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

Alessandro Cobbe

January 19, 2010

Abstract

The Steinitz class of a number field extension $K/k$ is an ideal class in the ring of integers $\mathcal{O}_k$ of $k$, which, together with the degree $[K : k]$ of the extension determines the $\mathcal{O}_k$-module structure of $\mathcal{O}_K$. We call $R_t(k, G)$ the classes which are Steinitz classes of a tamely ramified $G$-extension of $k$. We will say that those classes are realizable for the group $G$; it is conjectured that the set of realizable classes is always a group.

In this paper we will develop some of the ideas contained in [8] to study some $l$-groups, where $l$ is an odd prime number. In particular, together with [1] we will complete the study of realizable Steinitz classes for groups of order $l^3$. We will also give an alternative proof of the results of [1], based on class field theory.

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 [18] 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 [18] 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 $\text{st}(K/k)$. Let $k$ be a number field and $G$ a finite group, then we define:

$$R_t(k, G) = \{ x \in \text{Cl}(k) : \exists K/k \text{ tame, } \text{Gal}(K/k) \cong G, \text{st}(K/k) = x \}.$$
1 Preliminary results

In this paper we will use the notations and some techniques from [8] to study the realizable classes for some $l$-groups, where $l$ is an odd prime number.

Some of the results in this paper are parts of the author’s PhD thesis [7]. For earlier results see [1], [2], [3], [4], [5], [6], [9], [10], [11], [13], [14], [15], [16], [17], [20], [21] and [22].

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.

1 Preliminary results

We start recalling the following two fundamental results.

**Theorem 1.1.** If $K/k$ is a finite tame Galois extension then

$$d(K/k) = \prod_p p^{(e_p - 1)[K:A]/e_p},$$

where $e_p$ is the ramification index of $p$.

**Proof.** This follows by Propositions 8 and 14 of chapter III of [12].

**Theorem 1.2.** Assume $K$ is a finite Galois extension of a number field $k$.

(a) If its Galois group either has odd order or has a noncyclic 2-Sylow subgroup then $d(K/k)$ is the square of an ideal and this ideal represents the Steinitz class of the extension.

(b) If its 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 $d(K/k)/\alpha$ 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 [9]. In particular it is shown in [9] that in case (b) $K/k$ does have exactly one quadratic subextension. 

\[2\]
Further, considering Steinitz classes in towers of extensions, we will need the following proposition.

**Proposition 1.3.** Suppose $K/k_1$ and $k_1/k$ are number fields extensions. Then

$$\text{st}(K/k) = \text{st}(k_1/k)[k_1:E]N_{k_1/k}(\text{st}(K/k_1)).$$

**Proof.** This is Proposition I.1.2 in [9].

We will also use some other preliminary results.

**Lemma 1.4.** Let $m, n, x, y$ be integers. If $x \equiv y \pmod{m}$ and any prime $q$ dividing $n$ divides also $m$ 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 $q_r | m$, as above, for some $c \in \mathbb{N}$ we have

$$x^n = (y^{q_1 \ldots q_{r-1}} + cmq_1 \ldots q_{r-1})^{q_r}$$

$$= y^n + \sum_{i=1}^{q_r} \binom{q_r}{i} (cmq_1 \ldots q_{r-1})^i y^{q_1 \ldots q_{r-1}(q_r-i)} \equiv y^n \pmod{mn}.$$

**Definition 1.5.** Let $K/k$ be a finite abelian extension of number fields. 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 [9], Proposition 1.10):

- $W(k, K) = \{x \in J_K/P_k : x \text{ contains infinitely many primes of absolute degree 1 splitting completely in } K\}$
- $W(k, K) = \{x \in J_K/P_k : x \text{ contains a prime splitting completely in } K\}$
- $W(k, K) = N_{K/k}(J_K) \cdot P_k/P_k$.

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


Lemma 1.6. If $q | n \Rightarrow q | m$ then $W(k, m)^n \subseteq W(k, mn)$.

