Steinitz classes of tamely ramified Galois extensions of algebraic number fields

Alessandro Cobbe

October 27, 2009

Abstract

The Steinitz class of a number field extension $K/k$ is an ideal class in the ring of integers $O_k$ of $k$, which, together with the degree $[K : k]$ of the extension determines the $O_k$-module structure of $O_K$. 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.

We define $A'$-groups inductively, starting by abelian groups and then considering semidirect products of $A'$-groups with abelian groups of relatively prime order and direct products of two $A'$-groups. Our main result is that the conjecture about realizable Steinitz classes for tame extensions is true for $A'$-groups of odd order; this covers many cases not previously known. Further we use the same techniques to determine $R_t(k, D_n)$ for any odd integer $n$.

In contrast with many other papers on the subject, we systematically use class field theory (instead of Kummer theory and cyclotomic descent).

Introduction

Let $K/k$ be an extension of number fields and let $O_K$ and $O_k$ be their rings of integers. By Theorem 1.13 in [15] we know that

$$O_K \cong O_k^{[K : k]-1} \oplus I$$

where $I$ is an ideal of $O_k$. By Theorem 1.14 in [15] the $O_k$-module structure of $O_K$ is determined by $[K : k]$ and the ideal class of $I$. This class is called
the \textit{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:

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

\textbf{Definition 0.1.} We define \textit{$A'$-groups} inductively:

1. Finite abelian groups are \textit{$A'$-groups}.

2. If $\mathcal{G}$ is an \textit{$A'$-group} and $H$ is finite abelian of order prime to that of $\mathcal{G}$, then $H \rtimes \mu \mathcal{G}$ is an \textit{$A'$-group}, for any action $\mu$ of $\mathcal{G}$ on $H$.

3. If $\mathcal{G}_1$ and $\mathcal{G}_2$ are \textit{$A'$-groups}, then $\mathcal{G}_1 \times \mathcal{G}_2$ is an \textit{$A'$-group}.

In the following proposition we find a relation between \textit{$A'$-groups} and more classical kinds of groups.

\textbf{Proposition 0.2.} Every \textit{$A'$-group} is a solvable \textit{$A$-group} (an \textit{$A$-group} is a finite group with the property that all of its Sylow subgroups are abelian).

\textit{Proof.} Since abelian groups are obviously solvable \textit{$A$-groups}, we have only to prove that the property of being a solvable \textit{$A$-group} is preserved by constructions 2 and 3 in Definition 0.1.

If $\mathcal{G}$, $\mathcal{G}_1$ and $\mathcal{G}_2$ are solvable and $H$ is abelian, then $H \rtimes \mu \mathcal{G}$ and $\mathcal{G}_1 \times \mathcal{G}_2$ are clearly solvable.

If $\mathcal{G}$ is an $A$-group and $H$ is abelian of order prime to that of $\mathcal{G}$, then for any prime $l$ dividing the order of $H$ an $l$-Sylow subgroup of $H \rtimes \mu \mathcal{G}$ must be a subgroup of $H$ and thus must be abelian. If $l$ divides the order of $\mathcal{G}$ then an $l$-Sylow subgroup of $H \rtimes \mu \mathcal{G}$ is isomorphic to one of $\mathcal{G}$ and thus it is abelian, by hypothesis. So $H \rtimes \mu \mathcal{G}$ is an $A$-group.

If $\mathcal{G}_1$ and $\mathcal{G}_2$ are $A$-groups, then for any prime $l$, an $l$-Sylow subgroup of $\mathcal{G}_1 \times \mathcal{G}_2$ is a direct product of $l$-Sylow subgroups of $\mathcal{G}_1$ and $\mathcal{G}_2$ and hence it is abelian, and $\mathcal{G}_1 \times \mathcal{G}_2$ is an $A$-group.

It is an open question whether the converse of the proposition is true or not.

The main result we are going to prove is that the realizable classes for a number field $k$ and an \textit{$A'$-group} $G$ of odd order form a group; this covers many cases not previously known. Further we use the same techniques to determine $R_t(k, D_n)$ for any odd integer $n$.

In contrast with many other papers on the subject, we systematically use class field theory (instead of Kummer theory and cyclotomic descent).

This paper is a slightly shortened version of parts of the author’s PhD thesis [5]. For earlier results see [1], [2], [3], [4], [7], [8], [9], [11], [12], [13], [14], [18], [19] and [20].
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 and corrections. 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

1.1 Steinitz classes

We start recalling some well-known results about Steinitz classes.

It is a classical result (which can be deduced by Propositions 8 and 14 of chapter III of [10]) that the discriminant of a tamely ramified Galois extension $K/k$ of number fields is

$$d(K/k) = \prod_p p^{(e_p-1)\left\lceil \frac{[K:k]}{e_p} \right\rceil}$$

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

The discriminant is closely related to the Steinitz class by the following theorem.

**Theorem 1.1.** 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 [7]. In particular it is shown in [7] that in case (b) $K/k$ does have exactly one quadratic subextension.

Further, considering Steinitz classes in towers of extensions, we will need the following proposition.
Proposition 1.2. Suppose $K/E$ and $E/k$ are number fields extensions. Then
\[ \text{st}(K/k) = \text{st}(E/k)^{[K:E]}N_{E/k}(\text{st}(K/E)). \]

Proof. This is Proposition I.1.2 in [7].

1.2 Class field theory

To prove our results we will use techniques from class field theory. We will use the notations and some results of [16].

We will denote by $U_p$ the units of a number field $k$ completed at a prime $p$, by $I_k$ the idele group of $k$ and by $C_k = I_k/k^*$ the idele class group. We set
\[ U_p^m = \begin{cases} U_p & \text{if } n = 0 \\ 1 + p^n & \text{if } n > 0. \end{cases} \]

For any cycle $m = \prod_p p^{n_p}$ we consider the groups $I_k^m = \prod_p U_p^{n_p}$ and the congruence subgroup mod $m$ of $C_k$, i.e. $C_k^m = I_k^m/k^*/k^* \subseteq C_k$.

For every prime $p$ we have the canonical injection \( [ ] : k_p^* \to C_k, \) which associates to $a_p \in k_p^*$ the class of the idele \( [a_p] = (\ldots, 1, 1, 1, a_p, 1, 1, 1, \ldots). \)

To construct number fields extensions with a given Steinitz class we will use the following results.

Theorem 1.3. Let $G$ be an abelian group. Every surjective homomorphism $\varphi : C_k \to G$ whose kernel contains a congruence subgroup $C_k^m$ is the norm residue symbol of a unique extension $K/k$ with Galois group isomorphic to $G$ and $\varphi([U_p])$ is its inertia group for the prime $p$. In particular
\[ e_p(K/k) = \#\varphi([U_p]) \]
and if the primes dividing the order of $G$ do not divide $m$, then the extension is tame.

Proof. By Theorem IV.7.1 of [16] there exists a unique abelian extension $K/k$ with $N_{K/k}C_K = \ker \varphi$. By Theorem IV.6.5 in [16] the global residue symbol of $K/k$ gives an isomorphism $C_k/\ker \varphi = C_k/N_{K/k}C_K \to \text{Gal}(K/k)^{ab} = \text{Gal}(K/k)$ and thus clearly $\text{Gal}(K/k) \cong G$. Now let $K_1$ and $K_2$ be two fields corresponding to the same residue symbol, then $N_{K_1/k}C_{K_1} = N_{K_2/k}C_{K_2}$ and so, by Theorem IV.7.1 of [16], $K_1 = K_2$.

The group $\varphi([U_p])$ is the inertia group for the prime $p$ because of Theorem III.8.10 in [16] and Proposition IV.6.6 in [16]. \( \square \)
Let $L/K$ and $K/k$ be an abelian and a Galois extension of number fields respectively, such that $L/k$ is normal, $U = \text{Gal}(L/K)$ and $\Delta = \text{Gal}(K/k)$. Let $\delta \in \Delta$, $\sigma \in U$ and let $\tilde{\delta}, \tilde{\delta}' \in \text{Gal}(L/k)$ be two extensions of $\delta$ to $\text{Gal}(L/k)$. Then $\tilde{\delta}'^{-1}\tilde{\delta} \in U$ and, by the commutativity of $U$, we have that

$$\tilde{\delta}^{-1}\tilde{\delta}'\tilde{\delta}^{-1} = \tilde{\delta}'\tilde{\delta}\tilde{\delta}^{-1} = \tilde{\delta}'\tilde{\delta}\tilde{\delta}'^{-1} = \tilde{\delta}'\tilde{\delta}'^{-1}\tilde{\delta}\tilde{\delta}'^{-1} = \tilde{\delta}'\tilde{\delta}\tilde{\delta}'^{-1},$$

so that we can define $\delta_* : U \to U$ by $\delta_* = \tilde{\delta}_*$.

**Proposition 1.4.** Let $K/k$ be a finite tame extension with Galois group $\Delta$, let $U$ be a finite abelian group and let $\phi : \Delta \to \text{Aut}(U)$ be an action of $\Delta$ on $U$. Then for a $\Delta$-invariant surjective homomorphism $\varphi : C_K \to U$, whose kernel contains a congruence subgroup $C^m_K$, the extension $L/K$ given by Theorem 1.3 is Galois over $k$. The following sequence is exact

$$1 \to U \to \text{Gal}(L/k) \to \Delta \to 1$$

and the induced action of $\Delta$ on $U$ is the given one.

**Proof.** Let $\tilde{K}$ be the maximal abelian extension of $K$; by standard arguments $\tilde{K}/k$ is Galois. Since $\tilde{K} \supset L$, there is a normal closure $L_1$ of $L/k$ in $\tilde{K}$ and the extension $L_1/K$ is finite and abelian. Let $\pi : \text{Gal}(L_1/K) \to \text{Gal}(L/K)$ be the projection, then $L$ is the fixed field of $\ker \pi$. By Proposition II.3.3 in [16]

$$\pi = (L/K) \circ r_{L_1/K} = \varphi \circ r_{L_1/K}$$

and for $\delta \in \text{Gal}(L_1/k)$ we have, using also the hypothesis of $\Delta$-invariance,

$$\delta_* \circ \pi = \delta_* \circ \varphi \circ r_{L_1/K} = \varphi \circ \delta \circ r_{L_1/K} = \varphi \circ r_{L_1/K} \circ \delta_* = \pi \circ \delta_*.$$

Thus

$$\delta_* \ker \pi = \ker(\pi \circ \delta_*^{-1}) = \ker(\delta_*^{-1} \circ \pi) = \ker \pi.$$

So $\ker \pi$ is normal in $\text{Gal}(L_1/k)$. It follows that $L/k$ is Galois. The exactness of the sequence is obvious and the statement about the action of $\Delta$ on $U$ follows from Proposition II.3.3 in [16], since the given action is the only one for which the diagram on the right commutes.

For any cycle $m = \prod_p p^{n_p}$ we call $H^m_{K/k} = N_{K/K} J^m_K \cdot P^m_k$, where $J^m_k$ is the group of all ideals prime to $m$ and $P^m_k$ is the group of all principal ideals generated by an element $a \equiv 1 \pmod{p^{n_p}}$ for all $p|m$.

