はじめての群論

hora-algebra

初めての記事を書くにあたり、題材を何にするかでかなり迷いました。数学で書くことは決めていましたが、大人数に向けて TEX で文章を書いた経験がないので、自分の理解度の高い題材で経験を積もうと群論に決定しました。この記事は、群を知らない高校生が群論に楽しく触れることを目標にしています。そのため、前提知識をあまり仮定しておらず、時々助長に感じるかもしれません。また、厳密さも多少犠牲にしています。群論のお話は抽象的になることが多く、自分自身最初は混乱した記憶があります。そこでこの記事では群論の一般的な理論を習得することは諦め、具体的な現実問題の解決になるところを見てもらいます。この記事の目標は、ルービックキューブに関するある性質を群論を用いて示すことです。

1　ルービックキューブ

ルービックキューブでは、与えられた状態のルービックキューブに操作をして全ての面を揃えることを目指します。ルービックキューブの揃え方はいくつか知られています。それらはどれも複数の操作を覚えて、それらを組み合わせて揃えるという方法です。ここでは、ある意味で最も単純な揃え方、すなわち使う操作が一つだけの揃え方あるのかを考えてみます。以下の定理がそれを否定的に解決します。今後、ルービックキューブの操作について数学的に議論していきます。そのために操作という言葉の意味を明確にしておきます。操作とは、ルービックキューブの面を何回か回転させることを指します。複数の面を回転させて構いません。何も回転させないことも一つの操作と考えることにします。二つの操作は、操作の結果が同じとき同じ操作とみなします。例えば、ある面を時計回りに 90 度回転させた後に同じ面を反時計回りに 90 度回転させる操作は、何もしない操作と同じ操作とみなします。

Theorem 1.1. 操作であって、与えられたどんな状態のルービックキューブに対してもその操作の繰り返しで揃えられるようなものは存在しない。

Proof. 背理法で示します。定理の条件を満たすような操作が存在したと仮定します。その操作を g と書くことにします。どんな状態のルービックキューブも揃えられるというのは、どんな状態にもできるということと同値で、これはさらにどんな操作も可能であることと同値で

す。従って、背理法の仮定より、どんな操作も g を有限回繰り返す操作になります。二つの操作 a, b を順に行うことを考えてみましょう。今まで示したことより、a, b は g を有限回繰り返す操作になります。a は g の n 回の繰り返し、b は g の m 回の繰り返しであったとします。a を行ってから b を行う操作は、g を n 回行ってから g を m 回行う操作です。b をおこなってから a を行う操作は g を m 回行ってから g を n 回行う操作です。これらは共に g を $n+m$ 回行う操作に他ならないので、二つの操作 a, b を両方行うとき、その順番に寄らず同じ操作になります。a, b は今どんな操作でもよかったので、a はある面を半回転させる操作、b はその隣の面を半回転させる操作、のときを考えます。すると、この二つの操作を両方行うとき、その順序によって違う操作になっていることが確認できます。これは矛盾です。 □

上の証明はあえてルービックキューブの言葉からできるだけ離れないように書きました。というのも、上の定理は群論の基本的な定理の一例にすぎず、群の言葉で書いた方が楽なのです。次の節で群を定義し、ルービックキューブと群を結びつけます。そしてその次の節では上のルービックキューブの性質が群の性質の一例にすぎないということをみていきます。

2 群

群とは何か、定義する前にまずそのお気持ちを説明します。群とは、最も基本的な代数構造といってよいでしょう。代数構造というのは、演算を考えられる集合の構造だと思ってください。例えば実数集合 $\mathbb{R}$ には四則演算を考えられますし、0 以上の整数の集合 $\mathbb{N}$ には加法と乗法が考えられます。群とは、演算を考えられる集合のうちいくつかの良い性質を満たすものです。我々が今回考える演算は特に二項演算と呼ばれるものです。

Definiton 2.1 (二項演算)**.** 集合 X 上の二項演算 $*$ とは X の元の組に対して X の元を一つ対応させる規則である。(a, b) に対応する X の元を $a * b$ と書く。

ここで注意ですが、X の元の組には順序を考えます。つまり、X の元の組 $a * b \neq b * a$ でも構いません。

Example 2.1. 加法減法乗法は、それぞれ $\mathbb{R}$ 上の二項演算です。それぞれ、実数の組 (a, b) を $a+b, a-b, a \times b$ に対応させます。除法は $\mathbb{R}$ 上の二項演算ではありません。$a/0$ は定義されていないので $(a, 0)$ に対応させる実数がないからです。

Example 2.2. 加法と乗法は、それぞれ $\mathbb{N}$ 上の二項演算です。それぞれ、0 以上の整数の組 (a, b) を $a+b, a \times b$ に対応させます。減法除法は $\mathbb{N}$ 上の二項演算ではありません。$a < b$ の時 (a, b) に対応させる 0 以上の整数がないからです。除法は前の例と同様に $(a, 0)$ に対応させる 0 以上の整数がなく、さらに a が b で割り切れない時も (a, b) に対応させる 0 以上の整数が

