

EMBEDDING 2-GROUPS IN GROUPS GENERATED BY INVOLUTIONS

NIGEL BOSTON

Department of Mathematics, University of Wisconsin, Madison, WI 53706

I. INTRODUCTION

This paper addresses a group theory problem that arises from number theory. Namely, given a quadratic field K and an unramified extension L/K which is Galois over \mathbf{Q} , does the structure of $\text{Gal}(L/K)$ determine that of $\text{Gal}(L/\mathbf{Q})$? Since \mathbf{Q} has no nontrivial unramified extensions, $\text{Gal}(L/\mathbf{Q})$ is generated by its inertia subgroups. Since L/K is unramified, these inertia subgroups have order 1 or 2.

In group-theoretical terms, given a finite or profinite group H , we want to classify those groups G that contain H as a subgroup of index 2 and that are generated by the involutions in G outside H . My paper with Leedham-Green [3] showed that, contrary to a conjecture of Lemmermeyer, there exist infinite families of finite 2-groups H for which no such G exists. Here we extend this result to show that for 2-generated H , if such a G exists, then it is unique.

Definition. Let H be a (finite or profinite) group. A *GI-extension* of H is a group G into which H embeds with index 2 such that G is generated by the involutions in G outside H .

For example, if H is abelian, then $\text{Dih}(H)$, the semidirect product of H by the automorphism of order 2 that inverts every element of H , is a GI-extension of H . Some groups have no GI-extensions. The smallest examples are the Frobenius groups of order 20 and 21. [3] gives many more, in the case of 2-groups. Some groups have more than one GI-extension (up to isomorphism). The smallest such are three of the four groups of order 16 that have exactly 3 generators. Investigations with the computer algebra system MAGMA on groups of order ≤ 128 led to the conjecture that 2-generated 2-groups always have at most one GI-extension, which is proven in this paper.

Theorem 1. Let H be a finite 2-group or pro-2 group that is 2-generated. Then H has at most one GI-extension up to isomorphism.

The main consequence of this is then as follows.

The author thanks Elliot Benjamin for raising the number-theoretical question that led to these investigations.

Theorem 2. Let K be a quadratic field and L/K an unramified 2-extension, Galois over \mathbf{Q} , with $\text{Gal}(L/K)$ 2-generated. Then the structure of $\text{Gal}(L/K)$ determines that of $\text{Gal}(L/\mathbf{Q})$.

We make some further observations regarding this in the last section of the paper.

2. PRELIMINARIES.

Let H be a (finite or profinite) group and G a GI-extension of it. Then H is normal in G (since its index is 2) and G splits over H since it is generated by the involutions outside H . Thus G is a semidirect product of H by some $\sigma \in \text{Aut}(H)$ of order 2.

Let I be the set of involutions in G outside H . Then $I = \{h\sigma|h \in H, h^\sigma = h^{-1}\}$ since $(h\sigma)^2 = 1$ if and only if $h^\sigma = h^{-1}$. Given a group H and an automorphism σ of H , we therefore investigate $X_\sigma := \{h \in H|h^\sigma = h^{-1}\}$. Let H be a (pro)-2-group.

Lemma 1. If H is not elementary 2-abelian and $\sigma \in \text{Aut}(H)$ of order 2, then $H \rtimes \langle \sigma \rangle$ is a GI-extension of H if and only if X_σ generates H . We then call σ a GI-automorphism of H .

This explains the terminology GI (i.e. generator-inverting)-extension. Lemma 1 follows easily by comparing maximal subgroups of H and G . The next lemma gives a criterion for when two extensions $H \rtimes \langle \sigma \rangle$ and $H \rtimes \langle \tau \rangle$ are isomorphic.

Lemma 2. ([5],p.4) Suppose that σ and τ have conjugate images in $\text{Out}(H)$. Then $H \rtimes \langle \sigma \rangle$ and $H \rtimes \langle \tau \rangle$ are isomorphic.

The reason why the condition of being 2-generated is sufficient for uniqueness in Theorem 1 comes from the following result. Note that if H is any group, then since inner automorphisms act trivially on the abelianization H/H' , the map $\text{Aut}(H) \rightarrow \text{Aut}(H/H')$ yields a homomorphism $\pi_H : \text{Out}(H) \rightarrow \text{Aut}(H/H')$.

Lemma 3. Let F be the free pro-2 group on 2 generators. Then π_F is an isomorphism.

This result was first proven by Nielsen (Prop. 4.5, [6]) in the case of a discrete free group of rank two. For our purposes below we could also use [4], where Herfort, Ribes, and Zaleskii find the four conjugacy classes of elements of order 2 in $\text{Aut}(F)$.

3. PROOF OF THE MAIN THEOREM.

First we prove Theorem 1 in the case when H is the free pro-2 group on 2 generators. Suppose H has two GI-automorphisms σ and τ . By Lemma 1 H is generated by say a, b such that $a^\sigma = a^{-1}$ and $b^\sigma = b^{-1}$. This implies that the image of σ in $\text{Aut}(H/H')$ is the automorphism of H/H' that inverts every element. The same is true of the image of τ . By Lemma 3, σ and τ have the same image in

$\text{Out}(H)$ and so by Lemma 2 the corresponding GI-extensions are isomorphic.

