March 1980

NORMAL AUTOMORPHISMS OF ABSOLUTE GALOIS GROUPS OF $\mathfrak{p}$-ADIC FIELDS

MOSHE JARDEN AND JÜRGEN RITTER

Introduction. A (topological) automorphism σ of a profinite group G is said to be *normal* if $N^\sigma = N$ for every normal closed subgroup N of G; it is said to be *families preserving* if for all $g \in G$, the closed subgroup $\langle g^\sigma \rangle$ generated by g^σ is conjugate in G to $\langle g \rangle$. Finally σ is called *point-wise inner* if g^σ is conjugate to g for every $g \in G$.

The groups of all normal automorphisms, families preserving automorphisms, point-wise inner automorphisms and inner automorphisms of G are denoted by $\mathrm{Aut}_n(G)$, $\mathrm{Aut}_f(G)$, $\mathrm{Aut}_c(G)$ and $\mathrm{Aut}_i(G)$, respectively. Clearly $\mathrm{Aut}_i(G) \leqslant \mathrm{Aut}_c(G) \leqslant \mathrm{Aut}_f(G) \leqslant \mathrm{Aut}_n(G)$.

Neukirch proved in [17] that every automorphism of the absolute Galois group, $G(\mathbf{Q})$, of $\mathbf{Q}$ is normal. Applying Representation Theory of finite groups and a theorem of Scholz [19], Ikeda continued this result and proved in [7] that $\mathrm{Aut}_n(G(\mathbf{Q})) = \mathrm{Aut}_c(G(\mathbf{Q}))$. This was also done, in a different way, by Komatsu in [14]. Then Uchida in [21], Iwasawa in [10], and Ikeda in [8] and [9] have finally proved the famous conjecture of Neukirch, namely that every automorphism of $G(\mathbf{Q})$ is actually inner. Beyond this Ikeda showed in [9] that if p is a prime and K is a finite extension of $\mathbf{Q}_p$, then every point-wise inner automorphism of $G(K)$, the absolute Galois group of K, is inner. The main purpose of this note is to strengthen this result and to prove:

THEOREM A. *If K is a finite extension of $\mathbf{Q}_p$, then every normal automorphism of $G(K)$ is inner.*

An analogous result was obtained in [12], where it was concluded from the main result that every normal automorphism of a non-abelian free profinite group is inner. Here we generalize this result in the following way.

We call a class of finite groups *full* if it is closed under the formation of subgroups, homomorphic images and group extensions. Examples of full classes are the class of all finite groups, all p-groups and all solvable finite groups. Let $\mathcal{C}$ be a full class of finite groups. A *pro-$\mathcal{C}$-group presented by e generators and d word-relations* is the pro-$\mathcal{C}$-completion of a discrete group presented by e generators and d relations in these generators. We prove:

Received November 24, 1978. Revision received September 24, 1979. The first author was partially supported by a DAAD grant. The work was partially done while the second author was visiting Tel-Aviv University.

THEOREM B. *Let $\mathcal{C}$ be a full class of finite groups and let G be a pro-$\mathcal{C}$-group presented by e generators and d word-relations. If $e \geqslant d+2$, then every normal automorphism of G is inner.*

Every free pro-$\mathcal{C}$-group is a projective limit of free pro-$\mathcal{C}$-groups on finitely many generators (cf. Ribes [18, p. 67]), hence:

COROLLARY C. *Let $\mathcal{C}$ be a full class of finite groups and let F be a non-abelian free pro-$\mathcal{C}$-group. Then every normal automorphism of F is inner.*

Both Theorem A and Theorem B are special cases of a more general theorem. In section 1 we define what are 'pseudo-p-free' profinite groups. We prove in two steps that if G is a pseudo-p-free profinite group, then $\mathrm{Aut}_n(G) = \mathrm{Aut}_i(G)$. First we prove, by Representation Theory, that every normal automorphism of G is families preserving. Then we show that every families preserving automorphism of G is inner. This is done by refining an argument of Ikeda and Iwasawa. In Section 2 we prove, using local class field theory, that $G(K)$ is pseudo-p-free and thus complete the proof of Theorem A. Sections 3 and 4 are devoted to the proof that G, in Theorem B, is a pseudo-p-free group. The main tools used there are the Gaschütz Theory for relation modules and pro-$\mathcal{C}$-completions.

