Projective modules of group rings over quadratic number fields

Iftikhar Ahmed

Iftikhar Ahmed

Projective Modules of Group Rings over Quadratic Number Fields

— a thesis submitted in 1994 for the degree of Ph.D.

Department of Mathematics
University of Durham
Science Laboratories
South Road
Durham DH1 3LE
England

Abstract

Let K be a quadratic number field, $\mathcal{O}_K$ its ring of integers, and G a cyclic group of order prime p. In this thesis, we study the kernel group $D(\mathcal{O}_K G)$ and obtain a number of results concerning its order and structure. For K imaginary, we also investigate the subset $R(\mathcal{O}_K G)$ of the locally free class group $Cl(\mathcal{O}_K G)$ consisting of classes which occur as rings of integers of tame extensions of K with Galois group isomorphic to G. We calculate $R(\mathcal{O}_K G)$ under a variety of conditions and obtain, for an arbitrary tame extension L of K with group G, invariants which determine the class of $\mathcal{O}_L$ in $R(\mathcal{O}_K G)$.

Declaration

The material in this thesis has not been submitted previously for any degree in this or any other university and is my own work unless referenced to the contrary in the text.

Acknowledgements

I would like to record my indebtedness to Dr. S.M.J. Wilson, my supervisor during my postgraduate studies. It is customary for a research student to indicate, at the completion of his thesis, his indebtedness to his supervisor. But in my case, it must be acknowledged, it is not through a sense of conforming with custom that I express my gratitude to my supervisor. Because of my initial education in theoretical physics and the lack of any training in pure mathematics, he was not only responsible for overseeing my research but, in the earlier part of my studies, he also had the extra burden of guiding me through introductory literature on various aspects of pure mathematics. I am very grateful for all the help and advice I received from him throughout the course. I am particularly grateful to him for putting up with the rather retarded pace at which I carried out my research. It indeed has been a pleasure to work under his supervision and I thank him for his constant guidance and unfailing patience.

Contents

1. Introduction

Let K be an algebraic number field, $\mathcal{O}_K$ the ring of integers in K, and A a finite dimensional semisimple K-algebra with 1. Let Λ be an $\mathcal{O}_K$-order in A. By definition, Λ is a subring of A which is a finitely generated $\mathcal{O}_K$-module, and $K \otimes_{\mathcal{O}_K} \Lambda \simeq A$. For each prime P of K we denote by $\mathcal{O}_{K,P}$ the localization of $\mathcal{O}_K$ at P. A Λ-lattice is a finitely generated (left) Λ-module which is $\mathcal{O}_K$-torsion free. Let M be a Λ-lattice and $M_P = \mathcal{O}_{K,P} \otimes_{\mathcal{O}_K} M$ its localization at a prime P of K. Then M_P is a (left) Λ_P-module where $\Lambda_P = \mathcal{O}_{K,P} \otimes_{\mathcal{O}_K} \Lambda$. The Λ-lattice M is said to be a locally free Λ-module if M_P is a free Λ_P-module for all P. In the case when M is locally free let $r(M)$ denote its local rank. The rank $r(M)$ is the same for all P.

Next we define the locally free class group $Cl(\Lambda)$. Let $S(\Lambda)$ denote the abelian group of locally free Λ-modules. The group $S(\Lambda)$ is the free abelian group generated by symbols $[M]$, one for each isomorphism class of locally free Λ-modules M. Let $T(\Lambda)$ be the subgroup of $S(\Lambda)$ generated by expressions of the form $[M \oplus N] - [M] - [N]$. Set

$$P(\Lambda) = \frac{S(\Lambda)}{T(\Lambda)}.$$

The map $[M] \mapsto r(M)$ induces a surjective homomorphism between the groups $P(\Lambda)$ and $\mathbb{Z}$, and $Cl(\Lambda)$ is defined to be its kernel. The locally free class group $Cl(\Lambda)$ thus occurs in the following exact sequence:

$$1 \to Cl(\Lambda) \to P(\Lambda) \to \mathbb{Z} \to 0.$$

The class group $Cl(\Lambda)$ is the subgroup of $P(\Lambda)$ consisting of elements of the form $[M] - [N]$ where M and N are of the same rank. The group $Cl(\Lambda)$ is a finite group. This follows from the fact that each element of $Cl(\Lambda)$ can be written as $[M] - [\Lambda]$ where M is a locally free Λ-lattice in A with $r(M) = 1$ (see [13]), and by the Jordan-Zassenhaus theorem (see, for example, [11], §26) there are finitely many isomorphism classes of such lattices.

Let $\Lambda' \supset \Lambda$ be a maximal $\mathcal{O}_K$-order in A. The map defined by

$$[M] \mapsto [\Lambda' \otimes_\Lambda M]$$

gives a surjective homomorphism $Cl(\Lambda) \to Cl(\Lambda')$ (see [14]). Let $D(\Lambda)$ denote the kernel, then we have the exact sequence:

$$1 \to D(\Lambda) \to Cl(\Lambda) \to Cl(\Lambda') \to 1.$$

It can be shown that up to isomorphism $D(\Lambda)$ is independent of the choice of the

maximal order Λ' containing Λ (see [8]).

