Lemmermeyer's problem on the existence of unramified extensions over quadratic fields

Akito Nomura (Kanazawa University)

Notations (non-abelian group)

A_n : alternating group

$H_8 = \langle x, y \mid x^4 = 1, y^2 = x^2, [x, y] = y^2 \rangle$ quaternion group

$$32\Gamma_5 a_2 = \left\langle x, y, z, w \;\middle|\; \begin{array}{r} w^2 = 1, x^2 = y^2 = z^2 = [y, z] = [x, w], \\ [x, y] = [x, z] = [y, w] = [z, w] = 1 \end{array} \right\rangle$$

$D_{p^3} = \langle x, y \mid x^p = y^{p^2} = 1, [x, y] = y^p \rangle (p : \text{odd})$

§1 Inverse Galois Problem with unramified conditions

不分岐条件を付けたガロアの逆問題は，次のように定式化できる．

Problem k を代数体，G を有限群とする．このとき，不分岐ガロア拡大 M/k でそのガロア群が G と同型なものが存在するか？

注：この講演において，「不分岐」とは「すべての有限素点で不分岐」を意味する．

Remark G がアーベル群のとき，類体論により上記問題は k のイデアル類群の構造と密接な関係がある．

知られている結果をいくつか述べる．

Fact 1 (1992:Bachoc-Kwon[1], Couture-Derhem[3])
$k/\mathbf{Q}$ を 3 次巡回拡大とする．k の類数が偶数ならば不分岐ガロア拡大 M/k でそのガロア群が H_8 と同型なものが存在する．

Fact 2 (2002:Nomura[6])
$k/\mathbf{Q}$ 5 次巡回拡大とする．k の類数が偶数ならば不分岐ガロア拡大 M/k でそのガロア群が $32\Gamma_5 a_2$ と同型なものが存在する．

Fact 3 (1996:Lemmermeyer[5])
$k = \mathbf{Q}(\sqrt{m})$ を 2 次体とする.
m がある条件を満たすとき, 不分岐ガロア拡大 M/k で
(1) $G(M/k) \cong H_8$ (2) $M/\mathbf{Q}$: Galois
となるものが存在する.

注 : m の条件については省略する. 詳しくはレジメあるいは [5] を参照して下さい.
例えば, $m = -3 * 17 * 29,\ 5 * 13 * 37$ は条件を満たす.

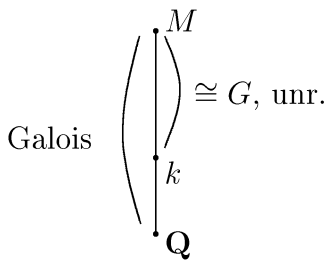
これらの 3 つの Fact では, 基礎体 k は固定されている. 次に基礎体が固定されていない Fact について述べる.

Fact 4 (1962:Fröhlich[4])
任意の有限群 G に対して, 代数体 k とその不分岐ガロア拡大 M/k でガロア群が G と同型なものが存在する.

Fact 5 (1970:Yamamoto[8], Uchida[7])
任意の自然数 n に対して, 2 次体 k とその不分岐ガロア拡大 M/k でガロア群が A_n と同型なものが存在する.

§2 Lemmermeyer's problem and counter examples

Problem (Lemmermeyer)
G を有限 2 群とする. このとき, 2 次体 k とその不分岐拡大 M/k で条件
(1) $G(M/k) \cong G$, (2) $M/\mathbf{Q}$: Galois
を満たすものが存在するか?



Remark Fact 3 より, $G = H_8$ の場合は Problem の答は肯定的である.

Remark Lemmermeyer の問題は, 2 次体の Hilbert 2-類体塔と密接にか関係している. M を 2 次体 k の Hilbert 2-類体塔の layer とすると条件
M/k : 不分岐, $M/\mathbf{Q}$: Galois
を満たす.

次に，この問題を考えるときに Key となる補題を述べる．

Lemma (Cebotarev monodromy theorem)
p を素数とし，ガロア拡大 $M/k/\mathbf{Q}$ は次の条件を満たすとする．
(1) k は p 次巡回体
(2) M/k は不分岐拡大
(3) $M/\mathbf{Q}$ はガロア拡大
このとき，ガロア群 $G(M/\mathbf{Q})$ は $M/\mathbf{Q}$ における惰性群で生成される．従って $G(M/\mathbf{Q})$ は位数 p の元で生成される．

(証明) 背理法で示す．惰性群で生成される群を I とし，$G(M/\mathbf{Q}) \supsetneq I$ と仮定する．F を I の固定体とすると
$F \supsetneq \mathbf{Q}$, $F/\mathbf{Q}$: 不分岐.
一方，$\mathbf{Q}$ は不分岐拡大を持たない．これは矛盾.