In a previous version of this paper, the group G in Theorem B was restricted to be a non-abelian free pro-p-group with $p \neq 2$. The proof of this special case was based on a realization of G as a Galois group over a finite extension of $\mathbf{Q}_p$ and therefore failed for the case $p = 2$. Jean-Pierre Serre then pointed out to us the possibility of extending the result to free pro-2-groups and to Demuskin groups on $e \geqslant 3$ generators by outlining a cohomological proof to the extended theorem. We combined Serre's ideas with the theory of group-rings to bring up the result to its present form. Our sincere gratitude is therefore given to Serre. We are also indebted to Irving Reiner for referring us to Gaschütz Theory in Gruenberg's book [4]. Finally we would like to express our indebtedness to Alexander Lubotzky for his comment that the proof of Theorem B, previously given for pro-p-groups, actually works for pro-$\mathcal{C}$-groups.

We would also like to note that Lubotzky, [16], has used our results about profinite groups to deduce similar results for discrete groups.

1. Pseudo-p-free profinite groups

Definition. A profinite group G is said to be pseudo-p-free if every open normal subgroup N of G has a closed subgroup M such that:

(a) M is normal in G.

(b) The quotient group $A = N/M$ is an abelian group; thus $\Gamma = G/N$ acts on A by conjugation.

(c) The group A contains a closed subgroup B which is a pro-p-group, it is invariant under Γ and Γ-isomorphic to the group-ring $\mathbf{Z}_p\Gamma$.

If σ is a normal automorphism of G, then σ acts on the finite quotient group Γ and on the closed subgroups A and B. In particular σ is a $\mathbf{Z}_p$-linear operator of B.

The basic result of this work is:

THEOREM 1. *If G is a pseudo-p-free profinite group, then every normal automorphism of G is inner.*

Proof. The proof is carried out in two steps

Step 1. $\mathrm{Aut}_n G = \mathrm{Aug}_f G$

Let σ be a normal automorphism of G and let N be an open normal subgroup of G. We prove that σ is families preserving. Using compactness arguments it suffices to prove that the automorphism induced by σ on $\Gamma = G/N$ is families preserving.

Let M be the closed subgroup of N that satisfies conditions (a)–(c) of the Definition. If $b \in B$ and $x \in \Gamma$, then $(b^x)^\sigma = b^{\sigma \cdot x^\sigma}$, hence

$$b^x = b^{\sigma \cdot x^\sigma \cdot \sigma^{-1}} \tag{1}$$

Recall that B was assumed to be isomorphic to $\mathbf{Z}_p\Gamma$. Hence we can extend the action of σ to $\mathbf{Q}_p\Gamma$, by linearity.

Let E be a simple submodule of $\mathbf{Q}_p\Gamma$. Then $E' = E \cap \mathbf{Z}_p\Gamma$ is a submodule of $\mathbf{Z}_p\Gamma$ and is therefore left invariant by σ. Also, for every element $b \in E$ there exists a positive integer r such that $p^r b \in E'$. It follows that σ acts also on E and that (1) is true for every $b \in E$. This means that x is equal to $\sigma x^\sigma \sigma^{-1}$ as linear operators of E. Hence, if we denote by χ_E the character of E, we obtain $\chi_E(x) = \chi_E(x^\sigma)$, for every $x \in \Gamma$.

It is now well-known that every irreducible character χ of Γ over $\mathbf{Q}_p$ appears as a character of a simple submodule of $\mathbf{Q}_p\Gamma$ (cf. Huppert [6, p. 474]). It follows therefore from Representation Theory that $\langle x \rangle$ is conjugate to $\langle x^\sigma \rangle$ for every $x \in \Gamma$ (cf. Serre [20, p. 111, Cor 2]).

Step 2. $\mathrm{Aut}_f G = \mathrm{Aut}_i G$

Let σ be a families preserving automorphism of G and let N be an open normal subgroup of G. Again, using compactness arguments, it suffices to prove that the automorphism induced by σ on $\Gamma = G/N$ is inner. As before we consider a closed subgroup M of N with the properties (a)–(c) of the Definition. In particular it follows from (c) that B is isomorphic to $\mathbf{Z}_p^n$, where $n = |\Gamma|$ and that Γ acts faithfully on B.

