

# Projective extensions of fields

Jochen Koenigsmann\*

Freiburg — Konstanz — Basel

## Abstract

A field  $K$  admits proper projective extensions, i.e. Galois extensions where the Galois group is a nontrivial projective group, unless  $K$  is separably closed or  $K$  is a pythagorean formally real field without cyclic extensions of odd degree. As a consequence, it turns out that almost all absolute Galois groups decompose as proper semidirect products.

We show that each local field has a unique maximal projective extension, and that the same holds for each global field of positive characteristic. In characteristic 0, we prove that Leopoldt's conjecture for all totally real number fields is equivalent to the statement that, for all totally real number fields, all projective extensions are cyclotomic. So the realizability of any non-procyclic projective group as Galois group over  $\mathbf{Q}$  produces counterexamples to the Leopoldt conjecture, while the non-realizability may produce counterexamples to the classical inverse Galois problem.

## Contents

<b>1</b>	<b>Projective quotients of profinite groups</b>	<b>3</b>
1.1	Prosimple groups . . . . .	3
1.2	Examples of indecomposable profinite groups . . . . .	5
1.3	Maximal projective quotients . . . . .	9
1.4	Demushkin groups . . . . .	10
<b>2</b>	<b>Projective extensions of arbitrary fields</b>	<b>12</b>

---

\*Heisenberg-Stipendiat der Deutschen Forschungsgemeinschaft (KO 1962/1-2)

<b>3</b>	<b>Projective extensions of local fields</b>	<b>16</b>
<b>4</b>	<b>Projective extensions of global fields</b>	<b>17</b>
4.1	Function fields over finite fields . . . . .	18
4.2	Number fields . . . . .	20

## Introduction

In [K4] it is shown that the absolute Galois group  $G_K := \text{Gal}(K^{\text{sep}}/K)$  of a field  $K$  hardly ever decomposes into a proper direct product  $G_K = G_1 \times G_2$ . In contrast, almost all absolute Galois groups are *semidirect* products (Corollary 2.4). This will be shown by studying *projective* extensions of fields, i.e. Galois extensions  $L/K$  where  $\text{Gal}(L/K)$  is a non-trivial projective (profinite) group.

Recall that a profinite group  $G$  is called projective if all epimorphisms  $\pi : H \twoheadrightarrow G$  split or, equivalently, if all finite embedding problems for  $G$  have solutions (cf. [FJ], chapter 20, or [RZ], section 7.6). Examples of projective groups are free profinite groups, but also the (additive) group  $\mathbf{Z}_p$  of  $p$ -adic integers. Projective groups are always torsion-free. Section 1 contains group-theoretic tools on projective quotients of profinite groups. In particular, we prove that pro- $p$  Demushkin groups have a unique maximal projective quotient (Proposition 1.10).

In many cases it is known that a field  $K$  admits projective extensions. For example, if  $K$  has cyclic Galois extensions of prime degree  $p > 2$  or of degree 4 for  $p = 2$ , then, by a result of Whaples (Theorem 2 in [W]),  $K$  admits  $\mathbf{Z}_p$ -extensions, i.e. Galois extensions  $L/K$  with  $\text{Gal}(L/K) \cong \mathbf{Z}_p$ . In section 2, we will show that this is a general phenomenon: Any field  $K$  admits projective extensions, unless  $K$  is separably closed or  $K$  is a pythagorean formally real field without cyclic extensions of odd degree (Theorem 2.3). And any projective extension  $L/K$  gives rise to a semidirect product decomposition of  $G_K$ , as the canonical exact sequence

$$1 \rightarrow G_L \rightarrow G_K \rightarrow \text{Gal}(L/K) \rightarrow 1$$

splits by the projectivity of  $\text{Gal}(L/K)$ .

It is one of the main open questions in Galois theory to give a group-theoretic characterization of those profinite groups which occur as absolute Galois groups. The most well-known group-theoretic obstruction for a profinite group to be an absolute Galois group, is — by Artin-Schreier theory —

the presence of torsion-elements of order  $> 2$ . The lack of non-trivial projective quotients of a torsion-free profinite group may now be regarded as a new group-theoretic obstruction: there are non-trivial torsion-free profinite (or even pro- $p$ ) groups without non-trivial projective quotients (cf. Example 1.4 and 1.5).

Apart from this general Galois-theoretic observation it can be rewarding to study, for a specific field  $K$  which projective groups can be realized as Galois groups over  $K$ . We made ‘field studies’ on local and global fields (section 3 and 4). The outcome for a (non-archimedean) local field  $K$  is that any projective extension  $L/K$  of  $K$  is wild in the sense that  $L$  is contained in the maximal Galois extension  $K^{wild}$  of  $K$  without tame ramification, and that  $K$  always has a unique maximal projective extension (Proposition 3.1). We prove the same conclusions for global fields of positive characteristic (Proposition 4.2). As consequence for a profinite inverse Galois problem one obtains e.g. that if  $\hat{A}_5$  is the (unique) smallest projective group with quotient  $A_5$  then  $\hat{A}_5$  (a projective group on two generators) is not realizable over any global field of positive characteristic.

For global fields of characteristic 0, i.e. for number fields, we obtain a surprising connection to Leopoldt’s conjecture. Let us, for simplicity, consider a totally real number field  $K$ . Leopoldt’s conjecture then says that for each prime  $p$  there is exactly one  $\mathbf{Z}_p$ -extension of  $K$ , namely the cyclotomic  $\mathbf{Z}_p$ -extension in  $K(\mu_{p^\infty})$ , where  $\mu_{p^\infty}$  is the group of all  $p$ -power roots of unity. It turns out that Leopoldt’s conjecture holds in all totally real number fields iff in all totally real number fields  $K$  the cyclotomic  $\hat{\mathbf{Z}}$ -extension is the unique maximal projective extension of  $K$  (Proposition 4.9). So, for example, if  $\hat{A}_5$  is realizable over  $\mathbf{Q}$  then Leopoldt’s conjecture is false for infinitely many totally real number fields. If not, then there is a good chance that a large finite quotient of  $\hat{A}_5$  is not realizable over  $\mathbf{Q}$ , thus giving a negative answer to the inverse Galois problem.

## 1 Projective quotients of profinite groups

### 1.1 Prosimple groups

We recall that the **Frattini subgroup**  $\Phi(G)$  of a profinite group  $G$  is the intersection of all maximal subgroups of  $G$ . It is the pronilpotent characteristic subgroup of non-generators of  $G$ . We also recall that any profinite group  $G_0$

allows a unique **universal Frattini cover**, i.e. an epimorphism  $\phi : G \twoheadrightarrow G_0$ , where  $G$  is projective and  $\ker \phi \subseteq \Phi(G)$  (cf. [CKK] or [FJ], sections 20.6 and 20.7). If  $G_0$  is a finite simple group, this implies  $\ker \phi = \Phi(G)$ . We say that a profinite group  $G$  is **prosimple**<sup>1</sup> if  $G$  is projective and  $G_0 := G/\Phi(G)$  is a finite simple group, i.e.  $G$  is the universal Frattini cover of  $G_0$ .

Any prosimple group occurs naturally as absolute Galois group, not only because, by [LvD], any projective profinite group is the absolute Galois group of some PAC-field, but also by the following canonical construction:

**Example 1.1** *Let  $G_0$  be a finite simple group, let  $L/K$  be a Galois extension of number fields with  $\text{Gal}(L/K) \cong G_0$ , and let  $F$  be a maximal algebraic extension of  $K$  such that  $\text{Gal}(LF/F) \cong G_0$ . Then  $G := G_F$  is prosimple with  $G/\phi(G) \cong G_0$  or  $G \cong G_0 \cong \mathbf{Z}/2\mathbf{Z}$ .*

**Proof:**  $\Phi(G_F) = G_{LF}$ , because any minimal proper algebraic extension  $F'/F$  is contained in  $LF$ : otherwise  $F' \cap LF = F$  and so  $\text{Gal}(LF'/F') \cong \text{Gal}(LF/F) \cong G_0$ , contradicting the maximality of  $F$ .

Now assume that  $G_F \not\cong \mathbf{Z}/2\mathbf{Z}$ . We have to show that  $G_F$  is projective. If  $G_0$  is abelian, i.e.  $\cong \mathbf{Z}/p\mathbf{Z}$  for some prime  $p$ , then, as the rank of  $G_F$  is the rank of the Frattini quotient  $G_F/\Phi(G_F) \cong G_0$ ,  $G_F$  is procyclic, and pro- $p$ , and, by Artin-Schreier, torsion-free. So  $G_F \cong \mathbf{Z}_p$  which is projective. If  $G_0$  is non-abelian, it has no proper abelian quotient, and this property is inherited by  $G_F$  (any minimal proper quotient of  $G_F$  is a quotient of  $G_0$ ). So  $F$  contains the maximal prosolvable extension  $\mathbf{Q}^{sol}$  of  $\mathbf{Q}$ . But  $G_{\mathbf{Q}^{sol}}$  is projective and then so is the subgroup  $G_F$ . **q.e.d.**

We say that a profinite group  $G$  **decomposes as proper semidirect product**, if there is a nontrivial proper normal subgroup  $N \triangleleft G$  having a complement in  $G$ , i.e. a subgroup  $H \leq G$  with  $G = NH$  and  $N \cap H = 1$ . In this case we write  $G = N \rtimes H$ .