Lemmermeyer は自分のホームページ
http://www.rzuser.uni-heidelberg.de/ hb3/unsol.ps
の中で次の予想を提出した.

Conjecture (Lemmermeyer)
任意の 2 群 G に対して，2 群 H で条件
(1) H は G を部分群として含み，$(H : G) = 2$
(2) H は位数 2 の元で生成される
を満たすものが存在する.

Conjecture に対する反例
$G_1 = \langle x^{16} = y^4 = 1, [y, x] = x^4 \rangle$
$G_2 = \langle x^{16} = y^4 = 1, [y, x] = x^{-2} \rangle$
この反例は，Boston,Leedham-Green [2] によって MAGMA を用いて得られた.

ここでは，GAP を用いて反例の再構成を行う.

MAGMA と GAP
• 共通点
位数 128 の群の表や群の計算に便利な関数を装備している.
• 違う点
MAGMA は有料であるが，GAP は無料である.

MAGMA と GAP に関する精細は次のホームページを参照して下さい.
MAGMA (http://magma.maths.usyd.edu.au/magma/)
GAP(http://www-history.mcs.st-and.ac.uk/~gap/)

反例構成アルゴリズムの流れ (by using GAP)

1)　位数 64 の群をリストアップする．（ 267 個ある）

2)　位数 128 の群をリストアップする．（ 2328 個ある）

3)　2) で求めた群の中で位数 2 の元で生成されるものをリストアップする．（ 359 個ある）

(この部分のプログラムは 木田雅成氏に教えていただきました)

4)　3) で求めた各群の極大部分群を求める．（ 同型を除いて 265 個ある）

5)　位数 64 の群の中で反例は 2 個

次に Lemmermeyer の問題を奇素数 p に対して考える．

Question　p を奇素数とし，G を有限 p 群とする．このとき，p 次巡回体 k とその不分岐拡大 M/k で条件

(1) $G(M/k) \cong G$,　(2) $M/\mathbf{Q}$: Galois

を満たすものが存在するか？

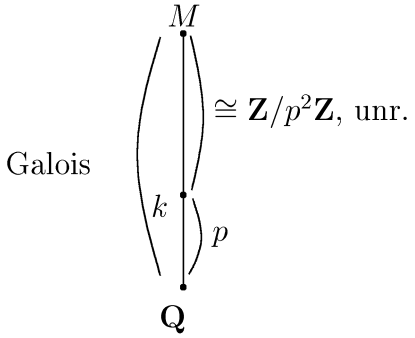
この Question は $p = 2$ の場合より易しく答は否定的である．

Question の反例

$G = \mathbf{Z}/p^2\mathbf{Z}$

(証明)

背理法で示す．$G = \mathbf{Z}/p^2\mathbf{Z}$ に対応する k, M が存在するとする．



$G(M/\mathbf{Q})$ は $\mathbf{Z}/p^2\mathbf{Z}$ を部分群として持つ位数 p^3 の群なので,

$G(M/\mathbf{Q}) = \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p^2\mathbf{Z}$ or D_{p^3}(dihedral).

これらの群は位数 p の群で生成されない．これは Lemma(Cebotarev monodromy theorem) に反する．

最後に，いろいろ助言をいただいた木田雅成氏と山村健氏に感謝します．

参考文献

[1] C. Bachoc and S. H. Kwon, Sur les extensions de group de Galois $\widetilde{A}_4$, Acta Arith. **62** (1992), 1–10.

[2] N. Boston and C. Leedeham-Green, Counterexamples to a conjecture of Lemmermeyer, Arch. Math. **72** (1999), 177–179.

[3] R. Couture and A. Derhem, Un problème de capitulation, C. R. Acad. Sci. Paris **314** (1992), 785–788.

[4] A. Fröhlich, On non-ramified extensions with prescribed Galois group, Mathematika **9** (1962), 133–134.

[5] F. Lemmermeyer, Unramified quaternion extensions of quadratic number fields, J. Théor. Nombres Bordeaux **9**(1997), 51–68.

[6] A. Nomura, Notes on the existence of certain unramified 2-extensions (to appear in Illinoi J. of Math.)

[7] K. Uchida, Unramified extensions of quadratic number fields II, Tôhoku Math. J. **22**(1970), 220–224.

[8] Y. Yamamoto, On unramified Galois extensions of quadratic number fields , Osaka J. Math. **7**(1970), 57–76.