Pacific Journal of Mathematics

ON THE MINIMAL NUMBER OF RAMIFIED PRIMES IN SOME SOLVABLE EXTENSIONS OF $\mathbb{Q}$

Bernat Plans

Volume 215 No. 2 June 2004

PACIFIC JOURNAL OF MATHEMATICS
Vol. 215, No. 2, 2004

ON THE MINIMAL NUMBER OF RAMIFIED PRIMES IN SOME SOLVABLE EXTENSIONS OF $\mathbb{Q}$

Bernat Plans

For each finite solvable group G, there is a minimal positive integer $\mathrm{ram}(G)$ (resp. $\mathrm{ram}^t(G)$) such that G appears as the Galois group of an extension of $\mathbb{Q}$ (resp. a tamely ramified extension of $\mathbb{Q}$) ramified at only $\mathrm{ram}(G)$ (resp. $\mathrm{ram}^t(G)$) finite primes. We obtain bounds for $\mathrm{ram}(G)$ and $\mathrm{ram}^t(G)$, where G is either a nilpotent group of odd order or a generalized dihedral group.

1. Introduction

Given a finite group G, let $\mathrm{ram}(G)$ (resp. $\mathrm{ram}^t(G)$) denote the minimal positive integer such that G can be realized as the Galois group of an extension of $\mathbb{Q}$ (resp. a tamely ramified extension of $\mathbb{Q}$) ramified only at $\mathrm{ram}(G)$ (resp. $\mathrm{ram}^t(G)$) finite primes. The present paper is devoted to study $\mathrm{ram}(G)$ and $\mathrm{ram}^t(G)$, for some solvable groups G. More precisely, we consider the case where G is either a finite nilpotent group of odd order or a generalized dihedral group.

Let l be an odd prime number. The Scholz-Reichardt's Theorem establishes that every l-group G can be realized as the Galois group of some extension of $\mathbb{Q}$ [**Re**]. By Burnside's Basis Theorem and Kronecker–Weber's Theorem, $\mathrm{ram}(G)$ must be greater than or equal to the minimal number of generators of G. At present, it is not known whether this lower bound coincides with the exact value of $\mathrm{ram}(G)$ and $\mathrm{ram}^t(G)$, although this is claimed in [**Cu-He**] (see Remark 2.10). A Galois extension of $\mathbb{Q}$ with Galois group G arises by proper resolution of a chain of central embedding problems, starting with the trivial epimorphism $G_{\mathbb{Q}} \to \{1\}$. Moreover, if one restricts himself to embedding problems with kernel of order l, then this process can be made adding only one new ramified prime at each step. Hence, $\mathrm{ram}^t(G) \leq n$, where l^n is the order of G [**Se**, Chap. 2] (see also the generalization in [**Ge-Ja**], where the ground field $\mathbb{Q}$ is replaced by a general global field). We prove a better upper bound for $\mathrm{ram}^t(G)$, less than or equal to the sum of the minimal number of generators of the factors in the lower central series of G. In order to obtain this improvement, we allow arbitrary cyclic kernels and we show that it still suffices to admit just one new ramified prime (for Frattini or split embedding problems). In addition,

we obtain the best possible generalization of this bound to the case of finite nilpotent groups of odd order.

Now let G be a generalized dihedral group. From the theory of ring class fields of quadratic fields, we prove that $\mathrm{ram}^t(G)$ can be upper bounded by the minimal number of generators of G. We also consider the question of which of these groups can have $\mathrm{ram}^t(G) = 1$ (resp. $\mathrm{ram}(G) = 1$). Assuming the validity of Hypothesis (H) of Schinzel, we give the exact value of $\mathrm{ram}^t(D_{2n})$ and $\mathrm{ram}(D_{2n})$, where D_{2n} denotes the dihedral group of order $2n$.

2. Finite nilpotent groups of odd order

For a finite group G, let $d(G)$ denote the minimal number of generators of G. Given a prime number p, we always assume that a prime $\overline{p}$ of $\overline{\mathbb{Q}}$ over p has been fixed. We denote by D_p (resp. I_p) its corresponding decomposition (resp. inertia) subgroup in $G_{\mathbb{Q}}$.

Let us first recall the so-called Scholz's condition for an l-extension of $\mathbb{Q}$.

Definition 2.1. Let l be an odd prime number and let G be an l-group. Given a positive integer N, an epimorphism $\varphi : G_{\mathbb{Q}} \to G$ is said to be **of type** (S_N) if, for every prime number p ramified by φ, the following conditions hold:

- $p \equiv 1 \pmod{l^N}$,
- $\varphi(I_p) = \varphi(D_p)$.

One also says that the extension of $\mathbb{Q}$ given by (the fixed field of the kernel of) φ is **of type** (S_N).