Proof. Let $x \in W(k, m)$. According to Proposition 1.10 and Lemma 1.11, both from [8], $x$ contains a prime ideal $p$, prime to $mn$ and such that $N_{k/Q}(p) \in P_m^n$, where $m = m \cdot p_\infty$. Then by Lemma 1.4 $N_{k/Q}(p^n) \in P_m^n$, with $n = mn \cdot p_\infty$, and it follows from Lemma 1.12 of [8] that $x^n \in W(k, mn)$.  

Definition 1.7. We will call a finite group $G$ of order $m$ good if the following properties are verified:

1. For any number field $k$, $R_t(k, G)$ 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 $p$, with ramification index $e_p$ in $K/k$, the ideal class of
   
   $\left(p^{(e_p-1)m_{e_p}} - e_p(\alpha_{K/k})\right)^{\frac{1}{2}}$
   
   is in $R_t(k, G)$.
3. For any tame $G$-extension $K/k$ of number fields, for any prime ideal $p$ of $k$ and any rational prime $l$ dividing its ramification index $e_p$, the class of the ideal
   
   $p^{(l-1)m_{e_p(l)}}$
   
   is in $R_t(k, G)$ and, if $2$ divides $(l-1)m_{e_p(l)}$, the class of
   
   $p^{\frac{l-1}{2}m_{e_p(l)}}$
   
   is in $R_t(k, G)$.
4. $G$ is such that for any number field $k$, for any class $x \in R_t(k, G)$ and any integer $a$, there exists a tame $G$-extension $K$ with Steinitz class $x$ and such that every non trivial subextension of $K/k$ is ramified at some primes which are unramified in $k(\zeta_a)/k$.
2 Some \(l\)-groups

In [1], 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 \(R_k(k, G) = W(k, l)^{u(l-1)/2}\) 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 \(R_k(k, C(l^2) \rtimes \mu C(l)) = W(k, l)^{l(l-1)/2}\), 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 \(l^3\).

**Lemma 2.1.** 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 \(\mu\).

**Proof.** Let \(G\) be the group written 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 \(x\tau x^{-1} = \tau^{n-1}+1\), i.e. \(x\tau = \tau^{n-1}+1x\). 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

\[\tau^a x^n = x^l = 1,\]

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

\[(\tau^{-b} x)^m = \tau^{-(bl-b^{l-1}(m-1)m/2)} x^m.\]

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

\[(\tau^{-b} x)^m = \tau^{-(bl-1-b^{l-1}(m-2)(m-1)/2)} x^{m-1} \tau^{-b} x = \tau^{-(bl-1-b^{l-1}(m-2)(m-1)/2)} x^{m-1} \tau^{-b} x = \tau^{-(bl-1-b^{l-1}(m-1)/2)} x^m = \tau^{-(bl-1-b^{l-1}(m-1)/2)} x^m = \tau^{-(bl-1-b^{l-1}(m-1)/2-2b(m-1)))} x^m = \tau^{-(bm-b^{l-1}(m-1)m/2)} x^m.\]

Then calling \(\sigma = \tau^{-b} x\), we obtain that

\[\sigma^l = (\tau^{-b} x)^l = \tau^{-bl} x^l = \tau^{-a+a} = 1.\]
Further
\[ \sigma \tau \sigma^{-1} = \tau^{-b} x \tau x^{-1} \tau^b = \tau^{-b} \tau^{l^n - 1} \tau^b = \tau^{l^n - 1} \]
and \( \sigma, \tau \) are generators of \( G \). Thus \( G \) must be a quotient of the group
\[ \langle \sigma, \tau : \sigma^l = \tau^n = 1, \sigma \tau \sigma^{-1} = \tau^{l^n - 1} \rangle. \]
But this group has the same order of \( G \) and thus they must be equal. \( \square \)

It follows that we can use Proposition 2.13 of \[8\] to study \( \text{R}_t(k, C(l^n) \rtimes \mu C(l)) \), for any number field \( k \).
For any \( \tau \in H \) we define \( E_{k,\mu,\tau} \) as the fixed field in \( k(\zeta_{o(\tau)}) \) of
\[ G_{k,\mu,\tau} = \left\{ g \in \text{Gal}(k(\zeta_{o(\tau)})/k) : \exists g_1 \in \mathcal{G}, \mu(g_1)(\tau) = \tau^{\nu_{k,\tau}(g)} \right\} \]
where \( g_2(\zeta_{o(\tau)}) = \zeta_{o(\tau)}^{\nu_{k,\tau}(g_2)} \) for any \( g_2 \in \text{Gal}(k(\zeta_{o(\tau)})/k) \).