ありません。

Example 2.3. 一つだけ元を持つ集合 $\{e\}$ 上の二項演算を考えます。(e,e) に対応させる元を選べば決まりますが、これは e を選ぶしかありません。$\{e\}$ 上の二項演算はただ一つです。

Example 2.4. ルービックキューブの操作の集合を $\mathcal{R}$ と書くことにします。$\mathcal{R}$ の元の組 (a,b) に対して、b をした後に a をする操作 $a \bullet b$ を対応させる規則 $\bullet$ を考えます。これは二項演算です。二つの操作を連続して行うと、それらをまとめて一つの操作とみなせることに注意してください。

二項演算が一つ定義された集合のうち、良い性質を持つものを群と呼びます。

Definiton 2.2 (群)**.** 集合 G と G 上の二項演算 $*$ であって、以下の 3 条件を満たすものを群と呼ぶ。

1. G のどんな元 a,b,c に対しても、$(a*b)*c = a*(b*c)$ となる。
2. ある G の元 e が存在して、G のどんな元 a に対しても $a*e = e*a = a$ となる。
3. どんな G の元 a に対してもある G の元 b が存在して $a*b = b*a = e$ となる。

1 の性質を結合則と呼ぶ。2 での e を群 G の単位元と呼び、3 での b を a の逆元と呼ぶ。

抽象的な定義で、満たすべき条件もわかりにくく感じるかもしれませんが、それぞれ実はよく知っている性質です。具体例を通じて一つ一つを確認していきます。

Example 2.5. 実数集合 $\mathbb{R}$ と加法 $+$ は群になります。条件を確認していきましょう。まず、加法の結合則はよく知られている通り成り立ちます。実際、どんな実数 a,b,c に対しても、$(a+b)+c = a+(b+c)$ です。次に、単位元の存在を示します。この場合、単位元は 0 です。実際、どんな実数 a に対しても、$a+0 = 0+a = a$ です。最後に、逆元の存在を示します。実数 a の逆元は $-a$ です。実際、$a+(-a) = (-a)+a = 0$ です。

Example 2.6. 0 以上の整数の集合 $\mathbb{N}$ と乗法 $\times$ は群になりません。結合則は成り立ちますし、単位元は 1 です。ただ、1 以外の逆元は存在しません。例えば、2 の逆元 b が存在したと仮定すると、$2 \times b = 1$ となりますが、$b = 1/2$ は $\mathbb{N}$ の元ではありません。

Example 2.7. 集合 $\{e\}$ と、その上の唯一の二項演算は群を成します。結合則は自明です。どんな演算をしても結果は e だからです。単位元は e で、e の逆元は e です。

Example 2.8. ルービックキューブの操作の集合 $\mathcal{R}$ と、二項演算 $\bullet$ は群になります。ここで、$\bullet$ は、先ほど定義した、$\mathcal{R}$ の元の組 (a,b) に対して、b をした後に a をする操作 $a \bullet b$ を対応させる規則です。条件を確認していきます。結合則は成り立ちます。$(a \bullet b) \bullet c$ も $a \bullet (b \bullet c)$

も、どこをまとまりとして見るかの差があるだけで、操作としては c, b, a をこの順に行う操作だからです。単位元 e は、何もしないという操作です。実際、どんな操作 a に対しても、a をしてから何もしない、何もしないをしてから a をする、はどちらも単に a をすることに同じです。最後に逆元です。操作 a の逆元は、逆の操作です。逆再生することを考えると、実際に逆元の条件を満たす操作であることがわかります。

ここまでで、群という概念を獲得して、ルービックキューブの操作が群の一例になっていることを理解してもらえたかと思います。なぜルービックキューブの操作が群であることを確かめたかというと、群の一例になっていることがわかれば、群の一般論が使えるからです。一般の群で成り立つことはルービックキューブの操作に関しても成り立ちます。定義が抽象的な分、群論の定理は強力なのです。次の章では、「巡回群ならば可換群」という群論の単純な性質を示します。 1 節の定理、ルービックキューブは一つの操作の繰り返しでは解けない、はこの群論の性質の一例になります。

3　巡回群と可換群

2 で割れる自然数を偶数、自身と 1 以外で割れない自然数を素数と呼ぶように、群の中にも分類があります。これから二つの分類、巡回群と可換群、を定義して、巡回群なら可換群になることを示します。まず、巡回群の定義のために、群の冪乗の記法を定義しておきます。

Definiton 3.1. a を群 G(演算は $*$) の元、n を整数とする。$n > 0$ のとき、a の n 乗とは、a 自身を n 個演算したもの $a^n = \underbrace{a * \cdots * a}_{n}$ のこととする。$n = 0$ のとき a の 0 乗は $a^0 = e$（単位元）とし、$n < 0$ のとき、a の n 乗は a の逆元の $-n$ 乗とする。

