方程式を解くということ

方程式を解くという操作は、問題をより小さな次数の方程式に還元することである。
それは、方程式の群を、より小さな部分群に分解するということでもある。
そしてまた、有理数Ｑから拡大してきた代数体の階段を、一段ずつ降りてゆくことでもある。
方程式、群、体は、1つの同じものを、別の側面から見た姿といえる。

Ｎ次方程式の答の入れ替えが作る群は、対称群Ｓnである。
その対称群Ｓnが、次のような仕方で順次部分群に分けられるとき、もとの方程式は解ける。

１．もとの群から、正規部分群が取り出せること。
　(答が全て、体に含まれていること)
２．正規部分群を取り出したときにできる商群が、素数位数の巡回群となっていること。
　(べき根という操作によって解けること)
３．上記 1. 2. で次々と作る部分群の系列が、最後には恒等変換{e}に達すること。
　(最後には完全に解けること)

群Ｇが群Ｈを含むとき、群Ｇは、
　Ｇ = H + HS + HS' + ･･･
と、Ｈの順列に同じ置換を掛けて作られる組へと分解される、また
　Ｇ = H + TH + T'H + ･･･
と、同じ置換にＨの順列を掛けて作られる組へとも分解される。
この２通りの分解は、通常、一致しない。一致するときを固有分解と呼ぶ。

方程式の群が固有分解されない場合には、その方程式をどんなに変換しても、変換された方程式の群は、いつでも同じ個数の順列を持つ。
これに反して、方程式の群がＮ個の順列を持つＭ個の組へと固有分解される場合には、
与えられた方程式を2つの方程式によって解くことができる。
方程式の群が、Ｍ個の順列を持つものと、Ｎ個の順列を持つものとで。

　体：　Ｑ ⊂ L1 ⊂ L2 ⊂ L3 ⊂ Ｑ(α,β,γ,･･･)
　群：　S4 ⊃ A4 ⊃ V4 ⊃ U ⊃ {e}
　式：　既約 F(x) → ･･･ f1(x) f2(x) ･･･ → (x-α)(x-β)(x-γ)(x-δ) 完全に分解

分解不可能な群が持つことのできる順列の個数で最小なものは、素数の場合を除けば
５ x ４ x ３。

５つの文字 i, j, k, l, m の全ての置換Ｓ5の中には、３つの文字の巡回置換 i, j, k が含まれている
実はこの３文字の巡回置換を部分群として取り出せないということから、
Ｓ5 (Ａ5)が分解不可能であることが証明される。

いまφ1 = (i, j, k) という巡回置換を考える。（i→j, j→k, k→i という入れ替えのこと）
φ1 の逆、φ1^-1 = (k, j, i) である。
もう１つ、φ2 = (k, l, m) という巡回置換と、その逆、φ2^-1 = (m, l, k) というものを考える。
そして、２種類の巡回置換を組み合わせた

　　Ｘ = φ1^-1 * φ2^-1 * φ1 * φ2

という連続変換を考える。
実際にやってみると、

　　Ｘ = (k,j,i)(m,l,k)(i,j,k)(k,l,m) = (k,j,m)

となる。

最初のＳ５ に正規部分群Ｈが存在していたとして、その商群を Ｓ5/H としよう。
このとき、上で考えた変換φ1と連続変換Ｘが、どの商群に含まれるのか考えてみる。
剰余類とは、

　　S5 = {a0 * H} + {a1 * H} + {a2 * H} + ・・・

のようにグループ分けすることだった。
変換φ1は、剰余類 {φ1 * H} に含まれている。
この {φ1 * H} を φ1' という記号で書くと、連続変換Ｘは、φ1^-1' * φ2^-1' * φ1' * φ2' という剰余類に含まれることになる。

ところで、方程式を解くためには商群 Ｓ5/H は巡回群でなければならなかった。
巡回群は可換なので(順回転と逆回転の組み合わせだから)、連続変換Ｘの剰余類

　　φ1^-1' * φ2^-1' * φ1' * φ2' は、実は単位元 e の剰余類 e' となる。

ということは、ＸはＨに属していることを意味する。

もともとＸというのは (k,j,m) のことだったのだが、同じことが (k,j,m) 以外の、あらゆる３文字の巡回置換についても言えるから、
結局のところ、全ての３文字の巡回置換はＨに含まれる。
そのように考えてみると、３文字の巡回置換は、もとのＳ5の中から決して取り出せないことに気付く。もし、

　　Ｓ５ ⊃ H1 ⊃ H2 ⊃ H3 ・・・ Hn ⊃ {e}

という部分群への分解列があったなら、３文字の巡回置換は、H1 にも含まれているはず、
次の H2 にも含まれているはず、次の H3 にも・・・
といった具合に、いつまでたっても部分群の中に残り続ける。
つまり、Ｓ5は決して正規部分群に分解されることはない。