**Lemma 2.2.** Let \( \tau \) be a generator of \( C(l^n) \) in \( C(l^n) \rtimes \mu C(l) \). 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
\[ G_{k,\mu,\tau} = \left\{ g \in \text{Gal}(k(\zeta_{l^n})/k) : \exists g_1 \in C(l) \mu(g_1)(\tau) = \tau^{\nu_{k,\tau}(g)} \right\} \]
\[ = \left\{ g \in \text{Gal}(k(\zeta_{l^n})/k) : \exists a \in \mathbb{N} \tau^{al^n - 1} = \tau^{\nu_{k,\tau}(g)} \right\} \]
\[ = \left\{ g \in \text{Gal}(k(\zeta_{l^n})/k) : \nu_{k,\tau}(g) \equiv 1 \pmod{l^n - 1} \right\} \]
\[ = \left\{ g \in \text{Gal}(k(\zeta_{l^n})/k) : g(\zeta_{l^n - 1}) = \zeta_{l^n - 1} \right\} = \text{Gal}(k(\zeta_{l^n})/k(\zeta_{l^n - 1})). \]
Hence \( E_{k,\mu,\tau} = k(\zeta_{l^n - 1}) \). \( \square \)

**Lemma 2.3.** We have
\[ \text{R}_t(k, C(l^n) \rtimes \mu C(l)) \supseteq W(k, l^{n-1}) \mathbb{Z}^l. \]
Further, for any \( x \in W(k, l^{n-1}) \) and any positive integer \( a \), there exists a tame \( G \)-extension of \( k \) with Steinitz class \( x_{l^a} \) and such that any nontrivial subextension of \( K/k \) is ramified at some primes which are unramified in \( k(\zeta_a)/k \).

**Proof.** By Proposition 2.13 of \[8\] and Lemma 2.1
\[ \text{R}_t(k, C(l^n) \rtimes \mu C(l)) \supseteq \text{R}_t(k, C(l))^l \cdot W(k, E_{k,\mu,\tau})_{l^{n-1}}, \]
where \( \tau \) is a generator of \( C(l^n) \). We easily conclude since \( 1 \in \text{R}_t(k, C(l)) \) and, by Lemma 2.2 \( E_{k,\mu,\tau} = k(\zeta_{l^n - 1}) \), i.e.
\[ W(k, E_{k,\mu,\tau}) = W(k, l^{n-1}). \]
The second part of the lemma follows again by Proposition 2.13 of \[8\]. \( \square \)
To prove the opposite inclusion we need some lemmas.

**Lemma 2.4.** Let \( \tau \) be a generator of \( C(l^n) \) in \( C(l^n) \rtimes \mu \) \( C(l) \) and \( 0 < c < n \) be an integer, then
\[
G_{k,\mu,\tau^c}^{lc} \subseteq G_{k,\mu,\tau}.
\]

**Proof.** For any positive integer \( a \) we define
\[
\hat{\mu}^a : G \to (\mathbb{Z}/o(\tau^c))^*
\]
by \( \tau^a \hat{\mu}^a (g_1) = \mu(g_1)(\tau^a) \) for all \( g_1 \in G \). By definition, if \( g \in G_{k,\mu,\tau^c} \), then there exists \( g_1 \in G \) such that
\[
\tau^c \hat{\mu}^c (g_1) = \mu(g_1)(\tau^c) = \tau^c \hat{\mu}^c (g_1).
\]
We also observe that
\[
\zeta_{l^n-c}^{\nu_{k,\tau^c}} (g) = \zeta_{l^n}^{\nu_{k,\tau^c}} (g) = g (\zeta_{l^n-c}) = \zeta_{l^n-c}^{\nu_{k,\tau^c}} (g)
\]
and that
\[
\tau^{\nu_{k,\tau^c}} (g_1) = \mu(g_1)(\tau^c) = \mu(g_1)(\tau) = \tau^{\nu_{k,\tau^c}} (g_1).
\]
From the above equalities we deduce that
\[
\nu_{k,\tau^c} (g) \equiv \nu_{k,\tau^c} (g_1) \equiv \hat{\mu}^c (g_1) \equiv \hat{\mu}^c (g_1) \pmod{l^n-c}
\]
and therefore by Lemma 1.4 we obtain that
\[
\nu_{k,\tau^c} (g^c) \equiv \hat{\mu}^c (g_1^c) \pmod{l^n}.
\]
We conclude that
\[
\tau^{\nu_{k,\tau^c}} (g^c) = \hat{\mu}^c (g_1^c) = \mu(g_1^c)(\tau)
\]
and hence that \( g^c \in G_{k,\mu,\tau}. \)

