ACTA ARITHMETICA
149.4 (2011)

# Steinitz classes of tamely ramified nonabelian extensions of odd prime power order

by

Alessandro Cobbe (Pisa)

**1. Introduction.** Let $K/k$ be an extension of number fields and let $\mathcal{O}_K$ and $\mathcal{O}_k$ be their rings of integers. By Theorem 1.13 in [Na] we know that

$$\mathcal{O}_K \cong \mathcal{O}_k^{[K:k]-1} \oplus I,$$

where $I$ is an ideal of $\mathcal{O}_k$. By Theorem 1.14 in [Na] the $\mathcal{O}_k$-module structure of $\mathcal{O}_K$ is determined by $[K:k]$ and the ideal class of $I$. This class is called the *Steinitz class* of $K/k$ and we will indicate it by $\mathrm{st}(K/k)$. Let $k$ be a number field and $G$ a finite group; then we define

$$\mathrm{R}_t(k,G) = \{x \in \mathrm{Cl}(k) : \exists K/k \text{ tame}, \mathrm{Gal}(K/k) \cong G, \mathrm{st}(K/k) = x\}.$$

It is conjectured that this subset of $\mathrm{Cl}(k)$ is always a subgroup. The problem has been studied by a lot of authors since the 1960s and $\mathrm{R}_t(k,G)$ has been proved to be a group for some particular choices of $G$. In particular the conjecture for finite abelian groups is a consequence of a paper by Leon McCulloh of 1987 ([MC2]). Other results from literature cover some particular nonabelian groups: see for example [B], [BS], [BGS], [Ca1], [Ca2], [CaS], [E], [GS1], [GS2], [Lo1], [Lo2], [MS], [MC1], [S1], [S2] and [Sov].

The study of realizable Steinitz classes is closely connected to a similar question involving Galois module structure. In that context $\mathrm{R}_t(\mathcal{O}_k[G])$ denotes a subset of the locally free class group $\mathrm{Cl}(\mathcal{O}_k[G])$ and is defined in a similar way to $\mathrm{R}_t(k,G)$. Again $\mathrm{R}_t(\mathcal{O}_k[G])$ is conjectured to be a group, which is in some sense a generalization of the conjecture about Steinitz classes.

In this paper we will study $\mathrm{R}_t(k,G)$ when $G$ is a semidirect product of the form $C(l^n) \rtimes C(l)$, where $l$ is an odd prime number and $C(m)$ denotes a cyclic group of order $m$. We will use the notation and some techniques from [C2] to prove the conjecture for such groups and to give an explicit

2010 *Mathematics Subject Classification*: Primary 11R32; Secondary 11R37.
*Key words and phrases*: Steinitz classes, realizable classes, tame extensions of number fields, class field theory.

DOI: 10.4064/aa149-4-4

description of $\mathrm{R}_t(k,G)$. In particular the case $n=2$ is interesting because, together with [B], it completes the study of realizable Steinitz classes for groups of order $l^3$. We will also give an alternative proof of the results of [B], based on class field theory.

Some of the results in this paper are parts of the author's PhD thesis [C1].

**2. Preliminary results.** We start by recalling the following two fundamental results.

THEOREM 2.1. *If $K/k$ is a finite tame Galois extension then*

$$\mathrm{d}(K/k)=\prod_{\mathfrak{p}}\mathfrak{p}^{(e_{\mathfrak{p}}-1)[K:k]/e_{\mathfrak{p}}},$$

*where $e_{\mathfrak{p}}$ is the ramification index of $\mathfrak{p}$.*

*Proof.* This follows by Propositions 8 and 14 of Chapter III of [L]. ∎

THEOREM 2.2. *Assume $K$ is a finite Galois extension of a number field $k$.*

(a) *If the Galois group of $K/k$ either has odd order or has a noncyclic 2-Sylow subgroup then* $\mathrm{d}(K/k)$ *is the square of an ideal and this ideal represents the Steinitz class of the extension.*
(b) *If the Galois group is of even order with a cyclic 2-Sylow subgroup and $\alpha$ is any element of $k$ whose square root generates the quadratic subextension of $K/k$ then $\mathrm{d}(K/k)/\alpha$ is the square of a fractional ideal and this ideal represents the Steinitz class of the extension.*

*Proof.* This is a corollary of Theorem I.1.1 in [E]. In particular it is shown in [E] that in case (b), $K/k$ has exactly one quadratic subextension. ∎

Further, considering Steinitz classes in towers of extensions, we will need the following proposition.

PROPOSITION 2.3. *Suppose $K/k_1$ and $k_1/k$ are extensions of number fields. Then*

$$\mathrm{st}(K/k)=\mathrm{st}(k_1/k)^{[K:k_1]}\mathrm{N}_{k_1/k}(\mathrm{st}(K/k_1)).$$

*Proof.* This is Proposition I.1.2 in [E]. ∎

We will also use some other preliminary results.

