体論要約 No.14

今日のテーマ: **ガロア拡大により正規拡大は正規部分群に対応する。ほか**

命題 14.1. 体 L は体 K の有限次ガロア拡大とする。ガロア対応により L と M の間の中間体 M はガロア群 G の部分群 H に対応するとする。このとき

M が K の正規拡大 $\Leftrightarrow$ H は G の正規部分群

この２つの条件のうち一方が成り立つとき、*(必然的に他方も成り立つわけだが)*, $\mathrm{Gal}(M/K) \cong G/H$.

証明. ($\Rightarrow$:) G から $\mathrm{Gal}(M/K)$ への群準同型 φ を

$$\varphi(\sigma) = \sigma|_M$$

で定義する。次のことがわかる。

- $\mathrm{Ker}(\varphi) = \mathrm{Gal}(L/M)$.
- $|G/H| = |G|/|H|$
- $|\,\mathrm{Gal}(M/K)| = [M : K] = [L : K]/[M : K] = |G|/|H|$

よってこのときたしかに $\mathrm{Gal}(M/K) \cong G/H$ が成り立つ.
($\Leftarrow$:) $x \in L^H, g \in G$ とする。$\forall \sigma \in H$ にたいして、

$$\sigma.(g.x) = g(g^{-1}\sigma g).x = g.x$$

よって $g.x \in L^H$.

命題 14.2. K が 1 の原始 n 乗根 ζ_n を含むとする。$L = K(\alpha)$, $\alpha^n \in K$, $\mathrm{char}(L) \nmid n$ ならば、L は K のガロア拡大であり、ガロア群 $\mathrm{Gal}(L/K)$ は可換群である。*(言い方を換えると、L は K のアーベル拡大である。)*

定義 14.1 (参考)**.** 群 G が可解群であるとは、G の部分群の列

$$\{e_G\} = G_0 \subset G_1 \subset G_2 \subset \cdots \subset G_n = G$$

であって、次の条件を満たすようなものが存在するときに言う。

- 各 i について、 G_i は G_{i+1} の正規部分群である。
- 各 i について、 G_{i+1}/G_i はアーベル群である。

命題 14.3. k は 1 のべき根を十分多く含んでいるとする。体 k 上代数的独立な元 $x_1, x_2, \ldots, x_n$ にたいして、$s_1, s_2, \ldots, s_n$ をその基本対称式とする。

$$(X - x_1)(X - x_2)\ldots(X - x_n) = X^n - s_1 X^{n-1} + s_2 X^{n-2} - s_3 X^{n-3} + \cdots + (-1)^n s_n.$$

このとき $L = k(x_1, x_2, \ldots, x_n)$, $K = k(s_1, s_2, \ldots, s_n)$ とおくと、

1. L は K のガロア拡大である。
2. $G = \mathrm{Gal}(L/K) \cong \mathfrak{S}_n$ *(n 次の対称群).*
3. $n \geq 5$ のとき、G は可解群ではない。

このことから、*5* 次以上の一変数代数方程式について、和、差、積、商とべき根だけからなる解の公式は存在しないことがわかる。