群論はじめの一歩(5)

5.1 消去法則と群

①G を空でない次の積演算を持つ有限集合とする

② 結合法則

③ 消去法則：

$ax = ay$ なら $x = y$

$xa = ya$ なら $y = x$

この時Gは群となることを示そう。

そのためには次の４つの条件を満たす必要である

①積の下に閉じている

②結合法則

③単位元 e が存在する。すなわち、$xe = ex = x$

④逆元 が存在する。すなわち$\forall x \in G$ に対して$\exists x^{-1}$ があり、$x^{-1}x = xx^{-1} = e$ をいう。

5.2 証明

G が有限集合、結合法則、消去法則をもつとき、

③単位元e が存在する。④逆元が存在する の二つを言えばよい。

ステップ１： $e_a a = ae_a = a$ となる a の単位元e_a の存在

いま、$\{a, a^2, \cdots\} \subset G$ を考えると、G の有限性から$a^k = a^l \ (k > l)$ となるものがあるはずである。消去法則から、$a^{k-l+1} = a$ が成り立つ。いま、$i = k - l$ と置くと$a^{i+1} = a$ である。そこで、$e_a = a^i$ と置くと$e_a a = a^i a = a, ae_a = aa^i = a$ が成り立つのでe_a の存在が言えた。

ステップ２：G 単位元 e が存在する。

$a, b \in G$ とし、これらの積$ab \in G$の単位元をe_{ab} とする。すなわち、

１） $e_{ab}ab = ab$

a の単位元e_aはステップ１のものとすると

２） $ab=(e_a a)b=e_a(ab)$

である。１）２）より、$e_{ab}(ab)=e_a(ab)$ となるが消去法則から $e_{ab}=e_a$ 。また、

３） $ab(e_{ab})=ab=a(be_b)=(ab)e_b$

に消去法則を使うと $e_{ab}=e_b$ 。２）の結果と合わせると $e_a=e_b$ 。

つまり、ステップ１で G 各元に応じた単位元があるがステップ２によりその単位元は共通のものすなわちそれが G の単位元である。
ステップ３：逆元が存在する。
ステップ１において $a^{i+1}=a$ となる i の存在を示した。
$i=1$ とすると $a^2=a$ すなわち、$aa=a$ でこの式に消去法則を当てはめると $a=e$ である。つまり $ea=ae=e$ となり $a^{-1}=e$ としてよい。また、$i>1$ のような a については、$a^i a=aa^i=a$ となるので、消去法則をもちいて、$a^{i-1}a=aa^{i-1}=e$ をえて、$a^{-1}=a^{i-1}$ を得る。つまり、$\forall a\in G$ に対して、a^{-1} を見つけることができた。