This condition is introduced in order to ensure (N large) the local solvability, at all ramified primes, of central embedding problems for φ with, say, kernel $\mathbb{Z}/l\mathbb{Z}$. Hence, one also obtains globally solvable embedding problems of the same type.

Theorem 2.2 (cf. [**Se**, Chap. 2])**.** *Let $1 \to C \to G \xrightarrow{\pi} H \to 1$ be a central extension of l-groups ($l \neq 2$) and let $\varphi : G_{\mathbb{Q}} \to H$ be an epimorphism of type (S_N). If the exponent of G is at most l^N, then the embedding problem given by (π, φ) is solvable.*

We want to twist an arbitrary solution to the above embedding problem in order to obtain a (proper) solution of type (S_N). Moreover, we want to increase as few as possible the ramification set when carrying over this process. This amounts to finding suitable elements in $H^1(G_{\mathbb{Q}}, C) = \mathrm{Hom}(G_{\mathbb{Q}}, C)$, whose existence must first be proved.

Let $\mathrm{Ram}(K/\mathbb{Q})$ (resp. $\mathrm{Ram}(\varphi)$) denote the set of ramified prime numbers in an extension $K/\mathbb{Q}$ (resp. an epimorphism $\varphi : G_{\mathbb{Q}} \to G$).

Proposition 2.3. *Let l be an odd prime number, $K/\mathbb{Q}$ an l-extension of type (S_N) and $C = \langle c \rangle$ a cyclic group of order l^r such that $r \leq N$. Let*

us define $S = \mathrm{Ram}(K/\mathbb{Q})\backslash\{p_0\}$, *where* p_0 *is a fixed prime number which ramifies in* $K/\mathbb{Q}$. *Let* $\{\nu_p\}_{p\in S}$ *be arbitrary integers. Then:*

(i) *For every positive integer* $k < r$, *there exist infinitely many prime numbers* q *such that:*
- q *splits completely in* $K\left(\zeta_{l^N}, \left\{\sqrt[l^r]{\frac{p}{{p_0}^{\nu_p}}}\right\}_{p\in S}, \sqrt[l^k]{p_0}\right)$,
- q *does not split completely in* $\mathbb{Q}\left(\zeta_{l^N}, \sqrt[l^{k+1}]{p_0}\right)$.

(ii) *For every integer* ν_0 *such that* $v_l(\nu_0) < r$ *and every prime* q *which satisfies Statement* (i) *for* $k = v_l(\nu_0)$, *there exists an epimorphism* $\chi : (\mathbb{Z}/q\mathbb{Z})^* \to C$ *such that:*
- $\chi(p_0) = c^{\nu_0}$,
- $\chi(p) = c^{\nu_0.\nu_p}$, *for every* $p \in S$.

Proof. By Txebotarev's density theorem, Statement (i) is reduced to showing that

$$\sqrt[l^{k+1}]{p_0} \notin K\left(\zeta_{l^N}, \left\{\sqrt[l^r]{\frac{p}{{p_0}^{\nu_p}}}\right\}_{p\in S}, \sqrt[l^k]{p_0}\right).$$

From Kummer's theory, it suffices to prove that

$$\sqrt[l]{p_0} \notin K\left(\zeta_{l^N}, \left\{\sqrt[l^{r-k}]{\frac{p}{{p_0}^{\nu_p}}}\right\}_{p\in S}\right)$$

or, equivalently,

$$K\left(\zeta_{l^N}, \left\{\sqrt[l]{\frac{p}{{p_0}^{\nu_p}}}\right\}_{p\in S}, \sqrt[l]{p_0}\right) \not\subseteq K\left(\zeta_{l^N}, \left\{\sqrt[l^{r-k}]{\frac{p}{{p_0}^{\nu_p}}}\right\}_{p\in S}\right).$$

In order to see that this is always true, we first note that the following isomorphism holds (see [**Se**, Lemma 2.1.9]):

$$\mathrm{Gal}\left(K\left(\zeta_{l^N}, \left\{\sqrt[l]{\frac{p}{{p_0}^{\nu_p}}}\right\}_{p\in S}, \sqrt[l]{p_0}\right) \Big/ K\left(\zeta_{l^N}\right)\right) \cong \mathbb{Z}/l\mathbb{Z} \times \overset{s+1}{\cdots} \times \mathbb{Z}/l\mathbb{Z},$$

where s denotes the cardinality of S. This is all we need, since the Galois group

$$\mathrm{Gal}\left(K\left(\zeta_{l^N}, \left\{\sqrt[l^{r-k}]{\frac{p}{{p_0}^{\nu_p}}}\right\}_{p\in S}\right) \Big/ K\left(\zeta_{l^N}\right)\right)$$

can be generated with s elements.