**Lemma 2.5.** Let \( \tau \) be a generator of \( C(l^n) \) in \( C(l^n) \rtimes \mu \) \( C(l) \) and \( 0 < c < n \) be an integer, then
\[
W(k, E_{k,\mu,\tau^c})^{lc} \subseteq W(k, l^n-1).
\]

**Proof.** Let \( x \) be a class in \( W(k, E_{k,\mu,\tau^c}) \). By Proposition 1.10 in [8] there exists a prime \( p \) in the class of \( x \) splitting completely in \( E_{k,\mu,\tau^c}/k \). By Theorem IV.8.4 in [19], \( p \in H_m^{E_{k,\mu,\tau^c}/k} \), where \( m \) is a cycle of declaration of \( E_{k,\mu,\tau^c}/k \). Then, by Proposition II.3.3 in [19],
\[
\left( \frac{k(\zeta_{l^n})/k}{p} \right)_{E_{k,\mu,\tau^c}} = \left( \frac{E_{k,\mu,\tau^c}/k}{p} \right) = 1.
\]
2 Some $l$-groups

Thus
\[
\left( \frac{k(\zeta_{ln})/k}{\mathfrak{p}} \right) \in \text{Gal}(k(\zeta_{ln})/E_{k,\mu,\tau^{lc}}) = G_{k,\mu,\tau^{lc}}
\]
and it follows by Lemma 2.4 that
\[
\left( \frac{k(\zeta_{ln})/k}{\mathfrak{p}^{e^p}} \right) = \left( \frac{k(\zeta_{p^n})/k}{\mathfrak{p}} \right)^{lc} \in G_{k,\mu,\tau} \subseteq \text{Gal}(k(\zeta_{ln})/E_{k,\mu,\tau}).
\]
Then
\[
\left( \frac{E_{k,\mu,\tau}/k}{\mathfrak{p}^{e^p}} \right) = \left( \frac{k(\zeta_{p^n})/k}{\mathfrak{p}^{e^p}} \right)_{E_{k,\mu,\tau}} = 1
\]
and so the class $x^{e^p}$ of $\mathfrak{p}^{e^p}$ is in $W(k, E_{k,\mu,\tau})$, which is equal to $W(k, l^{n-1})$ by Lemma 2.2.

**Lemma 2.6.** 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 $e$, then $N_{k/\mathbb{Q}}(\mathfrak{p}) \in \mathcal{P}_m$, where $m = e \cdot p^\infty$. In particular, by Lemma 1.12 of [8], $\mathfrak{p} \in H^m_{k(\zeta_{e^n})/k}$ and so its class is in $W(k, e)$.

**Proof.** This is Lemma I.2.1 of [9].

**Lemma 2.7.** Let $K/k$ be a tame $C(l^n) \ltimes_{\mu} C(l)$-extension of number fields and let $\mathfrak{p}$ be a ramifying prime, with ramification index $e_{\mathfrak{p}}$. Then the class of
\[
\mathfrak{p}^{e_{\mathfrak{p}} - 1} \cdot \frac{p^{\frac{n^p + 1}{e_{\mathfrak{p}}}}}{p^{\frac{n^p}{e_{\mathfrak{p}}}}}
\]
and the class of
\[
\mathfrak{p}^{\frac{1}{2}} \cdot \frac{p^{\frac{n^{p+1}}{e_{\mathfrak{p}}}}}{p^{\frac{n^p}{e_{\mathfrak{p}}}}}
\]
are both in
\[
W(k, l^{n-1}) \frac{1}{2} l.
\]

