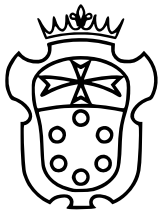

SCUOLA
NORMALE
SUPERIORE
PISA

Corso di Perfezionamento in Matematica
Triennio 2006-2009

Steinitz classes of tamely ramified Galois extensions of algebraic number fields

Candidato:

Alessandro Cobbe

Relatori:

Prof. Roberto Dvornicich
Università di Pisa

Prof. Cornelius Greither
Universität der Bundeswehr
München

Contents

Introduction **5**

Acknowledgements **9**

1 Preliminary results **11**
1.1 Class field theory 12
1.2 Ideal-theoretic formulation of class field theory 17
1.3 Steinitz classes 23

2 Abelian extensions **27**
2.1 General results 27
2.2 Cyclic extensions of 2-power degree 34
2.3 Abelian extensions of even degree 37

3 Nonabelian extensions **43**
3.1 General results 43
3.2 A'-groups 59
3.3 Some l-groups 76
3.4 Some more groups 83

Bibliography **92**

Introduction

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 $\mathcal{O}_K$. More precisely, if I is an ideal in the Steinitz class of K/k, then

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

as $\mathcal{O}_k$-modules. The Steinitz class of an extension of number fields can easily be calculated and it is related to the discriminant and hence to the ramifying primes. An interesting question about Steinitz classes is the following:

Given a number field k and a finite group G, which ideal classes of $\mathcal{O}_k$ are Steinitz classes of a (tamely ramified) G-extension of k?

We will restrict our attention to tamely ramified extensions and call $\mathrm{R}_t(k,G)$ 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 not difficult to find examples in which $\mathrm{R}_t(k,G)$ is neither the whole ideal class group, nor only the class of principal ideals, so the answer to the above question is not trivial.

Calculating realizable classes in some easy concrete examples, we always obtain subgroups of the ideal class group. So we can conjecture that this is always true:

Conjecture. *$\mathrm{R}_t(k,G)$ is always a subgroup of the ideal class group of k.*

It is not known if the conjecture is true, but there are a lot of cases in which it has been proved. We summarize some of the most important results in this direction.

In 1966 Leon McCulloh [17] studied the case in which $G = C(n)$ is cyclic of order n and k contains a primitive n-th root of unity. Under the above hypotheses he proved that $R(k,G) = \mathrm{R}_t(k,G) = \mathrm{Cl}(k)^{d(n)}$ (in $R(k,G)$ we consider also wild extensions), where $d(n)$ is the greatest common divisor of

the $d(l)$ for all the prime divisors l of n and $d(l) = (l-1)/2$ if l is an odd prime and $d(2) = 1$.

In 1971 Robert L. Long [15] was able to remove the hypothesis that some roots of unity are contained in the number field k, in the case of cyclic groups of odd prime order. In this case $R(k, G)$ is no more equal to $\mathrm{R}_t(k, G)$, but they continue both to be subgroups of the ideal class group of k. Later, in [14], he describes explicitly $\mathrm{R}_t(k, G)$ for any cyclic group of odd prime power order, proving in particular that it is a group. Further he refers to an example in his PhD thesis of a number field and an abelian group G for which $R(k, G)$ is not a group.

In 1974 Lawrence P. Endo, in his unpublished PhD thesis [9], extended Long's results about $\mathrm{R}_t(k, G)$ to any abelian group of odd order and he also studied the case of a cyclic G of 2-power order. In this case he obtained only a partial solution, since he assumed that the extension of the base field k given by the adjunction of an appropriate 2-power root of unity is cyclic. Further he considered semidirect products of a cyclic group of odd prime power order with another cyclic group, which acts faithfully on the first one. In all these cases he proved that $\mathrm{R}_t(k, G)$ is a group, giving an explicit description of it.

In 1987 Leon McCulloh [18] studied the Galois module structure of the rings of integers in number fields. It follows from his results that $\mathrm{R}_t(k, G)$ is a subgroup of $\mathrm{Cl}(k)$ for any finite abelian group G. However, this result does not yield an explicit description of $\mathrm{R}_t(k, G)$.

In 1996 James E. Carter [5] considered the nonabelian group G of order p^3 and exponent p. He assumed that the base field k includes the p-th roots of unity, he fixed a cyclic extension E/k of order p and he determined the realizable classes for tame extensions of k with Galois group G and containing E. He proved that those classes are $(\mathfrak{c}W(E/k))^{p^2(p-1)/2}$, where $\mathfrak{c}^{(p-1)/2}$ is the Steinitz class of E/k and $W(k, E)$ will be defined in 1.2.9. In 1997 in [6] he proved that if G is a nonabelian group of order $p^3 = uv$ and exponent v then $\mathrm{R}_t(k, G) = \mathrm{Cl}(k)^{u(p-1)/2}$ whenever k contains a v-th root of unity ζ_v.

In 1997 Richard Massy and Bouchaïb Sodaïgui [16] constructed for each class c of the ideal class group of k a quadratic extension K of k that can be embedded in a quaternion extension of degree 8 such that the Steinitz class of K/k is c.

In 1999 Bouchaïb Sodaïgui [22] proved that $\mathrm{R}_t(k, G) = \mathrm{Cl}(k)$ if $G = C(2) \times C(2)$ and that the same is true if $G = C(4)$ or $G = H_8$, the quaternion group, provided the class number of k is odd. He also proved that every ideal class is the Steinitz class of a quadratic (respectively biquadratic with $\zeta_4 \in k$ or $k(\zeta_4)/k$ ramifying) tame extension K of k, which can be embedded in a tame extension N/k with Galois group $C(4)$ (respectively H_8). In [23] he extends this results to the dihedral group D_4, proving that if the class

number of k is odd then $\mathrm{R}_t(k, D_4) = \mathrm{Cl}(k)$.

In 2001 Elena Soverchia [24] considered the case of metacyclic groups G of order pq, where p and q are odd primes such that $p \equiv 1 \pmod{q}$. She proved that $\mathrm{R}_t(k, G)$ is a group and found an explicit characterization for it.

In 2002 Marjory Godin and Bouchaïb Sodaïgui [10] proved that $\mathrm{R}_t(k, A_4) = \mathrm{Cl}(k)$. In 2003 ([11]) they also proved that, if the class number of k is odd, then $\mathrm{R}_t(k, S_4) = \mathrm{Cl}(k)$.

In 2006 Nigel P. Byott, Cornelius Greither and Bouchaïb Sodaïgui [4] considered groups of the form $G = V \rtimes_\rho C$, where V is a $\mathbb{F}_2$-vector space of dimension $r \geq 2$, C is a cyclic group of order $2^r - 1$ and $\rho : C \to \mathrm{Aut}_{\mathbb{F}_2}(V)$ is a faithful representation. They obtained that $\mathrm{R}_t(k, G) = \mathrm{R}_t(k, C)^{2^r}\mathrm{Cl}(k)^{2^{r-2}(2^r-1)}$.

In 2007 James E. Carter and Bouchaïb Sodaïgui [7] studied the case of the groups of generalized quaternions: $H_{4p^r} = \langle \sigma, \tau : \ \sigma^{2p^r} = 1, \sigma^{p^r} = \tau^2, \tau\sigma\tau^{-1} = \sigma^{-1} \rangle$, where p is an odd prime and r is a positive integer. They proved that $\mathrm{R}_t(k, H_{4p^r}) = \mathrm{Cl}(k)^{p^r} W(k, E_0)^{p-1}$, where $W(k, E_0)$ will be defined in 1.2.9, E_0 is the subextension of $k(\zeta_{p^r})/k$ such that $[k(\zeta_{p^r}) : E_0] = m_0$ and $m_0 = 1$ if $[k(\zeta_{p^r}) : k]$ is odd, $m_0 = 2$ else.

In 2008 Clement Bruche and Bouchaïb Sodaïgui [3] carried on the work of [4]. They considered groups of the form $G = V \rtimes_\rho C$, where V is a $\mathbb{F}_p$-vector space of dimension $r \geq 1$, p is an odd prime, C is a cyclic group of order $p^r - 1$ and $\rho : C \to \mathrm{Aut}_{\mathbb{F}_p}(V)$ is a faithful representation. The result they proved is that if $\zeta_p \in k$ then $\mathrm{R}_t(k, G) = \mathrm{R}_t(k, C)^{p^r}\mathrm{Cl}(k)^{p^{r-1}(p^r-1)(p-1)/2}$.

In 2009 Clement Bruche [2] proved that if G is a nonabelian group of order $p^3 = uv$ and exponent v then $\mathrm{R}_t(k, G) = W(k, p)^{u(p-1)/2}$ under the hypothesis that the extension $k(\zeta_v)/k(\zeta_p)$ is unramified, thereby giving an unconditional result when G has exponent p.

Most of the results have been obtained with techniques from Kummer theory. In this thesis, we obtain some already known results and some generalizations of them, with a different kind of proof, based on class field theory. This method simplifies the proofs, if compared with Kummer theory, since it permits to construct the desired number fields extensions directly, without first adjoining roots of unity and then eliminating them again by passing to suitable subextensions.

In the first chapter we collect some preliminary results about class field theory and Steinitz classes and we prove some simple propositions.

The second chapter is dedicated to abelian extensions. We describe the realizable classes of tame abelian extensions of odd degree (obtaining in a different way the same results as in [9]) and we obtain some information also in the even case. In particular we show that it is enough to study the case of cyclic groups of 2-power degree. Further we also prove the conjecture for

abelian groups whose 2-Sylow subgroup is of the form $C(2^{m_1}) \times \cdots \times C(2^{m_r})$, where $m_1 = m_2 \geq m_3 \geq \cdots \geq m_r$ and $C(n)$ is cyclic of order n.

The most interesting results are contained in chapter 3, in which we study nonabelian extensions. 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. The main result of chapter 3 is that the conjecture about realizable Steinitz classes for tame extensions is true for A'-groups of odd order. We conclude the chapter considering some more groups which can be studied using the same techniques.

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 with a lot of suggestions and corrections. I also wish to thank the Scuola Normale Superiore, for its role in my mathematical education and for its support during the time I was working on my tesi di perfezionamento.

Chapter 1

Preliminary results

In this chapter we recall some general results related to class field theory and to Steinitz classes.

Let k be a number field, i.e. a finite extension of $\mathbb{Q}$, let $\mathcal{O}_k$ be its ring of integers and U_k be its group of units. A prime (or a place) $\mathfrak{p}$ of k is a class of equivalent valuations of k. We distinguish between the finite and the infinite primes, writing $\mathfrak{p} \nmid \infty$ or $\mathfrak{p}|\infty$, respectively. The finite primes belong to the prime ideals of k, for which we use the same notation $\mathfrak{p}$. The infinite primes correspond to the real embeddings or to a pair of conjugate complex embeddings. For the finite primes we consider the valuation $v_\mathfrak{p}$, normalized by $v_\mathfrak{p}(k^*) = \mathbb{Z}$.

We also define the absolute value $|\cdot|_\mathfrak{p}$ in the following way.

1. If $\mathfrak{p} \nmid \infty$ and $q_\mathfrak{p}$ is the cardinality of the residue class field $\kappa_\mathfrak{p} = \mathcal{O}_k/\mathfrak{p}$, then $|a|_\mathfrak{p} = q_\mathfrak{p}^{-v_\mathfrak{p}(a)}$ for $a \in k^*$.

2. If $\mathfrak{p}$ is real infinite and $\iota : k \to \mathbb{R}$ is the corresponding embedding then $|a|_\mathfrak{p} = |\iota a|$ for $a \in k$.

3. If $\mathfrak{p}$ is complex infinite and if $\iota : k \to \mathbb{C}$ is one of the associated embeddings then $|a|_\mathfrak{p} = |\iota a|^2$ for $a \in k$.

For each prime we consider the completion $k_\mathfrak{p}$ of k with respect to $|\cdot|_\mathfrak{p}$. A local field is a field which is complete with respect to a discrete valuation with finite residue class field; in particular if $\mathfrak{p}$ is a finite prime, $k_\mathfrak{p}$ is a local field.

1.1 Class field theory

We recall some of the most important results of class field theory, referring mainly to [20].

Theorem 1.1.1. *For every finite Galois extension $K_\mathfrak{P}/k_\mathfrak{p}$ of local fields we have a canonical isomorphism*

$$r_{K_\mathfrak{P}/k_\mathfrak{p}} : \mathrm{Gal}(K_\mathfrak{P}/k_\mathfrak{p})^{\mathrm{ab}} \to k_\mathfrak{p}^*/\mathrm{N}_{K_\mathfrak{P}/k_\mathfrak{p}} K_\mathfrak{P}^*.$$

The inverse of $r_{K_\mathfrak{P}/k_\mathfrak{p}}$ yields the local norm residue symbol

$$(\ ,K_\mathfrak{P}/k_\mathfrak{p}) : k_\mathfrak{p}^* \to \mathrm{Gal}(K_\mathfrak{P}/k_\mathfrak{p})^{\mathrm{ab}}$$

with kernel $\mathrm{N}_{K_\mathfrak{P}/k_\mathfrak{p}} K_\mathfrak{P}^*$.

Proof. This is Theorem III.2.1 in [20]. □

Theorem 1.1.2. *If $K_\mathfrak{P}/k_\mathfrak{p}$ is a finite abelian extension of local fields, then the norm residue symbol*

$$(\ ,K_\mathfrak{P}/k_\mathfrak{p}) : k_\mathfrak{p}^* \to \mathrm{Gal}(K_\mathfrak{P}/k_\mathfrak{p})$$

maps the group $U_\mathfrak{p}$ on the the inertia group of $K_\mathfrak{P}/k_\mathfrak{p}$.

If $K_\mathfrak{P}/k_\mathfrak{p}$ is tame, then $(\ ,K_\mathfrak{P}/k_\mathfrak{p})$ is trivial on $1+\mathfrak{p} \subseteq U_\mathfrak{p}$.

Proof. This is a particular case of Theorem III.8.10 in [20]. For the triviality of $(\ ,K_\mathfrak{P}/k_p)$ on $1+\mathfrak{p}$ in the tame case we use Proposition III.8.2 of [20]. □

We set

$$U_\mathfrak{p} = \begin{cases} \text{group of units of } k_\mathfrak{p} & \text{if } \mathfrak{p} \nmid \infty \\ k_\mathfrak{p}^* & \text{if } \mathfrak{p}|\infty. \end{cases}$$

Let S be a finite set of primes of the field k. The group

$$I_K^S = \prod_{\mathfrak{p}\in S} k_\mathfrak{p}^* \times \prod_{\mathfrak{p}\notin S} U_\mathfrak{p} \subseteq \prod_\mathfrak{p} k_\mathfrak{p}^*$$

is called the group of S-ideles of k. The union

$$I_k = \bigcup_S I_k^S \subseteq \prod_\mathfrak{p} k_\mathfrak{p}^*,$$

where S runs through all the finite sets of primes of k, is called the *idele group* of k. If $x \in k^*$, then $(x) \in I_k$ is the idele whose $\mathfrak{p}$-th component is $x \in k_\mathfrak{p}^*$ and we may regard k^* as embedded in this way in I_k and thus consider

k^* to be a subgroup of I_k. The ideles from k^* are known as *principal ideles* of k. The factor group

$$C_k = I_k/k^*$$

is called the *idele class group* of k.

We define a cycle of k as a formal product

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_\mathfrak{p}}$$

of prime powers, such that $n_\mathfrak{p} \geq 0$ and $n_\mathfrak{p} = 0$ for almost all $\mathfrak{p}$; for the real infinite primes we admit only the exponents $n_\mathfrak{p} = 0$ and 1, for the complex ones only 0. We set

$$U_\mathfrak{p}^{n_\mathfrak{p}} = \begin{cases} U_\mathfrak{p} & \text{if } n_\mathfrak{p} = 0 \\ 1 + \mathfrak{p}^{n_\mathfrak{p}} \subseteq U_\mathfrak{p} & \text{if } \mathfrak{p} \nmid \infty \text{ and } n_\mathfrak{p} > 0 \\ \mathbb{R}_+ \subseteq k_\mathfrak{p}^* & \text{if } \mathfrak{p} \text{ is real and } n_\mathfrak{p} = 1 \end{cases}$$

and we consider the groups

$$I_k^\mathfrak{m} = \prod_{\mathfrak{p}} U_\mathfrak{p}^{n_\mathfrak{p}}.$$

The quotient

$$C_k^\mathfrak{m} = I_k^\mathfrak{m} \cdot k^*/k^* \subseteq C_k$$

is called the *congruence subgroup* mod $\mathfrak{m}$ of C_k.

The following theorem proves the existence of some abelian extensions of a number field, corresponding to particular subgroups of C_k.

Theorem 1.1.3 (existence theorem)**.** *The map*

$$K \mapsto \mathcal{N}_{K/k} = \mathrm{N}_{K/k} C_K$$

is a 1-1 correspondence between the finite abelian extensions K/k and the subgroups of C_k containing a congruence subgroup $C_k^\mathfrak{m}$. Moreover

$$K_1 \subseteq K_2 \iff \mathcal{N}_{K_1/k} \supseteq \mathcal{N}_{K_2/k},$$

$$\mathcal{N}_{K_1 \cdot K_2/k} = \mathcal{N}_{K_1/k} \cap \mathcal{N}_{K_2/k}, \quad \mathcal{N}_{K_1 \cap K_2/k} = \mathcal{N}_{K_1/k} \cdot \mathcal{N}_{K_2/k},$$

i.e. the correspondence is an anti-isomorphism of lattices. If K/k is associated to the subgroup $\mathcal{N}$ of C_k, then K is called the class field of $\mathcal{N}$. The class field $k^\mathfrak{m}/k$ of the congruence subgroup $C_k^\mathfrak{m}$ is called the ray class field *mod $\mathfrak{m}$. The ray class field mod 1 is also called the* Hilbert class field *of k.*

Proof. All this follows immediately by Theorem IV.7.1 and IV.7.3 of [20]. □

Let K/k be an abelian extension of number fields. The *conductor* $\mathfrak{f}$ of K/k is the g.c.d. of all cycles $\mathfrak{m}$ such that $K \subseteq k^{\mathfrak{m}}$, where $k^{\mathfrak{m}}$ is the ray class field mod $\mathfrak{m}$. By Theorem 1.1.3, $k^{\mathfrak{f}}$ is the smallest ray class field containing K.

Proposition 1.1.4. *Let K/k be an abelian extension of number fields. A prime $\mathfrak{p}$ of k is ramified in K if and only if $\mathfrak{p}|\mathfrak{f}$.*

In particular the Hilbert class field k^1/k is the maximal unramified abelian extension of k.

Proof. See Corollary IV.7.6 in [20]. □

Theorem 1.1.5. *Let m be a natural number, p_∞ the infinite prime of $\mathbb{Q}$ and let $\mathfrak{m}$ be the cycle $\mathfrak{m} = m \cdot p_\infty$. Then the ray class field mod $\mathfrak{m}$ of $\mathbb{Q}$ is the field*

$$\mathbb{Q}^{\mathfrak{m}} = \mathbb{Q}(\zeta_m),$$

where ζ_m is a primitive m-th root of unity.

Proof. This is Theorem IV.7.7 in [20]. □

Now we state a global version of Theorem 1.1.1.

Theorem 1.1.6. *For every finite Galois extension K/k of number fields we have a canonical isomorphism*

$$r_{K/k} : \mathrm{Gal}(K/k)^{\mathrm{ab}} \to C_k/\mathrm{N}_{K/k}C_K.$$

The inverse of $r_{K/k}$ yields the surjective homomorphism

$$(\ , K/k) : C_k \to \mathrm{Gal}(K/k)^{\mathrm{ab}}$$

with kernel $\mathrm{N}_{K/k}C_K$, the global norm residue symbol.

Proof. This is Theorem IV.6.5 in [20]. □

For every prime $\mathfrak{p}$ we have the canonical injection

$$[\ ] : k_{\mathfrak{p}}^* \to C_k,$$

which associates to $a_{\mathfrak{p}} \in k_{\mathfrak{p}}^*$ the class of the idele

$$[a_{\mathfrak{p}}] = (\dots, 1, 1, 1, a_{\mathfrak{p}}, 1, 1, 1, \dots).$$

The following proposition shows the compatibility of local and global class field theory.

Proposition 1.1.7. *If K/k is an abelian extension and $\mathfrak{p}$ a prime of k, then the diagram*

$$\begin{array}{ccc} k_{\mathfrak{p}}^* & \xrightarrow{(\ ,K_{\mathfrak{P}}/k_{\mathfrak{p}})} & \mathrm{Gal}(K_{\mathfrak{P}}/k_{\mathfrak{p}}) \\ \downarrow{\scriptstyle [\ ]} & & \downarrow \\ C_k & \xrightarrow{(\ ,K/k)} & \mathrm{Gal}(K/k) \end{array}$$

is commutative.

Proof. This is Proposition IV.6.6 in [20]. □

Theorem 1.1.8. *Let G be an abelian group. Every surjective homomorphism $\varphi : C_k \to G$ whose kernel contains a congruence subgroup $C_k^{\mathfrak{m}}$ is the norm residue symbol of a unique extension K/k with Galois group isomorphic to G and $\varphi([U_{\mathfrak{p}}])$ is its inertia group for the prime $\mathfrak{p}$. In particular*

$$e_{\mathfrak{p}}(K/k) = \#\varphi([U_{\mathfrak{p}}])$$

and if the primes dividing the order of G do not divide $\mathfrak{m}$, then the extension is tame.

Proof. By Theorem 1.1.3 there exists a unique abelian extension K/k with $\mathrm{N}_{K/k}C_K = \ker\varphi$. By Theorem 1.1.6 the global residue symbol of K/k gives an isomorphism $C_k/\ker\varphi = C_k/\mathrm{N}_{K/k}C_K \to \mathrm{Gal}(K/k)^{\mathrm{ab}} = \mathrm{Gal}(K/k)$ and thus clearly $\mathrm{Gal}(K/k) \cong G$. Now let K_1 and K_2 be two fields corresponding to the same residue symbol, then $\mathrm{N}_{K_1/k}C_{K_1} = \mathrm{N}_{K_2/k}C_{K_2}$ and so, by Theorem 1.1.3, $K_1 = K_2$.

The group $\varphi([U_{\mathfrak{p}}])$ is the inertia group for the prime $\mathfrak{p}$ because of Theorem 1.1.2 and Proposition 1.1.7. □

Proposition 1.1.9. *Let K/k and K'/k' be finite Galois extensions such that $k \subseteq k'$ and $K \subseteq K'$ and let $\delta \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. We then have the commutative diagrams*

$$\begin{array}{ccc} C_{k'} & \xrightarrow{(\ ,K'/k')} & \mathrm{Gal}(K'/k')^{\mathrm{ab}} \\ \downarrow{\scriptstyle \mathrm{N}_{k'/k}} & & \downarrow \\ C_k & \xrightarrow{(\ ,K/k)} & \mathrm{Gal}(K/k)^{\mathrm{ab}} \end{array} \qquad \begin{array}{ccc} C_k & \xrightarrow{(\ ,K/k)} & \mathrm{Gal}(K/k)^{\mathrm{ab}} \\ \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \delta_*} \\ C_{k^\delta} & \xrightarrow{(\ ,K^\delta/k^\delta)} & \mathrm{Gal}(K^\delta/k^\delta)^{\mathrm{ab}} \end{array}$$

where the right arrow in the second diagram is induced by the conjugation $\sigma \mapsto \delta\sigma\delta^{-1}$.

Proof. These are particular cases of Proposition II.3.3 in [20]. □

Let L/K and K/k be an abelian and a Galois extension of number fields respectively, such that L/k is normal, $\mathcal{U} = \mathrm{Gal}(L/K)$ and $\Delta = \mathrm{Gal}(K/k)$. Let $\delta \in \Delta$ and let $\tilde{\delta}, \tilde{\delta}' \in \mathrm{Gal}(L/k)$ be two extensions of δ to $\mathrm{Gal}(L/k)$. Then $\tilde{\delta}'^{-1}\tilde{\delta} \in \mathcal{U}$ and, by the commutativity of $\mathcal{U}$, we have that

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

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

Corollary 1.1.10. *The residue symbol $(\ , L/K) : C_K \to \mathcal{U}$ associated to the extension L/K is Δ-invariant, i.e. for each $\delta \in \Delta$ the following diagram is commutative.*

$$\begin{array}{ccc} C_K & \xrightarrow{(\ ,L/K)} & \mathcal{U} \\ \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \delta_*} \\ C_K & \xrightarrow{(\ ,L/K)} & \mathcal{U}. \end{array}$$

Proof. This follows immediately by Proposition 1.1.9. □

Proposition 1.1.11. *Let K/k be a finite tame extension with Galois group Δ, let $\mathcal{U}$ be a finite abelian group and let $\phi : \Delta \to \mathrm{Aut}(\mathcal{U})$ be an action of Δ on $\mathcal{U}$. Then for a Δ-invariant surjective homomorphism $\varphi : C_K \to \mathcal{U}$, whose kernel contains a congruence subgroup $C_K^{\mathfrak{m}}$, the extension L/K constructed as in Theorem 1.1.8 is Galois over k. The following sequence is exact*

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

and the induced action of Δ on $\mathcal{U}$ 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 $\pi : \mathrm{Gal}(L_1/K) \to \mathrm{Gal}(L/K)$ be the projection, then L is the fixed field of $\ker\pi$. By Proposition 1.1.9

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

and for $\delta \in \mathrm{Gal}(L_1/k)$ we have, using also the hypothesis of Δ-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 $\mathrm{Gal}(L_1/k)$. It follows that L/k is Galois. The exactness of the sequence is obvious and the statement about the action of Δ on $\mathcal{U}$ follows from Proposition 1.1.9, since the given action is the only one for which the diagram on the right commutes. □

1.2 Ideal-theoretic formulation of class field theory

Class field theory has also an ideal-theoretic formulation.

Let k be a number field and let $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_\mathfrak{p}}$ be a cycle of k. We denote by $J_k^\mathfrak{m}$ the group of all ideals prime to $\mathfrak{m}$ and by $P_k^\mathfrak{m}$ the group of all principal ideals generated by an element $a \equiv 1 \pmod{\mathfrak{p}^{n_\mathfrak{p}}}$ for all $\mathfrak{p}|\mathfrak{m}$. The group $J_k^\mathfrak{m}/P_k^\mathfrak{m}$ is called the *ray class group* mod $\mathfrak{m}$. The ray class group mod 1 is the usual ideal class group $Cl(k) = J_k/P_k$, where $J_k = J_k^1$ and $P_k = P_k^1$.

Proposition 1.2.1. *The homomorphism*

$$\pi : I_k \to J_k, \qquad \alpha \mapsto \prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{v_\mathfrak{p}(\alpha_\mathfrak{p})}$$

induces an isomorphism

$$\pi_\mathfrak{m} : C_k/C_k^\mathfrak{m} \to J_k^\mathfrak{m}/P_k^\mathfrak{m}.$$

Proof. This is Proposition IV.8.1 in [20]. □

Let K be an abelian extension of k, contained in the ray class field mod $\mathfrak{m}$; the cycle $\mathfrak{m}$ is called a *cycle of declaration* for K/k. We define

$$\left(\frac{K/k}{\mathfrak{a}}\right) = \prod_{\mathfrak{p}} ([\pi_\mathfrak{p}], K/k)^{\nu_\mathfrak{p}},$$

where $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_\mathfrak{p}} \in J_k^\mathfrak{m}$ and $\pi_\mathfrak{p}$ is a prime element in $k_\mathfrak{p}$. By Proposition 1.1.4, every prime ideal $\mathfrak{p} \nmid \mathfrak{m}$ is unramified in K and hence by Theorem 1.1.2 and Proposition 1.1.7 the above expression does not depend on the choice of the $\pi_\mathfrak{p}$. It is called the *Artin symbol*.