Finally, Statement (ii) is clear once we observe that, if q satisfies the conditions in Statement (i), then:

p_0 is an l^k-th power residue modulo q,
$\frac{p}{{p_0}^{\nu_p}}$ is an l^r-th power residue modulo q, for each $p \in S$,
p_0 is not an l^{k+1}-th power residue modulo q.

□

We can now prove the following generalization of [**Se**, Thm. 2.1.3]:

Proposition 2.4. *Let l be an odd prime number. Suppose given a cyclic central extension of l-groups $1 \to C \to G \xrightarrow{\pi} H \to 1$ and an epimorphism $\varphi : G_{\mathbb{Q}} \to H$ of type (S_N), for some positive integer N such that the exponent of G is at most l^N. If the embedding problem (π, φ) is Frattini or split, then (π, φ) admits a proper solution $\widetilde{\varphi}$ of type (S_N) such that:*

$$\sharp \operatorname{Ram}(\widetilde{\varphi}) \leq 1 + \sharp \operatorname{Ram}(\varphi).$$

Proof. For each prime number p, let us choose a preimage $\sigma_p \in D_p$ of the Frobenius automorphism $\operatorname{Frob}_p \in D_p/I_p \cong G_{\mathbb{F}_p} \cong \widehat{\mathbb{Z}}$. Hypothesis (S_N) over φ allows us to assume that $\varphi(\sigma_p) = 1$, for every $p \in \operatorname{Ram}(\varphi)$.

In order to deal with the Frattini case, let us first consider a (necessarily proper) solution ψ to the embedding problem (π, φ), such that $\operatorname{Ram}(\psi) = \operatorname{Ram}(\varphi)$. Such a ψ always exists [**Se**, Cor. 2.1.8]. Let $p_0 \in \operatorname{Ram}(\varphi)$ be such that all the elements $\{\psi(\sigma_p)\}_{p \in \operatorname{Ram}(\varphi)}$ belong to $\langle \psi(\sigma_{p_0}) \rangle \subseteq C$. From Proposition 2.3, it follows that there exists a prime number $q \equiv 1 \pmod{l^N}$ such that $\varphi(D_q) = \{1\}$, and an epimorphism

$$\chi : G_{\mathbb{Q}} \to \operatorname{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \cong (\mathbb{Z}/q\mathbb{Z})^* \to C$$

such that $\chi(\sigma_p) = \psi(\sigma_p)$, for every $p \in \operatorname{Ram}(\varphi)$. Clearly, $\widetilde{\varphi} := \psi.\chi^{-1}$ is a proper solution to the embedding problem (π, φ) such that $\operatorname{Ram}(\widetilde{\varphi}) = \operatorname{Ram}(\varphi) \cup \{q\}$. Furthermore, it is of type (S_N), since $\widetilde{\varphi}(D_q) \subseteq C = \widetilde{\varphi}(I_q)$ and $\widetilde{\varphi}(D_p) = \langle \widetilde{\varphi}(\sigma_p), \widetilde{\varphi}(I_p) \rangle = \widetilde{\varphi}(I_p)$, for every $p \in \operatorname{Ram}(\varphi)$.

In the split case, it suffices to argue as in [**Se**, p. 11]. More precisely, let $K/\mathbb{Q}$ denote the H-extension obtained from φ and let q be a prime number which splits completely in $K\left(\zeta_{l^N}, \left\{\sqrt[l^r]{p}\right\}_{p \in \operatorname{Ram}(\varphi)}\right)/\mathbb{Q}$. Then, for every epimorphism $\chi : G_{\mathbb{Q}} \to \operatorname{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \cong (\mathbb{Z}/q\mathbb{Z})^* \to C$, we can take

$$\widetilde{\varphi} : G_{\mathbb{Q}} \xrightarrow{(\varphi,\chi)} H \times C \cong G.$$

□

Let $C_i(G)$ be the i-th higher commutator subgroup of a finite group G. This is defined inductively by $C_1(G) = G$ and $C_{i+1}(G) = [C_i(G), G]$. Recall that G is nilpotent if there exists a positive integer n such that $C_{n+1}(G) = \{1\}$. The smallest such n is the nilpotency class of G. Let us denote $d_i(G) = d(C_i(G)/C_{i+1}(G))$.

Proposition 2.5. *Let l be an odd prime number and let n be the nilpotency class of an l-group G. Then:*

$$d(G) \leq \operatorname{ram}(G) \leq \operatorname{ram}^t(G) \leq d(G) + \sum_{2 \leq i \leq n-1} d_i(G),$$

where the above sum is assumed to be 0 in case $n \leq 2$.

Proof. The first inequality is a direct consequence of Burnside's basis theorem and Kronecker–Weber's theorem.

