代数学入門

花木 章秀

2007 年前期
(2007/11/06)

目次

Chapter 2

群

2.1 群の定義と例

すべての元が正則元であるモノイドを**群** (group) という。すなわち、演算の定義された集合 G で

(G1) [**結合法則**] 任意の $a, b, c \in G$ について $a(bc) = (ab)c$ である。

(G2) [**単位元の存在**] ある $e \in G$ が存在して、任意の $a \in G$ に対して $ea = ae = a$ である。(このとき e を 1_G とも書く。)

(G3) [**逆元の存在**] 任意の $a \in G$ に対して、ある $b \in G$ が存在して $ab = ba = e$ である。(このときの b を a^{-1} と書く。)

がすべて成り立つとき G を群という。群は半群やモノイドの特別なものであるから、それらに対して成り立つことはすべて成り立つ。群 G において、更に

(G4) [**交換法則**] 任意の $a, b \in G$ について $ab = ba$ である。

が成り立つとき G を**アーベル群** (abelian group)、または**可換群** (commutative group) という。

命題 2.1.1. 群 G について次が成り立つ。

(1) [**簡約法則**] $ax = ay$ ならば $x = y$ である。また $xa = ya$ ならば $x = y$ である。

(2) $f : G \to G$ $(x \mapsto x^{-1})$ は全単射である。

(3) $a \in G$ を一つ固定するとき

$$\begin{aligned} g_a &: G \to G \quad (x \mapsto xa) \\ h_a &: G \to G \quad (x \mapsto ax) \\ k_a &: G \to G \quad (x \mapsto a^{-1}xa) \end{aligned}$$

はすべて全単射である。

証明. (1) $ax = ay$ とすると、両辺に左から a^{-1} をかけて $x = y$ となる。逆も同様である。(2) $(x^{-1})^{-1} = x$ より $f^2 = \mathrm{id}_G$ となり f は全単射である。(3) $g_a \circ g_{a^{-1}} = g_{a^{-1}} \circ g_a = \mathrm{id}_G$ となり g_a は全単射である。他も同様である。 □

命題 2.1.2. 群 G において、任意の $x \in G$ が $x^2 = 1$ を満たすならば、G はアーベル群である。

証明. 任意の $x \in G$ に対して $x^2 = 1$ より $x^{-1} = x$ である。よって任意の $a, b \in G$ に対して $(ab)^{-1} = ab$ である。一方 $(ab)^{-1} = b^{-1}a^{-1} = ba$ であるから $ab = ba$ となる。 □

例 2.1.3. $\mathbb{Q}^\sharp = \mathbb{Q} - \{0\}$ とおく。このとき $\mathbb{Q}^\sharp$ は乗法に関してアーベル群で、単位元は 1、$a \in \mathbb{Q}^\sharp$ の逆元は $1/a$ である。$\mathbb{R}^\sharp = \mathbb{R} - \{0\}$, $\mathbb{C}^\sharp = \mathbb{C} - \{0\}$ でも同様である。

例 2.1.4. (1) $\mathbb{Q}$ は乗法に関してモノイドではあるが群ではない。なぜならば 0 に逆元がないからである。

(2) $\mathbb{Z}^\sharp = \mathbb{Z} - \{0\}$ は乗法に関してモノイドではあるが群ではない。なぜならば 2 に逆元がないからである。

命題 2.1.5. M をモノイドとし U を M の正則元全体の集合とする。このとき U は M の演算で群になる。

証明. $a, b \in U$ ならば $ab \in U$ なので演算は U で定義される。また $1 \in U$ より U はモノイドである。$a \in U$ ならば $a^{-1} \in U$ も成り立ち U は群である。 □

この命題の U を $U(M)$ と書いて M の**単数群** (unit group) という。

例 2.1.6. (1) $\mathbb{Q}$ は乗法に関してモノイドである。その単数群は$U(\mathbb{Q}) = \mathbb{Q}^\sharp = \mathbb{Q} - \{0\}$ である。

