

## NILPOTENT EXTENSIONS OF NUMBER FIELDS WITH BOUNDED RAMIFICATION

A. CUETO-HERNÁNDEZ AND G.D. VILLA-SALVADOR

We study a variant of the inverse problem of Galois theory and Abhyankar's conjecture. If  $p$  is an odd rational prime and  $G$  is a finite  $p$ -group generated by  $s$  elements,  $s$  minimal, does there exist a normal extension  $L/\mathbb{Q}$  such that  $\text{Gal}(L/\mathbb{Q}) \cong G$  with at most  $s$  rational primes that ramify in  $L$ ? Given a nilpotent group of odd order  $G$  with  $s$  generators, we obtain a Galois extension  $L/\mathbb{Q}$  with precisely  $s$  prime divisors of  $\mathbb{Q}$  ramified. Furthermore if  $K$  is a number field satisfying  $K \cap \mathbb{Q}(\zeta_{p_i^{n_i}}) = \mathbb{Q}$  for each rational prime  $p_i$ , such that  $p_i^{n_i} \mid \circ(G)$ ,  $p_i^{n_i+1} \nmid \circ(G)$ , and such that there exists a rational prime  $q$  inert in  $K/\mathbb{Q}$ , we obtain a Galois extension  $E/K$  with precisely  $s$  prime divisors of  $K$  ramified. An adaptation of the Scholz-Reichardt method for the embedding problem is our main tool.

### 1. Introduction.

Let  $G$  be a finite group. Does there exist a finite Galois extension  $L$  of  $\mathbb{Q}$ , the field of rational numbers, such that its Galois group  $\text{Gal}(L/\mathbb{Q})$  is isomorphic to  $G$ ? This is the Inverse Problem of Galois Theory. When such extension exists we say that  $G$  is realizable over  $\mathbb{Q}$ . Scholz [18] and independently Reichardt [12] proved that if  $G$  is a finite  $p$ -group,  $p$  an odd prime, then  $G$  is realizable over  $\mathbb{Q}$ . They used a criterion given by Brauer [2]. The method of Scholz and Reichardt does not work for  $p = 2$  because the primitive 2-root of unity  $-1$  belongs to  $\mathbb{Q}$ .

Šafarevič [16] solved the case  $p = 2$ , but he had to allow many primes to ramify in the extension. In contrast, Serre [19] shows that the method of Scholz and Reichardt gives, for a group  $G$  of order  $p^m$ ,  $p$  an odd prime number, a Galois extension  $L/\mathbb{Q}$  where only  $m$  primes ramify.

Given an algebraic function field  $K/k$  of one variable and a finite group  $G$  and a positive integer  $s$ , does there exist a Galois extension  $L/k$  of  $K/k$  such that the Galois group of  $L/K$  is isomorphic to  $G$  and at most  $s$  prime divisors of  $K$  ramify?

In 1957 S. Abhyankar [1] conjectured that if  $k$  is an algebraically closed field of characteristic  $p$ , then there exists an extension  $L/K$  of function fields

over  $k$  such that  $\text{Gal}(L/K) \cong G$  with at most  $s$  prime divisors of  $K$  ramified in  $L$  if and only if  $G/p(G)$  can be generated by  $2g_K + s - 1$  elements where  $g_K$  denotes the genus of  $K$  and  $p(G)$  denotes the subgroup of  $G$  generated by its  $p$ -subgroups.

Recently Geyer and Jarden [5] gave a unified treatment for global fields. They considered a finite  $p$ -group  $G$  of order  $p^n$  and  $K$  a global field of characteristic different from  $p$  and such that the primitive  $p$ -root of 1,  $\zeta_p$ , is not in  $K$ . They proved that there exists an extension  $L/K$  with Galois group  $G$  and a nonnegative integer  $r$  depending only on  $K$  such that  $|\text{Ram}(L/K)| \leq n + r$  where  $\text{Ram}(L/K)$  denotes the set of prime divisors in  $K$  ramified in  $L$ . In particular, they obtain Serre's result again. Their proof is based in a systematic application of class field theory.

In this paper we consider a finite nilpotent group  $G$  of odd order. We construct a Galois extension  $L/\mathbb{Q}$  with Galois group  $G$  and such that the number of ramified prime divisors in  $L/\mathbb{Q}$ ,  $|\text{Ram}(L/\mathbb{Q})| = s$ , where  $s$  is the minimum number of generators of  $G$  (Theorem 5). This improves Serre's result.

Our proof is based on cyclotomic fields. We first consider a  $p$ -group  $G$  and then the abelianization of  $G$ ,  $G/G'$ ,  $G'$  denoting the commutator subgroup of  $G$ . Next we construct a Galois extension  $K_0/\mathbb{Q}$  with Galois group  $G/G'$  with exactly  $s$  prime divisors of  $\mathbb{Q}$  ramified in  $K_0$ . Then we follow the construction of Scholz and Reichardt keeping the number of ramified primes. For this end we have to remove new ramification, tame and wild. For the later we use Šafarevič results on  $p$ -extensions [15].

We also prove that if  $G$  is a finite nilpotent group of odd order with minimum number of generators  $s$ , then for any extension  $L/\mathbb{Q}$  with Galois group  $G$  we have  $|\text{Ram}(L/\mathbb{Q})| \geq s$  (Theorem 6). We note that there are Galois non-nilpotent extensions  $L/\mathbb{Q}$  where  $|\text{Ram}(L/\mathbb{Q})| < s$  (Theorem 8).

Finally, we construct a Galois extension  $E/K$  with Galois group  $G$  and such that  $|\text{Ram}(E/K)| = s$  where  $s$  is the minimum number of generators of  $G$ ,  $K$  is a number field such that  $K \cap \mathbb{Q}(\zeta_{p_i^{n_i}}) = \mathbb{Q}$  for each prime  $p_i$  such that  $p_i^{n_i} \mid \circ(G)$  and  $p_i^{n_i+1} \nmid \circ(G)$  and there exists a prime  $q \in \mathbb{Q}$  such that  $q$  is inert in  $K/\mathbb{Q}$  (Theorem 10).

## 2. Realization of a $p$ -group.

All fields under consideration are finite number fields, and  $p$  is an odd rational prime.

Let  $G$  be a finite  $p$ -group. Consider

$$1 \longrightarrow H \longrightarrow \tilde{G} \longrightarrow G \longrightarrow 1,$$

an exact sequence of  $p$ -groups with  $H \cong C_p$ , the cyclic group of  $p$ -elements and  $H$  a central subgroup of  $\tilde{G}$ . Let  $L/K$  be a Galois extension such that



**Theorem 2.** *Let  $G$  be an arbitrary finite  $p$ -group,  $p$  an odd prime, and let  $K$  be a number field. Then there exists a Galois extension  $L/K$  such that  $\text{Gal}(L/K) \cong G$ .*

*Proof.* [7], Theorem 3.95, page 188.  $\square$

Let  $G$  denote a  $p$ -group of order  $p^n$ , and let  $s$  denote the minimum number of generators of  $G$ . We will construct an extension  $L/\mathbb{Q}$  such that precisely  $s$  primes ramify.

When  $G$  is cyclic, the problem is well known. We present the proof for the sake of completeness.

**Proposition 1.** *Let  $G$  be cyclic  $p$ -group. There exists an extension  $L/\mathbb{Q}$  such that  $\text{Gal}(L/\mathbb{Q}) \cong G$  and  $|\text{Ram}(L/\mathbb{Q})| = 1$ .*

*Proof.* Let  $q$  be a prime number such that  $p^n | q - 1$ . Then the field  $L = E_q \subseteq \mathbb{Q}(\zeta_q)$  with  $[E_q : \mathbb{Q}] = p^n$  satisfies what we want.  $\square$

When  $G$  is an abelian  $p$ -group the problem has two solutions one without any restriction and another that satisfies Scholz conditions.

**Proposition 2.** *Let  $G$  be an abelian  $p$ -group. There exists an extension  $L/\mathbb{Q}$  such that  $\text{Gal}(L/\mathbb{Q}) \cong G$  and  $|\text{Ram}(L/\mathbb{Q})| = s$ , where  $s$  is the minimum number of generators of  $G$ .*

*Proof.* Let

$$G = C_{p^{a_1}} \times C_{p^{a_2}} \times \cdots \times C_{p^{a_s}},$$

where  $C_{p^{a_i}}$  is the cyclic group of order  $p^{a_i}$ ,  $\sum_{i=1}^s a_i = n$ ,  $a_1 \geq a_2 \geq \dots \geq a_s \geq 1$ .

Let  $q_i$  and  $E_{q_1}, \dots, E_{q_s}$  be as in Proposition 1 with  $q_1 < q_2 < \dots < q_s$ . Then  $L = E_{q_1} \cdots E_{q_s}$  is the required extension.  $\square$

Thus, when  $G$  is an abelian  $p$ -group, the problem has a solution without any restriction.

Now, we will show that there exists a solution that is a Scholz extension. First we prove two propositions.