Our assumption implies that for every $b \in B$ there exists an element $x(b) \in \Gamma$ and a unit $\mu(b) \in \mathbf{Z}_p^\times$ such that

$$b^\sigma = b^{\mu(b)x(b)} \tag{2}$$

We contend that there exists a $\nu \in Z_p^\times$ such that for every $b \in B$ there exists a root of unity $\zeta(b)$ in $\mathbf{Z}_p$ such that $\mu(b) = \nu\zeta(b)$.

Indeed write $\mu = \mu(b)$ and $x = x(b)$ in (2). If we apply σ $i-1$ times on both sides of (2) we obtain

$$b^{\sigma^i} = b^{\mu^i x x^\sigma \dots x^{\sigma^{i-1}}}$$

Remember that Γ is a finite group. Hence there exists a positive integer l such that $z^{\sigma^l} = z$ for every $z \in \Gamma$. Hence if $y = xx^\sigma \dots x^{\sigma^{l-1}}$, we get that $b^{\sigma^{lj}} = b^{\mu^{lj} y^j}$ for every positive integer j. In particular for $j = |\Gamma|$ and $m = l|\Gamma|$ we obtain

$$b^{\sigma^m} = b^{\mu(b)^m} \tag{3}$$

Let now $b_1, \dots, b_n$ be a (multiplicative) basis for B over Z_p. Substituting $b = b_i$ for $i = 1, \dots, n$, in (3) and multiplying the corresponding equalities we have

$$(b_1 \dots b_n)^{\sigma^m} = \prod_{i=1}^{n} b_i^{\mu(b_i)^m} \tag{4}$$

On the other hand, if we apply (3) for $c = b_1 \dots b_n$ we obtain

$$(b_1 \dots b_n)^{\sigma^m} = \prod_{i=1}^{n} b_i^{\mu(c)^m} \tag{5}$$

Equating (4) and (5) we deduce that $\mu(b_i)^m = \mu(c)^m$ for $i = 1, \dots, n$. Writing $\nu = \mu(c)$ we obtain that $\mu(b_i) = \nu\zeta(b_i)$, where $\zeta(b_i)$ is an mth root of unity in Z_p.

Let now $1 \neq d \in B$. Then we can write $d = b_1^{\lambda_1} \dots b_r^{\lambda_n}$ with $\lambda_i \in Z_p$ and not all of them are zero. It follows that

$$d^{\sigma^m} = \prod_{i=1}^{r} b_i^{\sigma^m \lambda_i} = \prod_{i=1}^{r} b_i^{\nu^m \lambda_i}.$$

On the other hand, applying (3) for d we have

$$d^{\sigma^m} = d^{\mu(d)^m} = \prod_{i=1}^{m} b_i^{\mu(d)^m \lambda_i}$$

Hence $\mu(d)^m = \nu^m$, that is $\mu(d) = \nu\zeta(d)$ with $\zeta(d)^m = 1$. Our contention is therefore proved.

We proceed and define for every $x \in \Gamma$ and every root of unity ζ in Z_p the following closed subgroup of B:

$$B^{(x,\zeta)} = \{ b \in B \mid b^\sigma = b^{\nu\zeta x} \}.$$

There are only finitely many such groups and their union covers B. It follows that there exists a pair (x, ζ) such that $B^{(x,\zeta)}$ is open in B and hence of a finite index, say k (c.f. [12, Section 2] or Bourbaki [1, chap. II, §1, exerc. 1b]). It follows that if $b \in B$, then $(b^\sigma)^k = (b^{\nu\zeta x})^k$, hence $b^\sigma = b^{\nu\zeta x}$, since B is torsion free. This means that $B^{(x,\zeta)} = B$.

