Vol. 62, No. 1, January 1980
Printed in Belgium

(24)

Normal Automorphisms of Free Profinite Groups

MOSHE JARDEN*

Tel-Aviv University, Tel-Aviv, Israel

Communicated by A. Fröhlich

Received January 20, 1979

INTRODUCTION

Kenkichi Iwasawa and Kaji Uchida proved independently in [6, 11] the following remarkable theorem.

THEOREM. *Let H and J be two open subgroups of the absolute Galois group, $G(\mathbb{Q})$, of the field of rational numbers $\mathbb{Q}$. Suppose that $\sigma: H \to J$ is a (topological) isomorphism. Then σ is induced by an inner automorphism of $G(\mathbb{Q})$; i.e., there exists a $g \in G(\mathbb{Q})$ such that $x^\sigma = x^g$ for every $x \in G(\mathbb{Q})$.*

The main purpose of this note is to prove an analogous result for non-Abelian free profinite groups. Here the notion of a free profinite group is used in the sense defined, e.g., by Ribes [9, p. 60]; in particular such a group has a free system of generators that converges to 1. Let H and J be open subgroups of a profinite group G. An isomorphism $\sigma: H \to J$ is said to be *normal in G* if $N^\sigma = N$ for every open normal subgroup N of G which is contained in $H \cap J$. If $G = G(\mathbb{Q})$, then a celebrated theorem of Neukirch [8], on which the above theorem of Iwasawa and Uchida is based, ensures that every such an isomorphism is normal. This is certainly no longer the case for free profinite groups. We therefore have to assume normality in order to obtain our

MAIN THEOREM. *Let H and J be two open subgroups of a non-Abelian free profinite group F. Suppose that $\sigma: H \to J$ is a normal isomorphism in F. Then σ is induced by an inner automorphism of F.*

We prove the theorem first for $\hat{F}_e$, the free profinite group on $e \geqslant 2$ generators. This is done in two steps: First we prove that σ is pointwise inner in $\hat{F}_e$; then we show that σ is inner in $\hat{F}_e$. In Section 3 we deduce the theorem for an arbitrary F.

* Partially supported by a DAAD grant.

1. An Application of Representation Theory

Let $\sigma: H \to J$ be an isomorphism of open subgroups of a profinite group G. Then σ is said to be *pointwise inner in* G, if for every $h \in H$ there exists an $x \in G$, such that $h = h^x$. Ikeda applied Representation Theory in [5] in order to deduce from the Neukirch theorem that every automorphism of $G(\mathbb{Q})$ is pointwise inner. The application of Ikeda's argument in our case is made possible by

Lemma 1.1. *Let p be a prime number and let Γ be a finite group of order relatively prime to p. Let A be a simple $\mathbb{F}_p[\Gamma]$-module (written multiplicatively). Denote by $E = \Gamma \cdot A$ the corresponding semidirect product. If Γ is not cyclic, then every system of generators of Γ can be lifted to a system of generators of E.*

Proof (Thompson). Let $x_1, \ldots, x_e$ be a system of generators of Γ. For every system $(a) = (a_1, \ldots, a_e) \in A^e$ let Γ_a be the subgroup of E generated by $x_1a_1, \ldots, x_ea_e$. Then Γ_a is mapped onto Γ under the canonical homomorphism $h: E \to E/A = \Gamma$. Hence, $\Gamma_a \cap A$, which is the kernel of $h \mid \Gamma_a$, is left invariant under the action of Γ. It follows that $\Gamma_a \cap A = 1$ or $\Gamma_a \cap A = A$, since A is a simple $\mathbb{F}_p[\Gamma]$-module. If there exists an $(a) \in A^e$ such that $\Gamma_a \cap A = A$, then Γ_a is equal to E, which is therefore generated by $x_1a_1, \ldots, x_ea_e$.