Let $K$ be an abelian extension of $k$, contained in the ray class field mod $m$; the cycle $m$ is called a cycle of declaration for $K/k$. 
Proposition 1.5. Let $K, K_1, K_2$ be finite abelian extensions of a number field $k$ and let $\mathfrak{m}$ be a cycle of declaration for them. Then there is an isomorphism

$$\pi_\mathfrak{m} : N_{K/k} C_K / C_k^\mathfrak{m} \to H_{K/k}^\mathfrak{m} / P_k^\mathfrak{m},$$

and

$$K_1 \subseteq K_2 \iff H_{K_1/k}^\mathfrak{m} \supseteq H_{K_2/k}^\mathfrak{m},$$

$$H_{K_1,K_2/k}^\mathfrak{m} = H_{K_1/k}^\mathfrak{m} \cap H_{K_2/k}^\mathfrak{m},$$

$$H_{K_1 \cap K_2/k}^\mathfrak{m} = H_{K_1/k}^\mathfrak{m} \cdot H_{K_2/k}^\mathfrak{m}.$$

Proof. By Proposition IV.8.1 in [16], there exists a surjective homomorphism $\pi_\mathfrak{m} : C_k \to J_k^\mathfrak{m} / P_k^\mathfrak{m}$ and by the exact commutative diagram in Theorem IV.8.2 in [16], we obtain that $\pi_\mathfrak{m}(N_{K/k} C_K) = H_{K/k}^\mathfrak{m} / P_k^\mathfrak{m}$. By Theorem IV.7.1 of [16], $N_{K/k} C_K \supseteq C_k^\mathfrak{m}$ (\(\mathfrak{m}\) is a cycle of declaration of $K/k$) and then by Proposition IV.8.1 in [16] it is the kernel of $\pi_\mathfrak{m} : N_{K/k} C_K \to H_{K/k}^\mathfrak{m} / P_k^\mathfrak{m}$.

Now the result follows by Theorem IV.7.1 of [16] and by the fact that $H_{K/k}^\mathfrak{m}$ is the counterimage of $H_{K/k}^\mathfrak{m} / P_k^\mathfrak{m}$ by the projection $J_k^\mathfrak{m} \to J_k^\mathfrak{m} / P_k^\mathfrak{m}$. \(\square\)

Proposition 1.6. Let $k^\mathfrak{m}$ be the ray class field modulo a cycle $\mathfrak{m}$ of a number field $k$. Then

$$\left( \frac{k^\mathfrak{m}/k}{.} \right) : J_k^\mathfrak{m} / P_k^\mathfrak{m} \to \text{Gal}(k^\mathfrak{m}/k)$$

is an isomorphism.

Proof. By definition of the ray class field mod $\mathfrak{m}$, $N_{k^\mathfrak{m}/k} C_{k^\mathfrak{m}} = C_k^\mathfrak{m}$ and thus by Proposition 1.5, we obtain that $H_{k^\mathfrak{m}/k}^\mathfrak{m} / P_k^\mathfrak{m}$ is the trivial group. We conclude using Theorem IV.8.2 in [16]. \(\square\)

Proposition 1.7. Let $\mathfrak{m}$ be a cycle for a number field $k$. Then each class in the ray class group modulo $\mathfrak{m}$ contains infinitely many prime ideals of absolute degree 1.

Proof. For each ray class in $J_k^\mathfrak{m} / P_k^\mathfrak{m}$ we can consider the automorphisms $\sigma \in \text{Gal}(k^\mathfrak{m}/k)$ corresponding to it by the isomorphism of Proposition 1.6. By Chebotarev Theorem (V.6.4 in [16]), there exist infinitely many prime ideals $\mathfrak{p}$ in $k$, unramified in $k^\mathfrak{m}$, of absolute degree 1 and with $\sigma = \left( \frac{k^\mathfrak{m}/k}{.} \right)$. By construction they must be in the given ray class. \(\square\)

Definition 1.8. Let $K/k$ be a finite abelian extension of number fields and let $\mathfrak{m}$ be a cycle of declaration of $K/k$. We define

$$W(k, K) = N_{K/k} J_K^\mathfrak{m} \cdot P_k / P_k = H_{K/k}^\mathfrak{m} \cdot P_k / P_k.$$

If $\zeta_\mathfrak{m}$ is an $\mathfrak{m}$-th root of unity we use the notation $W(k, \mathfrak{m}) = W(k, k(\zeta_\mathfrak{m}))$. 


Proposition 1.9. By class field theory $W(k, K)$ corresponds to the maximal unramified subextension of $K/k$, i.e.

$$W(k, K) = H^1_{K \cap k^1/k}/P_k,$$

where $k^1$ is the Hilbert class field of $k$. In particular $W(k, K)$ does not depend on the choice of the cycle of declaration $\mathfrak{m}$ of $K/k$.

Proof. By Theorem IV.8.2 of [16] and by Proposition 1.6 the kernel of

$$\left( \frac{k^1/k}{m} \right) : J^m_k/P^m_k \to \text{Gal}(k^1/k)$$

is $H^m_{K \cap k^1/k}/P_k = (P_k \cap J^m_k)/P_k$, i.e. $H^m_{K^1/k} = P_k \cap J^m_k$ and, by Proposition 1.5,

$$H^m_{K \cap k^1/k} = H^m_{K/k} \cdot H^m_{k/k} = H^m_{K/k} \cdot (P_k \cap J^m_k).$$

Let $x \in H^1_{K \cap k^1/k}/P_k$, then by Proposition 1.7 there exists a prime $p \nmid \mathfrak{m}$ in the class of $x$, i.e., recalling also the definition of $H^m_{K \cap k^1/k}$,

$$p \in H^1_{K \cap k^1/k} \cap J^m_k = H^m_{K \cap k^1/k} \cdot P_k = H^m_{K/k} \cdot (P_k \cap J^m_k) \cdot P_k = H^m_{K/k} \cdot P_k$$

and so $x \in H^m_{K/k} \cdot P_k/P_k$. Thus

$$H^1_{K \cap k^1/k}/P_k \subseteq H^m_{K/k} \cdot P_k/P_k = H^m_{K \cap k^1/k}/P_k$$

and the opposite inclusion is trivial.

Thus we have proved that

$$W(k, K) = H^m_{K/k} \cdot P_k/P_k = H^1_{K \cap k^1/k}/P_k.$$

The following results are similar to the characterizations of $W(k, K)$ given in [7].

Proposition 1.10. Let $K/k$ be a finite abelian extension of number fields. Then the following subsets of the class group of $k$ are equal to $W(k, K)$:

$$W_1 = \{ x \in J_k/P_k : x \text{ contains infinitely many primes of absolute degree 1 splitting completely in } K \}$$

$$W_2 = \{ x \in J_k/P_k : x \text{ contains a prime splitting completely in } K \}$$

$$W_3 = N_{K/k}(J_K) \cdot P_k/P_k.$$
1 Preliminary results

Proof. Let $x \in W(k, K)$ and let $m$ be a cycle of declaration of $K/k$. By definition $x = a \cdot P_k$, where $a \in H^m_{K/k}$. By Proposition 1.7 there exist infinitely many primes of absolute degree 1 in the ray class modulo $m$ containing $a$; let $p$ be one of them, which does not ramify in $K/k$. Then $p = a \cdot (b)$, where $(b) \in P^m_k$, and thus $p \in H^m_{K/k}$ and by Theorem IV.8.4 in [16] we can conclude that $p$ splits completely in $K$. Thus $x \in W_1$ and we have proved that $W(k, K) \subseteq W_1$.

Obviously $W_1 \subseteq W_2$.

Let $x \in W_2$ and $p$ be a prime in $x$ which splits completely in $K$. Then for any prime divisor $\mathfrak{p}$ of $p$ in $K$, $N_{K/k}(\mathfrak{p}) = p$. Thus $x = N_{K/k}(\mathfrak{p}) \cdot P_k$ and hence $W_2 \subseteq W_3$.

Recalling Proposition 1.9 we obtain that

$$N_{K/k}(J_K) \cdot P_k/P_k \subseteq N_{K\cap k^1/k}(J_K\cap k^1) \cdot P_k/P_k = H^1_{K\cap k^1/k}/P_k = W(k, K).$$

In the case of cyclotomic extensions we obtain some further results.

Lemma 1.11. Let $p$ be a prime in $k$ of absolute degree 1, splitting completely in $k(\zeta_m)$ and unramified over $\mathbb{Q}$. Then $N_{k/\mathbb{Q}}(p) \in P^m_{\mathbb{Q}}$, where $m = m \cdot p_\infty$.

Proof. By hypothesis $\mathcal{O}_k/p$ is the finite field with $p$ elements, where $N_{k/\mathbb{Q}}(p) = (p)$, and $(\mathcal{O}_k/p)^*$ contains a primitive $m$-th root of unity, i.e. an element of order $m$. Hence $m$ must divide $|\mathcal{O}_k/p| - 1 = p - 1$, i.e. $p \equiv 1 \pmod{m}$, which is equivalent to the assertion.

Lemma 1.12. Let $k$ be a number field, let $m$ be a cycle of declaration of $k(\zeta_m)/k$ and let $a \in J^m_k$ be such that $N_{k/\mathbb{Q}}(a) \in P^m_{\mathbb{Q}}$, then $a \in H^m_{k(\zeta_m)/k}$, i.e. the class of $a$ is in $W(k, m)$.

Proof. By Proposition II.3.3 in [16],

$$\left(\frac{k(\zeta_m)/k}{a}\right)_{\mathbb{Q}(\zeta_m)} = \left(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{N_{k/\mathbb{Q}}(a)}\right) = 1.$$
Lemma 1.13. Let $K/k$ be a tamely ramified abelian extension of number fields and let $p$ be a prime ideal in $k$ whose ramification index in $K/k$ is $e$, then $N_{k/Q}(p) \in P^m_Q$, where $m = e \cdot p_{\infty}$. In particular, by Lemma 1.12, $p \in H^m_{k(\zeta_e)/k}$ and so its class is in $W(k, e)$.

Proof. This is Lemma I.2.1 of [7].

2 Main results

Let $G$ be a finite group of order $m$, let $H = C(n_1) \times \cdots \times C(n_r)$ be an abelian group of order $n$, with generators $\tau_1, \ldots, \tau_r$ and with $n_{i+1}|n_i$. Let

$$\mu : G \rightarrow \text{Aut}(H)$$

be an action of $G$ on $H$ and let

$$0 \rightarrow H \xrightarrow{\varphi} G \xrightarrow{\psi} G \rightarrow 0$$

be an exact sequence of groups such that the induced action of $G$ on $H$ is $\mu$. We assume that the group $G$ is determined, up to isomorphism, by the above exact sequence and by the action $\mu$ (this is true e.g. if $|G|$ and $|H|$ are coprime). We are going to study $R_t(k, G)$.

We define

$$\eta_G = \begin{cases} 
1 & \text{if some (and hence every) 2-Sylow subgroup of } G \text{ is not cyclic} \\
2 & \text{if some (and hence every) 2-Sylow subgroup of } G \text{ is cyclic}
\end{cases}$$

and in a similar way we define $\eta_H$ and $\eta_G$. We will always use the letter $l$ only for prime numbers, even if not explicitly indicated.

We say that $(K, k_1, k)$ is of type $\mu$ if $k_1/k$, $K/k_1$ and $K/k$ are Galois extensions with Galois groups isomorphic to $G$, $H$ and $G$ respectively and such that the action of $\text{Gal}(k_1/k) \cong G$ on $\text{Gal}(K/k_1) \cong H$ is given by $\mu$. For any $G$-extension $k_1$ of $k$ we define $R_t(k_1, k, \mu)$ as the set of those ideal classes of $k_1$ which are Steinitz classes of a tamely ramified extension $K/k_1$ for which $(K, k_1, k)$ is of type $\mu$.

