1, 2, 3, 4\}$ は G の 25 個の元であるが，G の位数は 10 なので，ある $i_1, i_2, j_1, j_2 \in \{0, 1, 2, 3, 4\}, i_1 \neq i_2, j_1 \neq j_2$ が存在して，$h_1^{i_1} h_2^{j_1} = h_1^{i_2} h_2^{j_2}$ となる．このとき、$h_1^{i_1 - i_2} = h_2^{j_2 - j_1} \in H_1 \cap H_2$ である．

いま $H_1 \cap H_2$ は H_1 の部分群であるが，一方 H_1 の位数 5 は素数なので H_1 の部分群は $\{e\}$ か H_1 のいずれかである．ここで $H_1 \cap H_2 = \{e\}$ と仮定すると，$h_1^{i_1 - i_2} = h_2^{j_2 - j_1} = e$ となるが，$i_1, i_2, j_1, j_2 \in \{0, 1, 2, 3, 4\}$ より，$i_1 \neq i_2, j_1 \neq j_2$ のときこれを満たす i_1, i_2, j_1, j_2 は存在しない．よって，$H_1 \cap H_2 = H_1$ であり，特に $H_1 \subset H_2$ となる．いま H_1 と H_2 の位数はともに 5 であるので，これより $H_1 = H_2$．よって，G の位数 5 の部分群はただ一つである． □

実はさらに考察を進めると，位数が 10 の群は $\mathbb{Z}/10\mathbb{Z}$，あるいは D_5 のいずれかに同型なものしか存在しないことがわかる．さらに一般に，位数が $2p$(p は奇素数) の群 G は $\mathbb{Z}/2p\mathbb{Z}$，あるいは D_p のいずれかに同型になることが知られている．(この事実の略証は参考書の第 1 章章末問題 (65) を参照のこと.) □

問題 3

p を素数，n を p と互いに素な正の整数とし，G を位数 pn の群とする．

$$X := \{\{g_1, \ldots, g_p\} \subset G \mid g_1, \ldots, g_p \text{は相異なる } G \text{ の } p \text{ 元 }\}$$

としたとき，

$$G \times X \to X, (g, \{g_1, \ldots, g_p\}) \mapsto \{gg_1, \ldots, gg_p\}$$

は X 上の G の作用を定める (このことは証明しなくて良い)．このとき，以下の問に答えよ．

(1) X の元の個数を求めよ．解答は答えのみで良い．
(2) 任意の $\{g_1, \ldots, g_p\} \in X$ に対し，その固定部分群 $G_{\{g_1,\ldots,g_p\}}$ の位数は p 以下であることを証明せよ．
(3) X 上の G の作用は元の個数が n である G-軌道を少なくとも 1 つ持つことを証明せよ．
(4) G は $g \neq e$ かつ $g^p = e$ を満たす元 g を少なくとも 1 つ持つことを証明せよ．

問題 3 解答例．

(1) $|X| = {}_{pn}\mathrm{C}_p = \dfrac{pn!}{p!(pn-p)!} = \dfrac{pn(pn-1)\cdots(pn-p+1)}{p(p-1)\cdots 1}$. □

(2) $G_{\{g_1,\ldots,g_p\}} = \{g \in G \mid \{gg_1, \ldots, gg_p\} = \{g_1, \ldots, g_p\}\}$ であるので，各 $g \in G_{\{g_1,\ldots,g_p\}}$ に対してある $i \in \{1, \ldots, p\}$ が定まり，$gg_1 = g_i$，つまり $g = g_i g_1^{-1}$．よって，

$$G_{\{g_1,\ldots,g_p\}} \subset \{g_i g_1^{-1} \mid i = 1, \ldots, p\}.$$

これより，$|G_{\{g_1,\ldots,g_p\}}| \leq p$. □

(3) 各 $\{g_1, \ldots, g_p\} \in X$ に対し，

$$|G.\{g_1, \ldots, g_p\}| = \frac{|G|}{|G_{\{g_1,\ldots,g_p\}}|} = \frac{pn}{|G_{\{g_1,\ldots,g_p\}}|}$$

が成立する．(2) より $|G_{\{g_1,\ldots,g_p\}}| \leq p$ で，さらに Lagrange の定理よりこの値は $|G| = pn$ の約数だが，p と n が互いに素であることより $|G_{\{g_1,\ldots,g_p\}}| < p$ のとき $|G_{\{g_1,\ldots,g_p\}}|$ は n の約数である．よって $|G.\{g_1, \ldots, g_p\}|$ は，p の倍数または n となる．