Let now $y \in \Gamma$ and let g be an element of G that lies over y. Then for every $b \in B$ we have

$$(g^{-1}bg)^{\sigma} = (g^{\sigma})^{-1} b^{\sigma} g^{\sigma} = (g^{\sigma})^{-1} b^{\nu_S \zeta x} g^{\sigma}$$

$$(g^{-1}bg)^{\sigma} = (g^{-1}bg)^{\nu_S \zeta x} = (g^{x})^{-1} b^{\nu_S \zeta x} g^{x}$$

Hence

$$(b^{\nu_S \zeta x})^{g^{\sigma} g^{-x}} = b^{\nu_S \zeta x}.$$

The element $b^{\nu_S \zeta x}$ runs over B when b does. Hence $y^{\sigma} y^{-x}$ acts trivially on B. By (d) Γ acts faithfully on B, hence $y^{\sigma} = y^{x}$.

2. The absolute Galois group of a local field. The first instance of a pseudo-p-free profinite group is presented by the following

THEOREM 2. *If K is a finite extension of $\mathbb{Q}_p$, then $G(K)$ is a pseudo-p-free profinite group.*

Proof. Let L be a finite Galois extension of K with a Galois group $\Gamma = \mathcal{G}(L/K)$. The group of units U of L is a compact group on which Γ acts. Denote also by L_{nr} and L_{ab} the maximal non-ramified and the maximal abelian extensions, respectively, of L. The group Γ acts on the inertia group $A_1 = \mathcal{G}(L_{\mathrm{ab}}/L_{\mathrm{nr}}) \leqslant A = \mathcal{G}(L_{\mathrm{ab}}/L)$ via extension to L_{ab} and conjugation. The local reciprocity map $\theta : U \to A_1$ is a continuous Γ-isomorphism, by local class field theory (cf. [2, p. 144] and Koch [13, p. 79]).

Denote now by $\mathfrak{p}$ the maximal ideal of the ring of integers of L and let $U_r = 1 + \mathfrak{p}^r$ be the group of units of L of level r. Then U_r is a pro-p-group. If r is sufficiently large, then the map $\exp : \mathfrak{p}^r \to U_r$ is an isomorphism (c.f. Goldstein [3, p. 96]). By the normal basis theorem there exists an element $\alpha \in L$ such that $\{\alpha^x \mid x \in \Gamma\}$ is a basis for the extension L/K (c.f. Lang [15, p. 229]), in particular it is linearly independent over Z_p. Multiplying α by a sufficiently high power of p we can assume that $\alpha \in \mathfrak{p}^r$. Let $\mu = \exp(\alpha)$. Then $\{\mu^x \mid x \in \Gamma\}$ is a basis for a multiplicative free Z_p-module. The image of this module by θ is a closed subgroup of A which is isomorphic to $Z_p\Gamma$ as a $Z_p\Gamma$-module.

Theorem A follows from Theorems 1 and 2.

If we denote by $K^{(p)}$ the maximal p-extension of K, then we can prove, as in Theorem 2, that $\mathcal{G}(K^{(p)}/K)$ is a pseudo-p-free group and hence that every normal automorphism of $\mathcal{G}(K^{(p)}/K)$ is inner. It is well-known that $\mathcal{G}(K^{(p)}/K)$ is either the free pro-p-group on $[K : \mathbb{Q}_p] + 1$ generators or a pro-p-group presented by $[K : \mathbb{Q}_p] + 2$ generators and one relation (a Demuskin group), according to whether the primitive pth root of unity, ζ_p, does not belong or does belong to K (cf. Koch [13, p. 97, Satz 10.5 and p. 96, Satz 10.3]). In any case, the number of generators of $\mathcal{G}(K^{(p)}/K)$ exceeds the number of its defining relations by at least 2. Theorem B which is proved in the next section by group-theoretical

methods appears therefore as a generalization of the theorem about $\mathcal{G}(K^{(p)}/K)$ which is proved using arithmetical methods.

Problem: Is every automorphism of $G(\mathbb{Q}_p)$ normal?

3. The Gaschütz theory. We use the Gaschütz theory about relation modules in order to establish our second example of pseudo-p-free groups, which is necessary in order to complete the proof of Theorem B.