LEMMA 2.4. *Let $m,n,x,y$ be integers. If $x\equiv y \pmod{m}$ and any prime $q$ dividing $n$ also divides $m$ then*

$$x^n\equiv y^n \pmod{mn}.$$

*Proof.* Let $n=q_1\ldots q_r$ be the prime decomposition of $n$ ($q_i$ and $q_j$ with $i\neq j$ are allowed to be equal). We prove by induction on $r$ that $x^n\equiv y^n \pmod{mn}$. If $r=1$, then $mn=mq_1$ must divide $m^{q_1}$ and there exists $b\in\mathbb{N}$

such that

$$x^n = (y + bm)^{q_1} = y^{q_1} + \sum_{i=1}^{q_1-1} \binom{q_1}{i} (bm)^i y^{q_1-i} + (bm)^{q_1} \equiv y^n \pmod{mn}.$$

Let us assume that the lemma is true for $r-1$ and prove it for $r$. Since $q_r \mid m$, as above, for some $c \in \mathbb{N}$ we have

$$\begin{aligned} x^n &= (y^{q_1 \dots q_{r-1}} + cmq_1 \dots q_{r-1})^{q_r} \\ &= y^n + \sum_{i=1}^{q_r} \binom{q_r}{i} (cmq_1 \dots q_{r-1})^i y^{q_1 \dots q_{r-1}(q_r-i)} \equiv y^n \pmod{mn}. \ \blacksquare \end{aligned}$$

Definition 2.5. Let $K/k$ be a finite abelian extension of number fields, let $J_k$ be the group of ideals of $k$, let $P_k$ be the group of principal ideals, let $\mathfrak{m}$ be a cycle of declaration of $K/k$ and let $H^{\mathfrak{m}}_{K/k}$ be the kernel of the Artin symbol $\left(\frac{K/k}{\cdot}\right) : J^{\mathfrak{m}}_k \to \mathrm{Gal}(K/k)$, where $J^{\mathfrak{m}}_k$ is the group of all ideals of $k$ prime to $\mathfrak{m}$. Then we define the subgroup $W(k,K)$ of the ideal class group of $k$ in the following equivalent ways (the equivalence is shown in [C2, Proposition 2.10]):

$$W(k,K) = H^{\mathfrak{m}}_{K/k} \cdot P_k/P_k,$$

$$W(k,K) = \{x \in J_k/P_k : x \text{ contains infinitely many primes of absolute degree 1 splitting completely in } K\},$$

$$W(k,K) = \{x \in J_k/P_k : x \text{ contains a prime splitting completely in } K\},$$

$$W(k,K) = \mathrm{N}_{K/k}(J_K) \cdot P_k/P_k.$$

In the case of cyclotomic extensions we will also use the shorter notation $W(k,m) = W(k,k(\zeta_m))$.

Lemma 2.6. *Let $m,n$ be integers. If any prime $q$ dividing $n$ also divides $m$ then $W(k,m)^n \subseteq W(k,mn)$.*

*Proof.* Let $x \in W(k,m)$. By definition and by Lemma 2.11 from [C2], $x$ contains a prime ideal $\mathfrak{p}$ prime to $mn$ and such that $\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{p}) \in P^{\mathfrak{m}}_{\mathbb{Q}}$, where $\mathfrak{m} = m \cdot p_\infty$ and $P^{\mathfrak{m}}_{\mathbb{Q}}$ is the group of all principal ideals in $\mathbb{Z}$ generated by a natural number $a \equiv 1 \pmod{m}$. Then, by Lemma 2.4, $\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{p}^n) \in P^{\mathfrak{n}}_{\mathbb{Q}}$ with $\mathfrak{n} = mn \cdot p_\infty$, and it follows from Lemma 2.12 of [C2] that $x^n \in W(k,mn)$. $\blacksquare$

We conclude this section by recalling a technical definition from [C2].

Definition 2.7. We will call a finite group $G$ of order $m$ *good* if the following properties are satisfied:

1. For any number field $k$, $\mathrm{R}_t(k,G)$ is a group.
2. For any tame $G$-extension $K/k$ of number fields there exists an element $\alpha_{K/k} \in k$ such that:

(a) If $G$ is of even order with a cyclic 2-Sylow subgroup, then a square root of $\alpha_{K/k}$ generates the quadratic subextension of $K/k$; if $G$ either has odd order or has a noncyclic 2-Sylow subgroup, then $\alpha_{K/k} = 1$.

(b) For any prime $\mathfrak{p}$, with ramification index $e_{\mathfrak{p}}$ in $K/k$, the ideal class [1] of

$$(\mathfrak{p}^{(e_{\mathfrak{p}}-1)m/e_{\mathfrak{p}}-v_{\mathfrak{p}}(\alpha_{K/k})})^{1/2}$$

is in $\mathrm{R}_t(k, G)$.

3. For any tame $G$-extension $K/k$ of number fields, for any prime ideal $\mathfrak{p}$ of $k$ and any rational prime $l$ dividing its ramification index $e_{\mathfrak{p}}$, the class of the ideal

$$\mathfrak{p}^{(l-1)\frac{m}{e_{\mathfrak{p}}(l)}},$$

is in $\mathrm{R}_t(k, G)$, where $e_{\mathfrak{p}}(l)$ is the exact power of $l$ dividing $e_{\mathfrak{p}}$, and, if 2 divides $(l-1)\frac{m}{e_{\mathfrak{p}}(l)}$, the class of

$$\mathfrak{p}^{\frac{l-1}{2}\frac{m}{e_{\mathfrak{p}}(l)}}$$

is in $\mathrm{R}_t(k, G)$.

4. $G$ is such that for any number field $k$, for any class $x \in \mathrm{R}_t(k, G)$ and any integer $a$, there exists a tame $G$-extension $K$ with Steinitz class $x$ and such that every nontrivial subextension of $K/k$ is ramified at some primes which are unramified in $k(\zeta_a)/k$.

The importance of this definition lies in the fact that for good groups $G$ we can apply Theorems 3.19 and 3.22 of [C2] to obtain a description of $\mathrm{R}_t(k, \tilde{G})$ for certain group extensions $\tilde{G}$ of $G$.