Proposition 1.2.2. *Let K/k and K'/k' be finite Galois extensions, with cycles of declaration $\mathfrak{m}$ and $\mathfrak{m}'$, such that $k \subseteq k'$ and $K \subseteq K'$ Then we have the commutative diagram*

$$\begin{array}{ccc} J_{k'}^{\mathfrak{m}'} & \xrightarrow{\left(\frac{K'/k'}{\cdot}\right)} & \mathrm{Gal}(K'/k')^{\mathrm{ab}} \\ \downarrow{\scriptstyle \mathrm{N}_{k'/k}} & & \downarrow \\ J_k^\mathfrak{m} & \xrightarrow{\left(\frac{K/k}{\cdot}\right)} & \mathrm{Gal}(K/k)^{\mathrm{ab}} \end{array}.$$

Proof. Let $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}} \in J_{k'}^{\mathfrak{m}'}$ and let $\pi_{\mathfrak{p}}$ be a prime element in $k'_{\mathfrak{p}}$, then

$$\left(\frac{K'/k'}{\mathfrak{a}}\right)\Big|_K = \prod_{\mathfrak{p}} ([\pi_{\mathfrak{p}}], K'/k')^{\nu_{\mathfrak{p}}}|_K = \prod_{\mathfrak{p}} (\mathrm{N}_{k'/k}([\pi_{\mathfrak{p}}]), K/k)^{\nu_{\mathfrak{p}}}$$
$$= \prod_{\mathfrak{p}} \left(\frac{K/k}{\mathrm{N}_{k'/k}(\mathfrak{p})}\right)^{\nu_{\mathfrak{p}}} = \left(\frac{K/k}{\mathrm{N}_{k'/k}(\mathfrak{a})}\right),$$

where we used Proposition 1.1.9. □

Theorem 1.2.3. *Let K/k be an abelian extension and let $\mathfrak{m}$ be a cycle of declaration of K/k. Then the Artin symbol induces a surjective homomorphism*

$$\left(\frac{K/k}{\cdot}\right) : J_k^{\mathfrak{m}}/P_k^{\mathfrak{m}} \to \mathrm{Gal}(K/k)$$

with kernel $H_{K/k}^{\mathfrak{m}}/P_k^{\mathfrak{m}}$, where $H_{K/k}^{\mathfrak{m}} = \mathrm{N}_{K/k} J_K^{\mathfrak{m}} \cdot P_k^{\mathfrak{m}}$.

Moreover we have an exact commutative diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathrm{N}_{K/k}C_K & \longrightarrow & C_k & \xrightarrow{(\ ,K/k)} & \mathrm{Gal}(K/k) & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \pi_{\mathfrak{m}}} & & \downarrow{\scriptstyle \pi_{\mathfrak{m}}} & & \downarrow{\scriptstyle \mathrm{id}} & & \\
1 & \longrightarrow & H_{K/k}^{\mathfrak{m}}/P_k^{\mathfrak{m}} & \longrightarrow & J_k^{\mathfrak{m}}/P_k^{\mathfrak{m}} & \xrightarrow{\left(\frac{K/k}{\cdot}\right)} & \mathrm{Gal}(K/k) & \longrightarrow & 1
\end{array}$$

Proof. This is Theorem IV.8.2 in [20]. □

Corollary 1.2.4. *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*

$$\pi_{\mathfrak{m}} : \mathcal{N}_{K/k}/C_k^{\mathfrak{m}} \to H_{K/k}^{\mathfrak{m}}/P_k^{\mathfrak{m}}$$

is an isomorphism, and

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

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

Proof. By Proposition 1.2.1, $\pi_{\mathfrak{m}} : C_k \to J_k^{\mathfrak{m}}/P_k^{\mathfrak{m}}$ is surjective and thus by the exact commutative diagram in the above theorem, we obtain that $\pi_{\mathfrak{m}}(\mathcal{N}_{K/k}) = H_{K/k}^{\mathfrak{m}}/P_k^{\mathfrak{m}}$. By Theorem 1.1.3, $\mathcal{N}_{K/k} \supseteq C_k^{\mathfrak{m}}$ ($\mathfrak{m}$ is a cycle of declaration of K/k) and then by Proposition 1.2.1 it is the kernel of $\pi_{\mathfrak{m}} : \mathcal{N}_{K/k} \to H_{K/k}^{\mathfrak{m}}/P_k^{\mathfrak{m}}$.

Now the result follows by Theorem 1.1.3 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 $J_k^{\mathfrak{m}} \to J_k^{\mathfrak{m}}/P_k^{\mathfrak{m}}$. □

Corollary 1.2.5. *Let $k^{\mathfrak{m}}$ be the ray class field modulo a cycle $\mathfrak{m}$ of a number field k. Then*

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

is an isomorphism.

Proof. By definition of the ray class field mod $\mathfrak{m}$, $\mathcal{N}_{k^{\mathfrak{m}}/k} = C_k^{\mathfrak{m}}$ and thus by Corollary 1.2.4 we obtain that $H_{k^{\mathfrak{m}}/k}^{\mathfrak{m}}/P_k^{\mathfrak{m}}$ is the trivial group. We conclude using Theorem 1.2.3. □

Theorem 1.2.6. *Let K/k be an abelian extension of degree n and let $\mathfrak{p}$ be an unramified prime ideal. Let $\mathfrak{m}$ be a cycle of declaration of K/k not divisible by $\mathfrak{p}$ and let $H_{K/k}^{\mathfrak{m}}$ be the corresponding ideal group.*

If f is the order of $\mathfrak{p}$ mod $H_{K/k}^{\mathfrak{m}}$ in the ideal class group $J_k^{\mathfrak{m}}/H_{K/k}^{\mathfrak{m}}$, i.e. the smallest positive number such that

$$\mathfrak{p}^f \in H_{K/k}^{\mathfrak{m}},$$

then $\mathfrak{p}$ splits in K into a product

$$\mathfrak{p} = \mathfrak{P}_1 \dots \mathfrak{P}_r$$

of $r = \frac{n}{f}$ different prime ideals $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ of degree f over $\mathfrak{p}$.

Proof. This is Theorem IV.8.4 in [20]. □

Theorem 1.2.7 (Chebotarev)**.** *Let K/k be a finite abelian extension and let $\sigma \in \mathrm{Gal}(K/k)$. Then there exist infinitely many prime ideals $\mathfrak{p}$ in k, unramified in K, of absolute degree 1 and with $\sigma = \left(\frac{K/k}{\mathfrak{p}}\right)$.*

Proof. This follows by Theorem V.6.4 in [20] and the observation that the Dirichlet density of a subset of the primes of k depends only on the prime ideals of the first degree (page 130 of [20]). Further we use also the fact that the Dirichlet density can be positive only if the cardinality of the considered set is infinite (again, see page 130 of [20]). □

Proposition 1.2.8. *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. By Corollary 1.2.5,

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

is an isomorphism, where $k^{\mathfrak{m}}$ is the ray class field modulo $\mathfrak{m}$. Thus for each ray class we can consider the corresponding automorphisms $\sigma \in \mathrm{Gal}(k^{\mathfrak{m}}/k)$ and, by Theorem 1.2.7, there exist infinitely many prime ideals $\mathfrak{p}$ in k, unramified in $k^{\mathfrak{m}}$, of absolute degree 1 and with $\sigma = \left(\frac{k^{\mathfrak{m}}/k}{\mathfrak{p}}\right)$. By construction they must be in the given ray class. □

Definition 1.2.9. *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*

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

If ζ_m is an m-th root of unity we use the notation $W(k,m) = W(k,k(\zeta_m))$.

Proposition 1.2.10. *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 1.2.3 and by Corollary 1.2.5 the kernel of

$$\left(\frac{k^1/k}{\cdot}\right) : J_k^{\mathfrak{m}}/P_k^{\mathfrak{m}} \to \mathrm{Gal}(k^1/k)$$

is $H^{\mathfrak{m}}_{k^1/k}/P_k^{\mathfrak{m}} = (P_k \cap J_k^{\mathfrak{m}})/P_k^{\mathfrak{m}}$; so we have $H^{\mathfrak{m}}_{k^1/k} = P_k \cap J_k^{\mathfrak{m}}$ and, by Corollary 1.2.4,

$$H^{\mathfrak{m}}_{K\cap k^1/k} = H^{\mathfrak{m}}_{K/k} \cdot H^{\mathfrak{m}}_{k^1/k} = H^{\mathfrak{m}}_{K/k} \cdot (P_k \cap J_k^{\mathfrak{m}}).$$

Let $x \in H^1_{K\cap k^1/k}/P_k$, then by Proposition 1.2.8 there exists a prime $\mathfrak{p} \nmid \mathfrak{m}$ in the class of x, and, recalling also the definition of $H^{\mathfrak{m}}_{K\cap k^1/k}$,

$$\mathfrak{p} \in H^1_{K\cap k^1/k} \cap J_k^{\mathfrak{m}} = H^{\mathfrak{m}}_{K\cap k^1/k} \cdot (P_k \cap J_k^{\mathfrak{m}}) = H^{\mathfrak{m}}_{K/k} \cdot (P_k \cap J_k^{\mathfrak{m}}),$$

i.e. $x \in H^{\mathfrak{m}}_{K/k} \cdot P_k/P_k$. Thus

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

and the opposite inclusion is trivial.

Thus we have proved that

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

□

Corollary 1.2.11. *Let $K_1, K_2/k$ be abelian extensions of number fields, then*

$$K_1 \subseteq K_2 \iff W(k, K_1) \supseteq W(k, K_2),$$

$$W(k, K_1)W(k, K_2) = W(k, K_1 \cap K_2), \quad W(k, K_1) \cap W(k, K_2) \supseteq W(k, K_1 K_2).$$

Proof. By Proposition 1.2.10 and Corollary 1.2.4:

$$K_1 \subseteq K_2 \iff W(k, K_1) = H^1_{K_1 \cap k^1/k}/P_k \supseteq H^1_{K_2 \cap k^1/k}/P_k = W(k, K_2),$$

$$\begin{aligned} W(k, K_1)W(k, K_2) &= H^1_{K_1 \cap k^1/k} H^1_{K_2 \cap k^1/k}/P_k \\ &= H^1_{K_1 \cap K_2 \cap k^1/k}/P_k = W(k, K_1 \cap K_2), \\ W(k, K_1) \cap W(k, K_2) &= (H^1_{K_1 \cap k^1/k} \cap H^1_{K_2 \cap k^1/k})/P_k = H^1_{(K_1 \cap k^1)(K_2 \cap k^1)/k}/P_k \\ &\supseteq H^1_{K_1 K_2 \cap k^1/k}/P_k = W(k, K_1 K_2). \end{aligned}$$

□

The following result is similar to the characterizations of $W(k, K)$ given in [9].

Proposition 1.2.12. *Let K/k be a finite abelian extension of number fields. Then the following subsets of the class group of k are equal to $W(k, K)$:*

$$\begin{aligned} W_1 &= \{x \in J_k/P_k : x \text{ contains infinitely many primes of absolute degree } 1 \\ &\qquad \text{splitting completely in } K\}, \\ W_2 &= \{x \in J_k/P_k : x \text{ contains a prime splitting completely in } K\}, \\ W_3 &= \mathrm{N}_{K/k}(J_K) \cdot P_k/P_k. \end{aligned}$$

Proof. Let $x \in W(k, K)$ and let $\mathfrak{m}$ be a cycle of declaration of K/k. By definition $x = \mathfrak{a} \cdot P_k$, where $\mathfrak{a} \in H^{\mathfrak{m}}_{K/k}$. By Proposition 1.2.8 there exist infinitely many primes of absolute degree 1 in the ray class modulo $\mathfrak{m}$ containing $\mathfrak{a}$; let $\mathfrak{p}$ be one of them, which does not ramify in K/k. Then $\mathfrak{p} = \mathfrak{a} \cdot (b)$, where $(b) \in P^{\mathfrak{m}}_k$, and thus $\mathfrak{p} \in H^{\mathfrak{m}}_{K/k}$ and by Theorem 1.2.6 we can conclude that $\mathfrak{p}$ 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 $\mathfrak{p}$ be a prime in x which splits completely in K. Then for any prime divisor $\mathfrak{P}$ of $\mathfrak{p}$ in K, $\mathrm{N}_{K/k}(\mathfrak{P}) = \mathfrak{p}$. Thus $x = \mathrm{N}_{K/k}(\mathfrak{P}) \cdot P_k$ and hence $W_2 \subseteq W_3$.

Recalling Proposition 1.2.10 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 important results.

Lemma 1.2.13. *Let $\mathfrak{p}$ be a prime in k of absolute degree 1, splitting completely in $k(\zeta_m)$. Then $\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{p}) \in P_{\mathbb{Q}}^{\mathfrak{m}}$, where $\mathfrak{m} = m \cdot p_\infty$.*

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

Lemma 1.2.14. *Let k be a number field, let $\mathfrak{m} = m \cdot p_\infty$, with $m \in \mathbb{N}$, and let $\mathfrak{a} \in J_k^{\mathfrak{m}}$ be such that $\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{a}) \in P_{\mathbb{Q}}^{\mathfrak{m}}$, then $\mathfrak{a} \in H_{k(\zeta_m)/k}^{\mathfrak{m}}$, i.e. the class of $\mathfrak{a}$ is in $W(k, m)$.*

Proof. By Proposition 1.2.2,

$$\left(\frac{k(\zeta_m)/k}{\mathfrak{a}}\right)\Big|_{\mathbb{Q}(\zeta_m)} = \left(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{a})}\right) = 1.$$

Of course also the restriction of $\left(\frac{k(\zeta_m)/k}{\mathfrak{a}}\right)$ to k is trivial; thus we have proved that

$$\left(\frac{k(\zeta_m)/k}{\mathfrak{a}}\right) = 1,$$

i.e. that $\mathfrak{a} \in H_{k(\zeta_m)/k}^{\mathfrak{m}}$. □

Lemma 1.2.15. *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 $\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{p}) \in P_{\mathbb{Q}}^{\mathfrak{m}}$, where $\mathfrak{m} = e \cdot p_\infty$. In particular, by Lemma 1.2.14, $\mathfrak{p} \in H_{k(\zeta_e)/k}^{\mathfrak{m}}$ and so its class is in $W(k, e)$.*

Proof. This is Lemma I.2.1 of [9]. □

Proposition 1.2.16. *Let k be a number field and let $\mathfrak{m} = m \cdot p_\infty$, with $m \in \mathbb{N}$. Then the following subsets of the class group of k are equal to $W(k, m)$:*

$$W_4 = \{x \in J_k/P_k : x \text{ contains infinitely many primes } \mathfrak{p} \text{ of degree } 1 \text{ with } \mathrm{N}_{k/\mathbb{Q}}(\mathfrak{p}) \in P_{\mathbb{Q}}^{\mathfrak{m}}\},$$
$$W_5 = \{x \in J_k/P_k : x \text{ contains an ideal } \mathfrak{a} \text{ prime to } m \text{ with } \mathrm{N}_{k/\mathbb{Q}}(\mathfrak{a}) \in P_{\mathbb{Q}}^{\mathfrak{m}}\}.$$

Proof. Let $x \in W(k, m)$. By Proposition 1.2.12 there exist infinitely many prime ideals of absolute degree 1 splitting completely in $k(\zeta_m)$. By Lemma 1.2.13 we conclude that $W(k, m) \subseteq W_4$.

By Lemma 1.2.14 we know that $W_4 \subseteq W_5 \subseteq W(k, m)$. □

In the following we will also consider rational powers of some $W(k,K)$. They are defined as follows

$$W(k,K)^{1/b} = \{x \in \mathrm{Cl}(k) : \ x^b \in W(k,K)\}$$

and, if a and b are coprime,

$$W(k,K)^{a/b} = \left(W(k,K)^{1/b}\right)^a.$$

Lemma 1.2.17. *Let m, n, x be integers. If $x \equiv 1 \pmod m$ and any prime q dividing n divides also m then*

$$x^n \equiv 1 \pmod{mn}.$$

Proof. Let $n = q_1 \dots q_r$ 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 $x^n \equiv 1 \pmod{mn}$. If $r = 1$, then $mn = mq_1$ must divide m^{q_1} and there exists $b \in \mathbb{N}$ such that

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

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

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

□

Lemma 1.2.18. *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 1.2.16, x contains a prime ideal $\mathfrak{p}$, prime to mn and such that $\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{p}) \in P_{\mathbb{Q}}^{\mathfrak{m}}$, where $\mathfrak{m} = m \cdot p_\infty$. Then by Lemma 1.2.17, $\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{p}^n) \in P_{\mathbb{Q}}^{\mathfrak{n}}$, with $\mathfrak{n} = mn \cdot p_\infty$, and it follows from Proposition 1.2.16 that $x^n \in W(k,mn)$. □

1.3 Steinitz classes

In this section we recall the definition and some properties of Steinitz classes.

Theorem 1.3.1. *Let R be a Dedekind domain, let M be a finitely generated R-module and let A be the submodule of M consisting of all torsion elements of M, i.e. of the elements $x \in M$ which, for some nonzero $r \in R$, satisfy $rx = 0$. Then M can be written as a direct sum*

$$M \cong R^n \oplus I \oplus A,$$

where n is a natural number and I is some ideal of R.

Proof. This is Theorem 1.13 in [19]. □

Theorem 1.3.2. *Let R be a Dedekind domain and let*

$$M_1 = I_1 \oplus \cdots \oplus I_m, \qquad M_2 = J_1 \oplus \cdots \oplus J_n,$$

be finitely generated torsion-free R-modules, where I_i, J_i are nonzero fractional ideals of R. Then M_1 and M_2 are isomorphic if and only if $m = n$ and, with a suitable $a \in K$, the field of quotients of R, the equality

$$I_1 \cdots I_m = aJ_1 \cdots J_n$$

holds. Equivalently $I_1 \cdots I_m \cong J_1 \cdots J_n$ as R-modules.

Proof. This is Theorem 1.14 in [19]. □

Definition 1.3.3. *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 1.3.1 we know that*

$$\mathcal{O}_K \cong \mathcal{O}_k^{n-1} \oplus I,$$

where $n = [K : k]$ and I is an ideal of $\mathcal{O}_k$. By Theorem 1.3.2 the $\mathcal{O}_k$-module structure of $\mathcal{O}_K$ is determined by n and the ideal class of I. This class is called the Steinitz class *of K/k.*

We are going to study the realizable classes for a number field k and a finite group G.

Definition 1.3.4. *Let k be a number field and G a finite group, then we define*

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

In general it is not known if $\mathrm{R}_t(k, G)$ is a subgroup of the ideal class group.

Let K/k be a finite extension of number fields and let $w_1, \ldots, w_{[K:k]}$ be $[K : k]$ elements of K. We define the *discriminant*

$$d_{K/k}(w_1, \ldots, w_{[K:k]}) = \det(\sigma_i w_j)^2$$

to be the square of the determinant taken with σ_i ranging over the $[K : k]$ distinct embeddings of K in a given algebraic closure of k.

If I is an ideal of $\mathcal{O}_K$, we denote by $d_{K/k}(I)$ the ideal of $\mathcal{O}_k$ generated by all the $d_{K/k}(w_1, \ldots, w_{[K:k]})$, as $\{w_1, \ldots, w_{[K:k]}\}$ ranges over the bases of K over k such that $w_i \in I$ and we call this the discriminant of the ideal. In particular we can associate to an extension of number fields the discriminant of the trivial ideal in $\mathcal{O}_K$ and call it the discriminant of the extension:

$$d(K/k) = d_{K/k}(1).$$

Theorem 1.3.5. *If K/k is a finite tame Galois extension then*

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

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

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

Theorem 1.3.6. *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 $\mathrm{d}(K/k)$ 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 α is any element of k whose square root generates the quadratic subextension of K/k then $\mathrm{d}(K/k)/\alpha$ is the square of a fractional ideal and this ideal represents the Steinitz class of the extension.

Proof. This is a corollary of Theorem I.1.1 in [9]. In particular it is shown in [9] that in case (b) K/k does have exactly one quadratic subextension. □

Proposition 1.3.7. *Suppose K/E and E/k are number fields extensions. Then*

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

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

Lemma 1.3.8. *Let K_1, K_2 be two arithmetically disjoint*[1] *abelian extensions of a number field k, whose Galois groups are isomorphic to a given group G. Then there exists an extension K of k, contained in K_1K_2, with $\mathrm{Gal}(K/k) \cong G$ and $\mathrm{st}(K/k) = \mathrm{st}(K_1/k)\mathrm{st}(K_2/k)$. Furthermore the discriminant of K_1K_2 over K is equal to 1.*

If we fix isomorphisms $G \cong \mathrm{Gal}(K_1/k)$ and $G \cong \mathrm{Gal}(K_2/k)$, then a field K with the above properties is constructed by considering the fixed field of the image of the diagonal embedding of G in $\mathrm{Gal}(K_1/k) \times \mathrm{Gal}(K_2/k) \cong \mathrm{Gal}(K_1K_2/k)$.

Proof. This is the Multiplication Lemma on page 22 in [9]. □

We conclude this section with a general result about tame Galois extensions.

[1] This means that $K_1 \cap K_2 = k$ and $(\mathrm{d}(K_1/k), \mathrm{d}(K_2/k)) = 1$.

Proposition 1.3.9. *The inertia group $I_{\mathfrak{P}}$ of a prime $\mathfrak{P}$ in a tame Galois extension L of a number field K is cyclic.*

Proof. We can assume that $\mathfrak{P}$ is totally ramified in L/K, by substituting K with the fixed field of $I_{\mathfrak{P}}$. Localizing at $\mathfrak{P}$ we obtain a totally ramified tame Galois extension of local fields $L_{\mathfrak{P}}/K_{\mathfrak{p}}$. By Proposition 1 in chapter I.8 of [1] $L_{\mathfrak{P}} = K_{\mathfrak{p}}(c^{1/e})$ with $c, \zeta_e \in K_{\mathfrak{p}}$. Hence $I_{\mathfrak{P}} = \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ is cyclic. □

Chapter 2

Abelian extensions

In this chapter we study the realizable classes in the case of abelian extensions. We start proving some general results, which easily lead to the description of realizable classes in the odd case (this result was first obtained by Endo in his PhD thesis [9]). In the second section we study cyclic extensions of 2-power degree, but we do not obtain a general characterization of Steinitz classes. The most interesting results of this chapter are those contained in the last section, in which we prove that a description of the realizable classes in the cyclic case of 2-power degree would lead to a solution of our problem for any abelian extension of even degree.

2.1 General results

In this section we prove some general results about Steinitz classes of abelian extensions of number fields and we obtain a characterization of the realizable Steinitz classes in the case of abelian groups of odd order. This result has already been proved in a different way in [9]. More precisely, let k be a number field and G an abelian group of order m; we are going to study $\mathrm{R}_t(k,G)$. We start introducing some notations about k and G.

We denote the class group of k by $\mathrm{Cl}(k) = C(h_1) \times \cdots \times C(h_t)$, which is a product of cyclic groups of orders $h_1, \dots, h_t$, generated by $x_1 \dots, x_t$. Choosing prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ of degree 1 contained in the ideal classes $x_1, \dots, x_t$ (they exist because of Proposition 1.2.8), we know that $\mathfrak{p}_i^{h_i} = (\alpha_i)$ are principal ideals. Let $\pi_{\mathfrak{p}_i}$ be prime elements in $k_{\mathfrak{p}_i}$ and let $y_i = [\pi_{\mathfrak{p}_i}] = (\dots, 1, 1, \pi_{\mathfrak{p}_i}, 1, 1, \dots) \in I_k$, then we define

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

Let $\{u_1, \dots, u_s\}$ be the union of a system of generators of the abelian group U_k with $\{a_1, \dots, a_t\}$.

For any $\mathfrak{p}$ let $g_\mathfrak{p}$ be a fixed generator of $\kappa_\mathfrak{p}^* = U_\mathfrak{p}/U_\mathfrak{p}^1$; then for each $a \in \prod_\mathfrak{p} U_\mathfrak{p}$ and for any prime $\mathfrak{p}$ we choose $\tilde{h}_{\mathfrak{p},a} \in \mathbb{Z}$ such that $g_\mathfrak{p}^{\tilde{h}_{\mathfrak{p},a}} \equiv a_\mathfrak{p} \pmod{\mathfrak{p}}$.

Let $G = C(m_1) \times \cdots \times C(m_r)$ be the decomposition of G into cyclic groups with generators $\tau_1, \dots, \tau_r$ and orders $m_{i+1} | m_i$ (sometimes it will be useful to consider $m_i = 1$ for $i > r$). If n is an integer and S is a set of primes, we will use the notation $n(S)$ to indicate the product for $l \in S$ of the l-components of n and, for simplicity, we will also write $n(l) = n(\{l\})$. The letter l will always indicate a prime, even if not explicitly mentioned.

Then we also define

$$\eta = \begin{cases} 1 & \text{if } 2 \nmid m \text{ or } m_2(2) \neq 1 \\ 2 & \text{if } 2 | m \text{ and } m_2(2) = 1. \end{cases}$$

Lemma 2.1.1. *A group homomorphism $\varphi_0 : (\prod_\mathfrak{p} U_\mathfrak{p})/U_k \to G$ can be extended to $\varphi : C_k \to G$ if and only if for $j = 1, \dots, t$, $\varphi_0(a_j) = g_j^{h_j}$ 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

$$B_k = \left(\left(\prod_\mathfrak{p} U_\mathfrak{p} \right) / U_k \times \langle e_1, \dots, e_t \rangle \right) / \{ e_j^{h_j} / a_j | j = 1, \dots, t \},$$

where the second component in the direct product is a free abelian group. We may extend the inclusion $i : (\prod_\mathfrak{p} U_\mathfrak{p})/U_k \hookrightarrow C_k$ to B_k by $e_j \mapsto y_j$ and thus also the map $\pi \circ i : (\prod_\mathfrak{p} U_\mathfrak{p})/U_k \to \mathrm{Cl}(k)$ by $e_j \mapsto x_j$. We obtain the following commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \left(\prod_\mathfrak{p} U_\mathfrak{p}\right)/U_k & \longrightarrow & B_k & \longrightarrow & \mathrm{Cl}(k) & \longrightarrow & 1 \\ & & \downarrow \mathrm{id} & & \downarrow & & \downarrow \mathrm{id} & & \\ 1 & \longrightarrow & \left(\prod_\mathfrak{p} U_\mathfrak{p}\right)/U_k & \longrightarrow & C_k & \longrightarrow & \mathrm{Cl}(k) & \longrightarrow & 1 \end{array}$$

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 $a \in (\prod_\mathfrak{p} U_\mathfrak{p})/U_k$ 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 $\left(\prod_{\mathfrak{p}} U_{\mathfrak{p}}\right)/U_k$ is the identity map, it is clear that φ is an extension of φ_0. □

Lemma 2.1.2. *Let x be any class in $W(k, m_1)$. Then there exist G-Galois extensions of k, whose Steinitz classes are $\eta\alpha$-th powers of x, where*

$$\alpha = \sum_{i=1}^{r} \frac{m_i - 1}{2} \frac{m}{m_i} + \frac{m_1 - 1}{2} \frac{m}{m_1}.$$

In particular $1 \in \mathrm{R}_t(k, G)$, since $1 \in W(k, m_1)$.