The significance of the class group $Cl(\Lambda)$ and the kernel group $D(\Lambda)$ is that if L is a tame Galois extension of K with Galois group G then $\Lambda = \mathcal{O}_K G$ is an $\mathcal{O}_K$-order contained in the K-algebra KG and

$$(\mathcal{O}_L) = [\mathcal{O}_L] - [\mathcal{O}_K G]$$

defines a class in $Cl(\mathcal{O}_K G)$. Identification of the class $(\mathcal{O}_L)$ in $Cl(\mathcal{O}_K G)$ is of great interest and is the central problem of "relative additive Galois module structure". In "absolute additive Galois module structure" where $K = \mathbb{Q}$ it was proved by Fröhlich [4] that $(\mathcal{O}_L) \in D(\mathcal{O}_K G)$. It is this discovery that makes $D(\mathbb{Z}G)$ and, in general, $D(\mathcal{O}_K G)$ interesting to study, and indeed it is precisely this group $D(\mathcal{O}_K G)$ that is the topic of our investigations here. We will study $D(\mathcal{O}_K G)$ in the case when K is a quadratic number field and G is a cyclic group of order odd prime p.

The calculation of $D(\mathcal{O}_K G)$, as we will see, depends on whether or not p is ramified in K. The case when p is unramified in K was partially dealt by Homayouni in his Ph.D. thesis [6]. In this case we give results which can be regarded as an extension of Homayouni's work. We will also discuss the case when p is ramified in K. This case, we will see, splits into two further cases: K is ramified at p only, and K is ramified at p as well as at primes distinct from p. We will study both cases. In the latter we will show that the calculation of $D(\mathcal{O}_K G)$ can be reduced to a calculation of a kernel group of the form $D(\mathcal{O}_{K'} G)$ where K' is a quadratic number field which is unramified at p but otherwise has the same ramification as the field K.

For the rational case where $K = \mathbb{Q}$ it is well known that the kernel group $D(\mathbb{Z}G)$ is trivial (see [3]). It will be interesting for us to see here how our findings for $D(\mathcal{O}_K G)$ compare with $D(\mathbb{Z}G)$.

Another aspect of $Cl(\mathcal{O}_K G)$ which we will investigate in the present work is the subset $R(\mathcal{O}_K G)$ of $Cl(\mathcal{O}_K G)$ consisting of realizable classes, i.e., classes of the form $(\mathcal{O}_L)$ where L is a tame extension of K with Galois group isomorphic to G. (An extension L/K is tame if for each prime r of $\mathcal{O}_K$, the ramification index e_r of r in L is relatively prime to r.) For an arbitrary tame extension L of K with group G the ring $\mathcal{O}_L$ of integers is a locally free $\mathcal{O}_K G$-module and hence it defines a class $(\mathcal{O}_L)$ in $R(\mathcal{O}_K G)$. The problem of determining the structure of $\mathcal{O}_L$ as an $\mathcal{O}_K G$-module is equivalent to identifying the class of $\mathcal{O}_L$ in $R(\mathcal{O}_K G)$. If $\mathcal{O}_L$ corresponds to the trivial class in $R(\mathcal{O}_K G)$ then the extension L/K has the interesting property of possessing a normal integral basis, i.e., an $\mathcal{O}_K$-basis for $\mathcal{O}_L$ consisting of G-conjugates of a single

element in $\mathcal{O}_L$.

L. McCulloh in [10] showed that for an arbitrary finite abelian group G the set $R(\mathcal{O}_K G)$ of realizable classes forms a subgroup of $Cl(\mathcal{O}_K G)$ which in the case of a cyclic group G of order prime p can be described in terms of the action on $Cl^0(\mathcal{O}_K G)$ of a Stickelberger ideal in the integral group ring $\mathbb{Z}\Delta$, where

$$Cl^0(\mathcal{O}_K G) = \mathrm{Ker}(Cl(\mathcal{O}_K G) \to Cl(\mathcal{O}_K)),$$

and $\Delta \simeq \mathrm{Aut}(G)$. We will use this description to study $R(\mathcal{O}_K G)$ in the case when K is a quadratic imaginary number field and G is a cyclic group of order prime p. In the case when $K(\zeta_p)$ (ζ_p here is a primitive pth root of unity) has trivial ideal class group we will calculate $R(\mathcal{O}_K G)$ and determine the precise conditions under which a tame extension L of K with group G has a normal integral basis. We will also discuss $R(\mathcal{O}_K G)$ under a slightly less restrictive set of conditions.

Again for comparison with our calculations, it is worth mentioning briefly here that in the rational case we have Taylor's theorem [15] which implies, for an arbitrary finite group G, $R(\mathbb{Z}G) = 1$ if G has no complex irreducible symplectic characters, and if G has such characters then the elements of $R(\mathbb{Z}G)$ have order at most 2 in $Cl(\mathbb{Z}G)$. In particular, if G is abelian then $R(\mathbb{Z}G) = 1$.

In the next section we will start in earnest with the task of calculating $D(\mathcal{O}_K G)$, but we end the present section with the description of a technique for calculating $D(\Lambda)$ which we will repeatedly use. Let

$$\begin{array}{ccc} \Lambda & \xrightarrow{i_1} & \Lambda_1 \\ \downarrow{\scriptstyle i_2} & & \downarrow{\scriptstyle j_1} \\ \Lambda_2 & \xrightarrow{j_2} & \overline{\Lambda} \end{array}$$

be a commutative square of rings and ring homomorphisms. The square is said to be cartesian if for all $(\lambda_1, \lambda_2) \in \Lambda_1 \times \Lambda_2$ with $j_1(\lambda_1) = j_2(\lambda_2)$ there is a unique $\lambda \in \Lambda$ with $i_1(\lambda) = \lambda_1$, $i_2(\lambda) = \lambda_2$. If the square is cartesian then Λ can be identified with the subring

$$\{(\lambda_1, \lambda_2) \in \Lambda_1 \times \Lambda_2 \mid j_1(\lambda_1) = j_2(\lambda_2)\}$$

of $\Lambda_1 \times \Lambda_2$. Cartesian squares can arise in a variety of ways. If, for example, I and J were two two-sided ideals of the ring Λ which have trivial intersection then there is a cartesian square

$$\begin{array}{ccc} \Lambda & \xrightarrow{i_1} & \Lambda/J \\ \downarrow{\scriptstyle i_2} & & \downarrow{\scriptstyle j_1} \\ \Lambda/I & \xrightarrow{j_2} & \Lambda/(I+J) \end{array}$$

where all the maps are canonical.