**Proof.** The Galois group of $K/k$ is $C(l^n) \ltimes_{\mu} C(l)$, i.e.
\[
G = \langle \sigma, \tau : \sigma^l = \tau^n = 1, \sigma \tau \sigma^{-1} = \tau^{n^p - 1} \rangle.
\]

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 $\tau^l = 1$, we obtain that
\[
e_{\mathfrak{p}} = \text{smallest positive integer such that} 
\]
\[
\tau^{ae_{\mathfrak{p}}} \sigma^{be_{\mathfrak{p}}} = 1.
\]
First of all we assume that $l^2$ divides $e_p$. If $l^2$ is the exact power of $l$ dividing $a$, we obtain that $e_p = l^{n-\beta}$ and in particular that $\beta \leq n - 2$. So we have

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

and

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

where $a \tilde{\alpha} \equiv l^2 \pmod{l^n}$. 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 $p$ is totally ramified in $K/k_1$ and unramified in $k_1/k$. By Lemma 2.14 of [5] the class of $p$ 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 $\tau$ to the elevation to the $-\tilde{\alpha}bl^{n-1} \beta + 1$-th power, as seen above, and $\sigma$ to the elevation to the $l^{n-1}+1$-th power. The group $G_{k,\rho,\tau^a \sigma^b}$ consists of those elements $g$ of $\text{Gal}(k_1(\zeta_{l^{n-1}})/k)$ such that $\nu_{k,\tau^a \sigma^b}(g)$ is congruent to a product of powers of $l^{n-1}+1$ and $-\tilde{\alpha}bl^{n-1} \beta + 1$ modulo $l^{n-1} \beta$. 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

$$E_{k,\rho,\tau^a \sigma^b} \supseteq k(\zeta_{l^{n-1} \beta}) \supseteq k(\zeta_{\frac{l^n}{l}})$$

i.e.

$$W(k, E_{k,\rho,\tau^a \sigma^b}) \subseteq W(k, \frac{e_p}{l^2}).$$

Hence, by the assumption that $l^2|e_p$, the class of

$$p^\frac{l-1}{2} \frac{l^{n+1}}{\text{e}_p}$$

is in

$$W(k, \frac{e_p}{l^2}) \frac{l-1}{2} \frac{l^{n+1}}{\text{e}_p} \subseteq W(k, l^{n-1}) \frac{l-1}{2},$$

and the same is true for

$$p^\frac{e_p-1}{2} \frac{l^{n+1}}{\text{e}_p}.$$

It remains to consider the case $e_p = l$. We now define $k_1$ as the fixed field of $\tau$ and we first assume that $p$ ramifies in $K/k_1$. Then its inertia group in $\text{Gal}(K/k_1) = C(l^n)$ is of order $l$ and thus must be generated by $\tau^{l^{n-1}}$. Hence by Lemma 2.14 of [5] the class of $p$ is in $W(k, E_{k,\mu,\tau^{l^{n-1}}})$ and $p^\frac{(l-1) \frac{l^{n+1}}{\text{e}_p}}{2}$ is the square of an ideal in $W(k, E_{k,\mu,\tau^{l^{n-1}}}) \frac{l-1}{2} l^{n}$, which is contained in $W(k, E_{k,\mu,\tau^{l^{n-1}}}) \frac{l-1}{2} l^{n}$ by Lemma 2.5. Hence, by Lemma 2.2 the class of

$$p^\frac{l-1}{2} \frac{l^{n+1}}{\text{e}_p} = p^\frac{e_p-1}{2} \frac{l^{n+1}}{\text{e}_p}$$

9
3 Nonabelian extensions of order \( l^3 \)

is in

\[
W(k, l^n)^{\frac{l-1}{2}}.
\]

Finally let us consider the case of \( p \) ramified in \( k_1/k \). By Lemma 2.6 the class of \( p \) is in \( W(k, l) \). Hence the class of

\[
p^{\frac{l-1}{2} \cdot (n+1)} = p^{\frac{p-1}{2} \cdot (n+1)}
\]

is in

\[
W(k, l)^{\frac{l-1}{2}ln}.
\]