In order to obtain a G-extension of $\mathbb{Q}$ it suffices to properly solve a chain of n central embedding problems given by the natural central extensions

$$1 \to C_i(G)/C_{i+1}(G) \to G/C_{i+1}(G) \to G/C_i(G) \to 1,$$

and starting from the trivial epimorphism $G_{\mathbb{Q}} \to G/C_1(G) = \{1\}$. Since $C_1(G) = G$ and $C_2(G)$ is nothing but the derived subgroup of G, our first $(i = 1)$ embedding problem can be decomposed into $d(G) = d_1(G)$ cyclic split ones. For every $i > 1$, the abelianizations of $G/C_{i+1}(G)$ and $G/C_i(G)$ are the same (namely, $G/C_2(G)$). In this case, we thus have to consider a Frattini embedding problem which gives rise to $d_i(G)$ cyclic (Frattini) ones. The stated result then follows from Proposition 2.4. It should be noted that, since the final G-extension of $\mathbb{Q}$ is not required to be of type (S_N), the (last) Frattini central embedding problem with kernel $C_n(G)$ can be (properly) solved without adding new ramification. □

In the above process, we certainly have to add a new ramified prime in order to properly solve each of the $d(G)$ first cyclic split embedding problems. For the remaining Frattini embedding problems, it may happen that we are not forced to increase the number of ramified primes. However, this would be restricted (if possible) by the following fact:

Proposition 2.6. *Let l be an odd prime number and let G be an l-group of exponent at most l^N. Let $1 \to \mathbb{Z}/l\mathbb{Z} \to G \xrightarrow{\pi} H \to 1$ be a central Frattini extension and let $\varphi : G_{\mathbb{Q}} \to H$ be an epimorphism of type (S_N) ramified at $d(H)$ finite primes. Then, the solutions to the embedding problem (π, φ) ramified at $d(H)$ finite primes are, either all of them or none, of type (S_N).*

Proof. We will show that all solutions to (π, φ) ramified at $d(H)$ finite primes define the same extension of $\mathbb{Q}$.

Let $\widetilde{\varphi}_1$, $\widetilde{\varphi}_2$ be different solutions to (π, φ) ramified at $d(H)$ finite primes. Hence, $\widetilde{\varphi}_1 = \widetilde{\varphi}_2.\chi$, for some epimorphism $\chi \in \mathrm{Hom}(G_{\mathbb{Q}}, \mathbb{Z}/l\mathbb{Z})$ ramified only at finite primes in $\mathrm{Ram}(\varphi)$. We are assuming that φ defines an H-extension of $\mathbb{Q}$ ramified at $d(H) = d(H^{ab})$ finite primes, where H^{ab} denotes the abelianization of H. Hence, every abelian extension of $\mathbb{Q}$ of exponent l ramified only at finite primes in $\mathrm{Ram}(\varphi)$ must be a subextension of (the maximal abelian subextension of) $\overline{\mathbb{Q}}^{\mathrm{Ker}\,\varphi}/\mathbb{Q}$.

Thus, $\overline{\mathbb{Q}}^{\mathrm{Ker}\,\chi} \subseteq \overline{\mathbb{Q}}^{\mathrm{Ker}\,\varphi}$ and we have that

$$\overline{\mathbb{Q}}^{\mathrm{Ker}\,\widetilde{\varphi}_1} = \overline{\mathbb{Q}}^{\mathrm{Ker}\,\widetilde{\varphi}_2}.$$

□

The following one is the main result of this section. It is the best possible generalization of Proposition 2.5 for nilpotent groups of odd order.

Theorem 2.7. *Let G be a finite nilpotent group of odd order and let $\{G_1, \ldots, G_s\}$ be their Sylow subgroups, each of nilpotency class n_j. Then:*

$$d(G) \leq \mathrm{ram}(G) \leq \mathrm{ram}^t(G) \leq \max_{1\leq j\leq s} \left\{ d(G_j) + \sum_{2\leq i\leq n_j-1} d_i(G_j) \right\}.$$

What must be proved is that the bounds for each G_i obtained from Proposition 2.5 can be reached in a compatible way. This is reduced to show the following generalization of Proposition 2.4:

Proposition 2.8. *Let $\mathcal{L} = \{l_1, \ldots, l_s\}$ be a finite set of odd prime numbers. For each $l_j \in \mathcal{L}$, let us consider a cyclic central extension of l_j-groups*

$$1 \to C_j \to G_j \stackrel{\pi_j}{\to} H_j \to 1$$

and an epimorphism $\varphi_j : G_{\mathbb{Q}} \to H_j$. Let N be a positive integer. Let us assume that, for every $1 \leq j \leq s$, the exponent of G_j is at most ${l_j}^N$, the epimorphism φ_j is of type (S_N), the set $\mathrm{Ram}(\varphi_j)$ does not contain any prime of $\mathcal{L}$ and the embedding problem (π_j, φ_j) is Frattini or split. Then, there exist proper solutions $\{\widetilde{\varphi_j}\}_j$ to the embedding problems $\{(\pi_j, \varphi_j)\}_j$, each of them of type (S_N), such that

$$\sharp \left(\bigcup_j \mathrm{Ram}(\widetilde{\varphi_j}) \right) \leq 1 + \sharp \left(\bigcup_j \mathrm{Ram}(\varphi_j) \right).$$

Proof. It suffices to show the appropriate generalization of Proposition 2.3 (i).