Assume therefore that $\Gamma_a \cap A = 1$, i.e., that Γ_a is a complement of A for every $(a) \in A^e$. If $(a) \neq (b)$, then $\Gamma_a \neq \Gamma_b$, since otherwise we would have $a^{-1}b_i \in \Gamma_a \cap A = 1$ for $i = 1, \ldots, e$, which is a contradiction. It follows that A has at least $|A|^e$ complements in E. On the other hand, it is known that all the complements of A are conjugate to one, say to Γ, since $|A|$ and $|\Gamma|$ are relatively prime (cf. Huppert [3, p. 120]). It follows that the number of conjugates of Γ are at most $(E : \Gamma) = |A|$. The desired contradiction follows now from the fact that $e > 1$. ∎

Lemma 1.2. *Let $e \geqslant 2$ and let $\sigma: H \to J$ be a normal isomorphism of two open subgroups H and J of $\hat{F}_e$. Then σ is pointwise inner in $\hat{F}_e$.*

Proof. Let N be an open normal subgroup of $\hat{F}_e$ which is contained in $H \cap J$ and let $\Gamma = \hat{F}_e/N$. Let χ be an irreducible character of Γ and let K be a number field over which χ is defined (cf. Serre [10, p. 106]). This means that there exists a representation $\rho: \Gamma \to GL(n, K)$ such that $\operatorname{Tr} \rho(x) = \chi(x)$ for every $x \in \Gamma$. Denote by S the set of all primes p that split completely in K and that do not divide the order of Γ, and such that if $\mathfrak{p}$ is a prime of K lying over P, then $\rho(x)$ is $\mathfrak{p}$-integral for every $x \in \Gamma$. By Čebotarev density theorem, S is an infinite set.

Let $p \in S$ and let $\mathfrak{p}$ be a prime of K lying over p. Then reducing module $\mathfrak{p}$ we obtain a representation $\tilde{\rho}: \Gamma \to GL(n, \mathbb{F}_p)$, which is also irreducible (cf. [10, p. 140]; note that ρ is also defined over $\mathbb{Q}_p$). Let A be the corresponding simple $\mathbb{F}_p[\Gamma]$-module. Let $z_1, \ldots, z_e$ be generators of $\hat{F}_e$ and let $x_1, \ldots, x_e$ be the corre-

sponding generators of Γ under the canonical map $\hat{F}_e \to \Gamma$. By Lemma 1.1, $x_1, \ldots, x_e$ can be lifted to a system of generators of the semidirect product $E = \Gamma \cdot A$. Hence $\hat{F}_e$ has an open normal subgroup M which is contained in N such that $\hat{F}_e/M \cong E$, $N/M \cong A$, and the canonical action of Γ on A corresponds to the one given by $\bar{\rho}$. The given isomorphism σ leaves M and N invariant; hence it induces isomorphisms $H/N \to J/N$, $H/M \to J/M$, and $A \to A$, which are also denoted by σ. Thus $(a^x)^\sigma = a^{\sigma \cdot x^\sigma}$ for every $a \in A$ every $x \in H/M$. This, written as $a^x = a^{\sigma \cdot x^\sigma \cdot \sigma^{-1}}$, implies that x and x^σ are conjugate as A-operators; hence

$$\chi(x) \equiv \chi(x^\sigma) \bmod \mathfrak{p}, \qquad \text{for all} \quad x \in H/N.$$

This congruence holds now for infinitely many primes $\mathfrak{p}$ of K. Hence $\chi(x) = \chi(x^\sigma)$. This equation holds for every irreducible character χ of Γ. Hence x is conjugate to x^σ in Γ (cf. [10, p. 32]).

Letting N run over a cofinite system of open normal subgroups of $\hat{F}_e$ and using compact arguments, we obtain that every $x \in H$ is conjugate in $\hat{F}_e$ to x^σ. ∎

2. An Argument of Iwasawa

Ikeda used in [4] an argument of Iwasawa in order to prove that every pointwise inner isomorphism of two subgroups H and J of $G(\mathbb{Q}_p)$ is inner in $G(\mathbb{Q}_p)$. We modify the argument in order to obtain the analogous result for $\hat{F}e$. We start with two lemmas that replace the local class field theory in Ikeda's work.

