



2002

Embedding Problems and Finite Quotients

Ted Chinburg

Darren B. Glass
Gettysburg College

Follow this and additional works at: <http://cupola.gettysburg.edu/mathfac>

 Part of the [Mathematics Commons](#)

Share feedback about the accessibility of this item.

Chinburg T, and D. Glass, Embedding Problems and Finite Quotients. *Pacific Journal of Mathematics*. 2002. 205(1): 31-41.

This is the publisher's version of the work. This publication appears in Gettysburg College's institutional repository by permission of the copyright owner for personal use, not for redistribution. Cupola permanent link: <http://cupola.gettysburg.edu/mathfac/13>

This open access article is brought to you by The Cupola: Scholarship at Gettysburg College. It has been accepted for inclusion by an authorized administrator of The Cupola. For more information, please contact cupola@gettysburg.edu.

Embedding Problems and Finite Quotients

Abstract

We give a condition on a family of solutions of quotients of an embedding problem which implies the embedding problem has a solution. This shows, in particular, that to solve an embedding problem associated to the maximal extension of a number field unramified outside a fixed finite set of places, it suffices to find a solution for each finite quotient of the embedding problem. This statement is not true in general over global function fields, but one can prove variants of it in this case in which extra conditions on the embedding problems or on the ramification of solutions are assumed.

Disciplines

Mathematics

EMBEDDING PROBLEMS AND FINITE QUOTIENTS

TED CHINBURG AND DARREN GLASS

We give a condition on a family of solutions of quotients of an embedding problem which implies the embedding problem has a solution. This shows, in particular, that to solve an embedding problem associated to the maximal extension of a number field unramified outside a fixed finite set of places, it suffices to find a solution for each finite quotient of the embedding problem. This statement is not true in general over global function fields, but one can prove variants of it in this case in which extra conditions on the embedding problems or on the ramification of solutions are assumed.

1. Introduction.

Let \mathcal{C} be a finite class of finite groups which is closed under taking subgroups, quotients and group extensions. The category of \mathcal{C} -profinite groups is the category of topological groups Γ which are isomorphic topologically to the inverse limit of their discrete finite quotients, each of which is in \mathcal{C} . By an embedding problem we will mean a diagram

$$(1.1) \quad \begin{array}{ccccccc} & & \Gamma & & & & \\ & & \downarrow & & & & \\ 1 & \leftarrow & T & \leftarrow & G & \leftarrow & A \leftarrow 0 \\ & & \downarrow & & & & \\ & & 1 & & & & \end{array}$$

of \mathcal{C} -profinite groups and \mathcal{C} -profinite group homomorphisms, in which the vertical and horizontal sequences are exact. A solution of this embedding problem is a continuous homomorphism $h : \Gamma \rightarrow G$ making the diagram commute. Call h a proper solution if h is surjective.

Suppose C is a closed normal subgroup of G which is contained in A . One then has a related embedding problem

$$(1.2) \quad \begin{array}{ccccccc} & & \Gamma & & & & \\ & & \downarrow & & & & \\ 1 & \leftarrow & T & \leftarrow & G/C & \leftarrow & A/C \leftarrow 0 \\ & & \downarrow & & & & \\ & & 1 & & & & \end{array}$$

The study of embedding problems with the following property was suggested to us by D. Harbater and A. Tamagawa.

Definition 1.1. An embedding problem (1.1) will be said to be determined by finite quotients if it has a (proper) solution whenever there is a (proper) solution to (1.2) for each closed normal subgroup C of G of finite index in A .

We will prove:

Theorem 1.2. *Suppose T is finite. Let K be a global field, and let D be a finite set of places of K . Define $\Gamma_{K,D}$ to be Galois group over K of the maximal Galois extension of K unramified outside of D . The embedding problem (1.1) is determined by finite quotients if Γ and G satisfy one of the following conditions:*

- (a) *For all positive integers n , Γ has only finitely many closed subgroups of index n .*
- (b) *$\Gamma = \Gamma_{K,D}$ and K is a number field.*
- (c) *$\Gamma = \Gamma_{K,D}$ for a global function field K , and the group G is abelian with a countable basis of open neighborhoods of the identity element.*

Theorem 1.2(a) is a consequence of a compactness result, Theorem 2.2 of Section 2. Part (b) of Theorem 1.2 follows from Part (a) and a theorem of Hermite and Minkowski. Note that Part (b) is equivalent to the statement that if (1.1) is not determined by finite quotients, but (1.2) has a (proper) solution for each C , then the latter solutions must acquire ramification at an unbounded set of places of K .