For an arbitrary number field K if an $\mathcal{O}_K$-order Λ contained in a commutative finite-dimensional semisimple K-algebra A is given by a cartesian square

$$\begin{array}{ccc} \Lambda & \xrightarrow{i_1} & \Lambda_1 \\ \downarrow{\scriptstyle i_2} & & \downarrow{\scriptstyle j_1} \\ \Lambda_2 & \xrightarrow{j_2} & \overline{\Lambda} \end{array}$$

in which

a) each Λ_i is an $\mathcal{O}_K$-order contained in K-algebra A_i,
b) $\overline{\Lambda}$ is an $\mathcal{O}_K$-torsion $\mathcal{O}_K$-algebra, and
c) at least one of the maps j_1 and j_2 is surjective,
then the sequence

$$1 \to \Lambda^\times \to \Lambda_1^\times \times \Lambda_2^\times \to \overline{\Lambda}^\times \to D(\Lambda) \to D(\Lambda_1) \times D(\Lambda_2) \to 1 \qquad (1.1)$$

is exact (see [12]). The map $D(\Lambda) \to D(\Lambda_1) \times D(\Lambda_2)$ is the restriction of

$$Cl(\Lambda) \to Cl(\Lambda_1) \times Cl(\Lambda_2),$$
$$[M] - [\Lambda] \mapsto ([\Lambda_1 \otimes_\Lambda M] - [\Lambda_1], [\Lambda_2 \otimes_\Lambda M] - [\Lambda_2]),$$

to $D(\Lambda)$, and the map $\overline{\Lambda}^\times \to D(\Lambda)$ sends $u \in \overline{\Lambda}^\times$ to $[(\Lambda, u)] - [\Lambda]$, where

$$(\Lambda, u) = \{(\lambda_1, \lambda_2) \in \Lambda_1 \times \Lambda_2 \mid j_1(\lambda_1)u = j_2(\lambda_2)\}$$

is a locally free Λ-lattice.

The usefulness of the sequence (1.1) lies in the fact that often it is easier to calculate $D(\Lambda_1)$ and $D(\Lambda_2)$ than calculating $D(\Lambda)$ directly. In cases where Λ_1 or Λ_2 is a maximal order, the corresponding kernel group vanishes and this simplifies the calculation of $D(\Lambda)$ even further.

Later on when calculating $D(\mathcal{O}_K G)$ in the case when p is ramified in K, we will encounter a cartesian square for which the condition (a) given above will not hold. For such a square the exact sequence (1.1) is replaced by

$$1 \to \Lambda^\times \to \Lambda_1^\times \times \Lambda_2^\times \to \overline{\Lambda}^\times \to \mathrm{Pic}(\Lambda) \to \mathrm{Pic}(\Lambda_1) \times \mathrm{Pic}(\Lambda_2) \to \mathrm{Pic}(\overline{\Lambda}), \qquad (1.2)$$

where $\mathrm{Pic}(\Lambda)$ is the group of isomorphism classes of invertible Λ-modules, with group operation given by $\otimes_\Lambda$ (see [12]). The sequence (1.2) does not explicitly involve $D(\Lambda)$, but, in spite of this, we will still be able to use it to calculate the kernel group $D(\mathcal{O}_K G)$. We leave the details till we actually come to calculate $D(\mathcal{O}_K G)$.

Notation

For a finite abelian extension L of $\mathbb{Q}$ we will write $\mathcal{O}_L$ for the ring of integers in L, E_L for the group of units in $\mathcal{O}_L$, and W_L for the group of roots of unity in E_L. We may also use $\mathcal{O}_L^\times$ to denote E_L. For x in L, $\mathrm{norm}_L(x)$ will denote the absolute norm of x from L to $\mathbb{Q}$. The maximal real subfield of L will be denoted by L^+.

We will represent comlpex conjugation by c; if x is an algebraic number then the complex conjugate of x will be written as x^c. The rest of the notation is as follows.

p = an odd prime,
$G = \langle g \mid g^p = 1 \rangle$, a cyclic group of order p,
$K = \mathbb{Q}(\sqrt{-d})$, a quadratic number field (d is square-free),
$Gal(K/\mathbb{Q}) = \langle \sigma \mid \sigma^2 = 1 \rangle$,
$d(K/\mathbb{Q})$ = discriminant of K,
$\mathcal{O}_K = \mathbb{Z}[\alpha]$, $\alpha = (1 + \sqrt{-d})/2$ if $d \equiv 3 \bmod (4)$, $\alpha = \sqrt{-d}$ otherwise,
$\zeta_p = e^{2\pi i/p}$, a primitive pth root of unity,
$N = \mathbb{Q}(\zeta_p)$,
$M = KN = \mathbb{Q}(\sqrt{-d}, \zeta_p)$.

2. $D(\mathcal{O}_K G)$, p unramified in K

In this section we will calculate the kernel group $D(\mathcal{O}_K G)$ in the case when p is unramified in K. We will prove:

(2.1) THEOREM. *The kernel group $D(\mathcal{O}_K G)$ is cyclic whose order divides $p+1$ or $p-1$ depending on whether p is inert or it splits in K.*

(2.2) THEOREM. *If K is a quadratic imaginary number field, then the cyclic group $D(\mathcal{O}_K G)$ has order*

$$|D(\mathcal{O}_K G)| = \begin{cases} p^*/4, & \text{if } K = \mathbb{Q}(\sqrt{-1}), \\ p^*/6, & \text{if } K = \mathbb{Q}(\sqrt{-3}), \\ p^*/Q_M, & \text{otherwise,} \end{cases}$$

where

$$p^* = \begin{cases} p+1, & \text{if } p \text{ is inert in } K, \\ p-1, & \text{if } p \text{ splits in } K, \end{cases}$$

and Q_M is the index of $W_M E_{M^+}$ in E_M. The possible values for Q_M are 1 and 2.

