

2 次体の不分裂拡大について

東大大理 内田興二

有理数体が不分裂代数拡大を持たないことはよく知られている。2 次体の場合、不分裂アーベル拡大についてはいろいろの結果があるが、アーベルでない不分裂拡大がどのくらいあるかはあまり知られていないように思う。そこで特殊な形の方程式を考えてそれから得られる（交代群とガロア群にもつ）不分裂拡大について調べてみた。ここで不分裂拡大とはすべての有限素点が不分裂を意味し、無限素点は分裂してもかまわないものとする。この研究集会において、以下の結果は山本芳彦氏が既に 1 年以上前に得ており、*Osaka Math. J.* に発表されることを知った。山本氏に御迷惑をおかけたことを深くお詫びします。以下に主な結果と証明の方針を述べますが、山本氏の手法と殆んど同じということです。くれしくはそううを見て下さい。

定理 1. k を代数数体, a, b を k の整数とする。方程式

$$X^n - aX + b = 0$$

のすべての根を添加した体を K とし, この方程式の判別式を D とする。もし $((n-1)a, nb) = 1$ ならば, K は $k(\sqrt{D})$ 上不合岐である。

証明. K の k 上のガロア群を上の方程式の根の置換群と考える。そのとき $k(\sqrt{D})$ に対応する部分群は偶置換全体から成る。 K の任意の prime p に対してその慣性群を調べる。条件 $((n-1)a, nb) = 1$ により $X^n - aX + b$ は $\text{mod } p$ で重根をもつとしても高々一次式一個を 2 重根にもつにすぎない。従って慣性群は 1 以外に高々一個の互換のみを含み, 1 以外の偶置換を含まない。従って p は $k(\sqrt{D})$ 上不合岐である。 p は任意だから K は $k(\sqrt{D})$ 上不合岐である。

定理 2. $n \geq 3$ なる任意の整数 n に対し, A_n を n 次交代群とする。そのとき無限に多くの 2 次体が存在して, それらは A_n をガロア群とする不合岐拡大をもつ。

$k = \mathbb{Q}$ を有理数体として定理 1 の形の既約方程式を考える。 K の $\mathbb{Q}$ 上のガロア群が n 次対称群になるようにすればよい。

$\mathbb{Q}$ 上不分解拡大が存在しないことから、少なくとも一つの prime が分解しその慣性群が互換を含む。ガロア群を計算するために次の補題を用いる。

補題. primitive な有限置換群が互換を含めばそれは対称群である。

既約多項式 $f(X) = X^n - aX + b$ がある素数 p を mod として、 $n-1$ 次と 1 次の既約因子の積に分解できれば、 $f(X) = 0$ のガロア群は primitive になる。そのような a, b をとるには $\ell \equiv 1 \pmod{n-1}$ なる素数 ℓ を一つとって、 $b \equiv 0 \pmod{\ell}$, a は $\text{mod } \ell$ の原始根とすればよい。 a を十分大きくとれば $f(X)$ は既約になる。又、 $((n-1)a, nb) = 1$ を満足するようにとることも可能である。そのような a, b に対して判別式を $D = D(a, b)$ とすると $\mathbb{Q}(\sqrt{D})$ は求める形の不分解拡大をもつ。そのような $\mathbb{Q}(\sqrt{D})$ が無限に多く存在することと... ためには、 $p \nmid n(n-1)$ なる任意の素数 p に対して、 p が D の因数としてちょうど 1 回現われるような a, b のえらびおきができることを示せばよい。これは $a \equiv n \pmod{p}$, $b \equiv n-1 \pmod{p}$ なる a, b を適当にとると、 $D = (-1)^{\frac{n(n-1)}{2}} \{ n^n b^{n-1} - (n-1)^{n-1} a^n \}$ の形から可能である。