**3. Some $l$-groups.** In [B], Clément Bruche proved that if $G$ is a nonabelian group of order $l^3 = uv$ and exponent $v$, where $l$ is an odd prime, then $\mathrm{R}_t(k, G) = W(k, l)^{u(l-1)/2}$ under the hypothesis that the extension $k(\zeta_v)/k(\zeta_l)$ is unramified, thereby giving an unconditional result when $G$ has exponent $l$.

In this section we prove that $\mathrm{R}_t(k, C(l^2) \rtimes_\mu C(l)) = W(k, l)^{l(l-1)/2}$, without any additional hypothesis on the number field $k$. Indeed we will consider a more general situation, studying groups of the form $G = C(l^n) \rtimes_\mu C(l)$, with $n \geq 2$, where $\mu$ sends a generator of $C(l)$ to the elevation to the $(l^{n-1} + 1)$th power. Together with Bruche's result this will conclude the study of realizable Steinitz classes for tame Galois extensions of degree $l^3$.

---

[1] Actually $\mathfrak{p}^{(e_{\mathfrak{p}}-1)m/e_{\mathfrak{p}}-v_{\mathfrak{p}}(\alpha_{K/k})}$ is the square of an ideal by Theorems 2.1 and 2.2.

LEMMA 3.1. *Let $l$ be an odd prime. The group $G = C(l^n) \rtimes_\mu C(l)$ with $n \geq 2$ is identified by the exact sequence*

$$1 \to \ C(l^n) \to G \to C(l) \to 1$$

*if the action of $C(l)$ on $C(l^n)$ is given by $\mu$. Further $G$ is isomorphic to*

$$\langle \sigma, \tau : \sigma^l = \tau^{l^n} = 1,\ \sigma\tau\sigma^{-1} = \tau^{l^{n-1}+1} \rangle.$$

*Proof.* Let $G$ be the group in the above exact sequence, let $H$ be a subgroup of $G$ isomorphic to $C(l^n)$ and generated by $\tau$; let $x \in G$ be such that its class modulo $H$ generates $G/H$, which is cyclic of order $l$, and such that $x\tau x^{-1} = \tau^{l^{n-1}+1}$, i.e. $x\tau = \tau^{l^{n-1}+1}x$. Then $x^l = \tau^a$ for some $a \in \mathbb{N}$. Since $G$ is of order $l^{n+1}$ and it is not cyclic, the order of $x$ must divide $l^n$ and so

$$\tau^{al^{n-1}} = x^{l^n} = 1,$$

i.e. $l$ divides $a$ and there exists $b \in \mathbb{N}$ such that $a = bl$. By induction we prove that, for $m \geq 1$,

$$(\tau^{-b}x)^m = \tau^{-bm-bl^{n-1}(m-1)m/2}x^m.$$

This is obvious for $m = 1$; we have to prove the inductive step:

$$\begin{aligned}
(\tau^{-b}x)^m &= \tau^{-b(m-1)-bl^{n-1}(m-2)(m-1)/2}x^{m-1}\tau^{-b}x \\
&= \tau^{-b(m-1)-bl^{n-1}(m-2)(m-1)/2}x^{m-1}\tau^{-b}x^{-(m-1)}x^m \\
&= \tau^{-b(m-1)-bl^{n-1}(m-2)(m-1)/2}\tau^{-b(1+l^{n-1})^{m-1}}x^m \\
&= \tau^{-b(m-1)-bl^{n-1}(m-2)(m-1)/2-b-b(m-1)l^{n-1}}x^m \\
&= \tau^{-bm-bl^{n-1}(m-1)m/2}x^m.
\end{aligned}$$

Then writing $\sigma = \tau^{-b}x$, we obtain

$$\sigma^l = (\tau^{-b}x)^l = \tau^{-bl}x^l = \tau^{-a+a} = 1.$$

Further

$$\sigma\tau\sigma^{-1} = \tau^{-b}x\tau x^{-1}\tau^b = \tau^{-b}\tau^{l^{n-1}+1}\tau^b = \tau^{l^{n-1}+1}$$

and $\sigma, \tau$ are generators of $G$. Thus $G$ must be a quotient of the group

$$\langle \sigma, \tau :\ \sigma^l = \tau^{l^n} = 1,\ \sigma\tau\sigma^{-1} = \tau^{l^{n-1}+1} \rangle.$$

But this group has the same order as $G$ and thus they must be isomorphic. ∎

It follows that to study $\mathrm{R}_t(k, C(l^n) \rtimes_\mu C(l))$, for any number field $k$, we can use Proposition 3.13 of [C2].

For any $\gamma \in C(l^n)$ of order $o(\gamma)$ we define $E_{k,\mu,\gamma}$ as the fixed field in $k(\zeta_{o(\gamma)})$ of

$$G_{k,\mu,\gamma} = \{g \in \mathrm{Gal}(k(\zeta_{o(\gamma)})/k) : \exists g_1 \in C(l),\ \mu(g_1)(\gamma) = \gamma^{\nu_{k,\gamma}(g)}\},$$

where $g(\zeta_{o(\gamma)}) = \zeta_{o(\gamma)}^{\nu_{k,\gamma}(g)}$ for any $g \in \mathrm{Gal}(k(\zeta_{o(\gamma)})/k)$.