We begin with the proof of (2.1).

Proof of (2.1). Let $\Lambda = \mathcal{O}_K G$, $I = (1-g)\mathcal{O}_K G$, and $J = (1+g+\cdots+g^{p-1})\mathcal{O}_K G$. Then

$$\begin{array}{ccc} \Lambda/(I \cap J) & \xrightarrow{i_1} & \Lambda/J \\ \downarrow{\scriptstyle i_2} & & \downarrow{\scriptstyle j_1} \\ \Lambda/I & \xrightarrow{j_2} & \Lambda/(I+J) \end{array}$$

is a cartesian square.

The ring Λ/I is isomorphic to $\mathcal{O}_K$. To show that, consider the map $\Lambda \to \mathcal{O}_K$, $g \mapsto 1$, which clearly is a surjective ring homomorphism. The ideal I lies in the kernel. In fact, I is the kernel. Let $x = x_1 g_1 + \cdots + x_p g_p \in \Lambda$, $g_i = g^i$, be an element which lies in the kernel. We want to show that

$$x = (1-g)(a_1 g_1 + \cdots + a_p g_p),$$

or

$$x_1 g_1 + \cdots + x_p g_p = (a_1 - a_p)g_1 + (a_2 - a_1)g_2 + \cdots + (a_p - a_{p-1})g_p$$

is soluble for $a_i \in \mathcal{O}_K$. Equating coefficients of g_i for $1 \leq i \leq p$ gives

$$\begin{aligned} a_1 - a_p &= x_1, \\ a_i - a_{i-1} &= x_i, \qquad 2 \leq i \leq p. \end{aligned}$$

The above equations are soluble and they give

$$a_i = \sum_{j=1}^{i} x_j + x_p, \qquad 1 \leq i \leq p-1,$$

and $a_p = x_p$. Therefore if x lies in the kernel then it can be written as $x = (1 - g)(a_1 g_1 + \cdots + a_p g_p)$, $a_i \in \mathcal{O}_K$, which shows that $x \in I = (1-g)\Lambda$. Therefore, under the map $g \mapsto 1$, $\Lambda/I \simeq \mathcal{O}_K$.

The ring Λ/J is isomorphic to $\mathcal{O}_M$. The isomorphism is induced by the map $\Lambda \to \mathcal{O}_M$, $g \mapsto \zeta_p$, which is a surjective ring homomorphism. Let $x = x_1 g_1 + \cdots + x_p g_p$ be an element which lies in the kernel. Then $x_1 \zeta_p + \cdots + x_{p-1}\zeta_p^{p-1} + x_p = 0$ and therefore $x_1 = x_2 = \cdots = x_p$. So any element which lies in the kernel lies in $(1 + g + \cdots + g^{p-1})\mathcal{O}_K$ and, of course, $(1 + g + \cdots + g^{p-1})\mathcal{O}_K$ lies in the kernel. So the kernel is $(1 + g + \cdots + g^{p-1})\mathcal{O}_K$. But the element $1 + g + \cdots + g^{p-1}$ is unchanged under the multiplication by the elements of G, and therefore

$$(1 + g + \cdots + g^{p-1})\mathcal{O}_K = (1 + g + \cdots + g^{p-1})\mathcal{O}_K G,$$

which proves our assertion that J is the kernel and $\Lambda/J \simeq \mathcal{O}_M$.

Finally, the ring $\Lambda/(I + J)$ is isomorphic to $\mathcal{O}_K/p\mathcal{O}_K$. The map $\Lambda \to \mathcal{O}_K/p\mathcal{O}_K$, $g \mapsto 1$, is clearly surjective. Let $x = x_1 g_1 + \cdots + x_p g_p$ be an element which lies in the kernel. Then $x_1 + \cdots + x_p \equiv 0 \bmod (p\mathcal{O}_K)$. So x can be written as $y_1 g_1 + \cdots + y_p g_p + pa$ where $y_i, a \in \mathcal{O}_K$, and $y_1 + \cdots + y_p = 0$. But we have already seen that any element $y_1 g_1 + \cdots + y_p g_p$ with $y_1 + \cdots + y_p = 0$ lies in $(1 - g)\mathcal{O}_K G$. Therefore if x lies in the kernel then

$$x \in (1 - g)\mathcal{O}_K G + p\mathcal{O}_K.$$

But $(1-g)\mathcal{O}_K G + p\mathcal{O}_K$ clearly lies in the kernel. So $(1-g)\mathcal{O}_K G + p\mathcal{O}_K$ is the kernel. The ideal $I + J$ lies in the kernel and therefore

$$(1 - g)\mathcal{O}_K G + (1 + g + \cdots + g^{p-1})\mathcal{O}_K G \subseteq (1 - g)\mathcal{O}_K G + p\mathcal{O}_K.$$

But, since

$$(1 - g)x + (1 + g + \cdots + g^{p-1}) = p,$$

where

$$x = -\sum_{i=1}^{p-1} ig_i,$$

p lies in $(1-g)\mathcal{O}_K G + (1+g+\cdots+g^{p-1})\mathcal{O}_K G$. Therefore

$$(1-g)\mathcal{O}_K G + p\mathcal{O}_K \subseteq (1-g)\mathcal{O}_K G + (1+g+\cdots+g^{p-1})\mathcal{O}_K G,$$

and hence $I + J = (1-g)\mathcal{O}_K G + p\mathcal{O}_K$. So the kernel of the surjective ring homomorphism $\Lambda \to \mathcal{O}_K/p\mathcal{O}_K$, $g \mapsto 1$, is $I+J$ and therefore $\Lambda/(I+J) \simeq \mathcal{O}_K/p\mathcal{O}_K$ as we had claimed.