**Lemma 1.2** *Let  $G$  be a profinite group such that  $G_0 := G/\Phi(G)$  is a finite simple group. Then:*

(a) *Any proper normal subgroup  $N \triangleleft G$  is contained in  $\Phi(G)$ . In particular,  $G$  does not decompose as proper semidirect product.*

---

<sup>1</sup>There will be no confusion with the standard terminology of a pro- $\star$  group being a projective limit of finite  $\star$ -groups: there is no non-constant inverse system of finite simple groups.

- (b)  $\#G_0$  and  $\#G$  have the same prime divisors.  
(c)  $G$  is of rank at most 2.

**Proof:** (a) Choose some maximal subgroup  $U$  of  $G$  containing  $N$  and let  $M$  be the intersection of the conjugates of  $U$  in  $G$ . Then  $M$  is a proper normal subgroup of  $G$  with  $N \subseteq M$  and  $\Phi(G) \subseteq M$ . As  $G/\Phi(G)$  is simple, this implies  $\Phi(G) = M$ , and so  $N \subseteq \Phi(G)$ .

If  $G = N \rtimes H$  then  $G = NH = \Phi(G)H = H$ , as  $\Phi(G)$  is the set of nongenerators of  $G$ . Hence  $N = 1$ .

(b) Assume there is a prime  $p$  with  $p \mid \#G$  but  $p \nmid \#G_0$ . Let  $P$  be a  $p$ -Sylow subgroup of  $G$ . Then  $P$  is the unique characteristic  $p$ -Sylow subgroup of  $\Phi(G)$ , and hence  $P$  is normal in  $G$ . Thus, by the well-known Zassenhaus theorem,  $P$  has a complement  $H$  in  $G$ . But then any maximal subgroup  $M$  of  $G$  containing  $H$  has  $p$ -power index in  $G$ , and so  $p \mid [G : M] \mid \#G_0$ : contradiction.

(c) follows from the classification of finite simple groups  $G_0$ : they all have rank 2 in the nonabelian case. **q.e.d.**

Prosimple groups can now be characterized in terms of semidirect products:

**Lemma 1.3** *Let  $G$  be a nontrivial projective profinite group. Then  $G$  has a prosimple quotient. In particular,  $G$  is prosimple iff  $G$  does not decompose as proper semidirect product.*

**Proof:** Let  $G_0$  be a finite simple quotient of  $G$  and let  $G'$  be the universal Frattini cover of  $G_0$ . Then, by [FJ], Proposition 20.33(c), there is an epimorphism  $\pi : G \twoheadrightarrow G'$ , i.e.  $G'$  is a prosimple quotient of  $G$ . As  $G'$  is projective, the epimorphism  $\pi : G \twoheadrightarrow G'$  splits, so there is a subgroup  $H \leq G$  which maps isomorphically onto  $G'$  via  $\pi$ . So  $G = N \rtimes H$ , where  $N = \ker \pi$ .

If  $G$  is not prosimple, then  $N$  is nontrivial, and  $G$  decomposes as proper semidirect product.

If  $G$  is prosimple, then, by Lemma 1.2(a),  $G$  does not decompose as proper semidirect product. **q.e.d.**

## 1.2 Examples of indecomposable profinite groups

If one drops projectivity one still finds other torsion-free profinite groups which do not decompose as proper semidirect product (as we will see in

Corollary 2.4 such groups cannot occur as absolute Galois groups):

**Example 1.4** *Let  $H$  be a non-abelian prosimple group such that all Sylow subgroups of  $H/\Phi(H)$  are abelian (e.g. the prosimple group with Frattini quotient  $A_5$ ). Let  $G := H/[\Phi(H), \Phi(H)]$ . Then  $G$  is a non-projective torsion-free profinite group which does not decompose as proper semidirect product.*

**Proof:**  $G/\Phi(G) \cong H/\Phi(H)$  is a finite simple group, so, by Lemma 1.2(a),  $G$  does not decompose as proper semidirect product.

Let  $\mathcal{P}$  be the (finite) set of primes for which  $H$  (or, by Lemma 1.2(b), equivalently  $H/\Phi(H)$ ) has non-trivial  $p$ -Sylow subgroups. For each  $p \in \mathcal{P}$  choose a  $p$ -Sylow subgroup  $H_p$  of  $H$  and let  $Q_p := H_p \cap \Phi(H)$ . Then  $Q_p$  is a  $p$ -Sylow subgroup of  $\Phi(H)$ . As  $\Phi(H)$  is nilpotent,  $Q_p$  is the unique characteristic  $p$ -Sylow subgroup of  $\Phi(H)$ , and hence normal in  $H$ . As  $H$  is projective,  $H_p$  is a free pro- $p$  group, say of rank  $r_p$ .

The rank  $r_p$  is finite because the canonical epimorphism

$$H \twoheadrightarrow^p H := H / \prod_{q \neq p} Q_q$$

maps  $H_p$  isomorphically onto an open subgroup of  ${}^p H$ . By Lemma 1.2(c), the rank of  $H$  is 2, so the rank of  ${}^p H$  is  $\leq 2$ , and so any open subgroup has finite rank. And, as open subgroup of the free pro- $p$  group  $H_p$ ,  $Q_p$  is again a free pro- $p$  group of finite rank  $s_p \geq r_p$  (by the Nielsen-Schreier Theorem, cf. e.g. [RZ], Theorem 3.6.2). Note that there is some  $p_0 \in \mathcal{P}$  with  $r_{p_0} > 1$  because in the non-abelian simple group  $H/\Phi(H)$  at least one Sylow subgroup is non-cyclic (finite groups with cyclic Sylow subgroups are metacyclic, cf. e.g. [H], Satz IV.2.11).

$\Phi(G)$  is the abelianization of  $\Phi(H) = \prod_{p \in \mathcal{P}} Q_p$ , so

$$\Phi(G) \cong \prod_{p \in \mathcal{P}} \mathbf{Z}_p^{s_p}.$$

This implies that  $G$  is not projective:  $cd_{p_0}(G) \geq cd_{p_0} \Phi(G) = s_{p_0} \geq r_{p_0} > 1$ .

In order to check that  $G$  is torsion-free it suffices to check this for all Sylow subgroups of  $G$ . Since  $[\Phi(H), \Phi(H)] \cap H_p = [Q_p, Q_p]$ , the  $p$ -Sylow subgroups  $G_p$  of  $G$  are of the shape  $G_p \cong H_p/[Q_p, Q_p]$ . The subgroup  $\overline{Q}_p := Q_p/[Q_p, Q_p]$  of  $G_p$  is torsion-free: it is an abelianization of the free pro- $p$  group  $Q_p$  of rank  $s_p$  isomorphic to  $\mathbf{Z}_p^{s_p}$ . On the other hand, the epimorphism

$$\psi_p : G_p \twoheadrightarrow H_p/[H_p, H_p] \cong \mathbf{Z}_p^{r_p}$$

has  $\ker \psi_p \subseteq \overline{Q_p}$  because, by assumption, the  $p$ -Sylow subgroup  $H_p/Q_p$  of  $H/\Phi(H)$  is abelian. But this means that  $\psi_p$  maps any  $x \in G_p \setminus \overline{Q_p}$  to a non-zero element of  $\mathbf{Z}_p^{r_p}$ , which implies that  $x$  is not torsion. **q.e.d.**

There is even a pro- $p$  example <sup>2</sup>:

**Example 1.5** *Let  $p$  be a prime, let  $n$  be an integer  $\geq 3$ , and let  $G$  be the first congruence subgroup of  $SL_n(\mathbf{Z}_p)$ , i.e. the kernel of the canonical epimorphism*

$$\pi_1 : SL_n(\mathbf{Z}_p) \twoheadrightarrow SL_n(\mathbf{F}_p).$$

*Then  $G$  is a non-procyclic torsion-free pro- $p$  group which does not decompose as proper semidirect product.*

**Proof:** Let  $\Gamma_n(\mathbf{Z}_p)$  be the first congruence subgroup of  $GL_n(\mathbf{Z}_p)$ , i.e. the kernel of the canonical epimorphism  $GL_n(\mathbf{Z}_p) \twoheadrightarrow GL_n(\mathbf{F}_p)$ . Then

$$G = \Gamma_n(\mathbf{Z}_p) \cap SL_n(\mathbf{Z}_p),$$

and one has the following well-known facts:

**Fact 1:**  $\Gamma_n(\mathbf{Z}_p)$  is a torsion-free pro- $p$  group.

**Fact 2:** All normal subgroups of  $SL_n(\mathbf{Z}_p)$  of infinite index are central, i.e. contained in the center of  $SL_n(\mathbf{Z}_p)$ .

Fact 1 clearly implies that  $G$  is a torsion-free pro- $p$  group as well. And Fact 2 implies that  $G$  is **just infinite**, i.e. all proper quotients of  $G$  are finite, because the center of  $SL_n(\mathbf{Z}_p)$  has trivial intersection with  $G$ . Since  $G$  is obviously not procyclic, this proves everything.