Lemma 3.2. *Let $\tau$ be a generator of $C(l^n)$. Then $E_{k,\mu,\tau} = k(\zeta_{l^{n-1}})$.*

*Proof.* By definition $E_{k,\mu,\tau}$ is the fixed field in $k(\zeta_{l^n})$ of

$$\begin{aligned} G_{k,\mu,\tau} &= \{g \in \mathrm{Gal}(k(\zeta_{l^n})/k) : \exists g_1 \in C(l),\ \mu(g_1)(\tau) = \tau^{\nu_{k,\tau}(g)}\} \\ &= \{g \in \mathrm{Gal}(k(\zeta_{l^n})/k) : \exists a \in \mathbb{N},\ \tau^{al^{n-1}+1} = \tau^{\nu_{k,\tau}(g)}\} \\ &= \{g \in \mathrm{Gal}(k(\zeta_{l^n})/k) : \nu_{k,\tau}(g) \equiv 1 \pmod{l^{n-1}}\} \\ &= \{g \in \mathrm{Gal}(k(\zeta_{l^n})/k) : g(\zeta_{l^{n-1}}) = \zeta_{l^{n-1}}\} = \mathrm{Gal}(k(\zeta_{l^n})/k(\zeta_{l^{n-1}})). \end{aligned}$$

Hence $E_{k,\mu,\tau} = k(\zeta_{l^{n-1}})$. ∎

Lemma 3.3. *We have*

$$\mathrm{R}_t(k, C(l^n) \rtimes_\mu C(l)) \supseteq W(k, l^{n-1})^{(l-1)l/2}.$$

*Further, for any $x \in W(k, l^{n-1})$ and any positive integer $a$, there exists a tame $G$-extension $K$ of $k$ with Steinitz class $x^{(l-1)l/2}$ and such that any nontrivial subextension of $K/k$ is ramified at some primes which are unramified in $k(\zeta_a)/k$.*

*Proof.* By Theorem 3.23 of [C2], $C(l)$ is a good group and so, recalling also Lemma 3.1, the hypotheses of Proposition 3.13 of [C2] are satisfied and we obtain

$$\mathrm{R}_t(k, C(l^n) \rtimes_\mu C(l)) \supseteq \mathrm{R}_t(k, C(l))^{l^n} \cdot W(k, E_{k,\mu,\tau})^{(l-1)l/2},$$

where $\tau$ is a generator of $C(l^n)$. We easily conclude the proof since $1 \in \mathrm{R}_t(k, C(l))$ and, by Lemma 3.2, $E_{k,\mu,\tau} = k(\zeta_{l^{n-1}})$, i.e.

$$W(k, E_{k,\mu,\tau}) = W(k, l^{n-1}).$$

Further the extensions constructed in Lemmas 3.10 and 3.11 of [C2] can be chosen so that all their proper subextensions are ramified at some primes which are unramified in $k(\zeta_a)/k$. Hence, actually, the same is true for the extensions obtained using Proposition 3.13 of [C2]. ∎

To prove the opposite inclusion we need some lemmas.

Lemma 3.4. *Let $\tau$ be a generator of $C(l^n)$ and $0 < c < n$ be an integer. Then*

$$\tilde{G}^{l^c}_{k,\mu,\tau^{l^c}} \subseteq G_{k,\mu,\tau},$$

*where $\tilde{G}_{k,\mu,\tau^{l^c}}$ is the subgroup of $\mathrm{Gal}(k(\zeta_{l^n})/k)$ consisting of all the elements whose restrictions to $\mathrm{Gal}(k(\zeta_{l^{n-c}})/k)$ are in $G_{k,\mu,\tau^{l^c}}$.*

*Proof.* For any positive integer $a$ we define

$$\hat{\mu}_{\tau^a} : C(l) \to (\mathbb{Z}/o(\tau^a)\mathbb{Z})^*$$

by $\tau^{a\hat{\mu}_{\tau^a}(g_1)} = \mu(g_1)(\tau^a)$ for all $g_1 \in C(l)$. To simplify notation, for $g \in \tilde{G}_{k,\mu,\tau^{l^c}}$ we will write $\nu_{k,\tau^{l^c}}(g)$ instead of $\nu_{k,\tau^{l^c}}(g|_{k(\zeta_{l^{n-c}})})$. By definition, if

$g \in \tilde{G}_{k,\mu,\tau^{l^c}}$, then there exists $g_1 \in C(l)$ such that

$$\tau^{l^c \nu_{k,\tau^{l^c}}(g)} = \mu(g_1)(\tau^{l^c}) = \tau^{l^c \hat{\mu}_{\tau^{l^c}}(g_1)}.$$

We also observe that

$$\zeta_{l^{n-c}}^{\nu_{k,\tau}(g)} = \zeta_{l^n}^{l^c \nu_{k,\tau}(g)} = g(\zeta_{l^n})^{l^c} = g(\zeta_{l^{n-c}}) = \zeta_{l^{n-c}}^{\nu_{k,\tau^{l^c}}(g)}$$

and

$$\tau^{l^c \hat{\mu}_{\tau^{l^c}}(g_1)} = \mu(g_1)(\tau^{l^c}) = \mu(g_1)(\tau)^{l^c} = \tau^{l^c \hat{\mu}_\tau(g_1)}.$$