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 1.2.16 there are infinitely many prime ideals $\mathfrak{q}$, for which $\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{q}) \in P_{\mathbb{Q}}^{\mathfrak{m}_1}$, where $\mathfrak{m}_1 = m_1 \cdot p_\infty$, and whose ideal class is x. For those primes the order of $\kappa_{\mathfrak{q}}^*$ is a multiple of m_1 and so for any $a \in \prod_{\mathfrak{p}} U_{\mathfrak{p}}$ the class $h_{\mathfrak{q},a}$ of $\tilde{h}_{\mathfrak{q},a}$ modulo m_1 is well defined. The set of all the possible s-tuples $(h_{\mathfrak{q},u_1}, \ldots, h_{\mathfrak{q},u_s})$ is finite and so it follows from the pigeonhole principle that there are infinitely many $\mathfrak{q}$ corresponding to the same s-tuple.

Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_{r+1}$ be $r+1$ such prime ideals. We can assume that they are prime to a fixed ideal I and to m.

Let us define $\varphi_0 : \prod_{\mathfrak{p}} \kappa_{\mathfrak{p}}^* \to G$, posing

$$\begin{cases} \varphi_0(g_{\mathfrak{q}_i}) = \tau_i & \text{for } i = 1, \ldots, r \\ \varphi_0(g_{\mathfrak{q}_{r+1}}) = (\tau_1 \ldots \tau_r)^{-1} & \\ \varphi_0(g_{\mathfrak{p}}) = 1 & \text{for } \mathfrak{p} \notin \{\mathfrak{q}_1, \ldots, \mathfrak{q}_{r+1}\}. \end{cases}$$

This is well defined since the order of $g_{\mathfrak{q}_i}$ is a multiple of m_1 and hence of the order of τ_i. By construction $\varphi_0(u_j) = 1$ for $j = 1, \ldots, s$ and so in particular φ_0 is trivial on U_k and on the $a_1, \ldots, a_t$. This means that φ_0 is well defined on $(\prod_{\mathfrak{p}} U_{\mathfrak{p}})/U_k$ and that $\varphi_0(a_j) = 1$. Then it follows from Lemma 2.1.1 that φ_0 can be extended to $\varphi : C_k \to G$; the kernel of φ_0 contains $I_k^{\mathfrak{m}}$, where $\mathfrak{m} = \prod_{i=1}^{r+1} \mathfrak{q}_i$, and so $C_k^{\mathfrak{m}} \subseteq \ker \varphi$. By Theorem 1.1.8 there is a G-Galois extension of k, ramifying only in $\mathfrak{q}_1, \ldots, \mathfrak{q}_{r+1}$, with indices m_i for

$i \in \{1, \dots, r\}$ and m_1 for $i = r+1$. By Theorem 1.3.5 the corresponding discriminant is

$$\mathrm{d} = \left(\prod_{i=1}^{r} \mathfrak{q}_i^{(m_i-1)\frac{m}{m_i}} \right) \mathfrak{q}_{r+1}^{(m_1-1)\frac{m}{m_1}}.$$

If $2 \nmid m$ or $m_2(2) \neq 1$ then by Theorem 1.3.6 the Steinitz class is x^α, where

$$\alpha = \sum_{i=1}^{r} \frac{m_i - 1}{2} \frac{m}{m_i} + \frac{m_1 - 1}{2} \frac{m}{m_1}.$$

It is immediate to verify that the additional conditions are verified.

If $2|m$ and $m_2(2) = 1$ we obtain extensions whose Steinitz classes have $x^{2\alpha}$ as their square. We may construct infinitely many such extensions which are arithmetically disjoint and whose discriminants are relatively prime and so, by the pigeonhole principle, there are two of them with the same Steinitz class. Then the conclusion follows by Lemma 1.3.8. □

Lemma 2.1.3. *Let l be a prime dividing the order m of G and let x be any class in $W(k, m_1(l))$. There exist G-Galois extensions of k, whose Steinitz classes are $\eta\alpha_{l,j}$-th powers of x, where:*

(a) $$\alpha_{l,1} = (l-1)\frac{m}{l},$$

(b) $$\alpha_{l,2} = (m_1(l) - 1)\frac{m}{m_1(l)},$$

(c) $$\alpha_{l,3} = \frac{3(l-1)}{2}\frac{m}{l} \qquad \textit{(only if } l \neq 2\textit{)}.$$

Further there exist G-Galois extensions of k whose Steinitz classes have $x^{2\alpha_{l,j}}$ as their square. We can choose these extensions so that they satisfy the additional conditions of Lemma 2.1.2.

Proof. By Lemma 2.1.2 there exists a tame G-Galois extension K/k with trivial Steinitz class and such that it 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.

As in Lemma 2.1.2 there are infinitely many prime ideals $\mathfrak{q}$ in the class of x such that the order of $\kappa_{\mathfrak{q}}^*$ is a multiple of $m_1(l)$. Then the class $h_{\mathfrak{q},a}$ of $\tilde{h}_{\mathfrak{q},a}$ modulo $m_1(l)$ is again well defined and there are infinitely many $\mathfrak{q}$ corresponding to the same s-tuple $(h_{\mathfrak{q},u_1}, \dots, h_{\mathfrak{q},u_s})$.

Let $\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{q}_3$ be 3 such prime ideals and let us assume that they are all distinct and that they are prime to a fixed ideal I, to m and to $\mathrm{d}(K/k)$.

(a) Let us define $\varphi_0 : \prod_{\mathfrak{p}} \kappa_{\mathfrak{p}}^* \to G$, posing

$$\begin{cases} \varphi_0(g_{\mathfrak{q}_1}) = \tau_1^{m_1/l} \\ \varphi_0(g_{\mathfrak{q}_2}) = \tau_1^{-m_1/l} \\ \varphi_0(g_{\mathfrak{p}}) = 1 \qquad\qquad \text{for } \mathfrak{p} \notin \{\mathfrak{q}_1, \mathfrak{q}_2\}. \end{cases}$$

As in the previous lemma we can extend φ_0 to a homomorphism

$$\varphi : C_k \to G$$

whose kernel contains $C_k^{\mathfrak{m}}$, where $\mathfrak{m} = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3\mathfrak{f}$ and $\mathfrak{f}$ is the conductor of K/k. Of course

$$\varphi \cdot (\ , K/k) : C_k \to G$$

is surjective and its kernel contains $C_k^{\mathfrak{m}}$. Thus we obtain a G-Galois extension of k, ramifying only in $\mathfrak{q}_1$ and $\mathfrak{q}_2$ with both indices l and in the primes ramifying in K/k with the same ramification indices as in K/k. Hence the extension is tame and the discriminant is

$$\mathrm{d}(K/k)(\mathfrak{q}_1\mathfrak{q}_2)^{(l-1)\frac{m}{l}}.$$

As in Lemma 2.1.2 we can conclude that the class $x^{\eta\alpha_{l,1}}$ is realizable. Further there exist G-Galois extensions of k whose Steinitz classes have $x^{2\alpha_{l,1}}$ as their square.

(b) Now let us define $\varphi_0 : \prod_{\mathfrak{p}} \kappa_{\mathfrak{p}}^* \to G$, posing

$$\begin{cases} \varphi_0(g_{\mathfrak{q}_1}) = \tau_1^{m_1/m_1(l)} \\ \varphi_0(g_{\mathfrak{q}_2}) = \tau_1^{-m_1/m_1(l)} \\ \varphi_0(g_{\mathfrak{p}}) = 1 \qquad\qquad \text{for } \mathfrak{p} \notin \{\mathfrak{q}_1, \mathfrak{q}_2\}. \end{cases}$$

In this case we obtain a tame G-Galois extension of k with discriminant

$$\mathrm{d}(K/k)(\mathfrak{q}_1\mathfrak{q}_2)^{(m_1(l)-1)\frac{m}{m_1(l)}}$$

and as usually we can conclude that the class $x^{\eta\alpha_{l,2}}$ is realizable and that $x^{2\alpha_{l,2}} \in \mathrm{R}_t(k,G)^2$.

(c) We define $\varphi_0 : \prod_{\mathfrak{p}} \kappa_{\mathfrak{p}}^* \to G$, posing

$$\begin{cases} \varphi_0(g_{\mathfrak{q}_1}) = \tau_1^{m_1/l} \\ \varphi_0(g_{\mathfrak{q}_2}) = \tau_1^{m_1/l} \\ \varphi_0(g_{\mathfrak{q}_3}) = \tau_1^{-2m_1/l} \\ \varphi_0(g_{\mathfrak{p}}) = 1 \qquad\qquad \text{for } \mathfrak{p} \notin \{\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{q}_3\}. \end{cases}$$

Then we have a tame G-Galois extension of k, whose discriminant is

$$\mathrm{d}(K/k)(\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3)^{(l-1)\frac{m}{l}}$$

and again we obtain the desired results.

The additional conditions of Lemma 2.1.2 are also verified. □

Lemma 2.1.4. *Let k be a number field, let G be an abelian group of order m, G_2 be its 2-Sylow subgroup and $\tilde{G}$ such that $G = G_2 \times \tilde{G}$. Then*

$$\mathrm{R}_t(k, \tilde{G})^{m(2)} \subseteq \mathrm{R}_t(k, G).$$

Proof. Let $x \in \mathrm{R}_t(k, \tilde{G})$ and let $\tilde{K}/k$ be a $\tilde{G}$-extension of k with Steinitz class x, which is the class of

$$\mathrm{d}(\tilde{K}/k)^{\frac{1}{2}}.$$

Let K/k be a G_2-extension of k with trivial Steinitz class and arithmetically disjoint from $\tilde{K}/k$ (it exists because of Lemma 2.1.2). The Steinitz class of K/k is the class of

$$\left(\frac{\mathrm{d}(K/k)}{\alpha}\right)^{\frac{1}{2}}$$

for a certain $\alpha \in k$. Then the extension $K\tilde{K}/k$ has Galois group $G = G_2 \times \tilde{G}$ and its Steinitz class is the class of

$$\left(\frac{\mathrm{d}(K\tilde{K}/k)}{\alpha^{\frac{m}{m(2)}}}\right)^{\frac{1}{2}} = \mathrm{d}(\tilde{K}/k)^{\frac{m(2)}{2}} \left(\frac{\mathrm{d}(K/k)}{\alpha}\right)^{\frac{m}{2m(2)}}$$

which is $x^{m(2)}$. □

Proposition 2.1.5. *Let $l \neq 2$ be a prime dividing m, then*

$$W(k, m_1(l))^{\frac{l-1}{2}\frac{m}{m_1(l)}} \subseteq \mathrm{R}_t(k, G).$$

If $2|m$ then

$$W(k, m_1(2))^{\eta\frac{m}{m_1(2)}} \subseteq \mathrm{R}_t(k, G)$$

and

$$W(k, m_1(2))^{2\frac{m}{m_1(2)}} \subseteq \mathrm{R}_t(k, G)^2.$$

We can choose the corresponding extensions so that they satisfy the additional conditions of Lemma 2.1.2.

Proof. Let G_2 be the 2-Sylow subgroup of G and $\tilde{G}$ be such that $G = G_2 \times \tilde{G}$. Let $l \neq 2$ be a prime dividing m and let $x \in W(k, m_1(l))$. It follows from Lemma 1.3.8 and Lemma 2.1.3 that x^{β_l} is in $\mathrm{R}_t(k, \tilde{G})$, where

$$\begin{aligned}\beta_l &= \gcd\left((l-1)\frac{m}{m(2)l}, (m_1(l)-1)\frac{m}{m(2)m_1(l)}, \frac{3(l-1)}{2}\frac{m}{m(2)l}\right) \\ &= \gcd\left((m_1(l)-1)\frac{m}{m(2)m_1(l)}, \frac{l-1}{2}\frac{m}{m(2)l}\right).\end{aligned}$$

Clearly $\beta_l(l) = \frac{m(l)}{m_1(l)}$ and, if S is the set of all primes different from l, $\beta_l(S)$ divides $\frac{l-1}{2}\frac{m(S)}{m(2)}$. Thus β_l divides $\frac{l-1}{2}\frac{m}{m(2)m_1(l)}$ and we conclude that

$$x^{\frac{l-1}{2}\frac{m}{m(2)m_1(l)}} \in \mathrm{R}_t(k, \tilde{G}).$$

Hence by Lemma 2.1.4

$$x^{\frac{l-1}{2}\frac{m}{m_1(l)}} \in \mathrm{R}_t(k, G).$$

Now let us assume that $2|m$ and let $x \in W(k, m_1(2))$. It follows from Lemma 1.3.8 and Lemma 2.1.3 that $x^{\eta\beta_2}$ is in $\mathrm{R}_t(k, G)$ and $x^{2\beta_2}$ is in $\mathrm{R}_t(k, G)^2$, where

$$\beta_2 = \gcd\left(\frac{m}{2}, (m_1(2)-1)\frac{m}{m_1(2)}\right).$$

As above we obtain

$$x^{\eta\frac{m}{m_1(2)}} \in \mathrm{R}_t(k, G_1)$$

and

$$x^{2\frac{m}{m_1(2)}} \in \mathrm{R}_t(k, G_1)^2.$$

To conclude we observe that Lemma 1.3.8 preserves the additional conditions of Lemma 2.1.2. □

Lemma 2.1.6. *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. First of all it is clear that we can assume that $m = e$.

Let I be the $\mathbb{Z}$-ideal generated by the $l-1$, for any prime $l|e$. Then $e \equiv 1 \pmod{I}$, since it is the product of prime factors, each one congruent to 1 modulo I. It follows that for any prime $l \nmid e$, there exists an $l_1|e$, such that the l-component of $l_1 - 1$, which coincides with that of $(l_1-1)\frac{e}{e(l_1)}$, divides that of $e-1$. Finally, for any $l|e$, l does not divide $(l-1)\frac{e}{e(l)}$. □

Proposition 2.1.7. *Let k be a number field and let G be an abelian group, then*

$$\mathrm{R}_t(k,G) \subseteq \prod_{l|m} W(k, m_1(l))^{\frac{l-1}{2}\frac{m}{m_1(l)}}.$$

Proof. Let K/k be a tamely ramified extension of number fields with Galois group G. By Theorem 1.3.5 and by Lemma 2.1.6 there exist $b_{e_\mathfrak{p},l} \in \mathbb{Z}$ such that

$$\mathrm{d}(K/k) = \prod_{e_\mathfrak{p}\neq 1} \mathfrak{p}^{(e_\mathfrak{p}-1)\frac{m}{e_\mathfrak{p}}} = \prod_{e_\mathfrak{p}\neq 1}\prod_{l|e_\mathfrak{p}} \mathfrak{p}^{b_{e_\mathfrak{p},l}(l-1)\frac{m}{e_\mathfrak{p}(l)}} = \prod_{l|m}\prod_{e_\mathfrak{p}(l)\neq 1} \mathfrak{p}^{b_{e_\mathfrak{p},l}(l-1)\frac{m}{e_\mathfrak{p}(l)}}.$$

Since K/k is tame, the ramification index $e_\mathfrak{p}$ of a prime $\mathfrak{p}$ in K/k divides m_1. Thus, defining

$$J_l = \prod_{e_\mathfrak{p}(l)\neq 1} \mathfrak{p}^{b_{e_\mathfrak{p},l}\frac{m_1(l)}{e_\mathfrak{p}(l)}},$$

we obtain

$$\mathrm{d}(K/k) = \prod_{l|m} J_l^{(l-1)\frac{m}{m_1(l)}}$$

and by Lemma 1.2.15 and Lemma 1.2.18 the class of the ideal J_l belongs to $W(k, m_1(l))$. We easily conclude by Theorem 1.3.6. □

The characterization of the realizable Steinitz classes of abelian extensions of odd order follows easily from the results proved in this section.

Theorem 2.1.8. *Let k be a number field and let $G = C(m_1) \times \cdots \times C(m_r)$ with $m_{i+1}|m_i$ be an abelian group of odd order. Then*

$$\mathrm{R}_t(k,G) = \prod_{l|m} W(k, m_1(l))^{\frac{l-1}{2}\frac{m}{m_1(l)}}.$$

Proof. This follows from Lemma 1.3.8, Proposition 2.1.5 and Proposition 2.1.7. □

2.2 Cyclic extensions of 2-power degree

In this section we recall some results concerning cyclic extensions of 2-power degree, obtained by Lawrence P. Endo in his PhD thesis [9]. Unfortunately Endo could not determine the corresponding realizable classes in the most general case and it does not seem possible to obtain any interesting result with the techniques from class field theory developed in the preceding section.

The following proposition is the only result we can prove by class field theory.

Proposition 2.2.1. *Let k be a number field with an odd class number and let $G = C(2^n) = \langle\sigma\rangle$. Then*

$$\mathrm{R}_t(k, G) = W(k, 2^n).$$

Proof. By Proposition 2.1.5 and Proposition 2.1.7

$$W(k, 2^n)^2 \subseteq \mathrm{R}_t(k, C(2^n)) \subseteq W(k, 2^n)^{1/2}.$$

Since the class number is odd,

$$W(k, 2^n) = W(k, 2^n)^2 = W(k, 2^n)^{1/2},$$

and this concludes the proof. □

We recall the following well-known lemma.

Lemma 2.2.2. *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

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

and so

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

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

Proposition 2.2.3. *Let k be any number field, then*

$$\mathrm{R}_t(k, C(2)) = \mathrm{Cl}(k).$$

We can choose $C(2)$-extensions with a given Steinitz class so that they satisfy the additional conditions of Lemma 2.1.2.

Proof. Let $x \in \mathrm{Cl}(k)$ be any ideal class and let $\mathfrak{q}_1$ and $\mathfrak{q}_2$ be prime ideals in it, which are in the same ray class modulo 4. Thanks to Proposition 1.2.8, we can choose a prime ideal $\mathfrak{q}_0$ in the ray class modulo 4, which is inverse to that of $\mathfrak{q}_1$ and $\mathfrak{q}_2$.

By construction, $\mathfrak{q}_0^2\mathfrak{q}_1\mathfrak{q}_2$ is principal generated by an $\alpha \equiv 1 \pmod 4$. It follows from Theorem 1.3.6 that

$$D = \frac{\mathrm{d}(k(\sqrt{\alpha})/k)}{\alpha}$$

is the square of a fractional ideal and by Lemma 2.2.2 the extension $k(\sqrt{\alpha})/k$ is tame. In particular all the primes dividing $\mathrm{d}(k(\sqrt{\alpha})/k)$ appear with exponent 1 in its factorization. Then, since $(\alpha) = \mathfrak{q}_0^2\mathfrak{q}_1\mathfrak{q}_2$, the only possibility for D to be a square, is that it equals $\mathfrak{q}_0^{-2}$. Then, again by Theorem 1.3.6, the Steinitz class of $k(\sqrt{\alpha})/k$ is x. □

In the next section we will use the following proposition proved by Endo.

Proposition 2.2.4. *For any number field k*

$$W(k, 2^n) \subseteq \mathrm{R}_t(k, C(2^n)).$$

Proof. This is Proposition II.2.4 in [9]. □

Further Endo proved the following result, which determines the realizable classes if the extension $k(\zeta_{2^n})/k$ is cyclic.

Proposition 2.2.5. *Suppose* $\mathrm{Gal}(k(\zeta_{2^n})/k)$ *is cyclic. Then*

$$\mathrm{R}_t(k, C(2^n)) = W(k, 2^n)$$

unless $k(\zeta_{2^n})/k$ is unramified and $\mathrm{Gal}(k(\zeta_{2^n})/k) = \langle -5^{2^t} \rangle$, $0 \leq t \leq n-2$, *in which case*

$$\mathrm{R}_t(k, C(2^n)) = W(k, 2^n)^{\frac{1}{2}}.$$

Proof. This is Proposition II.2.6 in [9]. □

From the above result James E. Carter and Bouchaïb Sodaïgui in [7] deduced the following proposition, which they used to study generalized quaternions extensions.

Proposition 2.2.6. *Let k be a number field and $C(4)$ the cyclic group of order 4. Then $\mathrm{R}_t(k, C(4)) = \mathrm{Cl}(k)$. Further, for any $x \in \mathrm{Cl}(k)$ and any ideal I in O_k, there exists a tame cyclic extension K/k of degree 4 such that $\mathrm{st}(K/k) = x$, whose discriminant is prime to I and such that any nontrivial subextension of K/k is ramified.*

Proof. It is Proposition 2.6 of [7]. □

2.3 Abelian extensions of even degree

In this section we relate the realizable Steinitz classes of abelian extensions of even degree to those of cyclic extensions of order a power of 2. In this way we also obtain some definitive results in a few particular situations.

Lemma 2.3.1. *If $2|m$ and $m_2(2) \neq 1$ then*

$$W(k, m_2(2))^{\frac{m}{2m_2(2)}} \subseteq \mathrm{R}_t(k, G).$$

We can choose the corresponding extensions so that they satisfy the additional conditions of Lemma 2.1.2.

Proof. By Lemma 2.1.2 there exists a tame G-Galois extension K/k with trivial Steinitz class and such that it 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. We can choose three prime ideals $\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{q}_3$ whose ideal class is a fixed $x \in W(k, m_2(2))$ and which satisfy analogous conditions as in Lemma 2.1.3.

Now let us define $\varphi_0 : \prod_{\mathfrak{p}} \kappa_{\mathfrak{p}}^* \to G$, posing

$$\begin{cases} \varphi_0(g_{\mathfrak{q}_1}) = \tau_1^{m_1/m_2(2)} \\ \varphi_0(g_{\mathfrak{q}_2}) = \tau_2^{m_2/m_2(2)} \\ \varphi_0(g_{\mathfrak{q}_3}) = \tau_1^{-m_1/m_2(2)} \tau_2^{-m_2/m_2(2)} \\ \varphi_0(g_{\mathfrak{p}}) = 1 \qquad\qquad\qquad\qquad \text{for } \mathfrak{p} \notin \{\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{q}_3\}. \end{cases}$$

As in Lemma 2.1.3 we obtain a tame G-Galois extension of k with discriminant

$$\mathrm{d} = \mathrm{d}(K/k)(\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3)^{(m_2(2)-1)\frac{m}{m_2(2)}}$$

and the Steinitz class is $x^{\alpha_{2,4}}$, where

$$\alpha_{2,4} = 3(m_2(2) - 1)\frac{m}{2m_2(2)}.$$

By Proposition 2.1.5,

$$x^{\frac{m}{m_2(2)}} = x^{\frac{m_1(2)}{m_2(2)}\frac{m}{m_1(2)}} \in \mathrm{R}_t(k, G),$$

since $x^{m_1(2)/m_2(2)} \in W(k, m_1(2))$ by Lemma 1.2.18. Thus

$$x^{\frac{m}{2m_2(2)}} = x^{\gcd\left(\alpha_{2,4}, \frac{m}{m_2(2)}\right)} \in \mathrm{R}_t(k, G).$$

□

Using this lemma we can easily prove a first interesting proposition, which gives a characterization of realizable classes in a particular situation.

Proposition 2.3.2. *Let k be a number field, let $G = C(m_1) \times \cdots \times C(m_r)$, with $m_{i+1}|m_i$, be an abelian group of order m. If $2|m$ and $m_1(2) = m_2(2)$, then*

$$\mathrm{R}_t(k, G) = \prod_{l|m} W(k, m_1(l))^{\frac{l-1}{2}\frac{m}{m_1(l)}}.$$

The result is the same as in the odd order case (see Theorem 2.1.8).

Further we can choose G-extensions with a given Steinitz class so that they satisfy the additional conditions of Lemma 2.1.2.

Proof. One inclusion is Proposition 2.1.7.