Denote by $I_G = \{\sum_{i=1}^n \alpha_i x_i \in ZG \mid \sum_{i=1}^n \alpha_i = 0\}$ the augmentation ideal of the group-ring ZG of a group G over Z. Then $I_G = \sum_{x \in G}(x-1)ZG$. If $1 \to N \to G \xrightarrow{\pi} \Gamma \to 1$ is a short exact sequence of groups, then π extends in a canonical way to an epimorphism of rings, $\pi : ZG \to Z\Gamma$, the kernel of which is $I_N G$ and we therefore obtain the following exact sequence of rings

$$0 \longrightarrow I_N G \longrightarrow ZG \xrightarrow{\pi} Z\Gamma \longrightarrow 0 \tag{1}$$

The ideal I_G is mapped by π onto I_Γ, hence (1) induces the following exact sequence

$$0 \longrightarrow I_N G \longrightarrow I_G \xrightarrow{\pi} I_\Gamma \longrightarrow 0 \tag{2}$$

Dividing by $I_N I_G$ we obtain

$$0 \longrightarrow I_N G/I_N I_G \longrightarrow I_G/I_N I_G \xrightarrow{\pi} I_\Gamma \longrightarrow 0. \tag{3}$$

Pulling back the action of Γ on I_Γ through π, the group $I_G/I_N I_G$ becomes a Γ-module and π becomes a Γ-homomorphism

$$(\alpha + I_N I_G)^x = \alpha x + I_N I_G, \qquad \text{for } \alpha \in I_G \text{ and } x \in \Gamma.$$

The subgroup $I_N G/I_N I_G$ is invariant under the action of Γ and one can prove that the map $(n-1) + I_N I_G \to nN'$ is a Γ-isomorphism of $I_N G/I_N I_G$ onto $\overline{N} = N/N'$, where Γ acts on $\overline{N}$ by conjugation (cf. Gruenberg [4, p. 6]). We can therefore replace $I_N G/I_N I_G$ in (3) by $\overline{N}$ and obtain the following exact sequence of right Γ-modules

$$0 \longrightarrow \overline{N} \longrightarrow I_G/I_N I_G \xrightarrow{\pi} I_G \longrightarrow 0. \tag{4}$$

Then we tensor the short sequence (4) with a field K of characteristic 0, apply Maschke's Theorem saying that short sequences of $K\Gamma$-modules split and obtain the following decomposition of $K\Gamma$-modules

$$K \otimes (I_G/I_N I_G) \cong K\overline{N} \oplus KI_G \tag{5}$$

Also, $K\Gamma = K \oplus KI_\Gamma$, hence adding K as a direct summand to both sides of (5) we have:

$$K \otimes (I_G/I_N I_G) \oplus K \cong K\overline{N} \oplus K\Gamma \tag{6}$$

Consider now the special case where $G = F$ is the free group on a set X and also replace N by M. Then it can be proved that I_F is the free ZF-module on the set $\{x - 1 \mid x \in X\}$ and one can further deduce that $I_F/I_F I_M$ is the free $Z\Gamma$-module on the set $\{(x-1) + I_F I_M \mid x \in X\}$. In particular if X consists of e elements, say $x_1', \ldots, x_e'$, then we may conclude from (6) that

$$(K\Gamma)^e \oplus K \cong K\overline{M} \oplus K\Gamma \tag{7}$$

Applying Krull-Schmidt's Theorem to (7) (cf. Huppert [3, p. 66]) we can cancel $K\Gamma$ on both sides and achieve the structure of $K\overline{M}$ as a $K\Gamma$-module

$$K\overline{M} \cong (K\Gamma)^{e-1} \oplus K$$

This is a theorem of Gaschütz (cf. Gruenberg [4, p. 8]).

We extend this theorem to groups presented by e generators and d relations.

Let $r_1, \ldots, r_d$ be d elements of F. Denote by R the smallest normal subgroup of F that contains $r_1, \ldots, r_d$, and let $G = F/R$. Denote by $x_1, \ldots, x_e$ the images of $x_1', \ldots, x_e'$ in G. Then G is *presented* as the group on e generators $x_1, \ldots, x_e$ and the d defining relations $r_1, \ldots, r_d$. Retain for G all the notation included in (6). Denote also by θ the canonical homomorphism from F to G and let $M = \theta^{-1}N$. As in (2) we have an exact sequence

$$0 \longrightarrow I_R F \longrightarrow I_F \xrightarrow{\theta} I_G \longrightarrow 0$$

which gives rise to the following exact sequence of Γ-modules

$$0 \longrightarrow (I_R F + I_F I_M)/I_F I_M \longrightarrow I_F/I_F I_M \xrightarrow{\theta} I_G/I_G I_N \longrightarrow 0 \tag{8}$$

