

交換子群

Joh @物理のかぎプロジェクト

2007-03-03

五次方程式の可解性に関して、交換子群の定理を使いたいので、ここで交換子群という群を紹介します。この記事は補足的なもので、ガロア理論の大筋とは、あまり関係がありません。交換子群について知りたくて、いきなりこの記事を読んでいる人は、ガロア理論に関する説明は無視して読んで下さい。

交換子群

群 G の元 x, y に対し、 $xyx^{-1}y^{-1} (\in G)$ を、元 x, y の交換子もしくは交換子積と呼びます。そして、交換子によって生成される群を交換子群と呼びます。交換子群は単位元 $\{e\}$ だけの最小のものから、群 G 自身になる場合もあります。交換子を $[x, y]$ と表わし、群 G の交換子群を $D(G)$ と表わします。(G' と表わしている本もありますが、ここでは $D(G)$ を採用します。) まずは、交換子群がたしかに群になることを見てみましょう。

1. 交換子を取る操作に対して、交換子群は閉じています。($xyx^{-1}y^{-1}$ と $zwx^{-1}w^{-1}$ の交換子積 $xyx^{-1}y^{-1}zwx^{-1}w^{-1}(xyx^{-1}y^{-1})^{-1}(zwx^{-1}w^{-1})^{-1} = xyx^{-1}y^{-1}zwx^{-1}w^{-1}yxy^{-1}x^{-1}wz^{-1}z^{-1}$ で、 $xyx^{-1}y^{-1} = \alpha, zwx^{-1}w^{-1} = \beta$ と置けば、 $\alpha\beta\alpha^{-1}\beta^{-1}$ と書けて、確かに交換子群に含まれることが分かります。)
2. 任意の元 x と e との交換子積は e になりますので、 e 交換子群に含まれ、交換子積の単位元だと言えます。
3. $xyx^{-1}y^{-1}$ の逆元は $yxy^{-1}x^{-1}$ ですが、これも確かに交換子群の元です。

また、 G の元の積に関して結合則はなりたつはずなので、 $D(G)$ の元の交換子積でも結合則がなりたつことは明らかです。

次に、交換子群に関して、いくつか重要な定理を紹介します。(これらは、ガロア理論の証明で使うので、いまここで何の役に立つのかよく分からなくても、気にしないで下さい。)

theorem

群 G が可換群であることと、 $D(G) = \{e\}$ となることは同値です。

proof

G が可換群なら，任意の元 $x, y \in G$ に対して $xyx^{-1}y^{-1} = xyy^{-1}x^{-1} = e$ となります．

この定理の証明は簡単すぎでしたが，結果は大事です．

theorem

群 G の交換子群 $D(G)$ は G の正規部分群で，商群 $G/D(G)$ は可換群になります．

proof

群 G の任意の元 z に対して， $z(xyx^{-1}y^{-1})z^{-1} = (zxxz^{-1})(zyz^{-1})(zxxz^{-1})^{-1}(zyz^{-1})^{-1}$ と書けますので， $zD(G)z^{-1} \subset D(G)$ が言えます．これより $D(G)$ が正規部分群であることが分かりました．

theorem

群 G の正規部分群 N に対して，商群 G/N が可換群となることは， $N \supset D(G)$ となることと同値です．

proof

まず $G \supset N \supseteq D(G)$ とすると， $(xN)(yN) = (xyNy^{-1})(yN) = xyN = yxN = (yN)(xN)$ が成り立つので，商群 G/N は可換群だということが言えます．(商群 G/N の単位元は N ， xN の逆元は $x^{-1}N$ であることを思い出してください．) 逆に， G/N が可換群であれば，任意の元 x, y に対して $xyN = yxN$ より $xyx^{-1}y^{-1} \in N$ ，すなわち $D(G) \subset N$ が示せます．

立て続けに定理を紹介してしまいましたが，証明は簡単だったので大丈夫だと思います．少し混乱してしまった人も，定理を使うときに再び戻って来れば，大丈夫だと思います．次の定理が，ガロア理論で本質的に重要です．実は，あとでこの定理を使いたくて，ここに交換子群の記事を挿んだのでした．

theorem

五次以上の交代群 A_n ($n \geq 5$) では， $D(A_n) = A_n$ となります．

proof

五次以上の対称群 S_n を考えてみます．最低，五次の置換を考えることができるので， i, j, k, l, m の五文字を考えると，常に $(i j k) = (i j m)(i k l)(i j m)^{-1}(i k l)^{-1}$ が成り立ちますので，三次の置換全体は $D(S_n)$ になることが分かります．一方，交代群は偶置換の集まりでしたが，三次以上の偶置換は全て三次の巡回置換の積として表現できるということでしたので (対称群 2 参照)， $D(S_n) \supseteq A_n$ が言えます (*)．また，商群 S_n/A_n は位数 2 なので可換群ですが，先ほど示した定理によって， S_n/A_n が可換群になることは， $D(S_n) \subseteq A_n$ となることと同値です (**)．(*) と (**) より，一般に $D(S_n) = A_n$ が分かります．特に $S_n = A_n$ と置けば， $D(A_n) = A_n$ が示されます．

交換子群の交換子群, つまり $D(D(G))$ を $D^2(G)$ のように書くことがあります. 交換子群は正規部分群になるのですから, $G \supseteq D(G) \supseteq D^2(G) \supseteq \dots$ となるはずで, $D^n(G)$ ($n = 0, 1, 2, \dots$) の並びは, G の正規部分群の組成列 (かその一部) になるはずで, こんな話題があったことも, 頭の片隅に引っ掛けておいて下さい.