Our cartesian square can now be written as

$$\begin{array}{ccc} \mathcal{O}_K G & \xrightarrow{i_1} & \mathcal{O}_M \\ \downarrow i_2 & & \downarrow j_1 \\ \mathcal{O}_K & \xrightarrow{j_2} & \mathcal{O}_K/p\mathcal{O}_K \end{array} \tag{2.3}$$

The action of various maps is given by

$$\begin{array}{ccc} g & \xrightarrow{i_1} & \zeta_p \\ \downarrow i_2 & & \downarrow j_1 \\ 1 & \xrightarrow{j_2} & [1] \end{array}$$

The Mayer-Vietoris sequence attached to the square (2.3) gives

$$j_1(\mathcal{O}_M^\times) \times j_2(\mathcal{O}_K^\times) \to (\mathcal{O}_K/p\mathcal{O}_K)^\times \to D(\mathcal{O}_K G) \to D(\mathcal{O}_M) \times D(\mathcal{O}_K) \to 1.$$

The rings of integers $\mathcal{O}_K$ and $\mathcal{O}_M$ are maximal orders in K and M respectively, and therefore their kernel groups $D(\mathcal{O}_K)$ and $D(\mathcal{O}_M)$ vanish. Since $j_2(\mathcal{O}_K^\times) \subset j_1(\mathcal{O}_M^\times)$, we can rewrite the above sequence omitting $j_2(\mathcal{O}_K^\times)$ as

$$1 \to j_1(\mathcal{O}_M^\times) \to (\mathcal{O}_K/p\mathcal{O}_K)^\times \to D(\mathcal{O}_K G) \to 1, \tag{2.4}$$

or

$$D(\mathcal{O}_K G) \simeq \frac{(\mathcal{O}_K/p\mathcal{O}_K)^\times}{j_1(\mathcal{O}_M^\times)}.$$

Since M contains ζ_p, the group $\mathcal{O}_M^\times$ of units contains the cyclotomic units

$$\begin{aligned} \xi_a &= \frac{1-\zeta_p^a}{1-\zeta_p}, \qquad 1 \le a \le p-1, \\ &= 1 + \zeta_p + \cdots + \zeta_p^{a-1}. \end{aligned}$$

The image of ξ_a under j_1 is a, and so

$$(\mathbb{Z}/p\mathbb{Z})^\times \subseteq j_1(\text{cyclotomic units}) \subseteq j_1(\mathcal{O}_M^\times).$$

The kernel group $D(\mathcal{O}_K G)$ is therefore isomorphic to a quotient group of $(\mathcal{O}_K/p\mathcal{O}_K)^\times/(\mathbb{Z}/p\mathbb{Z})^\times$. The ideal $p\mathcal{O}_K$ is either a prime or it is a product of two primes. If it is a prime then

$$\begin{aligned} \frac{\mathcal{O}_K}{p\mathcal{O}_K} &\simeq \mathrm{GF}(p^2), \\ \left(\frac{\mathcal{O}_K}{p\mathcal{O}_K}\right)^\times &\simeq C_{p^2-1}, \\ \frac{(\mathcal{O}_K/p\mathcal{O}_K)^\times}{(\mathbb{Z}/p\mathbb{Z})^\times} &\simeq C_{p+1}, \end{aligned} \tag{2.5}$$

and if it is a product of two primes then

$$\begin{aligned} \frac{\mathcal{O}_K}{p\mathcal{O}_K} &\simeq \mathrm{GF}(p) \times \mathrm{GF}(p), \\ \left(\frac{\mathcal{O}_K}{p\mathcal{O}_K}\right)^\times &\simeq C_{p-1} \times C_{p-1}, \\ \frac{(\mathcal{O}_K/p\mathcal{O}_K)^\times}{(\mathbb{Z}/p\mathbb{Z})^\times} &\simeq C_{p-1}. \end{aligned} \tag{2.6}$$

In both cases $(\mathcal{O}_K/p\mathcal{O}_K)^\times/(\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group. Since $D(\mathcal{O}_K G)$ is isomorphic to a quotient group of a cyclic group, it is cyclic. The order of $D(\mathcal{O}_K G)$ divides $p+1$ if p is inert in K or it divides $p-1$ if p splits in K. □

Next we calculate the order of $D(\mathcal{O}_K G)$ in the case when K is imaginary. Let

$$\bar{j}_1 : \mathcal{O}_M^\times \to \frac{(\mathcal{O}_K/p\mathcal{O}_K)^\times}{(\mathbb{Z}/p\mathbb{Z})^\times}$$

be the map induced by j_1. Then $D(\mathcal{O}_K G) \simeq \mathrm{Coker}(\bar{j}_1)$ and the order of $D(\mathcal{O}_K G)$ is $p^*/|\bar{j}_1(\mathcal{O}_M^\times)|$ where p^* is the order of $(\mathcal{O}_K/p\mathcal{O}_K)^\times/(\mathbb{Z}/p\mathbb{Z})^\times$. From (2.5) and (2.6) we have

$$p^* = \begin{cases} p+1, & \text{if } p \text{ is inert in } K, \\ p-1, & \text{if } p \text{ splits in } K. \end{cases}$$

So in order to calculate the order of $D(\mathcal{O}_K G)$ we need to obtain $\bar{j}_1(\mathcal{O}_M^\times)$. A subgroup of $\mathcal{O}_M^\times$ $(= E_M)$ is $W_M E_{M^+}$. So let us first calculate the image of $W_M E_{M^+}$ under $\bar{j}_1$.