Let $j \in \{1, \ldots, s\}$ be momentarily fixed. Let $K/\mathbb{Q}$ be the H_j-extension obtained from φ_j and let us denote $l = l_j$, $C = C_j$ and $S = \mathrm{Ram}(\varphi_j)$. Given p_0, k for which the hypothesis of Prop. 2.3 hold, let us define $M_j = \mathbb{Q}\left(\zeta_{l^N}, \sqrt[l^{k+1}]{p_0}\right)$ and

$$L_j = K\left(\zeta_{l^N}, \left\{ \sqrt[l^r]{\frac{p}{{p_0}^{\nu_p}}} \right\}_{p\in S}, \sqrt[l^k]{p_0}\right).$$

We want to prove that there exists a prime number q such that, for every $j \in \{1, \ldots, s\}$, q splits completely in $L_j/\mathbb{Q}$ and does not in $M_j/\mathbb{Q}$.

From Prop. 2.3 (i) we know that $[L_j.M_j : L_j] = l_j$, for every j. Let us denote $a = (l_1 \cdot \cdots \cdot l_s)^N$ and $a(j) = \frac{a}{{l_j}^N}$. Since the extensions $L_j.M_j/\mathbb{Q}$ and $\mathbb{Q}(\zeta_{a(j)})/\mathbb{Q}$ have no common ramified finite primes, it must be $[L_j.M_j(\zeta_a) : L_j(\zeta_a)] = l_j$. As a consequence, we have that $[L_1 \ldots L_s.M_j : L_1 \ldots L_s] = l_j$. Hence, there exists some $\sigma \in \mathrm{Gal}(L_1 \ldots L_s.M_1 \ldots M_s/L_1 \ldots L_s)$ such that:

$$\sigma_{|M_j} \neq id, \quad \text{for every } j \in \{1, \ldots, s\}.$$

It only remains to invoke Txebotarev's density theorem. □

Remark 2.9. From Theorem 2.7, we obtain that $\mathrm{ram}(G) = \mathrm{ram}^t(G) = d(G)$, for every finite nilpotent group G of odd order such that

$$d(G) = \max_{1\leq j\leq s}\left\{ d(G_j) + \sum_{2\leq i\leq n_j-1} d(C_i(G_j)/C_{i+1}(G_j)) \right\}.$$

This equality holds for more groups than just the easy ones of nilpotency class $n = \max_j\{n_j\} \leq 2$.

Remark 2.10. In [**Cu-He**, Thm. 5] it is claimed that the equality $\mathrm{ram}(G) = \mathrm{ram}^t(G) = d(G)$ holds for every finite nilpotent group G of odd order. However, there is an error in the proof of this result (p. 308, "Therefore, $q_1, \ldots, q_{h+1}$ are fleissig in $K_1''/\mathbb{Q}$ ..."). Moreover, Proposition 2.6 contradicts the argument followed there.

3. Generalized dihedral groups

Given a finite abelian group A, consider the $\mathbb{Z}/2\mathbb{Z}$-action on A which sends $\overline{1} \in \mathbb{Z}/2\mathbb{Z}$ to $\{\sigma \mapsto \sigma^{-1}\} \in \mathrm{Aut}(A)$. One says that the corresponding semidirect product $A \rtimes \mathbb{Z}/2\mathbb{Z}$ is a generalized dihedral group and it will be denoted by $D_{2.A}$. Note that, if B is a quotient of A, then $D_{2.B}$ is a quotient of $D_{2.A}$. The abelianization of $D_{2.A}$ will be denoted by $D_{2.A}^{ab}$. One easily checks that $D_{2.A}^{ab} \cong D_{2.A}/A^2 \cong D_{2.A/A^2}$.

Let K be a quadratic field. Given a positive integer $f \geq 2$, $K(\widetilde{f})$ will denote the ring class field of K of conductor $\widetilde{f} := (f)\mathcal{O}_K.\infty_K$ (see, for example, [**Co**]). Let us just recall that $K(\widetilde{f})/K$ is a finite abelian extension, unramified away from $\widetilde{f}$, which contains the narrow Hilbert class field of K. Every intermediate field between K and some $K(\widetilde{f})$ will be called a ring class field of K.