**Proposition 3.** *Let  $p$  be an odd prime number,  $n$  and  $s$  positive integers. Then there exist infinitely many collections of  $s$  prime numbers  $\{q_1, \dots, q_s\}$  such that*

- (i)  $q_1 \equiv 1 \pmod{p^n}$ ,
- (ii) for  $2 \leq i \leq s$ ,  $q_i$  is fully decomposed in

$$\mathbb{Q}(\zeta_{p^n}, \zeta_{q_1}, \dots, \zeta_{q_{i-1}}, \sqrt[p^n]{q_1}, \dots, \sqrt[p^n]{q_{i-1}})/\mathbb{Q}.$$

*Proof.* By Dirichlet density theorem there exists a prime number  $q_1$  such that  $q_1 \equiv 1 \pmod{p^n}$ . Let  $K_1 = \mathbb{Q}(\zeta_{p^n}, \zeta_{q_1}, \sqrt[p^n]{q_1})$ . From Tchebotarev density theorem we have that there exists a rational prime  $q_2$  which has a divisor

of degree one in  $K_1/\mathbb{Q}$ . Let  $K_2 = K_1(\zeta_{q_2}, \sqrt[p^n]{q_2})$ . From Tchebotarev density theorem we have that there exists a rational prime  $q_3$  which has a divisor of degree one in  $K_2/\mathbb{Q}$ . Continuing with this process we obtain one of such collections. From Tchebotarev density theorem it follows that there exists infinitely many of these collections.  $\square$

**Definition 2.** Let  $\mathfrak{P}$  be a prime divisor of  $K$ , we say that  $\mathfrak{P}$  is **fleissig** in  $L/K$  if  $\mathfrak{P}$  has inertia degree 1.

**Proposition 4.** Let  $p$  be an odd prime,  $n$  and  $s$  positive integers. Let  $a_i \in \mathbb{N}, 1 \leq i \leq s$ , such that  $\sum_{i=1}^s a_i = n$ . Then there exist infinitely many collections of  $s$  fields  $\{E_1, \dots, E_s\}$  such that

- (i)  $\text{Gal}(E_i/\mathbb{Q}) \cong C_{p^{a_i}}$ ,
- (ii)  $|\text{Ram}(E_i/\mathbb{Q})| = 1$ ,
- (iii) the ramified prime divisor in  $E_i/\mathbb{Q}$  is fleissig in  $E_j/\mathbb{Q}$ ,  $j = 1, \dots, s$ .

*Proof.* Let  $\{q_1, \dots, q_s\}$  be one of the collections of  $s$  primes given in Proposition 3. Let

$$\begin{aligned} K_1 &= \mathbb{Q}(\zeta_{p^n}, \zeta_{q_1}, \sqrt[p^n]{q_1}), \\ K_i &= K_{i-1}(\zeta_{q_i}, \sqrt[p^n]{q_i}), \quad 2 \leq i \leq s. \end{aligned}$$

Let  $\alpha_j = \sqrt[p^n]{q_j} \in K_{i-1}$ ,  $j = 1, \dots, i-1$ . Then  $\alpha_j^{p^n} = q_j$ . Hence

$$\alpha_j^{p^n} \equiv q_j \pmod{\mathfrak{P}_i},$$

where  $\mathfrak{P}_i$  is a prime ideal in  $K_{i-1}$  such that  $\mathfrak{P}_i | q_i$ . Since  $q_i$  has a divisor of degree one in  $K_{i-1}$ , we have that

$$\mathfrak{D}_{K_{i-1}/\mathfrak{P}_i} \cong \mathbb{F}_{q_i} = \mathbb{Z}/q_i\mathbb{Z}.$$

Therefore, there exists  $\beta_j \in \mathbb{Z}$  such that

$$\beta_j^{p^n} \equiv q_j \pmod{q_i}.$$

Since  $1 \equiv \beta_j^{q_i-1} = (\beta_j^{p^n})^{\frac{q_i-1}{p^n}} \equiv q_j^{\frac{q_i-1}{p^n}} \pmod{q_i}$ , it follows that if  $f_{q_i}(q_j)$  is the order of  $q_j$  modulo  $q_i$ , then  $f_{q_i}(q_j) | \frac{q_i-1}{p^n}$ .

We consider the extension  $\mathbb{Q}(\zeta_{q_i})/\mathbb{Q}$ . For the primes  $q_j$  we have

$$q_i - 1 = e(q_j | \mathbb{Q}(\zeta_{q_i})/\mathbb{Q}) f(q_j | \mathbb{Q}(\zeta_{q_i})/\mathbb{Q}) g(q_j | \mathbb{Q}(\zeta_{q_i})/\mathbb{Q})$$

where  $e(q_j | \mathbb{Q}(\zeta_{q_i})/\mathbb{Q})$ ,  $f(q_j | \mathbb{Q}(\zeta_{q_i})/\mathbb{Q})$  and  $g(q_j | \mathbb{Q}(\zeta_{q_i})/\mathbb{Q})$  denote the ramification index, the inertia degree and the number of primes above  $q_j$  in  $\mathbb{Q}(\zeta_{q_i})/\mathbb{Q}$  respectively.

Hence,

$$\begin{aligned} q_i - 1 &= f_{q_i}(q_j) g(q_j | \mathbb{Q}(\zeta_{q_i})/\mathbb{Q}), \\ f_{q_i}(q_j) r_j p^n &= f_{q_i}(q_j) g(q_j | \mathbb{Q}(\zeta_{q_i})/\mathbb{Q}), \quad r_j \in \mathbb{Z}. \end{aligned}$$

Therefore,  $p^n |g(q_j|\mathbb{Q}(\zeta_{q_i})/\mathbb{Q})$ .

Thus, we have that there exists a subfield  $E_i$  of  $\mathbb{Q}(\zeta_{q_i})$  such that

- (1)  $\text{Gal}(E_i/\mathbb{Q}) \cong C_{p^{a_i}}$ ,
- (2)  $|\text{Ram}(E_i/\mathbb{Q})| = 1$ ,
- (3)  $q_j, j = 1, \dots, i$  are fleissig in  $E_i/\mathbb{Q}$ .

The collection of  $s$  fields  $\{E_1, \dots, E_s\}$  satisfies the conditions of the proposition. The existence of infinitely many of these collections follows from the existence of infinitely many collections of  $s$  primes given in Proposition 3.  $\square$

**Corollary 1.** *Let  $G$  be an abelian  $p$ -group. There exists a Scholz extension  $L/\mathbb{Q}$  such that  $\text{Gal}(L/\mathbb{Q}) \cong G$  and  $|\text{Ram}(L/\mathbb{Q})| = s$ , where  $s$  is the minimum number of generators.*

Hence for an abelian  $p$ -group  $G$ , we have a Scholz extension  $L/\mathbb{Q}$  with  $\text{Gal}(L/\mathbb{Q}) \cong G$ .

Now we consider  $G$  a non-abelian  $p$ -group.

The following theorem is the main result of the present work and it is the basis of the following results.

**Theorem 3.** *Let  $G$  be a finite arbitrary  $p$ -group. There exists an extension  $L/\mathbb{Q}$ , such that*

- (i)  $\text{Gal}(L/\mathbb{Q}) \cong G$ ,
- (ii)  $|\text{Ram}(L/\mathbb{Q})| = s$ ,

where  $s$  is the minimum number of generators of  $G$ .

*Proof.* Let  $G'$  be the commutator subgroup of  $G$ . Let  $|G| = p^n$ ,  $|G'| = p^t$ ,  $1 \leq t < n$ . We have that  $G/G'$  is an abelian group, say  $G/G' \cong C_{p^{a_1}} \times \dots \times C_{p^{a_s}}$ .

Let  $G_0 = G/G'$ ,  $G_1, \dots, G_t = G$  be such that

$$G_{i-1} \cong G_i/H_i \quad i = 1, \dots, t \quad \text{with} \quad H_i \subseteq Z(G_i), |H_i| = p.$$

We will construct fields  $K_0 \subseteq K_1 \subseteq \dots \subseteq K_t$ , such that  $\text{Gal}(K_i/\mathbb{Q}) \cong G_i$ ,  $i = 0, \dots, t$  and  $|\text{Ram}(K_i/\mathbb{Q})| = s$ .

From Corollary 1, we obtain that there exists a Scholz extension  $K_0/\mathbb{Q}$  such that  $\text{Gal}(K_0/\mathbb{Q}) \cong G_0$  and  $|\text{Ram}(K_0/\mathbb{Q})| = s$ .

From Theorem 1, it follows that there exists  $K_1/\mathbb{Q}$  such that  $K_0 \subseteq K_1$  and  $\text{Gal}(K_1/\mathbb{Q}) \cong G_1$ .

In order to continue our construction, we need a Scholz extension  $L_1/\mathbb{Q}$  such that  $K_0 \subset L_1$ ,  $\text{Gal}(L_1/\mathbb{Q}) \cong G_1$  and  $|\text{Ram}(L_1/\mathbb{Q})| = s$ .

If the field  $K_1$  given by Theorem 1 already satisfies these conditions we set  $L_1 = K_1$ . Otherwise, we proceed as follows. Let  $q_1, \dots, q_s$  be the ramified primes in  $K_0/\mathbb{Q}$  which are fleissig. Therefore,  $K_1/\mathbb{Q}$  may fail to be a Scholz extension because of any of the following:

- (I) There are new ramified primes.
- (II) Some of the ramified primes in  $K_0/\mathbb{Q}$  are inert in  $K_1/K_0$ , that is, they are not fleissig in  $K_1/\mathbb{Q}$ .

**First step.** Elimination of new ramification

We consider two cases: when the new ramification is tame and when it is wild.