*ad Fact 1:* Let  $1_n$  be the identity matrix of size  $n$ . Then

$$\Gamma_n(\mathbf{Z}_p) = 1_n + pM_n(\mathbf{Z}_p) \cong \varprojlim_k (1_n + pM_n(\mathbf{Z}/p^k\mathbf{Z})).$$

Since  $\sharp(1_n + pM_n(\mathbf{Z}/p^k\mathbf{Z})) = \sharp M_n(\mathbf{Z}/p^k\mathbf{Z}) = p^{kn^2}$ ,  $\Gamma_n(\mathbf{Z}_p)$  is a pro- $p$  group.

Any nontrivial  $A \in \Gamma_n(\mathbf{Z}_p)$  can be written (uniquely) as  $A = 1_n + p^m B$  with  $m \geq 1$  and  $B \in M_n(\mathbf{Z}_p) \setminus pM_n(\mathbf{Z}_p)$ . So

$$A^p = 1_n + p^{m+1}B + p^{m+2}C \neq 1_n$$

for some  $C \in M_n(\mathbf{Z}_p)$ . Hence  $\Gamma_n(\mathbf{Z}_p)$  contains no elements of order  $p$ , and therefore (as pro- $p$  group) no torison elements at all.

---

<sup>2</sup>I would like to thank Marcus du Sautoy for pointing out this example to me

*ad Fact 2:*  $SL_n(\mathbf{Z})$  is dense in  $SL_n(\mathbf{Z}_p)$ , since the natural homomorphism  $SL_n(\mathbf{Z}) \rightarrow SL_n(\mathbf{Z}/p^k\mathbf{Z})$  is surjective for each  $k \in \mathbf{N}$  (cf. e.g. [RZ], p. 158). So for any open normal subgroup  $N \triangleleft SL_n(\mathbf{Z}_p)$ , one has  $SL_n(\mathbf{Z}_p)/N \cong SL_n(\mathbf{Z})/SL_n(\mathbf{Z}) \cap N$ .

Consider for each  $k \geq 1$  the canonical epimorphisms  $\pi_k$  and  $\hat{\pi}_k$ :

$$\begin{array}{ccc} SL_n(\mathbf{Z}_p) & \xrightarrow{\hat{\pi}_k} & SL_n(\mathbf{Z}_p/p^k\mathbf{Z}_p) \\ \uparrow & & \parallel \\ SL_n(\mathbf{Z}) & \xrightarrow{\pi_k} & SL_n(\mathbf{Z}/p^k\mathbf{Z}) \end{array}$$

and define the (open normal) congruence subgroups

$$\begin{aligned} G^k(\mathbf{Z}_p) &:= \ker \hat{\pi}_k & \text{and} & & G_\star^k(\mathbf{Z}_p) &:= \hat{\pi}_k^{-1}(C(SL_n(\mathbf{Z}_p/p^k\mathbf{Z}_p))) \\ G^k(\mathbf{Z}) &:= \ker \pi_k & \text{and} & & G_\star^k(\mathbf{Z}) &:= \pi_k^{-1}(C(SL_n(\mathbf{Z}/p^k\mathbf{Z}))), \end{aligned}$$

where  $C(\star)$  denotes the center of  $\star$ . Then, obviously, the  $G^k$  form a neighbourhood of 1 for the  $p$ -adic topology on  $SL_n$ , and the bottom groups are the intersection of the top groups with  $SL_n(\mathbf{Z})$ . Note also, that for any commutative ring  $R$ , the center of  $SL_n(R)$  consists of scalar matrices  $\zeta \cdot 1_n$  with  $\zeta$  an  $n$ -th root of unity in  $R$ . In particular,

$$G_\star^k(\mathbf{Z}_p) \cap G_\star^{k+1}(\mathbf{Z}_p) = G_\star^{k+1}(\mathbf{Z}_p) \cdot C(SL_n(\mathbf{Z}_p)).$$

Now it follows from [Mc], that for each open normal subgroup  $N \triangleleft SL_n(\mathbf{Z}_p)$  there is a unique  $k = k(N)$  with

$$G^k(\mathbf{Z}_p) \subseteq N \subseteq G_\star^k(\mathbf{Z}_p).$$

Indeed, let  $k$  be minimal with  $G^k(\mathbf{Z}_p) \subseteq N$ . Then  $G^k(\mathbf{Z}) \subseteq N \cap SL_n(\mathbf{Z}) \not\subseteq G^{k-1}(\mathbf{Z})$ . Hence, by the main Theorem and (1.1) of [Mc] (cf. also [BLS]),  $N \cap SL_n(\mathbf{Z}) \subseteq G_\star^k(\mathbf{Z})$  and so  $N \subseteq G_\star^k(\mathbf{Z}_p)$ . It is for this result of Mennicke that the assumption  $n \geq 3$  is needed.

Finally, assume that  $N \triangleleft SL_n(\mathbf{Z}_p)$  is of *infinite* index. Then there is a properly descending chain  $N_1 \supset N_2 \supset \dots$  of open normal subgroups of  $SL_n(\mathbf{Z}_p)$  with  $N = \bigcap N_i$ . Hence the  $k(N_i)$  get arbitrarily large, i.e.  $N \subseteq \bigcap_{k=1}^{\infty} G_\star^k(\mathbf{Z}_p) = C(SL_n(\mathbf{Z}_p))$ . **q.e.d.**

### 1.3 Maximal projective quotients

**Observation 1.6** *Let  $G$  be a profinite group. Then  $G$  has a maximal projective quotient, i.e. a minimal normal subgroup  $N \triangleleft G$  s.t.  $G/N$  is projective.*

**Proof:** Projectivity can be expressed in terms of finite embedding problems: A profinite group  $G$  is projective iff for any pair of epimorphisms  $\alpha : A \twoheadrightarrow B$ ,  $\beta : G \twoheadrightarrow B$  there is a homomorphism  $\gamma : G \rightarrow A$  with  $\beta = \alpha \circ \gamma$  (cf. e.g. [RZ], Prop. 7.5.4).

There is always the trivial projective quotient  $G/G$ . And if  $\mathcal{N}$  is a family of normal subgroups  $N \triangleleft G$  such that  $G/N$  is projective and  $\mathcal{N}$  is linearly ordered by inclusion, then  $G/\bigcap_{N \in \mathcal{N}} N$  is again projective, since any finite embedding problem for this group factors through some (in fact almost all)  $G/N$  with  $N \in \mathcal{N}$ . By Zorn's Lemma this implies existence of a maximal projective quotient. **q.e.d.**

Note that for a non-trivial maximal projective quotient  $G/N$  it may happen that  $cd N = cd G < \infty$ . For example, if  $H$  is a group with  $1 < cd H < \infty$  but without proper projective quotient (e.g. the group constructed in Example 1.4 or 1.5) then  $G := H \star \hat{\mathbf{Z}}$  with  $N$  the normal subgroup of  $G$  generated (as such) by  $H$  has this property.

If  $G$  is projective,  $G$  is its own unique maximal projective quotient. In general, however, maximal projective quotients are not unique. For example, if  $G = \hat{\mathbf{Z}} \times \hat{\mathbf{Z}}$  there are  $\aleph_1$  many distinct maximal projective quotients, all isomorphic to  $\hat{\mathbf{Z}}$ : any subset  $S \subseteq \mathbf{P} := \{p \mid p \text{ prime}\}$  gives rise to a quotient of the form  $\prod_{p \in S} \mathbf{Z}_p \times \prod_{q \in \mathbf{P} \setminus S} \mathbf{Z}_q$ .

For non-projective groups one has the following

**Observation 1.7** *Let  $G$  be a non-projective group and let  $\bar{G} = G/N$  be a projective quotient of  $G$ . Then  $N \not\subseteq \Phi(G)$ .*

**Proof:** Since  $\bar{G}$  is projective, the canonical epimorphism  $\pi : G \twoheadrightarrow \bar{G}$  has a section  $\rho : \bar{G} \rightarrow G$ , and so  $G = N \rtimes \rho(\bar{G})$ . Assume  $N \subseteq \Phi(G)$ . Then  $G = N \rtimes \rho(\bar{G}) = \Phi(G) \cdot \rho(\bar{G})$ . Since  $\Phi(G)$  is the group of non-generators of  $G$  this implies that  $G = \rho(\bar{G}) \cong \bar{G}$ . But  $\bar{G}$  is projective and  $G$  is not. **q.e.d.**

**Corollary 1.8** *Let  $G$  be a non-projective pro- $p$  group of finite rank, and let  $\bar{G} = G/N$  be a projective quotient of  $G$ . Then  $rk \bar{G} < rk G$ .*

**Proof:** Let  $\pi : G \twoheadrightarrow \overline{G}$  be the canonical epimorphism. As  $G$  is pro- $p$ ,  $\Phi(G) = \langle G^p, [G, G] \rangle$ , and so  $\pi(\Phi(G)) = \Phi(\overline{G})$ . Hence  $\pi$  canonically induces an epimorphism of Frattini quotients

$$\pi_\Phi : G/\Phi(G) \twoheadrightarrow \overline{G}/\Phi(\overline{G})$$

(cf. e.g. [RZ], Lemma 2.8.7 and Corollary 2.8.8). Since, by the observation,  $N \not\subseteq \Phi(G)$  this epimorphism is not injective. So

$$rk G = \dim_{\mathbf{F}_p} G/\Phi(G) < \dim_{\mathbf{F}_p} \overline{G}/\Phi(\overline{G}) = rk \overline{G}.$$

**q.e.d.**

Note that the Corollary does, in general, not hold if  $G$  is not pro- $p$ : For example, if  $p$  and  $q$  are primes with  $p \mid q - 1$ , if

$$G = (\langle \rho \rangle \times \langle \sigma \rangle) \rtimes \langle \tau \rangle$$

with  $N = \langle \rho \rangle \cong \langle \tau \rangle \cong \mathbf{Z}_p$ ,  $\langle \sigma \rangle \cong \mathbf{Z}_q$ ,  $\rho^\tau = \rho$  and  $\sigma^\tau = \zeta_p \cdot \sigma$  then  $rk G = rk G/N = 2$ ,  $G/N$  is projective, but  $G$  is not.