The other inclusion follows by Proposition 2.1.5 and Lemma 2.3.1, using Lemma 1.3.8. □

Lemma 2.3.3. *If $2|m$ then*

$$\mathrm{R}_t(k, C(m_1(2)))^{\frac{m}{m_1(2)}} \subseteq \mathrm{R}_t(k, G).$$

Proof. By hypothesis $G = C(m_1(2)) \times \tilde{G}$, where $\tilde{G}$ is an abelian group. Let $x \in \mathrm{R}_t(k, C(m_1(2)))$ and let L be a tame $C(m_1(2))$-extension whose Steinitz class is x. Because of Lemma 2.1.2 there exists a tame $\tilde{G}$-extension K of k whose discriminant is prime to that of L over k, with trivial Steinitz class and with no unramified subextensions. The composition of the two extensions is a G-extension and its discriminant is

$$\mathrm{d}(L/k)^{\frac{m}{m_1(2)}}\mathrm{d}(K/k)^{m_1(2)}.$$

If the 2-Sylow subgroup of G is not cyclic then the Steinitz class is the class of

$$\mathrm{d}(KL/k)^{\frac{1}{2}} = \mathrm{d}(L/k)^{\frac{m}{2m_1(2)}}\mathrm{d}(K/k)^{m_1(2)/2},$$

that is

$$(x^2)^{\frac{m}{2m_1(2)}} = x^{\frac{m}{m_1(2)}}.$$

Now we have to consider the case in which the 2-Sylow subgroup of G is cyclic. The subextension $k(\sqrt{\alpha})$ of L of degree 2 over k is also a subextension of KL. We have $k(\sqrt{\alpha}) = k\left(\sqrt{\alpha^{\frac{m}{m_1(2)}}}\right)$ (the exponent $\frac{m}{m_1(2)}$ is odd) and so the Steinitz class of KL/k is the class of the square root of

$$\frac{\mathrm{d}(KL/k)}{\alpha^{\frac{m}{m_1(2)}}} = \left(\frac{\mathrm{d}(L/k)}{\alpha}\right)^{\frac{m}{m_1(2)}}\mathrm{d}(K/k)^{m_1(2)},$$

that is exactly $x^{\frac{m}{m_1(2)}}$. □

Lemma 2.3.4. *If $2|m$ and $m_2(2) \neq 1$ then*

$$\mathrm{R}_t(k,G) \subseteq \mathrm{R}_t(k, C(m_1(2)))^{\frac{m}{m_1(2)}} \cdot W(k, m_2(2))^{\frac{m}{2m_2(2)}} \cdot \prod_{\substack{l|m \\ l\neq 2}} W(k, m_1(l))^{\frac{l-1}{2}\frac{m}{m_1(l)}}.$$

Proof. Let K/k be a G-Galois extension whose Steinitz class is $x \in \mathrm{R}_t(k,G)$ and let L be a subextension of K/k whose Galois group over k is the first component of the 2-Sylow subgroup $C(m_1(2)) \times \cdots \times C(m_r(2))$ of G. By Theorem 1.1.8 and Proposition 1.1.9

$$\begin{aligned} e_{\mathfrak{p},K} &= e_{\mathfrak{p},K}(2)e'_{\mathfrak{p},K} = \#([U_\mathfrak{p}], K/k); \\ e_{\mathfrak{p},L} &= e_{\mathfrak{p},L}(2) = \#([U_\mathfrak{p}], L/k) = \#([U_\mathfrak{p}], K/k)|_L, \end{aligned}$$

where $e_{\mathfrak{p},L}$ and $e_{\mathfrak{p},K}$ are the ramification indices of $\mathfrak{p}$ in L and K respectively and $e'_{\mathfrak{p},K}$ is odd. By Theorem 1.3.5 and Theorem 1.3.6, x is the class of

$$\prod_{\mathfrak{p}} \mathfrak{p}^{\frac{e_{\mathfrak{p},K}-1}{2}\frac{m}{e_{\mathfrak{p},K}}}.$$

The class x_1 of the ideal

$$\prod_{\mathfrak{p}} \mathfrak{p}^{\frac{e_{\mathfrak{p},L}-1}{2}\frac{m}{e_{\mathfrak{p},L}}}$$

is the $m/m_1(2)$-th power of the Steinitz class of L/k and thus

$$x_1 \in \mathrm{R}_t(k, C(m_1(2)))^{\frac{m}{m_1(2)}}.$$

Since $e_{\mathfrak{p},L}|e_{\mathfrak{p},K}(2)$ and $2e_{\mathfrak{p},K}(2)|m$ we can define x_2 as the class of

$$\prod_{\mathfrak{p}} \mathfrak{p}^{\left(\frac{e_{\mathfrak{p},K}(2)}{e_{\mathfrak{p},L}}-1\right)\frac{m}{2e_{\mathfrak{p},K}(2)}} = \prod_{\mathfrak{p}} \mathfrak{p}^{\left(\frac{e_{\mathfrak{p},K}(2)}{e_{\mathfrak{p},L}}-1\right)\frac{m_2(2)}{e_{\mathfrak{p},K}(2)}\frac{m}{2m_2(2)}}.$$

The only primes for which we obtain a nontrivial contribution are those for which $e_{\mathfrak{p},L} < e_{\mathfrak{p},K}(2)$ and for those we must have $e_{\mathfrak{p},K}(2)|m_2(2)$ (since $e_{\mathfrak{p},K}(2)$ must then be the order of a cyclic subgroup of $C(m_2(2)) \times \cdots \times C(m_r(2))$) and thus, recalling Lemma 1.2.15 and Lemma 1.2.18,

$$x_2 \in W(k, m_2(2))^{\frac{m}{2m_2(2)}}.$$

Let x_3 be the class of

$$\prod_{\mathfrak{p}} \mathfrak{p}^{\frac{e'_{\mathfrak{p},K}-1}{2}\frac{m}{e_{\mathfrak{p},K}}} = \prod_{\mathfrak{p}} \mathfrak{p}^{a_\mathfrak{p}\frac{e'_{\mathfrak{p},K}-1}{2}\frac{m}{e'_{\mathfrak{p},K}}} \prod_{\mathfrak{p}} \mathfrak{p}^{b_\mathfrak{p}\frac{e'_{\mathfrak{p},K}-1}{2}\frac{m}{e_{\mathfrak{p},K}(2)}},$$

where $a_{\mathfrak{p}}$ and $b_{\mathfrak{p}}$ are integers such that

$$\frac{m}{e_{\mathfrak{p},K}} = a_{\mathfrak{p}}\frac{m}{e'_{\mathfrak{p},K}} + b_{\mathfrak{p}}\frac{m}{e_{\mathfrak{p},K}(2)}.$$

By Lemma 2.1.6 there exist $b_{\mathfrak{p},l} \in \mathbb{Z}$ such that

$$\prod_{\mathfrak{p}} \mathfrak{p}^{a_{\mathfrak{p}}\frac{e'_{\mathfrak{p},K}-1}{2}\frac{m}{e'_{\mathfrak{p},K}}} = \prod_{\substack{l|m\\ l\neq 2}}\prod_{\mathfrak{p}} \mathfrak{p}^{b_{\mathfrak{p},l}\frac{m_1(l)}{e'_{\mathfrak{p},K}(l)}\frac{l-1}{2}\frac{m}{m_1(l)}}$$

and thus by Lemma 1.2.15 and Lemma 1.2.18 the class of this ideal is in

$$\prod_{\substack{l|m\\ l\neq 2}} W(k, m_1(l))^{\frac{l-1}{2}\frac{m}{m_1(l)}}.$$

By the same lemmas the class of

$$\prod_{\mathfrak{p}} \mathfrak{p}^{b_{\mathfrak{p}}\frac{e'_{\mathfrak{p},K}-1}{2}\frac{m}{e_{\mathfrak{p},K}(2)}}$$

is in

$$W(k, m_1(2))^{\frac{m}{m_1(2)}},$$

which is contained in

$$\mathrm{R}_t(k, C(m_1(2)))^{\frac{m}{m_1(2)}}$$

by Proposition 2.2.4. Hence

$$x_3 \in \prod_{\substack{l|m\\ l\neq 2}} W(k, m_1(l))^{\frac{l-1}{2}\frac{m}{m_1(l)}}\mathrm{R}_t(k, C(m_1(2)))^{\frac{m}{m_1(2)}}.$$

By an easy calculation

$$\frac{e_{\mathfrak{p},K}-1}{2}\frac{m}{e_{\mathfrak{p},K}} = \frac{e_{\mathfrak{p},L}-1}{2}\frac{m}{e_{\mathfrak{p},L}} + \left(\frac{e_{\mathfrak{p},K}(2)}{e_{\mathfrak{p},L}} - 1\right)\frac{m}{2e_{\mathfrak{p},K}(2)} + \frac{e'_{\mathfrak{p},K}-1}{2}\frac{m}{e_{\mathfrak{p},K}}$$

and we conclude that $x = x_1x_2x_3$, obtaining the desired inclusion. □

Theorem 2.3.5. *Let k be a number field, let $G = C(m_1) \times \cdots \times C(m_r)$, with $m_{i+1}|m_i$, be an abelian group of order m. If $2|m$ and $m_2(2) \neq 1$ then*

$$\mathrm{R}_t(k, G) = \mathrm{R}_t(k, C(m_1(2)))^{\frac{m}{m_1(2)}} \cdot W(k, m_1(2))^{\frac{m}{2m_2(2)}} \cdot \prod_{\substack{l|m\\ l\neq 2}} W(k, m_1(l))^{\frac{l-1}{2}\frac{m}{m_1(l)}}.$$

Proof. $\subseteq$ This is Lemma 2.3.4.

$\supseteq$ This follows by Proposition 2.1.5, by Lemma 2.3.1 and by Lemma 2.3.3, using Lemma 1.3.8.

□

Remark. The only unknown term in the expression for $\mathrm{R}_t(k,G)$ in the above theorem is $\mathrm{R}_t(k,C(m_1(2)))$. But we really need to determine only its square, because it appears with an even exponent. This simplifies the problem, because this allows us to consider directly the discriminants of the extensions.

In the second part of the section we consider the case in which the 2-Sylow subgroup of G is cyclic, i.e. $2|m$ and $m_2(2)=1$.

Lemma 2.3.6. *If the 2-Sylow subgroup of G is cyclic, i.e. $2|m$ and $m_2(2)=1$, then*

$$\mathrm{R}_t(k,G) \subseteq \mathrm{R}_t(k,C(m_1(2)))^{\frac{m}{m_1(2)}} \cdot \prod_{\substack{l|m \\ l\neq 2}} W(k,m_1(l))^{\frac{l-1}{2}\frac{m}{m_1(l)}}.$$

Proof. Let K/k be a G-Galois extension whose Steinitz class is $x \in \mathrm{R}_t(k,G)$ and let L be the subextension of K/k whose Galois group over k is the 2-Sylow subgroup $C(m_1(2))$ of G. By Theorem 1.1.8 and Proposition 1.1.9

$$\begin{aligned} e_{\mathfrak{p},K} &= e_{\mathfrak{p},K}(2)e'_{\mathfrak{p},K} = \#([U_\mathfrak{p}],K/k); \\ e_{\mathfrak{p},L} &= e_{\mathfrak{p},L}(2) = \#([U_\mathfrak{p}],L/k) = \#([U_\mathfrak{p}],K/k)|_L, \end{aligned}$$

where $e_{\mathfrak{p},L}$ and $e_{\mathfrak{p},K}$ are the ramification indices of $\mathfrak{p}$ in L and K respectively, $e'_{\mathfrak{p},K}$ is odd and $e_{\mathfrak{p},K}(2) = e_{\mathfrak{p},L}(2)$. Let $\alpha \in k$ be such that $k \subsetneq k(\sqrt{\alpha}) \subseteq L$.

Since $k(\sqrt{\alpha}) = k\left(\sqrt{\alpha^{m/m_1(2)}}\right)$, by Theorem 1.3.5 and Theorem 1.3.6, x is the class of

$$\left(\frac{\prod_\mathfrak{p} \mathfrak{p}^{(e_{\mathfrak{p},K}-1)\frac{m}{e_{\mathfrak{p},K}}}}{\alpha^{\frac{m}{m_1(2)}}}\right)^{\frac{1}{2}}.$$

As in the proof of Lemma 2.3.4 we can define

$$x_1 \in \mathrm{R}_t(k,C(m_1(2)))^{\frac{m}{m_1(2)}} \cdot \prod_{\substack{l|m \\ l\neq 2}} W(k,m_1(l))^{\frac{l-1}{2}\frac{m}{m_1(l)}}.$$

as the class of the ideal

$$\prod_{\mathfrak{p}} \mathfrak{p}^{\frac{e'_{\mathfrak{p},K}-1}{2}\frac{m}{e_{\mathfrak{p},K}}}.$$

By Theorem 1.3.5 and Theorem 1.3.6,

$$\left(\frac{\prod_{\mathfrak{p}} \mathfrak{p}^{(e_{\mathfrak{p},L}-1)\frac{m_1(2)}{e_{\mathfrak{p},L}}}}{\alpha}\right)^{\frac{m}{2m_1(2)}}$$

is an ideal, whose class x_2 is the $m/m_1(2)$-th power of the Steinitz class of L/k. Thus

$$x_2 \in \mathrm{R}_t(k, C(m_1(2)))^{\frac{m}{m_1(2)}}.$$

By an easy calculation

$$\left(\frac{\prod_{\mathfrak{p}} \mathfrak{p}^{(e_{\mathfrak{p},K}-1)\frac{m}{e_{\mathfrak{p},K}}}}{\alpha^{\frac{m}{m_1(2)}}}\right)^{\frac{1}{2}} = \prod_{\mathfrak{p}} \mathfrak{p}^{\frac{e'_{\mathfrak{p},K}-1}{2}\frac{m}{e_{\mathfrak{p},K}}} \left(\frac{\prod_{\mathfrak{p}} \mathfrak{p}^{(e_{\mathfrak{p},L}-1)\frac{m_1(2)}{e_{\mathfrak{p},L}}}}{\alpha}\right)^{\frac{m}{2m_1(2)}}$$

and we conclude that $x = x_1 x_2$, from which we obtain the desired inclusion. □

Theorem 2.3.7. *Let k be a number field, let $G = C(m_1) \times \cdots \times C(m_r)$, with $m_{i+1}|m_i$, be an abelian group of order m. If $2|m$ and $m_2(2) = 1$ then*

$$\mathrm{R}_t(k, G) = \mathrm{R}_t(k, C(m_1(2)))^{\frac{m}{m_1(2)}} \prod_{\substack{l|m \\ l\neq 2}} W(k, m_1(l))^{\frac{l-1}{2}\frac{m}{m_1(l)}}.$$

Proof. $\subseteq$ This is Lemma 2.3.6.

$\supseteq$ This follows by Lemma 2.3.3, Proposition 2.1.5 and Lemma 1.3.8.

□

We conclude this section with an interesting corollary.

Corollary 2.3.8. *Let k be a number field, let G be an abelian group of order m and let G_l be its l-Sylow subgroup for any prime $l|m$. Then*

$$\mathrm{R}_t(k, G) = \prod_{l|m} \mathrm{R}_t(k, G_l)^{\frac{m}{m(l)}}.$$

Proof. This is immediate by Theorem 2.1.8, Theorem 2.3.5 and Theorem 2.3.7. □

In the next chapter we will prove a similar result concerning a relation between the realizable classes for two groups and for their direct product, in a quite general situation, which however does not include abelian groups of even order. Thus the above corollary will not follow from Theorem 3.2.15.

Chapter 3

Nonabelian extensions

In this chapter we will study some nonabelian extensions, with an abelian normal subgroup. In the first section we obtain some very general results, which are used in the second section to describe the realizable classes for a particular class of nonabelian groups of odd order. In the last two sections we obtain results for the Steinitz classes in some more cases, which have not been considered in the second section. The theorems proved in this chapter are the main results of this PhD thesis.

3.1 General results

Let $\mathcal{G}$ 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

$$\mu : \mathcal{G} \to \mathrm{Aut}(H)$$

be an action of $\mathcal{G}$ on H and let

$$0 \to H \xrightarrow{\varphi} G \xrightarrow{\psi} \mathcal{G} \to 0$$

be an exact sequence of groups such that the induced action of $\mathcal{G}$ on H is μ. We assume that the group G is determined, up to isomorphism, by the above exact sequence and by the action μ. We are going to study $\mathrm{R}_t(k, G)$. The following well-known proposition shows a class of situations in which our assumption is true.

Proposition 3.1.1 (Schur-Zassenhaus, 1937)**.** *If the order of H is prime to the order of $\mathcal{G}$ then G is a semidirect product:*

$$G \cong H \rtimes_\mu \mathcal{G}.$$

Proof. This is Theorem 7.41 in [21]. □

As in the abelian case we also define

$$\eta_G = \begin{cases} 1 & \text{if } 2 \nmid n \text{ or the 2-Sylow subgroups of } G \text{ are not cyclic} \\ 2 & \text{if } 2|n \text{ and the 2-Sylow subgroups of } G \text{ are cyclic} \end{cases}$$

and in a similar way we define η_H and $\eta_{\mathcal{G}}$. We continue to use the letter l only for prime numbers, even if not explicitly indicated.

We say that (K, k_1, k) is of type μ if k_1/k, K/k_1 and K/k are Galois extensions with Galois groups isomorphic to $\mathcal{G}$, H and G respectively and such that the action of $\mathrm{Gal}(k_1/k) \cong \mathcal{G}$ on $\mathrm{Gal}(K/k_1) \cong H$ is given by μ. For any $\mathcal{G}$-extension k_1 of k we define $\mathrm{R}_t(k_1, k, \mu)$ 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 μ.

It will be useful to have a generalization of Lemma 1.3.8.

Lemma 3.1.2. *Let (K_1, k_1, k) and (K_2, k_1, k) be extensions of type μ, such that $(\mathrm{d}(K_1/k_1), \mathrm{d}(K_2/k_1)) = 1$ and K_1/k_1 and K_2/k_1 have no nontrivial unramified subextensions. Then there exists an extension (K, k_1, k) of type μ, such that $K \subseteq K_1K_2$ and for which*

$$\mathrm{st}(K/k_1) = \mathrm{st}(K_1/k_1)\mathrm{st}(K_2/k_1).$$

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 $\mathcal{G} \cong \mathrm{Gal}(k_1/k)$ on $H \cong \mathrm{Gal}(K_i/k_1)$ given by conjugation coincides with μ. Let us embed H into $\mathrm{Gal}(K_1K_2/k_1)$ by means of the corresponding diagonal map

$$\mathrm{diag} : H \to \mathrm{Gal}(K_1/k_1) \times \mathrm{Gal}(K_2/k_1) \cong \mathrm{Gal}(K_1K_2/k_1).$$

Let K be the fixed field of $\mathrm{diag}(H)$. Then, by Lemma 1.3.8, we know that $\mathrm{Gal}(K/k_1) \cong H$ and that

$$\mathrm{st}(K/k_1) = \mathrm{st}(K_1/k_1)\mathrm{st}(K_2/k_1).$$

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

$$\mathrm{Gal}(K_1K_2/k_1) \cong \mathrm{Gal}(K_1/k_1) \times \mathrm{Gal}(K_2/k_1)$$

is given by

$$\tilde{\mu}(g)((h_1, h_2)) = (\mu(g)(h_1), \mu(g)(h_2)).$$

It follows that the action of $\mathcal{G} \cong \mathrm{Gal}(k_1/k)$ on

$$\mathrm{Gal}(K/k_1) = \mathrm{Gal}(K_1K_2/k_1)/\mathrm{diag}(H) \cong H$$

(where the last isomorphism is given by the projection on the first component) coincides with the action μ. Hence (K, k_1, k) is of type μ. □

For any $\tau \in H$ and for any prime l dividing the order $o(\tau)$ of τ we define the element

$$\tau(l) = \tau^{\frac{o(\tau)}{o(\tau)(l)}}$$

in the l-Sylow subgroup $H(l)$ of H.

We now recall some definitions and a classical result.

Definition 3.1.3. *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 $\mathrm{res}^G_H(M)$, 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 3.1.4. *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 $\mathrm{ind}^G_H(L)$, given by*

$$\mathrm{ind}^G_H(L) = R[G] \otimes_{R[H]} L.$$

Theorem 3.1.5 (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*

$$\tau : \mathrm{Hom}_{R[H]}(L, \mathrm{res}^G_H(M)) \to \mathrm{Hom}_{R[G]}(\mathrm{ind}^G_H(L), M).$$

This isomorphism is such that

$$(\tau f)(g \otimes l) = g \cdot f(l).$$

Proof. This is Theorem 10.8 in [8]. The explicit description of τ may be deduced from the proof. □

We will only use the above result with $R = \mathbb{Z}$.

Let k_1/k be an extension of number fields with Galois group $\mathcal{G}$. 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 $\mathrm{Cl}(k_1)$ (they exist because of Proposition 1.2.8) and let $\mathfrak{P}_i^{h_i} = (\alpha_i)$, where h_i is the order of x_i.

Let $\pi_{\mathfrak{P}_i}$ be a prime element in the completion $(k_1)_{\mathfrak{P}_i}$ of k_1 with respect to $|\cdot|_{\mathfrak{P}_i}$ and let $y_i = [\pi_{\mathfrak{P}_i}] \in I_{k_1}$. 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 $\delta \in \mathcal{G}$ 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 $1 \to \prod_{\mathfrak{P}} U_{\mathfrak{P}}/U_{k_1} \to C_{k_1} \to \mathrm{Cl}(k_1) \to 1$) be such that

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

Let $\{u_1, \dots, u_s\}$ be the union of a system of generators of the abelian group U_{k_1} with $\{a_1, \dots, a_t\}$ and $\bigcup_{\delta\in\mathcal{G}}\{b_{\delta,1}, \dots, b_{\delta,t}\}$.

Let ι be the map from the class group of k to the class group of k_1 which is induced by the map which pushes up ideals of k to ideals of k_1.

Now we can easily generalize some results obtained for abelian extensions. Lemma 2.1.2, for example, becomes the following.

Lemma 3.1.6. *Let k_1 be a tame $\mathcal{G}$-extension of k and let $x \in W(k, k_1(\zeta_{n_1}))$. Then there exist tame extensions of k_1 of type μ, whose Steinitz classes (over k_1) are $\iota(x)^{\eta_H \alpha}$, where*

$$\alpha = \sum_{i=1}^{r} \frac{n_i - 1}{2} \frac{n}{n_i} + \frac{n_1 - 1}{2} \frac{n}{n_1}.$$

In particular there exist tame extensions of k_1 of type μ with trivial Steinitz class. We can choose these extensions so that they satisfy the additional conditions of Lemma 2.1.2.

Proof. By Proposition 1.2.12, x contains infinitely many primes $\mathfrak{q}$ of absolute degree 1 splitting completely in $k_1(\zeta_{n_1})$. Let $\mathfrak{q}$ be any such prime and let $\mathfrak{q}\mathcal{O}_{k_1} = \prod_{\delta\in\mathcal{G}} \delta(\mathfrak{Q})$ be its decomposition in k_1, let $g_{\mathfrak{Q}}$ be a generator of $\kappa^*_{\mathfrak{Q}} = U_{\mathfrak{Q}}/U^1_{\mathfrak{Q}}$. Now δ 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 $\delta \in \mathcal{G}$. 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 $g_{\mathfrak{P}}^{\tilde{h}_{\mathfrak{P},a}} \equiv a_{\mathfrak{P}} \pmod{\mathfrak{P}}$.

For any prime $\delta(\mathfrak{Q})$, dividing a prime $\mathfrak{q}$ of absolute degree 1 splitting completely in $k_1(\zeta_{n_1})$, let $h_{\delta(\mathfrak{Q}),a}$ be the class of $\tilde{h}_{\delta(\mathfrak{Q}),a}$ modulo n_1 (since $\delta(\mathfrak{Q})$ is of absolute degree 1, it follows by Lemma 1.2.13 that the order of $g_{\delta(\mathfrak{Q})}$ is a multiple of n_1, i.e. that $h_{\delta(\mathfrak{Q}),a}$ is well defined). The set of all the possible ms-tuples

$$(h_{\delta(\mathfrak{Q}),u_j})_{\delta\in\mathcal{G};\ j=1,\dots,s}$$

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

Let $\mathfrak{q}_1, \dots, \mathfrak{q}_{r+1}$ be $r+1$ such prime ideals and $\mathfrak{Q}_1, \dots, \mathfrak{Q}_{r+1}$ 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 $\mathfrak{P}_1, \dots, \mathfrak{P}_t$.

Now let us define $\varphi_i : \kappa^*_{\mathfrak{Q}_i} \to H$, posing

$$\varphi_i(g_{\mathfrak{Q}_i}) = \tau_i,$$

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

$$\varphi_{r+1}(g_{\mathfrak{Q}_{r+1}}) = (\tau_1 \dots \tau_r)^{-1}.$$

Then we extend φ_i to

$$\tilde{\varphi}_i : \mathrm{ind}^{\mathcal{G}}_{\langle 1 \rangle} \kappa^*_{\mathfrak{Q}_i} \cong \prod_{\delta \in \mathcal{G}} \kappa^*_{\delta(\mathfrak{Q}_i)} \to H$$

using Theorem 3.1.5.

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

$$\begin{cases} \varphi_0|_{\kappa^*_{\delta(\mathfrak{Q}_i)}} = \tilde{\varphi}_i & \text{for } i = 1, \dots, r+1 \text{ and } \delta \in \mathcal{G} \\ \varphi_0|_{\kappa^*_{\mathfrak{P}}} = 1 & \text{for } \mathfrak{P} \nmid \mathfrak{q}_1, \dots, \mathfrak{q}_{r+1}. \end{cases}$$

By construction φ_0 is $\mathcal{G}$-invariant and hence, for any $\delta \in \mathcal{G}$,

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

It follows that $\varphi_0(u_j) = 1$ for $j = 1, \dots, s$ and thus, as in Lemma 2.1.2, we can extend φ_0 to a surjective homomorphism $\varphi : C_{k_1} \to H$, whose kernel contains a congruence subgroup of C_{k_1}. We can also assume that $\varphi(y_j) = 1$, for all j. It follows from Theorem 1.1.8 that there is an H-Galois extension of k_1, ramifying only in the primes above $\mathfrak{q}_1, \dots, \mathfrak{q}_{r+1}$, with indices n_i for $i \in \{1, \dots, r\}$ and n_1 for $j = r+1$.

Further the action of an element of $\mathcal{G}$ on one of the y_j gives a combination of some $b_{\delta,i}$ and y_j, on which φ is trivial. Recalling that φ_0 is $\mathcal{G}$-invariant, it follows that also the homomorphism φ is $\mathcal{G}$-invariant and so, by Proposition 1.1.11 and the assumption that G is identified by the exact sequence

$$1 \to H \to G \to \mathcal{G} \to 1$$

and by the action μ, we obtain an extension of type μ. Its discriminant is

$$\mathrm{d} = \left(\prod_{i=1}^{r} \mathfrak{q}_i^{(n_i - 1)\frac{n}{n_i}} \right) \mathfrak{q}_{r+1}^{(n_1 - 1)\frac{n}{n_1}} \mathcal{O}_{k_1}$$

and so its Steinitz class has $\iota(x)^{2\alpha}$ as its square. We conclude as in Lemma 2.1.2. □

For any $\tau \in H$ we define

$$\tilde{\mu}_{k,\mu,\tau} : \mathcal{G} \times \mathrm{Gal}(k(\zeta_{o(\tau)})/k) \to \mathrm{Aut}(H)$$

by $\tilde{\mu}_{k,\mu,\tau}((g_1, g_2)) = \mu(g_1)$ for any $(g_1, g_2) \in \mathcal{G} \times \mathrm{Gal}(k(\zeta_{o(\tau)})/k)$ and

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

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

$$\begin{aligned}\tilde{G}_{k,\mu,\tau} &= \left\{ g \in \mathcal{G} \times \mathrm{Gal}(k(\zeta_{o(\tau)})/k) :\ \tilde{\mu}_{k,\mu,\tau}(g)(\tau) = \tau^{\tilde{\nu}_{k,\mu,\tau}(g)} \right\} \\ &= \left\{ (g_1, g_2) \in \mathcal{G} \times \mathrm{Gal}(k(\zeta_{o(\tau)})/k) :\ \mu(g_1)(\tau) = \tau^{\nu_{k,\tau}(g_2)} \right\}.\end{aligned}$$

We define

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

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

Lemma 3.1.7. *For any $\tau \in H$, $G_{k,\mu,\tau}$ is a subgroup of* $\mathrm{Gal}(k(\zeta_{o(\tau)})/k)$.

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

$$\begin{aligned}\tau^{\tilde{\nu}_{k,\mu,\tau}((g_1\tilde{g}_1, g_2\tilde{g}_2))} &= \tau^{\nu_{k,\tau}(g_2)\nu_{k,\tau}(\tilde{g}_2)} = \mu(g_1)\left(\tau^{\nu_{k,\tau}(\tilde{g}_2)}\right) \\ &= \mu(g_1)(\mu(\tilde{g}_1)(\tau)) = \tilde{\mu}_{k,\mu,\tau}((g_1\tilde{g}_1, g_2\tilde{g}_2))(\tau)\end{aligned}$$

and

$$\begin{aligned}\tau^{\tilde{\nu}_{k,\mu,\tau}\left(\left(g_1^{-1}, g_2^{-1}\right)\right)} &= \tau^{\nu_{k,\tau}(g_2)^{-1}} = \mu\left(g_1^{-1}\right)\left(\mu(g_1)\left(\tau^{\nu_{k,\tau}(g_2)^{-1}}\right)\right) \\ &= \tilde{\mu}_{k,\mu,\tau}\left(\left(g_1^{-1}, g_2^{-1}\right)\right)(\tau).\end{aligned}$$

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

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

$$\tilde{G}_{k_1/k,\mu,\tau} = \tilde{G}_{k,\mu,\tau} \cap \mathrm{Gal}(k_1(\zeta_{o(\tau)})/k)$$

of $\tilde{G}_{k,\mu,\tau}$. 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 $\mathrm{Gal}(k_1(\zeta_{o(\tau)})/k) \cong \mathcal{G} \times \mathrm{Gal}(k(\zeta_{o(\tau)})/k)$ and hence $\tilde{G}_{k_1/k,\mu,\tau} = \tilde{G}_{k,\mu,\tau}$.