2.1 Some definitions and simple properties

For any $\tau \in H$ we define

$$\tilde{\mu}_{k, \mu, \tau} : G \times \text{Gal}(k(\zeta_{o(\tau)})/k) \rightarrow \text{Aut}(H)$$
by $\bar{\mu}_{k,\mu,\tau}(g_1, g_2) = \mu(g_1)$ for any $(g_1, g_2) \in \mathcal{G} \times \text{Gal}(k(\zeta_{o(\tau)})/k)$ and

$$\bar{\nu}_{k,\mu,\tau} : \mathcal{G} \times \text{Gal}(k(\zeta_{o(\tau)})/k) \to (\mathbb{Z}/o(\tau)\mathbb{Z})^*$$

by $\bar{\nu}_{k,\mu,\tau}(g_1, g_2) = \nu_{k,\tau}(g_2)$ where $g_2(\zeta_{o(\tau)}) = \zeta_{o(\tau)}^{\nu_{k,\tau}(g_2)}$ for any $(g_1, g_2) \in \mathcal{G} \times \text{Gal}(k(\zeta_{o(\tau)})/k)$. Let

$$\bar{\mathcal{G}}_{k,\mu,\tau} = \{g \in \mathcal{G} \times \text{Gal}(k(\zeta_{o(\tau)})/k) : \bar{\mu}_{k,\mu,\tau}(g)(\tau) = \tau^{\bar{\nu}_{k,\mu,\tau}(g)}\}$$

$$= \{(g_1, g_2) \in \mathcal{G} \times \text{Gal}(k(\zeta_{o(\tau)})/k) : \mu(g_1)(\tau) = \tau^{\nu_{k,\tau}(g_2)}\}.$$

We define

$$G_{k,\mu,\tau} = \{g \in \text{Gal}(k(\zeta_{o(\tau)})/k) : \exists g_1 \in \mathcal{G}, (g_1, g) \in \bar{\mathcal{G}}_{k,\mu,\tau}\}$$

and $E_{k,\mu,\tau}$ as the fixed field of $G_{k,\mu,\tau}$ in $k(\zeta_{o(\tau)})$.

**Lemma 2.1.** For any $\tau \in H$, $G_{k,\mu,\tau}$ is a subgroup of $\text{Gal}(k(\zeta_{o(\tau)})/k)$.

**Proof.** If $(g_1, g_2), (\tilde{g}_1, \tilde{g}_2) \in \bar{\mathcal{G}}_{k,\mu,\tau}$, then

$$\tau^{\bar{\nu}_{k,\mu,\tau}((g_1\tilde{g}_1, g_2\tilde{g}_2))} = \tau^\nu_{k,\tau}(g_2)\nu_{k,\tau}(\tilde{g}_2) = \mu(g_1)(\tau^{\nu_{k,\tau}(\tilde{g}_2)}) = \mu(g_1)(\mu(\tilde{g}_1)(\tau)) = \bar{\mu}_{k,\mu,\tau}((g_1\tilde{g}_1, g_2\tilde{g}_2))(\tau)$$

and

$$\tau^{\bar{\nu}_{k,\mu,\tau}((g_1^{-1}, g_2^{-1}))} = \tau^{\nu_{k,\tau}(g_2^{-1})} = \mu(g_1)^{-1}(\mu(g_1)(\tau^{\nu_{k,\tau}(g_2^{-1})})) = \bar{\mu}_{k,\mu,\tau}((g_1^{-1}, g_2^{-1}))(\tau).$$

Hence $(g_1\tilde{g}_1, g_2\tilde{g}_2), (g_1^{-1}, g_2^{-1}) \in \bar{\mathcal{G}}_{k,\mu,\tau}$ and the set $G_{k,\mu,\tau}$ is a subgroup of $\text{Gal}(k(\zeta_{o(\tau)})/k)$. \hfill $\square$

Given a $\mathcal{G}$-extension $k_1$ of $k$, there is an injection of $\text{Gal}(k_1(\zeta_{o(\tau)})/k)$ into $\mathcal{G} \times \text{Gal}(k(\zeta_{o(\tau)})/k)$ (defined in the obvious way). We will always identify $\text{Gal}(k_1(\zeta_{o(\tau)})/k)$ with its image in $\mathcal{G} \times \text{Gal}(k(\zeta_{o(\tau)})/k)$. So we may consider the subgroup

$$\bar{\mathcal{G}}_{k_1/k,\mu,\tau} = \bar{\mathcal{G}}_{k,\mu,\tau} \cap \text{Gal}(k_1(\zeta_{o(\tau)})/k)$$

of $\bar{\mathcal{G}}_{k,\mu,\tau}$. Let $Z_{k_1/k,\mu,\tau}$ be its fixed field in $k_1(\zeta_{o(\tau)})$.

If $k_1 \cap k(\zeta_{o(\tau)}) = k$ then $\text{Gal}(k_1(\zeta_{o(\tau)})/k) \cong \mathcal{G} \times \text{Gal}(k(\zeta_{o(\tau)})/k)$ and hence

$$\bar{\mathcal{G}}_{k_1/k,\mu,\tau} = \bar{\mathcal{G}}_{k,\mu,\tau}.$$

**Lemma 2.2.** For any $\tau \in H$, $k_1Z_{k_1/k,\mu,\tau} = k_1(\zeta_{o(\tau)})$. 

10
2.1 Some definitions and simple properties

Proof. Let \( g \in \text{Gal}(k_1(\zeta_o(\tau))/k_1) \cap \tilde{G}_{k_1/k,\mu,\tau} \), then \( g|_{k_1} = 1 \), i.e. \( \tilde{\mu}_{k,\mu,\tau}(g)(\tau) = \tau \), and \( \tilde{\tau}_{\mu,\mu,\tau}(g) = \tilde{\mu}_{k,\mu,\tau}(g)(\tau) \). Thus \( g(\zeta_o(\tau)) = \zeta_o(\tau) \) and we conclude that \( g = 1 \). We have proved that

\[
\text{Gal}(k_1(\zeta_o(\tau))/k_1) \cap \tilde{G}_{k_1/k,\mu,\tau} = 1
\]

i.e. that

\[
k_1Z_{k_1/k,\mu,\tau} = k_1(\zeta_o(\tau)).
\]

\[\square\]

Lemma 2.3. Let \( \tau \in H \), then

\[
E_{k,\mu,\tau} \subseteq Z_{k_1/k,\mu,\tau} \cap k(\zeta_o(\tau))
\]

and we have an equality if \( k_1 \cap k(\zeta_o(\tau)) = k \).

Proof. We observe that

\[
G_{k,\mu,\tau} \supseteq \left\{ g_2 \in \text{Gal}(k(\zeta_o(\tau))/k) : \exists g_1 \in G, (g_1, g_2) \in \tilde{G}_{k_1/k,\mu,\tau} \right\}
\]

\[
= \text{res}_{k(\zeta_o(\tau))}^{k_1(\zeta_o(\tau))}(\tilde{G}_{k_1/k,\mu,\tau})
\]

\[
= \text{res}_{k(\zeta_o(\tau))}^{k_1(\zeta_o(\tau))}(\tilde{G}_{k_1/k,\mu,\tau})\text{res}_{k(\zeta_o(\tau))}^{k_1(\zeta_o(\tau))}(\text{Gal}(k_1(\zeta_o(\tau))/k(\zeta_o(\tau))))
\]

\[
= \text{res}_{k(\zeta_o(\tau))}^{k_1(\zeta_o(\tau))}(\text{Gal}(k_1(\zeta_o(\tau))/Z_{k_1/k,\mu,\tau} \cap k(\zeta_o(\tau))))
\]

\[
= \text{Gal}(k(\zeta_o(\tau))/Z_{k_1/k,\mu,\tau} \cap k(\zeta_o(\tau)))
\]

i.e. that

\[
E_{k,\mu,\tau} \subseteq Z_{k_1/k,\mu,\tau} \cap k(\zeta_o(\tau)).
\]

If \( k_1 \cap k(\zeta_o(\tau)) = k \) then \( \tilde{G}_{k_1/k,\mu,\tau} = \tilde{G}_{k,\mu,\tau} \) and we have equalities. \[\square\]

Lemma 2.4. Let \( \tau \in H \), then

\[
W(k, Z_{k_1/k,\mu,\tau}) \subseteq W(k, E_{k,\mu,\tau}).
\]

If \( k_1 \cap k(\zeta_o(\tau)) = k \) and every subextension of \( k_1/k \) is ramified then

\[
W(k, Z_{k_1/k,\mu,\tau}) = W(k, E_{k,\mu,\tau}).
\]

Proof. By Lemma 2.3 it is obvious that

\[
W(k, Z_{k_1/k,\mu,\tau}) \subseteq W(k, E_{k,\mu,\tau}).
\]
Now we assume that $k_1/k$ has no unramified subextensions and we prove that
\[ k^1 \cap k_1(\zeta_{o(\tau)}) \subseteq k(\zeta_{o(\tau)}), \]
where $k^1$ is the ray class field modulo 1, i.e. the Hilbert class field. If that is not true, then $k(\zeta_{o(\tau)}) \nsubseteq (k^1 \cap k_1(\zeta_{o(\tau)})) \cdot k(\zeta_{o(\tau)}) \subseteq k_1(\zeta_{o(\tau)})$ and the extension $(k^1 \cap k_1(\zeta_{o(\tau)})) \cdot k(\zeta_{o(\tau)})/k(\zeta_{o(\tau)})$ is ramified at a prime ramified in $k_1/k$. This prime must ramify also in $k^1 \cap k_1(\zeta_{o(\tau)})/k$, which is impossible. Thus if $k_1 \cap k(\zeta_{o(\tau)}) = k$ and $k_1/k$ has no unramified subextensions then, recalling also Lemma 2.3

\[ k^1 \cap E_{k,\mu,\tau} = k^1 \cap Z_{k_1/k,\mu,\tau} \cap k(\zeta_{o(\tau)}) = k^1 \cap Z_{k_1/k,\mu,\tau} \cap k_1(\zeta_{o(\tau)}) = k^1 \cap Z_{k_1/k,\mu,\tau} \]
and by Proposition 1.9 we conclude that $W(k, E_{k,\mu,\tau}) = W(k, Z_{k_1/k,\mu,\tau})$. □

### 2.2 Some realizable classes for nonabelian groups

First of all we need a more general version of the Multiplication Lemma on page 22 in [7] by Lawrence P. Endo.