Tensoring (8) by K and using Maschke's Theorem we arrive at the $K\Gamma$-decomposition

$$(K\Gamma)^e \cong (K \otimes (I_R F + I_F I_M)/I_F I_M) \oplus (K \otimes (I_G/I_G I_N)) \tag{9}$$

Using the two identities

$$x^{-1}rx - 1 = (x^{-1} - 1)(r - 1)(x - 1) + (x^{-1} - 1)(r - 1) + (r - 1)x$$

$$xy - 1 = (x - 1)(y - 1) + (x - 1) + (y - 1)$$

and the normality of R in F one concludes that $(I_R F + I_F I_M)/I_F I_M$ is the $Z\Gamma$-module generated by $\{r_i - 1 \mid i = 1, \ldots, d\}$. Using Maschke's Theorem again we see that there exists a $K\Gamma$-module C such that

$$C \oplus (K \otimes (I_R F + I_F M)/I_F I_M) \cong (K\Gamma)^d.$$

If we combine this result with (9) we have

$$C \oplus (K\Gamma)^e \cong (K\Gamma)^d \oplus (K \otimes (I_G/I_G I_N)) \tag{10}$$

Assume now that $d \leqslant e$ and use Krull-Schmidt's Theorem to cancel $(K\Gamma)^d$ from both sides of (10) to obtain

$$K \otimes (I_G / I_G I_N) \cong C \oplus (K\Gamma)^{e-d}. \tag{11}$$

If $e \geqslant d+1$ and if we use (11) in (6) we get a weak generalization of Gaschütz' Theorem

$$K\overline{N} \cong C \oplus K \oplus (K\Gamma)^{e-d-1}. \tag{12}$$

The group N is finitely generated, hence $\overline{N}$ is a finitely generated abelian group. Denote by T the maximal subgroup of N that contains N' such that T/N' is a torsion group. Then T is a normal subgroup of G and N/T is a torsion-free abelian group of rank, say m. Moreover, $K \otimes (N/N') \cong K \otimes (N/T)$, as $K\Gamma$-modules and we can therefore replace (12) by

$$K \otimes (N/T) \cong C \oplus K \oplus (K\Gamma)^{e-d-1}, \qquad \text{as } K\Gamma\text{-modules.} \tag{13}$$

Also

$$N/T \cong Z^m, \qquad \text{as groups.} \tag{14}$$

The results of this Section can be summed up in the following theorem.

THEOREM 3: *Let G be a discrete group presented by e generators and d relations with $e \geqslant d+1$. Let N be a normal subgroup of G with a finite quotient group Γ. Then N contains a subgroup T which is normal in G such that* (14) *holds for some positive integer m. Moreover, if K is a field of characteristic zero, then $K \oplus (K\Gamma)^{e-d-1}$ appears as a direct summand of the $K\Gamma$-module $K \otimes N/T$.*

4. Pro-$\mathcal{C}$-group. The object of this section is to pass to the pro-$\mathcal{C}$-limit, starting from Theorem 3. Here $\mathcal{C}$ is a full class of finite groups which is fixed throughout this Section.

Let G be a group and denote by $\mathfrak{F} = \mathfrak{F}_G$ the family of all normal subgroups of G that belong to $\mathcal{C}$. Then $\hat{G}(\mathcal{C}) = \lim_{H \in \mathfrak{F}} G/H$ is the pro-$\mathcal{C}$-completion of G. There is a canonical homomorphism τ of G into $\hat{G}(\mathcal{C})$, the kernel of which is the intersection G_0 of all H in $\mathfrak{F}$. The image of G is dense in $\hat{G}(\mathcal{C})$.