Lemma 2.1. *Let B be the free $\hat{\mathbb{Z}}$-module of rank f. Then every open subgroup A of B is also a free $\hat{\mathbb{Z}}$-module of rank f.*

Proof. Denote by B_0 the free $\mathbb{Z}$-module of rank f. This module has only finitely many subgroups of a given index m and the intersection of all subgroups of B_0 of finite indices is trivial. It follows that $B = \hat{B}$ is the profinite completion of B_0. Moreover, denote, for every subgroup A_0 of B_0 of a finite index, the closure of A_0 by $\hat{A}_0$. Then the map $A_0 \to \hat{A}_0$ is a bijection onto the set of all open subgroups of B (compare also the proof of Lemma 2 in [7]). By the fundamental theorem of Abelian groups every A_0 is a free $\mathbb{Z}$-modle of rank f. Hence. $A = \hat{A}_0$ is a free $\hat{\mathbb{Z}}$-module of rank f. ∎

Lemma 2.2. *Let $e \geqslant 2$, and let N be an open normal subgroup of $\hat{F}_e$ with commutator subgroup N'. Then the canonical action of $\Gamma = \hat{F}_e/N$ on $A = N/N'$ is faithful, in other words, N/N' is self-centralizer in $\hat{F}_e/N'$.*

Proof. The group N is isomorphic to $\hat{F}_F$, where $f = 1 + n(e - 1)$ and $n = (\hat{F}_e : N)$ (cf. [7, p. 283]). The group A, as the maximal Abelian quotient of

N, is therefore a free $\hat{\mathbb{Z}}$-module of rank f. Let x be an element of $\hat{F}_e$ that commutes with every element of N modulo N' and let $M = \langle N, x\rangle$. Then M/N' is Abelian; hence $M' \leqslant N'$. But N/M', as a subgroup of M/M', is also Abelian; hence $M' = N'$. It follows that A is an open subgroup of $B = M/M'$. Moreover, B is also a free $\hat{\mathbb{Z}}$-module of rank $1 + m(e-1)$, where $m = [\hat{F}_e : M]$. By Lemma 2.1, $1 + m(e-1) = 1 + n(e-1)$; hence $m = n$, since $e \geqslant 2$, therefore $M = N$ and $x \in N$. ∎

LEMMA 2.3. *Let $\sigma: H \to J$ be a pointwise inner isomorphism of two open subgroups of $\hat{F}_e$. Then σ is inner in $\hat{F}_e$.*

Proof. If $e = 1$, then $H = J$ and σ is the identity automorphism. The Lemma is therefore trivially true. Suppose that $e \geqslant 2$ and consider an open normal subgroup N of $\hat{F}_e$ which is contained in $H \cap J$. As in the proof of Lemma 1.2, it suffices to prove that σ is inner in $\hat{F}_e$ modulo N.

Indeed, let $\Gamma = \hat{F}_e/N$ and $A = N/N'$ be as in Lemma 2.2. For every $x \in \Gamma$ let $A^{(x)} = \{a \in A \mid a^\sigma = a^x\}$. Then $A^{(x)}$ is a closed subgroup of A, and the finite union of all these groups covers A. It follows that there exists an $x \in \Gamma$ such that $A^{(x)}$ is open in A.[1] For this x, let $B = (A : A^{(x)})$. Then $(a^\sigma)^k = (a^x)^k$; hence $a^\sigma = a^x$ for every $a \in A$, since A is torsion free.

Now let $y \in H/N$ and let g be a lifting of y to an element of H/N'. Then $g^{-1}ag \in A$ for every $a \in A$ and hence

$$(g^{-1}ag)^\sigma = (g^\sigma)^{-1}a^\sigma g^\sigma = (g^\sigma)^{-1}a^x g^\sigma,$$
$$(g^{-1}ag)^\sigma = (g^{-1}ag)^x = (g^x)^{-1}a^x g^x.$$

It follows that $(a^x)^{g^\sigma g^{-x}} = a^x$ for every $a \in A$. But when a runs over the elements of A, so does a^x. It follows from Lemma 2.2 that $y^\sigma = y^x$. ∎

3. PROOF OF THE MAIN THEOREM

Let F be a free profinite group on a set X that contains at least two elements and let $\sigma: H \to J$ be a normal isomorphism of two open subgroups of F. Again, it suffices to consider an open normal subgroup N of F which is contained in $H \cap J$ and to prove that σ is induced by an inner automorphism module N.