**Lemma 2.5.** Let $(K_1, k_1, k)$ and $(K_2, k_1, k)$ be extensions of type $\mu$, such that $(d(K_1/k_1), d(K_2/k_1)) = 1$ and $K_1/k_1$ and $K_2/k_1$ have no non-trivial unramified subextensions. Then there exists an extension $(K, k_1, k)$ of type $\mu$, such that $K \subseteq K_1 K_2$ and for which

\[ \text{st}(K/k_1) = \text{st}(K_1/k_1) \text{st}(K_2/k_1). \]

**Proof.** The hypotheses of the lemma imply that $K_1$ and $K_2$ are linearly disjoint over $k_1$. Let us fix isomorphisms such that the action of $\mathcal{G} \cong \text{Gal}(k_1/k)$ on $H \cong \text{Gal}(K_i/k_1)$ given by conjugation coincides with $\mu$. Let us embed $H$ into $\text{Gal}(K_1 K_2/k_1)$ by means of the corresponding diagonal map

\[ \text{diag} : H \to \text{Gal}(K_1/k_1) \times \text{Gal}(K_2/k_1) \cong \text{Gal}(K_1 K_2/k_1). \]

Let $K$ be the fixed field of $\text{diag}(H)$. Then, by Endo’s Multiplication Lemma (page 22 in [7]), we know that $\text{Gal}(K/k_1) \cong H$ and that

\[ \text{st}(K/k_1) = \text{st}(K_1/k_1) \text{st}(K_2/k_1). \]

The action of $\mathcal{G} \cong \text{Gal}(k_1/k)$ on

\[ \text{Gal}(K_1 K_2/k_1) \cong \text{Gal}(K_1/k_1) \times \text{Gal}(K_2/k_1) \]

is given by

\[ \tilde{\mu}(g)((h_1, h_2)) = (\mu(g)(h_1), \mu(g)(h_2)). \]
It follows that the action of $\mathcal{G} \cong \text{Gal}(k_1/k)$ on
\[
\text{Gal}(K/k_1) = \text{Gal}(K_1 K_2/k_1) / \text{diag}(H) \cong H
\]
(where the last isomorphism is given by the projection on the first component) coincides with the action $\mu$. Hence $(K, k_1, k)$ is of type $\mu$. $\Box$

For any integer $n \in \mathbb{N}$ and any prime $l$, we denote by $n(l)$ the power of $l$ such that $n(l)|n$ and $l \nmid n/n(l)$. For any $\tau \in H$ and for any prime $l$ dividing the order $o(\tau)$ of $\tau$ we define the element
\[
\tau(l) = \tau^{o(\tau)\text{mod}l}
\]
in the $l$-Sylow subgroup $H(l)$ of $H$. From now on we will assume that $H$ is of odd order.

We recall some definitions and a classical result.

**Definition 2.6.** Let $R$ be a commutative ring, $G$ a finite group and $H$ a subgroup of $G$. The operation of restriction of scalars from $R[G]$ to $R[H]$ assigns to each left $R[G]$-module $M$ a left $R[H]$-module $\text{res}_H^G(M)$, whose underlying abelian group is still $M$ and such that for $h \in H$ and $m \in M$, $hm$ is obtained considering $h$ as an element of $G$.

**Definition 2.7.** Let $R$ be a commutative ring, $G$ a finite group and $H$ a subgroup of $G$. The operation of induction from $R[H]$-modules to $R[G]$-modules assigns to each left $R[H]$-module $L$ a left $R[G]$-module $\text{ind}_H^G(L)$, given by
\[
\text{ind}_H^G(L) = R[G] \otimes_R R[H] L.
\]

**Theorem 2.8** (Frobenius reciprocity). Let $H$ be a subgroup of a group $G$ and let $L$ be a left $R[H]$-module and $M$ a left $R[G]$-module. Then there exists an isomorphism of $R$-modules
\[
\tau : \text{Hom}_{R[H]}(L, \text{res}_H^G(M)) \to \text{Hom}_{R[G]}(\text{ind}_H^G(L), M).
\]
This isomorphism is such that
\[
(\tau f)(g \otimes l) = g \cdot f(l)
\]

**Proof.** This is Theorem 10.8 in [6]. The explicit description of $\tau$ may be deduced from the proof. $\Box$
We will only use the above result with \( R = \mathbb{Z} \).

Let \( k_1/k \) be an extension of number fields with Galois group \( G \). Let \( \mathfrak{p}_1, \ldots, \mathfrak{p}_t \) be prime ideals in \( \mathcal{O}_{k_1} \), unramified over \( p_1, \ldots, p_t \in \mathbb{N} \), so that the classes \( x_i \) of the \( \mathfrak{p}_i \) are generators of \( \text{Cl}(k_1) \) (they exist because of Proposition 1.7) and let \( \mathfrak{p}_i^{h_i} = (\alpha_i) \), where \( h_i \) is the order of \( x_i \).

We define the homomorphism (the so-called content map)

\[
\pi : I_k \to J_k, \quad \alpha \mapsto \prod_{p \mid \infty} p^{v_p(\alpha_p)}.
\]

Let \( \pi_{\mathfrak{p}_i} \) be a prime element in \( (k_1)_{\mathfrak{p}_i} \) and \( y_i = [\pi_{\mathfrak{p}_i}] \in I_{k_1} \), then \( \pi(y_i) = \mathfrak{p}_i \) and

\[
a_i = \frac{1}{\alpha_i} y_i^{h_i} \in \prod_{\mathfrak{p}} U_{\mathfrak{p}}
\]

is congruent to \( y_i^{h_i} \mod k_1^* \).

For any \( \delta \in G \) let \( b_{\delta,i} \in \prod_{\mathfrak{p}} U_{\mathfrak{p}} \) and \( \lambda_{\delta,i,j} \in \mathbb{Z} \) (they exist thanks to the exactness of the sequence \( 1 \to \prod_{\mathfrak{p}} U_{\mathfrak{p}} / U_{k_1} \to C_{k_1} \to \text{Cl}(k_1) \to 1 \)) be such that

\[
\delta(y_i) = b_{\delta,i} \prod_{j=1}^t y_j^{\lambda_{\delta,i,j}}.
\]

Let \( \{u_1, \ldots, u_T\} \) be the union of a system of generators of the abelian group \( U_{k_1} \) with \( \{a_1, \ldots, a_t\} \) and \( \bigcup_{\delta \in G} \{b_{\delta,1}, \ldots, b_{\delta,t}\} \).

Let \( \iota \) be the map from the class group of \( k \) to the class group of \( k_1 \) induced by the map which pushes up ideals of \( k \) to ideals of \( k_1 \).

**Lemma 2.9.** A group homomorphism \( \varphi_0 : (\prod_p U_p)/U_k \to G \) can be extended to \( \varphi : C_k \to G \) if and only if for \( j = 1, \ldots, t \), \( \varphi_0(a_j) = g_j^{h_j} \) with \( g_j \in G \). We can request also that \( \varphi(y_j) = g_j \).

**Proof.** (\( \Rightarrow \)) We have

\[
\varphi_0(a_j) = \varphi(y_j^{h_j}) = \varphi(y_j)^{h_j} \in G^{h_j}.
\]

(\( \Leftarrow \)) Let us define

\[
B_k = \left( \left( \prod_p U_p \right) / U_k \times \langle e_1, \ldots, e_t \rangle \right) / \{ e_j^{h_j} / a_j \mid j = 1, \ldots, t \}
\]

where the second component in the direct product is a free abelian group.

We may extend the inclusion \( i : (\prod_p U_p)/U_k \hookrightarrow C_k \) to \( B_k \) by \( e_j \mapsto y_j \) and
thus also the map \( \pi \circ i : (\prod_p U_p)/U_k \to \text{Cl}(k) \) by \( e_j \mapsto x_j \). We obtain the following commutative diagram

\[
\begin{array}{cccccc}
1 & \longrightarrow & (\prod_p U_p)/U_k & \longrightarrow & B_k & \longrightarrow & \text{Cl}(k) & \longrightarrow & 1 \\
\downarrow\text{id} & & \downarrow\text{id} & & \downarrow\text{id} & & \downarrow\text{id} & & \downarrow\text{id} \\
1 & \longrightarrow & (\prod_p U_p)/U_k & \longrightarrow & C_k & \longrightarrow & \text{Cl}(k) & \longrightarrow & 1
\end{array}
\]

where the horizontal sequences are exact. It follows that \( B_k \cong C_k \). Now we define \( \tilde{\varphi} : B_k \to G \) by \( \tilde{\varphi}(a) = \varphi_0(a) \) for \( a \in \prod U_p/U_k \) and \( \tilde{\varphi}(e_j) = g_j \). This is a good definition since

\[
\tilde{\varphi}\left(\frac{e_j^{h_j}}{a_j}\right) = \frac{g_j^{h_j}}{\varphi_0(a_j)} = 1.
\]

By the isomorphism between \( B_k \) and \( C_k \) we obtain the requested \( \varphi : C_k \to G \). Since the restriction of the isomorphism \( B_k \cong C_k \) to \( (\prod_p U_p)/U_k \) is the identity map, it is clear that \( \varphi \) is an extension of \( \varphi_0 \).

The following lemma is a crucial technical result.

**Lemma 2.10.** Let \( k_1 \) be a tame \( G \)-extension of \( k \) and let \( x \in W(k, k_1(\zeta_{n_1})) \). Then there exist tame extensions of \( k_1 \) of type \( \mu \), whose Steinitz classes (over \( k_1 \)) are \( \iota(x)^\alpha \), where:

\[
\alpha = \sum_{j=1}^r \frac{n_j - 1}{2} \frac{n}{n_j} + \frac{n_1 - 1}{2} \frac{n}{n_1}.
\]

In particular there exist tame extensions of \( k_1 \) of type \( \mu \) with trivial Steinitz class.

We can choose these extensions so that they are unramified at all infinite primes, that the discriminants are prime to a given ideal \( I \) of \( \mathcal{O}_k \) and that all their proper subextensions are ramified.

**Proof.** By Proposition \([1, 10]\) \( x \) contains infinitely many primes \( q \) of absolute degree 1 splitting completely in \( k_1(\zeta_{n_1}) \). Let \( q \) be any such prime and let \( q \mathcal{O}_{k_1} = \prod_{\delta \in \mathcal{E}} \delta(\Omega) \) be its decomposition in \( k_1 \), let \( g_\Omega \) be a generator of \( k_1^* = U_\Omega/U_1^{1} \). Now \( \delta \) gives an isomorphism from \( k_1^* \) to \( k_1^* \delta(\Omega) \) and so we may define a generator

\[
g_{\delta(\Omega)} = \delta(g_\Omega)
\]

15
of $\kappa^*_\delta(Q)$ for any $\delta \in \mathcal{G}$. We also define generators $g_{\mathfrak{p}}$ of $\kappa^*_\mathfrak{p}$ for all the other prime ideals and for any $a \in \prod_{\mathfrak{p}} U_{\mathfrak{p}}$ we define $\tilde{h}_{\mathfrak{p},a} \in \mathbb{Z}$, through $g_{\mathfrak{p},a} \equiv a_{\mathfrak{p}} \pmod{\mathfrak{p}}$.

For any prime $\delta(Q)$, dividing a prime $q$ of absolute degree 1 splitting completely in $k_1(\zeta_{n_1})$, let $h_{\delta(Q),a}$ be the class of $\tilde{h}_{\delta(Q),a}$ modulo $n_1$ (since $\delta(Q)$ is of absolute degree 1, it follows by Lemma 1.11 that the order of $g_{\delta(Q)}$ is a multiple of $n_1$, i.e. that $h_{\delta(Q),a}$ is well defined). The set of all the possible $mT$-tuples

$$(h_{\delta(Q),a_j})_{\delta \in \mathcal{G}; j=1,...,T}$$

is finite. Then it follows from the pigeonhole principle that there are infinitely many $q$ corresponding to the same $mT$-tuple.

Let $q_1, \ldots, q_{r+1}$ be $r+1$ such prime ideals and $\Omega_1, \ldots, \Omega_{r+1}$ primes of $k_1$ dividing them. We can assume that they are distinct and that they are prime to a fixed ideal $I$ and to $\mathfrak{P}_1, \ldots, \mathfrak{P}_t$.