Another consequence of Observation 1.7 is the next

**Corollary 1.9** *Let  $G$  be a non-projective pro- $p$  group with  $G^{ab}$  torsion-free. Then  $G$  has distinct maximal projective quotients.*

**Proof:** Let  $\overline{G} = G/N$  be a maximal projective quotient of  $G$ . Then, by Observation 1.7,  $N \not\subseteq \Phi(G)$ . Pick  $\nu \in N \setminus \Phi(G)$ , let  $\alpha : G \rightarrow G^{ab}$  be the abelianization of  $G$  and observe that  $\alpha(\nu) \neq 1$ . By assumption,  $G^{ab}$  is torsion-free, and so  $\langle \alpha(\nu) \rangle \cong \mathbf{Z}_p$ . The (nontrivial) image of  $\langle \nu \rangle$  in the (elementary abelian) Frattini quotient has a complement which lifts to a complement  $M$  of  $\langle \alpha(\nu) \rangle$  in  $G^{ab}$ . Hence  $\alpha^{-1}(M)$  is a normal subgroup of  $G$  with projective quotient  $G' := G/\alpha^{-1}(M) \cong \mathbf{Z}_p$ . But  $\alpha^{-1}(M) \not\subseteq N$ , because  $\nu \in N \setminus \alpha^{-1}(M)$ , and so any maximal projective quotient of  $G$  above  $G'$  differs from  $\overline{G}$ . **q.e.d.**

## 1.4 Demushkin groups

If  $G^{ab}$  is not torsion-free, the Corollary above may become false. A prominent example which we will need in section 3 are Demushkin groups. Recall that a finitely generated pro- $p$  group  $G$  is called a (pro- $p$ ) **Demushkin group** if

- $cd_p G = 2$
- $H^2(G) \cong \mathbf{Z}/p\mathbf{Z}$  and
- the cup product  $H^1(G) \times H^1(G) \xrightarrow{\cup} H^2(G)$  is a non-degenerate bilinear form

(Here  $H^i(G)$  is the  $i$ -th cohomology group  $H^i(G, \mathbf{Z}/p\mathbf{Z})$ ). Pro- $p$  Demushkin groups occur as maximal pro- $p$  quotients of the absolute Galois groups of local fields of mixed characteristic  $(0, p)$  containing a primitive  $p$ -th root of unity. We shall need two facts:

*If  $G$  is a Demushkin group of rank  $n$  then*

$$G^{ab} \cong (\mathbf{Z}/p^{s_G}\mathbf{Z}) \times \mathbf{Z}_p^{n-1},$$

where  $s_G$  is an integer  $\geq 1$  or  $s_G = \infty$  (and then  $\mathbf{Z}/p^s\mathbf{Z} := \mathbf{Z}_p$ ). Pro- $p$  Demushkin groups are classified up to isomorphism by these two invariants  $n$  and  $s_G$  (cf. e.g. [NSW], p. 185 ff).

*If  $G$  is a Demushkin group of rank  $n > 1$  with  $s_G < \infty$ , and if  $H$  is an open subgroup of  $G$  then  $H$  is a Demushkin group of rank  $2 + [G : H](n - 2)$  with  $s_H < \infty$  (cf. [NSW], Theorem 3.9.15).*

Now we can prove the following

**Proposition 1.10** *Let  $G$  be a pro- $p$  Demushkin group of rank  $n > 1$  with  $s_G < \infty$ . Then  $G$  has a unique maximal projective quotient (of rank  $n - 1$ ).*

**Proof:** For any pro- $p$  Demushkin group  $D$  of rank  $d$  with  $s_D < \infty$  let  $\alpha_D : D \rightarrow D^{ab} \cong (\mathbf{Z}/p^{s_D}\mathbf{Z}) \times \mathbf{Z}_p^{d-1}$  be the abelianization of  $D$  and define

$$\Phi^{free}(D) := \Phi(D) \cdot \alpha_D^{-1}(\mathbf{Z}/p^{s_D}\mathbf{Z}).$$

Then  $[D : \Phi^{free}(D)] = p^{d-1}$  and so  $\Phi^{free}(D)$  is a Demushkin group of rank  $2 + p^{d-1}(d-2)$  with  $s_{\Phi^{free}(D)} < \infty$ . Note also, that  $\Phi^{free}(D)$  is a characteristic subgroup of  $D$ .

Now let  $\Phi^1 = \Phi^{free}(G)$  and for  $i \geq 1$ , let  $\Phi^{i+1} = \Phi^{free}(\Phi^i)$ . Then the  $\Phi^i$  form a chain of characteristic open subgroups of  $G$ :

$$G \triangleright \Phi^1 \triangleright \Phi^2 \triangleright \dots$$

Observe that for each  $i \geq 1$ :

$$rk \Phi^i / \Phi^{i+1} = 1 + [G : \Phi^i](n - 2).$$

This is because  $\Phi^i$  is a Demushkin group of rank  $d = 2 + [G : \Phi^i](n - 2)$  and  $[\Phi^i : \Phi^{i+1}] = p^{d-1}$ , so  $\Phi^i/\Phi^{i+1}$  is of rank  $d - 1$ .

Let  $N = \bigcap_{i=1}^{\infty} \Phi^i$ . Then  $\overline{G} := G/N$  is a quotient of  $G$  with characteristic open subgroups  $\overline{\Phi}^i := \Phi^i/N$  such that  $\Phi(\overline{G}) = \overline{\Phi}^1$ ,  $\Phi(\overline{\Phi}^i) = \overline{\Phi}^{i+1}$  (for  $i \geq 1$ ) and  $\bigcap_{i=1}^{\infty} \overline{\Phi}^i = 1$ . Then

$$rk \overline{G} = rk \overline{G}/\overline{\Phi}^1 = rk G/\Phi^1 = n - 1$$

and for each  $i \geq 1$ ,

$$rk \overline{\Phi}^i = rk \overline{\Phi}^i/\overline{\Phi}^{i+1} = rk \Phi^i/\Phi^{i+1} = 1 + [G : \Phi^i](n - 2) = 1 + [\overline{G} : \overline{\Phi}^i](rk \overline{G} - 1).$$

This means that the Nielsen-Schreier index formula holds for all the subgroups  $\overline{\Phi}^i$  of  $\overline{G}$ , and therefore for all open subgroups of  $\overline{G}$  (each open subgroup contains some  $\overline{\Phi}^i$ , and if the Nielsen-Schreier index formula holds for some open normal subgroup of a profinite group then it holds for any larger open subgroup as well). By Theorem 8.4.7 of [RZ] this implies that  $\overline{G}$  is free pro- $p$ , i.e. projective.

As  $\overline{G}$  is, by Corollary 1.8, a projective quotient of maximal possible rank, it is maximal: any epimorphism between free pro- $p$  groups of the same finite rank is an isomorphism.

Now let  $G' := G/N'$  be an arbitrary projective quotient of  $G$  with projection  $\pi : G \rightarrow G'$ . Then  $G'^{ab}$  is free abelian and so  $\Phi^1 = \Phi^{free}(G) \subseteq \pi^{-1}(\Phi(G'))$ . Since  $\Phi(G')$  is again projective we may continue like this to see that  $\Phi^2 \subseteq \pi^{-1}(\Phi(\Phi(G')))$ , and, more generally,  $\Phi^i \subseteq \pi^{-1}(\Phi_i(G'))$ , where  $\Phi_i(G')$  is the  $i$ -th iteration of applying Frattini to  $G'$ . Hence

$$N = \bigcap_{i=1}^{\infty} \Phi^i \subseteq \bigcap_{i=1}^{\infty} \pi^{-1}(\Phi_i(G')) = \pi^{-1}\left(\bigcap_{i=1}^{\infty} \Phi_i(G')\right) = N'.$$

**q.e.d.**

## 2 Projective extensions of arbitrary fields

Let us first recall Whaples' criterion for the existence of  $\mathbf{Z}_p$ -extensions. We shall use the following terminology: for a field  $K$  and a prime  $p$ ,  $K(p)$  denotes the maximal pro- $p$  Galois extension of  $K$  and  $G_K(p)$  its Galois group.