これより元の個数が n の軌道が存在しないとすると，X を軌道分解したときに元の個数が p の倍数の軌道で軌道分解されるので，特に X の元の個数は p の倍数となる．一方，(1) より

$$|X| = \frac{pn(pn-1)\cdots(pn-p+1)}{p(p-1)\cdots 1} = n\frac{(pn-1)\cdots(pn-p+1)}{(p-1)\cdots 1}$$

であるが，n は p と互いに素であり，さらに

$$(pn-1)\cdots(pn-p+1) \equiv (p-1)(p-2)\cdots 1 \not\equiv 0 \mod p$$

より，$\dfrac{(pn-1)\cdots(pn-p+1)}{(p-1)\cdots 1} (= {}_{pn-1}\mathrm{C}_{p-1})$ も p と互いに素である．よって，X の元の個数は p の倍数ではない．以上より，元の個数が n である G-軌道が少なくとも 1 つ存在することがわかる．

(4) (3) より元の個数が n である G-軌道がとれるので，この軌道に含まれる元を $\{g_1, \ldots, g_p\}$ とすると，

$$|G_{\{g_1,\ldots,g_p\}}| = \frac{|G|}{|G.\{g_1, \ldots, g_p\}|} = \frac{pn}{n} = p.$$

よって，この $G_{\{g_1,\ldots,g_p\}}$ は位数 p の G の部分群である．$p > 1$ なので，$G_{\{g_1,\ldots,g_p\}}$ の単位元でない元 g が取れるが，Laglange の定理よりこの元は $g^p = e$ を満たす． □

問題 3 補足解説. 本問は問題 2 の設定 $(p=5, n=2)$ の一般化である．このような状況は問題 1 の設定も含む形で一般化され，以下の事実が一般に正しいことが問題 1–3 と同様の方法で証明される．これは Sylow の定理と呼ばれ，群の分類問題を扱う際に非常に基本的で重要となる定理である[*1][*2]：

Sylow の定理

p を素数，G を有限群とし，G の位数が p^ℓ では割り切れるが，$p^{\ell+1}$ では割り切れなかったとする．(ただし ℓ は正の整数.) このとき，任意の $1 \leq k \leq \ell$ に対し，G は位数 p^k の部分群を持つ．

定理より，特に G は位数 p^ℓ の部分群をもつ．これを *p-Sylow* **部分群**という．

注意．問題 1(1)–(4) で示したことはこの定理で $p=3, \ell=2, k=1$ としたものである．問題 2 の位数 5 の部分群は 5-Sylow 部分群である．

Sylow の定理の証明 (興味のある方向け). 仮定より，G の位数は $p^\ell n$(ただし，p と n は互いに素) という形で書かれる．

$$X := \{\{g_1, \ldots, g_{p^k}\} \subset G \mid g_1, \ldots, g_{p^k} \text{は相異なる } G \text{ の } p^k \text{元 }\}$$

としたとき，

$$G \times X \to X, (g, \{g_1, \ldots, g_{p^k}\}) \mapsto \{gg_1, \ldots, gg_{p^k}\}$$

は X 上の G の作用を定める．このとき，各 $\{g_1, \ldots, g_{p^k}\} \in X$ の固定部分群の定義は，$G_{\{g_1,\ldots,g_{p^k}\}} = \left\{g \in G \mid \{gg_1, \ldots, gg_{p^k}\} = \{g_1, \ldots, g_{p^k}\}\right\}$ であるので，各 $g \in G_{\{g_1,\ldots,g_{p^k}\}}$ に対してある $i \in \{1, \ldots, p^k\}$ が定まり，$gg_1 = g_i$，つまり $g = g_i g_1^{-1}$．よって，

$$G_{\{g_1,\ldots,g_{p^k}\}} \subset \{g_i g_1^{-1} \mid i = 1, \ldots, p^k\}$$

となるので，$|G_{\{g_1,\ldots,g_{p^k}\}}| \leq p^k$ である．さらに，Lagrange の定理より $|G_{\{g_1,\ldots,g_{p^k}\}}|$ の値は $|G| = p^\ell n$ の約数なので，$|G_{\{g_1,\ldots,g_p\}}| < p^k$ のとき特に $p^{k-1}n$ の約数である．

