群は対称性を表す

1　前書き

テイリ0
X：何か。このとき $\mathrm{Aut}(X)$ は群である。

何らかの数学的な体系があればその自己同型写像の全体は（写像の合成を積として）群になる。自己同型群ってやつである。このことを根拠に「群は対称性を表現する概念である」と言われる。

確かに方程式に対してその解の入れ替え方のパターンを集めたガロア群は群の公理をみたすし、点が（バラバラにあるだけの）集合の対称性は対称群で記述できるし、裏表の区別できない多角形の対称性は二面体群で表される。

だが「群は対称性を表現する概念である」と言われると個人的には引っかかりを覚えたものである。数量詞を省いた表現は原則として「全ての」が省略されているとみなすのが数学者の流儀であろう。であれば上記言明は

(1) 任意の群は何らかの体系の自己同型群として実現される

という意味だと解釈するのが自然であろう。

……いやまあ、多数決をとるとそういう意味ではないという意見が勝つとは思うのだが。だが「○○（主語）は××（述語）である」を上記の数量詞補完の原則で読み解けば「全ての○○は××という性質を持つ」としか読めないのは確かで。定式化していない言明をそんなガチガチに解釈したがる辺りが邪道たる所以なのだと生暖かく見守ってもらいたい。

何であれ (1) の真偽を明らかにするのが本ノートの目的である。結論から先に述べておくと肯定的な解答を与えることになる。

2　主定理

この問題に取りかかるには「数学的体系」の定義を考えることから始めるのが順当であろう。少なくとも否定的に解決するのであれば数学的体系の厳密な定義を行い、そのどれの自己同型群にもならないような群が存在することを示さないといけない。

だが肯定的に解決するなら何らかの「これは数学的体系に含まれるべきだ」と言える族で、任意の群が実現されることを示せればよい。数学的体系の必要条件ははっきりしなくても、何らかの十分条件を与えるだけで事足りる可能性はあるのである。

何を含むべきか。これは間違いなく含まれる、というものをいくつか挙げていこう。

(i) 群や環など、集合にいくつかの演算を付加したものは数学的体系である。

(ii) 圏の射の結合のように定義域が全体でない半演算も許可されるべきである。

(iii) 演算の引数が 2 でなくもっと多くてもいいだろう。演算の個数もいっぱいあって良い。極限のように引数が有限である必要すらないだろうし、演算の個数も無限にあっても良い。

(iv) グラフ (V, E) など複数の台集合があってもよい。演算に加えて（頂点 v が辺 e のどちらかの端点であるということを記述する $V \times E$ の部分集合のような）関係を付加したものもありだろう。関係の引数も任意の濃度で良いだろう。

(v) 位相空間 $(X, \mathcal{O})$ や σ 加法族 $(\Omega, \mathcal{F})$ のように、台集合に部分集合族が付加されたものも認めるのがよいと思われる。

(vi) 部分集合（＝一項関係）の族がありなら演算族や関係族だってありだろう。

(vii) 同じように続けていって、部分集合族の族、演算の族から集合族への写像の族 $\cdots$ という感じのものも、個々のものは具体的に書けてしまうので排除するのはおそらく難しい。

最後のものまで全て含むようにきちんと言葉を用意するのはやや大変である。

が、幸か不幸か自己同型群を作るだけなら台集合は一つで、二項関係を用意するだけで良い。拍子抜けである。

あまりにあっけなく終わるのはあっけないので、主定理の主張はきちんと言葉を用意し、慎重に述べて紙数を稼いでおこう（笑）

定義 2.1. $(A, \{R_i\}_{i\in I})$ は次の条件をみたすとき二項関係を持つ体系であるという。

- A, I は集合である.
- 任意の $i \in I$ に対し $R_i \subset A \times A$ である。

定義 2.2. $(A, \{R_i\}_{i\in I})$ が二項関係を持つ体系であるとき次の条件をみたす $f : A \to A$ を $(A, \{R_i\}_{i\in I})$ の自己同型と言い、全体を $\mathrm{Aut}(A, \{R_i\}_{i\in I})$ と書く。

- f は全単射である。
- $\forall x, y \in A, \forall i \in I\,[(x, y) \in R_i \iff (f(x), f(y)) \in R_i]$.