We discuss in Section 2 an example due to D. Haran, D. Harbater, F. Pop and A. Tamagawa which shows (1.1) may not be determined by finite quotients if $\Gamma = \Gamma_{K,D}$ and K is a global function field. Motivated by this example, we show in Corollary 2.8 and Remark 2.9 that if one has a proper solution to (1.2) for each C in the function field case, the non-existence of a proper solution to (1.1) results from the fact that solutions to (1.2) acquire too much ramification as C varies.

In Section 3 we compare condition (a) of Theorem 1.2 to a finiteness condition Φ_p of Mazur on the group Γ . The proof of Theorem 1.2(c) is given in Section 4 and relies on class field theory. An example given in Remark 4.3 showing that (1.1) is not determined by finite quotients for arbitrary profinite abelian groups Γ and G having a countable basis of open neighborhoods of the identity.

We end this introduction with an open problem.

Question 1.3. Is Theorem 1.2(c) true if one drops the hypothesis that G is abelian?

2. A compactness theorem.

Let \mathcal{T} be a collection of closed normal subgroups C of G which are contained in A , and whose intersection is the identity element of G . Let \mathcal{S}_C be a (possibly empty) set of solutions h_C of the embedding problem (1.2)

Question 2.1. For which embedding problems (1.1) and collections $\{\mathcal{S}_C\}_{C \in \mathcal{T}}$ of solutions to (1.2) are the following conditions equivalent?

- (1) There exists a (proper) solution h .
- (2) For all $C \in \mathcal{T}$, there exists a (proper) solution h_C in \mathcal{S}_C .

Clearly (1) implies (2) if for each $C \in \mathcal{T}$, \mathcal{S}_C is the set of all solutions to (1.2). We will focus on finding sufficient conditions for (2) to imply (1).

If Γ_1 and Γ_2 are topological groups, let $\text{Hom}_c(\Gamma_1, \Gamma_2)$ be the set of continuous homomorphisms from Γ_1 to Γ_2 . Choose topologies on the sets $\text{Hom}_c(\Gamma, G/C)$ as C ranges over \mathcal{T} with the property that the natural maps

$$\pi_{C'}^C : \text{Hom}_c(\Gamma, G/C') \rightarrow \text{Hom}_c(\Gamma, G/C)$$

for $C, C' \in \mathcal{T}$ and $C' \subset C$ are continuous. The usual choice is the uniform convergence topology, in which a countable sequence $\{f_i\}_i$ of functions in $\text{Hom}_c(\Gamma, G/C)$ converges to a function f if it does so uniformly on compact subsets of Γ . If Γ is compact and G/C is discrete, then the uniform convergence topology on $\text{Hom}_c(\Gamma, G/C)$ is the discrete topology. However, there are other choices than the uniform convergence topology on the $\text{Hom}_c(\Gamma, G/C)$ which one could consider.

Theorem 2.2. *Condition (2) of Question 2.1 implies Condition (1) if \mathcal{T} and $\{\mathcal{S}_C\}_{C \in \mathcal{T}}$ have the following properties:*

- (a) *The intersection of any finite set of elements of \mathcal{T} contains an element of \mathcal{T} .*
- (b) *\mathcal{S}_C is a compact subset of $\text{Hom}_c(\Gamma, G/C)$ for all $C \in \mathcal{T}$.*
- (c) *If $C, C' \in \mathcal{T}$ and $C' \subset C$ then $\pi_{C'}^C(\mathcal{S}_{C'}) \subset \mathcal{S}_C$.*

Proof. The elements of \mathcal{T} form an inverse system under inclusion. Let $\{C_1, \dots, C_n\}$ be a finite subset of \mathcal{T} . By Condition (a) of Theorem 2.2, there is a $C \in \mathcal{T}$ which is a subset of $\cap_{i=1}^n C_i$. We may assume (2) of Question 2.1 holds, so \mathcal{S}_C is nonempty. Each element of \mathcal{S}_C gives an element of the finite inverse limit of the \mathcal{S}_{C_i} as i ranges from 1 to n because of assumption (c) of Theorem 2.2. The compactness assumption (b) then implies the inverse limit of \mathcal{S}_C over all $C \in \mathcal{T}$ is nonempty.