From the above equalities we deduce

$$\nu_{k,\tau}(g) \equiv \nu_{k,\tau^{l^c}}(g) \equiv \hat{\mu}_{\tau^{l^c}}(g_1) \equiv \hat{\mu}_\tau(g_1) \pmod{l^{n-c}}$$

and therefore by Lemma 2.4 we obtain

$$\nu_{k,\tau}(g^{l^c}) \equiv \hat{\mu}_\tau(g_1^{l^c}) \pmod{l^n}.$$

We conclude that

$$\tau^{\nu_{k,\tau}(g^{l^c})} = \tau^{\hat{\mu}_\tau(g_1^{l^c})} = \mu(g_1^{l^c})(\tau)$$

and hence $g^{l^c} \in G_{k,\mu,\tau}$. ∎

LEMMA 3.5. *Let $\tau$ be a generator of $C(l^n)$ and $0 < c < n$ be an integer. Then*

$$W(k, E_{k,\mu,\tau^{l^c}})^{l^c} \subseteq W(k, l^{n-1}).$$

*Proof.* Let $x$ be a class in $W(k, E_{k,\mu,\tau^{l^c}})$. By definition there exists a prime $\mathfrak{p}$ in the class of $x$ splitting completely in $E_{k,\mu,\tau^{l^c}}/k$. By Theorem IV.8.4 in [Ne],

$$\mathfrak{p} \in H^{\mathfrak{m}}_{E_{k,\mu,\tau^{l^c}}/k},$$

where $\mathfrak{m}$ is a cycle of declaration of $E_{k,\mu,\tau^{l^c}}/k$ and $H^{\mathfrak{m}}_{E_{k,\mu,\tau^{l^c}}/k}$ is the kernel of the Artin symbol

$$\left(\frac{E_{k,\mu,\tau^{l^c}}/k}{\cdot}\right) : J_k^{\mathfrak{m}} \to \mathrm{Gal}(E_{k,\mu,\tau^{l^c}}/k).$$

Then, by Proposition II.3.3 in [Ne],

$$\left(\frac{k(\zeta_{l^n})/k}{\mathfrak{p}}\right)\Bigg|_{E_{k,\mu,\tau^{l^c}}} = \left(\frac{E_{k,\mu,\tau^{l^c}}/k}{\mathfrak{p}}\right) = 1.$$

Thus

$$\left(\frac{k(\zeta_{l^n})/k}{\mathfrak{p}}\right) \in \mathrm{Gal}(k(\zeta_{l^n})/E_{k,\mu,\tau^{l^c}}) = \tilde{G}_{k,\mu,\tau^{l^c}}$$

and it follows by Lemma 3.4 that

$$\left(\frac{k(\zeta_{l^n})/k}{\mathfrak{p}^{l^c}}\right) = \left(\frac{k(\zeta_{l^n})/k}{\mathfrak{p}}\right)^{l^c} \in \tilde{G}^{l^c}_{k,\mu,\tau^{l^c}} \subseteq G_{k,\mu,\tau} = \mathrm{Gal}(k(\zeta_{l^n})/E_{k,\mu,\tau}).$$

Then

$$\left(\frac{E_{k,\mu,\tau}/k}{\mathfrak{p}^{lc}}\right) = \left(\frac{k(\zeta_{l^n})/k}{\mathfrak{p}^{lc}}\right)\bigg|_{E_{k,\mu,\tau}} = 1$$

and so the class $x^{lc}$ of $\mathfrak{p}^{lc}$ is in $W(k, E_{k,\mu,\tau})$, which is equal to $W(k, l^{n-1})$ by Lemma 3.2. ∎

LEMMA 3.6. *Let $K/k$ be a tamely ramified abelian extension of number fields and let $\mathfrak{p}$ be a prime ideal in $k$ whose ramification index in $K/k$ is $e_{\mathfrak{p}}$. Then $\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{p}) \in P_{\mathbb{Q}}^{\mathfrak{m}}$, where $\mathfrak{m} = e_{\mathfrak{p}} \cdot p_\infty$, i.e. $\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{p})$ is an ideal of $\mathbb{Z}$ generated by a natural number $a \equiv 1 \pmod{e_{\mathfrak{p}}}$. In particular, by Lemma* 2.12 *of* [C2], *$\mathfrak{p} \in H_{k(\zeta_{e_{\mathfrak{p}}})/k}^{\mathfrak{m}}$ and so its class is in $W(k, e_{\mathfrak{p}})$.*

*Proof.* This is Lemma I.2.1 of [E]. ∎

LEMMA 3.7. *Let $K/k$ be a tame $C(l^n) \rtimes_\mu C(l)$-extension of number fields and let $\mathfrak{p}$ be a ramifying prime, with ramification index $e_{\mathfrak{p}}$. Then the classes of*

$$\mathfrak{p}^{\frac{e_{\mathfrak{p}}-1}{2}\frac{l^{n+1}}{e_{\mathfrak{p}}}} \quad \text{and} \quad \mathfrak{p}^{\frac{l-1}{2}\frac{l^{n+1}}{e_{\mathfrak{p}}}}$$

*are both in $W(k, l^{n-1})^{(l-1)l/2}$.*

*Proof.* The Galois group of $K/k$ is $C(l^n) \rtimes_\mu C(l)$, which is isomorphic to

$$G = \langle \sigma, \tau : \sigma^l = \tau^{l^n} = 1,\ \sigma\tau\sigma^{-1} = \tau^{l^{n-1}+1} \rangle,$$

by Lemma 3.1.