First we consider tame ramification. Let  $q$  be a new ramified prime divisor, that is,  $q$  ramifies in  $K_1/\mathbb{Q}$  but not in  $K_0/\mathbb{Q}$ . Let  $K_{0(q)}$  be the local field of  $K_0$ . In that case we have that  $[K_0 : \mathbb{Q}] = p^{n-t}$  and  $[K_{0(q)} : \mathbb{Q}_q] = p^{\alpha'}$ , where we have that  $\alpha' \leq n-t$ . We have that  $x^{q^{p^{\alpha'}}} - x = 0$  has  $q^{p^{\alpha'}}$  solutions in  $\mathbb{F}_{q^{p^{\alpha'}}}$ . Since  $q$  is ramified in  $K_1/K_0$ , the residue fields of  $K_1$  and  $K_0$  are the same, namely,  $\mathbb{F}_{q^{p^{\alpha'}}}$ . Now,  $q$  is totally and tamely ramified in  $K_1/K_0$  with index ramification  $p$ . It follows that  $\zeta_p \in K_{1(q)}$  ([8, Prop. 12, Chap. II]). Thus  $\zeta_p \in \mathbb{F}_{q^{p^{\alpha'}}}$ . Hence  $p | (q^{p^{\alpha'}} - 1)$ .

Now, we have that  $q^{p^{\alpha'}} - 1 = ((q-1) + 1)^{p^{\alpha'}} - 1 = (q-1)^{p^{\alpha'}} + ph$ . Therefore  $p | (q-1)^{p^{\alpha'}}$ . Hence  $p | (q-1)$ .

Let  $\wedge_q$  be the extension of  $\mathbb{Q}$  such that  $\wedge_q \subset \mathbb{Q}(\zeta_q)$  and  $[\wedge_q : \mathbb{Q}] = p$ . Then  $q$  is the unique prime of  $\mathbb{Q}$  ramified in  $\wedge_q/\mathbb{Q}$ .

Since  $q$  is unramified in  $K_0$  and ramified in  $\wedge_q$ ,  $\wedge_q \cap K_0 = \mathbb{Q}$ . If  $\wedge_q$  were contained in  $K_1$ , then it would equal  $K_0 \wedge_q$  which would imply that  $G_1 \cong G_0 \times C_p$ . This contradicts that  $s$  is the minimum number of generators of  $G$ .

Since  $q$  is tamely ramified, we have that the inertia group of  $q$  in  $K_1 \wedge_q / K_0$  is cyclic. Therefore,  $q$  is not fully ramified in  $K_1 \wedge_q / K_0$ . Let  $K'_1$  be the fixed field by the inertia group of  $q$ . Then  $\text{Gal}(K'_1/\mathbb{Q}) \cong \text{Gal}(K_1/\mathbb{Q})$  [13, page 4]. Then we obtain that  $\text{Gal}(K'_1/\mathbb{Q}) \cong \text{Gal}(K_1/\mathbb{Q}) \cong G_1$ ,  $q$  is not ramified in  $K'_1/K_0$  and there are no new ramified prime divisors in  $K'_1/K_0$  different from those ramified in  $K_1/K_0$ .

We denote  $K'_1$  again by  $K_1$ . We have  $\text{Gal}(K_1/\mathbb{Q}) \cong G_1$  and  $q$  is not ramified in  $K_1/\mathbb{Q}$ .

Continuing in this way, we delete the new tame ramification and we obtain an extension, which we denote again by  $K_1$ , such that  $\text{Gal}(K_1/\mathbb{Q}) \cong G_1$  and there is no new tame ramification in  $K_1/\mathbb{Q}$  different to that in  $K_0/\mathbb{Q}$ .

Now we consider wild ramification.

In this case we have that  $p$  ramifies in  $K_1/\mathbb{Q}$ . We consider the subextension  $T$  of  $\mathbb{Q}(\zeta_{p^2})$  such that  $T/\mathbb{Q}$  is a cyclic extension of degree  $p$ , and  $p$  is the unique ramified prime divisor.

We have that  $p$  ramifies in  $K_0T/K_0$  and in  $K_1/K_0$ .

We will prove that any divisor of  $K_0$  above  $p$  is not fully ramified in  $K_1T/K_0$ . Assuming this, we have that there exists a field  $K'_1$ , the field fixed

by the inertia group of  $p$ , such that  $\text{Gal}(K'_1/\mathbb{Q}) \cong \text{Gal}(K_1/\mathbb{Q}) \cong G_1$  and  $p$  is not ramified in  $K'_1/K_0$ .

For a  $p$ -adic field  $F$  not containing the  $p$ -th roots of unity, Šafarevič proved the following theorem [15].

**Theorem 4.** *The  $p$ -extensions of  $F$  are in one-to-one correspondence with the normal subgroups of a free group  $S$  with  $n_0 + 1$  generators, whose indices are powers of  $p$ , where  $n_0 = [F : \mathbb{Q}_p]$ . Moreover, the correspondence is such that if a  $p$ -extension  $L$  corresponds to the normal subgroup  $N$ , then the Galois group of  $L$  is isomorphic to the quotient group  $S/N$ . If two  $p$ -extensions  $L$  and  $L_1$  correspond to the normal subgroups  $N$  and  $N_1$  respectively, then  $L \supset L_1$  implies  $N \subset N_1$ , and conversely.*

As consequences of the above theorem we have:

**Corollary 2.** *A  $p$ -group  $G$  is a Galois group of some extension of the field  $F$  if and only if the (minimum) number of generators of  $G$  does not exceed  $n_0 + 1$ .*

**Corollary 3.** *Let  $\circ(G) = p^n$ ,  $s$  be the minimum number of generators of  $G$  and  $\alpha$  be the number of automorphisms of  $G$ . If  $s \leq n_0 + 1$ , then the number of extensions of  $F$ , whose Galois groups are isomorphic to  $G$  is*

$$S(F, G) = \frac{1}{\alpha} p^{(n_0+1)(n-s)} (p^{n_0+1} - 1)(p^{n_0+1} - p) \cdots (p^{n_0+1} - p^{s-1}).$$

**Corollary 4.** *Let  $G$  and  $\overline{G}$  be two  $p$ -groups with  $\overline{G}$  a homomorphic image of  $G$  by some fixed homomorphism, such that the (minimum) number of generators of  $G$ , and hence of  $\overline{G}$ , does not exceed  $n_0 + 1$ . Then for every extension  $\overline{K}/F$  with Galois group  $\overline{G}$ , there exists an extension  $K/F$  with Galois group  $G$  such that  $\overline{K} \subset K$  and the given homomorphism of  $G$  onto  $\overline{G}$  is realized by a natural homomorphism of a Galois group of a field onto a Galois group of a subfield.*

Now we apply these results to show that  $p$  is not fully ramified in the extension  $K_1T/K_0$ . We consider the local fields of  $K_1$ ,  $T$  and  $K_0$ . If  $T_{(p)} \subseteq K_{1(p)}$  then we have  $[K_{1(p)}T_p : K_{0(p)}] = p$ . It follows that  $p$  is not fully ramified in  $K_1T/K_0$  in this case. Therefore we may assume that  $T_{(p)} \not\subseteq K_{1(p)}$ . We will see that  $K_{1(p)}T_p/K_{0(p)}$  is not fully ramified. This will prove that  $p$  is not fully ramified in  $K_1T/K_0$ .

We consider the following two cases:

- (i)  $p$  is fully decomposed in  $K_0/\mathbb{Q}$ ,
- (ii)  $p$  is not fully decomposed in  $K_0/\mathbb{Q}$ .

*Case (i).* In this case we have that  $K_{0(p)} = \mathbb{Q}_p$ . Applying Corollary 3 to  $F = \mathbb{Q}_p$  and  $G = C_p \times C_p$ , we have  $n_0 = 1, s = 2, n = 2$  and  $\alpha =$

$|\text{Aut}(C_p \times C_p)| = (p^2 - 1)(p^2 - p)$ . Then

$$S(\mathbb{Q}_p, C_p \times C_p) = \frac{1}{(p^2 - 1)(p^2 - p)} p^{(2)(0)} (p^2 - 1)(p^2 - p) = 1.$$

Therefore, it follows that  $\mathbb{Q}_p$  has only one extension with group isomorphic to  $C_p \times C_p$ . This extension must be  $K_{1(p)}T_{(p)}$ .

Now, applying Corollary 3 to  $F = \mathbb{Q}_p$  and  $G = C_p$ , we have  $n_0 = 1, n = 1, s = 1$  and  $\alpha = |\text{Aut}(C_p)| = p - 1$ . Then

$$S(\mathbb{Q}_p, C_p) = \frac{1}{p - 1} p^{(2)(0)} (p^2 - 1) = p + 1.$$

Therefore, we have that  $\mathbb{Q}_p$  has  $p + 1$  Galois extensions with Galois group isomorphic to  $C_p$ , all of these are subextensions of  $K_{1(p)}T_{(p)}$ .

On the other hand, it is well known that  $\mathbb{Q}_p$  has a unique unramified extension of degree  $p$ . Therefore this is one of the  $p + 1$  extensions given above. In particular,  $K_{1(p)}T_{(p)}/K_{0(p)}$  is not fully ramified.