Lemma 3.1.8. *For any $\tau \in H$, $k_1 Z_{k_1/k,\mu,\tau} = k_1(\zeta_{o(\tau)})$.*

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

$$\mathrm{Gal}(k_1(\zeta_{o(\tau)})/k_1) \cap \tilde{G}_{k_1/k,\mu,\tau} = 1$$

i.e. that

$$k_1 Z_{k_1/k,\mu,\tau} = k_1(\zeta_{o(\tau)}).$$

□

Lemma 3.1.9. *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

$$\begin{aligned} G_{k,\mu,\tau} &\supseteq \left\{ g_2 \in \mathrm{Gal}(k(\zeta_{o(\tau)})/k) : \ \exists g_1 \in \mathcal{G}, \ (g_1, g_2) \in \tilde{G}_{k_1/k,\mu,\tau} \right\} \\ &= \mathrm{res}^{k_1(\zeta_{o(\tau)})}_{k(\zeta_{o(\tau)})}(\tilde{G}_{k_1/k,\mu,\tau}) \\ &= \mathrm{res}^{k_1(\zeta_{o(\tau)})}_{k(\zeta_{o(\tau)})}(\tilde{G}_{k_1/k,\mu,\tau}) \mathrm{res}^{k_1(\zeta_{o(\tau)})}_{k(\zeta_{o(\tau)})}(\mathrm{Gal}(k_1(\zeta_{o(\tau)})/k(\zeta_{o(\tau)}))) \\ &= \mathrm{res}^{k_1(\zeta_{o(\tau)})}_{k(\zeta_{o(\tau)})}(\mathrm{Gal}(k_1(\zeta_{o(\tau)})/Z_{k_1/k,\mu,\tau} \cap k(\zeta_{o(\tau)}))) \\ &= \mathrm{Gal}(k(\zeta_{o(\tau)})/Z_{k_1/k,\mu,\tau} \cap k(\zeta_{o(\tau)})) \end{aligned}$$

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. □

Lemma 3.1.10. *Let $\tau \in H$, then*

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

If $k_1 \cap k(\zeta_{o(\tau(l))}) = k$ 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 3.1.9 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

$$k^1 \cap k_1(\zeta_{o(\tau)}) \subseteq k(\zeta_{o(\tau)}).$$

If that is not true, then

$$k(\zeta_{o(\tau)}) \subsetneq (k^1 \cap k_1(\zeta_{o(\tau)})) \cdot k(\zeta_{o(\tau)}) \subseteq k_1(\zeta_{o(\tau)})$$

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. Therefore if $k_1 \cap k(\zeta_{o(\tau)}) = k$ and k_1/k has no unramified subextensions then, recalling also Lemma 3.1.9,

$$k^1 \cap E_{k,\mu,\tau} = k^1 \cap Z_{k_1/k,\mu,\tau} \cap k(\zeta_{o(\tau)}) = k^1 \cap Z_{k_1/k,\mu,\tau} \cap k_1(\zeta_{o(\tau)}) = k^1 \cap Z_{k_1/k,\mu,\tau}$$

and by Proposition 1.2.10 we conclude that $W(k, E_{k,\mu,\tau}) = W(k, Z_{k_1/k,\mu,\tau})$. □

Lemma 3.1.11. *Let k_1 be a $\mathcal{G}$-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 μ, whose Steinitz classes (over k_1) are $\iota(x)^{\eta_H \alpha_{l,j}}$, where:*

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

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

(c) $$\alpha_{l,3} = \frac{3(l-1)}{2}\frac{n}{l} \qquad \textit{(only if } l \neq 2\textit{)}.$$

Further there exist extensions whose Steinitz classes have $\iota(x)^{2\alpha_{l,j}}$ as their square. We can choose these extensions so that they satisfy the additional conditions of Lemma 2.1.2.

Proof. By Lemma 3.1.6 there exists an extension K of k_1 of type μ 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 1.2.12, x contains infinitely many primes $\mathfrak{q}$ of absolute degree 1 splitting completely in $Z_{k_1/k,\mu,\tau}$. Those primes obviously split completely also in the extension $k_1(\zeta_{o(\tau)}) = k_1 Z_{k_1/k,\mu,\tau}$ (the equality holds by Lemma 3.1.8) 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 Δ of representatives of the cosets δD, with $\delta \in \mathcal{G}$. Then $\mathfrak{q}\mathcal{O}_{k_1} = \prod_{\delta\in\Delta} \delta(\mathfrak{Q})$ are the decompositions of the primes $\mathfrak{q}$ in k_1.

Let $g_{\mathfrak{Q}}$ be a generator of $\kappa^*_{\mathfrak{Q}} = U_{\mathfrak{Q}}/U^1_{\mathfrak{Q}}$. 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 $\tilde{\delta} \in \mathrm{Gal}(k_1(\zeta_{o(\tau)})/k)$ in a way such that $\tilde{\delta}(\tilde{\mathfrak{Q}}) = \tilde{\mathfrak{Q}}$, where $\tilde{\mathfrak{Q}}$ is a prime in $k_1(\zeta_{o(\tau)})$ above $\mathfrak{Q}$ (it is enough to extend δ in some way and then to multiply it by an appropriate element of $\mathrm{Gal}(k_1(\zeta_{o(\tau)})/k_1)$). This element acts as a $\lambda_{\mathfrak{Q},\delta}$-th power on $\kappa^*_{\tilde{\mathfrak{Q}}} = \kappa^*_{\mathfrak{Q}}$ (the equality holds because $\mathfrak{Q}$ splits completely in $k_1(\zeta_{o(\tau)})$). Thus, for $\delta \in D$,

$$\zeta_{o(\tau)}^{\tilde{\nu}_{k,\mu,\tau}(\tilde{\delta})} = \tilde{\delta}\left(\zeta_{o(\tau)}\right) \equiv \zeta_{o(\tau)}^{\lambda_{\mathfrak{Q},\delta}} \pmod{\tilde{\mathfrak{Q}}}$$

and, recalling that the powers of $\zeta_{o(\tau)}$ 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 $\tilde{\delta} \in \mathrm{Gal}(k_1(\zeta_{o(\tau)})/Z_{k_1/k,\mu,\tau})$ and hence

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

Defining the $h_{\delta(\mathfrak{Q}),u_j}$ as in the proof of Lemma 3.1.6, the set of all the possible ρs-tuples

$$(h_{\delta(\mathfrak{Q}),u_j})_{\delta\in\Delta;\ j=1,\dots,s}$$

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

Let $\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{q}_3$ 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 and to $\mathrm{d}(K/k_1)$ and that they satisfy all the above requests.

(a) Now let us define $\varphi_i : \kappa^*_{\mathfrak{Q}_i} \to H$, for $i = 1, 2$, posing

$$\varphi_1(g_{\mathfrak{Q}_1}) = \tau^{\frac{o(\tau)}{l}}$$

and

$$\varphi_2(g_{\mathfrak{Q}_2}) = \tau^{-\frac{o(\tau)}{l}}.$$

For $\delta \in D$, we have

$$\mu(\delta)(\varphi_1(g_{\mathfrak{Q}_1})) = \mu(\delta)\left(\tau^{\frac{o(\tau)}{l}}\right) = \tau^{\lambda_{\mathfrak{Q}_1,\delta}\frac{o(\tau)}{l}} = \varphi_1(g_{\mathfrak{Q}_1}^{\lambda_{\mathfrak{Q}_1,\delta}}) = \varphi_1(\delta(g_{\mathfrak{Q}_1})).$$

Thus φ_1 is a D-invariant homomorphism and the same is true for φ_2.

Then, for $i = 1, 2$, we extend φ_i to

$$\tilde{\varphi}_i : \mathrm{ind}_D^{\mathcal{G}} \kappa^*_{\mathfrak{Q}_i} \cong \prod_{\delta \in \Delta} \kappa^*_{\delta(\mathfrak{Q}_i)} \to H$$

using Theorem 3.1.5 and we define $\varphi_0 : \prod_{\mathfrak{P}} \kappa^*_{\mathfrak{P}} \to H$, posing

$$\begin{cases} \varphi_0|_{\kappa^*_{\delta(\mathfrak{Q}_i)}} = \tilde{\varphi}_i & \text{for } i = 1, 2 \text{ and } \delta \in \Delta \\ \varphi_0|_{\kappa^*_{\mathfrak{P}}} = 1 & \text{for } \mathfrak{P} \nmid \mathfrak{q}_1, \mathfrak{q}_2. \end{cases}$$

As in Lemma 3.1.6 we can extend φ_0 to a $\mathcal{G}$-invariant surjective homomorphism $\varphi : C_{k_1} \to H$, whose kernel contains a congruence subgroup of C_{k_1} and hence this is true also for

$$\varphi \cdot (\ , K/k_1) : C_{k_1} \to H.$$

We can conclude that there exists an extension of type μ, with discriminant

$$\mathrm{d}(K/k_1)\left((\mathfrak{q}_1\mathfrak{q}_2)^{(l-1)\frac{n}{l}}\mathcal{O}_{k_1}\right).$$

Its Steinitz class has $\iota(x)^{2\alpha_{l,1}}$ as its square and we conclude as in Lemma 2.1.2.

(b) Now let us define $\varphi_i : \kappa^*_{\mathfrak{Q}_i} \to H$, for $i = 1, 2$, posing

$$\varphi_1(g_{\mathfrak{Q}_1}) = \tau$$

and

$$\varphi_2(g_{\mathfrak{Q}_2}) = \tau^{-1}.$$

Exactly as in the first case we obtain an extension of type μ with discriminant

$$\mathrm{d}(K/k_1)\left((\mathfrak{q}_1\mathfrak{q}_2)^{(o(\tau)-1)\frac{n}{o(\tau)}}\mathcal{O}_{k_1}\right).$$

Its Steinitz class has $\iota(x)^{2\alpha_{l,2}}$ as its square and it is easy to conclude as in (a).

(c) If $l \neq 2$ we define $\varphi_i : \kappa^*_{\mathfrak{Q}_i} \to H$, for $i = 1, 2, 3$, posing

$$\varphi_1(g_{\mathfrak{Q}_1}) = \tau^{\frac{o(\tau)}{l}},$$

$$\varphi_2(g_{\mathfrak{Q}_2}) = \tau^{\frac{o(\tau)}{l}},$$

and

$$\varphi_3(g_{\mathfrak{Q}_3}) = \tau^{-\frac{2o(\tau)}{l}}.$$

Now we obtain an extension of type μ with discriminant

$$\mathrm{d}(K/k_1)\left((\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3)^{(l-1)\frac{n}{l}}\mathcal{O}_{k_1}\right).$$

Its Steinitz class has $\iota(x)^{2\alpha_{l,3}}$ as its square and we conclude in the usual way.

Lemma 3.1.11 is now completely proved. □

Now we generalize Lemma 2.1.4.

Lemma 3.1.12. *Let k_1/k be a $\mathcal{G}$-extension of number fields, let $H(2)$ be the 2-Sylow subgroup of H and $\tilde{H}$ such that $H = H(2) \times \tilde{H}$. Let $\mu_{\tilde{H}}$ and $\mu_{H(2)}$ the actions of $\mathcal{G}$ induced by μ on $\tilde{H}$ and $H(2)$ respectively. Then*

$$\mathrm{R}_t(k_1, k, \mu_{\tilde{H}})^{n(2)} \subseteq \mathrm{R}_t(k_1, k, \mu).$$

Proof. Let $x \in \mathrm{R}_t(k_1, k, \mu_{\tilde{H}})$ and let $(\tilde{K}, k_1, k)$ be a $\mu_{\tilde{H}}$-extension of k_1 with Steinitz class x, which is the class of

$$\mathrm{d}(\tilde{K}/k_1)^{\frac{1}{2}}.$$

Let (K, k_1, k) be a $\mu_{H(2)}$-extension of k_1 with trivial Steinitz class and such that K/k_1 and $\tilde{K}/k_1$ are arithmetically disjoint (it exists because of Lemma 3.1.6). The Steinitz class of K/k is the class of

$$\left(\frac{\mathrm{d}(K/k_1)}{\alpha}\right)^{\frac{1}{2}}$$

for a certain $\alpha \in k_1$. Then the extension $(K\tilde{K}, k_1, k)$ is a μ-extension and its Steinitz class is the class of

$$\left(\frac{\mathrm{d}(K\tilde{K}/k)}{\alpha^{\frac{n}{n(2)}}}\right)^{\frac{1}{2}} = \mathrm{d}(\tilde{K}/k)^{\frac{n(2)}{2}} \left(\frac{\mathrm{d}(K/k)}{\alpha}\right)^{\frac{n}{2n(2)}}$$

which is $x^{n(2)}$. □

At this point we can prove a more general version of Proposition 2.1.5.

Proposition 3.1.13. *Let $l \neq 2$ be a prime dividing n and let $\tau \in H(l) \setminus \{1\}$, then*

$$\iota\left(W\left(k, Z_{k_1/k,\mu,\tau}\right)\right)^{\frac{l-1}{2}\frac{n}{o(\tau)}} \subseteq \mathrm{R}_t(k_1, k, \mu)$$

If $2|n$ then, for any $\tau \in H(2) \setminus \{1\}$,

$$\iota\left(W\left(k, Z_{k_1/k,\mu,\tau}\right)\right)^{\eta_H \frac{n}{o(\tau)}} \subseteq \mathrm{R}_t(k_1, k, \mu)$$

and

$$\iota\left(W\left(k, Z_{k_1/k,\mu,\tau}\right)\right)^{2\frac{n}{o(\tau)}} \subseteq \mathrm{R}_t(k_1, k, \mu)^2.$$

We can choose the corresponding extensions so that they satisfy the additional conditions of Lemma 2.1.2.

Proof. Let $H(2)$ be the 2-Sylow subgroup of H and $\tilde{H}$ be such that $H = H(2) \times \tilde{H}$. Let $l \neq 2$ be a prime dividing n, let $\tau \in H(l) \setminus \{1\} \subseteq \tilde{H}$ and let $x \in W(k, Z_{k_1/k,\mu,\tau})$. It follows from Lemma 3.1.2 and Lemma 3.1.11 that $\iota(x)^{\beta_l}$ is in $\mathrm{R}_t(k_1, k, \mu_{\tilde{H}})$, where

$$\begin{aligned}\beta_l &= \gcd\left((l-1)\frac{n}{n(2)l}, (o(\tau)-1)\frac{n}{n(2)o(\tau)}, \frac{3(l-1)}{2}\frac{n}{n(2)l}\right) \\ &= \gcd\left((o(\tau)-1)\frac{n}{n(2)o(\tau)}, \frac{l-1}{2}\frac{n}{n(2)l}\right).\end{aligned}$$

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

$$\iota(x)^{\frac{l-1}{2}\frac{n}{n(2)o(\tau)}} \in \mathrm{R}_t(k_1, k, \mu_{\tilde{H}}).$$

Hence by Lemma 3.1.12

$$\iota(x)^{\frac{l-1}{2}\frac{n}{o(\tau)}} \in \mathrm{R}_t(k_1, k, \mu).$$

Now let us assume that $2|n$, let $\tau \in H(2)\setminus\{1\}$ and let $x \in W(k, Z_{k_1/k,\mu,\tau})$. It follows from Lemma 3.1.2 and Lemma 3.1.11 that $\iota(x)^{\eta_H\beta_2}$ is in $\mathrm{R}_t(k_1, k, \mu)$ and $\iota(x)^{2\beta_2}$ is in $\mathrm{R}_t(k_1, k, \mu)^2$, where

$$\beta_2 = \gcd\left(\frac{n}{2}, (o(\tau)-1)\frac{n}{o(\tau)}\right).$$

So we obtain

$$\iota(x)^{\eta_H\frac{n}{o(\tau)}} \in \mathrm{R}_t(k_1, k, \mu)$$

and

$$\iota(x)^{2\frac{n}{o(\tau)}} \in \mathrm{R}_t(k_1, k, \mu)^2.$$

To conclude we observe that Lemma 3.1.2 preserves the additional conditions of Lemma 2.1.2. □

The next proposition is the main result we want to prove in this section.

Proposition 3.1.14. *Let k be a number field and let $\mathcal{G}$ be a finite group such that for any class $x \in \mathrm{R}_t(k, \mathcal{G})$ there exists a tame $\mathcal{G}$-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 $k(\zeta_a)/k$, where a is a multiple of n_1.*

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

$$0 \to H \xrightarrow{\varphi} G \xrightarrow{\psi} \mathcal{G} \to 0,$$

in which the induced action of $\mathcal{G}$ on H is μ, determines the group G, up to isomorphism. Further we assume that H is of odd order or with noncyclic 2-Sylow subgroup, or that $\mathcal{G}$ is of odd order. Then

$$\mathrm{R}_t(k, G) \supseteq \mathrm{R}_t(k, \mathcal{G})^n \prod_{\substack{l|n \\ l\neq 2}} \prod_{\tau\in H(l)\setminus\{1\}} W\left(k, E_{k,\mu,\tau}\right)^{\frac{l-1}{2}\frac{mn}{o(\tau)}} \prod_{\tau\in H(2)\setminus\{1\}} W\left(k, E_{k,\mu,\tau}\right)^{\frac{\eta_G mn}{o(\tau)}},$$

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

$$G_{k,\mu,\tau} = \left\{g \in \mathrm{Gal}(k(\zeta_{o(\tau)})/k) : \ \exists g_1 \in \mathcal{G},\ \mu(g_1)(\tau) = \tau^{\nu_{k,\tau}(g)}\right\}$$

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

Further we can choose tame G-extensions K/k with a given Steinitz class (of the ones considered above), such that every nontrivial subextension of K/k is ramified at some primes which are unramified in $k(\zeta_a)/k$.

Proof. Let $x \in \mathrm{R}_t(k,\mathcal{G})$ and let k_1 be a tame $\mathcal{G}$-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 $k(\zeta_a)/k$. Thus, since a is a multiple of n_1, it follows also that $k_1 \cap k(\zeta_{n_1}) = k$.

By Lemma 3.1.2, Lemma 3.1.10, Proposition 3.1.13 and Proposition 1.3.7 we obtain

$$\mathrm{R}_t(k,G) \supseteq x^n \prod_{\substack{l|n \\ l\neq 2}} \prod_{\tau\in H(l)\setminus\{1\}} W\left(k, E_{k,\mu,\tau}\right)^{\frac{l-1}{2}\frac{mn}{o(\tau)}} \prod_{\tau\in H(2)\setminus\{1\}} W\left(k, E_{k,\mu,\tau}\right)^{\frac{\eta_H mn}{o(\tau)}},$$

from which we obtain the result we wanted to prove, if $\eta_H = \eta_G$.

With our hypotheses $\eta_H \neq \eta_G$ implies that the order of H is odd, i.e. that there does not exist any nontrivial $\tau \in H(2)$. Hence we obtain the desired result also in this case. □

We will now generalize Lemma 2.3.1 to the above setting.

Proposition 3.1.15. *Let $\tau, \tilde{\tau} \in H(2)\setminus\{1\}$ be elements such that $\tau, \tilde{\tau}, \tau\tilde{\tau}$ are all of the same order. Let k_1 be a $\mathcal{G}$-extension of k. Then*

$$\iota(W(k, Z_{k_1/k,\mu,\tau} Z_{k_1/k,\mu,\tilde{\tau}} Z_{k_1/k,\mu,\tau\tilde{\tau}}))^{\frac{n}{2o(\tau)}} \subseteq \mathrm{R}_t(k_1,k,\mu).$$

In particular, if $Z_{k_1/k,\mu,\tau} = Z_{k_1/k,\mu,\tau} Z_{k_1/k,\mu,\tilde{\tau}} Z_{k_1/k,\mu,\tau\tilde{\tau}}$, the factor[1]

$$W(k, E_{k,\mu,\tau})^{\frac{mn}{2o(\tau)}}$$

can be added in the expression of Proposition 3.1.14, giving more realizable classes. The additional condition of Proposition 3.1.14 is also satisfied.

Proof. Let

$$x \in W(k, Z_{k_1/k,\mu,\tau} Z_{k_1/k,\mu,\tilde{\tau}} Z_{k_1/k,\mu,\tau\tilde{\tau}}).$$

We will use all the notations of the proof of Lemma 3.1.11 and we also consider prime ideals $\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{q}_3$ with analogous conditions.

We define $\varphi_i : \kappa^*_{\mathfrak{Q}_i} \to H$, for $i = 1, 2, 3$, posing

$$\varphi_1(g_{\mathfrak{Q}_1}) = \tau,$$

$$\varphi_2(g_{\mathfrak{Q}_2}) = \tilde{\tau},$$

and

$$\varphi_3(g_{\mathfrak{Q}_3}) = (\tau\tilde{\tau})^{-1}.$$

[1] If the order of τ is 2 or 4 this condition is obviously verified.

In the usual way we obtain an extension of type μ with discriminant

$$\mathrm{d}(K/k_1)\left((\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3)^{(o(\tau)-1)\frac{n}{o(\tau)}}\mathcal{O}_{k_1}\right)$$

and so its Steinitz class is $\iota(x)^{\alpha_{2,4}}$ (with the above hypotheses the 2-Sylow subgroup of H can not be cyclic), where

$$\alpha_{2,4} = 3(o(\tau)-1)\frac{n}{2o(\tau)}.$$

Thus by Lemma 3.1.2 and Lemma 3.1.11 we obtain that

$$\iota(W(k, Z_{k_1/k,\mu,\tau}Z_{k_1/k,\mu,\tilde{\tau}}Z_{k_1/k,\mu,\tau\tilde{\tau}}))^{\frac{n}{2o(\tau)}} \subseteq \mathrm{R}_t(k_1, k, \mu).$$

To prove that

$$W(k, E_{k,\mu,\tau})^{\frac{mn}{2o(\tau)}}$$

can be added in the expression of Proposition 3.1.14, it is now enough to use Lemma 3.1.10, assuming that $k_1 \cap k(\zeta_{o(\tau)}) = k$ and that every subextension of k_1/k is ramified. □

Example. As an example we construct a group of order 168 and we calculate the Steinitz classes for that group and any number field. We consider the action $\mu_1 : C(3) \to \mathrm{Aut}(C(7))$, sending a generator of $C(3)$ to the automorphism of $C(7)$ defined as raising everything to the square. We call $\mathcal{G} = C(7) \rtimes_{\mu_1} C(3)$. Now we define a representation μ_2 of $\mathcal{G}$ on the 3-dimensional vector space over $\mathbb{F}_2$, by sending a generator of $C(7)$ to

$$M_1 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

and a generator of $C(3)$ to

$$M_2 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

It is easy to verify that this is well defined and we consider the corresponding semidirect product:

$$G = (C(2)\times C(2)\times C(2)) \rtimes_{\mu_2} \mathcal{G} = (C(2)\times C(2)\times C(2)) \rtimes_{\mu_2} (C(7) \rtimes_{\mu_1} C(3)).$$

We want to prove that, for any number field k,

$$\mathrm{R}_t(k, G) = \mathrm{Cl}(k)^2.$$

By Proposition 3.1.14 and Theorem 2.1.8

$$\begin{aligned}\mathrm{R}_t(k,\mathcal{G}) &\supseteq W(k,3)^7 \prod_{\tau\in C(7)\setminus\{1\}} \left(W\left(k,E_{k,\mu_1,\tau}\right)\right)^9 \supseteq W(k,3)^7 W(k,7)^9 \\ &\supseteq \mathrm{Cl}(k)^{14}\mathrm{Cl}(k)^{54} = \mathrm{Cl}(k)^2.\end{aligned}$$

If τ is an element of order 2 in the subgroup $C(2)\times C(2)\times C(2)$ of G, then $E_{k,\mu_2,\tau} = k$. Thus, by Proposition 3.1.15,

$$\mathrm{R}_t(k,G) \supseteq \mathrm{R}_t(k,\mathcal{G})^8\mathrm{Cl}(k)^{\frac{8}{2\cdot 2}21} \supseteq \mathrm{Cl}(k)^{16}\mathrm{Cl}(k)^{42} = \mathrm{Cl}(k)^2.$$

Conversely, the index of ramification of a prime in a tame G-extension clearly divides 42, because in a $C(2)\times C(2)\times C(2)$-extension the ramification index is at most 2 (the inertia group must be cyclic by Proposition 1.3.9). Thus the discriminant of a G-extension must be the 4-th power of an ideal and we conclude that

$$\mathrm{R}_t(k,G) \subseteq \mathrm{Cl}(k)^2$$

and hence we have obtained an equality.

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

Lemma 3.1.16. *Let (K,k_1,k) be a tame μ-extension, 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*

$$x \in W(k,Z_{k_1/k,\mu,\tau}) \subseteq W(k,E_{k,\mu,\tau}) \subseteq \bigcap_{l|e_{\mathfrak{P}}} W(k,E_{k,\mu,\tau(l)}),$$

where x is the class of $\mathfrak{p}$ and τ generates $([U_{\mathfrak{P}}],K/k_1)$.

Proof. Let $e_{\mathfrak{P}}$ be the ramification index of $\mathfrak{P}$ in K/k_1 and let $f_{\mathfrak{p}}$ be the inertia degree of $\mathfrak{p}$ in k_1/k. By Lemma 1.2.15, $\mathfrak{P}\in H^{e_{\mathfrak{P}}\cdot p_\infty}_{k_1(\zeta_{e_{\mathfrak{P}}})/k_1}$ and, since the extension is tame, $\mathfrak{P}\nmid e_{\mathfrak{P}}$, i.e. $\mathfrak{P}$ is unramified in $k_1(\zeta_{e_{\mathfrak{P}}})/k_1$. Hence, by Theorem 1.2.6, $\mathfrak{P}$ splits completely in $k_1(\zeta_{e_{\mathfrak{P}}})/k_1$. It follows that the inertia degree of $\mathfrak{p}$ in $k_1(\zeta_{e_{\mathfrak{P}}})/k$ is exactly the same as in k_1/k, i.e. $f_{\mathfrak{p}}$.

Let $u_{\mathfrak{P}}\in U_{\mathfrak{P}}$ be such that its class modulo $\mathfrak{P}$ is a generator $g_{\mathfrak{P}}$ of $\kappa^*_{\mathfrak{P}} = U_{\mathfrak{P}}/U^1_{\mathfrak{P}}$. By Theorem 1.1.2 and Proposition 1.1.7, $\tau = (g_{\mathfrak{P}},K/k_1)$ is an element of order $e_{\mathfrak{P}}$ in H. An element $\delta\in\mathrm{Gal}(k_1(\zeta_{e_{\mathfrak{P}}})/k)$ in the decomposition group of a prime $\tilde{\mathfrak{P}}$ in $k_1(\zeta_{e_{\mathfrak{P}}})$ dividing $\mathfrak{P}$, induces an automorphism of $\kappa^*_{\mathfrak{P}} = \kappa^*_{\tilde{\mathfrak{P}}}$ (the equality holds since $\mathfrak{P}$ splits completely in $k_1(\zeta_{e_{\mathfrak{P}}})/k_1$), given by

$$\delta(g_{\mathfrak{P}}) = g_{\mathfrak{P}}^{\lambda_{\mathfrak{P},\delta}},$$

where $\lambda_{\mathfrak{P},\delta}$ is an integer. Thus $\zeta_{e_\mathfrak{P}}^{\tilde{\nu}_{k,\mu,\tau}(\delta)} = \delta\left(\zeta_{e_\mathfrak{P}}\right) \equiv \zeta_{e_\mathfrak{P}}^{\lambda_{\mathfrak{P},\delta}} \pmod{\tilde{\mathfrak{P}}}$ and, recalling that the powers of $\zeta_{e_\mathfrak{P}}$ are distinct modulo $\tilde{\mathfrak{P}}$ (since $\tilde{\mathfrak{P}} \nmid e_\mathfrak{P}$), we deduce that $\lambda_{\mathfrak{P},\delta} \equiv \tilde{\nu}_{k,\mu,\tau}(\delta) \pmod{e_\mathfrak{P}}$. Recalling Proposition 1.1.9,

$$\begin{aligned}\tilde{\mu}_{k,\mu,\tau}(\delta)(\tau) &= \mu(\delta|_{k_1})(\tau) = (\delta(g_\mathfrak{P}), K/k_1) \\ &= \left(g_\mathfrak{P}^{\lambda_{\mathfrak{P},\delta}}, K/k_1\right) = \tau^{\lambda_{\mathfrak{P},\delta}} = \tau^{\tilde{\nu}_{k,\mu,\tau}(\delta)}.\end{aligned}$$

Thus $\delta \in \tilde{G}_{k_1/k,\mu,\tau} = \mathrm{Gal}(k_1(\zeta_{e_\mathfrak{P}})/Z_{k_1/k,\mu,\tau})$. Hence we conclude that $\mathfrak{p}$ 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 1.2.12, 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 3.1.10 and Corollary 1.2.11. □

3.2 A'-groups

We introduce a new kind of groups, which we call A'-groups.