Since the ramification is tame, the inertia group at $\mathfrak{p}$ is cyclic, generated by an element $\tau^a\sigma^b$; by induction we obtain

$$(\tau^a\sigma^b)^m = \tau^{am+abl^{n-1}(m-1)m/2}\sigma^{bm}.$$

The order $e_{\mathfrak{p}}$ of $\tau^a\sigma^b$ must be a multiple of $l$, since the element $\tau^a\sigma^b$ is nontrivial and $G$ is an $l$-group. Hence, recalling that $\tau^{l^n} = 1$, we find that $e_{\mathfrak{p}}$ is the smallest positive integer such that

$$\tau^{ae_{\mathfrak{p}}}\sigma^{be_{\mathfrak{p}}} = 1.$$

First of all we assume that $l^2$ divides $e_{\mathfrak{p}}$. If $l^\beta$ is the exact power of $l$ dividing $a$, we obtain $e_{\mathfrak{p}} = l^{n-\beta}$ and in particular $\beta \le n-2$. So we have

$$\sigma(\tau^a\sigma^b)\sigma^{-1} = \tau^{a(l^{n-1}+1)}\sigma^b = (\tau^a\sigma^b)^{l^{n-1}+1}$$

and

$$\tau(\tau^a\sigma^b)\tau^{-1} = \tau^{a-bl^{n-1}}\sigma^b = (\tau^a\sigma^b)^{-\tilde{a}bl^{n-1-\beta}+1},$$

where $a\tilde{a} \equiv l^\beta \pmod{l^n}$. Hence, in particular, the inertia group is a normal subgroup of $G$. Thus we can decompose our extension in $K/k_1$ and $k_1/k$, which are both Galois and such that $\mathfrak{p}$ is totally ramified in $K/k_1$ and unramified in $k_1/k$. By Lemma 3.14 of [C2] the class of $\mathfrak{p}$ is in $W(k, E_{k,\rho,\tau^a\sigma^b})$, where the action $\rho$ is induced by the conjugation in $G$ and, in particular, it sends the class of $\tau$ in $\mathrm{Gal}(k_1/k) = G/\langle\tau^a\sigma^b\rangle$ to elevation to the $(-\tilde{a}bl^{n-1-\beta}+1)$th power, as seen above, and the class of $\sigma$ to elevation to the $(l^{n-1}+1)$th power. The group $G_{k,\rho,\tau^a\sigma^b}$ consists of those elements $g$ of $\mathrm{Gal}(k(\zeta_{l^{n-\beta}})/k)$ such that $\nu_{k,\tau^a\sigma^b}(g)$ is congruent to a product of powers of $l^{n-1}+1$ and $-\tilde{a}bl^{n-1-\beta}+1$ modulo $l^{n-\beta}$. But all these are congruent to 1 modulo $l^{n-1-\beta}$ and thus $G_{k,\rho,\tau^a\sigma^b}|_{k(\zeta_{l^{n-1-\beta}})} = \{1\}$. Hence

$$E_{k,\rho,\tau^a\sigma^b} \supseteq k(\zeta_{l^{n-1-\beta}}) = k(\zeta_{e_{\mathfrak{p}}/l}),$$

i.e.

$$W(k, E_{k,\rho,\tau^a\sigma^b}) \subseteq W(k, e_{\mathfrak{p}}/l).$$

Therefore, by the assumption that $l^2 \mid e_{\mathfrak{p}}$ and by Lemma 2.6, the class of $\mathfrak{p}^{\frac{l-1}{2}\frac{l^{n+1}}{e_{\mathfrak{p}}}}$ is in

$$W(k, e_{\mathfrak{p}}/l)^{\frac{l-1}{2}\frac{l^{n+1}}{e_{\mathfrak{p}}}} \subseteq W(k, l^{n-1})^{(l-1)l/2}$$

and the same is true for $\mathfrak{p}^{\frac{e_{\mathfrak{p}}-1}{2}\frac{l^{n+1}}{e_{\mathfrak{p}}}}$.

It remains to consider the case $e_{\mathfrak{p}} = l$. We now define $k_1$ as the fixed field of $\tau$ and we first assume that $\mathfrak{p}$ ramifies in $K/k_1$. Then its inertia group in $\mathrm{Gal}(K/k_1) = C(l^n)$ is of order $l$ and thus must be generated by $\tau^{l^{n-1}}$. Hence by Lemma 3.14 of [C2] the class of $\mathfrak{p}$ is in $W(k, E_{k,\mu,\tau^{l^{n-1}}})$ and $\mathfrak{p}^{(l-1)l^{n+1}/e_{\mathfrak{p}}}$ is the square of an ideal of a class in $W(k, E_{k,\mu,\tau^{l^{n-1}}})^{(l-1)l^n/2}$, which is contained in $W(k, l^{n-1})^{(l-1)l/2}$ by Lemma 3.5.

Finally let us consider the case of $\mathfrak{p}$ ramified in $k_1/k$. By Lemma 3.6 the class of $\mathfrak{p}$ is in $W(k, l)$. Hence the class of

$$\mathfrak{p}^{\frac{l-1}{2}\frac{l^{n+1}}{e_{\mathfrak{p}}}} = \mathfrak{p}^{\frac{e_{\mathfrak{p}}-1}{2}\frac{l^{n+1}}{e_{\mathfrak{p}}}}$$

is in $W(k, l)^{(l-1)l^n/2}$. By Lemma 2.6,

$$W(k, l)^{(l-1)l^n/2} \subseteq W(k, l^{n-1})^{(l-1)l^2/2} \subseteq W(k, l^{n-1})^{(l-1)l/2}. \blacksquare$$