Now let us define $\varphi_i : \kappa^*_\delta \to H$, posing

$$\varphi_i(g_{\Omega_i}) = \tau_i,$$

for $i = 1, \ldots, r$, and $\varphi_{r+1} : \kappa^*_{\Omega_{r+1}} \to H$, posing

$$\varphi_{r+1}(g_{\Omega_{r+1}}) = (\tau_1 \ldots \tau_r)^{-1}.$$ 

Then we extend $\varphi_i$ to

$$\tilde{\varphi}_i : \text{ind}_{(1)}^{\mathcal{G}_{1}} \kappa^*_{\Omega_i} \cong \prod_{\delta \in \mathcal{G}} \kappa^*_{\delta(\Omega_i)} \to H$$

using Theorem 2.8.

Now let us define $\varphi_0 : \prod_{\Omega} \kappa^*_{\Omega} \to H$, posing

$$\begin{cases} 
\varphi_0|_{\kappa^*_{\delta(\Omega_i)}} = \tilde{\varphi}_i & \text{for } i = 1, \ldots, r + 1 \text{ and } \delta \in \mathcal{G} \\
\varphi_0|_{\kappa^*_{\mathfrak{p}}} = 1 & \text{for } \mathfrak{p} \nmid q_1, \ldots, q_{r+1}.
\end{cases}$$

By construction $\varphi_0$ is $\mathcal{G}$-invariant and hence, for any $\delta \in \mathcal{G}$,

$$\varphi_0 \left( \prod_{i=1}^{r+1} g_{\delta(\Omega_i)} \right) = \varphi_0 \left( \delta \left( \prod_{i=1}^{r+1} g_{\Omega_i} \right) \right) = \delta_* \varphi_0 \left( \prod_{i=1}^{r+1} g_{\Omega_i} \right) = \delta_* (1) = 1.$$ 

It follows that $\varphi_0(a_j) = 1$ for $j = 1, \ldots, T$ and thus in particular $\varphi_0$ is trivial on $U_{k_1}$, on the $a_1, \ldots, a_t$ and on $b_{\delta,1}, \ldots, b_{\delta,t}$ for any $\delta \in \mathcal{G}$. This means that $\varphi_0$ is well defined on $(\prod_{\mathfrak{p}} U_{\mathfrak{P}})/U_{k_1}$ and that $\varphi_0(a_j) = 1$ and $\varphi_0(b_{\delta,j}) = 1$. 

16
2.2 Some realizable classes for nonabelian groups

Then it follows from Lemma 2.9 that $\varphi_0$ can be extended to $\varphi : C_{k_1} \to G$; the kernel of $\varphi_0$ contains $I_{k_1}^m$, where $m = \prod_{j=1}^{r+1} Q_j$, and so $C_{k_1}^m \subseteq \ker \varphi$. We can also assume that $\varphi(y_j) = 1$, for all $j$. It follows from Theorem 1.3 that there is an $H$-Galois extension of $k_1$, ramifying only in the primes above $q_1, \ldots, q_{r+1}$, with indices $n_j$ for $j \in \{1, \ldots, r\}$ and $n_1$ for $j = r + 1$.

Further the action of an element of $G$ on one of the $y_j$ gives a combination of some $b_{i,\delta}$ and $y_j$, on which $\varphi$ is trivial. Recalling that $\varphi_0$ is $G$-invariant, it follows that also the homomorphism $\varphi$ is $G$-invariant and so by Proposition 1.4 and by the fact that $G$ is identified by the exact sequence $1 \to H \to G \to G \to 1$ and by the action $\mu$ (Theorem 7.41 in [17]) we obtain an extension of type $\mu$. Its discriminant is

$$d = \left( \prod_{i=1}^{r} q_i^{(n_i-1)\frac{n}{o(\tau)}} \right)^{(n_1-1)\frac{n}{o(\tau)}} \mathcal{O}_{k_1}$$

Since the order of $H$ is odd, by Theorem 1.1 the Steinitz class is $\iota(x)^{\alpha}$. It is immediate to verify the additional conditions.

Lemma 2.11. Let $k_1$ be a $G$-extension of $k$, let $l$ be a prime dividing $n$, $\tau \in H(l) \setminus \{1\}$ and let $x$ be any class in $W(k, Z_{k_1/k, \mu, \tau})$. Then there exist extensions of $k_1$ of type $\mu$, whose Steinitz classes (over $k_1$) are $\iota(x)^{\alpha_{l,j}}$, where:

(a) $\alpha_{l,1} = (l - 1)\frac{n}{o(\tau)}$;

(b) $\alpha_{l,2} = (o(\tau) - 1)\frac{n}{o(\tau)}$;

(c) $\alpha_{l,3} = \frac{3(l - 1)}{2}$.

We can choose these extensions so that they satisfy the additional conditions of Lemma 2.10.

Proof. By Lemma 2.10 there exists an extension $K$ of $k_1$ of type $\mu$ with trivial Steinitz class and such that $K/k_1$ is unramified at all infinite primes, that its discriminant is prime to a given ideal $I$ of $\mathcal{O}_k$ and that all its subextensions are ramified.

By Proposition 1.10, $x$ contains infinitely many primes $q$ of absolute degree 1 splitting completely in $Z_{k_1/k, \mu, \tau}$. Those primes obviously split completely also in the extension $k_1(\zeta_{o(\tau)}) = k_1Z_{k_1/k, \mu, \tau}$ (the equality holds by
Lemma 2.2) of \( k_1 \). We can assume that they do not ramify in \( k_1/k \), that they are prime to \( l \) and, by the pigeonhole principle, that there are prime ideals \( \mathfrak{Q} \) in \( k_1 \), dividing the \( \mathfrak{q} \), and with a fixed decomposition group \( D \), of order \( f \), in \( k_1/k \); let \( \rho = m/f \). We choose a set \( \Delta \) of representatives of the cosets \( \delta D \), with \( \delta \in \mathcal{G} \). Then \( q \mathcal{O}_{k_1} = \prod_{\delta \in \Delta} \delta(\mathfrak{Q}) \) are the decompositions of the primes \( q \) in \( k_1 \).

Let \( g_{\mathfrak{Q}} \) be a generator of \( \kappa_{\mathfrak{Q}}^* = U_{\mathfrak{Q}} / U_{\mathfrak{Q}}^1 \). Now \( \delta \in \Delta \) gives an isomorphism from \( \kappa_{\mathfrak{Q}}^* \) to \( \kappa_{\delta(\mathfrak{Q})}^* \) and so we may define a generator

\[
g_{\delta(\mathfrak{Q})} = \delta(g_{\mathfrak{Q}})
\]

of \( \kappa_{\delta(\mathfrak{Q})}^* \) for any \( \delta \in \Delta \). We know that any \( \delta \in D \) defines an automorphism of \( \kappa_{\mathfrak{Q}}^* \), of the form

\[
\delta(g_{\mathfrak{Q}}) = g_{\mathfrak{Q}}^{\lambda_{\mathfrak{Q},\delta}},
\]

where \( \lambda_{\mathfrak{Q},\delta} \) is an integer. We can extend \( \delta \in D \) to a \( \tilde{\delta} \in \text{Gal}(k_1(\zeta_0(\tau))/k_1) \) in a way such that \( \tilde{\delta}(\tilde{\mathfrak{Q}}) = \tilde{\mathfrak{Q}} \), where \( \tilde{\mathfrak{Q}} \) is a prime in \( k_1(\zeta_0(\tau)) \) above \( \mathfrak{Q} \) (it is enough to extend \( \delta \) in some way and then to multiply it by an appropriate element of \( \text{Gal}(k_1(\zeta_0(\tau))/k_1) \)). This element acts as a \( \lambda_{\mathfrak{Q},\delta} \)-th power on \( \kappa_{\mathfrak{Q}}^* = \kappa_{\mathfrak{Q}_1}^* \) (the equality holds because \( \mathfrak{Q} \) splits completely in \( k_1(\zeta_0(\tau)) \)). Thus, for \( \delta \in D \),

\[
\zeta_{\mathfrak{Q}_1}^{\tilde{\mu}_{k,\mu,\tau}(\tilde{\delta})} = \tilde{\delta}(\zeta_0(\tau)) \equiv \zeta_{\mathfrak{Q}_1}^{\lambda_{\mathfrak{Q},\delta}} \pmod{\tilde{\mathfrak{Q}}}
\]

and, recalling that the powers of \( \zeta_0(\tau) \) are distinct modulo \( \tilde{\mathfrak{Q}} \) (since \( \tilde{\mathfrak{Q}} \) is prime to \( l \) and thus to \( o(\tau) \)),

\[
\lambda_{\mathfrak{Q},\delta} \equiv \tilde{\nu}_{k,\mu,\tau}(\tilde{\delta}) \pmod{o(\tau)}.
\]

Since the prime \( \mathfrak{q} \) splits completely in \( Z_{k_1/k,\mu,\tau} \) and \( \tilde{\delta}(\tilde{\mathfrak{Q}}) = \tilde{\mathfrak{Q}} \), we obtain that \( \tilde{\delta} \in \text{Gal}(k_1(\zeta_0(\tau))/Z_{k_1/k,\mu,\tau}) \) and hence

\[
\mu(\delta)(\tau) = \tilde{\mu}_{k,\mu,\tau}(\tilde{\delta})(\tau) = \tau^{\tilde{\mu}_{k,\mu,\tau}(\tilde{\delta})} = \tau^{\lambda_{\mathfrak{Q},\delta}}.
\]

Defining the \( h_{\delta(\mathfrak{Q}),u_j} \) as in the previous lemma, the set of all the possible \( \rho T \)-tuples

\[
(h_{\delta(\mathfrak{Q}),u_j})_{\delta \in \Delta; \ j = 1, \ldots, T}
\]

is finite. Then it follows from the pigeonhole principle that there are infinitely many \( \mathfrak{q} \) corresponding to the same \( \rho T \)-tuple.

Let \( q_1, q_2, q_3 \) be 3 such prime ideals and let \( \mathfrak{Q}_1, \mathfrak{Q}_2, \mathfrak{Q}_3 \) be primes of \( k_1 \) dividing them. We can assume that they are distinct, that they are prime to a fixed ideal \( I \), to \( \mathfrak{P}_1, \ldots, \mathfrak{P}_t \) and to \( d(K/k_1) \) and that they satisfy all the above requests.
2.2 Some realizable classes for nonabelian groups

(a) Now let us define \( \varphi_i : \kappa_{\Delta_i}^* \rightarrow H \), for \( i = 1, 2 \), posing

\[
\varphi_1(g_{\Omega_1}) = \tau^\frac{\alpha_i}{l}
\]

and

\[
\varphi_2(g_{\Omega_2}) = \tau^{-\frac{\alpha_i}{l}}.
\]

For \( \delta \in D \), we have

\[
\mu(\delta)(\varphi_1(g_{\Omega_1})) = \mu(\delta) \left( \tau^{\frac{\alpha_i}{l}} \right) = \tau^{\lambda_{\Delta_i, \delta} \cdot \frac{\alpha_i}{l}} = \varphi_1(g_{\Omega_1}^\lambda_{\Delta_i, \delta}) = \varphi_1(\delta(g_{\Omega_1})).
\]

Thus \( \varphi_1 \) is a \( D \)-invariant homomorphism and the same is true for \( \varphi_2 \).