Definition 3.2.1. *We define A'-groups inductively:*

1. *Finite abelian groups are A'-groups.*
2. *If $\mathcal{G}$ is an A'-group and H is finite abelian of order prime to that of $\mathcal{G}$, then $H \rtimes_\mu \mathcal{G}$ is an A'-group, for any action μ of $\mathcal{G}$ on H.*
3. *If $\mathcal{G}_1$ and $\mathcal{G}_2$ are A'-groups, then $\mathcal{G}_1 \times \mathcal{G}_2$ is an A'-group.*

Before going forward, we recall the classical definition of an A-group and we relate it to the above concept of A'-group.

Definition 3.2.2. *An A-group is a finite group with the property that all of its Sylow subgroups are abelian.*

Proposition 3.2.3. *Every A'-group is a solvable A-group.*

Proof. Since abelian groups are obviously solvable A-groups, we have only to prove that the property of being a solvable A-group is preserved by constructions 2 and 3 in Definition 3.2.1.

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. □

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

Example. Thanks to the above proposition we can find finite groups which are not A'-groups. It is enough to consider any nonabelian l-group.

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

Definition 3.2.4. *We will call a finite group G* good *if the following properties are verified:*

1. *For any number field k, $\mathrm{R}_t(k, G)$ is a group.*
2. *For any tame G-extension K/k of number fields there exists an element $\alpha_{K/k} \in k$ such that:*
   (a) *If G is of even order with a cyclic 2-Sylow subgroup, then a square root of $\alpha_{K/k}$ generates the quadratic subextension of K/k; if G either has odd order or has a noncyclic 2-Sylow subgroup, then $\alpha_{K/k} = 1$.*
   (b) *For any prime $\mathfrak{p}$, with ramification index $e_\mathfrak{p}$ in K/k, the ideal class of*
   $$\left(\mathfrak{p}^{(e_\mathfrak{p}-1)\frac{m}{e_\mathfrak{p}}-v_\mathfrak{p}(\alpha)}\right)^{\frac{1}{2}}$$
   is in $\mathrm{R}_t(k, G)$.
3. *For any tame G-extension K/k of number fields, for any prime ideal $\mathfrak{p}$ of k and any rational prime l dividing its ramification index $e_\mathfrak{p}$, the class of the ideal*
   $$\mathfrak{p}^{(l-1)\frac{m}{e_\mathfrak{p}(l)}}$$
   is in $\mathrm{R}_t(k, G)$ and, if 2 divides $(l-1)\frac{m}{e_\mathfrak{p}(l)}$, the class of
   $$\mathfrak{p}^{\frac{l-1}{2}\frac{m}{e_\mathfrak{p}(l)}}$$

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

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

We start with a negative result, showing that the cyclic group of order 8 is not good.

Proposition 3.2.5. *The cyclic group $C(8)$ of order 8 is not good.*

Proof. Let $k = \mathbb{Q}(i, \sqrt{10})$. The field $k(\zeta_8)$ is obtained extending k with a root of the polynomial $x^2 - i$, whose roots are ζ_8 and ζ_8^5. Hence

$$\mathrm{Gal}(k(\zeta_8)/k) = \langle 5 \rangle$$

is cyclic of order 2 and it is different from $\langle -5 \rangle$ and $\langle -25 \rangle$. We obtain by Proposition 2.2.5 that

$$\mathrm{R}_t(k, C(8)) = W(k, 8).$$

With some calculations we can prove that the ring of integers of $k(\zeta_8)$ is a principal ideal domain, i.e. that the ideal class group is trivial, while the ideal class group of k is cyclic of order 2. It follows that $W(k, 8)$ is the trivial group and, in particular, that the realizable classes form a proper subgroup of $\mathrm{Cl}(k)$.

By Lemma 2.1.2 there exists a tame $C(8)$-Galois extension K/k with trivial Steinitz class. Since $k(\zeta_4) = k(i) = k$, we have that $W(k, 4) = \mathrm{Cl}(k)$. Hence we can choose two prime ideals $\mathfrak{q}_1, \mathfrak{q}_2$ whose ideal class is the nontrivial one of k and which satisfy analogous conditions as in Lemma 2.1.3, substituting $m_1(l)$ with 4.

We call τ a generator of the group $C(8)$ and we define $\varphi_0 : \prod_{\mathfrak{p}} \kappa_{\mathfrak{p}}^* \to G$, posing

$$\begin{cases} \varphi_0(g_{\mathfrak{q}_1}) = \tau^2 \\ \varphi_0(g_{\mathfrak{q}_2}) = \tau^{-2} \\ \varphi_0(g_{\mathfrak{p}}) = 1 \qquad \text{for } \mathfrak{p} \notin \{\mathfrak{q}_1, \mathfrak{q}_2\}. \end{cases}$$

As in Lemma 2.1.3 we use this to obtain a tame $C(8)$-Galois extension of k with ramification index equal to 4 in the prime ideals $\mathfrak{q}_1$ and $\mathfrak{q}_2$. Since we have shown above that the class of

$$\mathfrak{q}_1^{\frac{2-1}{2}\frac{8}{4}} = \mathfrak{q}_1$$

is not in $\mathrm{R}_t(k, C(8))$, the third property of good groups is not verified in this case. □

Now our aim is to show that some groups, such as A'-groups of odd order are good.

Lemma 3.2.6. *Let $\mathcal{G}$ be a good group, let H be an abelian group of order prime to that of $\mathcal{G}$, with trivial or noncyclic 2-Sylow subgroup, and let μ be an action of $\mathcal{G}$ on H. Suppose (K, k_1, k) is tamely ramified and of type μ. Let $e_{\mathfrak{p}}$ be the ramification index of a prime $\mathfrak{p}$ in k_1/k and $e_{\mathfrak{P}}$ be the ramification index of a prime $\mathfrak{P}$ of k_1 dividing $\mathfrak{p}$ in K/k_1. Then the class of*

$$\left(\mathfrak{p}^{(e_{\mathfrak{p}}e_{\mathfrak{P}}-1)\frac{mn}{e_{\mathfrak{p}}e_{\mathfrak{P}}}-v_{\mathfrak{p}}(\alpha^n_{k_1/k})}\right)^{\frac{1}{2}}$$

is in

$$\mathrm{R}_t(k,\mathcal{G})^n \cdot \prod_{l|n} \prod_{\tau\in H(l)\setminus\{1\}} W\left(k, E_{k,\mu,\tau}\right)^{\frac{l-1}{2}\frac{mn}{o(\tau)}}.$$

Proof. Clearly

$$(e_{\mathfrak{p}}e_{\mathfrak{P}}-1)\frac{mn}{e_{\mathfrak{p}}e_{\mathfrak{P}}} = (e_{\mathfrak{p}}-1)\frac{mn}{e_{\mathfrak{p}}} + (e_{\mathfrak{P}}-1)\frac{mn}{e_{\mathfrak{p}}e_{\mathfrak{P}}}$$

is divisible by

$$\gcd\left((e_{\mathfrak{p}}-1)\frac{mn}{e_{\mathfrak{p}}}, (e_{\mathfrak{P}}-1)\frac{mn}{e_{\mathfrak{p}}e_{\mathfrak{P}}}\right)$$

and, since $(m,n)=1$, i.e. also $(e_{\mathfrak{p}}, e_{\mathfrak{P}})=1$, this coincides with

$$\gcd\left((e_{\mathfrak{p}}-1)\frac{mn}{e_{\mathfrak{p}}}, (e_{\mathfrak{P}}-1)\frac{mn}{e_{\mathfrak{P}}}\right).$$

Thus, recalling Lemma 2.1.6,

$$\mathfrak{p}^{(e_{\mathfrak{p}}e_{\mathfrak{P}}-1)\frac{mn}{e_{\mathfrak{p}}e_{\mathfrak{P}}}} = \mathfrak{p}^{a_{\mathfrak{p}}(e_{\mathfrak{p}}-1)\frac{mn}{e_{\mathfrak{p}}}+a_{\mathfrak{P}}(e_{\mathfrak{P}}-1)\frac{mn}{e_{\mathfrak{P}}}} = \mathfrak{p}^{a_{\mathfrak{p}}(e_{\mathfrak{p}}-1)\frac{mn}{e_{\mathfrak{p}}}}\prod_{l|e_{\mathfrak{P}}}\mathfrak{p}^{b_{\mathfrak{p},l}(l-1)\frac{mn}{e_{\mathfrak{P}}(l)}}.$$

If $\mathcal{G}$ 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 $\mathcal{G}$ is good, by Lemma 3.1.16 and by the fact that, for any prime l dividing $e_{\mathfrak{P}}$, $(l-1)\frac{mn}{e_{\mathfrak{P}}(l)}$ is even (in the case $l=2$ this is due to the fact that the inertia group at $\mathfrak{P}$ must be cyclic by Proposition 1.3.9, while the 2-Sylow subgroup of H is not).

We now assume that $\mathcal{G}$ is of even order with a cyclic 2-Sylow subgroup and thus that the order of H is odd. Again using Lemma 2.1.6 we can find

some $c_{\mathfrak{p},l}$ such that

$$\begin{aligned}\mathfrak{p}^{(e_\mathfrak{p}e_\mathfrak{P}-1)\frac{mn}{e_\mathfrak{p}e_\mathfrak{P}}-v_\mathfrak{p}(\alpha_{k_1/k}^n)} &= \mathfrak{p}^{a_\mathfrak{p}(e_\mathfrak{p}-1)\frac{mn}{e_\mathfrak{p}}-v_\mathfrak{p}(\alpha_{k_1/k}^n)}\prod_{l|e_\mathfrak{P}}\mathfrak{p}^{b_{\mathfrak{p},l}(l-1)\frac{mn}{e_\mathfrak{P}(l)}}\\ &= \left(\mathfrak{p}^{(e_\mathfrak{p}-1)\frac{m}{e_\mathfrak{p}}(a_\mathfrak{p}-1)}\right)^n\left(\mathfrak{p}^{(e_\mathfrak{p}-1)\frac{m}{e_\mathfrak{p}}-v_\mathfrak{p}(\alpha_{k_1/k})}\right)^n\prod_{l|e_\mathfrak{P}}\mathfrak{p}^{b_{\mathfrak{p},l}(l-1)\frac{mn}{e_\mathfrak{P}(l)}}\\ &= \prod_{l|e_\mathfrak{p}}\mathfrak{p}^{c_{\mathfrak{p},l}(l-1)\frac{mn}{e_\mathfrak{p}(l)}(a_\mathfrak{p}-1)}\left(\mathfrak{p}^{(e_\mathfrak{p}-1)\frac{m}{e_\mathfrak{p}}-v_\mathfrak{p}(\alpha_{k_1/k})}\right)^n\prod_{l|e_\mathfrak{P}}\mathfrak{p}^{b_{\mathfrak{p},l}(l-1)\frac{mn}{e_\mathfrak{P}(l)}}.\end{aligned}$$

We know that $\mathfrak{p}^{(e_\mathfrak{p}e_\mathfrak{P}-1)\frac{mn}{e_\mathfrak{p}e_\mathfrak{P}}-v_\mathfrak{p}(\alpha_{k_1/k}^n)}$ and $\mathfrak{p}^{(e_\mathfrak{p}-1)\frac{m}{e_\mathfrak{p}}-v_\mathfrak{p}(\alpha_{k_1/k})}$ are squares of ideals and that any l dividing $e_\mathfrak{P}$ is odd. It follows that $c_{\mathfrak{p},2}\frac{mn}{e_\mathfrak{p}(2)}(a_\mathfrak{p}-1)$ is even, since all the other exponents are. Recalling the hypothesis that $\mathcal{G}$ is good, we conclude that the class of

$$\left(\mathfrak{p}^{(e_\mathfrak{p}e_\mathfrak{P}-1)\frac{mn}{e_\mathfrak{p}e_\mathfrak{P}}-v_\mathfrak{p}(\alpha_{k_1/k}^n)}\right)^{\frac{1}{2}}$$

is in

$$\mathrm{R}_t(k,\mathcal{G})^n\cdot\prod_{l|n}\prod_{\tau\in H(l)\setminus\{1\}}W\left(k,E_{k,\mu,\tau}\right)^{\frac{l-1}{2}\frac{mn}{o(\tau)}}.$$

□

Lemma 3.2.7. *Under the same hypotheses as in the preceding lemma, if $l|e_\mathfrak{p}e_\mathfrak{P}$, the class of*

$$\mathfrak{p}^{(l-1)\frac{mn}{e_\mathfrak{p}(l)e_\mathfrak{P}(l)}}$$

is in

$$\mathrm{R}_t(k,\mathcal{G})^n\prod_{\tau\in H(l)\setminus\{1\}}W\left(k,E_{k,\mu,\tau}\right)^{\frac{l-1}{2}\frac{mn}{o(\tau)}}.$$

and, if 2 divides $(l-1)\frac{mn}{e_\mathfrak{p}(l)e_\mathfrak{P}(l)}$, the class of

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

is in

$$\mathrm{R}_t(k,\mathcal{G})^n\prod_{\tau\in H(l)\setminus\{1\}}W\left(k,E_{k,\mu,\tau}\right)^{\frac{l-1}{2}\frac{mn}{o(\tau)}}.$$

Proof. If l is an odd prime dividing $e_\mathfrak{p}$, then 2 divides $(l-1)\frac{m}{e_\mathfrak{p}(l)}$ and the class of

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

is in $\mathrm{R}_t(k,\mathcal{G})$, by the hypothesis that $\mathcal{G}$ is good. We conclude that the class of

$$\mathfrak{p}^{\frac{l-1}{2}\frac{mn}{e_{\mathfrak{p}}(l)e_{\mathfrak{P}}(l)}} = \mathfrak{p}^{\frac{l-1}{2}\frac{mn}{e_{\mathfrak{p}}(l)}}$$

is in $\mathrm{R}_t(k,\mathcal{G})^n$. Analogously, if 2 divides $e_{\mathfrak{p}}$, the class of

$$\mathfrak{p}^{\frac{mn}{e_{\mathfrak{p}}(2)e_{\mathfrak{P}}(2)}} = \mathfrak{p}^{\frac{mn}{e_{\mathfrak{p}}(2)}}$$

is in $\mathrm{R}_t(k,\mathcal{G})^n$. Further if 2 divides $\frac{mn}{e_{\mathfrak{p}}(2)e_{\mathfrak{P}}(2)} = \frac{mn}{e_{\mathfrak{p}}(2)}$ then also $\frac{m}{e_{\mathfrak{p}}(2)}$ must be even (n is prime to m and so it must be odd). As above we conclude that the class of

$$\mathfrak{p}^{\frac{1}{2}\frac{mn}{e_{\mathfrak{p}}(2)e_{\mathfrak{P}}(2)}}$$

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

If l divides $e_{\mathfrak{P}}$, then $(l-1)\frac{mn}{e_{\mathfrak{p}}(l)e_{\mathfrak{P}}(l)}$ is even (by hypothesis the 2-Sylow subgroup of H is not cyclic and thus $\frac{n}{e_{\mathfrak{P}}(2)}$ is even). We conclude by Lemma 3.1.16 that the class of

$$\mathfrak{p}^{\frac{l-1}{2}\frac{mn}{e_{\mathfrak{p}}(l)e_{\mathfrak{P}}(l)}} = \mathfrak{p}^{\frac{l-1}{2}\frac{mn}{e_{\mathfrak{P}}(l)}}$$

is in $W\left(k,E_{k,\mu,\tau}\right)^{\frac{l-1}{2}\frac{mn}{o(\tau)}}$ for some $\tau \in H(l)\setminus\{1\}$. □

Now we can prove the following theorem.

Theorem 3.2.8. *Let k be a number field and let $\mathcal{G}$ be a good group of order m. Let $H = C(n_1)\times\cdots\times C(n_r)$ be an abelian group of odd order prime to m and let μ be an action of $\mathcal{G}$ on H. Then*

$$\mathrm{R}_t(k,H\rtimes_\mu\mathcal{G}) = \mathrm{R}_t(k,\mathcal{G})^n\prod_{l|n}\prod_{\tau\in H(l)\setminus\{1\}} W\left(k,E_{k,\mu,\tau}\right)^{\frac{l-1}{2}\frac{mn}{o(\tau)}},$$

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

$$G_{k,\mu,\tau} = \left\{g\in\mathrm{Gal}(k(\zeta_{o(\tau)})/k):\ \exists g_1\in\mathcal{G},\ \mu(g_1)(\tau)=\tau^{\nu_{k,\tau}(g)}\right\}$$

and $g(\zeta_{o(\tau)}) = \zeta_{o(\tau)}^{\nu_{k,\tau}(g)}$ for any $g\in\mathrm{Gal}(k(\zeta_{o(\tau)})/k)$. Furthermore $G = H\rtimes_\mu\mathcal{G}$ is good.

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

$$\left(\mathfrak{p}^{(e_{\mathfrak{p}}e_{\mathfrak{P}}-1)\frac{mn}{e_{\mathfrak{p}}e_{\mathfrak{P}}}-v_{\mathfrak{p}}(\alpha_{k_1/k}^n)}\right)^{\frac{1}{2}}.$$

Hence it is contained in

$$\mathrm{R}_t(k,\mathcal{G})^n \cdot \prod_{l|n} \prod_{\tau \in H(l)\setminus\{1\}} W\left(k, E_{k,\mu,\tau}\right)^{\frac{l-1}{2}\frac{mn}{o(\tau)}}$$

by Lemma 3.2.6 and the fact that the last expression is a group. Hence

$$\mathrm{R}_t(k, H \rtimes_\mu \mathcal{G}) \subseteq \mathrm{R}_t(k,\mathcal{G})^n \cdot \prod_{l|n} \prod_{\tau \in H(l)\setminus\{1\}} W\left(k, E_{k,\mu,\tau}\right)^{\frac{l-1}{2}\frac{mn}{o(\tau)}}.$$

The opposite inclusion is given by Proposition 3.1.14. 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 $\mathrm{R}_t(k, H \rtimes_\mu \mathcal{G})$.

2. This follows from Lemma 3.2.6, choosing $\alpha_{K/k} = \alpha^n_{k_1/k}$ for any extension (K, k_1, k) of type μ.

3. This follows from Lemma 3.2.7.

4. This comes from Proposition 3.1.14.

□

Corollary 3.2.9. *Under the hypotheses of the above theorem, if* $\mathcal{G} = C(m_1) \times \cdots \times C(m_r)$ *is abelian of odd order* m*, then*

$$\mathrm{R}_t(k, H \rtimes_\mu \mathcal{G}) = \prod_{l|m} W(k, m_1(l))^{\frac{l-1}{2}\frac{mn}{m_1(l)}} \cdot \prod_{l|n} \prod_{\tau \in H(l)\setminus\{1\}} W\left(k, E_{k,\mu,\tau}\right)^{\frac{l-1}{2}\frac{mn}{o(\tau)}}.$$

Proof. This follows by Theorem 2.1.8 and Theorem 3.2.8. □

Example. We consider $\mathcal{G} = C(3)$ and $H = C(5) \times C(5)$ and we define an action $\mu : \mathcal{G} \to \mathrm{Aut}(H)$ by its image on a generator of $C(3)$, which can be written in form of a matrix with coefficients in $\mathbb{Z}/5\mathbb{Z}$. We choose the following matrix

$$M = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}.$$

By Corollary 3.2.9 we obtain

$$\mathrm{R}_t(k, (C(5) \times C(5)) \rtimes_\mu C(3)) = W(k,3)^{25} \cdot \prod_{\tau \in H\setminus\{1\}} W\left(k, E_{k,\mu,\tau}\right)^{30}.$$

Since any nonidentity power of the matrix M induces linear endomorphisms of $C(5) \times C(5)$ without eigenvectors, we deduce that, for any τ, $G_{k,\mu,\tau}$ is trivial. Thus $E_{k,\mu,\tau} = k(\zeta_5)$ and so $W(k, E_{k,\mu,\tau}) = W(k, 5)$. Hence

$$\mathrm{R}_t(k, (C(5) \times C(5)) \rtimes_\mu C(3)) = W(k, 3)^{25} W(k, 5)^{30}.$$

By Theorem 2.1.8 this coincides with $\mathrm{R}_t(k, (C(5) \times C(5)) \times C(3))$.

By Proposition 1.2.12, $W(k, 3) = \mathrm{N}_{k(\zeta_3)/k}(J_{k(\zeta_3)}) \cdot P_k / P_k$ and since $[k(\zeta_3) : k]$ divides 2 we obtain that $\mathrm{Cl}(k)^2 \subseteq W(k, 3)$. Analogously $\mathrm{Cl}(k)^4 \subseteq W(k, 5)$; hence we have

$$\begin{aligned} \mathrm{Cl}(k)^{10} &= \mathrm{Cl}(k)^{2 \cdot 25} \mathrm{Cl}(k)^{4 \cdot 30} \\ &\subseteq W(k, 3)^{25} W(k, 5)^{30} = \mathrm{R}_t(k, (C(5) \times C(5)) \rtimes_\mu C(3)) \end{aligned}$$

and in particular $W(k, 3)^{10} \subseteq \mathrm{R}_t(k, (C(5) \times C(5)) \rtimes_\mu C(3))$. Since also $W(k, 3)^{25} \subseteq \mathrm{R}_t(k, (C(5) \times C(5)) \rtimes_\mu C(3))$ we can conclude that

$$W(k, 3)^5 \subseteq \mathrm{R}_t(k, (C(5) \times C(5)) \rtimes_\mu C(3)).$$

Conversely

$$W(k, 3)^5 \supseteq W(k, 3)^{25} \mathrm{Cl}(k)^{10} \supseteq W(k, 3)^{25} W(k, 5)^{30} = \mathrm{R}_t(k, (C(5) \times C(5)) \rtimes_\mu C(3))$$

and so we have proved that there is a simpler way to write the realizable classes of the group $(C(5) \times C(5)) \rtimes_\mu C(3)$, namely

$$\mathrm{R}_t(k, (C(5) \times C(5)) \rtimes_\mu C(3)) = W(k, 3)^5.$$

We also observe that there are no other semidirect products of $C(5) \times C(5)$ and $C(3)$, up to isomorphism. This follows from the fact that any other 2×2 matrix of order 3 with coefficients in $\mathbb{Z}/5\mathbb{Z}$ has $x^2 + x + 1$, which is irreducible, as its characteristic polynomial and as its minimal polynomial, and hence it is conjugate to M.

Example. As a second example we calculate the realizable classes for the group $C(3)^{(3)} \rtimes_{\mu_1} C(13)$, where the action μ_1 sends a generator of $C(13)$ to the automorphism of $C(3)^{(3)} = C(3) \times C(3) \times C(3)$ defined by the matrix

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

By Corollary 3.2.9 we obtain that

$$\mathrm{R}_t(k, C(3)^{(3)} \rtimes_{\mu_1} C(13)) = W(k, 13)^{6 \cdot 27} \prod_{\tau \in C(3)^{(3)} \setminus \{1\}} W(k, E_{k,\mu_1,\tau})^{13 \cdot 9}.$$

It is immediate to verify that $G_{k,\mu_1,\tau} = \{1\}$ for any $\tau \in C(3)^{(3)} \setminus \{1\}$. Hence

$$\mathrm{R}_t(k, C(3)^{(3)} \rtimes_{\mu_1} C(13)) = W(k,13)^{6\cdot 27} W(k,3)^{13\cdot 9}.$$

As in the preceding example we obtain that

$$\mathrm{Cl}(k)^{18} = \mathrm{Cl}(k)^{12\cdot 6\cdot 27}\mathrm{Cl}(k)^{2\cdot 13\cdot 9} \subseteq \mathrm{R}_t(k, C(3)^{(3)} \rtimes_{\mu_1} C(13))$$

and, recalling that $W(k,3)^{13\cdot 9} \subseteq \mathrm{R}_t(k, C(3)^{(3)} \rtimes_{\mu_1} C(13))$, we obtain that

$$W(k,3)^9 \subseteq \mathrm{R}_t(k, C(3)^{(3)} \rtimes_{\mu_1} C(13)).$$

Of course we also have that

$$W(k,3)^9 \supseteq W(k,13)^{6\cdot 27} W(k,3)^{13\cdot 9}.$$

Hence

$$\mathrm{R}_t(k, C(3)^{(3)} \rtimes_{\mu_1} C(13)) = W(k,3)^9.$$

If $H = C(n) = C(n_1)$ is cyclic, then Theorem 3.2.8 may be written in a simpler form. For this aim we first need the following lemmas.

