定義１． (群の位数，群の元の位数)

(1) 群 G の元の個数を G の位数といい，$|G|$ で表す．G が無限集合であるとき $|G| = \infty$ と書く．

(2) 群 G の元 $g \in G$ に対し，$g^m = e$ となる[1]正整数 m が存在するとき，そのうち最小の m を g の位数といい，$|g|$ で表す．そのような m が存在しないとき，g の位数は無限であるという．

定義２． (左剰余類)

H を G の部分群とする．このとき，$g \in G$ に対し

$$gH := \{gh \mid h \in H\}$$

を G の H に関する(左)剰余類という．

命題３． (剰余類は同値類)

H を G の部分群とする．$x, y \in G$ に対し

$$x \sim y \overset{\text{def}}{\iff} x = yh \ (h \in H)$$

と定めると，$\sim$ は同値関係であり，g の $\sim$ に関する同値類は gH と一致する．

(証明)

反射律：$e \in H$ より，任意の $x \in G$ は $x = xe$ と表せるので，$x \sim x$ である．

対称律：$x, y \in G$ とし $x \sim y$ とすると，ある $h \in H$ が存在して $x = yh$ である．このとき，$h^{-1} \in H$ であり，$y = xh^{-1}$ だから，$y \sim x$ が成り立つ．

推移律：$x, y, z \in G$ とする．$x \sim y$ かつ $y \sim z$ と仮定すると，ある $h_0, h_1 \in H$ が存在して $x = yh_0$ かつ $y = zh_1$ である．よって $x = (zh_1)h_0 = z(h_0h_1)$ であり，$h_0h_1 \in H$ だから $x \sim z$ が成り立つ．

以上より，$\sim$ は同値関係である．また，g の $\sim$ に関する同値類を $[g]$ と表すと

$$[g] = \{g' \mid g' \sim g\} = \{g' \mid g' = gh \ (h \in H)\} = \{gh \mid h \in H\}$$

であるから，g の $\sim$ に関する同値類は gH と一致する．　∎

命題４． (剰余類の性質[2])

$x, y \in G$ に対し，$xH = yH$ であることと $xH \cap yH \neq \emptyset$ であることは同値．

(証明)

$xH = yH$ ならば，$xH \cap yH = xH$ であり，$x \in xH$ だから $xH \cap yH \neq \emptyset$ が言える．

---

[1] e は G の単位元．

[2] 一般の同値類に対しても成り立つ．

逆に $xH \cap yH \neq \varnothing$ とし，$z \in xH \cap yH$ とすると，ある h_0, h_1 が存在して $z = xh_0 = yh_1$ である．このとき，任意の $x' \in xH$ を与えると，ある $h \in H$ が存在して

$$x' = xh = xh_0h_0^{-1}h = yh_1h_0^{-1}h \quad (\because xh_0 = yh_1)$$

となることから，$x' \in yH$ である．よって $xH \subset yH$ である．同様に $yH \subset xH$ も言えるから，$xH \cap yH \neq \varnothing$ ならば $xH = yH$ が成り立つ.

定義５．(指数)
$\sim$ による G の商集合 $G/\sim$ を G/H と書く．$|G/H|$ を G における H の指数といい，$[G:H]$ と表す.

命題６．(剰余類の位数)
任意の $g_0, g_1 \in G$ に対し，$|g_0H| = |g_1H|$ である．
(証明)
写像 $f : g_0H \to g_1H$ を $f(x) = g_1g_0^{-1}x$ と定める．このとき，写像 $\bar{f} : g_1H \to g_0H$ を $\bar{f}(x) = g_0g_1^{-1}x$ とすると，$(f \circ \bar{f})(x) = g_1g_0^{-1}g_0g_1^{-1}x = x$ かつ $(\bar{f} \circ f)(x) = g_0g_1^{-1}g_1g_0^{-1}x = x$ が成り立つから，$\bar{f}$ は f の逆写像である．よって f は全単射だから $|g_0H| = |g_1H|$ である．∎

定理７．(ラグランジュの定理)
有限群 G とその部分群 H に対し，$|G| = [G:H]|H|$が成り立つ.
(証明)
G が有限集合より，G/H も有限集合である．$|G/H| = n$ とおき，G/H の元である各剰余類から１つずつ，それに属する G の元(つまり代表元)を選んで $G/H = \{g_1H, \cdots, g_nH\}$ と表す[3]．$g_iH \neq g_jH\ (i \neq j)$ なので，命題４より $g_iH \cap g_jH = \varnothing\ (i \neq j)$ である．また，任意の $g \in G$ について $g \in gH,\ gH \in G/H$ だから

$$g \in \bigcup_{i=1}^{n} g_iH \qquad \therefore G \subset \bigcup_{i=1}^{n} g_iH$$

が成り立つ．逆の包含は明らかである．以上をまとめると

$$G = g_1H \cup \cdots \cup g_nH \quad (g_1H, \cdots, g_nH \text{ は互いに共通部分を持たない})$$

となり，命題６から $|H| = |eH| = |g_1H| = \cdots = |g_nH|$なので

$$G = n|H| = |G/H||H| = [G:H]|H|$$

が成り立つ.　∎

[3] このとき，選んできた $\{g_1, \cdots, g_n\}$ のことを $G/\sim$ の完全代表系という.

(参考文献)
[1]　木村達雄・竹内光弘・宮本雅彦・森田純「代数の魅力」数学書房
[2]　“ラグランジュの定理(群論)”. Wikipedia. 2023-02-02. https://ja.wikipedia.org/wiki/ラグランジュの定理_(群論)
[3]　“群”. Mathpedia. 2023-02-02. https://math.jp/wiki/群
[4]　雪江明彦「代数学 1　群論入門」日本評論社