Indeed, the set X is assumed to converge to 1. This means in particular that one can represent X as a disjoint union $X = Y \cup Z$, where Y is a finite set of, say, $e \geqslant 2$ elements and Z is contained in N. Let M be the smallest closed subgroup of F that contains Z. Then $M \leqslant N$ and $F/M \cong \hat{F}_e$ (cf. [9, p. 66]). Our

[1] This is a weak form of the lemma of Iwasawa. A quick proof of it can be given using the Haar measure of A: If none of the $A^{(x)}$ were open, then all of them would have measure zero; hence A would be of measure zero too, which is a contradiction.

σ induces an isomorphism of H/M onto J/M which is normal in F/M. By Lemmas 1.2 and 2.3 it is inner in F/M. In particular σ is induced modulo N by an inner automorphism. ∎

4. Applications

A straightforward corollary of the Main Theorem is the following one:

Corollary 4.1. *Let H and J be two open subgroups of a non-Abelian free profinite group F. If there exists an isomorphism $\sigma: H \to J$, normal in F, then $(F : H) = (F : J)$.*

Remark. The Main Theorem, as well as its proof remains valid for free prosolvable groups. The method of the proof, however, does not work for free pro-p-groups. We shall therefore take another course of proof and prove our results for pro-p-groups in a subsequent paper.

Let H be an open subgroup of a non-Abelian free profinite group F. Then H is also a non-Abelian free profinite group (cf. [2, p. 108]). Hence H has a trivial center (cf. [7, p. 306] or [1, p. 235]). It follows that the intersection of H with its centralizer C in F is 1. Hence C is a finite group. But F is torsion free (cf. [7, p. 306] for the finite rank case, from which the infiite rank case also follows). Hence $C = 1$. It follows that the normalizer $N_F(H)$, of H in F can be considered as a subgroup of the group $\mathrm{Aut}_{F,n}(H)$, of all normal automorphisms of H in F. The Main Theorem implies that:

Corollary 4.2. $\mathrm{Aut}_{F,n}(H) = N_F(H)$.

In particular if we denote by $\mathrm{Aut}_n(F)$ the group of all normal automorphisms of F, then we have

Corollary 4.3. $\mathrm{Aut}_n F = F$.

Remark. This result is, in a sense, the best possible. Indeed if F is Abelian, then necessarily $F = \hat{\mathbb{Z}}$, and every automorphism of $\hat{\mathbb{Z}}$ is normal, although none, except the identity, is inner. On the other hand, if X is a free system of generators of F that converges to 1, then every permutation π of X can be extended to an automorphism of F, which is certainly not inner, if π is not the identity.

Acknowledgments

The author is indebted to Jürgen Ritter and to Albrecht Brandis for valuable suggestions that lead to a better presentation of the paper. The author is also indebted to Wulf-Dieter Geyer for informing him about Thompson's proof of Lemma 1.1.

References

1. M. P. Anderson, Exactness properties of profinite completion functors, *Topology* **13** (1974), 229–239.
2. E. Binz, J. Neukirch, and G. H. Wenzel, A subgroup theory for free products of profinite groups, *J. Algebra* **19** (1971), 104–108.
3. B. Huppert, "Endliche Gruppen I," Springer, Berlin/Heidelberg/New York, 1967.
4. M. Ikeda, On automorphisms of Galois groups, manuscript.
5. M. Ikeda, On the group of automorphisms of the absolute Galois group of the rational number field, *Arch. Math. (Basel)* **26** (1975), 250–252.
6. K. Iwasawa, Automorphisms of Galois groups of number fields, manuscript.
7. M. Jarden, Algebraic extensions of finite corank of Hilbertion fields, *Israel J. Math.* **18** (1974), 279–307.
8. J. Neukirch, Kennzeichnung der p-adischen und der endlichen Zahlkörpers, *Invet. Math.* **6** (1969), 296–314.
9. L. Ribes, "Introduction to Profinite groups and Galois cohology," Queen's Papers in Mathematics. No. 24, Queen's University, Kingston, 1970.
10. J.-P. Serre, "Représentation linéaire des groupes finis," Hermann, Paris, 1971.
11. K. Uchida, Isomorphisms of Galois groups, *J. Math. Soc. Japan* **28** (1976), 617–620.