Lemma 3.2.10. *Let l be a prime dividing n. If $H(l)$ is cyclic, $\tau \in H(l)$ and $c | o(\tau)$, $c \neq o(\tau)$, then*

$$G^c_{k,\mu,\tau^c} \subseteq G_{k,\mu,\tau}.$$

Proof. We define

$$\hat{\mu}_\tau : \mathcal{G} \to (\mathbb{Z}/o(\tau)\mathbb{Z})^*$$

by $\tau^{\hat{\mu}_\tau(g_1)} = \mu(g_1)(\tau)$ for any $g_1 \in \mathcal{G}$. By definition if $g \in G_{k,\mu,\tau^c}$, then there exists $g_1 \in \mathcal{G}$ such that

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

and thus

$$\nu_{k,\tau^c}(g)\hat{\mu}_{\tau^c}(g_1)^{-1} \equiv 1 \pmod{o(\tau)/c}.$$

We observe that

$$\zeta_{o(\tau)/c}^{\nu_{k,\tau}(g)} = \zeta_{o(\tau)}^{c\nu_{k,\tau}(g)} = g\left(\zeta_{o(\tau)}^c\right) = g\left(\zeta_{o(\tau)/c}\right) = g\left(\zeta_{o(\tau^c)}\right) = \zeta_{o(\tau^c)}^{\nu_{k,\tau^c}(g)} = \zeta_{o(\tau)/c}^{\nu_{k,\tau^c}(g)}$$

and that

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

i.e. that

$$\nu_{k,\tau}(g) \equiv \nu_{k,\tau^c}(g) \pmod{o(\tau)/c}$$

and that

$$\hat{\mu}_\tau(g_1) \equiv \hat{\mu}_{\tau^c}(g_1) \pmod{o(\tau)/c}.$$

Thus

$$\nu_{k,\tau}(g)\hat{\mu}_\tau(g_1)^{-1} \equiv 1 \pmod{o(\tau)/c}$$

and by Lemma 1.2.17 we obtain that

$$\nu_{k,\tau}(g^c)\hat{\mu}_\tau(g_1^c)^{-1} = \left(\nu_{k,\tau}(g)\hat{\mu}_\tau(g_1)^{-1}\right)^c \equiv 1 \pmod{o(\tau)}$$

i.e. that

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

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

Lemma 3.2.11. *Let l be a prime dividing n. If $H(l)$ is cyclic, $\tau \in H(l)$ and $c|o(\tau)$, $c \neq o(\tau)$, then*

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

Proof. Let x be a class in $W(k, E_{k,\mu,\tau^c})$. By Proposition 1.2.12 there exists a prime $\mathfrak{p}$ in the class of x splitting completely in $E_{k,\mu,\tau^c}/k$. By Theorem 1.2.6, $\mathfrak{p} \in H^{\mathfrak{m}}_{E_{k,\mu,\tau^c}/k}$, where $\mathfrak{m}$ is a cycle of declaration of $E_{k,\mu,\tau^c}/k$. Then by Proposition 1.2.2

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

Thus

$$\left(\frac{k(\zeta_{o(\tau)})/k}{\mathfrak{p}}\right) \in \mathrm{Gal}(k(\zeta_{o(\tau)})/E_{k,\mu,\tau^c}) = G_{k,\mu,\tau^c}$$

and it follows by Lemma 3.2.10 that

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

Then

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

and so the class x^c of $\mathfrak{p}^c$ is in $W(k, E_{k,\mu,\tau})$. □

Proposition 3.2.12. *Let k be a number field and let $\mathcal{G}$ be a good group of order m, let n be an odd integer coprime to m, let μ be an action of $\mathcal{G}$ on $C(n)$, let τ be a generator of $C(n)$ and let $G = C(n) \rtimes_\mu \mathcal{G}$, then G is good and*

$$\mathrm{R}_t(k, G) = \mathrm{R}_t(k, \mathcal{G})^n \prod_{l|n} W(k, E_{k,\mu,\tau(l)})^{\frac{l-1}{2}\frac{mn}{n(l)}}.$$

Proof. Any element of $H(l) \setminus \{1\}$ is a c-th power of $\tau(l)$, for some $c|n(l)$, $c \neq n(l)$. Thus, by Theorem 3.2.8,

$$\mathrm{R}_t(k, C(n) \rtimes_\mu \mathcal{G}) = \mathrm{R}_t(k, \mathcal{G})^n \prod_{l|n} \prod_{\substack{c|n(l) \\ c \neq n(l)}} W\left(k, E_{k,\mu,\tau(l)^c}\right)^{\frac{l-1}{2}\frac{mn}{n(l)}c}.$$

Hence, by Lemma 3.2.11,

$$\mathrm{R}_t(k, C(n) \rtimes_\mu \mathcal{G}) \subseteq \mathrm{R}_t(k, \mathcal{G})^n \prod_{l|n} W\left(k, E_{k,\mu,\tau(l)}\right)^{\frac{l-1}{2}\frac{mn}{n(l)}}.$$

For the opposite inclusion it is enough to consider the factors corresponding to $c = 1$ in the above expression for $\mathrm{R}_t(k, C(n) \rtimes_\mu \mathcal{G})$. The fact that G is good has been proved in Theorem 3.2.8. □

In particular, if n is a power of a prime l and $\mathcal{G} = C(m)$ is cyclic of order prime to n we obtain exactly the same result as in [9].

Example. As an example of the above result we consider the group $C(13) \rtimes_{\mu_2} C(3)$, where the action μ_2 sends a generator of $C(3)$ to the elevation to the cube in $C(13)$. We explicitly calculate its realizable classes. By the above proposition and by Theorem 2.1.8 we obtain that

$$\mathrm{R}_t(k, C(13) \rtimes_{\mu_2} C(3)) = W(k,3)^{13} W(k, E_{k,\mu_2,\tau})^{18},$$

where τ is a generator of $C(13)$. Further since $\mathrm{Cl}(k)^2 \subseteq W(k,3)$ and $\mathrm{Cl}(k)^{12} \subseteq W(k,13) \subseteq W(k, E_{k,\mu_2,\tau})$ it follows that

$$\mathrm{Cl}(k)^2 = \mathrm{Cl}(k)^{2\cdot 13} \mathrm{Cl}(k)^{12\cdot 18} \subseteq \mathrm{R}_t(k, C(13) \rtimes_{\mu_2} C(3))$$

and, recalling that $W(k,3)^{13} \subseteq \mathrm{R}_t(k, C(13) \rtimes_{\mu_2} C(3))$, we obtain that

$$W(k,3) \subseteq \mathrm{R}_t(k, C(13) \rtimes_{\mu_2} C(3)).$$

Recalling that $\mathrm{Cl}(k)^2 \subseteq W(k,3)$ we also have that

$$W(k,3) \supseteq W(k,3)^{13} W(k, E_{k,\mu_2,\tau})^{18} = \mathrm{R}_t(k, C(13) \rtimes_{\mu_2} C(3)).$$

Hence

$$\mathrm{R}_t(k, C(13) \rtimes_{\mu_2} C(3)) = W(k,3).$$

Now we prove a result concerning direct products of good groups. We again need two lemmas.

Lemma 3.2.13. *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 $\mathcal{G}_2$ both have noncyclic 2-Sylow subgroups. Let K/k be a tame $\mathcal{G}_1 \times \mathcal{G}_2$-extension of number fields, where $K = k_1k_2$ and k_i/k are $\mathcal{G}_i$-extensions, let $e_\mathfrak{p}$ be the ramification index of a prime $\mathfrak{p}$ in K/k, and let*

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

Then the class of the ideal

$$\left(\mathfrak{p}^{(e_\mathfrak{p}-1)\frac{mn}{e_\mathfrak{p}} - v_\mathfrak{p}(\alpha_{K/k})}\right)^{\frac{1}{2}}$$

is in

$$\mathrm{R}_t(k,\mathcal{G}_1)^n \mathrm{R}_t(k,\mathcal{G}_2)^m.$$

Proof. Let $\mathfrak{p}$ 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 $\mathfrak{p}$ in k_1/k and g_2 in k_2/k. Let $e_{\mathfrak{p},i}$ be the ramification index of $\mathfrak{p}$ in k_i/k; then $e_\mathfrak{p} = \mathrm{lcm}(e_{\mathfrak{p},1}, e_{\mathfrak{p},2})$. In particular for any prime l dividing $e_\mathfrak{p}$, $e_\mathfrak{p}(l) = \max\{e_{\mathfrak{p},1}(l), e_{\mathfrak{p},2}(l)\}$.

Let us first consider the case in which the order of $\mathcal{G}_1 \times \mathcal{G}_2$ is odd or its 2-Sylow subgroups are not cyclic. In this case $\alpha_{K/k} = 1$ and, recalling Lemma 2.1.6, we have

$$\begin{aligned} \mathfrak{p}^{(e_\mathfrak{p}-1)\frac{mn}{e_\mathfrak{p}}} &= \prod_{l|e_\mathfrak{p}} \mathfrak{p}^{a_l(l-1)\frac{mn}{e_\mathfrak{p}(l)}} \\ &= \prod_{\substack{l|e_\mathfrak{p} \\ e_p(l)=e_{\mathfrak{p},1}(l)}} \left(\mathfrak{p}^{a_l(l-1)\frac{m}{e_{\mathfrak{p},1}(l)}}\right)^n \prod_{\substack{l|e_\mathfrak{p} \\ e_p(l)\neq e_{\mathfrak{p},1}(l)}} \left(\mathfrak{p}^{a_l(l-1)\frac{n}{e_{\mathfrak{p},2}(l)}}\right)^m, \end{aligned}$$

where all the exponents $a_l(l-1)\frac{m}{e_{\mathfrak{p},1}(l)}$ and $a_l(l-1)\frac{n}{e_{\mathfrak{p},2}(l)}$ are clearly even. Thus, since $\mathcal{G}_1$ and $\mathcal{G}_2$ are good, the class of $\mathfrak{p}^{\frac{1}{2}(e_\mathfrak{p}-1)\frac{mn}{e_\mathfrak{p}}}$ is in $\mathrm{R}_t(k,\mathcal{G}_1)^n \mathrm{R}_t(k,\mathcal{G}_2)^m$.

Let us now assume that $\mathcal{G}_1 \times \mathcal{G}_2$ is of even order with cyclic 2-Sylow subgroups. Thus we may suppose that the order of $\mathcal{G}_1$ is even, that $\mathcal{G}_1$ has cyclic 2-Sylow subgroups and that the order of $\mathcal{G}_2$ is odd. Then

$$\mathfrak{p}^{(e_\mathfrak{p}-1)\frac{mn}{e_\mathfrak{p}} - v_\mathfrak{p}(\alpha_{K/k})} = \mathfrak{p}^{n\left((e_{\mathfrak{p},1}-1)\frac{m}{e_{\mathfrak{p},1}} - v_\mathfrak{p}(\alpha_{k_1/k})\right)} \mathfrak{p}^{(e_\mathfrak{p}-1)\frac{mn}{e_\mathfrak{p}} - (e_{\mathfrak{p},1}-1)\frac{mn}{e_{\mathfrak{p},1}}}$$

and, recalling Theorem 1.3.6, we deduce that

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

is the square of an ideal and we have

$$\begin{aligned}
&\mathfrak{p}^{(e_{\mathfrak{p}}-1)\frac{mn}{e_{\mathfrak{p}}}-(e_{\mathfrak{p},1}-1)\frac{mn}{e_{\mathfrak{p},1}}} \\
&\quad = \prod_{l|e_{\mathfrak{p}}} \mathfrak{p}^{a_l(l-1)\frac{mn}{e_{\mathfrak{p}}(l)}} \prod_{l|e_{\mathfrak{p},1}} \mathfrak{p}^{-b_l(l-1)\frac{mn}{e_{\mathfrak{p},1}(l)}} \\
&\quad = \prod_{\substack{l|e_{\mathfrak{p}} \\ e_{\mathfrak{p}}(l)=e_{\mathfrak{p},2}(l)}} \mathfrak{p}^{a_l(l-1)\frac{mn}{e_{\mathfrak{p},2}(l)}} \prod_{\substack{l|e_{\mathfrak{p}} \\ e_{\mathfrak{p}}(l)\neq e_{\mathfrak{p},2}(l)}} \mathfrak{p}^{(a_l-b_l)(l-1)\frac{mn}{e_{\mathfrak{p},1}(l)}} \prod_{\substack{l|e_{\mathfrak{p},1} \\ e_{\mathfrak{p}}(l)=e_{\mathfrak{p},2}(l)}} \mathfrak{p}^{-b_l(l-1)\frac{mn}{e_{\mathfrak{p},1}(l)}}.
\end{aligned}$$

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 $2|e_{\mathfrak{p}}$), i.e. for $(a_2 - b_2)\frac{mn}{e_{\mathfrak{p},1}(2)}$, and hence also for $(a_2 - b_2)\frac{m}{e_{\mathfrak{p},1}(2)}$ since n is odd.

Thus by the hypothesis that $\mathcal{G}_1$ and $\mathcal{G}_2$ are good, we easily obtain that the class of the ideal

$$\left(\mathfrak{p}^{(e_{\mathfrak{p}}-1)\frac{mn}{e_{\mathfrak{p}}}-(e_{\mathfrak{p},1}-1)\frac{mn}{e_{\mathfrak{p},1}}}\right)^{\frac{1}{2}}$$

is in $\mathrm{R}_t(k,\mathcal{G}_1)^n\mathrm{R}_t(k,\mathcal{G}_2)^m$.

Now we can conclude that the class of

$$\left(\mathfrak{p}^{(e_{\mathfrak{p}}-1)\frac{mn}{e_{\mathfrak{p}}}-v_{\mathfrak{p}}(\alpha_{K/k})}\right)^{\frac{1}{2}} = \mathfrak{p}^{\frac{n}{2}\left((e_{\mathfrak{p},1}-1)\frac{m}{e_{\mathfrak{p},1}}-v_{\mathfrak{p}}(\alpha_{k_1/k})\right)}\left(\mathfrak{p}^{(e_{\mathfrak{p}}-1)\frac{mn}{e_{\mathfrak{p}}}-(e_{\mathfrak{p},1}-1)\frac{mn}{e_{\mathfrak{p},1}}}\right)^{\frac{1}{2}}$$

is in $\mathrm{R}_t(k,\mathcal{G}_1)^n\mathrm{R}_t(k,\mathcal{G}_2)^m$, since also

$$\mathfrak{p}^{\frac{n}{2}\left((e_{\mathfrak{p},1}-1)\frac{m}{e_{\mathfrak{p},1}}-v_{\mathfrak{p}}(\alpha_{k_1/k})\right)}$$

is in $\mathrm{R}_t(k,\mathcal{G}_1)^n$ and both $\mathrm{R}_t(k,\mathcal{G}_1)$ and $\mathrm{R}_t(k,\mathcal{G}_2)$ are groups. □

Lemma 3.2.14. *Under the same hypotheses as in the preceding lemma, if $l|e_{\mathfrak{p}}$, the class of the ideal*

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

is in $\mathrm{R}_t(k,\mathcal{G}_1)^n\mathrm{R}_t(k,\mathcal{G}_2)^m$ and, if 2 divides $(l-1)\frac{mn}{e_{\mathfrak{p}}(l)}$, the class of the ideal,

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

is in $\mathrm{R}_t(k,\mathcal{G}_1)^n\mathrm{R}_t(k,\mathcal{G}_2)^m$.

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

$$\mathfrak{p}^{(l-1)\frac{mn}{e_{\mathfrak{p}}(l)}} = \left(\mathfrak{p}^{(l-1)\frac{m}{e_{\mathfrak{p},1}(l)}}\right)^n$$

and its class is in $\mathrm{R}_t(k,\mathcal{G}_1)^n$, by the hypothesis that $\mathcal{G}_1$ is good. If $(l-1)\frac{mn}{e_{\mathfrak{p}}(l)}$ is even then 2 divides $(l-1)\frac{m}{e_{\mathfrak{p}}(l)}$ (if $l=2$ then this is true because $2|e_{\mathfrak{p}}(2) = e_{\mathfrak{p},1}(2)|m$ and thus by hypothesis n is odd or the 2-Sylow subgroup of $\mathcal{G}_1$ is not cyclic, i.e. 2 divides $m/e_{\mathfrak{p},1}(2) = m/e_{\mathfrak{p}}(2)$). Then

$$\mathfrak{p}^{\frac{l-1}{2}\frac{mn}{e_{\mathfrak{p}}(l)}} = \left(\mathfrak{p}^{\frac{l-1}{2}\frac{m}{e_{\mathfrak{p},1}(l)}}\right)^n$$

is in $\mathrm{R}_t(k,\mathcal{G}_1)^n$ by the assumption that $\mathcal{G}_1$ is good. The case $e_{\mathfrak{p}}(l) = e_{\mathfrak{p},2}(l)$ is identical. □

Theorem 3.2.15. *Let $\mathcal{G}_1$ and $\mathcal{G}_2$ be good groups of orders m and n respectively and let us assume that m and n are not both even or that $\mathcal{G}_1$ and $\mathcal{G}_2$ both have noncyclic 2-Sylow subgroups. Then*

$$\mathrm{R}_t(k,\mathcal{G}_1\times\mathcal{G}_2) = \mathrm{R}_t(k,\mathcal{G}_1)^n\mathrm{R}_t(k,\mathcal{G}_2)^m.$$

Furthermore the group $\mathcal{G}_1\times\mathcal{G}_2$ is good.

Proof. One inclusion is quite straightforward considering the composition of $\mathcal{G}_1$- and $\mathcal{G}_2$-extensions of k with appropriate Steinitz classes and using Proposition 1.3.7.

The opposite inclusion follows by Lemma 3.2.13 and Theorem 1.3.6.

Now again by Lemma 3.2.13 and by Lemma 3.2.14 it follows that $\mathcal{G}_1\times\mathcal{G}_2$ is good. □

Example. As an example we calculate the realizable classes for the group

$$G = (C(3)^{(3)} \rtimes_{\mu_1} C(13)) \times (C(13) \rtimes_{\mu_2} C(3)),$$

where the actions μ_1 and μ_2 are defined in the examples of the preceding pages. By the above results we obtain

$$\begin{aligned}\mathrm{R}_t(k,G) &= \mathrm{R}_t(k, C(3)^{(3)} \rtimes_{\mu_1} C(13))^{3\cdot 13} \cdot \mathrm{R}_t(k, C(13) \rtimes_{\mu_2} C(3))^{3^3 13}\\ &= W(k,3)^{9\cdot 3\cdot 13} W(k,3)^{3^3\cdot 13} = W(k,3)^{351}.\end{aligned}$$

At this point we obtain our most important result.

Theorem 3.2.16. *Every A'-group G of odd order is good. In particular for any such group and any number field k, $\mathrm{R}_t(k,G)$ is a subgroup of the ideal class group of k.*

Proof. Inductively, by Theorem 3.2.8 and Theorem 3.2.15, since the trivial group is obviously good. □

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

We can also obtain some results for groups of even order.

Proposition 3.2.17. *The cyclic groups $C(2)$ and $C(4)$ of order 2 and 4, respectively, are good and all the ideal classes are realizable for them.*

Proof. By Propositions 2.2.3 and 2.2.6 properties 1. and 4. of good groups are satisfied for $C(2)$ and $C(4)$ and

$$\mathrm{R}_t(k,C(2)) = \mathrm{R}_t(k,C(4)) = \mathrm{Cl}(k).$$

From this equality it is immediate to deduce also the second and the third requested property. □

Proposition 3.2.18. *If n is odd then D_n is a good group and*

$$\mathrm{R}_t(k,D_n) = \mathrm{Cl}(k)^n \cdot \prod_{l|n} W\left(k, E_{k,\mu,\tau(l)}\right)^{(l-1)\frac{n}{n(l)}},$$

where we write D_n as $C(n) \rtimes_\mu C(2)$ and τ is a generator of $C(n)$.

Proof. Immediate by Proposition 3.2.12 and Proposition 3.2.17. □

Example. As an example of the above result we consider the group $S_3 = D_3$. We explicitly calculate its realizable classes. By the above proposition

$$\mathrm{R}_t(k,S_3) = W(k,E_{k,\mu,\tau})^2\mathrm{Cl}(k)^3.$$

It is clear by definition that $G_{k,\mu,\tau} = \mathrm{Gal}(k(\zeta_3)/k)$ and hence that $E_{k,\mu,\tau} = k$. It follows that

$$\mathrm{R}_t(k,S_3) = \mathrm{Cl}(k)^2\mathrm{Cl}(k)^3 = \mathrm{Cl}(k).$$

Proposition 3.2.19. *If n is an odd integer, then the generalized quaternion group of order $4n$, which is defined by*

$$H_{4n} = \langle \sigma, \tau : \ \sigma^{2n} = 1, \sigma^n = \tau^2, \tau\sigma\tau^{-1} = \sigma^{-1} \rangle$$

is isomorphic to a semidirect product

$$C(n) \rtimes_\mu C(4).$$

This group is good and

$$\mathrm{R}_t(k, H_{4n}) = \mathrm{Cl}(k)^n \prod_{l|n} W(k, E_{k,\mu,\sigma(l)})^{(l-1)\frac{n}{n(l)}}.$$

Proof. The subgroup H of H_{4n}, generated by σ^2 is normal of order n and the quotient H_{4n}/H is cyclic of order 4. Thus we have the following exact sequence:

$$1 \to C(n) \to H_{4n} \to C(4) \to 1$$

and by Proposition 3.1.1 we conclude that

$$H_{4n} \cong C(n) \rtimes_\mu C(4).$$

Clearly $\sigma^2(l) = \sigma(l)$ for any prime l dividing n, since this is odd by hypothesis. Therefore by Proposition 3.2.12 we conclude that H_{4n} is a good group and that

$$\mathrm{R}_t(k, H_{4n}) = \mathrm{Cl}(k)^n \prod_{l|n} W(k, E_{k,\mu,\sigma(l)})^{(l-1)\frac{2n}{n(l)}}.$$

Finally, since n is odd and $\mathrm{Cl}(k)^n \subseteq \mathrm{R}_t(k, H_{4n})$, the 2 component of all the other exponents in the above expression can be omitted. So we obtain the desired equality. □

If in the above proposition n is a power of an odd prime number l, we obtain the result proved by James E. Carter and Bouchaïb Sodaïgui in [7].

In Proposition 2.3.2 we explicitly described the realizable classes for some particular abelian groups of even order. In the next proposition we show that these groups are good, so that we can use Theorem 3.2.8 and Theorem 3.2.15 to study some more groups.

Proposition 3.2.20. *Let $G = C(m_1) \times \cdots \times C(m_r)$, with $m_{i+1}|m_i$, be an abelian group of order m. If $2|m$ and $m_1(2) = m_2(2)$, then G is good.*

Proof. By Proposition 2.3.2, the first and the fourth property of good groups are verified and

$$\mathrm{R}_t(k,G) = \prod_{l|m} W(k, m_1(l))^{\frac{l-1}{2}\frac{m}{m_1(l)}}.$$

Let K/k be a tamely ramified extension of number fields with Galois group G. By Lemma 2.1.6 there exist $b_{e_\mathfrak{p},l} \in \mathbb{Z}$ such that

$$\mathfrak{p}^{(e_\mathfrak{p}-1)\frac{m}{e_\mathfrak{p}}} = \prod_{l|e_\mathfrak{p}} \mathfrak{p}^{b_{e_\mathfrak{p},l}(l-1)\frac{m}{e_\mathfrak{p}(l)}} = \prod_{l|e_\mathfrak{p}} \mathfrak{p}^{\frac{m_1(l)}{e_\mathfrak{p}(l)} b_{e_\mathfrak{p},l}(l-1)\frac{m}{m_1(l)}}.$$

By Lemma 1.2.15 and Lemma 1.2.18, the class of the ideal $\mathfrak{p}^{\frac{m_1(l)}{e_\mathfrak{p}(l)}}$ is contained in $W(k, m_1(l))$. Since $(l-1)\frac{m}{m_1(l)}$ is even for any prime l dividing $e_\mathfrak{p}$, we easily conclude that also the second and the third property of good groups hold for G. □

Proposition 3.2.21. *If n is odd then D_{2n} is a good group, it is isomorphic to a semidirect product of the form*

$$C(n) \rtimes_\mu (C(2) \times C(2))$$

and

$$\mathrm{R}_t(k, D_{2n}) = \mathrm{Cl}(k)^n \cdot \prod_{l|n} W\left(k, E_{k,\mu,\tau(l)}\right)^{(l-1)\frac{2n}{n(l)}},$$

where τ is a generator of $C(n)$.

Proof. It is easy to see that

$$D_{2n} \cong D_n \times C(2) \cong C(n) \rtimes_\mu (C(2) \times C(2)),$$

for a certain action $\mu : C(2) \times C(2) \to \mathrm{Aut}(C(n))$. By the above proposition $C(2) \times C(2)$ is good and

$$\mathrm{R}_t(k, C(2) \times C(2)) = \mathrm{Cl}(k).$$

Thus we conclude by Proposition 3.2.12 that D_{2n} is good and we obtain the desired expression for $\mathrm{R}_t(k, D_{2n})$. □

Proposition 3.2.22. *Let k be a number field and let $\mathcal{G}$ be a good group of odd order.*

Let $H = C(2)^{(n)} = C(2) \times \cdots \times C(2)$ and let μ be an action of $\mathcal{G}$ on H. Then

$$\mathrm{R}_t(k, H \rtimes_\mu \mathcal{G}) = \mathrm{R}_t(k, \mathcal{G})^{2^n} \mathrm{Cl}(k)^{m 2^{n-2}}.$$

Further $G = H \rtimes_\mu \mathcal{G}$ is good.

Proof. Clearly $E_{k,\mu,\tau} = k$, i.e. $W(k, E_{k,\mu,\tau}) = \mathrm{Cl}(k)$ for any $\tau \in H(2) = H$. Thus, by Propositions 3.1.14 and 3.1.15,

$$\mathrm{R}_t(k, H \rtimes_\mu \mathcal{G}) \supseteq \mathrm{R}_t(k, \mathcal{G})^{2^n} \mathrm{Cl}(k)^{m2^{n-2}}.$$

The opposite inclusion comes from Theorems 1.3.5 and 1.3.6 and from Lemma 3.2.6. So we obtain an equality and, in particular, this gives the first property of good groups. The other properties follow now respectively from Lemma 3.2.6, from Lemma 3.2.7 and from Propositions 3.1.14 and 3.1.15. □

If $\mathcal{G}$ is cyclic of order $2^n - 1$ and the representation μ is faithful, then the above proposition is one of the results proved by Nigel P. Byott, Cornelius Greither and Bouchaïb Sodaïgui in [4].

Example. The group A_4, which is isomorphic to a semidirect product of the form $(C(2) \times C(2)) \rtimes_\mu C(3)$, is good by Proposition 3.2.22. We calculate its realizable classes:

$$\mathrm{R}_t(k, A_4) = W(k, 3)^4 \mathrm{Cl}(k)^3 \supseteq \mathrm{Cl}(k)^8 \mathrm{Cl}(k)^3 = \mathrm{Cl}(k)$$

and hence

$$\mathrm{R}_t(k, A_4) = \mathrm{Cl}(k).$$

This result has been obtained by Marjory Godin and Bouchaïb Sodaïgui in [10].

3.3 Some l-groups

In this section we will consider some groups whose order is the power of an odd prime l. We start recalling some classical results concerning l-groups.

Proposition 3.3.1. *Every group G of order l^n has nontrivial center.*

Proof. This is Theorem I.6.5 of [13]. □

Lemma 3.3.2. *Let G be a finite group and let H be its center. If G/H is cyclic then it is trivial. In particular G/H does not have order l.*

Proof. Let H be the center of G and let us assume that G/H is not trivial. Then there exists $\tau \in G \setminus H$ such that its class modulo H generates G/H. Thus any element in G is of the form $\sigma\tau^a$ for $\sigma \in H$ and $a \in \mathbb{N}$. Since τ commutes both with $\sigma \in H$ (by the definition of H) and with τ^a, it commutes with any element $\sigma\tau^a$. Hence τ is in the center; contradiction. □

Proposition 3.3.3. *Every group G of order l^2 is abelian.*

Proof. Let H be the center of G. By Proposition 3.3.1 the order of H is not 1, by Lemma 3.3.2 it is not l, hence it must be l^2. □

Up to isomorphism there are two nonabelian groups of order l^3. We will describe them and then try to obtain information about the corresponding realizable Steinitz classes.