*Case (ii).* Let  $p^f, f \geq 1$ , be the inertia degree of  $p$  in  $K_0/\mathbb{Q}$ . Since  $p$  is not ramified in  $K_0/\mathbb{Q}$ , we have that  $K_{0(p)}/\mathbb{Q}_p$  is the unique unramified extension of degree  $p^f$ . From Corollary 2 we observe that for a group  $G$  to be realizable over  $\mathbb{Q}_p$ ,  $s$ , the minimum number of generators of  $G$ , must satisfy  $s \leq 2$ .

We will see that  $K_{1(p)}/\mathbb{Q}_p$  is cyclic. If  $K_{1(p)}/\mathbb{Q}_p$  were not cyclic, then  $\text{Gal}(K_{1(p)}/\mathbb{Q}_p)$  would have 2 generators. On the other hand, since  $T_{(p)} \cap K_{1(p)} = \mathbb{Q}_p$  it follows that

$$\begin{aligned} \text{Gal}(K_{1(p)}T_{(p)}/\mathbb{Q}_p) &\cong \text{Gal}(K_{1(p)}/\mathbb{Q}_p) \times \text{Gal}(T_{(p)}/\mathbb{Q}_p) \\ &\cong \text{Gal}(K_{1(p)}/\mathbb{Q}_p) \times C_p, \end{aligned}$$

which has 3 generators, contrary to Corollary 2. Therefore

$$\text{Gal}(K_{1(p)}/\mathbb{Q}_p) \cong C_{p^{f+1}}$$

and

$$\text{Gal}(K_{1(p)}T_{(p)}/\mathbb{Q}_p) \cong C_{p^{f+1}} \times C_p.$$

Let  $H = C_{p^{f+1}} \times C_p = \langle a, b \rangle$ . It is easy to see that

$$|\text{Aut}(H)| = p^{f+1}(p - 1)p(p - 1) = p^{f+2}(p - 1)^2.$$

Applying Corollary 3 with  $F = \mathbb{Q}_p$  and  $G = H$ , we have  $n_0 = 1, s = 2, n = f + 2$  and  $\alpha = |\text{Aut}(G)| = p^{f+2}(p - 1)^2$ . Then

$$\begin{aligned} S(\mathbb{Q}_p, C_{p^{f+1}} \times C_p) &= \frac{1}{p^{f+2}(p - 1)^2} p^{2(f+2-2)} (p^2 - 1)(p^2 - p) \\ &= p^{f-1}(p + 1). \end{aligned}$$

We have that  $\text{Gal}(K_{0(p)}/\mathbb{Q}_p) \cong C_{p^f}$  and  $|\text{Aut}(C_{p^f})| = p^{f-1}(p-1)$ . Applying Corollary 3 to  $F = \mathbb{Q}_p$  and  $G = C_{p^f}$ , we have  $n_0 = 1, s = 2, n = f$  and  $\alpha = |\text{Aut}(C_{p^f})| = p^{f-1}(p-1)$ . Thus, we obtain

$$\begin{aligned} S(\mathbb{Q}_p, C_{p^f}) &= \frac{1}{p^{f-1}(p-1)} p^{2(f-1)} (p^2 - 1) \\ &= p^{f-1}(p+1). \end{aligned}$$

It follows that

$$S(\mathbb{Q}_p, C_{p^f}) = S(\mathbb{Q}_p, C_{p^{f+1}} \times C_p) = p^{f-1}(p-1), f \geq 1$$

and

$$S(\mathbb{Q}_p, C_p \times C_p) = 1.$$

Let

$$\begin{aligned} \mathcal{A} &= \{L/\mathbb{Q}_p \mid \text{Gal}(L/\mathbb{Q}_p) \cong C_{p^f}\}, \\ \mathcal{B} &= \{E/\mathbb{Q}_p \mid \text{Gal}(E/\mathbb{Q}_p) \cong C_{p^{f+1}} \times C_p\}. \end{aligned}$$

We have that  $C_{p^{f+1}} \times C_p = \langle a, b \rangle$  has a unique subgroup isomorphic to  $C_p \times C_p$ , namely,  $J = \langle a^{p^f}, b \rangle$ .

Let  $\phi : \mathcal{B} \rightarrow \mathcal{A}$  be given by  $\phi(E) = E^J$ . We have  $\text{Gal}(E^J/\mathbb{Q}_p) \cong \frac{\langle a, b \rangle}{\langle a^{p^f}, b \rangle} \cong \langle \bar{a} \rangle \cong C_{p^f}$ .

From Corollary 4 we obtain that given  $L \in \mathcal{A}$ , there exists an extension  $E/\mathbb{Q}_p$  such that  $L \subseteq E$  and  $\text{Gal}(E/\mathbb{Q}_p) \cong C_{p^{f+1}} \times C_p$ . Therefore  $\phi$  is surjective. Since  $|\mathcal{A}| = |\mathcal{B}|$ , it follows that  $\phi$  is bijective.

Thus, we have that  $K_{1(p)}T_{(p)}/\mathbb{Q}_p$  is the unique extension with Galois group  $C_{p^{f+1}} \times C_p$  containing  $K_{0(p)}$ .

Let  $L_p$  be the unique unramified extension of  $\mathbb{Q}_p$  such that  $\text{Gal}(L_p/\mathbb{Q}_p) \cong C_{p^{f+1}}$ . Then  $K_{0(p)} \subseteq L_p$  and  $\text{Gal}(L_p T_{(p)}/\mathbb{Q}_p) \cong C_{p^{f+1}} \times C_p$ .

Therefore,  $L_p T_{(p)} = K_{1(p)} T_{(p)}$  and  $K_{1(p)} T_{(p)}/K_{0(p)}$  is not fully ramified.

Once we have removed the wild ramification, if such exists, we obtain a new extension, denoted again by  $K_1$ , such that  $\text{Gal}(K_1/\mathbb{Q}) \cong G_1$  and  $\text{Ram}(K_1/\mathbb{Q}) = \text{Ram}(K_0/\mathbb{Q})$ . However  $K_1/\mathbb{Q}$  is not necessarily a Scholz extension.

**Second step.** Recovering the fleissig property for the ramified primes.

We follow Serre [19] very closely. We include the details for the sake of completeness.

Let  $q_1, \dots, q_h$  be the ramified prime divisors which are fleissig in  $K_1/\mathbb{Q}$ , and let  $q_{h+1}, \dots, q_s$  be the ramified prime divisors that are not fleissig.

We have

**Proposition 5.** *Let  $M = \mathbb{Q}(\zeta_p, \sqrt[q_1] \dots, \sqrt[q_h])$ ,  $M_1 = M(\sqrt[q_{h+1}])$ ,  $\mathbb{Q}(\zeta_{p^n}) = \mathbb{Q}(\zeta_p)E$ , where  $E/\mathbb{Q}$  is cyclic of degree  $p^{n-1}$ . Then*

- (1)  $K_1$  and  $E$  are linearly disjoint over  $\mathbb{Q}$ ,

(2)  $K_1E$  and  $M_1$  are linearly disjoint over  $\mathbb{Q}$ ,  
where  $K_1$  is as above.

*Proof.* [19], Lemma 2.1.9, page 14.  $\square$

Let  $F = K_1EM$  and  $F_1 = K_1EM_1$ . Then  $F_1/F$  is an extension of degree  $p$ .

Let  $q$  be a prime in  $\mathbb{Q}$  such that  $q$  has a divisor of degree one in  $F/\mathbb{Q}$  and  $q$  is inert in  $F_1/F$ .

Let  $E_q$  be the subextension of  $\mathbb{Q}(\zeta_q)/\mathbb{Q}$  of degree  $p$ . Since  $x^p - q_{h+1}$  is irreducible over  $F$  and  $q$  is inert in  $F_1/F$ , we have that  $x^p - q_{h+1}$  is irreducible modulo  $q$ . Let  $\alpha \in \overline{\mathbb{F}}_q \setminus \mathbb{F}_q$  be such that

$$\alpha^p \equiv q_{h+1} \pmod{q}.$$

Let  $q - 1 = rp^t$ ,  $r = \frac{q-1}{p^t}$ ,  $t \geq 1$ ,  $(r, p) = 1$ . Then we have

$$q_{h+1}^{q-1} \equiv 1 \pmod{q}.$$

If we had that  $q_{h+1}^{\frac{q-1}{p}} \equiv 1 \pmod{q}$ , then  $\alpha^{q-1} \equiv q_{h+1}^{\frac{q-1}{p}} \equiv 1 \pmod{q}$ . Hence  $\alpha \in \mathbb{F}_q$ , which contradicts the choice of  $\alpha$ . Thus,  $q_{h+1}^r \not\equiv 1 \pmod{q}$  and the inertia degree of  $q_{h+1}$  in  $\mathbb{Q}(\zeta_q)/\mathbb{Q}$  is divisible by  $p^t$ . Hence  $q_{h+1}$  is inert in  $E_q/\mathbb{Q}$ .

Thus, in  $E_q/\mathbb{Q}$  we have that  $q_1, \dots, q_h$  are fully decomposed,  $q_{h+1}$  is inert and  $q$  is fully ramified.

