群の位数と元の位数

Joh @物理のかぎプロジェクト

2006-04-23

群の位数と，元の位数の区別が曖昧な人は，もう一度復習してから先へ進むようにしてください．この記事では，位数に関する美しい定理を幾つか勉強します．

巡回置換の位数

theorem

m 項の巡回置換 $p = (1\ 2\ .....\ m)$ の元の位数は，m です．

proof

巡回置換 $p = (1\ 2\ .....\ m)$ の冪乗を考えます．例えば p によって 1 がどのように置換されるかを考えると，p によって 1 は 2 と交換され，p^2 によって 3 と交換され，p^3 によって 4 と交換され,,,,,, p^{m-1} によって m と交換されます．これより，$p, p^2, ..., p^{m-1}$ は全て異なる元であり (少なくとも 1 が違うところにあるから)，また e でもないことが分かります．p^{m-1} にもう一つだけ p を掛けると，p^m は単位置換になることが分かります．すなわち，p を生成元として作った巡回群 $Z = \{e(= p^m), p, p^2, ..., p^{m-1}\}$ の位数は m です．p の位数も m だと言えます．■

とても美しい定理です．m 次の巡回群の位数は m でしたから，この定理を次のように言い換えることもできます．少し感動する結果です．

theorem

有限巡回群では，群の位数と元の位数が一致します．

群の位数と元の位数の関係

有限群の位数と，その元の位数については次のような簡単な定理がなりたちます．これも美しい定理です．

theorem

有限群 G の元 a の位数は，G の位数 $|G|$ の約数になります．

proof

群 G の位数を n とし，群 G の元 a の位数を k とします $(k \leq n)$．a の生成する部分巡回群を H とすると，さきほどの定理より $|H| = k$ が成り立ちます．一方，ラグランジェの定理より，$|H|$ は，$|G|$ の約数になっているはずでした．したがって，一般に，有限群 G の元 a の位数は，G の約数になります．■

位数が素数である群

前節で，有限群の元の位数は，必ず群の位数の約数であるという結果を得ました．約数と聞いて『じゃあ G の位数が素数だったらどうなるんだ？』と思った人は，なかなかセンスがあります．

ここで考える有限群群 G は，単位元 e だけの自明な群ではないとします．つまり，少なくとも単位元以外の元 a を持ち，$|G| \neq 1$ とします．

前節の定理より，a の位数は G の位数の約数でしたが，G の位数が素数 (p とします) だとすると，a の位数は，1 と p のどちらかのはずです．しかし $|G| \neq 1$ でしたので，結局，a の位数は p しかありえません．

つまり a の冪乗のつくる巡回群 $\{a, a^2, ..., a^p\}$ は，群 G 自身に一致するということです．

theorem

群の位数が素数ならば，その群は巡回群です．

[*1] この定理の意味するところは，なかなかショッキングです．ここまで巡回群を『対称群の特殊なもので一つの生成元だけからなる』という性質からのみ論じてきましたが，群の位数という，群の大局的な性質のみで決まってしまう事柄もあったのです．群論と整数論の隠された関係が，少し顔をのぞかせたような定理です．