Then, for \( i = 1, 2 \), we extend \( \varphi_i \) to

\[
\tilde{\varphi}_i : \text{ind}_D^G \kappa_{\Delta_i}^* \cong \prod_{\delta \in \Delta} \kappa_{\delta(\Delta_i)}^* \rightarrow H
\]

using Theorem 2.8 and we define \( \varphi_0 : \prod_{P} \kappa_{\mathfrak{P}}^* \rightarrow H \), posing

\[
\begin{cases}
\varphi_0|_{\kappa_{\delta(\Delta_i)}^*} = \tilde{\varphi}_i & \text{for } i = 1, 2 \text{ and } \delta \in \Delta \\
\varphi_0|_{\kappa_{\mathfrak{P}}^*} = 1 & \text{for } \mathfrak{P} \nmid q_1, q_2.
\end{cases}
\]

As in Lemma 2.10 we can extend \( \varphi_0 \) to a \( G \)-invariant surjective homomorphism \( \varphi : C_{k_1} \rightarrow H \), whose kernel contains a congruence subgroup of \( C_{k_1} \) and hence this is true also for

\[
\varphi \cdot (, K/k_1) : C_{k_1} \rightarrow H.
\]

We can conclude that there exists an extension of type \( \mu \), with discriminant

\[
d(K/k_1) \left( (q_1q_2)^{(l-1)} \mathfrak{O}_{k_1} \right)
\]

and so its Steinitz class is \( \iota(x)^{\alpha_{l,1}} \).

(b) Now let us define \( \varphi_i : \kappa_{\Omega_i}^* \rightarrow H \), for \( i = 1, 2 \), posing

\[
\varphi_1(g_{\Omega_1}) = \tau
\]

and

\[
\varphi_2(g_{\Omega_2}) = \tau^{-1}
\]

Exactly as in the first case we obtain an extension of type \( \mu \) with discriminant

\[
d(K/k_1) \left( (q_1q_2)^{(\alpha(l)-1)} \frac{n}{\alpha(l)} \mathfrak{O}_{k_1} \right)
\]

and so its Steinitz class is \( \iota(x)^{\alpha_{l,2}} \).
(c) We define $\varphi_i : \kappa_{\Omega_i}^* \to H$, for $i = 1, 2, 3$, posing

\[ \varphi_1(g_{\Omega_1}) = \tau^{\frac{o(\tau)}{l}}, \]

\[ \varphi_2(g_{\Omega_2}) = \tau^{\frac{o(\tau)}{l}}, \]

and

\[ \varphi_3(g_{\Omega_3}) = \tau^{-\frac{2o(\tau)}{l}} \]

Now we obtain an extension of type $\mu$ with discriminant

\[ d(K/k_1) \left( (q_1 q_2 q_3)^{(l-1)\frac{n}{2}} \mathcal{O}_{k_1} \right) \]

and so its Steinitz class is $\iota(x)^{a_{l,3}}$.

Lemma 2.11 is now completely proved. \hfill \Box

At this point we can prove the following proposition.

**Proposition 2.12.** Let $l$ be a prime dividing the order $n$ of $H$, which we assume to be odd, and let $\tau \in H(l)$, then

\[ \iota \left( W \left( k, Z_{k_1/k,\mu,\tau} \right) \right)^{\frac{l-1}{2} \frac{n}{o(\tau)}} \subseteq R_t(k_1, k, \mu). \]

**Proof.** Let $l$ be a prime dividing $n$, let $\tau \in H(l)$ and let $x \in W(k, Z_{k_1/k,\mu,\tau})$. It follows from Lemma 2.5 and Lemma 2.11 that $\iota(x)^{\beta_l}$ is in $R_t(k_1, k, \mu_{\tilde{H}})$, where:

\[ \beta_l = \gcd \left( \frac{(l-1)n}{l}, (o(\tau) - 1) \frac{n}{o(\tau)}, \frac{3(l-1)n}{2} \frac{n}{l} \right) \]

\[ = \gcd \left( (o(\tau) - 1) \frac{n}{o(\tau)}, \frac{l-1}{2} \frac{n}{l} \right). \]

Clearly $\beta_l$ divides $\frac{l-1}{2} \frac{n}{o(\tau)}$ and so we conclude that

\[ \iota(x)^{\frac{l-1}{2} \frac{n}{o(\tau)}} \in R_t(k_1, k, \mu_{\tilde{H}}). \]

\hfill \Box

The next proposition is the main result we want to prove in this section.
2.2 Some realizable classes for nonabelian groups

Proposition 2.13. Let \( k \) be a number field and let \( G \) be a finite group such that for any class \( x \in R_t(k, G) \) there exists a tame \( G \)-extension \( k_1 \) with Steinitz class \( x \) and such that every subextension of \( k_1/k \) is ramified at some primes which are unramified in \( k(\zeta_{n_1})/k \).

Let \( H = C(n_1) \times \cdots \times C(n_r) \) be an abelian group of odd order \( n \) and let \( \mu \) be an action of \( G \) on \( H \). We assume that the exact sequence

\[
0 \to H \xrightarrow{\varphi} G \xrightarrow{\psi} \mathbb{G} \to 0,
\]

in which the induced action of \( G \) on \( H \) is \( \mu \), determines the group \( G \), up to isomorphism. Then

\[
R_t(k, G) \supseteq R_t(k, G) \prod_{l \mid n} \prod_{\tau \in H(l)} W(k, E_{k,\mu,\tau})^{\frac{l-1}{\varphi(\tau)}}
\]

where \( E_{k,\mu,\tau} \) is the fixed field of \( G_{k,\mu,\tau} \) in \( k(\zeta_{\psi(\tau)}) \),

\[
G_{k,\mu,\tau} = \{ g \in \text{Gal}(k(\zeta_{\psi(\tau)})/k) : \exists g_1 \in G, \ \mu(g_1)(\tau) = \tau^{\nu_k,\tau}(g) \}
\]

and \( g(\zeta_{\psi(\tau)}) = \zeta_{\psi(\tau)}^{\nu_k,\tau}(g) \) for any \( g \in \text{Gal}(k(\zeta_{\psi(\tau)})/k) \).

Proof. Let \( x \in R_t(k, G) \) and let \( k_1 \) be a tame \( G \)-extension of \( k \), with Steinitz class \( x \), and such that every subextension of \( k_1/k \) is ramified at some primes which are unramified in \( k(\zeta_{n_1})/k \). Thus it follows also that \( k_1 \cap k(\zeta_{n_1}) = k \).

By Proposition 1.2, Lemma 2.4, Lemma 2.5 and Proposition 2.12 we obtain

\[
R_t(k, G) \supseteq R_t(k, G) \prod_{l \mid n} \prod_{\tau \in H(l)} W(k, E_{k,\mu,\tau})^{\frac{l-1}{\varphi(\tau)}}
\]

We can conclude since the above inclusion holds for any \( x \in R_t(k, G) \).

In this section we have only proved one inclusion concerning \( R_t(k, G) \). To prove the opposite one we will need some more restrictive hypotheses. However the following lemma is true in the most general setting.

Lemma 2.14. Let \((K, k_1, k)\) be a tame \( \mu \)-extension and let \( \mathfrak{p} \) be a prime in \( k_1 \) ramifying in \( K/k_1 \) and let \( \mathfrak{p} \) be the corresponding prime in \( k \). Then

\[
x \in W(k, Z_{k_1/k,\mu,\tau}) \subseteq W(k, E_{k,\mu,\tau}) \subseteq \bigcap_{l \mid \mathfrak{p} \mathfrak{q}} W(k, E_{k,\mu,\tau(l)})
\]

where \( x \) is the class of \( \mathfrak{p} \) and \( \tau \) generates \( ([U_\mathfrak{p}], K/k_1) \).
Proof. Let $e_P$ be the ramification index of $\mathfrak{P}$ in $K/k_1$ and let $f_p$ be the inertia degree of $p$ in $k_1/k$. By Lemma 1.13, $\mathfrak{P} \in H^1_{k_1(\zeta_{e_P})/k_1}$ and, since the extension is tame, $\mathfrak{P} \nmid e_P$, i.e. $\mathfrak{P}$ is unramified in $k_1(\zeta_{e_P})/k_1$. Hence, by Theorem IV.8.4 in [16], $\mathfrak{P}$ splits completely in $k_1(\zeta_{e_P})/k_1$. It follows that the inertia degree of $p$ in $k_1(\zeta_{e_P})/k$ is exactly the same as in $k_1/k$, i.e. $f_p$.

Let $u_P \in U_{\mathfrak{P}}$ be such that its class modulo $\mathfrak{P}$ is a generator $g^*_P$ of $\kappa^*_{\mathfrak{P}} = U_{\mathfrak{P}}/U_{\mathfrak{P}}^1$. By Theorem III.8.10 and Proposition IV.6.6 in [16], $\tau = (g_P, K/k_1)$ is an element of order $e_P$ in $H$. An element $\delta \in \text{Gal}(k_1(\zeta_{e_P})/k)$ in the decomposition group of a prime $\tilde{\mathfrak{P}}$ in $k_1(\zeta_{e_P})/k_1$, dividing $\mathfrak{P}$, induces an automorphism of $\kappa^*_{\tilde{\mathfrak{P}}} = \kappa^*_{\mathfrak{P}}(\text{the equality holds since } \mathfrak{P} \text{ splits completely in } k_1(\zeta_{e_P})/k_1)$, given by

$$\delta(g_P) = g^*_{\mathfrak{P}, \delta},$$

where $\lambda_{\mathfrak{P}, \delta}$ is an integer. Thus $\zeta_{\mathfrak{P}, \tau}^{\lambda_{\mathfrak{P}, \delta}} = \delta(\zeta_{e_P}) \equiv \zeta_{e_P}^{\lambda_{\mathfrak{P}, \delta}} \pmod{\mathfrak{P}}$ and, recalling that the powers of $\zeta_{e_P}$ are distinct modulo $\mathfrak{P}$ (since $\mathfrak{P} \nmid e_P$), we deduce that $\lambda_{\mathfrak{P}, \delta} \equiv \tilde{\nu}_{k, \mu, \tau}(\delta) \pmod{\mathfrak{P}}$. Recalling Proposition II.3.3 in [16],

$$\mu_{k, \mu, \tau}(\delta)(\tau) = \mu(\delta_{k_1})(\tau) = (\delta(g_P), K/k_1) = (g^*_{\mathfrak{P}}, K/k_1) = \tau^{\lambda_{\mathfrak{P}, \delta}} \equiv \nu_{k, \mu, \tau}(\delta).$$

Thus $\delta \in \tilde{G}_{k_1/k, \mu, \tau} = \text{Gal}(k_1(\zeta_{e_P})/Z_{k_1/k, \mu, \tau})$. Hence we conclude that $p$ has inertia degree 1 in $Z_{k_1/k, \mu, \tau}/k$ and thus it is the norm of a prime ideal in $Z_{k_1/k, \mu, \tau}$, i.e., by Proposition 1.10, its class is in $W(k, Z_{k_1/k, \mu, \tau})$.

The proof of the inclusions

$$W(k; Z_{k_1/k, \mu, \tau}) \subseteq W(k; E_{k, \mu, \tau}) \subseteq W(k; E_{k, \mu, \tau(l)})$$

is trivial, using Lemma 2.4 and the fact that $E_{k, \mu, \tau} \supseteq E_{k, \mu, \tau(l)}$. 

2.3 Realizable classes for $A'$-groups of odd order

The next definition is technical; it will be used to make an induction argument over the order of $G$ possible.