**Fact 2.1 ([W], Theorem 2)**

(a) Assume that  $G_K(p)$  is non-trivial. Then  $\mathbf{Z}_p$  is a quotient of  $G_K(p)$  unless  $p = 2$ , and  $K$  is formally real and pythagorean.

(b)  $K$  is formally real and pythagorean iff  $K$  admits cyclic extensions of degree 2, but none of degree 4.

**Corollary 2.2** *If  $G_K(p)$  is not procyclic, it is a non-trivial semidirect product.*

**Proof:** If  $p = 2$  and  $K$  is formally real then  $G_K(2) \cong G_{K(\sqrt{-1})}(2) \rtimes \mathbf{Z}/2\mathbf{Z}$ . This is a non-trivial semidirect product unless  $K(\sqrt{-1}) = K(2)$  and so  $G_K(2) \cong \mathbf{Z}/2\mathbf{Z}$  is procyclic. If  $p > 2$  or if  $K$  is not formally real, then, by the fact,  $G_K(p)$  has a  $\mathbf{Z}_p$ -quotient, so for some Galois subextension  $L/K$  of  $K(p)/K$ ,  $\text{Gal}(L/K) \cong \mathbf{Z}_p$ . As  $\mathbf{Z}_p$  is projective, the canonical epimorphism  $G_K(p) \twoheadrightarrow \text{Gal}(L/K)$  splits, and  $G_K(p) \cong G_L \rtimes \text{Gal}(L/K)$ , which, again is a non-trivial semidirect product unless  $L = K(p)$ , and so  $G_K(p) \cong \mathbf{Z}_p$  is procyclic. **q.e.d.**

**Theorem 2.3** *Let  $K$  be a field which is not separably closed. Then  $G_K$  has a prosimple quotient unless  $K$  is a pythagorean formally real field without cyclic extensions of odd degree.*

**Proof:** We may assume that  $\text{char } K = 0$ : if  $\text{char } K = p > 0$  one easily constructs a valued field  $(F, v)$  of characteristic 0 with  $v$  extending the  $p$ -adic valuation on  $\mathbf{Q}$  and with residue field  $Fv = K$ ; passing to the henselisation we may take  $v$  to be henselian and use the fact that then the canonical projection  $G_F \twoheadrightarrow G_{Fv} = G_K$  splits (by [KPR]).

If  $K$  admits cyclic Galois extensions of degree  $d > 2$  we may choose  $d$  to be a prime  $> 2$  or  $d = 4$ . Then, by Proposition 2.1,  $G_K(p)$  and hence  $G_K$  has a quotient  $\mathbf{Z}_p$  for some prime  $p$ .

If  $K$  admits cyclic extensions of order 2 but of no larger order then, again by Proposition 2.1,  $K$  is a pythagorean formally real field not allowing cyclic extensions of odd degree, i.e. we are in the ‘unless’ situation and nothing need be proved.

So it remains to consider the case that  $K$  is radically closed, i.e. that  $K = K^{ab}$ .

If  $K$  is algebraic over  $\mathbf{Q}$ , then  $\mathbf{Q}^{sol} \subseteq K$ . That implies that all completions of  $K$  are algebraically closed, and so, by the local global principle for the

Brauer group,  $G_K$  is projective and we may apply Lemma 1.3 to obtain a prosimple quotient of  $G_K$ .

If  $K$  is not algebraic over  $\mathbf{Q}$ , we denote the relative algebraic closure of  $\mathbf{Q}$  in  $K$  by  $K^{alg}$  which will be, again, radically closed and hence projective. If  $K^{alg}$  is not algebraically closed then, by what we have just seen,  $G_{K^{alg}}$  has a prosimple quotient which is a quotient of  $G_K$  as well via the canonical projection  $G_K \twoheadrightarrow G_{K^{alg}}$ .

If  $K^{alg}$  is algebraically closed we may choose a maximal algebraically closed subfield  $K_0$  of  $K$  and choose some  $t \in K \setminus K_0$ . Then the relative algebraic closure  $L$  of  $K_0(t)$  in  $K$  is not algebraically closed, but  $G_L$  is projective since  $G_{K_0(t)}$  is projective (in fact, a free profinite group of rank  $\sharp K_0$ , cf. [D]). By the same procedure as above we obtain a prosimple quotient of  $G_L$  and take it as quotient of  $G_K$  via the restriction epimorphism  $G_K \twoheadrightarrow G_L$ . **q.e.d.**

**Corollary 2.4** *Let  $K$  be a field. Then  $G_K$  decomposes as proper semidirect product iff  $K$  is not separably closed, not real closed and  $G_K$  is not prosimple.*

**Proof:** This is immediate from the previous Theorem: if  $K$  is formally real then  $G_K = G_{K(\sqrt{-1})} \rtimes \mathbf{Z}/2\mathbf{Z}$ , and this is a proper semidirect product unless  $K$  is real closed. If  $K$  is non-real, then  $G_K$  has prosimple quotients which are proper unless  $G_K$  is prosimple. By projectivity, any such quotient gives rise to a semidirect product decomposition of  $G_K$ . **q.e.d.**

The exceptional case in Theorem 2.3 that  $K$  is a pythagorean formally real field without cyclic extensions of odd degree, can be characterized in purely Galois-theoretic terms. To do this, let us denote the maximal abelian resp. prosolvable extension of  $K$  by  $K^{ab}$  resp.  $K^{solv}$ , and the corresponding maximal abelian resp. prosolvable quotient of  $G_K$  by  $G_K^{ab} := Gal(K^{ab}/K) = G_K/[G_K, G_K]$  resp.  $G_K^{solv} := Gal(K^{solv}/K)$ .

**Lemma 2.5** *For any field  $K$  the following conditions are equivalent:*

1.  $K$  is a pythagorean formally real field not allowing cyclic extensions of odd degree  $> 1$
2.  $G_K^{ab}$  is of exponent 2
3.  $G_K^{solv}$  is non-trivial and generated by involutions.

**Proof:** The equivalence of 1 and 2 follows from Fact 2.1(b) and the fact that  $K$  has no cyclic extensions of odd degree iff  $G_K^{ab}$  is a pro-2 group.

3  $\Rightarrow$  2 follows as  $G_K^{ab}$  is a quotient of  $G_K^{sol}$ : if the latter is generated by involutions then so is the former. But non-trivial abelian groups generated by involutions are of exponent 2. And  $G_K^{ab}$  is non-trivial because  $G_K^{sol}$  is.

1  $\Rightarrow$  3: Assume 1. Let  $K^{t.r.}$  be the maximal totally real algebraic extension of  $K$ , i.e. the intersection of all real closures of  $K$ . Then  $K^{t.r.}/K$  is a Galois extension and, hence so is  $L/K$ , where  $L := K^{t.r.} \cap K^{sol}$ . If  $L \neq K$ , then there is a cyclic subextension  $L'/K$  of  $L/K$  of prime degree  $p$ . By 1,  $K$  has no cyclic extensions of odd degree, so  $p = 2$ , and  $L' = K(\sqrt{d})$  for some  $d \in K \setminus K^2$ . As  $L'/K$  is totally real,  $d$  must be a sum of squares in  $K$ , and hence, by pythagoreanity of  $K$ , a square: contradiction. So  $L = K$ , and the restriction homomorphism  $G_{K^{t.r.}} \rightarrow G_K^{sol}$  is onto. As  $G_{K^{t.r.}}$  is generated by involutions, the same holds for  $G_K^{sol}$ . And  $K$  being formally real implies that  $G_K^{sol}$  is non-trivial. **q.e.d.**

There are fields  $K$  satisfying the equivalent conditions of the Lemma and also allowing projective extensions. For example, if  $R$  is a real closed field and if  $L$  is a field with  $G_L$  non-procyclic prosimple then there is a field  $K$  with  $G_K \cong G_R \star G_L$ , where  $\star$  denotes the free product in the category of profinite groups (by a theorem of Melnikov-Ershov-Pop, absolute Galois groups are closed under free profinite products, cf. e.g. [K2], Theorem 1). Then  $G_K^{ab} \cong G_R^{ab} \times G_L^{ab} \cong \mathbf{Z}/2\mathbf{Z} \times 1$ , and condition 2 of the Lemma is satisfied. On the other hand, by the universal property of the free product,  $G_L$  occurs as quotient of  $G_K$ , and hence  $K$  admits a projective extension with group  $G_L$ .

However, we have no answer to the following

**Question 2.6** *Is there a formally real field  $K$  without projective extensions such that  $G_K^{sol}$  is generated by involutions, but  $G_K$  is not.*

If no such field exists then Theorem 2.3 can be sharpened to a characterization of fields allowing projective extensions: they would be exactly the fields which are not separably closed and which are not intersections of real closed fields.