(2) $\mathbb{Z}$ は乗法に関してモノイドである。その単数群は$U(\mathbb{Z}) = \{-1, 1\}$ である。

例 2.1.7 (対称群)**.** モノイド X^X (例 **??**) について、その単数群 $U(X^X)$ を X 上の**対称群** (symmetric group) といい、これを $S(X)$ と書くことにする。$S(X)$ の元は X から X への全単射で、それを X 上の**置換** (permutation) という。置換を具体的に書くには

$$S(X) \ni \sigma = \begin{pmatrix} x \\ \sigma(x) \end{pmatrix}$$

のように書く。特に $|X| = n$ のとき、$X = \{1, 2, \cdots, n\}$ と考えても本質的には同じである。このとき $S(X)$ を S_n とも書き、これを n **次対称群**という。S_n の元を n 次の置換という。

例 2.1.8. 3 次対称群 S_3 の元をすべて書くと以下のようになる。

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

元の積は以下のようになる。

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

右の置換を先に行い、例えば 1 については $1 \mapsto 1 \mapsto 3$ となる。逆元は上の行と下の行を入れ替えて

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

と計算できる。置換を表す列の並びは元の対応を表しているだけなので、列を並び替えても構わない。

問 2.1.9. S_3 の演算表を書け。

問 2.1.10. $n \geq 3$ のとき S_n はアーベル群ではないことを、具体的に $\sigma\tau \neq \tau\sigma$ なる $\sigma, \tau \in S_n$ を見つけることによって示せ。

群 G について、$|G| < \infty$ のとき G を**有限群** (finite group) という。また $|G| = \infty$ のとき G を**無限群** (infinite group) という。$|G| < \infty$ のとき $|G|$ を G の**位数** (order) という。

問 2.1.11. n 次対称群 S_n の位数は $n!$ であることを示せ。

例 2.1.12 (一般線形群)**.** $\mathbb{R}$ を成分とする n 次正方行列の全体を $M(n, \mathbb{R})$ と書く。$M(n, \mathbb{R})$ が行列の積によって単位行列を単位元とするモノイドである。その単数群を $\mathbb{R}$ 上 n 次の**一般線形群** (general linear group) といい $GL(n, \mathbb{R})$ と書く。$M(n, \mathbb{R})$ の単数は正則行列のことであるから $GL(n, \mathbb{R})$ は正則行列全体の集合である。$GL(n, \mathbb{R})$ は無限群である。

$GL(n, \mathbb{Q})$, $GL(n, \mathbb{C})$ も同様である。

(これらは $M_n(\mathbb{R})$, $GL_n(\mathbb{R})$ などとも書かれる。)

問 2.1.13. $n \geq 2$ のとき $GL(n, \mathbb{R})$ はアーベル群ではないことを示せ。

問 2.1.14. A をモノイドで、集合として有限集合であるとする。右簡約法則「$x, y, z \in A$ に対して $xz = yz$ ならば $x = y$ である」が成り立つとすると A は群になる。これを示せ。また A が有限集合ではないとき、これは正しくない。そのような例を具体的に一つ示せ。

2.2 加群

群 G がアーベル群であるとき、その演算を加法の形で書くことが多い。このとき G を**加群** (additive group)、または**加法群**という。加群の単位元を**零元**といい 0 または 0_G と書く。また a の逆元は $-a$ と書く。群の定義を加法の形で書き直すと以下のようになる。

(A1) [**結合法則**] 任意の $a, b, c \in G$ について $a + (b + c) = (a + b) + c$ である。

(A2) [**零元の存在**] ある $0 \in G$ が存在して、任意の $a \in G$ に対して $0+a = a+0 = a$ である。

(A3) [**逆元の存在**] 任意の $a \in G$ に対して、ある $b \in G$ が存在して $a+b = b+a = 0$ である。(このときの b を $-a$ と書く。)

(A4) [**交換法則**] 任意の $a, b \in G$ について $a+b = b+a$ である。

加群 G において $a+(-b)$ を $a-b$ と書く。

例 2.2.1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ は (通常の加法によって) すべて加群である。$\mathbb{N}$ は加群ではない。

$n \in \mathbb{N}$ に対して、加群 G の元 a を n 個加えたものを na と書く。また $-a$ を n 個加えたものを $-na$ と書く。また $0a = 0$ と定める。これによって任意の $m \in \mathbb{Z}$ に対して ma が定義され、以下が成り立つ。$a, b \in G$, $m, n \in \mathbb{Z}$ とする。