Generalized dihedral groups and ring class fields are intimately related by the following known result:

Theorem 3.1 (cf. [**Bru**, Satz 8])**.** *The following conditions on a number field L are equivalent:*

(i) *$L/\mathbb{Q}$ is a generalized dihedral extension, that is, it is a Galois extension with group isomorphic to a generalized dihedral group ($D_{2.A}$).*
(ii) *L is a ring class field of some quadratic field ($K = L^A$).*

Our main result in this section is the following one:

Theorem 3.2. *Let A be a finite abelian group. Then:*

$$d(D_{2.A}^{ab}) \leq \mathrm{ram}^t(D_{2.A}) \leq d(D_{2.A}).$$

Proof. The first inequality follows from Kronecker–Weber's theorem.

Let us denote $r = d(A)$ and let $(m_1, \dots, m_r)$ be the invariant factors of A. Certainly, $d(D_{2.A}) = r + 1$.

In order to obtain the second inequality, we will prove the existence of a ring class field L (of some quadratic field K) such that:

(a) At most $r + 1$ finite primes ramify in the extension $L/\mathbb{Q}$, all of them being tamely ramified,
(b) A is isomorphic to a quotient of $\mathrm{Gal}(L/K)$.

The stated result then follows from Theorem 3.1 (and the remarks previous to it).

Let q be an arbitrary fixed odd prime number. Take $K := \mathbb{Q}(\sqrt{q^*})$, the unique quadratic field unramified away from $\{q, \infty\}$. Let H_+ denote the narrow Hilbert class field of K. The degree of the extension $K(\widetilde{f})/K$ is known to be [**Co**, Cor. 15.40]

$$[K(\widetilde{f}) : K] = [H_+ : K].f. \prod_{p|f} \left(1 - \frac{\left(\frac{d}{p}\right)}{p}\right) . \frac{1}{E_f},$$

where d denotes the discriminant of K and E_f is a suitable positive integer which, in case $d < 0$, depends only on K (not on f).

One can always find prime numbers $p_1, \dots, p_r$ such that:

$$p_i \equiv 1 \pmod{m_i.E_{p_i}.q},$$

for every $i \in \{1, \dots, r\}$. This is clear for imaginary K. For real K, it suffices to take p_i being completely split in $K(\zeta_{m_i.q}, \sqrt[m_i.q]{\epsilon_+})$, where ϵ_+ is the generator of the totally positive units in the ring of integers of K (see the proof of [**Je-Yui**, Thm. I.2.1]).

Let us fix a set of r prime numbers $\{p_1, \dots, p_r\}$ as above and let us define $L = K(\widetilde{p_1}) \dots K(\widetilde{p_r})$. Since L is a subfield of $K(\widetilde{p_1 \cdot \dots \cdot p_r})$, it is a ring class field of K. We are going to check Conditions (a) and (b) for such a choice of L (and K).

By assumption, each prime p_i splits completely in K, $p_i\mathcal{O}_K = \mathfrak{p}_i.\mathfrak{p}_i'$. The inertia subgroups in $\mathrm{Gal}(K(\widetilde{p_i})/K)$ at the primes $\mathfrak{p}_i$ and $\mathfrak{p}_i'$ are conjugate one from another in (the generalized dihedral group) $\mathrm{Gal}(K(\widetilde{p_i})/\mathbb{Q})$, hence they are equal. Moreover, they must be equal to the inertia subgroup $I_i \subset \mathrm{Gal}(K(\widetilde{p_i})/\mathbb{Q})$ at p_i. Since $\mathfrak{p}_i$ and $\mathfrak{p}_i'$ are the only ramified prime ideals in the extension $K(\widetilde{p_i})/K$, it must be $I_i = \mathrm{Gal}(K(\widetilde{p_i})/H_+)$. Let n_i denote the order of I_i. From the above formula (with $f = p_i$), we obtain that $n_i = \frac{p_i - 1}{E_{p_i}}$. Hence, it must be

$$\mathrm{Gal}(K(\widetilde{p_i})/H_+) \cong \mathbb{Z}/n_i\mathbb{Z},$$

the extension $K(\widetilde{p_i})/H_+$ being totally and tamely ramified at all primes of H_+ over p_i. In addition, for $i \neq j$, the extensions $K(\widetilde{p_i})/H_+$ and $K(\widetilde{p_j})/H_+$

have no common ramified finite primes. Thus, we obtain an isomorphism

$$\mathrm{Gal}(L/H_+) \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}.$$

Our choice of p_i ensures n_i being divisible by m_i. So, A is isomorphic to a quotient of $\mathrm{Gal}(L/K)$ (Condition (b)).

