数理解析研究所講究録
第 89 巻 1970 年 44-46

2次体の不分岐拡大について

東北大理　内田興二

有理数体が不分岐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，不分岐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岐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（交代群をガロア群にもつ）不分岐拡大について調べてみた。ここで不分岐拡大とはすべての有限素点が不分岐を意味し，無限素点は分岐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，実2次体のイデアル類群に関する結果と共にまもなく Osaka Math. J. に発表されることを知った。山本氏に御迷惑をかけたことを深くおわびします。以下に主な結果と証明の方針を述べますが，山本氏の方法と殆んど同じということですので，くわしくはそちらを見て下さい。

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$k(\sqrt{D})$上不分岐である。

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 $\mathfrak{P}$に対してその惰性群を調べる。条件$((n-1)a, nb) = 1$により$X^n - aX + b$は$\bmod \mathfrak{P}$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。従って惰性群は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$\mathfrak{P}$は$k(\sqrt{D})$上不分岐である。$\mathfrak{P}$は任意だからKは$k(\sqrt{D})$上不分岐である。

定理 2．$n \geqq 3$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分岐拡大をもつ。

$k = Q$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Q上のガロア群がn次対称群になるようにすればよい。

Q上不分岐拡大が存在しないことから，少なくとも一つの prime が分岐しその惰性群が互換を含む。 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 $f(X) = X^n - aX + b$ がある素数を mod として，$n-1$次と1次の既約因子の積に分解されれば，$f(X) = 0$ のガロア群は primitive になる。 そのような a，b をとるには $l \equiv 1 \pmod{n-1}$ なる素数 l を一つとって，$b \equiv 0 \pmod{l}$，a は mod l 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 $Q(\sqrt{D})$ は求める形の不分岐拡大をもつ。 そのような $Q(\sqrt{D})$ が無限に多く存在することをいうためには，$p \nmid n(n-1)$ 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 のえらび方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。