# 整数の剰余類の作る乗群

Joh @物理のかぎプロジェクト

2006-04-23

整数の剰余類を全て集めた集合は，加法に関して群となり，有限巡回群と同型となることを見ました．この記事では，剰余類が乗法に対しても群を作るかどうかを確認してみます．

## 剰余類が乗群になるかを確認してみる

まず，剰余類同士の乗法が次式のように閉じていることは言えます．

$$a \equiv a' \ , b \equiv b' \ (\mathrm{mod}.m) \implies ab \equiv a'b' \ (\mathrm{mod}.m)$$

**proof**

**左辺より，ある整数** $k, k'$ **を使って，**$a - a' = km, b - b' = k'm$ **と表わせるはずです．このとき** $ab - a'b' \equiv (a - a')b + a'(b - b') \equiv (kb + a'k')m \equiv 0 \ (\mathrm{mod}.m)$ **が言えます．∴** $ab \equiv a'b' \ (\mathrm{mod}.m)$ ■

単位元は 1 を含む剰余類 (これを [1] と書きます) です．ここまで順調ですね．ところが・・・，ううむ，逆元がうまく定義できません！ [0] を掛ければ，どの剰余類も 0 になってしまいますから，逆元が存在しないのです (ToT)/.

## 群になる剰余類の乗群

あと一歩で，剰余類は乗法についても群になりそうでしたが，逆元が問題でした．しかし，もし [0] を除いておけば，乗群を作るのも上手くいきそうです．

整数 $n$ に関する剰余類のうち，0 を含まないものを $n$ **と互いに素な剰余類** と呼びます．そして，$n$ と互いに素な剰余類だけを集めた集合を ${Z_n}^*$ と書くと，これは乗群を作ります．

---

*1 実は，既に似たような例を 群の公理 の例で見ています．実数全体の集合 ( $R$) は，乗法に関して群にはなりませんが，0 を除いた実数の集合 ( $R^*$ ) を考えれば，これは群になるのでした．行列の演算も，行列が正則でなければ逆元がありませんが，正則行列の集合は乗群を作ります．乗法の逆演算は一般に一筋縄ではいかないもので，『 0 を除けば』『正則ならば』など付帯条件が要るものなのです．零元を抜いた集合は星印 ( $*$ ) をつけて表わすのが普通です．

**theorem::**

**n と互いに素な剰余類全体は，乗群をつくります**

*2 整数の剰余類は加群になり，[0] を除いた整数の剰余類は乗群になるということでした．加群にも乗群にもなる，というのはなかなか特別な性質に思えます．群には一つだけ演算がなりたてば良かったので，いまは乗群と加群を別々に考えていますが，そのうち，加法と乗法を両方とも考える代数構造である 体 が出てきます．整数の剰余類は体になるのです．もうすぐ体も勉強しますので，そんなことも頭の片隅に覚えておくと良いと思います．

*3 抽象的な立場では，二項演算は全て積の形で $ab \longmapsto c$ のように書けますので，乗法と加法の違いは，加法が可換であることを除けば形式的なものだと見なすこともできます．群のあとに学ぶ体や環といった代数構造には二種類の演算が与えられており，これを形式的に加法と乗法と呼びますが，場合によってはこれらの演算が私達が「普通に知っている足し算や掛け算」とはかなり様子の異なる演算になる可能性があります．そこで，抽象的な概念であることを強調するため，$+$ や $\times$ の代わりに $\oplus$ や $\otimes$ を使ったりします．一般に加法と乗法を両方考えるときに注意すべきことは，本文で見たように，加法と乗法では単位元が異なること，および加法の単位元 ( 0 と呼ぶ) を含む積には逆演算が定義できないことです．