THEOREM 3.8. *We have*

$$\mathrm{R}_t(k, C(l^n) \rtimes_\mu C(l)) = W(k, l^{n-1})^{(l-1)l/2}.$$

*Further the group $C(l^n) \rtimes_\mu C(l)$ is good.*

*Proof.* From Theorems 2.1 and 2.2, by Lemmas 3.3 and 3.7, it is immediate that

$$\mathrm{R}_t(k, C(l^n) \rtimes_\mu C(l)) = W(k, l^{n-1})^{(l-1)l/2}.$$

Now we prove that $C(l^n) \rtimes_\mu C(l)$ satisfies all the defining conditions of good groups:

1. This follows immediately, since $W(k, l^{n-1})^{(l-1)l/2}$ is a group.

2. This is part of Lemma 3.7.
3. This is also proved in Lemma 3.7.
4. This follows by Lemma 3.3. ∎

**4. Nonabelian extensions of order $l^3$.** As a particular case of Theorem 3.8 we state the following proposition.

PROPOSITION 4.1. *The group $C(l^2) \rtimes_\mu C(l)$ is good and*

$$\mathrm{R}_t(k, C(l^2) \rtimes_\mu C(l)) = W(k,l)^{(l-1)l/2}.$$

Up to isomorphism, the only other nonabelian group of order $l^3$ is

$$G = \langle x, y, \sigma : x^l = y^l = \sigma^l = 1,\ \sigma x = x\sigma,\ \sigma y = y\sigma,\ yx = xy\sigma\rangle,$$

which is a semidirect product of the normal subgroup $\langle x, \sigma\rangle \cong C(l) \times C(l)$ and the cyclic subgroup $\langle y\rangle$ of order $l$, where the action $\mu_1$ is given by conjugation. Clément Bruche proved in [B] that

$$\mathrm{R}_t(k, G) = W(k,l)^{(l-1)l^2/2}.$$

We can give a different proof of Bruche's result, using class field theory. We will also prove that the nonabelian group of order $l^3$ and exponent $l$ studied by Bruche is a good group.

LEMMA 4.2. *Let $k$ be a number field. Then*

$$\mathrm{R}_t(k, G) \supseteq W(k,l)^{(l-1)l^2/2}.$$

*Further, for any $x \in W(k,l)$ and any positive integer $a$, there exists a tame $G$-extension of $k$ with Steinitz class $x^{(l-1)l^2/2}$ and such that any nontrivial subextension of $K/k$ is ramified at some primes which are unramified in $k(\zeta_a)/k$.*

*Proof.* Let $x \in W(k,l)$. By Theorem 3.19 in [C2] there exists a $C(l)$-extension $k_1$ with Steinitz class $x^{(l-1)/2}$ and which is totally ramified at some prime ideals which are unramified in $k(\zeta_a)/k$. Let $\mathfrak{p}$ be one of them.

Now we would like to use Lemma 3.10 of [C2] to obtain a $C(l) \times C(l)$-extension of $K/k_1$ which is Galois over $k$, with $\mathrm{Gal}(K/k) \cong G$. Unfortunately this is not possible since the exact sequence

$$1 \to C(l) \times C(l) \to \mathcal{H} \to C(l) \to 1$$

does not identify the group $\mathcal{H}$ uniquely as the group $G$. Nevertheless, the argument of that lemma at least produces a $C(l) \times C(l)$-extension of $k_1$ which is Galois over $k$ and with $\mathrm{st}(K/k_1) = 1$. Further we can assume that $\mathrm{Gal}(K/k)$ is nonabelian of order $l^3$ (since the action of $C(l)$ on $C(l) \times C(l)$ is the given one and in particular it is not trivial), that $K/k_1$ is unramified at $\mathfrak{p}$ and that any nontrivial subextension of $K/k$ is ramified at some primes which are unramified in $k(\zeta_a)/k$.

We want to prove that $\mathrm{Gal}(K/k) \cong G$. To this aim, we assume that this is not the case, i.e. that $\mathrm{Gal}(K/k) \cong C(l^2) \rtimes_\mu C(l)$, and we derive a contradiction. First of all, by construction, $\mathrm{Gal}(K/k_1) \cong C(l) \times C(l)$ and this must be a subgroup of $\mathrm{Gal}(K/k) \cong C(l^2) \rtimes_\mu C(l)$: the only possibility is that it is the subgroup $H$ consisting of all elements of $C(l^2) \rtimes_\mu C(l)$ having order 1 or $l$. Since the prime ideal $\mathfrak{p}$ ramifies in $k_1/k$ and not in $K/k_1$, its ramification index is $l$, and therefore its inertia group is contained in $H$. Hence by Galois theory we conclude that the inertia field of $\mathfrak{p}$ in $K/k$ contains $k_1$, i.e. $\mathfrak{p}$ ramifies in $K/k_1$ and not in $k_1/k$. This is a contradiction, since $\mathfrak{p}$ is ramified in $k_1/k$.

Hence we have proved that in the above construction the extension $K/k$ has Galois group $G$. By Proposition 2.3,

$$\mathrm{st}(K/k) = \mathrm{st}(k_1/k)^{[K:k_1]} \mathrm{N}_{k_1/k}(\mathrm{st}(K/k_1)) = x^{(l-1)l^2/2}. \ \blacksquare$$

To prove the opposite inclusion we need the following lemma.

Lemma 4.3. *Let $K/k$ be a tame $G$-extension of number fields. The ramification index of a prime ramifying in $K/k$ is $l$ and its class is contained in $W(k,l)$.*

*Proof.* The ramification index of a ramifying prime is equal to $l$, since the corresponding inertia group must be cyclic and any nontrivial element in $G$ is of order $l$.

Let $k_1$ be the subfield of $K$ fixed by the normal abelian subgroup $\langle x, \sigma\rangle$ of the Galois group $G$ of $K/k$.