いま各 $\{g_1, \ldots, g_{p^k}\} \in X$ に対し，

$$|G.\{g_1, \ldots, g_{p^k}\}| = \frac{|G|}{|G_{\{g_1,\ldots,g_{p^k}\}}|} = \frac{p^\ell n}{|G_{\{g_1,\ldots,g_{p^k}\}}|}$$

が成立するので，以上の考察から，$|G.\{g_1, \ldots, g_p\}|$ は $p^{\ell-k+1}$ の倍数 ($|G_{\{g_1,\ldots,g_{p^k}\}}| < p^k$ のとき)，または $p^{\ell-k}n$ ($|G_{\{g_1,\ldots,g_{p^k}\}}| = p^k$ のとき) となる．これより，もし $|G_{\{g_1,\ldots,g_{p^k}\}}| = p^k$ となる $\{g_1, \ldots, g_{p^k}\} \in X$ が存在しないと仮定すると，X を軌道分解したときに元の個数が $p^{\ell-k+1}$ の倍数の軌道で軌道分解されるので，特に $|X|$ は $p^{\ell-k+1}$ の倍数となる．今示したかったことは，位数 p^k の G の部分群の存在なので，あとは $|X|$ が $p^{\ell-k+1}$ の倍数でないことを示せば，$|G_{\{g_1,\ldots,g_{p^k}\}}| = p^k$ なる $G_{\{g_1,\ldots,g_{p^k}\}}$ が存在することがわかり，これが求める部分群の例となって定理が示されることとなる．

いま，

$$|X| = {}_{p^\ell n}\mathrm{C}_{p^k} = \frac{p^\ell n(p^\ell n - 1)\cdots(p^\ell n - p^k + 1)}{p^k(p^k - 1)\cdots 1} = p^{\ell-k}n \cdot \frac{(p^\ell n - 1)\cdots(p^\ell n - p^k + 1)}{(p^k - 1)\cdots 1}$$

である．ここで，$m \in \mathbb{Z}_{>0}$ に対し，$\ell(m)$ を

$$m \text{ は } p^{\ell(m)} \text{ で割り切れるが } p^{\ell(m)+1} \text{ では割り切れない}$$

[*1] 実はこの定理には続きがあり，群の分類問題を扱う上ではそこまで知っていることが重要である．興味のある方は是非続きを調べてみてほしい．(証明はないが主張は参考書の定理 1.9.1 にある.)

[*2] 個人的には群の位数を見ただけで群の構造について様々な主張が言える (ときには完全に分類できる！) というのは非常に面白いと感じる．あの抽象的で “最低限の仮定” のようにも見えた群の定義は実はその構造を強く定めるものだったのである．

という条件で定まる 0 以上の整数とすると，定義より $p^{-\ell(m)}m$ は p で割り切れない整数であり，$m = 1, 2, \ldots, p^k - 1$ のとき $\ell(m) < k$ である．よって，

$$\begin{aligned}&\frac{(p^\ell n - 1)\cdots(p^\ell n - p^k + 1)}{(p^k - 1)\cdots 1}\\ &= \frac{(p^{\ell-\ell(1)}n - p^{-\ell(1)}1)\cdots(p^{\ell-\ell(m)}n - p^{-\ell(m)}m)\cdots(p^{\ell-\ell(p^k-1)}n - p^{-\ell(p^k-1)}(p^k-1))}{(p^{k-\ell(1)} - p^{-\ell(1)}1)\cdots(p^{k-\ell(m)} - p^{-\ell(m)}m)\cdots(p^{k-\ell(p^k-1)} - p^{-\ell(p^k-1)}(p^k-1))}\end{aligned}$$

ここで，右辺の分子分母の積の各項は整数であることに注意する．このとき，右辺の分子に現れる $(p^{\ell-\ell(m)}n - p^{-\ell(m)}m),\ m = 1, \ldots, p^k - 1$ という形の整数は $p^{\ell-\ell(m)}n$ が p の倍数，$-p^{-\ell(m)}m$ が p で割り切れない整数であることより，p で割り切れない整数である．よって，それらの積である右辺の分子は p で割り切れず，それをさらに整数で割って得られる数である右辺の値は p の倍数ではない．

以上より，$\dfrac{(p^\ell n - 1)\cdots(p^\ell n - p^k + 1)}{(p^k - 1)\cdots 1}$ は p の倍数ではないことが示され，さらに p と n は互いに素であることより，結局 $|X|$ は $p^{\ell-k+1}$ の倍数ではないことがわかった．よって，示すべきことは全て示された． □

付録：群作用の基本事項

定義. 群 G と集合 X に対し，写像

$$f\colon G\times X\to X,\ (g,x)\mapsto f(g,x)$$

が次の 2 条件を満たすとき，これを X **上の** G **の作用** (action) という．(記号を簡潔にするため以下では $f(g,x)$ を単に $g.x$ と書く.)