We have that  $q_{h+1}$  is inert in  $K_0E_q/K_0$  and in  $K_1/K_0$ . Since  $K_1E_q/K_0$  is not cyclic,  $q_{h+1}$  is not fully inert in  $K_1E_q/K_0$ . Let  $K'_1$  be the field fixed by the decomposition group of  $q_{h+1}$ . Then

- (i)  $\text{Gal}(K'_1/\mathbb{Q}) \cong \text{Gal}(K_1/\mathbb{Q}) \cong G_1$ ,
- (ii)  $q_{h+1}$  is decomposed in  $K'_1/K_0$ , in particular  $q_{h+1}$  is fleissig in  $K'_1/\mathbb{Q}$ ,
- (iii)  $q_1, \dots, q_h$  are fleissig in  $K'_1/\mathbb{Q}$ ,
- (iv)  $q$  is ramified and fleissig in  $K'_1/\mathbb{Q}$ .

Now we will remove the ramification of  $q$  keeping the fleissig property for  $\{q_1, \dots, q_{h+1}\}$ .

Let  $E_i/\mathbb{Q}$ ,  $i = 1, \dots, h+1$  and  $E_q/\mathbb{Q}$  be the extensions of  $\mathbb{Q}$  such that

- (i)  $\text{Gal}(E_i/\mathbb{Q}) \cong C_p$ ,  $i = 1, \dots, h+1$  and  $\text{Gal}(E_q/\mathbb{Q}) \cong C_p$ ,
- (ii)  $q_i$  is fully ramified in  $E_i/\mathbb{Q}$  and it is the unique ramified prime divisor;  
 $q$  is fully ramified in  $E_q/\mathbb{Q}$  and it is the unique ramified prime divisor.

Using the technique of Madan [9], let  $E \subseteq E_{q_{h+1}}E_q$  be an extension such that  $[E : \mathbb{Q}] = p$  and  $q_{h+1}$  and  $q$  are ramified in  $E/\mathbb{Q}$ . We have that  $q_i$ ,  $1 \leq i \leq h$ , are decomposed in  $E_{q_{h+1}}$  (Proposition 4) and in  $E_q$ . It follows that they are decomposed in  $E$ .

Furthermore  $E$  is not contained in  $K_0$  because  $q$  is ramified in  $E$  but not in  $K_0$ . It follows that  $E$  is not contained in  $K'_1$  since otherwise  $EK_0 \subseteq K'_1$

would imply  $EK_0 = K'_1$ , but this can not be, since  $\text{Gal}(EK_0/\mathbb{Q})$  is a split group extension of  $G_0$ , whereas  $\text{Gal}(K'_1/\mathbb{Q})$  is not. Therefore,  $E \cap K'_1 = \mathbb{Q}$ .

Similarly to when we removed the new tame ramification, we obtain an extension  $K''_1/\mathbb{Q}$  such that  $\text{Gal}(K''_1/\mathbb{Q}) \cong \text{Gal}(K'_1/\mathbb{Q}) \cong G_1$ , the prime divisors above  $q_i$ ,  $1 \leq i \leq h$ , are decomposed in  $EK_0/K_0$ . Therefore  $q_1, \dots, q_{h+1}$  are fleissig in  $K''_1/\mathbb{Q}$  and  $q$  is not ramified in  $K''_1/\mathbb{Q}$ .

Continuing with this process, we obtain an extension, denoted again by  $K_1$ , such that  $\text{Gal}(K_1/\mathbb{Q}) \cong G_1$ ,  $\text{Ram}(K_1/\mathbb{Q}) = \text{Ram}(K_0/\mathbb{Q}) = \{q_1, \dots, q_s\}$  and the ramified primes are fleissig. That is,  $K_1/\mathbb{Q}$  is a Scholz extension.

By induction, we assume that we have constructed an extension  $K_{\nu-1}/\mathbb{Q}$  such that

- (i)  $K_{\nu-2} \subset K_{\nu-1}$ ,
- (ii)  $\text{Gal}(K_{\nu-1}/\mathbb{Q}) \cong G_{\nu-1}$ ,
- (iii)  $\text{Ram}(K_{\nu-1}/\mathbb{Q}) = \text{Ram}(K_0/\mathbb{Q})$ ,
- (iv) the ramified primes are fleissig.

That is,  $K_{\nu-1}/\mathbb{Q}$  is a Scholz extension. From Theorem 1, we have that there exists an extension  $K_\nu/\mathbb{Q}$  such that  $K_{\nu-1} \subset K_\nu$  and  $\text{Gal}(K_\nu/\mathbb{Q}) \cong G_\nu$ .

We proceed as in the case  $K_0$ . In this case we do not need that the extension  $K_0/\mathbb{Q}$  be abelian and the proofs can be applied to  $K_{\nu-1}$ . We first remove new ramification and then we modify the extension in order to have that the ramified prime divisors are fleissig. We obtain an extension, denoted again by  $K_\nu$ , such that  $\text{Gal}(K_\nu/\mathbb{Q}) \cong G_\nu$  and  $\text{Ram}(K_\nu/\mathbb{Q}) = \text{Ram}(K_0/\mathbb{Q})$ .

The field  $K_\nu$  satisfies the required conditions. □

### 3. Case $G$ a nilpotent group of odd order.

In this section  $G$  will denote a nilpotent group of odd order and  $s$  will denote the minimum number of generators of  $G$ .

Since  $G$  is nilpotent, we have

$$G = G_{p_1} \times \dots \times G_{p_r},$$

where  $G_{p_i}$  is a  $p_i$ -group,  $|G_{p_i}| = p_i^{n_i}$ ,  $p_1, \dots, p_r$  are distinct odd primes.

Let  $s_i = \dim_{\mathbb{F}_{p_i}} G_{p_i}/\Phi(G_{p_i})$ , where  $\Phi(G_{p_i})$  is the Frattini subgroup of  $G_{p_i}$ . Reordering  $p_1, \dots, p_r$ , we may assume  $s_1 \geq s_2 \geq \dots \geq s_r$ . Then  $s_i$  is the minimum number of generators of  $G_{p_i}$ ,  $i = 1, \dots, r$ , and  $s = s_1$ .

By Theorem 3, we obtain that there exist extensions  $L_i/\mathbb{Q}$ ,  $i = 1, \dots, r$ , such that  $\text{Gal}(L_i/\mathbb{Q}) \cong G_{p_i}$  and  $|\text{Ram}(L_i/\mathbb{Q})| = s_i$ .

The extension  $L/\mathbb{Q}$ , where  $L = L_1 \cdots L_r$  satisfies  $\text{Gal}(L/\mathbb{Q}) \cong G$  and  $|\text{Ram}(L/\mathbb{Q})| \geq s$ .

We will prove that there exists a collection of extensions  $L_i/\mathbb{Q}$  satisfying the conditions given in Theorem 3, and such that  $\text{Ram}(L_i/\mathbb{Q}) \subset \text{Ram}(L_1/\mathbb{Q})$ ,  $i = 2, \dots, r$ .

The following proposition is a direct generalization of Proposition 3.

**Proposition 6.** *Let  $p_1, \dots, p_r$ , be distinct odd primes,  $n_1, \dots, n_r$  and  $s$  are positive integers. Then there exist infinitely many collections of  $s$  primes  $\{q_1, \dots, q_s\}$  such that*

- (i)  $q_1 \equiv 1 \pmod{\prod_{i=1}^r p_i^{n_i}}$ .
- (ii) For  $2 \leq j \leq s$ ,  $q_j$  is fully decomposed in

$$\mathbb{Q}\left(\zeta_{p_i}^{n_i}, \zeta_{q_1}, \dots, \zeta_{q_{j-1}}, \sqrt[p_i]{q_1}, \dots, \sqrt[p_i]{q_{j-1}}; i = 1, \dots, r\right) / \mathbb{Q}.$$

The following proposition is a direct generalization of Proposition 4. For each  $i$ ,  $1 \leq i \leq r$ , we set  $G_{0_i} := G_{p_i} / G'_{p_i}$ .

**Proposition 7.** *Let  $p_1, \dots, p_r$ , be distinct odd primes,  $n_1, \dots, n_r$  and  $s$  be positive integers. Then there exist infinitely many collections of  $r$  fields  $\{F_{0_1}, \dots, F_{0_r}\}$  such that*

- (i)  $\text{Gal}(F_{0_i} / \mathbb{Q}) \cong G_{0_i}$ ,
- (ii)  $|\text{Ram}(F_{0_i} / \mathbb{Q})| \leq s$ ,
- (iii)  $\text{Ram}(F_{0_i} / \mathbb{Q}) \subseteq \text{Ram}(F_{0_1} / \mathbb{Q}) \quad i = 2, \dots, r$ ,
- (iv) the primes ramified in  $F_{0_i} / \mathbb{Q}$ ,  $i = 1, \dots, r$  are fleissig.

Therefore there exists  $L_{0_i} / \mathbb{Q}$  a Scholz extension such that  $\text{Gal}(L_{0_i} / \mathbb{Q}) \cong G_{0_i}$ ,  $\text{Ram}(L_{0_i} / \mathbb{Q}) \subset \text{Ram}(L_{0_1} / \mathbb{Q})$ ,  $i = 2, \dots, r$ , and  $|\text{Ram}(L_{0_1} / \mathbb{Q})| = s$ .