(1) $(-m)a = m(-a) = m(-a)$ である。特に $(-1)a = -a$ である。

(2) $(m+n)a = ma + na$

(3) $m(na) = (mn)a$

(4) $m(a+b) = ma + mb$

ここで (2), (3), (4) は通常の意味の分配法則、結合法則ではないことに注意する。

2.3 部分群

群 G の空でない部分集合 H が

(B1) $a, b \in H$ ならば $ab \in H$ である。

(B2) $a \in H$ ならば $a^{-1} \in H$ である。

を満たすとき、H を G の**部分群** (subgroup) という。

命題 2.3.1. 群 G の空でない部分集合 H について以下は同値である。

(1) H は G の部分群である。

(2) H は G の演算によって群である。

(3) $a, b \in H$ ならば $ab^{-1} \in H$ である。

証明. (1) $\Longrightarrow$ (2) H を G の部分群とする。(B1) より $a, b \in H$ ならば $ab \in H$ であるから G の演算は H の演算を定義する。結合法則は G で成り立つので H でも成り立つ。また H は空でないからある元 a を含む。このとき (B2) より $a^{-1} \in H$ でもある。よって $1_G = aa^{-1} \in H$ であり 1_G は H においても単位元である。(B2) により任意の元の逆元も存在する。

(2) $\Longrightarrow$ (3) 群の定義より明らかである。

(3) $\Longrightarrow$ (1) H は空でないから $a \in H$ をとると $1 = aa^{-1} \in H$ である。任意に $a \in H$ をとる。このとき $1 \in H$ より $a^{-1} = 1a^{-1} \in H$ である。よって (B2) が成り立つ。最後に任意に $a, b \in H$ をとる。(B2) より $b^{-1} \in H$ である。したがって $ab = a(b^{-1})^{-1} \in H$ となり (B1) が成り立つ。 □

命題 2.3.2. H, K が共に G の部分群であるとき $H \cap K$ も G の部分群である。

証明. $a, b \in H \cap K$ とする。$ab^{-1} \in H \cap K$ を示せばよい。$a \in H$, $b \in H$ であるから H が部分群であることにより $ab^{-1} \in H$ である。同様に K が部分群であることにより $ab^{-1} \in K$ である。よって $ab^{-1} \in H \cap K$ である。 □

群 G の部分集合 A, B に対して

$$\begin{aligned} AB &= \{ab \mid a \in A,\ b \in B\} \\ A^{-1} &= \{a^{-1} \mid a \in A\} \end{aligned}$$

と定める。特に $B = \{b\}$ のときには $A\{b\}$ を Ab とも書く。bA も同様である。

$$Ab = \{ab \mid a \in A\}, \quad bA = \{ba \mid a \in A\}$$

問 2.3.3. 群 G と、その部分集合 A, B, C に対して、次が成り立つことを示せ。

(1) $A(BC) = (AB)C$

(2) $(A^{-1})^{-1} = A$

(3) $(AB)^{-1} = B^{-1}A^{-1}$

問 2.3.4. 群 G と、その空でない部分集合 H に対して、以下は同値であることを示せ。

(1) H は G の部分群である。

(2) $HH \subset H$ かつ $H^{-1} \subset H$

(3) $HH^{-1} \subset H$

問 2.3.5. H が群 G の部分群であるとき

$$HH = HH^{-1} = H^{-1} = H$$

が成り立つ。これを示せ。

注意. 上記の計算を群の元の計算と混同してはいけない。例えば $HH^{-1} = 1$ は一般に正しくない。(なぜ正しくないのかを考えよ。)

命題 2.3.6. 群 G と、その空でない部分集合 H に対して、$|H| < \infty$ かつ $HH \subset H$ ならば H は G の部分群である。

証明. $h \in H$ に対して $h^{-1} \in H$ を示せばよい。$HH \subset H$ より $h^2 \in H$ であり、同様にに繰り返せば、任意の $n \in \mathbb{N}$ に対して $h^n \in H$ である。H は有限集合であるから、すべての h^n が異なることはできず、したがってある $m, n \in \mathbb{N}$, $m < n$ が存在して $h^m = h^n$ となる。このとき簡約法則によって $h^{n-m} = 1$ である。$n - m = 1$ ならば $1 = h \in H$ であり、$h^{-1} = 1 \in H$ である。$n - m > 0$ のとき $n - m - 1 \leq 0$ であって、よって $h^{-1} = h^{n-m-1} \in H$ となる。 □