This produces a continuous homomorphism

$$(2.1) \quad f : \Gamma \rightarrow \varprojlim_{\overline{C}} G/C.$$

We now construct a continuous homomorphism

$$(2.2) \quad \gamma : \varprojlim_C G/C \rightarrow G.$$

Write G as the inverse limit of finite quotients G/N_i . Pick one such G/N_i . Since we assumed that $\bigcap_{C \in \mathcal{T}} C = \{e\}$, there is a finite subset of \mathcal{T} whose intersection is contained in N_i . Hence Condition (a) of Theorem 2.2 implies $C \subset N_i$ for some $C \in \mathcal{T}$. We now send an element $\{g_C\}_C$ of the inverse limit on the left side of (2.2) to the element $\{h_i\}_i$ of G , where for each i we choose a group $C \in \mathcal{T}$ such that $C \subset N_i$ and we let h_i be the image of g_C in G/N_i . The composition of f in (2.1) and γ in (2.2) gives us a solution h to the embedding problem (1.1).

We still need to show that $h = \gamma \circ f$ is surjective if f in (2.1) is the inverse limit of surjections $f_C : \Gamma \rightarrow G/C$. Choose $g \in G$ and write it as the inverse limit of elements $g_C \in G/C$ as C ranges over \mathcal{T} . We know that $f_C^{-1}(g_C)$ is a nonempty compact subset of Γ for each C . Because of Assumption (a) of Theorem 2.2, the intersection of $f_C^{-1}(g_C)$ over any finite set of C 's contained in \mathcal{T} is nonempty. Therefore $h^{-1}(g) = \bigcap_{C \in \mathcal{T}} f_C^{-1}(g_C)$ is nonempty, so h is surjective.

Example 2.3. Suppose T is a finite group and that \mathcal{T} is the set of all closed normal subgroups C of G of finite index in A . Then Condition (a) of Theorem 2.2 holds. If all the groups $\text{Hom}_c(\Gamma, G/C)$ for $C \in \mathcal{T}$ are given the discrete topology, then Condition (b) of Theorem 2.2 is equivalent to \mathcal{S}_C being finite for all such C . If \mathcal{S}_C is the set of all solutions of (1.2) then Condition (c) of Theorem 2.2 holds.

The proof of Theorem 1.2(a) is now immediate from this example and Theorem 2.2. Part (b) of Theorem 1.2 is implied by Part (a), since by a Theorem of Hermite and Minkowski, there are only finitely many extensions of a number field K which have a given degree and are unramified outside a fixed finite set of places D of K .

The following example of Tamagawa motivated this note, and follows readily from classfield theory. It illustrates an embedding problem (1.1) which is not determined by finite quotients because proper solutions to (1.2) must acquire ramification at an unbounded number of places.

Example 2.4 (Tamagawa). Suppose G is the direct sum of two copies of the p -adic integers \mathbf{Z}_p , T is trivial and $\Gamma = \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Then (1.1) has no proper solutions, but (1.2) has a proper solution for each subgroup C of finite index in G .

We are grateful to D. Haran, D. Harbater, F. Pop and A. Tamagawa for the following example which shows Theorem 1.2(b) does not hold in general if K is a global function field.

Example 2.5 (Haran, Harbater, Pop, Tamagawa). Let G be the direct product of an uncountable number of copies of \mathbf{Z}/p , and give G the product topology. Let T be trivial, and let K be $\mathbf{F}_p(t)$. Let D have a single element consisting of the place of $\mathbf{F}_p(t)$ where t has normalized absolute value p . Then one can construct a proper solution to each finite embedding problem (1.2) using a compositum of Artin-Schreier covers of the form $x^p - x = j(t) \in \mathbf{F}_p[t]$, but one cannot solve the embedding problem (1.1).

We would like to explain how even in the function field case, Theorem 2.2 shows the non-existence of a proper solution to (1.1) results from the fact that solutions to (1.2) acquire too much ramification as C varies.

