有限巡回群

Joh @物理のかぎプロジェクト

2006-04-23

すでに，対称群 と 有限回転群 の稿で，巡回群の定義が出てきました．有限回転群や，それに対応する置換操作の作る群は，巡回群だということでした．巡回群の著しい特徴は，全ての元がたった一つの元の冪乗で表わせるという点です．この稿では，巡回群についてもう少し勉強します．新しく出てくる言葉は，部分巡回群，元の位数です．

有限巡回群

もう一度，有限回転群 で出てきた，五角形の有限回転群 G_5 を思い出しましょう．G_5 は，位数 5 の有限巡回群でした．一般に，図形を $\frac{2\pi}{n}$ だけ回転する変換を生成元 p として作られる群は，位数 n の有限巡回群になります．巡回群は Z で表わすことが多いようなので，以後，巡回群を表わす記号には Z を使います．

$$Z_n = \{e, p, p^2, ..., p^{n-1}\}$$

単位元を e で表わしたため，p の指数は $n-1$ までとなっています．p 以外の文字を見たくない人は，e を p^n，もしくは p^0 と表わしても良いですが，そうすると単位元があるのかどうか分かりにくくなってしまいますので，やはり上式のように書くのが良いでしょう．

指数についての注意

巡回群の元同士の演算では，普通の指数の計算のように，積に対して指数を足すような表記が可能です．便利ですね．

$$a^r a^t = a^{r+t}$$

---

*1 有限回転群と有限巡回群は，群としては同じと考えてよいもの (同型) なので，これを別々の稿に書いて並べるのはいかにもエレガンスに欠けるかもしれません (ToT)/~.

*2 巡回群は一種の対称群ですが，対称群が巡回群になるとは限りません．巡回群は全て可換群ですが，対称群には可換群も非可換群もあるからです．

ただし，n 次の巡回群には高々 n 個の元しかありませんから，もし $r+t>n$ となったら，これはどれか他の元と同じだと言うことになります．注意しないといけません．

全ての元を順番に並べてある場合 $\{a, a^2, a^3, ..., a^n\}$，$a^n$ が単位元 e と等しくなるのですから，$a^{n+1}=a, a^{n+2}=a^2$ という具合に，n を越えた分だけまた元に戻ります．そこで，指数として $r+t$ を n で割った剰余を考えるようにすれば心配いりません．

$$a^r a^t = a^k \quad (k \equiv r+t \ (\mathrm{mod}.n))$$

部分巡回群と元の位数

位数 n の巡回群 Z_n を考えましょう．つまり，Z_n の中には異なる元が n 個あるということです．

ここで，Z_n の任意の元を一つ選び (仮に b と名づけます)，b の冪乗を考えます．

$$b, b^2, b^3, ...$$

ここで b は有限巡回群 Z_n の要素なので，b の冪乗が無限種類あるということはなく，どこかで出尽くすはずです．全ての種類の出尽くした後の冪乗 (b^s とします) は，それまで出てきた b の冪乗のどれか (b^t $(t<s)$ とします) と等しいはずですから，次のように書けます．

$$b^s = b^t \quad \Leftrightarrow \quad b^{s-t} = e$$

ここで $s-t$ は n よりも小さいはずなので，結局，b の n 乗を b^1 から b^n まで順番に見ていく途中に，**どこかに単位元が出てくる** ということです．$s-t$ を k と置くと，一般的には $k \leq n$ が言えるということです．

ここまでの b の冪乗を使って，k 次の巡回群を生成することができます．

$$H_k = \{e, b, b^2, b^3, ..., b^{k-1}\}$$

この H_k を，Z_n の **部分巡回群** と呼びます．この k の値は，Z_n のどの元を生成元として選ぶかによって異なります．逆に，どの元を部分巡回群の生成元とするかを選べば，この k の値は一つに決まります．

つまり，巡回群の元の一つ一つは，その元を生成元として作る部分巡回群の位数と一対一に対応しているということです．

この k を，**元の位数** と言います．(今後混乱しないように，群の位数との意味の違いをしっかり確認しておいて下さい．) いろいろ書きましたが，要するに群の元 x が $x^k=e$ を満たすなら，そのような k で最小のものを元の位数と呼ぶということです．

---

*3 ここでは，最初に有限巡回群 Z_n を考えましたが，一般には，ある群 (有限群でも無限群でもよい) の元 a を生成元として巡回群が生成されれば，元 a の位数を定義できます．また，群有限群に対しては，その元の冪乗は群の中で閉じているはずで，有限種類しかありませんから，もし単位元が含まれれば巡回部分群を作ります．(単位元のみ，もしくは群自身も自明な部分群になりますので，絶対にそのような部分群があると言えます．) ですから，別にもとの群が巡回群である必要は全くありません．上の例では，巡回の意味が分かりやすいように巡回群 Z_n を考えましたが，元の位数は一般の有限群の元に対して定義できる，という点を混乱しないで下さい．元の位数は，ラグランジェの定理 でまた勉強します．

*4 もとの群 Z_n の元を任意に選び，それを生成元として巡回群を作ってみると，一般にはもっと次数の低い巡回群ができてしまう，ということでした．ここで巡回群の定義に立ち戻ってみると， Z_n は一つの生成元の冪乗によって作られたわけですから，その生成元の位数は n であるはずです．一般に n 次の巡回群の元の中には，位数が n であるものが存在すると言えます．

演習問題１

一つの元 a を生成元とする有限巡回群は，a^{-1} を生成元とする有限巡回群に等しいことを示してください.

演習問題２

巡回群は可換群であることを確認してください.

演習問題３

位数 15 の有限巡回群の生成元の選び方には何通りあるでしょうか.