Finally, the only finite ramified primes in $L/\mathbb{Q}$ are $q, p_1, \ldots, p_r$ and their ramification indices are, respectively, $2, n_1, \ldots, n_r$. Hence, Condition (a) also holds. □

Remark 3.3. We proved more than just the inequality $\mathrm{ram}^t(D_{2.A}) \leq d(D_{2.A})$. The given proof shows that, for every odd prime number q, there exist infinitely many ring class fields L of $\mathbb{Q}(\sqrt{q^*})$ such that the extension $L/\mathbb{Q}$ ramifies at most at $d(D_{2.A})$ finite primes and has Galois group isomorphic to $D_{2.A}$.

Corollary 3.4. *Let A be a finite abelian group such that $d(A) = d(A_2)$, where A_2 denotes the 2-primary component of A. Then, $\mathrm{ram}^t(D_{2.A}) = d(D_{2.A})$.*

In the general case, it certainly happens that $\mathrm{ram}^t(D_{2.A}) < d(D_{2.A})$.

Proposition 3.5. *Let A be a finite abelian group. Then, the following conditions are equivalent:*

(i) $\mathrm{ram}^t(D_{2.A}) = 1$.

(ii) *A is isomorphic to a subgroup of the narrow class group $\mathrm{Cl}_+(\mathbb{Q}(\sqrt{p^*}))$ of $\mathbb{Q}(\sqrt{p^*})$, for some odd prime number p.*

Proof. On the one hand, the Galois group over $\mathbb{Q}$ of the narrow Hilbert class field H_+ of a quadratic field K is isomorphic to a generalized dihedral group. On the other hand, if $K = \mathbb{Q}(\sqrt{p^*})$ for an odd p, then H_+/K is the maximal tamely ramified subextension of $K(\widetilde{p^m})/K$, for every $m \geq 1$. □

Given a finite abelian group A of even order, it must be $\mathrm{ram}^t(D_{2.A}) > 1$. However, it may be $\mathrm{ram}(D_{2.A}) = 1$.

Proposition 3.6. *Let A be a finite abelian group of even order and let p be a prime number. Let $L/\mathbb{Q}$ be a Galois extension unramified away from $\{p, \infty\}$, with Galois group $\mathrm{Gal}(L/\mathbb{Q}) \cong D_{2.A}$. Then, $p = 2$ and A is a cyclic 2-group.*

Proof. From Theorem 3.1, L must be a ring class field of the quadratic field $K = L^A$. Since $D_{2.A}^{ab}$ is isomorphic to a quotient of $(\mathbb{Z}/p^n\mathbb{Z})^*$ and $d(D_{2.A}^{ab}) = 1 + d(A_2) \geq 2$, it must be $p = 2$ and $d(A_2) = 1$. Hence, K is one of the fields $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(i)$. All of them have trivial narrow class group, so A must be a cyclic 2-group. □

Corollary 3.7. *Let A be a finite abelian group of even order. Then, the following conditions are equivalent:*

(i) $\mathrm{ram}(D_{2.A}) = 1$,
(ii) *A is a cyclic 2-group.*

Proof. (ii) $\Rightarrow$ (i) follows from the fact that a 2-group G appears as the Galois group of an extension of $\mathbb{Q}$ unramified away from $\{2, \infty\}$ if and only if G can be generated by two elements, one of them of order 2 (cf. [**Ma**] or [**Ha**, p. 59]). □

For the usual dihedral group D_{2n} of order $2n$, we have the following:

Corollary 3.8. *Let n be an even positive integer. Then:*
$\mathrm{ram}(D_{2n}) = 1$ *and* $\mathrm{ram}^t(D_{2n}) = 2$, *if n is a power of* 2,
$\mathrm{ram}(D_{2n}) = \mathrm{ram}^t(D_{2n}) = 2$, *otherwise.*

We next prove a conditional result about $\mathrm{ram}(D_{2n})$ and $\mathrm{ram}^t(D_{2n})$, for odd n. Let us first recall the:

Hypothesis (H) of Schinzel [**Sc-Si**]: Let $p_1(T), \ldots, p_r(T)$ be irreducible polynomials in $\mathbb{Z}[T]$, all of them having positive leading coefficient. Assume also that, for every prime number p, there exists an integer n_p such that p does not divide $p_1(n_p) \cdot \cdots \cdot p_r(n_p)$. Then, there exist infinitely many positive integers n such that $p_1(n), \ldots, p_r(n)$ are all prime numbers.

Proposition 3.9. *Under the Hypothesis* (H) *of Schinzel, every dihedral group D_{2n} satisfies* $\mathrm{ram}^t(D_{2n}) = d(D_{2n}^{ab})$.

Proof. We must prove the equality $\mathrm{ram}^t(D_{2n}) = 1$, for every odd n.