Let L/K be a finite separable extension of global function fields. The relative discriminant $d_{L/K}$ is an effective divisor of K defined locally as in [2, §III.3]. Thus for each place v of K , the multiplicity of v in $d_{L/K}$ is the valuation at v of the discriminant $d(R_v/A_v)$, where A_v is the local ring of v in K and R_v is the integral closure of A_v in L . (We do not take completions, so A_v is a discrete valuation ring and R_v is a semi-local Dedekind ring.)

For the convenience of the reader we will include a proof of the following well-known result.

Lemma 2.6. *Given K , an effective divisor B on K and an integer n , there are only finitely many separable extensions L of K of degree n for which $d_{L/K}$ is bounded above by B .*

Proof. We can reduce to considering only those L for which K is the only proper subfield of L which contains K . By [4, Cor. to Prop. VIII.14], the genus $g(L)$ of L is bounded by a function of K , n and $\deg(B)$. Let v be a place of K , and let d be the effective divisor of L associated to v . By applying the Riemann-Roch Theorem to K and L and multiples of v and d , respectively, we can conclude the following. There is an integer t bounded above by a function of v , K , n and B together with a function $f \in L$ not in K such that $\text{div}(f) + td$ is effective. Then $L = K(f)$. The valuations of f at places over v (resp. not over v) in the Galois closure of L over K are bounded below by functions which depend only on n , K and B (resp. are bounded below by 0). Taking elementary symmetric functions in the conjugates of f , we conclude that f is a root of a polynomial over K of degree at most n whose coefficients have divisors whose positive and negative parts have degrees bounded by functions of n , K and B . There are only finitely many such polynomials, so there are only finitely many L .

Definition 2.7. Let K^{sep} be a separable closure of K , and let $\Gamma = \text{Gal}(K^{\text{sep}}/K)$. Suppose f_C is a (proper) solution of (1.2) and G/C is a finite discrete quotient of G . Let $L = (K^{\text{sep}})^{\ker(f_C)}$ be the Galois extension of K associated to f_C , so $\text{Gal}(L/K)$ is a subgroup of G/C . We will say f_C

is bounded by an effective divisor $B = B(C)$ on K if $d_{L/K} \leq B(C)$. By Lemma 2.6, the set $\mathcal{S}_{C,B(C)}$ of all f_C bounded by $B(C)$ is finite.

Corollary 2.8. *Suppose that K is a global function field, T is finite, and that $\Gamma = \text{Gal}(K^{\text{sep}}/K)$. Let \mathcal{T} be the set of all closed normal subgroups C of G which are of finite index in A . Suppose that for $C \in \mathcal{T}$, there is a (proper) solution to (1.2). Then the following two statements are equivalent:*

- (1) *There is a (proper) solution to (1.1).*
- (2) *There is a function B from \mathcal{T} to effective divisors on K together with a nonempty subset \mathcal{S}_C of (proper) elements of $\mathcal{S}_{C,B(C)}$ for each $C \in \mathcal{T}$ such that $\pi_{C'}^C(\mathcal{S}_{C'}) \subset \mathcal{S}_C$ whenever $C' \subset C$ and $C', C \in \mathcal{T}$.*

Proof. If there is a (proper) solution h to (1.1), then we can take \mathcal{S}_C to be the single element set consisting of the induced (proper) solution to (1.2). Clearly \mathcal{S}_C satisfies (2) of Corollary 2.8 for some effective divisor $B(C)$. Conversely, suppose that there is a B and a subset \mathcal{S}_C for $C \in \mathcal{T}$ as in (2) of Corollary 2.8. Then \mathcal{S}_C is finite by Lemma 2.6, so Theorem 2.2 produces a (proper) solution to (1.1).

Remark 2.9. One can view Corollary 2.8 as saying that if (1.1) has no solution, then there is no way to set discriminant constraints on the embedding problem (1.2) for each $C \in \mathcal{T}$ in such a way that these constraints can be satisfied consistently as one varies C . This could be rephrased in terms of higher ramification groups using the connection between discriminants of finite Galois extensions and higher ramification groups (cf. [2, §III.4 and Prop. IV.4]).

It is a natural question whether (2) of Corollary 2.8 can be replaced by the following stronger condition:

- (2') *There is a function B from \mathcal{T} to effective divisors on K such that $\pi_{C'}^C(\mathcal{S}_{C',B(C')}) \subset \mathcal{S}_{C,B(C)}$ whenever $C' \subset C$ and $C', C \in \mathcal{T}$.*

The following counterexample shows that (1) of Corollary 2.8 need not imply (2').