命題 2.3.7. H, K が群 G の部分群であるとき次が成り立つ。

(1) HK が G の部分群であるための必要十分条件は $HK = KH$ である。

(2) L が H を含む G の部分群であるならば $(HK) \cap L = H(K \cap L)$ である。

証明. (1) HK が G の部分群であるとする。このとき $(HK)^{-1} = HK$ である。一方 $H^{-1} = H$, $K^{-1} = K$ なので $(HK)^{-1} = K^{-1}H^{-1} = KH$ となるので $HK = KH$ となる。

次に $HK = KH$ であるとする。このとき $(HK)(HK)^{-1} = HKK^{-1}H^{-1} = HKKH = HHKK = HK$ であるから HK は G の部分群である。

(2) $x \in HK \cap L$ とする。$x \in HK$ より $h \in H$ と $k \in K$ が存在して $x = hk$ である。$x \in L$ であって $h \in H \subset L$ であるから $k = h^{-1}x \in L$ である。よって $k \in K \cap L$ となり $x = hk \in H(K \cap L)$ である。以上より $(HK) \cap L \subset H(K \cap L)$ となる。

$y \in H(K \cap L)$ とする。ある $h \in H$ と $k \in K \cap L$ が存在して $y = hk$ である。このとき $y = hk \in HK$ であり、$h \in H \subset L$ であるから $y = hk \in L$ も成り立つ。よって $y \in HK \cap L$ であり $H(K \cap L) \subset HK \cap L$ である。

以上により $(HK) \cap L = H(K \cap L)$ が成り立つ。 □

群 G において G 自身と $\{1\}$ は G の部分群である。これらを G の**自明な部分群** (trivial subgroup) という。また G と異なる部分群を**真部分群** (proper subgroup) という。

S を群 G の部分集合とする。

$$a_1{}^{n_1} a_2{}^{n_2} \cdots a_r{}^{n_r} \quad (a_i \in S, n_i \in \mathbb{Z}, r \in \mathbb{N})$$

の形の元すべての集合は G の部分群である。これを $\langle S \rangle$ と書き、S **で生成される部分群** (subgroup generated by S) という。S が有限集合 $\{s_1, \cdots, s_\ell\}$ であるとき $\langle S \rangle$ を $\langle s_1 \cdots, s_\ell \rangle$ とも書く。

特に $S = \{a\}$ のとき

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} = \{\cdots, a^{-2}, a^{-1}, 1, a, a^2, \cdots\}$$

である。これを a で生成される**巡回群** (cyclic group) といい a をその**生成元** (generater) という。部分群 $\langle a \rangle$ の位数を元 a の**位数** (order) といい $o(a)$ と書く。

問 2.3.8. $\langle S \rangle$ が部分群であることを示せ。

命題 2.3.9. 巡回群 $\langle a \rangle$ について次が成り立つ。

(1) $a^m = 1$ となる $m \in \mathbb{N}$ が存在すれば $\langle a \rangle$ は有限巡回群である。$a^m = 1$ となる $m \in \mathbb{N}$ のうち最小のものを n をすれば $n = o(a)$ であって次が成り立つ。

(i) $a^m = 1 \iff n \mid m$

(ii) $\langle a \rangle = \{1, a, a^2, \cdots, a^{n-1}\}$ であって、これらの元はすべて相異なる。

(2) $\langle a \rangle$ が無限巡回群ならば

$$\cdots, a^{-2}, a^{-1}, 1, a, a^2, \cdots$$

はすべて相異なり $\langle a \rangle$ はこれらの元からなる。

証明. (1) まず $a^m = 1$ となる $m \in \mathbb{N}$ が存在すると仮定して (i) $a^m = 1 \iff n \mid m$ を示す。