(2.7) LEMMA. *The image of E_{M^+} under $\bar{j}_1$ is 1, and so $\bar{j}_1(W_M E_{M^+}) = \bar{j}_1(W_M)$.*

Proof. Since the extensions $K/\mathbb{Q}$ and $N/\mathbb{Q}$ are ramified at different primes, the ring of integers $\mathcal{O}_M$ in $M = KN$ is a compositum of the rings of integers in K and N, that is, $\mathcal{O}_M = \mathcal{O}_K\mathcal{O}_N$. The rings $\mathcal{O}_K$ and $\mathcal{O}_N$ are given by

$$\begin{aligned}\mathcal{O}_K &= \langle 1, \alpha\rangle_{\mathbb{Z}},\\ \mathcal{O}_N &= \langle \zeta_p, \ldots, \zeta_p^{p-1}\rangle_{\mathbb{Z}},\end{aligned}$$

and therefore

$$\mathcal{O}_M = \langle \zeta_p, \ldots, \zeta_p^{p-1}, \alpha\zeta_p, \ldots, \alpha\zeta_p^{p-1}\rangle_{\mathbb{Z}}.$$

Fixing $\mathcal{O}_M$ under complex conjugation gives the ring of integers in M^+:

$$\begin{aligned}\mathcal{O}_{M^+} = \langle &\zeta_p + \zeta_p^{-1}, \ldots, \zeta_p^{(p-1)/2} + \zeta_p^{-(p-1)/2}, \alpha(\zeta_p - \zeta_p^{-1}),\\ &\ldots, \alpha(\zeta_p^{(p-1)/2} - \zeta_p^{-(p-1)/2})\rangle_{\mathbb{Z}}, \qquad \text{if } d \not\equiv 3 \bmod (4),\end{aligned}$$

or

$$\begin{aligned}\mathcal{O}_{M^+} = \langle &\zeta_p + \zeta_p^{-1}, \ldots, \zeta_p^{(p-1)/2} + \zeta_p^{-(p-1)/2}, \zeta_p^{-1} + \alpha(\zeta_p - \zeta_p^{-1}),\\ &\ldots, \zeta_p^{-(p-1)/2} + \alpha(\zeta_p^{(p-1)/2} - \zeta_p^{-(p-1)/2})\rangle_{\mathbb{Z}}, \qquad \text{if } d \equiv 3 \bmod (4).\end{aligned}$$

So any element $u \in E_{M^+}$ can be written as

$$u = \sum_{i=1}^{(p-1)/2} [a_i(\zeta_p^i + \zeta_p^{-i}) + b_i\alpha(\zeta_p^i - \zeta_p^{-i})], \qquad \text{if } d \not\equiv 3 \bmod (4),$$

or

$$u = \sum_{i=1}^{(p-1)/2} [a_i(\zeta_p^i + \zeta_p^{-i}) + b_i(\zeta_p^{-i} + \alpha(\zeta_p^i - \zeta_p^{-i}))], \qquad \text{if } d \equiv 3 \bmod (4),$$

where $a_i, b_i \in \mathbb{Z}$. If we now apply j_1 to u we find

$$j_1(u) = \begin{cases} \sum_{i=1}^{(p-1)/2} 2a_i, & \text{if } d \not\equiv 3 \bmod (4),\\ \sum_{i=1}^{(p-1)/2}(2a_i + b_i), & \text{if } d \equiv 3 \bmod (4),\end{cases}$$

which shows that $j_1(u) \in (\mathbb{Z}/p\mathbb{Z})^\times$ and therefore $\overline{j}_1(E_{M^+}) = 1$. □

(2.8) LEMMA. *The image of W_M under $\overline{j}_1$ is 1 unless K is $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$ in which case*

$$\overline{j}_1(W_M) \simeq \begin{cases} C_2, & \text{if } K = \mathbb{Q}(\sqrt{-1}),\\ C_3, & \text{if } K = \mathbb{Q}(\sqrt{-3}).\end{cases}$$

Proof. Assume K is a field other than $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$. Then

$$W_M = \langle -1, \zeta_p \rangle.$$

Applying $\overline{j}_1$ to W_M gives $\overline{j}_1(W_M) = 1$.

If K is $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$, then

$$W_M = \begin{cases} \langle \zeta_4, \zeta_p \rangle, & \text{if } K = \mathbb{Q}(\sqrt{-1}), \\ \langle -1, \zeta_3, \zeta_p \rangle, & \text{if } K = \mathbb{Q}(\sqrt{-3}), \end{cases}$$

and therefore

$$\overline{j}_1(W_M) = \begin{cases} \langle [\zeta_4] \rangle, & \text{if } K = \mathbb{Q}(\sqrt{-1}), \\ \langle [\zeta_3] \rangle, & \text{if } K = \mathbb{Q}(\sqrt{-3}). \end{cases}$$

The group $\overline{j}_1(W_M)$ is cyclic of order 2 if $K = \mathbb{Q}(\sqrt{-1})$, and it is cyclic of order 3 if $K = \mathbb{Q}(\sqrt{-3})$. □

Now that we have obtained $\overline{j}_1(W_M E_{M^+})$, we would like to calculate the index of $\overline{j}_1(W_M E_{M^+})$ in $\overline{j}_1(E_M)$. But before we could do that we need to find the index of $W_M E_{M^+}$ in E_M. The following lemma will allow us to find this index.

(2.9) LEMMA. *Let L be an abelian extension of $\mathbb{Q}$. Then the index Q_L of $W_L E_{L^+}$ in E_L is either 2 or 1 depending on whether or not*

$$\begin{aligned} \overline{\psi} : E_L &\to \frac{W_L}{W_L^2}, \\ u &\mapsto [u/u^c], \end{aligned}$$

is surjective.