Let N be the compositum over $K = \mathbf{F}_p(t)$ of all cyclic extensions of degree p which are ramified at the place of K where t has normalized absolute value p . Let $\Gamma = G = \text{Gal}(N/K)$ and let T be the trivial group, so that the identity map h is a proper solution of the embedding problem (1.1). Then Γ is topologically isomorphic to the product of a countable number of copies of $\mathbf{Z}/p\mathbf{Z}$, since it is isomorphic to an inverse limit of $(\mathbf{Z}/p\mathbf{Z})^m$ over positive integers m with respect to the natural projection maps. Suppose B is a function from $C \in \mathcal{T}$ to effective divisors of K . Each proper $f \in \mathcal{S}_{C,B(C)}$ determines a Galois G/C extension N_f of K . Suppose $C', C \in \mathcal{T}$, $C' \subset C \neq \Gamma$, f' is a proper element of $\mathcal{S}_{C',B(C')}$ and that L is a subfield of degree p over K inside $N_{f'}$. Then L corresponds to an index p subgroup

H of G/C' . Since the natural projection $\mu : G/C' \rightarrow G/C$ is a surjection of nontrivial finite dimensional vector spaces over $\mathbf{Z}/p\mathbf{Z}$, we can find an automorphism of G/C' which sends $\ker(\mu)$ into H . Hence composing f' with a suitable automorphism of G/C' gives a proper element $f'' \in \mathcal{S}_{C,B(C)}$ such that when $f = \pi_{C'}^C(f'')$, the field L is a subfield of N_f . There is a function $t(C')$ which increases to positive infinity with $[G : C']$ such that for each proper $f' \in \mathcal{S}_{C',B(C')}$ there is a subfield L of $N_{f'}$ such that $[L : K] = p$ and $\deg(d_{L/K}) \geq t(C')$. Thus there must be a C' such that $\pi_{C'}^C(\mathcal{S}_{C',B(C')})$ is not contained in $\mathcal{S}_{C,B(C)}$, since $d_{L/K}$ is bounded if $f \in \mathcal{S}_{C,B(C)}$ is proper and L is a subfield of N_f with $[L : K] = p$.

3. Finiteness conditions.

Let Γ be a profinite group, and let p be a prime. In [1, §1.1], Mazur specifies that Γ satisfies the finiteness condition Φ_p if for every open subgroup Γ_0 of finite index in Γ , the following equivalent conditions hold:

- (a) The pro- p completion of Γ_0 is topologically finitely generated, or
- (b) The abelianized pro- p completion of Γ_0 , given its natural \mathbf{Z}_p -module structure, is of finite type over \mathbf{Z}_p , or
- (c) There are only a finite number of continuous homomorphisms from Γ_0 to \mathbf{F}_p .

(Note that a subgroup of finite index in Γ is open if and only if it is closed.)

Condition (ii) of the following Proposition is the hypothesis of Theorem 1.2(a).

Proposition 3.1. *Consider the following conditions on Γ :*

- (i) Γ is topologically finitely generated.
- (ii) For each positive integer n , Γ has only finitely many closed subgroups of index n .
- (iii) Γ satisfies the finiteness condition Φ_p for all primes p .

Then (i) implies (ii), and (ii) implies (iii), but neither converse implication holds.

Proof. Clearly Condition (i) implies (ii). The converse is not true, as seen by taking Γ to be the product of l copies of $\mathbf{Z}/l\mathbf{Z}$ as l ranges over all primes. Condition (ii) implies the same condition holds for each subgroup Γ_0 of finite index in Γ , so (ii) implies (iii). We now construct an example in which (iii) holds but (ii) does not. Let J be a finite nonabelian simple group. Let Γ be the direct product of a countable number of copies of J . There are a countable set of surjective projections $\Gamma \rightarrow J$ having distinct kernels, so Γ has infinitely many subgroups of index $\#J$. We claim that Γ satisfies condition Φ_p for all p . To show this, let Γ_0 be an open subgroup of finite index in Γ . By the definition of Γ as a topological group, Γ_0 must

contain a closed normal subgroup H of Γ which is isomorphic to the product of a countable number of copies of J such that Γ/H is isomorphic to the product of a finite number of copies of J . Any homomorphism from J to \mathbf{F}_p must be trivial, since J is a finite nonabelian simple group. Since H is the direct product of copies of J , we conclude that $\text{Hom}_c(H, \mathbf{F}_p)$ contains only the trivial homomorphism. Thus $\text{Hom}_c(\Gamma_0, \mathbf{F}_p) = \text{Hom}_c(\Gamma_0/H, \mathbf{F}_p)$ is finite because Γ_0/H is finite. This proves Γ satisfies condition (iii) but not (ii).