$a^m = 1$ とすると $m = nq + r$, $0 \leq r < n$ なる $q, r \in \mathbb{Z}$ が存在する。このとき

$$1 = a^m = (a^n)^q a^r = a^r$$

となるが n の最小性から $r = 0$ である。よって $n \mid m$ である。$n \mid m$ と仮定すれば、明らかに $a^m = (a^n)^{m/n} = 1$ である。

(i) より $\langle a \rangle = \{1, a, a^2, \cdots, a^{n-1}\}$ となることはすぐに分かる。これらがすべて異なることを示す。$0 \leq i < j < n$ に対して $a^i = a^j$ とすると $a^{j-i} = 1$, $0 < j - i < n$ となり n の最小性に反する。よってこれらはすべて異なり $o(a) = |\langle a \rangle| = n$ である。

(2) $\cdots, a^{-2}, a^{-1}, 1, a, a^2, \cdots$ がすべて異なることを示せばよい。$i < j$ $(i, j \in \mathbb{Z})$ に対して $a^i = a^j$ と仮定すると、前と同様に $a^{j-i} = 1$, $0 < j - i$ となり $\langle a \rangle$ は有限巡回群になる。よって、これらの元はすべて異なる。 □

2.4 剰余類

H を群 G の部分群とする。G 上の関係 $\sim$ を「$aH = bH$ のとき $a \sim b$」で定める。このとき $\sim$ は G 上の同値関係であることを示そう。

まず、任意の $a \in G$ に対して $aH = aH$ であるから $a \sim a$ である。次に $a \sim b$ と仮定する。このとき $aH = bH$ であるから $bH = aH$ で $b \sim a$ が成り立つ。$a \sim b$ かつ $b \sim c$ と仮定すれば $aH = bH = cH$ であるから $a \sim c$ である。以上より $\sim$ は同値関係である。

命題 2.4.1. H を群 G の部分群 H とする。$a, b \in G$ について次の条件は同値である。

(1) $a \sim b$ (すなわち $aH = bH$)

(2) $b \in aH$

(3) $a \in bH$

(4) $a^{-1}b \in H$

証明. (1) $\Longrightarrow$ (2) $b = b1 \in bH = aH$ である。

(2) $\Longrightarrow$ (3) $b \in aH$ とすると、ある $h \in H$ が存在して $b = ah$ である。このとき $h^{-1} \in H$ であるから $a = bh^{-1} \in bH$ である。

(3) $\Longrightarrow$ (4) $a \in bH$ とすると、ある $h \in H$ が存在して $a = bh$ である。このとき $a^{-1}b = h^{-1} \in H$ である。

(4) $\Longrightarrow$ (1) ある $h \in H$ が存在して $a^{-1}b = h$ である。このとき $a = bh^{-1}$, $b = ah$ に注意しておく。

任意の $h_1 \in H$ に対して $ah_1 = bh^{-1}h_1 \in bH$ であるから $aH \subset bH$ が成り立つ。任意の $h_2 \in H$ に対して $bh_2 = ahh_2 \in aH$ であるから $bH \subset aH$ が成り立つ。以上より $aH = bH$ である。 □

以上のことは関係 $\sim$ を $Ha = Hb$ で定義しても同様に成り立つ。

aH を H の**左剰余類** (left coset) といい、左剰余類全体の集合を G/H と書く。同様に Ha を H の**右剰余類** (right coset) といい、右剰余類全体の集合を $H \setminus G$ と書く。

$\sim$ は同値関係で左剰余類はその同値類となるので、左剰余類に関する類別

$$G = \bigcup_{i \in I} a_i H$$

が得られる。

問 2.4.2. $G = \bigcup_{i \in I} a_i H$ が左剰余類に関する類別であることと、$G = \bigcup_{i \in I} H a_i^{-1}$ が右剰余類に関する類別であることは同値であることを示せ。

例 2.4.3. 3 次対称群 S_3 を考える。S_3 の元は

$$g_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad g_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad g_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$
$$g_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad g_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad g_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

である。

$H = \langle g_2 \rangle = \{g_1, g_2\}$ として左剰余類を考えてみると

$$\begin{aligned} g_1 H &= g_2 H = \{g_1, g_2\} \\ g_3 H &= g_4 H = \{g_3, g_4\} \\ g_5 H &= g_6 H = \{g_5, g_6\} \end{aligned}$$