Definition 2.15. We will call a finite group $G$ good if the following properties are verified:

1. For any number field $k$, $\text{Res}_k(k, G)$ 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:
2.3 Realizable classes for $A'$-groups of odd order

(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

$$\left(p^{(e_p - 1)\frac{m}{e_p(l)}} - t_p(\alpha)\right)^{\frac{1}{2}}$$

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

$$p^{(l-1)\frac{m}{e_p(l)}}$$

is in $R_t(k, G)$ and, if $2$ divides $(l - 1)\frac{m}{e_p(l)}$, the class of

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

is in $R_u(k, G)$.

4. $G$ is such that for any number field $k$, for any class $x \in R_t(k, G)$ and any integer $n$, 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 $k(\zeta_n)/k$.

Our aim is to prove that $A'$-groups of odd order are good; but first of all at this point we need the following easy lemma.

**Lemma 2.16.** For any $e|m$ the greatest common divisor, for $l|e$, of the integers $(l - 1)\frac{m}{e(l)}$ divides $(e - 1)\frac{m}{e}$.

**Proof.** Let $I$ be the $\mathbb{Z}$-ideal generated by the integers $l - 1$, for all the primes $l|e$. Then $e \equiv 1 \pmod{I}$, since it is the product of prime factors, each one congruent to 1 modulo $I$. Hence $e - 1$ is a multiple of the greatest common divisor of the integers $l - 1$ for $l|e$.

In particular for any prime $l \nmid e$, there exists an $l_1|e$, such that the power of $l$ dividing $(l_1 - 1)\frac{m}{e(l_1)}$ divides also $(e - 1)\frac{m}{e}$.

Finally for any $l|e$ the power of $l$ dividing $(l - 1)\frac{m}{e(l)}$ divides $(e - 1)\frac{m}{e}$. □

**Lemma 2.17.** Let $G$ be a good group, let $H$ be an abelian group of odd order prime to that of $G$ and let $\mu$ be an action of $G$ on $H$. Suppose $(K, k_1, k)$ is tamely ramified and of type $\mu$. Let $e_p$ be the ramification index of a prime
$p$ in $k_1/k$ and $e_p$ be the ramification index of a prime $\mathfrak{P}$ of $k_1$ dividing $p$ in $K/k_1$. Then the class of
\[
(p - 1)^{(e_p - 1)\frac{mn}{e_p} - v_p(a_{k_1/k}^{n})})^{\frac{1}{2}},
\]
is in
\[
R_v(k, G)^n \cdot \prod_{l|n} \prod_{\tau \in H(\ell) \setminus \{1\}} W(k, E_{k, \mu, \tau})^{\frac{l-1}{2} \frac{mn}{\sigma(\ell)}}.
\]

**Proof.** Clearly
\[
(e_p - 1)^{\frac{mn}{e_p}} = (e_p - 1)^{\frac{mn}{e_p}} + (e_p - 1)^{\frac{mn}{e_p}}
\]
is divisible by
\[
gcd\left(\frac{mn}{e_p}, \frac{mn}{e_p}\right)
\]
and, since $(m, n) = 1$, i.e. also $(e_p, e_\mathfrak{P}) = 1$, this coincides with
\[
gcd\left(\frac{mn}{e_p}, \frac{mn}{e_\mathfrak{P}}\right).
\]
Thus, recalling Lemma 2.16
\[
p^{(e_p - 1)^{\frac{mn}{e_p}} - v_p(a_{k_1/k}^{n})} = p^{a_p(e_p - 1)^{\frac{mn}{e_p}} + a_p(e_p - 1)^{\frac{mn}{e_p}}} = p^{a_p(e_p - 1)^{\frac{mn}{e_p}}} \prod_{l|e_p} b_{\mathfrak{P}, l(l-1)^{\frac{mn}{e_\mathfrak{P}(l)}}}.
\]

If $G$ either has odd order or has a noncyclic 2-Sylow subgroup, i.e. $\alpha_{k_1/k} = 1$, then we conclude by the hypothesis that $G$ is good, by Lemma 2.14 and by the fact that any prime dividing $e_\mathfrak{P}$ is odd.

We now assume that $G$ is of even order with a cyclic 2-Sylow subgroup. Again using Lemma 2.16 we can find some $c_{p,l}$ such that
\[
p^{(e_p - 1)^{\frac{mn}{e_p}} - v_p(a_{k_1/k}^{n})} = p^{a_p(e_p - 1)^{\frac{mn}{e_p}} - v_p(a_{k_1/k}^{n})} \prod_{l|e_p} b_{\mathfrak{P}, l(l-1)^{\frac{mn}{e_\mathfrak{P}(l)}}}
\]
\[
= \left(p^{(e_p - 1)^{\frac{mn}{e_p}} - v_p(a_{k_1/k}^{n})}\right) \prod_{l|e_p} b_{\mathfrak{P}, l(l-1)^{\frac{mn}{e_\mathfrak{P}(l)}}}
\]
\[
= \prod_{l|e_p} c_{p,l(l-1)^{\frac{mn}{e_\mathfrak{P}(l)}}(a_p - 1)} \left(p^{(e_p - 1)^{\frac{mn}{e_p}} - v_p(a_{k_1/k}^{n})}\right) \prod_{l|e_p} b_{\mathfrak{P}, l(l-1)^{\frac{mn}{e_\mathfrak{P}(l)}}}.
\]

We know that $p^{(e_p - 1)^{\frac{mn}{e_p}} - v_p(a_{k_1/k}^{n})}$ and $p^{(e_p - 1)^{\frac{mn}{e_p}} - v_p(a_{k_1/k}^{n})}$ are squares of ideals and that any $l$ dividing $e_\mathfrak{P}$ is odd. It follows that $c_{p, 2^{mn}}(a_p - 1)$ is even,
since all the other exponents are. Recalling the hypothesis that $G$ is good, we conclude that the class of
\[
\left(p^{(e_p e_p - 1)} e_p^{-v_p(\alpha_{k_1/k})}\right)^{\frac{1}{2}}
\]
is in
\[
R_t(k, G)^n \prod_{l|n} \prod_{\tau \in H(l) \setminus \{1\}} W(k, E_{k,\mu,\tau})^{\frac{l-1}{2} \frac{m_n}{\alpha(\tau)}}.
\]

**Lemma 2.18.** Under the same hypotheses as in the preceding lemma, if $l|e_p e_p$, the class of
\[
p^{(l-1) \frac{m_n}{e_p(l)}}
\]
is in
\[
R_t(k, G)^n \prod_{\tau \in H(l) \setminus \{1\}} W(k, E_{k,\mu,\tau})^{\frac{l-1}{2} \frac{m_n}{\alpha(\tau)}}
\]
and, if 2 divides $(l-1) \frac{m_n}{e_p(l)}$, the class of
\[
p^{\frac{l-1}{2} \frac{m_n}{e_p(l)}}
\]
is in
\[
R_t(k, G)^n \prod_{\tau \in H(l) \setminus \{1\}} W(k, E_{k,\mu,\tau})^{\frac{l-1}{2} \frac{m_n}{\alpha(\tau)}}.
\]

**Proof.** If $l$ divides $e_p$ the result is an obvious consequence of the fact that $G$ is good. For $l|e_p$ we conclude by Lemma 2.14. \qed

Now we can prove the following theorem.

**Theorem 2.19.** Let $k$ be a number field and let $G$ be a good group.

Let $H = C(n_1) \times \cdots \times C(n_r)$ be an abelian group of odd order prime to that of $G$ and let $\mu$ be an action of $G$ on $H$. Then
\[
R_t(k, H \rtimes_{\mu} G) = R_t(k, G)^n \prod_{l|n} \prod_{\tau \in H(l) \setminus \{1\}} W(k, E_{k,\mu,\tau})^{\frac{l-1}{2} \frac{m_n}{\alpha(\tau)}}
\]
where $E_{k,\mu,\tau}$ is the fixed field of $G_{k,\mu,\tau}$ in $k(\zeta_{\alpha(\tau)})$,
\[
G_{k,\mu,\tau} = \{ g \in \text{Gal}(k(\zeta_{\alpha(\tau)})/k) : \exists g_1 \in G, \mu(g_1)(\tau) = \tau^{\nu_{k,\tau}(g)} \}
\]
and $g(\zeta_{\alpha(\tau)}) = \zeta_{\alpha(\tau)}^{\tau^{\nu_{k,\tau}(g)}}$ for any $g \in \text{Gal}(k(\zeta_{\alpha(\tau)})/k)$. Furthermore $G = H \rtimes_{\mu} G$ is good.
Main results

Proof. Let \( x \in \text{R}_t(k, H \rtimes \mu \mathcal{G}) \); then \( x \) is the Steinitz class of a tame extension \((K, k_1, k)\) of type \( \mu \) and it is the class of a product of elements of the form

\[
\left( p^{(e_p e_p - 1) \frac{m n}{e_p} - v_p (\alpha_{k_1/k})} \right)^{\frac{1}{2}}.
\]

Hence it is contained in

\[
\text{R}_t(k, H \rtimes \mu \mathcal{G}) \subseteq \text{R}_t(k, \mathcal{G})^n \cdot \prod_{l|n} \prod_{\tau \in H(l) \setminus \{1\}} W(k, E_{k,\mu,\tau})^{\frac{l - 1}{2} \frac{m n}{o(\tau)}},
\]

by Lemma 2.17 and the fact that the last expression is a group. Hence

\[
\text{R}_t(k, H \rtimes \mu \mathcal{G}) \subseteq \text{R}_t(k, \mathcal{G})^n \cdot \prod_{l|n} \prod_{\tau \in H(l) \setminus \{1\}} W(k, E_{k,\mu,\tau})^{\frac{l - 1}{2} \frac{m n}{o(\tau)}},
\]

The opposite inclusion is given by Theorem 1.1 and Proposition 2.13.

We now show that \( H \rtimes \mu \mathcal{G} \) is a good group.

1. The first point of the definition of good groups is clear by what we have just proved about \( \text{R}_t(k, H \rtimes \mu \mathcal{G}) \).

2. This follows from Lemma 2.17 choosing \( \alpha_{K/k} = \alpha_{k_1/k}^n \) for any extension \((K, k_1, k)\) of type \( \mu \).

3. This follows from Lemma 2.18.

4. This comes from Proposition 2.13.

Now we will consider direct products of good groups. We again need two lemmas.

Lemma 2.20. Let \( \mathcal{G}_1 \) and \( \mathcal{G}_2 \) be good groups of orders \( m \) and \( n \) respectively. Let us assume that \( m \) and \( n \) are not both even or that \( \mathcal{G}_1 \) and \( \mathcal{G}_2 \) have both non-cyclic 2-Sylow subgroups. Let \( K/k \) be a tame \( \mathcal{G}_1 \times \mathcal{G}_2 \)-extension of number fields, where \( K = k_1 k_2 \) and \( k_i/k \) are \( \mathcal{G}_i \)-extensions, let \( e_p \) be the ramification index of a prime \( p \) in \( K/k \), and let

\[
\alpha_{K/k} = \begin{cases} 
\alpha_{k_1/k}^n & \text{if } \mathcal{G}_1 \text{ has even order and cyclic 2-Sylow subgroups} \\
\alpha_{k_2/k}^m & \text{if } \mathcal{G}_2 \text{ has even order and cyclic 2-Sylow subgroups} \\
1 & \text{else}
\end{cases}
\]

26
Then the class of the ideal

\[ \left( p^{(e_p-1) \frac{mn}{e_p} - \nu_p(\alpha_{K/k})} \right)^{\frac{1}{2}} \]

is in

\[ R_t(k, G_1)^n R_t(k, G_2)^m. \]

Proof. Let \( p \) be a prime ramifying in \( K/k \). Let \( (g_1, g_2) \) be a generator of its inertia group (it is cyclic since the ramification is tame); then \( g_1 \) generates the inertia group of \( p \) in \( k_1/k \) and \( g_2 \) in \( k_2/k \). Let \( e_{p,i} \) be the ramification index of \( p \) in \( k_i/k \); then \( e_p = \text{lcm}(e_{p,1}, e_{p,2}) \). In particular for any prime \( l \) dividing \( e_p \), \( e_p(l) = \max\{e_{p,1}(l), e_{p,2}(l)\} \).