We end this section by showing that one cannot replace the hypothesis of Theorem 1.2(a) by the requirement that Γ satisfy Φ_p for all primes p .

Counterexample 3.2. Let T be the trivial group. Let Γ (resp. G) be the product of a countable (resp. uncountable) number of copies of a fixed nonabelian finite simple group J . Give Γ and G the product topology. It was shown in Proposition 3.1 that Γ satisfies condition Φ_p for all primes p . Each discrete finite quotient G/C of G is a quotient of a finite product of copies of J , and one can find a proper solution of the associated embedding problem (1.2). However, one cannot find a proper solution of the embedding problem (1.1), since G has uncountably many distinct discrete quotients isomorphic to J while Γ does not.

It is an interesting open question whether one can find counterexamples of this kind in which both Γ and G are countably topologically generated.

4. The abelian case.

Throughout this section we will suppose K is a global function field and that D is a finite set of places of K . Let $\Gamma = \Gamma_{K,D}$. To prove Theorem 1.2(c), we need the following description of the topological type of Γ^{ab} .

Theorem 4.1. *As a topological group, Γ^{ab} is isomorphic to $\hat{\mathbf{Z}} \times W$ if D is empty and to $\hat{\mathbf{Z}} \times W \times \prod_{i=1}^{\infty} \mathbf{Z}_p$ otherwise, where W is a finite group and $\hat{\mathbf{Z}}$ is the profinite completion of \mathbf{Z} .*

For lack of a suitable reference we will give a proof of this Theorem. Define J_K^1 to be the group of ideles of norm 1. By class field theory [3, §5-6] we have an exact sequence

$$(4.1) \quad 0 \longrightarrow \frac{J_K^1}{K^* \prod_{v \notin D} O_v^*} \longrightarrow \Gamma^{ab} \xrightarrow{\mu} \hat{\mathbf{Z}} \rightarrow 0$$

in which μ results from restricting automorphisms to the maximal constant field extension of K . Let $C = C_K$ be the smooth projective curve with function field K . Define

$$(4.2) \quad \text{Pic}_D^0(C) = \frac{J_K^1}{K^* \cdot \prod_{v \in D} (1 + \pi_v O_v) \cdot \prod_{v \notin D} O_v^*}$$

where π_v is a uniformizing parameter in O_v . We then have an exact sequence

$$(4.3) \quad 0 \rightarrow \prod_{v \in D} (1 + \pi_v O_v) \rightarrow \frac{J_K^1}{K^* \prod_{v \notin D} O_v^*} \rightarrow \text{Pic}_D^0(C) \rightarrow 0$$

in which $\text{Pic}_D^0(C)$ is a finite abelian group. By [4, Prop. II.10]¹, the multiplicative group $(1 + \pi_v O_v)$ is topologically isomorphic to $\prod_{i=1}^{\infty} \mathbf{Z}_p$ for each place v of K . Since one can find a topological splitting of (4.1) by lifting any generator of $\hat{\mathbf{Z}}$ to the middle term of this sequence, we see from (4.1) and (4.3) that Theorem 4.1 now results from the following Lemma.

Lemma 4.2. *Suppose there is an exact sequence*

$$(4.4) \quad 0 \rightarrow E \rightarrow A \rightarrow B \rightarrow 0$$

of abelian topological groups in which $E = \prod_{i=1}^{\infty} \mathbf{Z}_p$ and B is finite. Then A is topologically isomorphic to a product $E' \times B'$ in which E' is isomorphic to $\prod_{i=1}^{\infty} \mathbf{Z}_p$ and B' is finite.