Proof. Define

$$\begin{aligned} \psi : E_L &\to W_L, \\ u &\mapsto u/u^c. \end{aligned}$$

The extension $L/\mathbb{Q}$ is abelian. So the complex conjugation commutes with all other elements of $Gal(L/\mathbb{Q})$. For $u \in E_L$, u/u^c and its $Gal(L/\mathbb{Q})$-conjugates have absolute value 1. Therefore $u/u^c \in W_L$ (see [16], lemma (1.6)). Let

$$\overline{\psi} : E_L \to \frac{W_L}{W_L^2}$$

be the map induced by ψ. If $\zeta \in W_L$ then $\psi(\zeta) = \zeta/\zeta^{-1} = \zeta^2 \in W_L^2$, and so $W_L \subseteq \mathrm{Ker}(\overline{\psi})$. The group E_{L^+} also lies in $\mathrm{Ker}(\overline{\psi})$. On the other hand, suppose

$\psi(u) \in W_L^2$ for a $u \in E_L$. Then $u = \zeta^2 u^c$ for some $\zeta \in W_L$. We can write u as $u = \zeta v$ where $v = \zeta u^c$. One can easily check that $v^c = v$ and therefore $v \in E_{L^+}$. This shows that $u \in W_L E_{L^+}$, and so $\mathrm{Ker}(\overline{\psi}) = W_L E_{L^+}$. We thus have the exact sequence

$$1 \to W_L E_{L^+} \to E_L \xrightarrow{\overline{\psi}} \frac{W_L}{W_L^2}.$$

The group W_L/W_L^2 has order 2. If $\overline{\psi}$ is surjective then

$$\frac{E_L}{W_L E_{L^+}} \simeq \frac{W_L}{W_L^2},$$

and the order of $E_L/W_L E_{L^+}$ or, equivalently, the index Q_L of $W_L E_{L^+}$ in E_L is 2; if $\overline{\psi}$ is not surjective then $Q_L = 1$. □

Since M is an abelian extension of $\mathbb{Q}$, the above lemma applies to M and gives $Q_M = 1$ or 2.

(2.10) LEMMA. *If K is $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$ then $Q_M = 2$.*

Proof. By the above lemma, $Q_M = 2$ if the map

$$\overline{\psi} : E_M \to \frac{W_M}{W_M^2}$$

is surjective. Assume $K = \mathbb{Q}(\sqrt{-1})$. Then $W_M/W_M^2 = \langle [\zeta_4] \rangle$. The element $u = 1 - \zeta_4 \zeta_p$ is a unit in $\mathcal{O}_M$, and

$$\begin{aligned} \psi(u) &= \frac{1 - \zeta_4 \zeta_p}{1 - \zeta_4^{-1} \zeta_p^{-1}}, \\ &= -\zeta_4 \zeta_p, \end{aligned}$$

and therefore $\overline{\psi}(u) = [\zeta_4]$. So $\overline{\psi}$ is surjective, and hence $Q_M = 2$.

For $K = \mathbb{Q}(\sqrt{-3})$ we have $W_M/W_M^2 = \langle [-1] \rangle$. The element $u = 1 - \zeta_3 \zeta_p$ is a unit in $\mathcal{O}_M$, and $\overline{\psi}(u) = [-1]$. Therefore $Q_M = 2$. □

We can now return to the problem of calculating $\overline{j}_1(E_M)$. Since $[E_M : W_M E_{M^+}] = Q_M$, the index of $\overline{j}_1(W_M E_{M^+})$ in $\overline{j}_1(E_M)$ divides Q_M. In fact we have the following stronger result.

(2.11) THEOREM. *Let K be quadratic imaginary. Then*

$$[\overline{j}_1(E_M) : \overline{j}_1(W_M E_{M^+})] = Q_M.$$

Proof. If $K = \mathbb{Q}(\sqrt{-1})$ then, by (2.10),

$$E_M = \langle W_M E_{M^+}, 1 - \zeta_4 \zeta_p \rangle,$$

and therefore, by (2.7),

$$\overline{j}_1(E_M) = \langle \overline{j}_1(W_M), [1 - \zeta_4] \rangle.$$

The element $[1 - \zeta_4]$ has order 4 whereas, by (2.8), $\overline{j}_1(W_M)$ is of order 2. Therefore

$$[\overline{j}_1(E_M) : \overline{j}_1(W_M E_{M^+})] = 2.$$

If $K = \mathbb{Q}(\sqrt{-3})$ then, by (2.10),

$$E_M = \langle W_M E_{M^+}, 1 - \zeta_3 \zeta_p \rangle,$$

and therefore, by (2.7),

$$\overline{j}_1(E_M) = \langle \overline{j}_1(W_M), [1 - \zeta_3] \rangle.$$

The element $[1 - \zeta_3]$ has order 6 and, by (2.8), $\overline{j}_1(W_M)$ has order 3, and so

$$[\overline{j}_1(E_M) : \overline{j}_1(W_M E_{M^+})] = 2.$$

Now assume K is a field other than $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$. If $Q_M = 1$ then, since the index of $\overline{j}_1(W_M E_{M^+})$ in $\overline{j}_1(E_M)$ divides Q_M, $[\overline{j}_1(E_M) : \overline{j}_1(W_M E_{M^+})] = 1$. Assume $Q_M = 2$. By (2.7) and (2.8), $\overline{j}_1(W_M E_{M^+}) = 1$. To show that

$$[\overline{j}_1(E_M) : \overline{j}_1(W_M E_{M^+})] = 2,$$

we have to show that $\overline{j}_1(E_M) \neq 1$. Since $Q_M = 2$, by (2.9), the map