By the Lemma and its proof, the smallest candidate for a positive answer to the above question would be  $K = \mathbf{Q}^{sol} \cap \mathbf{Q}^{t.r.}$ . It is clear that  $K$  is formally real, that  $G_K^{sol}$  is generated by involutions, and that  $G_K$  is not (there are e.g. totally real Galois extensions of  $\mathbf{Q}$  — and hence of  $K$  — with group

A<sub>5</sub>). What is open is whether  $K$  admits projective extensions. This question is closely related to the question whether  $\mathbf{Q}$  allows non-procyclic projective extensions discussed in section 4.2.

### 3 Projective extensions of local fields

If  $K$  is an archimedean local field then, obviously, the unique maximal projective extension of  $K$  is  $K$  itself. The non-archimedean case is more interesting:

**Proposition 3.1** *Let  $K$  be a non-archimedean local field with residual characteristic  $p$ . Let  $K^{ur}$  be the maximal unramified extension of  $K$ , and let  $K^{wild}$  be the maximal Galois extension of  $K$  without tame ramification, i.e. the compositum of all finite Galois extensions of  $K$  with ramification index a power of  $p$ .*

*Then  $K^{wild} = K^{ur}(p)$  and  $K$  has a unique maximal projective extension  $F$ . Moreover,  $K^{ur} \subset F \subseteq K^{wild}$ , and  $F = K^{wild}$  iff  $\zeta_p \notin K^{ur}$  (e.g. if  $\text{char } K = p$ ).*

**Proof:** Let  $G = G_K$  and let  $\overline{G} = \text{Gal}(F/K) = G_K/G_F$  be a maximal projective quotient of  $G$ . Then for any prime  $q$  the maximal pro- $q$  quotient  $\overline{G}(q)$  of  $\overline{G}$  is a projective quotient of  $G(q)$  and any  $q$ -Sylow subgroup  $\overline{G}_q$  of  $\overline{G}$  is a projective quotient of a  $q$ -Sylow subgroup  $G_q$  of  $G$ .

If  $q \neq p$ , the only non-trivial projective quotient of  $G(q)$  resp. of  $G_q$  is the Galois group  $\mathbf{Z}_q$  of the maximal unramified  $q$ -extension  $K_q$  of  $K$  resp.  $K_q \text{Fix } G_q$  of  $\text{Fix } G_q$ . So  $\text{res} : \overline{G}_q \rightarrow \overline{G}(q)$  is an isomorphism and  $q \mid \#\overline{G}$  iff  $K_q \subseteq F$ . But if  $q \nmid \#\overline{G}$  then  $FK_q$  is a proper extension of  $F$ , Galois over  $K$ , with  $\text{Gal}(FK_q/K) \cong \overline{G} \times \mathbf{Z}_q$  still being projective. This contradicts maximality of  $F$ , and hence  $K_q \subseteq F$  for all  $q \neq p$ .

Let  $L$  be the compositum of all  $K_q$  with  $q \neq p$ . Then  $\text{Gal}(L/K) \cong \prod_{q \neq p} \mathbf{Z}_q$  and  $\text{Gal}(F/L)$  is a projective pro- $p$  group. Moreover,  $L(p) = K^{ur}(p) = K^{wild}$  and so  $F \subseteq K^{wild}$ . (Note that  $L(p)$  is Galois over  $K$  since  $G_{L(p)}$  is a characteristic subgroup of  $G_L$  and thus normal in  $G_K$ .)

If  $\text{char } K = p$  then  $cd_p G_L(p) = cd_p G_L = cd_p G_K = 1$ , and hence, by maximality,  $F = L(p) = K^{wild}$ .

If  $\text{char } K = 0$  and  $\zeta_p \notin K^{ur}$  then  $\zeta_p \notin L$ , and, for any finite subextension  $L'/K$  of  $L/K$ ,  $G_{L'}(p)$  is a free pro- $p$  group of rank  $[L' : \mathbf{Q}_p] + 1$ . So  $G_L(p)$  is a free pro- $p$  group of rank  $\aleph_0$  and, as in the  $\text{char } K = p$ -case,  $F = L(p) = K^{wild}$ .

If  $\text{char } K = 0$  and  $\zeta_p \in K^{ur}$  then  $\zeta_p \in L$  and  $G_E(p)$  is a pro- $p$  Demushkin group of finite rank  $[E : \mathbf{Q}_p] + 2$ , where  $E$  is a any finite extension of  $\mathbf{Q}_p$  with  $K(\zeta_p) \subseteq E \subseteq L$ . By Proposition 1.10,  $G_E(p)$  has a unique maximal projective quotient, and, by uniqueness, if  $E \subseteq E'$  are two such fields then the maximal projective quotient of  $G_{E'}(p)$  projects onto that of  $G_E(p)$ . Hence  $G_L(p)$  has a unique maximal projective quotient  $G_L(p)/G_F(p)$ . But then  $F$  is the unique maximal projective extension of  $K$  and  $F \neq L(p) = K^{wild}$ .

Finally, in all cases  $K^{ur} \subset F$  since  $K^{ur}/K$  is projective and  $F$  is the unique maximal projective extension of  $K$ . The inclusion is proper since  $\text{Gal}(F/L)$  is a pro- $p$  group of infinite rank while  $\text{Gal}(K^{ur}/L) \cong \mathbf{Z}_p$ . **q.e.d.**

## 4 Projective extensions of global fields

For a global field  $K$  we define  $K^{wild}$  to be the compositum of all finite Galois extensions of  $K$  which are tamely unramified, i.e. where for each non-archimedean place of  $K$  the ramification index is a power of the residual characteristic, and, if  $\text{char } K = 0$ , we require the extension to be totally real.

**Corollary 4.1** *For a global field  $K$  any projective extension  $F/K$  is contained in  $K^{wild}$ .*

**Proof:** This is immediate from the previous proposition: If  $\text{Gal}(F/K)$  is projective then so is the subgroup  $\text{Gal}(FK_v/K_v)$  for each completion  $K_v$  of  $K$ . So, for non-archimedean  $v$ ,  $FK_v \subseteq K_v^{wild}$ , and, for real  $v$ ,  $FK_v = K_v$ . **q.e.d.**

We will see in Corollary 4.4 and 4.8 that  $K^{wild}/K$  is, in general, not projective, so projective extensions of  $K$  are properly contained in  $K^{wild}$ .

A prominent example of a projective extension of a global field  $K$  is the **cyclotomic  $\mathbf{Z}$ -extension**  $\hat{K}^{cycl}$  of  $K$ . If  $\text{char } K = p > 0$  then  $\hat{K}^{cycl}$  is just the (unramified) constant field extension  $K\overline{\mathbf{F}}_p$ . If  $\text{char } K = 0$  then for each prime  $p$  there is a unique  $\mathbf{Z}_p$ -extension of  $K$  inside  $K(\mu_{p^\infty})$ , and  $\hat{K}^{cycl}$  is the compositum of them all.

In general,  $\hat{K}^{cycl}/K$  is not a maximal projective extension of  $K$ . For example, if  $\text{char } K = p > 0$ , then, arguing as in the proof of Proposition 3.1, the  $p$ -closure  $\hat{K}^{cycl}(p)$  of  $\hat{K}^{cycl}$  is a much larger projective extension of  $K$ ,

and, in fact, as we will see, it is the unique maximal projective extension of  $K$ .

## 4.1 Function fields over finite fields

In view of Proposition 4.9(b), the following proposition may be considered as (proven) analogue to the Leopoldt conjecture in positive characteristic.

**Proposition 4.2** *Let  $K$  be a global field of characteristic  $p > 0$ . Then  $\hat{K}^{cycl}(p) = (\overline{\mathbf{F}}_p K)(p)$  is the unique maximal projective extension of  $K$ .*

**Proof:** As we have already observed above, the  $p$ -closure  $\hat{K}^{cycl}(p)$  of  $\hat{K}^{cycl}$  is a projective extension of  $K$ .

Now let  $F/K$  be an arbitrary projective extension of  $K$ , and let  $G = Gal(F/K)$ . We have to show that  $F \subseteq \hat{K}^{cycl}(p)$ .

If  $G$  is pro- $p$  then  $F \subseteq K(p) \subseteq \hat{K}^{cycl}(p)$  and we are done. So we may assume that  $G$  is not pro- $p$ .

Let  $l \neq p$  be a prime with  $l \mid \#G$ . Let  $\hat{K}^l/K$  be the  $\mathbf{Z}_l$ -subextension of  $\hat{K}^{cycl}$ , i.e. the cyclotomic  $\mathbf{Z}_l$  extension of  $K$  inside  $K(\mu_{l^\infty})$ .

*We claim that  $\hat{K}^l \subseteq F$  and that  $l \nmid \#Gal(F/\hat{K}^l)$ .*

To prove this let  $L/K$  be a finite subextension of  $F/K$  admitting a cyclic extension  $E/L$  of degree  $l$  with  $E \subseteq F$ . Such an extension exists because  $l \mid \#G$ . The subgroup  $H := Gal(F/L)$  of  $G$  is again projective, and hence the  $\mathbf{Z}/l\mathbf{Z}$ -quotient  $Gal(E/L)$  of  $H$  factors through some  $\mathbf{Z}_l$ -quotient of  $H$ , i.e. there is a  $\mathbf{Z}_l$ -subextension  $\hat{E}/L$  of  $F/L$  with  $E \subseteq \hat{E}$ .