Proof. The torsion subgroup A_0 of A is finite, and A/A_0 is a torsion free profinite group which is the extension of a finite p -group by E . Since E is a projective object in the category of profinite groups, it will suffice to show that A/A_0 is isomorphic to E . On replacing A by A/A_0 , we can thus reduce to the case in which A is torsion free and B is a finite p -group. By induction on the order of B , we can reduce further to the case in which B has order p . For $j \geq 1$, let $\psi_j : E \rightarrow \mathbf{Z}_p$ be the projection of E onto its j^{th} direct factor. Since A is torsion free, pA is contained in E but not in pE . Hence there is a $j \geq 1$ so that $a \rightarrow \psi_j(pa)$ defines a surjection $\tau : A \rightarrow \mathbf{Z}_p$ inducing an isomorphism $A/E \rightarrow \mathbf{Z}_p/p\mathbf{Z}_p$. This implies the kernel of τ is contained in E , and must in fact be $E' = \prod_{1 \leq i \neq j}^{\infty} \mathbf{Z}_p$. Since the resulting exact sequence of profinite groups

$$0 \rightarrow E' \rightarrow A \xrightarrow{\tau} \mathbf{Z}_p \rightarrow 0$$

must split, we find that A is isomorphic to E .

Proof of Theorem 1.2(c).

We assume G is a profinite abelian group having a countable basis of open neighborhoods of the identity. By Theorem 4.1, the embedding problem (1.1) has the form

$$(4.5) \quad \begin{array}{ccccccc} \Gamma^{ab} = \hat{\mathbf{Z}} \times W \times E & & & & & & \\ & & \downarrow \delta & & & & \\ 1 \leftarrow & T & \leftarrow & G & \leftarrow & A & \leftarrow 0 \\ & \downarrow & & & & & \\ & 1 & & & & & \end{array}$$

¹The authors would like to thank Doug Ulmer for this reference.

in which W is finite and E is the trivial group or is isomorphic to $\prod_{i=1}^{\infty} \mathbf{Z}_p$. We assume that for every open normal subgroup C of G which is contained in A we can solve the embedding problem (1.2). We must show the existence of a map $h : \Gamma^{ab} \rightarrow G$ which lifts the map δ of the embedding problem. It will suffice to construct the restriction of h to each factor of $\Gamma^{ab} = \hat{\mathbf{Z}} \times W \times E$.

Consider first the factor W . The inverse limit of the sets $\text{Hom}(W, G/C) = \text{Hom}_c(W, G/C)$ as C varies is $\text{Hom}_c(W, G)$, where W and $\text{Hom}_c(W, G)$ have the discrete topology. Furthermore, because W and G/C are both finite sets, $\text{Hom}_c(W, G/C)$ is finite. By hypothesis, the subset of $\text{Hom}_c(W, G/C)$ consisting of lifts of the restriction δ_W of δ to W is thus finite and not empty. Hence the inverse limit of these subsets over C is not empty, and a continuous lift $h_W : W \rightarrow G$ of δ_W exists.

For the $\hat{\mathbf{Z}}$ factor, we can construct a continuous lift $h_{\hat{\mathbf{Z}}} : \hat{\mathbf{Z}} \rightarrow G$ of the restriction of δ to $\hat{\mathbf{Z}}$ by choosing any lift to G of the image in T of a topological generator of $\hat{\mathbf{Z}}$.

To deal with the E factor, we let h_E be trivial if E is trivial. Suppose $E = \prod_{i=1}^{\infty} \mathbf{Z}_p$. Since the restriction δ_E of δ to E is continuous, it is trivial on $E_n = \prod_{i=n+1}^{\infty} \mathbf{Z}_p$ for some n . By lifting from T to G images under δ of n topological generators of $\prod_{i=1}^n \mathbf{Z}_p$, we can construct a continuous lift $h'_E : \prod_{i=1}^n \mathbf{Z}_p \rightarrow G$ of the restriction of δ to $\prod_{i=1}^n \mathbf{Z}_p$. Extending h'_E to be trivial on E_n produces a continuous lift $h_E : E \rightarrow G$ of δ_E .

Putting together the lifts h_W , h_E and $h_{\hat{\mathbf{Z}}}$ leads to a continuous lift $h : \Gamma^{ab} \rightarrow G$ of δ . We now suppose that for all C as above, there exists a surjective lifting $h_C : \Gamma^{ab} \rightarrow G/C$. We must show there is a surjective lifting $h_0 : \Gamma^{ab} \rightarrow G$. It will suffice to construct continuous surjections $h' : \Gamma_{p'}^{ab} \rightarrow G_{p'}$ and $h_p : \Gamma_p^{ab} \rightarrow G_p$ which lift the restrictions δ' and δ_p of δ to the prime-to- p part $\Gamma_{p'}^{ab}$ and the p -part Γ_p^{ab} of Γ^{ab} , respectively.