By Lemma 1.6

\[
W(k, l)^{\frac{l-1}{2}ln} \subseteq W(k, l^n)^{\frac{l-1}{2}} \subseteq W(k, l^n)^{\frac{l-1}{2}}.
\]

Theorem 2.8. We have

\[
\text{R}_t(k, C(l^n) \rtimes \mu C(l)) = W(k, l^n)^{\frac{l-1}{2}}.
\]

Further the group \( C(l^n) \rtimes \mu C(l) \) is good.

Proof. By Theorems 1.1 and 1.2, by Lemma 2.3 and Lemma 2.7 it is immediate that

\[
\text{R}_t(k, C(l^n) \rtimes \mu C(l)) = W(k, l^n)^{\frac{l-1}{2}}.
\]

The prove that \( C(l^n) \rtimes \mu C(l) \) is good is now straightforward using the same results.

3 Nonabelian extensions of order \( l^3 \)

As a particular case of Theorem 2.8 we state the following proposition.

Proposition 3.1. The group \( C(l^2) \rtimes \mu C(l) \) is good and

\[
\text{R}_t(k, C(l^2) \rtimes \mu C(l)) = W(k, l)^{\frac{l-1}{2}}.
\]

Up to isomorphism, the only other nonabelian group of order \( l^3 \) is

\[
G = \langle x, y, \sigma : x^l = y^l = \sigma^l = 1, \sigma x = x \sigma, \sigma y = y \sigma, yx = x y \sigma \rangle,
\]

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 [1] that

\[
\text{R}_t(k, G) = W(k, l)^{\frac{l-1}{2}l^2}.
\]
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 3.2.** Let \( k \) be a number field, then

\[
R_t(k, G) \supseteq W(k, l)^{l^2l^2}.
\]

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

**Proof.** Let \( x \in W(k, l) \) and \( n \in \mathbb{N} \setminus \{0\} \). By Theorem 2.19 in [8] there exists a \( C(l) \)-extension \( k_1 \) with Steinitz class \( x^{l^2l^2} \) and which is totally ramified at some prime ideals, which are unramified in \( k(\zeta_a)/k \). Let \( p \) be one of them.

Now we would like to use Lemma 2.10 of [8] to obtain a \( C(l) \times C(l) \)-extension of \( k_1 \) which is Galois over \( k \), with \( \text{Gal}(K/k) \cong G \). 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 \( \text{st}(K/k_1) = x^{l^2l^2} \). Further we get that \( K/k_1 \) is unramified at \( p \) 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 \( \text{Gal}(K/k) \cong G \). To this aim, we assume that this is not the case, i.e. that \( \text{Gal}(K/k) \cong C(l^2) \times_{\mu} C(l) \), and we derive a contradiction. First of all, by construction, \( \text{Gal}(K/k_1) \cong C(l) \times C(l) \) and this must be a subgroup of \( \text{Gal}(K/k) \cong C(l^2) \times_{\mu} C(l) \): the only possibility is that it is the subgroup \( H \) which arises by replacing \( C(l^2) \) (the left hand factor in the semidirect product) by its subgroup of order \( l \); \( H \) happens to consist of all elements of \( C(l^2) \times_{\mu} C(l) \) having order 1 or \( l \). Since the prime ideal \( p \) 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 \( p \) in \( K/k \) contains \( k_1 \), i.e. that \( p \) ramifies in \( K/k_1 \) and not in \( k_1/k \). This is a contradiction, since \( p \) 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 1.3

\[
\text{st}(K/k) = \text{st}(k_1/k)^{[K:k_1]} = x^{l^{-1}l^2}N_{k_1/k}(\text{st}(K/k_1)).
\]
To prove the opposite inclusion we need the following lemma.

**Lemma 3.3.** 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 $p$ ramifies in $k_1/k$, then its class is in $W(k, l)$ by Lemma 2.6.

If a prime $p$ 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 2.14 of [8] the class of $p$ 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 $a^a\sigma^c$. 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 $p$ is contained in $W(k, l)$.