By [NSW], Proposition 10.3.20, the global function field  $L$  of positive characteristic  $p \neq l$  has a unique  $\mathbf{Z}_l$ -extension, the cyclotomic extension  $\hat{L}^l = L\hat{K}^l$ . Hence  $\hat{E} = L\hat{K}^l$ , and so  $\hat{K}^l \subseteq F$ . It also follows that there is exactly one Galois subextension of  $F/L$  of degree  $l$ . As this holds for any finite subextension  $L/K$  of  $F/K$ ,  $G = Gal(F/K)$  has pro-cyclic  $l$ -Sylow subgroups, all of them mapped isomorphically onto  $Gal(\hat{K}^l/K)$  under the restriction map  $G \rightarrow Gal(\hat{K}^l/L)$ . So  $l \nmid \#Gal(F/\hat{K}^l)$ , and the claim is proved.

Now let  $K'$  be the compositum of the  $\hat{K}^l$ , where  $l$  runs through all prime divisors of  $\#G$  with  $l \neq p$ . Then  $K' \subseteq F \cap \hat{K}^{cycl}$  and  $F/K'$  is a pro- $p$  Galois extension. Hence  $F \subseteq K'(p) \subseteq \hat{K}^{cycl}(p)$ . **q.e.d.**

Observe, that the Proposition, in particular, implies that any projective extension of  $K$  is prosolvable. The following example therefore provides in

some sense the smallest nonabelian profinite counterexample to the inverse Galois problem over a global function field  $K$ .

**Example 4.3** *Let  $K$  be a global field of positive characteristic and let  $\hat{A}_5$  be the universal Frattini cover of  $A_5$ , i.e. the prosimple group with Frattini quotient  $A_5$ . Then  $\hat{A}_5$  is not realizable as Galois group over  $K$ .*

Of course, there is also the abelian counterexample  $\mathbf{Z}_l \times \mathbf{Z}_l$  for primes  $l \neq p$  over  $K$ : by the quoted Proposition 10.3.20 of [NSW], there is just one  $\mathbf{Z}_l$ -extension of  $K$  (the one inside  $\hat{K}^{cycl} = \overline{\mathbf{F}}_p K$ ).

**Corollary 4.4** *Let  $K$  be a global field of characteristic  $p > 0$ . Then  $K^{wild}/K$  is not projective.*

**Proof:** By Proposition 4.2 it suffices to prove that the inclusion  $\hat{K}^{cycl}(p) \subseteq K^{wild}$  is proper. To this end let  $L/\hat{K}^{cycl}$  be a finite subextension of  $\hat{K}^{cycl}(p)/\hat{K}^{cycl}$  such that the genus  $g = g_L$  of the function field  $L/\overline{\mathbf{F}}_p$  is  $\geq 1$ . This is possible, because either  $g_K \geq 1$  (so we may take  $L = \hat{K}^{cycl}$ ), or  $g_K = 0$  and so (as function field over a finite field)  $K$  is a rational function field, say  $K = \mathbf{F}_q(t)$  and then  $L = \hat{K}^{cycl}(x)$  with  $x^p - x - t^{q-1} - a = 0$  has genus  $> 0$ , if  $a \in \mathbf{F}_q$  is chosen such that the polynomial  $X^p - X - a$  has no zero in  $\mathbf{F}_q$ :  $L$  is the function field of a curve defined over  $\mathbf{F}_q$  without  $\mathbf{F}_q$ -rational point.

Choose any prime  $l \neq p$ . Then, by [SGA], the maximal unramified pro- $l$  Galois extension  $L(l)$  of  $L$  has as Galois group the pro- $l$  group generated by elements  $\alpha_1, \beta_1, \dots, \alpha_g, \beta_g$  with the single relation  $[\alpha_1, \beta_1] \cdots [\alpha_g, \beta_g] = 1$ . In particular,  $L(l)/L$  is a non-trivial pro- $l$  subextension of  $K^{wild}/L$ , and hence

$$\hat{K}^{cycl}(p) \subset \hat{K}^{cycl}(p)L(l) \subseteq K^{wild},$$

where the first inclusion is proper.

**q.e.d.**

**Remark 4.5** *Proposition 4.2 can be used to describe, for a function field  $K$  of characteristic  $p > 0$  all semidirect product decompositions  $G_K = N \rtimes H$ , where  $H$  is a projective profinite group: they are all composed from the (by now) canonical decomposition  $G_K \cong G_{\hat{K}^{cycl}(p)} \rtimes \text{Gal}(\hat{K}^{cycl}(p)/K)$  with some semidirect product decomposition of  $\text{Gal}(\hat{K}^{cycl}(p)/K) \cong \Gamma \rtimes \hat{\mathbf{Z}}$ , where  $\Gamma$  is a free pro- $p$  group of rank  $\aleph_0$ .*

*However,  $G_K$  may decompose in other semidirect products. If, for example,  $\pi \in K$  is a uniformizing element for some valuation  $v$  on  $K$  (i.e.  $v(\pi)$  is*

the minimal positive element in the value group of  $v$ ), then  $F := \hat{K}^{cycl}(\{\pi^{1/n} \mid p \nmid n \in \mathbf{N}\})$  is a well-defined Galois extension of  $K$ , because  $\hat{K}^{cycl}$  contains all roots of unity of order prime to  $p$ . Now assume that the residue field of  $v$  is the constant field  $K \cap \bar{\mathbf{F}}_p$  of  $K$ . Then  $v$  extends uniquely to  $F$ , and if  $K_v$  is a henselisation of  $K$  w.r.t.  $v$ , then  $FK_v$  is the maximal tamely ramified extension of  $K_v$ , i.e. the fixed field of the ramification subgroup  $V$  of  $G_{K_v}$ . By [KPR],  $V$  has a complement  $W$  in  $G_{K_v}$ . So  $G_{K_v} = V \rtimes W$  and the restriction maps

$$W \rightarrow \text{Gal}(FK_v/K_v) \rightarrow \text{Gal}(F/K) \cong \left( \prod_{q \neq p} \mathbf{Z}_q \right) \rtimes \hat{\mathbf{Z}}$$

are isomorphisms. Thus  $W$  is a complement of  $G_F$  in  $G_K$  and so  $G_K = G_F \rtimes W$ . Note that  $W$  is not projective:  $cd_q W = 2$  for all primes  $q \neq p$ .

## 4.2 Number fields

Let us now turn to number fields. We don't know how large  $K^{wild}$  is for number fields, not even for  $K = \mathbf{Q}$ . We will see that the solvable part, i.e.  $\mathbf{Q}^{wild} \cap \mathbf{Q}^{solv}$  is not cyclotomic (by the proof of Corollary 4.8). The nilpotent part, however, is: denoting by  $\mathbf{Q}^{nil}$  the maximal pronilpotent extension of  $\mathbf{Q}$ , we obtain the following

**Lemma 4.6**

$$\mathbf{Q}^{wild} \cap \mathbf{Q}^{nil} = \hat{\mathbf{Q}}^{cycl}$$

**Proof:** Let  $F = \mathbf{Q}^{wild} \cap \mathbf{Q}^{nil}$ . Then, clearly,  $F \supseteq \hat{\mathbf{Q}}^{cycl}$ . Since  $G := \text{Gal}(F/\mathbf{Q})$  is pronilpotent, the Frattini quotient  $G/\Phi(G)$  is a direct product of cyclic groups of prime order. For each prime  $p$ , there is, by Kronecker-Weber together with the well-known ramification structure in cyclotomic fields, exactly one cyclic extension of  $\mathbf{Q}$  of degree  $p$  in  $\mathbf{Q}^{wild}$ , the one inside  $\hat{\mathbf{Q}}^{cycl}$ . Hence  $G/\Phi(G) \cong \prod_{p \text{ prime}} \mathbf{Z}/p\mathbf{Z}$  is procyclic, and, therefore, so is  $G$ . As  $\hat{\mathbf{Z}} \cong \text{Gal}(\hat{\mathbf{Q}}^{cycl}/\mathbf{Q})$  allows no proper procyclic extension,  $G = \text{Gal}(\hat{\mathbf{Q}}^{cycl}/\mathbf{Q})$  and  $F = \hat{\mathbf{Q}}^{cycl}$ . **q.e.d.**

Recall that the **Leopoldt conjecture** for a number field  $K$  and a prime  $p$  says that  $i_p(K) = s_K + 1$ , where  $s_K$  is the number of complex (nonreal) archimedean places of  $K$  and  $i_p(K)$  is the free rank of  $G_K(p)^{ab}$ , i.e. the maximal  $i \in \mathbf{N}$  for which  $\mathbf{Z}_p^i$  is a quotient of  $G_K$ . One always has

$$s_K + 1 \leq i_p(K) \leq \frac{1}{2}(r_K + 3s_K + 1),$$

where  $r_K$  is the number of real archimedean places of  $K$  (for a detailed exposition to the various forms of the Leopoldt conjecture cf. [NSW], X.3).