The prime-to- p part of h_C gives a surjection $h'_C : \Gamma_{p'}^{ab} = W_{p'} \times \hat{\mathbf{Z}}_{p'} \rightarrow (G/C)_{p'}$ for each C . There are only finitely many such surjections, since $\Gamma_{p'}^{ab}$ is topologically finitely generated and $(G/C)_{p'}$ is finite. Thus by the usual argument concerning inverse limit of finite sets, there is a surjective continuous lift $h' : \Gamma_{p'} \rightarrow G_{p'}$ of δ' .

We now construct h_p . If E is trivial, then $\Gamma_p^{ab} = W_p \times \mathbf{Z}_p$, and the argument is the same as for h' . Suppose now that E is not trivial, so that $E = \prod_{i=1}^{\infty} \mathbf{Z}_p$. We have constructed above one lift h of δ which is trivial on $E_n = \prod_{i=n}^{\infty} \mathbf{Z}_p$ for some n . The p -primary part A_p of A has a countable basis of open neighborhoods of 0, and is an abelian pro- p group. Hence there is a continuous surjection $\lambda : E_n \rightarrow A_p$. Extend λ to $\Gamma^{ab} = \hat{\mathbf{Z}} \times W \times (\prod_{i=1}^n \mathbf{Z}_p) \times E_n$ by making λ trivial on the other factors of Γ^{ab} . Define $h_p : \Gamma_p^{ab} \rightarrow G_p$ to be the restriction of $h + \lambda$ to Γ_p^{ab} . This h_p also lifts δ_p because λ has image in A . The group $h_p(\Gamma_p^{ab})$ contains $(h + \lambda)(E_n) = \lambda(E_n) = A_p$, and surjects

onto T_p because δ is surjective. Hence $h_p(\Gamma_p^{ab}) = G_p$, which completes the proof of Theorem 1.2(c).

Remark 4.3. In view of Theorem 1.2(c) and Question 1.3, it is natural to ask if all embedding problems (1.1) defined by profinite groups G and Γ having a countable basis of open neighborhoods of the identity are determined by finite quotients. The following example shows this is not the case even when G and Γ are abelian. Let T be the trivial group, $G = \prod_{i=1}^{\infty} \mathbf{Z}_p$, and $\Gamma = \prod_{j=1}^{\infty} (\prod_{s=1}^{\infty} \mathbf{Z}/p^j)$. Then (1.1) has no proper solution, but (1.2) has a proper solution for each open subgroup C of finite index in G .

Acknowledgement. The authors would like to thank the referee for several useful comments.

References

- [1] M. Mazur, *Deforming Galois representations*, in ‘Galois Groups over \mathbf{Q} ,’ Y. Ihara, K. Ribet and J.P. Serre eds., MSRI publications, **16**, Springer-Verlag (1989), 385-437, [MR 90k:11057](#), [Zbl 0714.11076](#).
- [2] J.P. Serre, *Corps Locaux*, Hermann, Paris (1968), [MR 50 #7096](#), [Zbl 0137.02601](#).
- [3] J. Tate, *Global class field theory*, in ‘Algebraic Number Theory,’ J.W.S. Cassels and A. Fröhlich, eds., Academic Press, London (1967), 162-203, [MR 36 #3749](#).
- [4] A. Weil, *Basic Number Theory*, Springer Verlag, New York (1968), [MR 38 #3244](#), [Zbl 0267.12001](#).

Received June 7, 2000 and revised April 9, 2001. The first author was partially supported by NSF grants DMS-9701411 and DMS-0070433.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF PENNSYLVANIA
PHILADELPHIA, PA 19104-6395
E-mail address: ted@math.upenn.edu

DEPARTMENT OF MATHEMATICS
COLUMBIA UNIVERSITY
990 BROADWAY
509 MATHEMATICS BUILDING, MAIL CODE: 4406
NEW YORK, NY 10027
E-mail address: glass@math.columbia.edu

This paper is available via <http://www.pacjmath.org/2002/205-1-2.html>.