整数の加法群の剰余類

Joh @物理のかぎプロジェクト

2006-04-23

整数全体は，加法に関して群をつくるということでした（ 群の公理 の例 6 を参照）．これを整数の加法群と呼びます．このページでは，ある整数で割ったときの余りに応じて，整数全体をグループ分けすること (類別です) を勉強します．

類別の概念自体は，類別 で勉強しましたが，この記事では同値関係と併せて，さらに理解を深めることを目標とします．

合同式

整数論を習っていない人のために，ここで少し合同式の復習をしておきます．

ある整数 p を，整数 $m(>1)$ で割ると，ただ一通りに次のように表現することができます．k も整数です．

$$p = km + q$$

ここで，k を **整商**，q を **剰余** と呼びます．剰余とは，要するに余りです．m で割ったとき，幾つ余るかという点だけに着目すると p と q は同じですから，これを次のように書き，『法 m について合同である』と言います．『 m で割ったときの余りが等しいよ』という意味です．これを合同式と言います．mod. とあるのが，何の数で割ったかを示す記号です．

$$p \equiv q \pmod{m}$$

同値関係

さて，群の類別のページで同値関係という概念を勉強しましたが，二つの整数 p, q は，実は合同式によって同値関係で結ばれると言えるのです．同値関係は，集合の二つの元 a, b について，次の三つの関係

---

*1 ここに出てくる記号 mod は *modulo* の略です．そのままモドと読む人もいますが，正しくはモジュロです．例えば mod.3 を『 3 を法として』と読んでもいいし『モジュロ 3 』と読んでも良いです．ラテン語で基準，単位などを意味する *modulus* から派生した前置詞が *modulo* です．

が成り立つような関係と定義されます.

1. $a \sim a$
2. $a \sim b \implies b \sim a$
3. $a \sim b, b \sim c \implies a \sim c$

最初の条件は，同値関係 $\sim$ がなりたつとき，どんな元も自分自身とは同値だという主張 (**反射律**)，二番目の条件は，同値関係はどちらの視点から見ても成り立つという主張 (**対称律**) です．三番目の条件は，**推移律** と呼ばれます.

剰余類

さて，二つの整数の間になりたつ合同関係は，同値関係の 3 つの条件を満たします.

1. $p \equiv p \ (\mathrm{mod}.m)$
2. $p \equiv q \ (\mathrm{mod}.m) \implies q \equiv p \ (\mathrm{mod}.m)$
3. $p \equiv q,\ q \equiv r \ (\mathrm{mod}.m) \implies p \equiv r \ (\mathrm{mod}.m)$

そこで，整数全体は，合同関係を使って類別できるといえます．一般に，集合は，元に同値関係がなりたつとき，類別できるのでした (類別 を参照)．例えば，5 を法とした合同関係を考えましょう．すると，どのような整数も，5 で割ったときの余りは $0, 1, 2, 3, 4$ のどれかであるはずですので，整数全体を 5 つに類別できることになります.

余りが 0 の類：$\{-10, -5, 0, 5, 10, 15, 20, 25, ...\}$
余りが 1 の類：$\{-9, -4, 1, 6, 11, 16, 21, 26, ...\}$
余りが 2 の類：$\{-8, -3, 2, 7, 12, 17, 22, 27, ...\}$
余りが 3 の類：$\{-7, -2, 3, 8, 13, 18, 23, 28, ...\}$
余りが 4 の類：$\{-6, -1, 4, 9, 14, 19, 24, 29, ...\}$
各類には，他の類と重複するような元がないことを確認してください．(剰余類 につづく．)

[*2] 余力のある人は 剰余類 に進む前に，余りが 0 の類だけは部分群になっていることを確認してみて下さい.