By a deep result of Brumer, the Leopoldt conjecture is known to be true for finite abelian extensions of  $\mathbf{Q}$  ([NSW], Theorem 10.3.16). We use this to prove our next result:

**Proposition 4.7**  $\hat{\mathbf{Q}}^{cycl}$  is the unique maximal projective prosolvable extension of  $\mathbf{Q}$ .

**Proof:** Assume  $F/\mathbf{Q}$  is a projective prosolvable extension not contained in  $\hat{\mathbf{Q}}^{cycl}$ . Then there is a finite subextension  $K/\mathbf{Q}$  of  $\hat{\mathbf{Q}}^{cycl}/\mathbf{Q}$  and, for some prime  $p$ , a Galois extension  $L/K$  of degree  $p$  with  $L \subseteq KF$ , but  $L \not\subseteq \hat{\mathbf{Q}}^{cycl}$ . The Galois extension  $KF/K$  is projective, since  $F/\mathbf{Q}$  is projective and the restriction homomorphism

$$res : Gal(KF/K) \rightarrow Gal(F/\mathbf{Q})$$

is injective. Hence  $K$  admits a  $\mathbf{Z}_p$ -extension  $L'/K$  with  $L \subseteq L'$ . But then  $K$  has two independent  $\mathbf{Z}_p$ -extensions:  $L'$  and the cyclotomic  $\mathbf{Z}_p$ -extension. As  $K/\mathbf{Q}$  is totally real, this contradicts Leopoldt's conjecture for  $K$  and  $p$ . But since  $K/\mathbf{Q}$  is finite abelian, Leopoldt's conjecture is true for  $K$  and all  $p$ , by the result quoted above. So our  $F$  cannot exist. **q.e.d.**

As a consequence we obtain the promised

**Corollary 4.8**  $\mathbf{Q}^{wild}/\mathbf{Q}$  is not projective.

**Proof:** Let  $L/\mathbf{Q}$  be a finite subextension of  $\hat{\mathbf{Q}}^{cycl}$  with class number  $h_L > 1$ . Then the small Hilbert class field  $F$  of  $L$ , i.e. the maximal unramified totally real abelian extension of  $L$ , is a proper finite extension of  $L$  (of degree  $h_L$ ). As  $G_F$  is a characteristic subgroup of  $G_L$ ,  $F$  is Galois over  $\mathbf{Q}$ . Moreover,  $F \not\subseteq \hat{\mathbf{Q}}^{cycl}$ , because for any pair  $L \subset F$  of distinct subfields of  $\hat{\mathbf{Q}}^{cycl}$  the extension  $F/L$  ramifies. And, by definition,  $F \subseteq L^{wild} = \mathbf{Q}^{wild}$ .

So  $F\hat{\mathbf{Q}}^{cycl}/\mathbf{Q}$  is a prosolvable Galois subextension of  $\mathbf{Q}^{wild}/\mathbf{Q}$  strictly larger than  $\hat{\mathbf{Q}}^{cycl}$ . If  $\mathbf{Q}^{wild}/\mathbf{Q}$  were a projective extension, then the maximal prosolvable subextension  $\mathbf{Q}^{solv} \cap \mathbf{Q}^{wild}$  of  $\mathbf{Q}^{wild}/\mathbf{Q}$  would be projective as well. But then Proposition 4.7 implies that  $\mathbf{Q}^{solv} \cap \mathbf{Q}^{wild} = \hat{\mathbf{Q}}^{cycl}$  contradicting the existence of a field  $F$  as constructed above. So  $\mathbf{Q}^{wild}/\mathbf{Q}$  cannot be projective. **q.e.d.**

The **weak Leopoldt conjecture** for a number field  $K$ , a prime  $p$  and a  $\mathbf{Z}_p$ -extension  $L/K$  says that there is some  $d = d(p, K, L) \in \mathbf{N}$  such that for all finite subextensions  $K'/K$  of  $L/K$ ,  $i_p(K') \leq s_{K'} + 1 + d$ . (cf. e.g. [NSW], X.3)

**Proposition 4.9** (a) *Assume the weak Leopoldt conjecture holds for all number fields  $K \subseteq \mathbf{Q}^{wild}$ , for all primes  $p$  and for all  $\mathbf{Z}_p$ -extensions  $L/K$ . Then  $\hat{\mathbf{Q}}^{cycl}$  is the unique maximal projective extension of  $\mathbf{Q}$ .*

(b) *The following are equivalent:*

(i) *The Leopoldt conjecture holds for all totally real number fields and all primes  $p$*

(ii)  *$\hat{K}^{cycl}$  is the unique maximal projective extension of  $K$  for all totally real number fields.*

**Proof:** (a) Let  $F/\mathbf{Q}$  be a projective extension with group  $G$ . Then, by Corollary 4.1,  $F \subseteq \mathbf{Q}^{wild}$ . If  $G$  is not prosolvable then there are finite extensions  $F_0 \subseteq F_1 \subseteq F$  of  $\mathbf{Q}$  such that  $F_1/F_0$  is Galois with a finite nonabelian simple Galois group  $H$ . For some prime  $p$ ,  $H$  has a non-cyclic  $p$ -Sylow subgroup, say with fixed field  $K$ . Then  $Gal(F/K)$  is projective with (again projective, i.e. free) maximal pro- $p$  quotient  $P = Gal(E/K)$  of rank  $> 1$ . Let  $L/K$  be a  $\mathbf{Z}_p$ -subextension of  $E/K$ . Then for each finite subextension  $K'/K$  of  $L/K$ ,  $Gal(E/K')$  is, by the Nielsen-Schreier theorem, a free pro- $p$  group of rank  $1 + n(rk P - 1) > n$ , where  $n = [K' : K]$ . Hence  $i_p(K') > n$  contradicting the weak Leopoldt conjecture for  $L/K$ . Hence  $G$  is prosolvable, i.e.  $F \subseteq \mathbf{Q}^{solv}$ . Then the previous Proposition implies  $F \subseteq \hat{\mathbf{Q}}^{cycl}$ .

(b) Assume (i), let  $K$  be a totally real number field and let  $F/K$  be a projective extension. Then  $F \subseteq K^{wild}$ , and, in particular, any finite subextension  $K'/K$  of  $F/K$  is again a totally real number field. By (i), this implies that, for each prime  $p$ , the maximal pro- $p$  extension of  $K'$  inside  $F$  is the cyclotomic  $\mathbf{Z}_p$ -extension of  $K'$ . But then  $F \subseteq \hat{K}^{cycl}$ .

(ii)  $\Rightarrow$  (i) is obvious.

**q.e.d.**

## References

[BLS] H. Bass, M. Lazard, J.-P. Serre, *Sous-groupes d'indice fini dans  $SL(n, \mathbf{Z})$* , Bulletin AMS **70** (1964), 385-392.

- [CKK] J. Cossey, O.H. Kegel, L.G. Kovács, *Maximal Frattini extensions*. Arch. Math. **35** (1980), 210-217.
- [D] A. Douady, *Détermination d'un groupe de Galois*, C.R. Acad. Sci. Paris **258** (1964), 5305-5308.
- [FJ] M. D. Fried, M. Jarden, *Field Arithmetic*, Ergebnisse der Mathematik (3), vol. **11**, Springer, Heidelberg 1986.
- [H] B. Huppert, *Endliche Gruppen I*, Springer, Heidelberg 1967.
- [K1] J. Koenigsmann, *Solvable absolute Galois groups are metabelian*, Inventiones math. **144** (2001), 1-22.
- [K2] J. Koenigsmann, *Relatively projective groups as absolute Galois groups*, Israel J. Math. **127** (2002), 93-129.
- [K3] J. Koenigsmann, *Encoding valuations in absolute Galois groups*, Fields Institute Communications **33** (2003), 107-132.
- [K4] J.Koenigsmann, *Products of absolute Galois groups*, to appear in Int. Math. Research Notices.
- [KPR] F.-V. Kuhlmann, M. Pank, P. Roquette. *Immediate and purely wild extensions of valued fields*, manusc. math. **55** (1986), 39-67.
- [LvD] A. Lubotzky, L. van den Dries, *Subgroups of free profinite groups and large subfields of  $\bar{\mathbf{Q}}$* , Israel J. Math. **39** (1981), 25-45.
- [Mc] J.L. Mennicke, *Finite factor groups of the unimodular group*, Annals of Math. **81** (1965), 31-37.
- [NSW] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of number fields*. Springer, Grundlehren der math. Wissenschaften **323**, 2000.
- [RZ] L. Ribes, P. Zalesskii, *Profinite groups*, Ergebnisse der Mathematik (3), vol. **40**, Springer, Heidelberg 2000.
- [SGA] A. Grothendieck, M. Raynaud, *Séminaire de Géométrie Algébrique du Bois Marie 1960/61, Revêtements Etales et Groupe Fondamental (SGA 1)*, Springer LNM **224**, Heidelberg 1971.

[W] G. Whaples, *Algebraic extensions of arbitrary fields*, Duke Math. J. **24** (1957), 201-204.

e-mail: `Jochen.Koenigsmann@unibas.ch`