

無題-群論-001

itmz153

2018 年 3 月 17 日

とある会話

K 氏「任意のアーベル群 $G(S, **)$ に対して $a ** b = abc (c \in S)$ としたとき $(S, **)$ も群になるやんけ！^{*1}」

M 氏「証明を^{*2}」

⋮

群構造

群の定義

群とは、集合と適切な演算の対である。すなわち集合を G 、演算を ϕ とすれば、 (G, ϕ) であり、演算について次の公理 γ_1, γ_2 を満たせば (G, ϕ) を群という。演算は 2 変数の写像、 $G \times G \rightarrow G$ である。

$$\gamma_1 : \forall x, y, z \in G [\phi(\phi(x, y), z) = \phi(x, \phi(y, z))]$$

$$\gamma_2 : \exists e \in G [\forall g \in G [\phi(g, e) = \phi(e, g) = g] \wedge \forall g \in G, \exists u \in G [\phi(g, u) = \phi(u, g) = e]]$$

γ_1 は演算の結合性、 γ_2 は、単位元の存在と逆元の存在性を述べている。今後、単位元は e と書き、 $x \in G$ の逆元は g^{-1} と書くことにする。今後毎回 ϕ を書くとややこしいので、代

^{*1} https://twitter.com/***** 許可待ち

^{*2} https://twitter.com/***** 許可待ち

わりに括弧を省き中置演算子 $*$ を使うことにする. また, 群 $(G, *)$ のことを, ただ単に群 G と書くことがある. その場合, 先に述べた適切な演算が G に入っていると思えば良い.

とある会話について

$(G, *)$ を群とする. ここで, $c \in G$ を固定して,

$$Gc = \{g * c \mid g \in G\}$$

なる集合を考える. G は群なので Gc も群である (表示は違うが同じ演算が自然に入ると思えば良い). ここで, 群 Gc に次のような演算 $\langle -, - \rangle_c$ を導入する.

$$\langle -, - \rangle_c : Gc \times Gc \longrightarrow Gc$$

$$\langle x, y \rangle_c \longmapsto (x * y) * c$$

実は, $Gc = G$ (集合としても (元の演算を考えれば) 群として等しい.) なので, 次を考えることと等価である.

$$\langle -, - \rangle_c : G \times G \longrightarrow G$$

$$\langle x, y \rangle_c \longmapsto x * y * c$$

この演算が, 群の演算の公理 γ_1, γ_2 を満たしているか確認していこう. 演算が閉じていることは明らか. はじめに, 結合法則がなりたつか見ていこう.

$$\begin{aligned} \langle \langle x, y \rangle_c, z \rangle_c &= \langle (x * y) * c, z \rangle_c \\ &= x * y * c * z * c \\ &= \dots \end{aligned}$$

なんだかこのままだと何もできそうにないので, c を群の中心 $Z(G)$ から取ってこよう. 群の中心とは, $\{x \in G \mid \forall g [g * x = x * g]\}$ のことである. 群の中心は G の正規部分群となるなど面白い性質がある (確認せよ).

今後, $c \in Z(G)$ とする.

$$\begin{aligned} \langle \langle x, y \rangle_c, z \rangle_c &= x * y * c * z * c \\ &= x * y * z * c * c \\ &= x * \langle y, z \rangle_c * c \\ &= \langle x, \langle y, z \rangle_c \rangle_c \end{aligned}$$

無事に新しく導入した演算は結合法則を満たすことがわかった。次に、単位元の存在性を確認しよう。

$$\exists e, \forall g [\langle g, e \rangle_c = \langle e, g \rangle_c = g]$$

いま、単位元の候補として $e' := c^{-1}$ と置こう。任意の g に対して、

$$\begin{aligned} \langle g, e' \rangle_c &= \langle g, c^{-1} \rangle_c \\ &= g * c^{-1} * c = g \end{aligned}$$

$$\begin{aligned} \langle e', g \rangle_c &= \langle c^{-1}, g \rangle_c \\ &= c^{-1} * g * c = g \end{aligned}$$

次に逆元について考察する。

$$\forall g, \exists u [\langle g, u \rangle_c = \langle u, g \rangle_c = e' = c^{-1}]$$

$u := g^{-1} * c^{-2}$ とすれば、

$$\begin{aligned} \langle g, u \rangle_c &= \langle g, g^{-1} * c^{-2} \rangle_c \\ &= g * g^{-1} * c^{-2} * c \\ &= c^{-1} = e' \end{aligned}$$

$$\begin{aligned} \langle u, g \rangle_c &= \langle g^{-1} * c^{-2}, g \rangle_c \\ &= g^{-1} * c^{-2} * g * c \\ &= c^{-1} = e' \end{aligned}$$

よって、 $e' := c^{-1}$ は単位元の公理を満たす。故に、新たな群の演算 \langle, \rangle_c は演算の公理 γ_1, γ_2 を満たしているので、 $c \in Z(G)$ なら (G, \langle, \rangle_c) は群である。

さて、この群はなんだろうか？