**Theorem 5.** *Let  $G$  be a nilpotent group of odd order. Then there exists an extension  $L / \mathbb{Q}$  such that  $\text{Gal}(L / \mathbb{Q}) \cong G$  and  $|\text{Ram}(L / \mathbb{Q})| = s$ .*

*Proof.* Let  $\{F_{0_1}, \dots, F_{0_r}\}$  be a collection given in Proposition 7. It follows from Theorem 3 that there exist fields  $F_1, \dots, F_r$  such that  $F_{0_i} \subset F_i$ ,  $\text{Gal}(F_i / \mathbb{Q}) \cong G_{p_i}$ ,  $|\text{Ram}(F_i / \mathbb{Q})| = s_i$  and  $\text{Ram}(F_i / \mathbb{Q}) = \text{Ram}(F_{0_i} / \mathbb{Q})$ . The field  $L = F_1 \cdots F_r$  satisfies the required conditions.  $\square$

#### 4. Minimal ramification.

We will prove that the number of ramified primes in a finite nilpotent extension  $K / \mathbb{Q}$  is greater than or equal to the minimum number of generators of  $\text{Gal}(K / \mathbb{Q})$ .

**Theorem 6.** *Let  $G$  be a nilpotent group of odd order. Let  $K / \mathbb{Q}$  be a finite Galois extension with Galois group  $G$ . If  $r$  is the number of ramified rational primes in  $K / \mathbb{Q}$ , we have that  $r \geq s$ , where  $s$  is the minimum number of generators of  $G$ .*

*Proof.* We have that the minimum number of generators of  $G$  equals the minimum number of generators of a  $p$ -Sylow subgroup of  $G$  for some  $p | o(G)$ . Therefore it suffices to prove the theorem for a  $p$ -group.

Thus, we consider  $G$  a  $p$ -group. Let  $G'$  be the commutator subgroup of  $G$ . Let  $E = K^{G'}$ . Then  $E / \mathbb{Q}$  is abelian.

Let  $t$  be the number of ramified rational primes in  $E/\mathbb{Q}$ . Therefore,  $t \leq r$ . Thus, it suffices to prove that  $s \leq t$ .

We have that  $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^* = \mathcal{G}$ . By a *Dirichlet character*  $\chi \bmod n$  we understand a multiplicative homomorphism  $\chi: \mathcal{G} \rightarrow \mathbb{C}^*$ . If  $\Omega_n$  is the group of characters  $\bmod n$  we have that  $\Omega_n = \widehat{\mathcal{G}} \cong \mathcal{G}$  under the pairing

$$\begin{aligned} \Omega_n \times \mathcal{G} &\rightarrow \mathbb{C}^* \\ (\chi, a) &\rightarrow \chi(a). \end{aligned}$$

For any subgroup  $Z$  of  $\mathcal{G}$ , let  $Z^\perp = \{\chi \in \widehat{\mathcal{G}} \mid \chi(y) = 1 \forall y \in Z\}$ . Then  $Z^\perp \cong \widehat{(\mathcal{G}/Z)}$  and  $Z^{\perp\perp} \cong Z$  when we identify  $\widehat{\widehat{\mathcal{G}}} \cong \mathcal{G}$ . We also have that  $Z = \bigcap_{\chi \in Z^\perp} \ker \chi$ .

Let  $E \subseteq \mathbb{Q}(\zeta_n)$  for some  $n$ . Let  $H = \text{Gal}(E/\mathbb{Q})$ ,  $Z = \text{Gal}(\mathbb{Q}(\zeta_n)/E)$ . Then  $H \cong \mathcal{G}/Z \cong \widehat{(\mathcal{G}/Z)} \cong Z^\perp$ .

We set  $X = Z^\perp$  which is called the group of Dirichlet characters associated to the field  $E$ .

Let  $n = \prod p^a$ . Corresponding to the canonical decomposition  $(\mathbb{Z}/n\mathbb{Z})^* \cong \prod (\mathbb{Z}/p^a\mathbb{Z})^*$  we may write any character  $\bmod n$  as  $\chi = \prod \chi_p$  where  $\chi_p$  is a character  $\bmod p^a$ . We let  $X_p = \{\chi_p \mid \chi \in X\}$ .

Let  $q_1, \dots, q_t$  be the rational primes ramified in  $E/\mathbb{Q}$ . Then, we have that  $|X_{q_i}| > 1, i = 1, \dots, t$  and  $|X_q| = 1$  for every rational prime  $q \notin \{q_1, \dots, q_t\}$  ([20, Theorem 3.5]). Since  $G$  is a  $p$ -group,  $X_{q_i}$  is a  $p$ -group and  $X_{q_i} \subseteq \widehat{\mathcal{G}}_i$  where  $\mathcal{G}_i = \text{Gal}(\mathbb{Q}(\zeta_{q_i^{m_i}})^+/\mathbb{Q})$  for some  $m_i \geq 1$ . Therefore  $X_{q_i}$  is a cyclic  $p$ -group, say  $X_{q_i} \cong C_{p^{a_i}}$ .

Let  $Y = X_{q_1} \times \dots \times X_{q_t} \cong C_{p^{a_1}} \times \dots \times C_{p^{a_t}}$ , and let  $F$  be its associated field. Then  $X \subseteq Y$ . Therefore we have that  $E \subseteq F$ .

We have  $\text{Gal}(F/\mathbb{Q}) \cong Y \cong C_{p^{a_1}} \times \dots \times C_{p^{a_t}}$ . Since  $E \subseteq F$ ,  $G = \text{Gal}(E/\mathbb{Q})$  is a quotient of  $\text{Gal}(F/\mathbb{Q})$  and the minimum number of generators of  $Y$  is  $t$ . Hence  $s \leq t$ . Therefore  $s \leq r$ .  $\square$

**Remark 1.** If  $p = 2$ , the result of Theorem 6 is not longer true for rational prime divisors. For instance,  $\text{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) \cong C_2 \times C_2$  has two generators and 2 is the only ramified rational prime divisor. In this case Theorem 6 holds if we include also the infinite prime.

Theorem 6 shows that the extension  $K/\mathbb{Q}$  constructed in Section 2 is optimal in the sense that we have obtained the minimum number of possible ramified primes.

Now we prove the existence of a finite Galois extension  $L/\mathbb{Q}$  such that the number of ramified rational primes in  $L/\mathbb{Q}$  is less than the minimum number of generators of  $\text{Gal}(L/\mathbb{Q})$ . From Theorem 6, we have that  $\text{Gal}(L/\mathbb{Q})$  is not a nilpotent group.

**Theorem 7.** *Let  $p$  be an odd prime. Then  $p$  is irregular if and only if there is an extension  $K/\mathbb{Q}(\zeta_p)^+$ , with  $K \neq \mathbb{Q}(\zeta_{p^2})^+$  such that  $\text{Gal}(K/\mathbb{Q}(\zeta_p)^+) \cong C_p$ , and such that it is unramified outside  $p$ .*

*Proof.* [20], Proposition 10.13, page 193. □

**Theorem 8.** *If  $p$  is an irregular prime, then there is a Galois extension  $F/\mathbb{Q}$  such that*

- (i) *the minimum number of generators of  $\text{Gal}(F/\mathbb{Q})$  is greater than or equal to 2,*
- (ii) *the number of ramified primes in  $F/\mathbb{Q}$  is 1.*

*Furthermore, the only ramified prime in  $F/\mathbb{Q}$  is  $p$ .*

*Proof.* Let  $K/\mathbb{Q}(\zeta_p)^+$  be the extension given in Theorem 7. Let  $F/\mathbb{Q}(\zeta_p)^+$  be the maximal abelian  $p$ -extension which is unramified outside  $p$ . Then we have that  $K \subseteq F$  and  $F/\mathbb{Q}$  is Galois.

Let us see that  $F/\mathbb{Q}$  is not cyclic. Since  $F/\mathbb{Q}$  is a Galois extension,  $F(\zeta_p)/\mathbb{Q}$  is also a Galois extension. If  $F(\zeta_p)/\mathbb{Q}$  were abelian, from the Kronecker-Weber theorem, we would obtain that  $F(\zeta_p) \subseteq \mathbb{Q}(\zeta_{p^n})$ , for some  $n$ , since  $F(\zeta_p)/\mathbb{Q}$  is unramified outside  $p$  and the infinite prime. Therefore  $F \subseteq \mathbb{Q}(\zeta_{p^n})^+$ . This contradicts the choice of  $K$ . Therefore,  $F(\zeta_p)/\mathbb{Q}$  is not abelian and  $F/\mathbb{Q}$  is not a cyclic extension.

In short, we have that  $F/\mathbb{Q}$  is a Galois extension which is not cyclic and it is unramified outside  $p$ . That is,  $F/\mathbb{Q}$  satisfies the required conditions. Since there are infinitely many irregular primes, we obtain that there exist infinitely many such extensions. □

## 5. Nilpotent extensions of number fields.

In this section  $K$  will denote a number field such that  $K \cap \mathbb{Q}(\zeta_{p_i^{n_i}}) = \mathbb{Q}$  for each prime  $p_i$  such that  $p_i^{n_i} | \circ(G)$  and  $p_i^{n_i+1} \nmid \circ(G)$  and there is a prime  $q \in \mathbb{Q}$  such that  $q$  is inert in  $K/\mathbb{Q}$ .