場合分けがあってわかりにくいかもしれませんが、これは指数法則が成り立つように自然に定義してあります。例えば、a の逆元は a^{-1} になっていて、$a * a^{-1} = a^{1-1} = a^0 = e$ とうまくいっています。指数法則が成り立つことは定義からすぐわかるのですが一応覚えておいてください。念のため注意しておくと、n 個演算する、と言うのが演算する順番に寄らずうまく定義されるために結合法則が使われています。ルービックキューブの群 $\mathcal{R}$ の例で言えば、n 乗するとは、同じ操作を n 回繰り返すことに対応します。

Definiton 3.2 (巡回群)**.** 群 G が巡回群であるとは、G の元 g が存在して、どんな G の元も g の整数乗でかけることを言う。

つまり、巡回群であるとは、一つの元を演算したり逆元とったりするだけで全体を回れることを主張しています。軸は、巡回群であるという性質はかなり強く、それだけでほとんど構造が決まってしまいます。以下に二つ巡回群の例を出しますが、ともに簡単な構造の群です。

Example 3.1. 集合 $\{e\}$ とその上の唯一の二項演算は群を成していましたが、この群は巡回群です。$\{e\}$ のどんな元も e のべき（すなわち e）でかけるからです。

Example 3.2. 整数の集合 $\mathbb{Z}$ と加法 $+$ は群をなします。結合則は既知、単位元は 0、a の逆元は $-a$ です。これは巡回群です。1 の n 乗は、今加法を考えているので 1 を n 個足したもの、すなわち $n \times 1 = n$ です。よって、どんな $\mathbb{Z}$ の元も 1 の整数乗 (ここでは整数倍になっている) でかけます。

では、巡回群でない例を出したいわけですが、これは存在を否定しなくてはならないので少し手間がかかります。

Example 3.3. 実数集合 $\mathbb{R}$ と加法 $+$ の群は巡回群ではありません。どんな $\mathbb{R}$ の元も、r の整数乗でかけるとしましょう。r の n（整数）乗は nr です。$r = 0$ だと $nr = 0$ ゆえ 1 が作れませんし、$r \neq 0$ なら $r/2$ が作れません。よって定義の条件を満たす r はありません。

ルービックキューブの操作の群 $\mathcal{R}$ は巡回群でしょうか。実は、これこそが最初の問題提起、ルービックキューブは一つの操作で解けるか、なのです。ルービックキューブを解くどんな操作も、一つの操作の繰り返しになるか、という疑問だからです。そして、最初の定理によって、巡回群でないことが証明されています。その少しテクニックな証明には、二つの操作の順番を入れ替えられないことを使いました。操作が入れ替えられるかを考えるのは、一般の群で、演算する元の順番を入れ変えられるか考えることに対応します。入れ替えられる群、つまり交換法則が成り立つ群を可換群と呼ぶわけです。

Definiton 3.3 (可換群)**.** 群 G（演算は $*$）が可換群であるとは、どんな G の元 a, b に対しても $a * b = b * a$ が成り立つことを言う。

巡回群の例ででた二つの群は可換群であることを見ます。

Example 3.4. $\{e\}$ と唯一の二項演算 $*$ は可換群です。元がただ一つなので、示すべき等式は $e * e = e * e$ のみですが、これは自明だからです。

Example 3.5. $\mathbb{Z}$ と加法 $+$ は可換群です。示すべき等式は、整数 n, m に対して $n+m = m+n$ となることです。これは加法の交換法則そのものです。

Example 3.6. $\mathbb{R}$ と加法 $+$ は可換群です。これは実数でも加法の交換法則が成り立つことそのものです。

Example 3.7. ルービックキューブの操作の群 $\mathcal{R}$ は可換群ではありません。交換法則が成り立たないような $\mathcal{R}$ の元の組 a, b を一つ持って来れば証明できます。例えば、a はある面を半回転させる操作、b はその隣の面を半回転させる操作、とします。このとき、$a \bullet b \neq b \bullet a$ です。

先ほど挙げた巡回群の例は全て可換群になっていました。実は以下の定理が成り立ちます。

Theorem 3.1. 巡回群は可換群である。

Proof. 群 G（演算は $*$）が巡回群であったと仮定し、どんな G の元も g の整数乗でかけるとします。このとき、どんな G の元 a, b も、整数 n, m を使って $a = g^n, b = g^m$ とかけます。したがって、指数法則が成り立つので $a * b = g^n * g^m = g^{n+m} = g^{m+n} = g^m * g^n = b * a$ となります。 □

群論の基本的な性質に一つ到達しました。最初の定理がこの性質の一例であることを明確にしておきます。対偶を考えると、「可換群でないならば巡回群でない」となります。示したいことは、ルービックキューブが一つの操作で解けないこと、つまりルービックキューブの操作の群 $\mathcal{R}$ が巡回群でないことでした。よって、$\mathcal{R}$ が可換群でないことを示せば証明が終わるわけです。

4　おわりに

今回、群という視点からルービックキューブを眺めてみたわけですが、群論はもっともっと深く面白い性質に言及します。文章を書いた経験があまりないもので、読みにくかったとは思いますが、最後まで読んでいただきありがとうございました。今後も記事を書くと思いますので、また読んでくださると嬉しいです。

参考文献

[1] 雪江明彦, 整数論 1 初等整数論から p 進数へ, 日本評論社, 2014.