If a prime $\mathfrak{p}$ ramifies in $k_1/k$, then its class is in $W(k,l)$ by Lemma 3.6.

If a prime $\mathfrak{p}$ ramifies in $K/k_1$, then it is unramified in $k_1/k$ (the ramification index is prime) and so its inertia group is generated by an element of the form $x^a\sigma^c$, where $a, c \in \{0, 1, \ldots, l-1\}$ are not both 0. By Lemma 3.14 of [C2] the class of $\mathfrak{p}$ is in $W(k, E_{k,\mu_1,x^a\sigma^c})$. For any $b \in \{0, 1, \ldots, l-1\}$ we have

$$\mu_1(y^b)(x^a\sigma^c) = y^b x^a \sigma^c y^{-b} = x^a \sigma^{c+ab},$$

and this expression cannot be a nontrivial power of $x^a\sigma^c$. Hence, by definition, the group $G_{k,\mu_1,x^a\sigma^c}$ must be trivial and we conclude that $E_{k,\mu_1,x^a\sigma^c} = k(\zeta_l)$. Therefore, in particular, the class of the prime ideal $\mathfrak{p}$ is contained in $W(k,l)$. $\blacksquare$

Proposition 4.4. *The group $G$ is good and*

$$\mathrm{R}_t(k,G) = W(k,l)^{(l-1)l^2/2}.$$

*Proof.* The proof is straightforward using the preceding lemmas. $\blacksquare$

**Acknowledgements.** I am very grateful to Professor Cornelius Greither and to Professor Roberto Dvornicich for their advice and for the patience they showed, assisting me in the writing of my PhD thesis with a lot of suggestions. I also wish to thank the Scuola Normale Superiore of Pisa, for its role in my mathematical education and for its support during the time I was working on my PhD thesis.

## References


[B] C. Bruche, *Classes de Steinitz d'extensions non abéliennes de degré $p^3$*, Acta Arith. 137 (2009), 177–191.

[BS] C. Bruche and B. Sodaïgui, *On realizable Galois module classes and Steinitz classes of nonabelian extensions*, J. Number Theory 128 (2008), 954–978.

[BGS] N. P. Byott, C. Greither et B. Sodaïgui, *Classes réalisables d'extensions non abéliennes*, J. Reine Angew. Math. 601 (2006), 1–27

[Ca1] J. E. Carter, *Steinitz classes of a nonabelian extension of degree $p^3$*, Colloq. Math. 71 (1996), 297–303.

[Ca2] —, *Steinitz classes of nonabelian extensions of degree $p^3$*, Acta Arith. 78 (1997), 297–303.

[CaS] J. E. Carter et B. Sodaïgui, *Classes de Steinitz d'extensions quaternioniennes généralisées de degré $4p^r$*, J. London Math. Soc. (2) 76 (2007), 331–344.

[C1] A. Cobbe, *Steinitz classes of tamely ramified Galois extensions of algebraic number fields*, PhD thesis, Scuola Normale Superiore, Pisa, 2010.

[C2] —, *Steinitz classes of tamely ramified Galois extensions of algebraic number fields*, J. Number Theory 130 (2010), 1129–1154.

[E] L. P. Endo, *Steinitz classes of tamely ramified Galois extensions of algebraic number fields*, PhD thesis, Univ. of Illinois at Urbana-Champaign, 1975.

[GS1] M. Godin et B. Sodaïgui, *Classes de Steinitz d'extensions à groupe de Galois $A_4$*, J. Théor. Nombres Bordeaux 14 (2002), 241–248.

[GS2] —, —, *Module structure of rings of integers in octahedral extensions*, Acta Arith. 109 (2003), 321–327.

[L] S. Lang, *Algebraic Number Theory*, 2nd ed., Grad. Texts in Math. 110, Springer, New York, 1994.

[Lo1] R. Long, *Steinitz classes of cyclic extensions of degree $l^r$*, Proc. Amer. Math. Soc. 49 (1975), 297–304.

[Lo2] —, *Steinitz classes of cyclic extensions of prime degree*, J. Reine Angew. Math. 250 (1971), 87–98.

[MS] R. Massy et B. Sodaïgui, *Classes de Steinitz et extensions quaternioniennes*, Proyecciones 16 (1997), 1–13.

[MC1] L. R. McCulloh, *Cyclic extensions without relative integral bases*, Proc. Amer. Math. Soc. 17 (1966), 1191–1194.

[MC2] —, *Galois module structure of abelian extensions*, J. Reine Angew. Math. 375/376 (1987), 259–306.

[Na] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 3rd ed., Springer Monogr. Math., Springer, Berlin, 2004.

[Ne] J. Neukirch, *Class Field Theory*, Grundlehren Math. Wiss. 280, Springer, Berlin, 1986.

[S1] B. Sodaïgui, *Classes de Steinitz d'extensions galoisiennes relatives de degré une puissance de 2 et problème de plongement*, Illinois J. Math. 43 (1999), 47–60.

[S2] —, *Relative Galois module structure and Steinitz classes of dihedral extensions of degree 8*, J. Algebra 223 (2000), 367–378.

[Sov] E. Soverchia, *Steinitz classes of metacyclic extensions*, J. London Math. Soc. (2) 66 (2002), 61–72.

Alessandro Cobbe
Scuola Normale Superiore
Piazza dei Cavalieri, 7
I-56126 Pisa, Italy
E-mail: a.cobbe@sns.it

*Received on 19.1.2010*
*and in revised form on 24.1.2011* (6273)