

整数の剰余類のつくる加群

Joh @物理のかぎプロジェクト

2006-04-23

整数全体の加群 Z を、自然数 n を法として類別した剰余類を考えます。このとき、異なる剰余類に属する二つの整数 a, b について、次の演算が成り立ちます。

$$a \equiv a', b \equiv b' \pmod{n} \implies a + b \equiv a' + b' \pmod{n}$$

proof

左辺より、ある整数を使って k, k' を使って、 $a - a' = kn, b - b' = k'n$ と表わせるはずです。このとき $(a + b) - (a' + b') = (a - a') + (b - b') = (k + k')n \equiv 0 \pmod{n}$ が示せます。∴ $a + b \equiv a' + b' \pmod{n}$ ■

ある剰余類の元に他の剰余類の元を足したものが、やはりどこかの剰余類に属する元になることが分かりましたので、どうやら整数の加群の剰余類は、剰余類同士の演算について閉じているようです。

このように、剰余類と剰余類を足すという加法演算を、『剰余類の集合』に導入しましょう。この加法演算には単位元があります（0 を含む剰余類、すなわち余りが零の剰余類です）。また、逆元もあります（ a を含む剰余類に $-a$ を含む剰余類を足すと、余りが零の剰余類になってしまいます）。

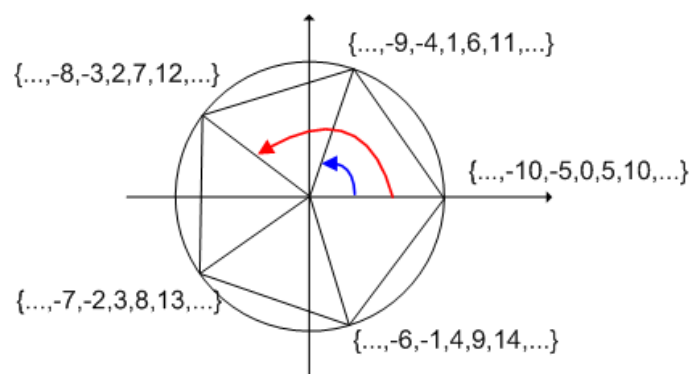
よって、この剰余類の集合は、加法に関して群になっていることが分かりました。これを n に関する剰余類群と呼び、 Z_n で表わします。

有限巡回群との同型

剰余類の辺りから少し話が抽象的になりましたから、剰余類群という、とても抽象的な群を求めたように感じるかも知れないのですが、実は、 n に関する剰余類群 Z_n は、 n 次の有限回転群と同型（つまり有限巡回群と同型）で、もう読者のみなさんが知っている群なのです。面白いことです！

整数と聞いて、数直線状にまっすぐ数が並んでいるイメージしか持っていないと、ピンとこないかも知れません。しかし、次の図を見れば、剰余類の加法が、有限回転変換に対応させられることが納得いくと思います。

*1 一つ一つの剰余類は集合ですが、一般に剰余類自身は群にはなりません。ところが、このように剰余類の集合（つまり、集合の集合！）を考えると、うまく群になったりするんですね。集合の集合、集合の集合の集合、のようなものをいくらでも考えられるのが、抽象数学の素晴らしさです。



あるいは、一直線の数直線を、周の長さが 5 の円筒にグルグル巻き付ければ、この図のようになると考えても良いでしょう。

*² n 次の有限巡回群を一般に Z_n と書くと、[有限巡回群](#) のページで触れましたが、このような事情があったのですね。 Z は整数 (ドイツ語で *Zahl*) の意味です。

*³ 整数は無限にあるわけですが、整数全体を 5 で割ったときの剰余は、0, 1, 2, 3, 4 の 5 種類しかありません。しかもその剰余はグルグル循環します。そう考えると、有限巡回群と同型だということも至極当然だと分かります。