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

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

order = 32 rank = 4

$G_1 = \langle x, y \mid x^{16} = y^4 = 1, [y, x] = x^4 \rangle$

$G_2 = \langle x, y \mid x^{16} = y^4 = 1, [y, x] = x^{-2} \rangle$

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

§1 Inverse Galois Problem with unramified conditions

Problem

Let k be an algebraic number field, and G a finite group. Does there exist an unramified Galois extension M/k such that $G(M/k) \cong G$?

(In this talk, "unramified" means that "unramified at all finite primes".)

Fact 1 (1992:Bachoc-Kwon, Couture-Derhem)

Let $k/\mathbf{Q}$ be a cyclic extension of degree 3. If the class number h_k is even, then there exists an unramified Galois extension M/k such that $G(M/k)$ is isomorphic to the quaternion group H_8.

Fact 2 (2002:Nomura)

Let $k/\mathbf{Q}$ be a cyclic extension of degree 5. If the class number h_k is even, then there exists an unramified Galois extension M/k such that $G(M/k)$ is isomorphic to the group $32\Gamma_5 a_2$.

Fact 3 (1996:Lemmermeyer)

Let k be a quadratic field with discriminant d. Assume that there is a factorization $d = d_1 d_2 d_3$ of d into three discriminants which are relatively prime and which satisfy the conditions $(d_1 d_2/p_3) = (d_2 d_3/p_1) = (d_3 d_1/p_2) = 1$ for all $p_i | d_i$. Then there exists an unramified H_8-extension M/k such that $M/\mathbf{Q}$ is Galois.

Fact 4 (1962 : Fröhlich)
For any finite group G, there exists infinitely many field k and an unramified Galois extension M/k such that $G(M/k)$ is isomorphic to G.

Fact 5 (1970 : Yamamoto, Uchida)
For any positive integer n, there exists infinitely many quadratic field k and an unramified Galois extension M/k such that $G(M/k)$ is isomorphic to A_n.

§2 Lemmermeyer's problem and counter example

Problem(Lemmermeyer)
For any finite 2-group G, does there exist a quadratic field k and an unramified Galois extension M/k such that $G(M/k)$ is isomorphic to G and that M is Galois over $\mathbf{Q}$?

Conjecture(Lemmermeyer)
For any 2-group G, G can embed as a subgroup of index 2 in a group generated by elements of order 2.

Remark
Problem(Lemmermeyer) $\Longrightarrow$ Conjecture(Lemmermeyer)

Counter examples of Conjecture (Boston,Leedham-Green)

$G_1 = \langle x^{16} = y^4 = 1, [y, x] = x^4 \rangle$
$G_2 = \langle x^{16} = y^4 = 1, [y, x] = x^{-2} \rangle$

Algorithm flow(by using GAP)
1) Pick up all groups of order 64.
(There are 267 groups.)
2) Pick up all groups of order 128.
(There are 2328 groups.)
3) Pick up all groups in 2) which is generated by elements of order 2.
(There are 359 groups.)
4) Calculate maximal subgroups of groups in 3).
(There are 265 kinds of groups.)
5) There are two counter examples.