Let H be a subgroup of G that belongs to $\mathfrak{F}_G$ and let $I \in \mathfrak{F}_H$. Then I is a normal subgroup of H but not necessarily of G. However, if $g_1, \ldots, g_n$ are representatives of left cosets of G modulo H and $I_i = I^{g_i}$ for $i = 1, \ldots, n$, then $J = I_1 \cap \cdots \cap I_n$ is normal in G and H/J is a subgroup of the direct product $H/I_1 \times \ldots \times H/I_n$ of groups belonging to $\mathcal{C}$. It follows that H/J and hence also G/J belong to $\mathcal{C}$. This implies that if we denote by $\hat{H}$ the closure of τH in $\hat{G}(\mathcal{C})$, then $\hat{H}$ is the pro-$\mathcal{C}$-completion of H. It is not difficult to see that in addition G/H is canonically isomorphic to $\hat{G}(\mathcal{C})/\hat{H}$ and that $H = \tau^{-1}\hat{H}$. Thus the correspondence $H \mapsto \hat{H}$ is a bijection from $\mathfrak{F}_G$ onto the collection of all open

normal subgroups of $\hat{G}(\mathcal{C})$. Standard arguments also show that if L is a closed normal subgroup of H, then $\hat{H}/\hat{L}$ is the pro-$\mathcal{C}$-completion of H/L.

We are interested in particular in the pro-$\mathcal{C}$-completion of Z. Denote therefore by Λ the set of all primes l that divide the order of groups belonging to $\mathcal{C}$. If $l \in \Lambda$, then $\mathbf{Z}/l\mathbf{Z}$ belong to $\mathcal{C}$, by Sylow's Theorem. It is well-known that every l-group has a normal sequence of subgroups with factors isomorphic to $\mathbf{Z}/l\mathbf{Z}$. Hence $\mathcal{C}$ contains every l-group. This implies that the pro-$\mathcal{C}$-completion of $\mathbf{Z}$ is $\prod_{l\in\Lambda}\mathbf{Z}_l$.

Return now to the case of Theorem 3, where G is a discrete group presented by e generators $x_1, \ldots, x_e$ and d relations $r_1, \ldots, r_d$ in these generators. We abuse our language by using $x_1, \ldots, x_e$ as elements of $\hat{G}(\mathcal{C})$ instead of their images by τ. Then $\hat{G}(\mathcal{C})$ is the pro-$\mathcal{C}$-group presented by the e generators $x_1, \ldots, x_e$ and the d word-relations $r_1, \ldots, r_d$. This means that if $\overline{G}$ is a pro-$\mathcal{C}$-group generated by e elements $\bar{x}_1, \ldots, \bar{x}_e$ satisfying the relations $r_1 = \cdots = r_d = 1$, then the map $x_i \mapsto \bar{x}_i$ $i = 1, \ldots, e$ can be extended to a continuous homomorphism of $\hat{G}(\mathcal{C})$ onto $\overline{G}$.

Return also to the subgroups N and T of Γ of formulas (13) and (14) of Section 3 and assume that Γ belongs to $\mathcal{C}$. It follows from the above discussion that $\hat{N}/\hat{T} \cong \prod_{l\in\Lambda} Z_l^m$. Let $z_1, \ldots, z_m$ be elements of N that generate N modulo T. Consider them also as elements of $\hat{N}$. Choose a prime number p in Λ and let α be the element of $\hat{Z}$ with components $\alpha_l = 0$ if $l \neq p$ and $\alpha_p = 1$. Denote $z_i' = z_i^{\alpha}$ for $i = 1, \ldots, m$ and let P be the closed subgroup of $\overline{N}$ generated by $z_1', \ldots, z_m'$ and $\hat{T}$. Then P is normal in $\hat{G}(\mathcal{C})$ and $P/\overline{T} \cong Z_p^m$. It follows that both $\mathbf{Q}_p \otimes_{Z_p} P/\hat{T}$ and $\mathbf{Q}_p \otimes N/T$ are m-dimensional $\mathbf{Q}_p$-vector spaces with bases $z_1', \ldots, z_m'$ and $z_1, \ldots, z_m$, respectively. Moreover, the action of Γ on N/T is determined by the action of Γ on the z_i modulo T, which is the same as the action of Γ on the z_i' modulo $\hat{T}$. It follows that $\mathbf{Q}_p \otimes_{Z_p} P/\hat{T}$ and $\mathbf{Q}_p \otimes N/T$ are even isomorphic as $\mathbf{Q}_p\Gamma$-modules. Thus, if we substitute $\mathbf{Q}_p$ for K in (13) of Section 3 we arrive at the following $\mathbf{Q}_p\Gamma$-isomorphism

$$\mathbf{Q}_p \otimes_{Z_p} P/\hat{T} \cong C \oplus \mathbf{Q}_p \oplus (\mathbf{Q}_p\Gamma)^{e-d-1} \tag{1}$$

Note that all the summands on the right hand side of (1) are finitely generated $\mathbf{Q}_p$-vector spaces and therefore they are closed under the p-adic topology.