(i) 任意の $g,h\in G$，$x\in X$ に対し，$(gh).x=g.(h.x)$.
(ii) 任意の $x\in X$ に対し，$e.x=x$. ただし，e は G の単位元.

G の作用に関する $x\in X$ **の** G**-軌道** (G-orbit) を

$$G.x:=\{g.x\mid g\in G\}$$

と定める．また，$x\in X$ における G の**固定部分群** (stabilizer) を

$$G_x:=\{g\in G\mid g.x=x\}$$

と定める．G_x は G の部分群となる．また，記号は似ているが $G.x$ は X の部分集合であり，G_x は G の部分群であることを注意しておく．

例 1. $X:=\{1,2,3,4,5\}$ としたとき，

$$\mathfrak{S}_5\times X\to X,(\sigma,i)\mapsto\sigma.i:=\sigma(i)$$

は X 上の $\mathfrak{S}_5$ の作用を定める．例えば，

$$\begin{pmatrix}1&2&3&4&5\\3&1&4&2&5\end{pmatrix}.1=3,\qquad\begin{pmatrix}1&2&3&4&5\\3&1&4&2&5\end{pmatrix}.2=1,\qquad\begin{pmatrix}1&2&3&4&5\\3&1&4&2&5\end{pmatrix}.5=5$$

などとなる．さらに，

$$\mathfrak{S}_5.1=\{1,2,3,4,5\}=X,\qquad(\mathfrak{S}_5)_1=\left\{\begin{pmatrix}1&2&3&4&5\\1&i_1&i_2&i_3&i_4\end{pmatrix}\in\mathfrak{S}_5\ \middle|\ \{i_1,i_2,i_3,i_4\}=\{2,3,4,5\}\right\}$$

となる．ちなみにこれが群作用であることは以下の計算から確かめられる．

(i) の確認 任意の $\sigma,\tau\in\mathfrak{S}_5$，$i\in X$ に対し，$(\sigma\tau).i=\sigma\tau(i)=\sigma(\tau(i))=\sigma.(\tau.i)$.

(ii) の確認 任意の $i\in X$ に対し，$\begin{pmatrix}1&2&3&4&5\\1&2&3&4&5\end{pmatrix}.i=i$.

例 2. $X:=\mathbb{R}^2$ としたとき，

$$GL_2(\mathbb{R})\times\mathbb{R}^2\to\mathbb{R}^2,\left(\begin{pmatrix}a&b\\c&d\end{pmatrix},\begin{pmatrix}x\\y\end{pmatrix}\right)\mapsto\begin{pmatrix}a&b\\c&d\end{pmatrix}\cdot\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}ax+by\\cx+dy\end{pmatrix}\ \text{(行列の積)}$$

は $\mathbb{R}^2$ 上の $GL_2(\mathbb{R})$ の作用を定める．これが群作用であることは以下の計算から確かめられる．

(i) の確認 任意の $g_1,g_2\in GL_2(\mathbb{R}),v\in\mathbb{R}^2$ に対し，$(g_1g_2)\cdot v=g_1\cdot(g_2\cdot v)$ (行列の積の結合法則).

(ii) の確認 任意の $\begin{pmatrix}x\\y\end{pmatrix}\in\mathbb{R}^2$ に対し，$\begin{pmatrix}1&0\\0&1\end{pmatrix}\cdot\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}x\\y\end{pmatrix}$.

