

部分群、剰余類、正規部分群、剰余群

G を群とする. G における演算を積 ab で表し、単位元を 1 で表す. また、 H を G の部分群とする. すなわち、 H は G の部分集合で、

$$(1) ab \in H \text{ for all } a, b \in H$$

$$(2) a^{-1} \in H \text{ for all } a \in H$$

の2つの条件をみたすものである.

定義 $a, b \in G$ について、 $a^{-1}b \in H$ が成立するとき

$$a \equiv b \pmod{H}$$

と書き、 a と b は H を法として左合同であるという.

補題 この関係は同値関係であり、 a を含む同値類、すなわち a と H を法として左合同であるような G の元全部の集合は

$$aH = \{ah \mid h \in H\}$$

である. これを a を含む H の左剰余類 (left coset) という.

証明 $a^{-1}a = 1 \in H$ だから $a \equiv a \pmod{H}$ である. $a^{-1}b \in H$ ならば、その逆元 $(a^{-1}b)^{-1} = b^{-1}a$ も H に含まれる. よって、 $a \equiv b \pmod{H}$ ならば $b \equiv a \pmod{H}$ である. また、 $a^{-1}b \in H$ かつ $b^{-1}c \in H$ ならば $a^{-1}c = a^{-1}bb^{-1}c \in H$ となるので、 $a \equiv b \pmod{H}$ かつ $b \equiv c \pmod{H}$ ならば $a \equiv c \pmod{H}$ である. 以上で同値関係であることがわかった.

$a \equiv b \pmod{H}$ ならば $a^{-1}b = h$ となる $h \in H$ がある. この両辺に左から a をかけて $b = ah$ を得る. 逆に $b = ah$ の形ならば両辺に左から a^{-1} をかけると $a^{-1}b = h$ が得られる. よって、 b が a と H を法として左合同であることと $b \in aH$ であることは同値である.

同値類の性質により、 $a, b \in G$ に対して

$$aH = bH \quad \text{または} \quad aH \cap bH = \emptyset$$

が成立する. a_1H, a_2H, \dots , を異なる H の左剰余類の全体とすると

$$G = a_1H \cup a_2H \cup \dots \quad \text{かつ} \quad i \neq j \quad \text{ならば} \quad a_iH \cap a_jH = \emptyset$$

となる. これを G の H による左剰余類分解 (left coset decomposition) という.

$h_1, h_2 \in H$ について、 $h_1 \neq h_2$ ならば任意の $a \in G$ に対して $ah_1 \neq ah_2$ である. よって H が有限群であれば、 H と aH の元の個数は等しい. 特に G が有限群のとき、 H の左剰余類の総数を $|G : H|$ で表すと、左剰余類分解より

$$|G| = |G : H| |H|$$

が成立する. $|G : H|$ を H の G における指数 (index) と呼ぶ. G が無限群であれば H の左剰余類が無限個存在する場合もあるが、そのときは $|G : H| = \infty$ と書く.

上記の等式より、次の定理が得られる。

定理 (Lagrange) 有限群 G の部分群 H の位数は、 G の位数の約数である。

注意 $a, b \in G$ について、 $ab^{-1} \in H$ が成立するとき、 a と b は H を法として右合同であるという。これも同値関係で、 a と H を法として右合同であるような G の元全部の集合は

$$Ha = \{ha \mid h \in H\}$$

である。 Ha を、 a を含む H の右剰余類 (right coset) という。

G の元 x にその逆元 x^{-1} を対応させる写像は G から G への全単射であるが、この写像により、 $a^{-1}b \in H$ と $b^{-1}a \in H$ 、すなわち左合同と右合同が対応し、 aH と Ha^{-1} 、すなわち左剰余類と右剰余類が対応する。 $(H = \{h^{-1} \mid h \in H\})$ であることに注意する。) よって、上に述べたことは右合同、右剰余類に対しても同様に成立する。

記号 H の左剰余類全部の集合を G/H で表し、右剰余類全部の集合を $H \backslash G$ で表す。

定義 群 G の部分群 H で

$$aH = Ha \quad \text{for all } a \in G$$

をみたすものを正規部分群 (normal subgroup) という。この条件は

$$aha^{-1} \in H \quad \text{for all } h \in H, a \in G$$

と同値である。 H が G の正規部分群であることを、 $H \triangleleft G$ と書く。

H が正規部分群であれば、 H の左剰余類と右剰余類は一致するので、この場合は単に H の剰余類という。 G が可換群であれば、その部分群はすべて正規部分群であるが、一般の群では部分群より正規部分群の方がずっと個数が少ない。特に G 自身と $\{1\}$ 以外の正規部分群がないとき、 G を単純群 (simple group) という。

N を群 G の正規部分群とする。 $a, b \in G, h, k \in N$ に対して、 N が正規部分群であることから $b^{-1}hb \in N$ となるので、

$$ahbk = abb^{-1}hbk \in abN$$

が成立する。すなわち、 N の剰余類 aN の任意の元と bN の任意の元の群 G における積は、 N の剰余類 abN に含まれる。(注意： N が正規部分群でないと、このことが成り立たない。) したがって、剰余類 aN と bN の積 $aNbN$ を

$$aNbN = abN$$

と定義しても矛盾は生じない。このように定義すると、次の (1), (2), (3) が成り立つ。

$$(1) (aNbN)cN = aN(bNcN)$$

$$(2) 1N = N \text{ で } aNN = NaN = aN$$

$$(3) aNa^{-1}N = a^{-1}NaN = N$$

実際、 $(aNbN)cN = abNcN = (ab)cN$, $aN(bNcN) = aNbcN = a(bc)N$ で、群 G における結合法則 $(ab)c = a(bc)$ により両者は一致する。よって、 N の剰余類全部の集合 G/N はここで定義した剰余類どうしの積に関して群になり、 $1N = N$ がその単位元である。また、 aN の逆元は $a^{-1}N$ である。この群 G/N を、 G の正規部分群 N による剰余群 (quotient group) という。 $\bar{a} = aN$ とおくと、積は $\bar{a} \cdot \bar{b} = \overline{ab}$ 、単位元は $\bar{1}$ 、逆元は $\bar{a}^{-1} = \overline{a^{-1}}$ となる。なお、 $b = ah$ となる $h \in N$ が存在することと $\bar{a} = \bar{b}$ は同値である。