である。一方、右剰余類は

$$\begin{aligned} H g_1 &= H g_2 = \{g_1, g_2\} \\ H g_3 &= H g_5 = \{g_3, g_5\} \\ H g_4 &= H g_6 = \{g_4, g_6\} \end{aligned}$$

である。よってこの場合、左剰余類による類別と右剰余類による類別は異なっている。

$K = \langle g_4 \rangle = \{g_1, g_4, g_5\}$ として左剰余類を考えてみると

$$\begin{aligned} g_1 H &= g_4 H = g_5 H = \{g_1, g_4, g_5\} \\ g_2 H &= g_3 H = g_6 H = \{g_2, g_3, g_6\} \end{aligned}$$

であり、右剰余類も

$$\begin{aligned} H g_1 &= H g_4 = H g_5 = \{g_1, g_4, g_5\} \\ H g_2 &= H g_3 = H g_6 = \{g_2, g_3, g_6\} \end{aligned}$$

となる。よってこの場合、左剰余類による類別と右剰余類による類別は一致している。

上の例のように、左剰余類による類別と右剰余類による類別が一致するとき、言い換えれば $aH = Ha$ が任意の $a \in G$ について成り立つとき、H を G の**正規部分群** (normal subgroup) という。特に G がアーベル群ならば任意の部分群は正規部分群である。

問 2.4.4. 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。(これを **Lagrange の定理**という。また $|G : H|$ を G における H の**指数** (index) という。右剰余類についても同様のことが成り立つ。)

2.5 剰余群

G を群とし N をその正規部分群とする。このとき、任意の $a \in G$ について $aN = Na$ である。よって剰余類は右、左の区別をする必要がない。剰余類全体の集合 G/N に以下のような演算を考える。

$$(aN)(bN) = (ab)N$$

まずこれが矛盾なく定義されることを示す。

> この場合 $aN = a'N$ となる $a' \in G$ が存在するかもしれない。違う a' を使うと結果が変わってしまうというのでは演算 (写像) が定義されているとはいえない。したがって、演算が矛盾なく定義されるためには $aN = a'N$ かつ $bN = b'N$ と仮定したとき $(ab)N = (a'b')N$ が成り立たなければならない。

$aN = a'N$ かつ $bN = b'N$ と仮定する。ある $n_1, n_2 \in N$ が存在して $a' = an_1$, $b' = bn_2$ である。また $bN = Nb$ なので、ある $n_3 \in N$ が存在して $n_1 b = bn_3$ である。よってこのとき

$$a'b' = an_1 bn_2 = abn_3 n_2 \in (ab)N$$

となり $(a'b')N = (ab)N$ である。よってこの演算は矛盾なく定義される。

この演算に関して、結合法則が成り立つことは明らかで、更に

$$(1N)(aN) = (aN)(1N) = aN, \quad (aN)(a^{-1}N) = (a^{-1}N)(aN) = 1N$$

が成り立つ。よって G/N はこの演算によって $1N$ を単位元とする群になる。aN の逆元は $a^{-1}N$ である。この群を G の N による**剰余群** (factor group) といい、剰余類全体の集合と同じ記号を使って G/N とかく。

例 2.5.1. $\mathbb{Z}$ を加群と見る。$n \in \mathbb{N}$ を一つ固定する。n で生成される部分群 $\langle n \rangle$ は n の倍数全体の集合で、これを $n\mathbb{Z}$ と書く。$a \in \mathbb{Z}$ を含む $n\mathbb{Z}$ による剰余類は

$$a + n\mathbb{Z} = \{a + n\ell \mid \ell \in \mathbb{Z}\}$$

である。また $\{0, 1, \cdots, n-1\}$ は剰余類による類別の完全代表系である。よって

$$\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z},\ 1 + n\mathbb{Z}, \cdots,\ (n-1) + n\mathbb{Z}\}$$

である。演算は、例えば

$$(3 + 5\mathbb{Z}) + (4 + 5\mathbb{Z}) = 7 + 5\mathbb{Z} = 2 + 5\mathbb{Z}$$

のようになる。

参考文献

[1] 代数学, 永尾汎, 朝倉書店

[2] 代数学入門, 石田信, 実教出版