例えば，

$$GL_2(\mathbb{R}).\begin{pmatrix}0\\0\end{pmatrix}=\left\{\begin{pmatrix}0\\0\end{pmatrix}\right\},$$
$$GL_2(\mathbb{R}).\begin{pmatrix}1\\0\end{pmatrix}=\left\{\begin{pmatrix}a\\c\end{pmatrix}\in\mathbb{R}^2\,\middle|\,\begin{pmatrix}a&b\\c&d\end{pmatrix}\in GL_2(\mathbb{R})\right\}=\mathbb{R}^2\setminus\{\tbinom{0}{0}\},$$
$$GL_2(\mathbb{R})_{\binom{1}{0}}=\left\{\begin{pmatrix}1&b\\0&d\end{pmatrix}\in GL_2(\mathbb{R})\,\middle|\,d\neq 0\right\}$$

となる．

例 3 (予告問題 1–3 の設定の一般化)**.** G を群とする．

$$X:=\{\{g_1,\dots,g_n\}\subset G\mid g_1,\dots,g_n\text{は相異なる}\,G\,\text{の}\,n\,\text{元}\,\}$$

としたとき，

$$G\times X\to X,(g,\{g_1,\dots,g_n\})\mapsto\{gg_1,\dots,gg_n\}$$

は X 上の G の作用を定める．これが群作用であることは以下のように確かめられる．

定義されること $\{gg_1,\dots,gg_n\}$ は $\{g_1,\dots,g_n\}$ が相異なる n 元であるとき，再び相異なる n 元となる．なぜなら，$gg_i=gg_j$ とすると両辺に左から g^{-1} を掛けて $g_i=g_j$ となるためである．

(i) の確認 任意の $g,h\in G,\{g_1,\dots,g_n\}\in X$ に対し，

$$(gh).\{g_1,\dots,g_n\}=\{ghg_1,\dots,ghg_n\}=g.(\{hg_1,\dots,hg_n\})=g.(h.(\{g_1,\dots,g_n\})).$$

(ii) の確認 任意の $\{g_1,\dots,g_n\}\in X$ に対し，$e.\{g_1,\dots,g_n\}=\{eg_1,\dots,eg_n\}=\{g_1,\dots,g_n\}$.

定義. G を群，X を集合とし，

$$G\times X\to X,\ (g,x)\mapsto g.x$$

を X 上の G の作用とする．このとき，X は G の作用に関する軌道の和に分割される．つまり，

$$X=\coprod_{\lambda\in\Lambda}O_\lambda$$

ただし，各 O_λ は軌道，Λ は各軌道を添え字付ける適当な添え字集合，という形に書ける．$\lambda\neq\lambda'$ であれば $O_\lambda\cap O_{\lambda'}=\emptyset$ である．これを**軌道分解**という．
G の作用を用いて X 上の同値関係 $\sim$ を

$$x\sim y\ \Leftrightarrow\ \text{ある}\,g\in G\,\text{が存在して，}\,x=g.y$$

で定めることができることを思い出すと，各軌道 O_λ は同値関係 $\sim$ に関する同値類とちょうど対応し，軌道分解できることは同値関係の一般論から従う．

例 4. 例 1 では，軌道分解は

$$X=\mathfrak{S}_5.1$$

であった．つまり，このとき X は 1 つの軌道に分解されていた．例 2 では，軌道分解は

$$\mathbb{R}^2=\{\tbinom{0}{0}\}\coprod\left(\mathbb{R}^2\setminus\{\tbinom{0}{0}\}\right)=GL_2(\mathbb{R}).\begin{pmatrix}0\\0\end{pmatrix}\coprod GL_2(\mathbb{R}).\begin{pmatrix}1\\0\end{pmatrix}$$

であった．特に，このとき $\mathbb{R}^2$ は 2 つの軌道に分解されていた．

群の軌道の構造については次の定理が基本的である.

定理

G を群，X を集合とし，

$$G \times X \to X,\ (g, x) \mapsto g.x$$

を X 上の G の作用とする. このとき，任意の $x \in X$ に対し，

$$G/G_x \to G.x,\ gG_x \mapsto g.x$$

は集合としての全単射である. 特に G が有限群のとき，

$$\frac{|G|}{|G_x|} = |G/G_x| = |G.x|$$

である. (これは G の G_x における指数に他ならない.)

この定理より，有限群 G の群作用に関する G-軌道の元の個数は必ず G の位数の約数となることがわかる.

例 5. 確かに例 1 では，

$$\frac{|\mathfrak{S}_5|}{|(\mathfrak{S}_5)_1|} = \frac{5!}{4!} = 5, \qquad |\mathfrak{S}_5.1| = |X| = 5$$

であった.