Let $l \equiv 1 \pmod{n}$ be an odd prime number and let x be an odd integer which generates $(\mathbb{Z}/l\mathbb{Z})^*$. A result of Yamamoto [**Ya**, Prop. 1] establishes that, if $t \in \mathbb{Z}$ is coprime with x and $x^2 - 4t^n l^n < 0$, then the class group of $\mathbb{Q}(\sqrt{x^2 - 4t^n l^n})$ has an element of order n.

On the other hand, $p(T) = 4l^n T^n - x^2 \in \mathbb{Z}[T]$ is an irreducible polynomial in $\mathbb{Q}[T]$ such that $(p(0), p(1)) = 1$. Then, Hypothesis (H) of Schinzel claims the existence of infinitely many integers $t \in \mathbb{N}$ such that $p(t)$ is a prime number q, necessarily $q \equiv 3 \pmod{4}$. Hence, q is the only ramified prime number in the extension $\mathbb{Q}(\sqrt{-q})/\mathbb{Q}$. □

Remark 3.10. Similar results can also be otained for other finite groups. For instance, assuming Hypothesis (H), one can always find monic trinomials in $\mathbb{Z}[X]$ of degree n (every n) whose Galois group over $\mathbb{Q}$ is isomorphic to the symmetric group S_n and whose discriminant is a prime number greater than n. Hence, under the Hypothesis (H) of Schinzel, the symmetric group satisfies $\mathrm{ram}(S_n) = \mathrm{ram}^t(S_n) = 1$, for every n. It should be mentioned that the analogous argument for other groups may not work. For example, if $n \equiv 2, 6 \pmod{8}$, then every realization of the alternating group A_n as the Galois group over $\mathbb{Q}$ of a degree n trinomial must be ramified at all prime numbers $p \equiv 3 \pmod{4}$ which divide n [**Pl-Vi**].

Acknowledgements. This work is part of my Ph.D. Thesis. I am very much indebted to my thesis advisor, Núria Vila, for many valuable suggestions concerning material in this paper.

References

[Bru] G. Bruckner, *Charakterisierung der galoisschen Zahlkörper, deren zerlegte Primzahlen durch binäre quadratische Formen gegeben sind*, Math. Nachr., **32** (1966), 317–326, MR 0217043 (36 #138), Zbl 0144.04203.

[Co] H. Cohn, *A Classical Invitation to Algebraic Numbers and Class Fields*, Springer, 1978, MR 0506156 (80c:12001), Zbl 0395.12001.

[Cu-He] A. Cueto-Hernández and G.D. Villa-Salvador, *Nilpotent extensions of number fields with bounded ramification*, Pacific J. Math., **196**(**2**) (2000), 297–316, MR 1800579 (2002b:12007), Zbl 0961.12003.

[Ge-Ja] 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, MR 1633151 (99d:12001), Zbl 0906.12002.

[Ha] D. Harbater, *Galois groups with prescribed ramification*, in 'Arithmetic Geometry', Contemp. Math., **174**, Amer. Math. Soc., Providence, 1994, 35–60, MR 1299733 (96a:12008), Zbl 0815.11053.

[Je-Yui] C.U. Jensen and N. Yui, *Polynomials with D_p as Galois group*, J. Number Theory, **15** (1982), 347–375, MR 0680538 (84g:12011), Zbl 0496.12004.

[Ma] H. Markscheitis, *On p-extensions with one critical prime* (Russian), Izv. Akad. Nauk. SSSR, Ser. Mat., **27** (1963), 463–466, MR 0151452 (27 #1437).

[Pl-Vi] B. Plans and N. Vila, *Trinomial extensions of $\mathbb{Q}$ with ramification conditions*, to appear in J. Number Theory.

[Re] H. Reichardt, *Konstruction von Zahlkörpern mit gegebener Galoisgruppe von Primzahlpotenzordnung*, J. Reine Angew. Math., **177** (1937), 1–5, Zbl 0016.15103.

[Sc-Si] A. Schinzel and W. Sierpinski, *Sur certaines hypothèses concernant les nombres premiers*, Acta Arith., **4** (1958), 185–208, MR 0106202 (21 #4936), Zbl 0082.25802.

[Se] J.-P. Serre, *Topics in Galois Theory*, Jones and Bartlett, Boston, 1992, MR 1162313 (94d:12006), Zbl 0746.12001.

[Ya] Y. Yamamoto, *On unramified Galois extensions of quadratic number fields*, Osaka J. Math., **7** (1970), 57–76, MR 0266898 (42 #1800), Zbl 0222.12003.

Received June 30, 2003 and revised September 25, 2003. Research partially supported by MCYT grant BFM2000-0794-C02-01.

Dept. de Matemàtica Aplicada I
Universitat Politècnica de Catalunya
Av. Diagonal, 647
08028 Barcelona
Spain
E-mail address: bernat.plans@upc.es