$\mathrm{Aut}(A, \{R_i\}_{i\in I})$ に写像の合成を積とする二項演算を考えると、これは群の公理をみたす。$\mathrm{Aut}(A, \{R_i\}_{i\in I})$ に写像の合成という演算を付加したものを $(A, \{R_i\}_{i\in I})$ の自己同型群と呼ぶ。

定理 2.3. G を群とする。このとき $G \simeq \mathrm{Aut}(A, \{R_i\}_{i\in I})$ となる二項関係を持つ体系 $(A, \{R_i\}_{i\in I})$ が存在する。

証明： 群 G の単位元を e と表すことにする。

$A = I = G$, $R_i = \{(a, b) \mid b = ai\}$ とおき、$G \simeq \mathrm{Aut}(A, \{R_i\}_{i\in I})$ であることを示そう。

全単射 $f : A \to A$ をとる。

f が $(A, \{R_i\}_{i\in I})$ の自己同型であるとする。$a \in A = G$ に対し $(e, a) \in R_a$ であり

$$
\begin{aligned}
&(e, a) \in R_a \\
\Longrightarrow &(f(e), f(a)) \in R_a \\
\Longrightarrow &f(a) = f(e)a
\end{aligned}
$$

であるから f は $f(e)$ のみで定まることがわかる。

逆に $b \in G$ に対し $f_c(a) := ca$ とおくと $a, b \in A = G, c \in G, d \in I = G$ に対し

$$
\begin{aligned}
&(a, b) \in R_d \\
\Longrightarrow &b = ad \\
\Longrightarrow &cb = cad \\
\Longrightarrow &(f_c(a), f_c(b)) \in R_d
\end{aligned}
$$

となる。よって f_c は $(A, \{R_i\}_{i\in I})$ の自己同型である。

$G \ni c \mapsto f_c \in \mathrm{Aut}(A, \{R_i\}_{i\in I})$ が群の同型写像となることを示そう。全単射はここまでの考察から明らかなので積との可換性を確認すればよい。任意の $a \in A$ に対し

$$f_{cd}(a) = (cd)a = c(da) = f_c(f_d(a))$$

となるので確かに $f_{cd} = f_c \circ f_d$ となる。

3 群以外の概念について

定理 2.3 により「（全ての）群は対称性を表す概念である」ことがわかった。

では群以外のものはどうであろうか。思いつくままに挙げると、環、アーベル群、モノイド、順序集合、束、位相空間、距離空間、多様体、層、可算加法族 $\cdots$ などなど。これらの概念は何を表しているのだろう？

名前が付けられた歴史的なきっかけは「何らかの重要な対象を（いくつか）含み、かつ性質がよく分かる程度に制限がかかった概念」をうまく見つけようとしたことなのだろう。だが、（誤解を恐れずに言えば）個々の概念が歴史などというものに依存せず、その定義を採用することの必然性を理論的に明らかにしたい、と思うのは自然な欲求であろう。そこを深追いするのは正道ではないかもしれないが。

はっきりした特徴付けが（それなりによく）知られているのは順序集合くらいであろうか。すなわち次の定理が成り立つ。

定理 3.1. A を集合、$R \subset X$ とする。次の条件は同値である。

1. (A, R) は順序集合である、すなわち R は A 上の二項関係として反射律、反対称律、推移律をみたす。
2. 集合 X と X の部分集合族 P で $(P, \subseteq) \simeq (A, R)$ をみたすものが存在する。

証明： 定理の主張全体がよく知られていることであろうが、与えられた順序集合 (A, R) に対し (X, P) を次のようにとれることのみ言及しておく。

$$X = A, P = \{Y_a \subseteq X \mid a \in A\}, Y_a = \{b \in A \mid (b, a) \in R\}.$$

この定理は「順序集合は集合族の包含関係を記述するものである」ことを意味するわけである。

順序集合以外では、モノイドなんかはいかにも何らかの体系 A の自己構造射の全体 $\mathrm{End}(A)$ として実現できそうである。というか定理 2.3 の証明を振り返ると自己同型群 Aut を自己構造射モノイド End に置き換えても成り立ち、置き換えたものは G が群でないモノイドの場合も成り立つ。なので実際、モノイドは自己構造射のなす体系を表すものなのである。

定理 3.2. M をモノイドとする。このとき $M \simeq \mathrm{End}(A, \{R_i\}_{i\in I})$ となる二項関係を持つ体系 $(A, \{R_i\}_{i\in I})$ が存在する。

現時点で私が知っているのはこの程度だと思う。（忘れているだけかもしれないが。）もし何か思い出したり、新しく何かを知ったときにはまた別のノートを作成したいと思う。

また、関連する話題をご存じの方はぜひ情報をお寄せ下さい。

公開	初版	2016 年 2 月 16 日	公開
	第 3 版	2017 年 9 月 24 日	公開
著者	河下希		
公開場所	邪道数学研究所		
	http://cubicsphere.web.fc2.com/index.html		