**Proposition 8.** *Let  $K$  be a number field such that exists a rational prime  $q$  inert in  $K/\mathbb{Q}$ . Then there exist infinitely many rational primes inert in  $K/\mathbb{Q}$ .*

*Proof.* Let  $\tilde{K}$  be the Galois closure of  $K/\mathbb{Q}$  and let  $\Omega = \text{Gal}(\tilde{K}/\mathbb{Q})$ . Since  $q$  is unramified in  $K/\mathbb{Q}$ , we have that  $q$  is unramified in  $\tilde{K}/\mathbb{Q}$ . Let  $\mathfrak{Q}$  be a prime divisor of  $\tilde{K}$  over  $q$ , and let  $\sigma = \left[ \begin{array}{c} \tilde{K}/\mathbb{Q} \\ \mathfrak{Q} \end{array} \right]$  be its Frobenius automorphism.

Set  $H = \langle \sigma \rangle$ .

Let  $M = \tilde{K}^H$ . From Tchebotarev density theorem, we have that there exist infinitely many rational primes that have a divisor of degree one in

$M/\mathbb{Q}$  and are inert in  $\tilde{K}/M$ . The prime divisor  $q$  satisfies this property. Since the decomposition group of  $\mathfrak{Q}$  is  $H$  and  $H \text{ Gal}(\tilde{K}/K) = \text{Gal}(\tilde{K}/\mathbb{Q})$ , it follows that  $M \cap K = \mathbb{Q}$ .

Let  $H_1 = \text{Gal}(\tilde{K}/K)$ . Since  $q$  is inert in  $K/\mathbb{Q}$  we have that  $q\mathfrak{D}_K$  is a prime divisor in  $K$ . It follows [11, Theorem 33] that  $\Omega = H_1 \cup H_1\sigma \cup \dots \cup H_1\sigma^{m-1}$  with  $m$  such that  $\sigma^m \in H_1$ .

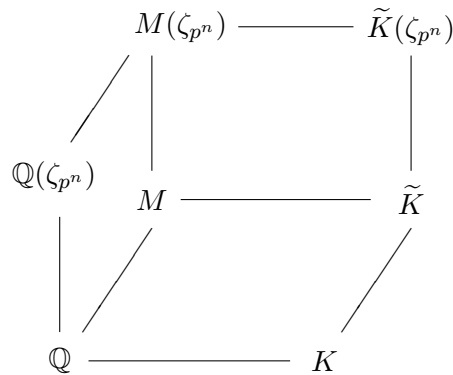
Let  $t_{\tilde{K}}$  be a prime divisor in  $\tilde{K}$ , which is inert in  $\tilde{K}/M$  and  $t_{\tilde{K}} \cap \mathbb{Q}$  has a divisor of degree one in  $M/\mathbb{Q}$ . We will see that its restriction to  $K$  is inert in  $K/\mathbb{Q}$ .

Let  $t_K = t_{\tilde{K}} \cap K$  and  $t = t_{\tilde{K}} \cap \mathbb{Q} = t_K \cap \mathbb{Q}$  be the restrictions to the respective fields. Then  $\left[ \frac{\tilde{K}/\mathbb{Q}}{t_{\tilde{K}}} \right] = \sigma$ . Since  $\Omega = H_1 \cup H_1\sigma \cup \dots \cup H_1\sigma^{m-1}$  from [11] follows that  $t_K = t\mathfrak{D}_K$  and  $t$  is inert in  $K/\mathbb{Q}$ .

Thus, we have shown that the restrictions of prime ideals of  $\tilde{K}$  to  $K$  inert in  $\tilde{K}/M$ , are inert in  $K/\mathbb{Q}$ . Therefore, there are infinitely many prime divisors inert in  $K/\mathbb{Q}$ .  $\square$

**Proposition 9.** *Let  $K$  be a number field that satisfies the conditions above and let  $\tilde{K}$  be the Galois closure of  $K/\mathbb{Q}$ . We consider  $l$  a rational prime inert in  $K$ . Let  $H$  be the subgroup of  $\text{Gal}(\tilde{K}/\mathbb{Q})$  generated by the Frobenius automorphism of a prime divisor of  $\tilde{K}$  above  $l$  and let  $M = \tilde{K}^H$ . Let  $q$  be any rational prime that has a divisor of degree one in  $M(\zeta_{p^n})/\mathbb{Q}$  and is inert in  $\tilde{K}(\zeta_{p^n})/M(\zeta_{p^n})$ . Then  $q$  is inert in  $K/\mathbb{Q}$ .*

*Proof.* Consider the following lattice of fields



We have that the rational prime  $q$  has a divisor of degree one in  $M/\mathbb{Q}$  and is inert in  $\tilde{K}(\zeta_{p^n})/M(\zeta_{p^n})$ . Thus, from the proof of Proposition 8, it follows that  $q$  is inert in  $\tilde{K}/M$  and that  $q$  is inert in  $K/\mathbb{Q}$ .  $\square$

From Tchebotarev density theorem, we have that there exist infinitely many rational primes satisfying the conditions in Proposition 9. Furthermore, we have that  $q$  has a divisor of degree one in  $\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}$ .

**Proposition 10.** *Let  $p$  be an odd prime number,  $n$  and  $s$  positive integers. Then there are infinitely many collections of  $s$  primes  $\{q_1, \dots, q_s\}$  that satisfy*

- (i)  $q_1 \equiv 1 \pmod{p^n}$ ,
- (ii) for  $2 \leq i \leq s$ ,  $q_i$  has a divisor of degree one in  $\mathbb{Q}(\zeta_{p^n}, \zeta_{q_1}, \dots, \zeta_{q_{i-1}}, \sqrt[p^n]{q_1}, \dots, \sqrt[p^n]{q_{i-1}})/\mathbb{Q}$ .
- (iii)  $q_i$  is inert in  $K/\mathbb{Q}$ ,  $i = 1, \dots, s$ .

*Proof.* By Tchebotarev density theorem, we have that there exists a rational prime  $q_1$  satisfying the conditions of Proposition 9. Therefore  $q_1$  is inert in  $K/\mathbb{Q}$ . Since  $q_1$  has a divisor of degree one in  $\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}$ , it follows that  $q_1 \equiv 1 \pmod{p^n}$ .

Let  $F_1 = \mathbb{Q}(\zeta_{p^n}, \zeta_{q_1}, \sqrt[p^n]{q_1})$ ,  $L_1 = F_1M$ ,  $\tilde{L}_1 = L_1\tilde{K}$  and  $M$  as in Proposition 9.

Since  $\tilde{L}_1/L_1$  is cyclic, it follows by Tchebotarev density theorem that there exists a rational prime  $q_2$  that has a divisor of degree one in  $L_1/\mathbb{Q}$  and is inert in  $\tilde{L}_1/L_1$ . Therefore  $q_2$  has a divisor of degree one in  $F_1/\mathbb{Q}$  and  $q_2$  satisfies the conditions of Proposition 9. Therefore  $q_2$  is inert in  $K/\mathbb{Q}$ . Let  $F_2 = F_1(\zeta_{q_2}, \sqrt[p^n]{q_2})$ ,  $L_2 = F_2M$  and  $\tilde{L}_2 = L_2\tilde{K}$ .

Since  $\tilde{L}_2/L_2$  is cyclic, it follows by Tchebotarev density theorem that there exists a rational prime  $q_3$  that has a divisor of degree one in  $L_2/\mathbb{Q}$  and is inert in  $\tilde{L}_2/L_2$ . Therefore,  $q_3$  has a divisor of degree one in  $F_2/\mathbb{Q}$  and it satisfies the conditions of Proposition 9. Hence,  $q_3$  is inert in  $K/\mathbb{Q}$ . Continuing with this process we obtain such a collection. By Tchebotarev density theorem, we have that there exist infinitely many of these collections.  $\square$

Let  $\text{Iner}(K/\mathbb{Q}) = \{q \in \mathbb{Q} \mid q \text{ is inert in } K/\mathbb{Q}\}$ .

**Theorem 9.** *Let  $G$  be a finite  $p$ -group of order  $p^n$  and let  $K$  be a number field such that  $K \cap \mathbb{Q}(\zeta_{p^n}) = \mathbb{Q}$  and such that there exists a prime divisor  $q$  inert in  $K/\mathbb{Q}$ . Then there exists an extension  $E/K$  such that  $E/K$  is a Galois extension with  $\text{Gal}(E/K) \cong G$  and  $|\text{Ram}(E/K)| = s$ , where  $s$  is the minimum number of generators of  $G$ .*

*Proof.* Let  $G'$  be the commutator subgroup of  $G$ . Let  $|G'| = p^t, 1 \leq t \leq n, |G| = p^n$ . We have that  $G/G'$  is an abelian group, say  $G/G' = C_{p^{a_1}} \times \dots \times C_{p^{a_s}}$ .

Let  $G_0 = G/G', G_1, \dots, G_t = G$  be such that  $G_{i-1} \cong G_i/H_i, i = 1, \dots, t$  with  $H_i \subseteq Z(G_i)$  and  $|H_i| = p$ .

Let  $\{q_1, \dots, q_s\}$  be a collection given by Proposition 10. By Proposition 4 and Corollary 1 we have that there exists a Scholz extension  $L/\mathbb{Q}$ , such that  $\text{Gal}(L/\mathbb{Q}) \cong G_0$  and  $\text{Ram}(L/\mathbb{Q}) = \{q_1, \dots, q_s\}$ . Hence, from Theorem 3 we have that there exists  $F/\mathbb{Q}$  such that  $L \subset F$ ,  $\text{Gal}(F/\mathbb{Q}) \cong G$  and  $\text{Ram}(F/\mathbb{Q}) = \{q_1, \dots, q_s\}$ .