**Proposition 3.4.** The group $G$ is good and

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

*Proof.* One inclusion is given by Lemma 3.2. The proof that $\text{R}_l(k, G) \subseteq W(k, l)^{1-1/2}$ follows by Lemma 3.3 since for any tame $G$-extension $K/k$ of number fields the Steinitz class is the class of the ideal

$$
\prod_{p: e_p \neq 1} p^{e_p - 1/2} = \prod_{p: e_p \neq 1} p^{1-1/2},
$$

which is contained in $W(k, l)^{1-1/2}$. Now we prove that all the properties of good groups are verified.

1. This is clear, since $W(k, l)$ is a group.

2. For any prime $p$, ramifying in a tame $G$-extension $K/k$ of number fields, by Lemma 3.3 the class of

$$
p^{e_p - 1/2}\frac{\sigma^3}{e_p} = p^{1-1/2}
$$

is contained in $W(k, l)^{1-1/2}$, which is equal to $\text{R}_l(k, G)$. 

12
3. Immediate by Lemma 3.3 and the explicit formula for $R_t(k, G)$.

4. This follows by Lemma 3.2.

References

[1] C. Bruche. Classes de Steinitz d’extensions non abéliennes de degré $p^3$. *Acta Arith.*, 137(2):177–191, 2009.

[2] C. Bruche and B. Sodaïgui. On realizable Galois module classes and Steinitz classes of nonabelian extensions. *J. Number Theory*, 128(4):954–978, 2008.

[3] N. P. Byott, C. Greither, and B. Sodaïgui. Classes réalisables d’extensions non abéliennes. *J. Reine Angew. Math.*, 601:1–27, 2006.

[4] J. E. Carter. Steinitz classes of a nonabelian extension of degree $p^3$. *Colloq. Math.*, 71(2):297–303, 1996.

[5] J. E. Carter. Steinitz classes of nonabelian extensions of degree $p^3$. *Acta Arith.*, 78(3):297–303, 1997.

[6] J. E. Carter and B. Sodaïgui. Classes de Steinitz d’extensions quaternionniennes généralisées de degré $4p^r$. *J. Lond. Math. Soc. (2)*, 76(2):331–344, 2007.

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

[8] A. Cobbe. *Steinitz classes of tamely ramified Galois extensions of algebraic number fields*. arXiv:0910.5080v1, to appear in Journal of Number Theory.

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

[10] M. Godin and B. Sodaïgui. Classes de Steinitz d’extensions à groupe de Galois $A_4$. *J. Théor. Nombres Bordeaux*, 14(1):241–248, 2002.

[11] M. Godin and B. Sodaïgui. Module structure of rings of integers in octahedral extensions. *Acta Arith.*, 109(4):321–327, 2003.
References

[12] S. Lang. *Algebraic number theory*. GTM 110. Springer-Verlag, New York, second edition, 1994.

[13] R. Long. Steinitz classes of cyclic extensions of degree $l$. *Proc. Amer. Math. Soc.*, 49:297–304, 1975.

[14] R. L. Long. Steinitz classes of cyclic extensions of prime degree. *J. Reine Angew. Math.*, 250:87–98, 1971.

[15] R. Massy and B. Sodaigui. Classes de Steinitz et extensions quaternioniennes. *Proyecciones*, 16(1):1–13, 1997.

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

[17] L. R. McCulloh. Galois module structure of abelian extensions. *J. Reine Angew. Math.*, 375/376:259–306, 1987.

[18] W. Narkiewicz. *Elementary and analytic theory of algebraic numbers*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, third edition, 2004.

[19] J. Neukirch. *Class field theory*, volume 280 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1986.

[20] B. Sodaigui. Classes de Steinitz d’extensions galoisiennes relatives de degré une puissance de 2 et problème de plongement. *Illinois J. Math.*, 43(1):47–60, 1999.

[21] B. Sodaigui. Relative Galois module structure and Steinitz classes of dihedral extensions of degree 8. *J. Algebra*, 223(1):367–378, 2000.

[22] E. Soverchia. Steinitz classes of metacyclic extensions. *J. London Math. Soc. (2)*, 66(1):61–72, 2002.