Proposition 3.3.4. *Up to isomorphism, there are two nonabelian groups of order l^3, where l is a prime:*

1. *$(C(l) \times C(l)) \rtimes_{\mu_1} C(l)$, where μ_1 sends a generator of $C(l)$ to the map defined by the matrix*
$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix};$$
2. *$C(l^2) \rtimes_{\mu_2} C(l)$, where μ_2 sends a generator of $C(l)$ to the elevation to the $l+1$-th power.*

Proof. Let G be a nonabelian group of order l^3 and let H be its center. By Proposition 3.3.1 and Lemma 3.3.2, the order of H must be l and G/H must be isomorphic to $C(l) \times C(l)$. Let $x, y \in G$ be such that xH, yH generate G/H, i.e. such that any element of G is of the form $x^a y^b \sigma$, where $a, b \in \{0, 1, \ldots, l-1\}$ and $\sigma \in H$. Since G/H is abelian, we know that $(xy)^{-1}yxH = y^{-1}Hx^{-1}HyHxH = H$, i.e. that $(xy)^{-1}yx = \gamma \in H$ and $yx = xy\gamma$. If x and y commute then, as in the proof of Lemma 3.3.2, they must be in the center of G, which is a contradiction. Hence they do not commute and, in particular, γ is nontrivial and therefore it is a generator of H. We also know that $x^l, y^l \in H$.

If $x^l = y^l = 1$, then G must be a quotient of the group

$$\langle x, y, \gamma : \ x^l = y^l = \gamma^l = 1, \gamma x = x\gamma, \gamma y = y\gamma, yx = xy\gamma \rangle.$$

This group is isomorphic to

$$(C(l) \times C(l)) \rtimes_{\mu_1} C(l)$$

and thus it is of order l^3 and it must coincide with G.

It remains to consider the case in which $x^l \neq 1$ or $y^l \neq 1$; we assume the first of these possibilities (the other case is analogous). Then clearly x^l generates H and we can find an integer a such that $x^{al} = y^{-l}$. We easily prove by induction on n that

$$(x^a y)^n = x^{an} y^n \gamma^{an(n-1)/2}$$

and in particular we obtain that $(x^a y)^l = 1$. Further, xH and $x^a yH$ continue to generate G/H. Thus we can assume that $y^l = 1$. Let $b \in \{1, \dots, l-1\}$ be such that $x^l = \gamma^b$; then $y^b x = xy^b\gamma^b = xy^b x^l$. Setting $\tau = x$, $\sigma = y^b$ we obtain the relations $\tau^{l^2} = \sigma^l = 1$ and, since τ^l is in the center of G, $\sigma\tau = \tau\sigma\tau^l = \tau^{l+1}\sigma$, i.e. $\sigma\tau\sigma^{-1} = \tau^{l+1}$.

Hence G must be a quotient of the group

$$G = \langle \sigma, \tau : \ \sigma^l = \tau^{l^2} = 1, \sigma\tau\sigma^{-1} = \tau^{l+1} \rangle.$$

This group is isomorphic to

$$C(l^2) \rtimes_{\mu_2} C(l)$$

and thus it is of order l^3 and it must coincide with G. □

We start studying $\mathrm{R}_t(k, (C(l) \times C(l)) \rtimes_{\mu_1} C(l))$ for any number field k.

Proposition 3.3.5. *We have*

$$\mathrm{R}_t(k, (C(l) \times C(l)) \rtimes_{\mu_1} C(l)) \subseteq \mathrm{Cl}(k)^{\frac{l-1}{2} l^2}.$$

Proof. Let (K, k_1, k) be a tame μ_1-extension of number fields. By Proposition 1.3.9 the inertia group corresponding to a ramifying prime is cyclic, generated by an element of the form $x^a y^b \sigma^c$ of

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

By induction we obtain

$$(x^a y^b \sigma^c)^n = x^{an} y^{bn} \sigma^{cn + abn(n-1)/2}$$

and thus any nontrivial element in G is of order l. Hence the ramification index of a ramifying prime must be equal to l, i.e.

$$\mathrm{d}(K/k) = \prod_{\mathfrak{p}: \ e_\mathfrak{p} \neq 1} \mathfrak{p}^{(l-1)l^2}$$

and we can conclude. □

Unfortunately the exact sequence

$$1 \to C(l) \times C(l) \to G \to C(l) \to 1$$

does not imply that the group G is isomorphic to $(C(l) \times C(l)) \rtimes_{\mu_1} C(l)$, even if we assume to know the action of $C(l)$ on $C(l) \times C(l)$. This means that we can not use Proposition 3.1.14 to construct extensions with a given Steinitz class and we can not prove that the inclusion in the above proposition is in fact an equality, as has been indeed proved by Clement Bruce in [2] in 2009.

As far as the group $C(l^2) \rtimes_{\mu_2} C(l)$ is concerned, we are going to consider a more general situation.

Lemma 3.3.6. *Let l be an odd prime. The group $G = C(l^n) \rtimes_\mu C(l)$, with $n \geq 2$, where μ sends a generator of $C(l)$ to the elevation to the $l^{n-1}+1$-th power, 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 μ.

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 τ; let $x \in G$ be such that its class modulo H generates G/H, which is cyclic of order l, and such that $x\tau x^{-1} = \tau^{l^{n-1}+1}$, i.e. $x\tau = \tau^{l^{n-1}+1}x$. Then $x^l = \tau^a$ for some $a \in \mathbb{N}$. Since G is of order l^{n+1} and it is not cyclic, the order of x must divide l^n and so

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

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

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

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

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

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

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

Further

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

and σ, τ are generators of G. Thus G must be a quotient of the group

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

But this group has the same order of G and thus they must be equal. □

It follows that we can use Proposition 3.1.14 to study $\mathrm{R}_t(k, C(l^n) \rtimes_\mu C(l))$, for any number field k.

Lemma 3.3.7. *Let τ 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

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

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

Lemma 3.3.8. *We have*

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

Further we can choose G-extensions with a given Steinitz class so that they satisfy the additional condition of Proposition 3.1.14.

Proof. By Proposition 3.1.14 and Lemma 3.3.6,

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

where τ is a generator of $C(l^n)$. We easily conclude since $1 \in \mathrm{R}_t(k, C(l))$ and, by Lemma 3.3.7, $E_{k,\mu,\tau} = k(\zeta_{l^{n-1}})$, i.e.

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

□

Now we consider the opposite inclusion.

Lemma 3.3.9. *Let K/k be a tame $C(l^n) \rtimes_\mu C(l)$-extension of number fields and let $\mathfrak{p}$ be a ramifying prime, with ramification index $e_\mathfrak{p}$. Then the class of*

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

and the class of

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

are both in

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

Proof. The Galois group of K/k is $C(l^n) \rtimes_\mu C(l)$, i.e.

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

By Proposition 1.3.9 the inertia group at $\mathfrak{p}$ is cyclic, generated by an element $\tau^a\sigma^b$; by induction we obtain

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

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

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

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

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

where $a\tilde{a} \equiv l^\beta \pmod{l^n}$. Hence, in particular, the inertia group is a normal subgroup of G. Thus we can decompose our extension in K/k_1 and k_1/k which are both Galois and such that $\mathfrak{p}$ is totally ramified in K/k_1 and unramified in k_1/k. By Lemma 3.1.16 the class of $\mathfrak{p}$ is in $W(k, E_{k,\rho,\tau^a\sigma^b})$, where the action ρ is induced by the conjugation in G and, in particular, it sends τ to the elevation to the $-\tilde{a}bl^{n-1-\beta}+1$-th power, as seen above, and σ 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 $\mathrm{Gal}(k(\zeta_{l^{n-\beta}})/k)$ such that $\nu_{k,\tau^a\sigma^b}(g)$ is congruent to a product of powers of $l^{n-1}+1$ and $-\tilde{a}bl^{n-1-\beta}+1$ modulo $l^{n-\beta}$. But all these are congruent to 1 modulo $l^{n-1-\beta}$ and thus $G_{k,\rho,\tau^a\sigma^b}|_{k(\zeta_{l^{n-1-\beta}})} = \{1\}$. Hence

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

i.e.

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

Hence, by the assumption that $l^2|e_\mathfrak{p}$, the class of

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

is in

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

and the same is true for

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

It remains to consider the case $e_{\mathfrak{p}} = l$. We now define k_1 as the fixed field of τ and we first assume that $\mathfrak{p}$ ramifies in K/k_1. Then its inertia group in $\mathrm{Gal}(K/k_1) = C(l^n)$ is of order l and thus must be generated by $\tau^{l^{n-1}}$. Hence by Lemma 3.1.16 the class of $\mathfrak{p}$ is in $W(k, E_{k,\mu,\tau^{l^{n-1}}})$ and $\mathfrak{p}^{(l-1)\frac{l^{n+1}}{e_{\mathfrak{p}}}}$ 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 $W(k, E_{k,\mu,\tau})^{\frac{l-1}{2}l}$ by Lemma 3.2.11. Hence, by Lemma 3.3.7, the class of

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

is in

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

Finally let us consider the case of $\mathfrak{p}$ ramified in k_1/k. By Lemma 1.2.15 the class of $\mathfrak{p}$ is in $W(k, l)$. Hence the class of

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

is in

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

By Lemma 1.2.18

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

□

Theorem 3.3.10. *We have*

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

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

Proof. By Theorems 1.3.5 and 1.3.6, by Lemma 3.3.8 and Lemma 3.3.9 it is immediate that

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

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

3.4 Some more groups

In this section we study the realizable classes for some groups, which are not included in the families considered in the previous sections.

We start with a proposition concerning the realizable classes for D_4-extensions of a number field.

Proposition 3.4.1. *Let k be a number field, then $\mathrm{R}_t(k, D_4) \supseteq \mathrm{Cl}(k)^2$. As a particular case we obtain a result proved by Bouchaïb Sodaïgui in [23]: if the class number of k is odd then $\mathrm{R}_t(k, D_4) = \mathrm{Cl}(k)$.*

Proof. By definition

$$D_4 = \langle \tau, \sigma : \ \tau^4 = \sigma^2 = 1, \sigma\tau\sigma = \tau^3 \rangle.$$

The subgroup generated by τ^2 and σ is normal in D_4, it is isomorphic to $C(2) \times C(2)$ and it has trivial intersection with the subgroup generated by $\tau\sigma$, which is cyclic of order 2. Further τ^2, σ and $\tau\sigma$ generate the whole group D_4. It follows that

$$D_4 \cong (C(2) \times C(2)) \rtimes_\mu C(2),$$

where the action μ is defined by the matrix

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

by an easy calculation. In particular, we have the following exact sequence:

$$1 \to C(2) \times C(2) \to D_4 \to C(2) \to 1.$$

This exact sequence identifies the group D_4, since the only other nonabelian group of order 8, i.e. Q_8, does not have subgroups isomorphic to $C(2) \times C(2)$. Hence, recalling that $W(k, 2) = \mathrm{Cl}(k)$, by Proposition 3.1.15 we obtain that

$$\mathrm{Cl}(k)^2 = \mathrm{Cl}(k)^{\frac{2\cdot 4}{2\cdot 2}} \subseteq \mathrm{R}_t(k, D_4).$$

□

The second group we are going to consider is S_4.

Proposition 3.4.2. *Let k be a number field, then $\mathrm{R}_t(k, S_4) \supseteq \mathrm{Cl}(k)^2$. As a particular case we obtain a result proved by Marjory Godin and Bouchaïb Sodaïgui in [11]: if the class number of k is odd then $\mathrm{R}_t(k, S_4) = \mathrm{Cl}(k)$.*

Proof. The subgroup H of S_4 generated by $(12)(34)$ and $(13)(24)$ is normal in S_4 and the quotient G/H is generated by $(124)H$ and by $(14)H$ and so it is isomorphic to S_3. Hence we have the following exact sequence:

$$1 \to C(2) \times C(2) \to S_4 \to S_3 \to 1.$$

The 2-Sylow subgroup D_4 of S_4 is identified by the above sequence, by the same arguments seen in the proof of Proposition 3.4.1. The only groups of order 24 with 2-Sylow subgroups isomorphic to D_4 are: S_4, D_{12}, $C(3) \times D_4$ and $(C(6) \times C(2)) \rtimes C(2)$. So let G be a group such that we have the following exact sequence

$$1 \to C(2) \times C(2) \to G \to S_3 \to 1$$

and that the action of S_3 on $C(2) \times C(2)$ is the same as in S_4. The group G cannot be D_{12}, since this has no normal subgroups isomorphic to $C(2) \times C(2)$, and it is also different from $C(3) \times D_4$, since in this group the elements of order 3 commute with everything else (while $(124)(12)(34) \neq (12)(34)(124)$, for example). To conclude we see that any element of order 3 in $(C(6) \times C(2)) \rtimes C(2)$ commutes with the elements of any normal subgroup isomorphic to $C(2) \times C(2)$. Hence G must be isomorphic to S_4.

Therefore, recalling that $W(k,2) = \mathrm{Cl}(k)$, by Proposition 3.1.14, by Proposition 3.1.15 and by the example following Proposition 3.2.18 we obtain that

$$\mathrm{Cl}(k)^2 = \mathrm{Cl}(k)^4\mathrm{Cl}(k)^6 = \mathrm{R}_t(k, S_3)^4 W(k,2)^{\frac{6\cdot 4}{2\cdot 2}} \subseteq \mathrm{R}_t(k, S_4).$$

□

Now we are going to consider the group $G = A_4 \times S_3$. This is an A'-group of even order and it is a direct products of two good groups, but we cannot conclude that G is good using Theorem 3.2.15, since A_4 and S_3 both have even order and S_3 has cyclic 2-Sylow subgroups.

Proposition 3.4.3. *Let k be a number field, then $\mathrm{R}_t(k, A_4 \times S_3) = \mathrm{Cl}(k)^6$. Further $G = A_4 \times S_3$ is a good group.*

Proof. First of all we calculate $\mathrm{R}_t(k, G)$, proving both the requested inclusions.

- $\supseteq$ As we have seen in the example after Proposition 3.2.22, A_4 is good and
$$\mathrm{R}_t(k, A_4) = \mathrm{Cl}(k).$$
By Proposition 3.2.18 we know that $S_3 = D_3$ is good and thus in particular that $1 \in \mathrm{R}_t(k, S_3)$, since this must be a group. Hence considering

compositions of disjoint A_4- and S_3-extensions of k and using Proposition 1.3.7 we obtain that

$$\mathrm{R}_t(k, A_4 \times S_3) \supseteq \mathrm{R}_t(k, A_4)^6 \mathrm{R}_t(k, S_3)^{12} \supseteq \mathrm{Cl}(k)^6.$$

$\subseteq$ Let K/k be a tame number fields extension with Galois group $A_4 \times S_3$.

By Proposition 1.3.9, the ramification index at a prime $\mathfrak{p}$, ramifying in the extension K/k must divide 6. Hence the class of

$$\mathfrak{p}^{\frac{1}{2}(e_\mathfrak{p}-1)\frac{72}{e_\mathfrak{p}}}$$

is in $\mathrm{Cl}(k)^6$ and so, by Theorems 1.3.5 and 1.3.6, the same is true also for the Steinitz class of K/k.

So we have proved that $\mathrm{R}_t(k, A_4 \times S_3) = \mathrm{Cl}(k)^6$. It is now straightforward to verify that the conditions of the definition of good groups are all satisfied. □

We are now going to study the group $G = (C(4) \times C(4)) \rtimes_\mu C(3)$, where μ sends a generator of $C(3)$ to the map defined by the matrix

$$\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

In other words,

$$G = \langle x, y, \sigma : \ x^4 = y^4 = \sigma^3 = 1, \sigma x \sigma^{-1} = xy, \sigma y \sigma^{-1} = xy^2, yx = xy \rangle.$$

Proposition 3.4.4. *Let k be a number field, then*

$$\mathrm{R}_t(k, (C(4) \times C(4)) \rtimes_\mu C(3)) = W(k, 4)^2.$$

Further $G = (C(4) \times C(4)) \rtimes_\mu C(3)$ is a good group.

Proof. First of all we prove the equality concerning the realizable classes $\mathrm{R}_t(k, (C(4) \times C(4)) \rtimes_\mu C(3))$.

$\supseteq$ By Proposition 1.2.12 and by Theorem 2.1.8,

$$W(k, 4)^2 \subseteq \mathrm{Cl}(k)^2 \subseteq W(k, 3) = \mathrm{R}_t(k, C(3)).$$

Hence by Propositions 3.1.14 and 3.1.15 we obtain that

$$\begin{aligned} \mathrm{R}_t(k, (C(4) \times C(4)) \rtimes_\mu C(3)) &\supseteq \mathrm{R}_t(k, C(3))^{16} W(k, 4)^6 \\ &\supseteq W(k, 4)^{32} W(k, 4)^6 = W(k, 4)^2. \end{aligned}$$

$\subseteq$ We observe that $E_{k,\mu,\tau} = k(\zeta_4)$, for any $\tau \in C(4) \times C(4)$ of order 4. Thus, with the notation of Lemma 3.2.6, if $e_{\mathfrak{P}} = 4$ then, by Lemma 3.1.16, the class of

$$\mathfrak{p}^{\frac{1}{2}(e_{\mathfrak{p}} e_{\mathfrak{P}} - 1)\frac{48}{e_{\mathfrak{p}} e_{\mathfrak{P}}}} = \mathfrak{p}^{(4e_{\mathfrak{p}} - 1)\frac{6}{e_{\mathfrak{p}}}}$$

is in

$$W(k, E_{k,\mu,\tau})^2 = W(k, 4)^2.$$

If $e_{\mathfrak{P}}|2$, then the class of

$$\mathfrak{p}^{\frac{1}{2}(e_{\mathfrak{p}} e_{\mathfrak{P}} - 1)\frac{48}{e_{\mathfrak{p}} e_{\mathfrak{P}}}}$$

is in

$$\mathrm{Cl}(k)^4 \subseteq W(k, 4)^2.$$

This proves the equality. At this point it is straightforward to prove that G is a good group. □

Proposition 3.4.5. *Let k be a number field, then*

$$\mathrm{R}_t(k, (C(4) \times C(4)) \rtimes_\mu C(3) \times C(2)) = W(k, 4)^4$$

and

$$\mathrm{R}_t(k, (C(4) \times C(4)) \rtimes_\mu C(3) \times C(4)) = W(k, 4)^8.$$

Further $G_1 = (C(4) \times C(4)) \rtimes_\mu C(3) \times C(2)$ and $G_2 = (C(4) \times C(4)) \rtimes_\mu C(3) \times C(4)$ are good groups.

Proof. To prove one inclusion we compose extensions with Galois group $G = (C(4) \times C(4)) \rtimes_\mu C(3)$ with arithmetically disjoint $C(2)$- and $C(4)$-extensions with trivial Steinitz classes.

Now let us prove the opposite inclusion for the group G_1. Let $\mathfrak{p}$ be a prime ramifying in a tame number fields extension K/k with Galois group G_1. As in Lemma 3.2.13 we call k_1 and k_2 subextensions of K/k with Galois groups G and $C(2)$ respectively and such that $K = k_1 k_2$. Further let $e_{\mathfrak{p},i}$ be the ramification index of $\mathfrak{p}$ in k_i/k and $e_{\mathfrak{p}} = \mathrm{lcm}(e_{\mathfrak{p},1}, e_{\mathfrak{p},2})$ the ramification index in K/k. In particular for any prime l dividing $e_{\mathfrak{p}}$, $e_{\mathfrak{p}}(l) = \max\{e_{\mathfrak{p},1}(l), e_{\mathfrak{p},2}(l)\}$.

Recalling Lemma 2.1.6, we have

$$\begin{aligned}\mathfrak{p}^{(e_{\mathfrak{p}} - 1)\frac{96}{e_{\mathfrak{p}}}} &= \prod_{l | e_{\mathfrak{p}}} \mathfrak{p}^{a_l (l-1)\frac{96}{e_{\mathfrak{p}}(l)}} \\ &= \prod_{\substack{l | e_{\mathfrak{p}} \\ e_p(l) = e_{\mathfrak{p},1}(l)}} \left(\mathfrak{p}^{a_l (l-1)\frac{48}{e_{\mathfrak{p},1}(l)}}\right)^2 \prod_{\substack{l | e_{\mathfrak{p}} \\ e_p(l) \neq e_{\mathfrak{p},1}(l)}} \left(\mathfrak{p}^{a_l (l-1)\frac{2}{e_{\mathfrak{p},2}(l)}}\right)^{48},\end{aligned}$$

where all the exponents $a_l(l-1)\frac{48}{e_{\mathfrak{p},1}(l)}$ are even (by Proposition 1.3.9). Thus, recalling that G is good, the class of

$$\mathfrak{p}^{\frac{1}{2}(e_{\mathfrak{p}}-1)\frac{96}{e_{\mathfrak{p}}}}$$

is in

$$\mathrm{R}_t(k,G)^2\mathrm{Cl}(k)^{24} = W(k,4)^4\mathrm{Cl}(k)^{24} = W(k,4)^4.$$

In the case of the group G_2 we can follow the same ideas, obtaining

$$\mathfrak{p}^{(e_{\mathfrak{p}}-1)\frac{192}{e_{\mathfrak{p}}}} = \prod_{\substack{l|e_{\mathfrak{p}} \\ e_p(l)=e_{\mathfrak{p},1}(l)}} \left(\mathfrak{p}^{a_l(l-1)\frac{48}{e_{\mathfrak{p},1}(l)}}\right)^4 \prod_{\substack{l|e_{\mathfrak{p}} \\ e_p(l)\neq e_{\mathfrak{p},1}(l)}} \left(\mathfrak{p}^{a_l(l-1)\frac{4}{e_{\mathfrak{p},2}(l)}}\right)^{48},$$

and so, recalling also Lemma 1.2.15 and Lemma 1.2.18, that the class of

$$\mathfrak{p}^{\frac{1}{2}(e_{\mathfrak{p}}-1)\frac{192}{e_{\mathfrak{p}}}}$$

is in

$$\mathrm{R}_t(k,G)^4W(k,4)^{24} = W(k,4)^8W(k,4)^{24} = W(k,4)^8.$$

At this point there is no difficulty in proving that G_1 and G_2 are good.

This proposition could also have been proved directly, without using the result for $\mathrm{R}_t(k,G)$, exactly with the same arguments of Proposition 3.4.4, i.e. writing G_1 and G_2 as follows:

$$G_1 = (C(4)\times C(4)\times C(2))\rtimes_{\mu_1} C(3)$$
$$G_1 = (C(4)\times C(4)\times C(4))\rtimes_{\mu_2} C(3),$$

where the actions μ_1 and μ_2 are defined in the obvious way.

On the contrary we remark that we could not simply use Theorem 3.2.15, since G is of even order and $C(2)$ (respectively $C(4)$) have cyclic 2-Sylow subgroups. □

Of course we have proved that the above groups are good and thus we can use Theorem 3.2.8 and Theorem 3.2.15 to prove that a lot of other groups obtained by the above ones with direct and semidirect products are good, and hence in particular satisfy the conjecture about realizable Steinitz classes.

We will now generalize the result of Lemma 3.3.8 to a slightly more general situation. We consider groups of the form $C(l^n)\rtimes_\mu C(ld)$, where d divides $l-1$ and μ sends a generator of $C(ld)$ to an automorphism of order ld of $C(l^n)$.

First of all we need a generalization of Lemma 3.3.6.

Lemma 3.4.6. *The group $C(l^n) \rtimes_\mu C(ld)$ is identified by the exact sequence*

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

if the action of $C(ld)$ on $C(l^n)$ is given by μ.

Proof. Let G be the group written in the above exact sequence. Let $\tilde{x}$ and $\tilde{y}$ be elements of order l and d in $C(ld)$; let x and y be elements of G in the counterimages of $\tilde{x}$ and $\tilde{y}$ by the projection $G \to C(ld)$. Let σ be a generator of $C(l^n) \subseteq G$ and let H_1 be the subgroup of G generated by σ and x. We have the following exact sequence

$$1 \to C(l^n) \to H_1 \to C(l) \to 1,$$

where the induced action is the same as in $C(l^n) \rtimes_\mu C(l)$. Thus by Lemma 3.3.6

$$H_1 \cong C(l^n) \rtimes C(l)$$

and it is clear that H_1 is normal in G. Further we can assume that the order of y is exactly d (if this is not true, we can simply redefine y as y^{l^n}), i.e. that y generates a cyclic subgroup H_2 of G of order d. By construction any element of G may be uniquely written as a product of an element of H_1 and one of H_2. It follows that

$$G \cong H_1 \rtimes H_2 \cong (C(l^n) \rtimes C(l)) \rtimes C(d).$$

At this point we easily conclude that

$$G \cong C(l^n) \rtimes_\mu C(ld).$$

□

Proposition 3.4.7. *We have*

$$\mathrm{R}_t(k, C(l^n) \rtimes_\mu C(ld)) \supseteq \mathrm{R}_t(k, C(d))^{l^{n+1}} W\left(k, E_{k,\mu,\sigma}\right)^{\frac{l-1}{2} ld},$$

where σ is a generator of the $C(l^n)$-normal subgroup of $C(l^n) \rtimes_\mu C(ld)$.

Proof. By Corollary 2.3.8, Proposition 3.1.14 and Lemma 3.4.6,

$$\begin{aligned}
\mathrm{R}_t(k, C(l^n) \rtimes_\mu C(ld)) &\supseteq \mathrm{R}_t(k, C(ld))^{l^n} W\left(k, E_{k,\mu,\sigma}\right)^{\frac{l-1}{2} ld} \\
&\supseteq \mathrm{R}_t(k, C(d))^{l^{n+1}} \mathrm{R}_t(k, C(l))^{l^n d} W\left(k, E_{k,\mu,\sigma}\right)^{\frac{l-1}{2} ld} \\
&\supseteq \mathrm{R}_t(k, C(d))^{l^{n+1}} W\left(k, E_{k,\mu,\sigma}\right)^{\frac{l-1}{2} ld}.
\end{aligned}$$

□

As a particular case of the above situation we consider the group $G = C(9) \rtimes_\mu C(6)$.

Proposition 3.4.8. *Let k be a number field, then*

$$\mathrm{R}_t(k, C(9) \rtimes_\mu C(6)) = \mathrm{Cl}(k)^3.$$

Further $G = C(9) \rtimes_\mu C(6)$ is a good group.

Proof. Since there are no cyclic subgroups of G of order 27, a prime ramifying in a tame G-extension of k, must have ramification index dividing 18. Thus every prime ideal dividing the discriminant appears with a power which is multiple of 3 and hence the square of the Steinitz class is in $\mathrm{Cl}(k)^3$ and the same must be true for the Steinitz class itself.

For the opposite inclusion we use Lemma 3.4.7 and Proposition 3.2.17, observing that $E_{k,\mu,\sigma} = k$, i.e. that $W(k, E_{k,\mu,\sigma}) = \mathrm{Cl}(k)$.

The proof of the properties of good groups is now straightforward. □

Bibliography

[1] *Algebraic number theory.* Proceedings of an instructional conference organized by the London Mathematical Society (a NATO Advanced Study Institute) with the support of the International Mathematical Union. Edited by J. W. S. Cassels and A. Fröhlich. Academic Press, London, 1967.

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

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

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

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

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

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

[8] C. W. Curtis and I. Reiner. *Methods of representation theory. Vol. I.* John Wiley & Sons Inc., New York, 1981.

[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.

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

[13] S. Lang. *Algebra*. GTM 211. Springer-Verlag, New York, third edition, 2002.

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

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

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

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

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

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

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

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

[22] B. Sodaïgui. 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.

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

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