Let  $E = FK$ . Since  $\{q_1, \dots, q_s\} \subset \text{Iner}(K/\mathbb{Q})$ , we have that above each  $q_i, i = 1, \dots, s$ , there is only one prime divisor  $Q_i$  in  $K$ . Therefore  $E$  satisfies the required conditions.  $\square$

Now we consider  $G$  a nilpotent group of odd order.

Let  $G$  be a nilpotent group of odd order and  $s$  the minimum number of generators of  $G$ .

Since  $G$  is nilpotent, we have

$$G = G_{p_1} \times \cdots \times G_{p_r},$$

where  $G_{p_i}$  is a  $p_i$ -group,  $|G_{p_i}| = p_i^{n_i}$ ,  $p_1, \dots, p_r$  distinct odd primes.

Let  $s_i = \dim_{\mathbb{F}_{p_i}} G_{p_i}/\Phi(G_{p_i})$ , where  $\Phi(G_{p_i})$  is the Frattini subgroup of  $G_{p_i}$ . Reordering  $p_1, \dots, p_r$ , we may assume  $s_1 \geq s_2 \geq \cdots \geq s_r$ . We have that  $s_i$  is the minimum number of generators of  $G_{p_i}$ ,  $i = 1, \dots, r$  and that  $s = s_1$ .

By Theorem 9, we have that there exist extensions  $E_i/K, i = 1, \dots, r$ , such that  $\text{Gal}(E_i/K) \cong G_{p_i}$  and  $|\text{Ram}(E_i/K)| = s_i$ . Let us consider the extension  $E/K$  where  $E = E_1 \cdots E_r$ . We have  $\text{Gal}(E/K) \cong G$  and  $|\text{Ram}(E/K)| \geq s$ . Therefore we will have a solution if we prove that there exists a collection of extensions  $E_i/K, i = 1, \dots, r$ , with the conditions given in Theorem 9 and that satisfies the condition

$$\text{Ram}(E_i/K) \subset \text{Ram}(E_1/K), i = 2, \dots, r.$$

For this end it suffices to prove that there exist extensions  $L_i/\mathbb{Q}, i = 1, \dots, r$  such that  $\text{Gal}(L_i/\mathbb{Q}) \cong G_{p_i}$ ,  $|\text{Ram}(L_i/\mathbb{Q})| = s_i$  and  $\text{Ram}(L_i/\mathbb{Q}) \subset \text{Ram}(L_1/\mathbb{Q}) \subset \text{Iner}(K/\mathbb{Q}), i = 2, \dots, r$ . The following proposition is a direct generalization of Proposition 10.

**Proposition 11.** *Let  $p_1, \dots, p_r$  be distinct odd primes,  $n_1, \dots, n_r$  and  $s$  positive integers. Then there are infinitely many collections of  $s$  primes  $\{q_1, \dots, q_s\}$  that satisfy*

$$(i) \quad q_1 \equiv 1 \left( \text{mod} \prod_{i=1}^r p_i^{n_i} \right).$$

(ii) *For  $2 \leq j \leq s, q_j$  is fully decomposed in*

$$\mathbb{Q} \left( \zeta_{p_i}^{n_i}, \zeta_{q_1}, \dots, \zeta_{q_{j-1}}, \sqrt[p_i]{q_1}, \dots, \sqrt[p_i]{q_{j-1}}; i = 1, \dots, r \right) / \mathbb{Q},$$

(iii)  *$q_i$  is inert in  $K/\mathbb{Q}$ ,  $i = 1, \dots, s$ .*

Let  $\{q_1, \dots, q_s\}$  be a collection of  $s$  primes satisfying the conditions of Proposition 11. By Proposition 7 and Theorem 3 we obtain that there exist

fields  $L_i, i = 1, \dots, r$  such that  $\text{Gal}(L_i/\mathbb{Q}) \cong G_{p_i}$ ,  $|\text{Ram}(L_i/\mathbb{Q})| = s_i$  and  $\text{Ram}(L_i/\mathbb{Q}) \subset \text{Ram}(L_1/\mathbb{Q}) \subset \text{Iner}(K/\mathbb{Q}), i = 2, \dots, r$ .

Let  $E_i = L_i K, i = 1, \dots, r$ . Then the collection  $\{E_1, \dots, E_r\}$  satisfies:  $\text{Gal}(E_i/K) \cong G_{p_i}$ ,  $\text{Ram}(E_i/K) \subset \text{Ram}(E_1/K), i = 1, \dots, r$ .

Finally, we have:

**Theorem 10.** *Let  $G$  be a nilpotent group of odd order and let  $K$  be a number field such that  $K \cap \mathbb{Q}(\zeta_{p_i}^{n_i}) = \mathbb{Q}$  for each prime  $p_i$  such that  $p_i^{n_i} \mid \circ(G)$  and  $p_i^{n_i+1} \nmid \circ(G)$  and there is a prime  $q \in \mathbb{Q}$  such that  $q$  is inert in  $K/\mathbb{Q}$ . Then there exists  $E/K$  such that  $\text{Gal}(E/K) \cong G$  and  $|\text{Ram}(E/K)| = s$ .*

*Proof.* Let  $E_i, i = 1, \dots, r$  be the collection given above. Let  $E = E_1 \cdots E_r$ . Then  $E$  satisfies the required conditions.  $\square$

**Acknowledgment.** The authors would like to thank the referee for his (her) very careful reading of the manuscript and for his (her) suggestions that have led to improvements in the exposition.

## References

- [1] S. Abhyankar, *Coverings of algebraic curves*, Amer. J. Math., **79** (1957), 825-856.
- [2] R. Brauer, *Über die Konstruktion der Schiefkörper, die von endlichem Rang in Bezug auf ein gegebenes Zentrum sind*, J. Reine Angew. Math., **168** (1932), 44-64.
- [3] J.W.S. Cassels and A. Fröhlich, *Algebraic Number Theory*, Academic Press, London, 1967.
- [4] M.D. Fried and M. Jarden, *Field Arithmetic*, Ergebnisse der Mathematik, **11**, Springer-Verlag, Berlin, Heidelberg, 1986.
- [5] W.-D. Geyer and M. Jarden, *Bounded realization of  $l$ -groups over global fields. The method of Scholz and Reichardt*, Nagoya Math. J., **150** (1998), 13-62.
- [6] G.J. Janusz, *Algebraic Number Fields*, Academic Press, New York, 1973.
- [7] H. Koch, *Number Theory II*, Encyclopaedia of Mathematical Sciences, **62**, Springer-Verlag, 1992.
- [8] S. Lang, *Algebraic Number Theory*, Graduate Text in Mathematics, **110**, Springer-Verlag, 1986.
- [9] M.L. Madan, *On class numbers of algebraic number fields*, J. Number Theory, **2** (1970), 116-119.
- [10] M.L. Madan, M. Rzedowski-Calderón and G. Villa-Salvador, *Galois extensions with bounded ramification in characteristic  $p$ . On a question of S. Abhyankar*, Manuscripta Math., **90** (1996), 121-135.
- [11] D.A. Marcus, *Number Fields*, Universitext, Springer-Verlag, 1977.
- [12] H. Reichardt, *Konstruktion von Zahlkörpern mit gegebener Galoisgruppe von Primzahlpotenzordnung*, J. Reine Angew. Math., **177** (1937), 1-5.
- [13] M. Rzedowski-Calderón, *Construction of global function fields with nilpotent automorphism groups*, Boletín de la Sociedad Matemática Mexicana, **34** (1989), 1-10.

- [14] M. Rzedowski-Calderón and G. Villa-Salvador, *Automorphisms of congruence function fields*, Pacific J. of Math., **150** (1991), 167-178.
- [15] I.R. Šafarevič, *On  $p$ -extensions*, Am. Math. Soc. Transl. Ser. 2, **4** (1956), 59-72.
- [16] ———, *On the construction of fields with a given Galois group of order  $\ell^\alpha$* , Am. Math. Soc. Transl. Ser. 2, **4** (1956), 107-142.
- [17] ———, *Construction of fields of algebraic numbers with given solvable Galois group*, Am. Math. Soc. Transl. Ser. 2, **4** (1956), 185-237.
- [18] A. Scholz, *Konstruktion algebraischer Zahlkörper mit beliebiger Gruppe von Primzahlpotenzordnung I*, Math. Z., **42** (1936), 161-188.
- [19] J.-P. Serre, *Topics in Galois Theory*, Jones and Barlett, Boston, 1992.
- [20] L.C. Washington, *Introduction to Cyclotomic Fields*, GTM, **83**, Springer-Verlag, New York, 1982.
- [21] E. Weiss, *Algebraic Number Theory*, McGraw Hill, New York, 1963.

Received April 9, 1999 and revised January 11, 2000. The research was partially supported by CONACyT project 25063-E.

UNIVERSIDAD AUTÓNOMA METROPOLITANA-ÁZCAPOTZALCO  
C.P. 02200, MEXICO  
*E-mail address:* arch@hp9000a1.uam.mx

CENTRO DE INVESTIGACIÓN Y DE ESTUDIOS AVANZADOS DEL I.P.N.  
07000 MÉXICO, D.F., MÉXICO  
*E-mail address:* villa@math.cinvestav.mx

This paper is available via <http://nyjm.albany.edu:8000/PacJ/2000/196-2-4.html>.