If $e \geqslant d+2$, then $\mathbf{Q}_p\Gamma$ appears as a direct summand of $\mathbf{Q}_p \otimes_{Z_p} P/\hat{T}$. After multiplying a $\mathbf{Q}_p$-basis of $\mathbf{Q}_p\Gamma$ by an appropriate power of p we may conclude that $\hat{N}/\hat{T}$ contains $\mathbf{Z}_p\Gamma$ as a closed $\mathbf{Z}_p\Gamma$-submodule.

We summarize our results in the following theorem.

THEOREM 4. *Let $\mathcal{C}$ be a full class of finite groups and let G be a pro-$\mathcal{C}$-group presented by e generators and d word-relations with $e \geqslant d+2$. If a prime p divides the order of a group belonging to $\mathcal{C}$, then G is a pseudo-p-free profinite group.*

With this Theorem, the proof of Theorem B is completed.

References

1. N. Bourbaki, *Algèbre Commutative*, Hermann, Paris, 1961.
2. J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory*, Academic Press, London/New York, 1967.
3. L. J. Goldstein, *Analytic Number Theory*, Prentice-Hall, Englewood Cliffs, New Jersey, 1971.
4. K. Gruenberg, *Relation modules of finite groups*, CBMS 25, Amer. Math. Soc. 1976.
5. H. Hasse, *Zahlentheorie*, Akademie Verlag, Berlin, 1969.
6. B. Huppert, *Endliche Gruppen* I, Springer, Berlin/Heidelberg/New York, 1967.
7. M. Ikeda, *On the group of automorphisms of the absolute Galois group of the rational number field*, Archiv der Math. **26** (1975), 250–252.
8. ———, *Completeness of the absolute Galois group of the rational number field*, Crelle Journal **291** (1977), 1–21.
9. ———, *On automorphisms of Galois groups*, a manuscript.
10. K. Iwasawa, *Automorphisms of Galois groups of number fields*, a manuscript.
11. A. V. Jakovlev, *The Galois group of the algebraic closure of a local field*, Math. U.S.S.R. Izvestija **2** (1968), 1231–1269.
12. M. Jarden, *Normal automorphisms of free profinite groups*, to appear in Journal of Algebra.
13. H. Koch, *Galoissche Theorie der p-Erweiterungen*, VEB Deutscher Verlag der Wissenschaften, Berlin, 1970.
14. K. Komatsu, *A remark on Neukirch's conjecture*, Proc. Japan Acad. **50** (1974), 253–255.
15. S. Lang, *Algebra*, Addison-Wesley, Reading, Massachusetts, 1965.
16. A. Lubotzky, *Normal automorphisms of free groups*, to appear in Journal of Algebra.
17. J. Neukirch, *Kennzeichning der p-adischen und der endlichen Zahlkörper*, Inventiones Mathematicae **6** (1969), 296–314.
18. L. Ribes, *Introduction to profinite groups and Galois cohomology*, Queen's Papers in Pure and Applied Mathematics 24, Queen's University, Kingston, 1970.
19. A. Scholz, *Über die Bildung algebraischer Zahlkörper mit auflösbarer Galoisscher Gruppe*, Math. Zeitschrift **30** (1929), 332–356.
20. J-P. Serre, *Représentations linéaires des groupes finis*, 2ème édition, Hermann, Paris, 1971.
21. K. Uchida, *Isomorphisms of Galois groups*, Journal of Mathematical Society of Japan **28** (1976), 617–620.

Jarden: Department of Mathematical Sciences, Tel Aviv University, Ramat-Aviv, Tel Aviv, Israel

Ritter: Mathematisches Institut Universität Heidelberg, Im Neuenheimer Feld 288, 6900 Heidelberg, Germany