Now suppose that H is any 2-generated finite 2-group or pro-2 group and that H has two GI-automorphisms σ and τ . As above, H has generators a and b inverted by σ . Let F be the free pro-2 group on x and y and define a surjection from F to H by mapping x to a and y to b . This becomes an operator homomorphism if we have σ act on F by inverting x and y . By the projective property of F , any automorphism of H lifts to an automorphism of F . By the first paragraph of this section, σ and τ lifted to automorphisms of F differ by an inner automorphism of F . Since under $\text{Aut}(F) \rightarrow \text{Aut}(H)$ the inner automorphisms of F map to those of H , σ and τ differ by an inner automorphism of H . By Lemma 2, the corresponding GI-extensions are isomorphic.

4. RELATED WORK.

The question remains as to whether for K quadratic and general 2-extensions L/K the structure of $\text{Gal}(L/K)$ determines that of $\text{Gal}(L/\mathbf{Q})$. In [1], Benjamin, Lemmermeyer, and Snyder consider various L/K with L the maximal unramified 2-extension of K and $\text{Gal}(L/K)$ a 2-group with exactly 3 generators. For example, they look at fields with $\text{Gal}(L/K) = 32.041$, which is the Hall-Senior notation for the group the MAGMA database denotes by $\langle 32, 33 \rangle$. These are the fields $\mathbf{Q}(\sqrt{d})$ whose discriminant d factors as $d_1 d_2 d_3 d_4$ where $d \not\equiv 4 \pmod{8}$, $d_i < 0$ for $i = 1, 2, 3$, $d_4 > 0$, and $(d_i/p_4) = -1$ for $i = 1, 2, 3$ and $(d_1/p_2) = (d_2/p_3) = (d_3/p_1) = -1$. For instance, $d = -2415, -3927, -11235, \dots$ yield this Galois group.

The group 32.041 has two GI-extensions, namely $\langle 64, 219 \rangle$ and $\langle 64, 241 \rangle$ in the database, but one finds computationally that $\text{Gal}(L/\mathbf{Q})$ is always isomorphic to $\langle 64, 241 \rangle$. This is established theoretically by showing that if

$$m = (a\sqrt{x} + b\sqrt{z})(c\sqrt{y} + d\sqrt{z})(e + f\sqrt{xy})$$

for some $a, b, c, d, e, f, x, y, z \in \mathbf{Q}$, then generically the splitting field of $\mathbf{Q}(\sqrt{m})$ over \mathbf{Q} has Galois group $\langle 32, 49 \rangle$. (It can collapse to a smaller group for some special choices of a, \dots, z .) By [1], these are the Galois groups over \mathbf{Q} of the subextensions of L of degree 32. Since not all quotients of $\langle 64, 219 \rangle$ of order 32 are isomorphic to $\langle 32, 49 \rangle$, we deduce the following theorem (cf. Theorem 2).

Theorem 3. Suppose K is an imaginary quadratic field and L/K an unramified 2-extension, Galois over \mathbf{Q} , with $\text{Gal}(L/K)$ isomorphic to the 3-generated group 32.041 (i.e. $\langle 32, 33 \rangle$). Then $\text{Gal}(L/\mathbf{Q})$ is always isomorphic to $\langle 64, 241 \rangle$.

Elliot Benjamin and I are planning an investigation of how general this phenomenon of $\text{Gal}(L/K)$ determining $\text{Gal}(L/\mathbf{Q})$ is.

In a preprint with Michael Bush [2], we conjecture that given a (pro-)2-group H the proportion of imaginary quadratic fields of discriminant $\geq -x$ that have maximal unramified 2-extension with Galois group H is asymptotic to

$$c(H) \frac{x(\log \log x)^{D(H)}}{\log x}$$

where the constants $c(H)$ and $D(H)$ depend only on H , and $D(H) \leq d(H)$, the minimal number of generators of H . The groups of [3] must have $c(H) = 0$.

REFERENCES.

1. E. Benjamin, F. Lemmermeyer, and C. Snyder, Imaginary quadratic fields with $Cl_2(k) = (2, 2, 2)$, *J. Number Theory* vol. 103, no. 1, (2003), 38–70.
2. N.Boston and M.Bush, The distribution of Galois groups of p-class towers of imaginary quadratic fields, preprint.
3. N.Boston and C.R.Leecham-Green, Counterexamples to a conjecture of Lemmermeyer, *Arch. Math. (Basel)* vol. 72, no. 3, (1999), 177–179.
4. W.N.Herfort, L.Ribes, and P. Zaleskii, Finite extensions of free pro-p groups of rank at most two, *Israel J. Math.* vol. 107 (1998), 195–207.
5. J.A.Hillman, *Four-manifolds, geometries and knots*, Geometry & Topology Monographs, vol. 5 (2002).
6. R.Lyndon and P.Schupp, *Combinatorial group theory*, Springer-Verlag, Berlin-New York, 1977.