Let us first consider the case in which the order of \( G_1 \times G_2 \) is odd or its 2-Sylow subgroups are not cyclic. In this case \( \alpha_{K/k} = 1 \) and, recalling Lemma 2.16, we have

\[ p^{(e_p-1) \frac{mn}{e_p}} = \prod_{l|e_p} p^{a_l(l-1) \frac{mn}{e_p,l}} \]

\[ = \prod_{l|e_p} \left( p^{a_l(l-1) \frac{mn}{e_p,l}} \right)^n \prod_{l|e_p} \left( p^{a_l(l-1) \frac{mn}{e_p,l}} \right)^{mn}, \]

where all the exponents \( a_l(l-1) \frac{mn}{e_p,l} \) and \( a_l(l-1) \frac{mn}{e_p,l} \) are clearly even. Thus, since \( G_1 \) and \( G_2 \) are good, the class of \( p^{\frac{1}{2}(e_p-1) \frac{mn}{e_p}} \) is in \( R_t(k, G_1)^n R_t(k, G_2)^m \).

Let us now assume that \( G_1 \times G_2 \) is of even order with cyclic 2-Sylow subgroups. Thus we may suppose that the order of \( G_1 \) is even, that \( G_1 \) has cyclic 2-Sylow subgroups and that the order of \( G_2 \) is odd. Then

\[ p^{(e_p-1) \frac{mn}{e_p} - \nu_p(\alpha_{K/k})} = n \left( p^{(e_p,-1) \frac{mn}{e_p,1} - \nu_p(\alpha_{K/k})} \right) p^{(e_p-1) \frac{mn}{e_p,1}} \]

and, recalling Theorem 1.11, we deduce that

\[ p^{(e_p-1) \frac{mn}{e_p} - (e_p,1-1) \frac{mn}{e_p,1}} \]

is the square of an ideal and we have

\[ p^{(e_p-1) \frac{mn}{e_p} - (e_p,1-1) \frac{mn}{e_p,1}} \]

\[ = \prod_{l|e_p} p^{a_l(l-1) \frac{mn}{e_p,l}} \prod_{l|e_p,1} p^{-b_l(l-1) \frac{mn}{e_p,1,l}} \]

\[ = \prod_{l|e_p} p^{a_l(l-1) \frac{mn}{e_p,2,l}} \prod_{l|e_p} p^{(a_l-b_l)(l-1) \frac{mn}{e_p,1,l}} \prod_{l|e_p,1} p^{-b_l(l-1) \frac{mn}{e_p,1,l}}, \]

27
Main results

For odd primes \( l \) all the exponents in the above expression are even; we deduce that this must be true also for the component corresponding to \( l = 2 \) (if \( 2 | e_p \)), i.e. for \((a_2 - b_2)_{e_p,1(2)}^{mn_{e_p}(2)}\) and hence also for \((a_2 - b_2)_{e_p,1(2)}^{m_{e_p}(2)}\) since \( n \) is odd.

Thus by the hypothesis that \( G_1 \) and \( G_2 \) are good, we easily obtain that the class of the ideal

\[
\left( p^{(e_p-1)\frac{mn_{e_p}(2)}{e_p(2)} - (e_p,1-1)\frac{mn_{e_p}(2)}{e_p(2)}} \right) \frac{1}{2}
\]

is in \( R_t(k; G_1)^n R_t(k; G_2)^m \).

Now we can conclude that the class of

\[
\left( p^{(e_p-1)\frac{mn_{e_p}(2)}{e_p(2)} - v_p(\alpha_K/k)} \right) \frac{1}{2} = p^\frac{n}{2} \left( (e_p,1-1)\frac{mn_{e_p}(2)}{e_p(2)} - v_p(\alpha_k/k) \right) \left( p^{(e_p-1)\frac{mn_{e_p}(2)}{e_p(2)} - (e_p,1-1)\frac{mn_{e_p}(2)}{e_p(2)}} \right) \frac{1}{2}
\]

is in \( R_t(k; G_1)^n R_t(k; G_2)^m \), since also

\[
p^\frac{n}{2} \left( (e_p,1-1)\frac{mn_{e_p}(2)}{e_p(2)} - v_p(\alpha_k/k) \right)
\]

is in \( R_t(k; G_1)^n \) and \( R_t(k; G_1) \) and \( R_t(k; G_2) \) are groups.

\[\square\]

Lemma 2.21. Under the same hypotheses as in the preceding lemma, if \( l | e_p \), the class of

\[
p^{(l-1)\frac{mn_{e_p}(l)}{e_p(l)}}
\]

is in \( R_t(k; G_1)^n R_t(k; G_2)^m \) and, if \( 2 \) divides \((l-1)\frac{mn_{e_p}(l)}{e_p(l)}\), the class of the ideal,

\[
p^{\frac{l-1}{2} \frac{mn_{e_p}(l)}{e_p(l)}}
\]

is in \( R_t(k; G_1)^n R_t(k; G_2)^m \).

Proof. Let \( l | e_p \) and let us assume that \( e_p(l) = e_{p,1}(l) \). Then

\[
p^{(l-1)\frac{mn_{e_p}(l)}{e_p(l)}} = \left( p^{(l-1)\frac{mn_{e_p}(l)}{e_p(l)}} \right)^n
\]

and its class is in \( R_t(k; G_1)^n \), by the hypothesis that \( G_1 \) is good. If \((l-1)\frac{mn_{e_p}(l)}{e_p(l)}\) is even then \( 2 \) divides \((l-1)\frac{m_{e_p}(l)}{e_p(l)}\) (if \( l = 2 \) then this is true because \( 2 | e_p(2) = e_{p,1}(2) \) \( m \) and thus by hypothesis \( n \) is odd or the 2-Sylow subgroup of \( G_1 \) is not cyclic, i.e. \( 2 \) divides \( m/e_{p,1}(2) = m/e_p(2) \)). Then

\[
p^{\frac{l-1}{2} \frac{mn_{e_p}(l)}{e_p(l)}} = \left( p^{\frac{l-1}{2} \frac{mn_{e_p}(l)}{e_p(l)}} \right)^n
\]

is in \( R_t(k; G_1)^n \) by the assumption that \( G_1 \) is good. The case \( e_p(l) = e_{p,2}(l) \) is identical.

\[\square\]
2.3 Realizable classes for $A'$-groups of odd order

**Theorem 2.22.** Let $G_1$ and $G_2$ be good groups of orders $m$ and $n$ respectively and let us assume that $m$ and $n$ are not both even or that $G_1$ and $G_2$ have both non-cyclic 2-Sylow subgroups. Then

$$R_t(k, G_1 \times G_2) = R_t(k, G_1)^n R_t(k, G_2)^m.$$  

Furthermore the group $G_1 \times G_2$ is good.

**Proof.** One inclusion is quite straightforward considering the composition of $G_1$- and $G_2$-extensions of $k$ with appropriate Steinitz classes and using Proposition 1.2.

The opposite inclusion follows by Lemma 2.20 and Theorem 1.1. Now again by Lemma 2.20 and by Lemma 2.21 it follows that $G_1 \times G_2$ is good.

So we obtain our most important result.

**Theorem 2.23.** Every $A'$-group $G$ of odd order is good. In particular for any such group and any number field $k$, $R_t(k, G)$ is a subgroup of the ideal class group of $k$.

**Proof.** Inductively, by Theorem 2.19 and Theorem 2.22, since the trivial group is obviously good.

Of course the above arguments can be used to calculate $R_t(k, G)$ explicitly for a given number field and a given $A'$-group of odd order.

Now we recall the following well-known lemma.

**Lemma 2.24.** Let $k$ be a number field and let $\alpha \in \mathcal{O}_k$ be such that $\alpha \equiv 1 \pmod{4\mathcal{O}_k}$. Then the extension $k(\sqrt{\alpha})/k$ is tame.

**Proof.** By an easy calculation, $\frac{\sqrt{\alpha}+1}{2}$ is an integer, so it is in $\mathcal{O}_{k(\sqrt{\alpha})}$. Now

$$d_{k(\sqrt{\alpha})/k}\left(\left\langle 1, \frac{\sqrt{\alpha}+1}{2}\right\rangle\right) = (\alpha)$$

and so

$$d(k(\sqrt{\alpha})/k)|(\alpha).$$

In particular it follows that $2 \nmid d(k(\sqrt{\alpha})/k)$, i.e. 2 does not ramify in $k(\sqrt{\alpha})/k$ and so the extension is tame.

**Proposition 2.25.** Let $k$ be any number field, then

$$R_t(k, C(2)) = \text{cl}(k).$$

Further $C(2)$ is a good group.
Proof. Let \( x \in \text{cl}(k) \) be any ideal class and let \( q_1 \) and \( q_2 \) be prime ideals in it, which are in the same ray class modulo 4. Thanks to Proposition 1.7, we can choose a prime ideal \( q_0 \) in the ray class modulo 4, which is inverse to that of \( q_1 \) and \( q_2 \).

By construction, \( q_0q_1q_2 \) is principal generated by an \( \alpha \equiv 1 \pmod{4} \). It follows from Theorem 1.1 that

\[
D = \frac{d(k(\sqrt{\alpha})/k)}{\alpha}
\]

is the square of a fractional ideal and by Lemma 2.24 the extension \( k(\sqrt{\alpha})/k \) is tame. In particular all the primes dividing \( d(k(\sqrt{\alpha})/k) \) appear with exponent 1 in its factorization. Then, since \((\alpha) = q_0^2q_1q_2\), the only possibility for \( D \) to be a square, is that it equals \( q_0^{-2} \). Then, again by Theorem 1.1 the Steinitz class of \( k(\sqrt{\alpha})/k \) is \( x \).

Now it is trivial to see that \( C(2) \) is good.

Finally we can also use Theorem 2.19 to prove the following result about dihedral groups.

**Theorem 2.26.** Every dihedral group \( D_n \) with odd \( n \) is good. In particular for any number field \( k \), \( R_t(k, D_n) \) is a subgroup of the ideal class group of \( k \).

**Proof.** Immediate by Theorem 2.19 and Proposition 2.25.

References

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

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

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

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

[5] A. Cobbe. *Steinitz classes of tamely ramified Galois extensions of algebraic number fields*. PhD thesis, Scuola Normale Superiore, Pisa, in preparation.
[6] C. W. Curtis and I. Reiner. *Methods of representation theory. Vol. I*. John Wiley & Sons Inc., New York, 1981.

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

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

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

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

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

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

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

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

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

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

[17] J. J. Rotman. *An introduction to the theory of groups*. GTM 148. Springer-Verlag, New York, fourth edition, 1995.

[18] B. Soudaïgui. 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.

[19] B. Soudaïgui. Relative Galois module structure and Steinitz classes of dihedral extensions of degree 8. *J. Algebra*, 223(1):367–378, 2000.
[20] E. Soverchia. Steinitz classes of metacyclic extensions. *J. London Math. Soc. (2)*, 66(1):61–72, 2002.