$$\overline{\psi} : E_M \to \frac{W_M}{W_M^2}$$

is surjective. The group W_M/W_M^2 is generated by $[-1]$. So there exists a unit $u \in E_M$ such that $\overline{\psi}(u) = [-1]$, or $u = -\zeta^2 u^c$ for some $\zeta \in W_M$. We can absorb ζ into u and

obtain $u = -u^c$. Since $u \in \mathcal{O}_M$ and

$$\mathcal{O}_M = \langle \zeta_p, \dots, \zeta_p^{p-1}, \alpha\zeta_p, \dots, \alpha\zeta_p^{p-1} \rangle \mathbb{Z},$$

we can write u as

$$u = \sum_{i=1}^{p-1} (a_i \zeta_p^i + \alpha b_i \zeta_p^i),$$

where $a_i, b_i \in \mathbb{Z}$. The condition $u = -u^c$ forces u to have the form

$$u = \sum_{i=1}^{(p-1)/2} [a_i(\zeta_p^i - \zeta_p^{-i}) + \alpha b_i(\zeta_p^i + \zeta_p^{-i})], \qquad \text{if } d \not\equiv 3 \bmod (4),$$

or

$$u = \sum_{i=1}^{p-1} [a_i \zeta_p^i - \alpha(a_i + a_{p-i})\zeta_p^i], \qquad \text{if } d \equiv 3 \bmod (4).$$

If we now apply $\bar{j}_1$ to u, we find

$$\bar{j}_1(u) = \begin{cases} [2(b_1 + \cdots + b_{(p-1)/2})\alpha], & \text{if } d \not\equiv 3 \bmod (4), \\ [(a_1 + \cdots + a_{p-1})(1 - 2\alpha)], & \text{if } d \equiv 3 \bmod (4). \end{cases}$$

In both cases $\bar{j}_1(u) \neq 1$, and therefore $\bar{j}_1(E_M) \neq 1$. □

We are now in a position to prove (2.2).

Proof of (2.2). By (2.11),

$$|\bar{j}_1(E_M)| = Q_M |\bar{j}_1(W_M E_{M^+})|,$$

and so, by (2.7), (2.8) and (2.10),

$$|\bar{j}_1(E_M)| = \begin{cases} 4, & \text{if } K = \mathbb{Q}(\sqrt{-1}), \\ 6, & \text{if } K = \mathbb{Q}(\sqrt{-3}), \\ Q_M, & \text{otherwise.} \end{cases}$$

Since

$$|D(\mathcal{O}_K G)| = \frac{p^*}{|\bar{j}_1(E_M)|},$$

(2.2) is obvious. □

We now briefly discuss the case when K is real. As in the imaginary case, the kernel group $D(\mathcal{O}_K G)$ is isomorphic to

$$\frac{(\mathcal{O}_K/p\mathcal{O}_K)^\times/(\mathbb{Z}/p\mathbb{Z})^\times}{\overline{j}_1(E_M)},$$

where the map $\overline{j}_1 : E_M \to (\mathcal{O}_K/p\mathcal{O}_K)^\times/(\mathbb{Z}/p\mathbb{Z})^\times$ sends ζ_p to 1. Unlike the imaginary case the index $Q_M = [E_M : W_M E_{M^+}]$ now is always 1. To prove this, we note that Q_M is 2 if and only if there exists a unit u in E_M such that $u^c = -u$. But any element x of $\mathcal{O}_M$ which satisfies $x^c = -x$ belongs to

$$\langle \zeta_p - \zeta_p^{-1}, \ldots, \zeta_p^{(p-1)/2} - \zeta_p^{-(p-1)/2}, \alpha(\zeta_p - \zeta_p^{-1}), \ldots, \alpha(\zeta_p^{(p-1)/2} - \zeta_p^{-(p-1)/2}) \rangle_{\mathbb{Z}},$$

and is therefore divisible by the prime ideal $(\zeta_p - \zeta_p^{-1})\mathcal{O}_N$ of $N = \mathbb{Q}(\zeta_p)$ lying above p. So there does not exist a unit $u \in E_M$ such that $u^c = -u$, and consequently $Q_M = 1$ or, equivalently, $E_M = W_M E_{M^+}$.

Since $W_M = \langle -1, \zeta_p \rangle$, the image of W_M under $\overline{j}_1$ is 1. Therefore $\overline{j}_1(E_M) = \overline{j}_1(E_{M^+})$. Since K is real, a subgroup of E_{M^+} is E_K. Because of the fundamental unit of K, the image of E_K under $\overline{j}_1$ may not always be trivial. One can ask the question: how close does $\overline{j}_1(E_K)$ come to generating $\overline{j}_1(E_{M^+})$?

(2.12) PROPOSITION. *If p is inert in K and $p \equiv 3 \bmod (4)$, then the image of*

$$\overline{j}_1 : E_{M^+} \to \frac{(\mathcal{O}_K/p\mathcal{O}_K)^\times}{(\mathbb{Z}/p\mathbb{Z})^\times}$$

is the same as the image of E_K under $\overline{j}_1$.

Proof. Let $u \in E_{M^+}$. Then $\mathrm{norm}_{M^+/K}(u)$ lies in E_K and

$$\overline{j}_1(\mathrm{norm}_{M^+/K}(u)) = (\overline{j}_1(u))^{(p-1)/2},$$

since the degree of M^+ over K is $(p-1)/2$. The order of the group $(\mathcal{O}_K/p\mathcal{O}_K)^\times/(\mathbb{Z}/p\mathbb{Z})^\times$ is $p+1$ which, as $p \equiv 3 \bmod (4)$, is prime to $(p-1)/2$. Therefore the subgroup generated by $\overline{j}_1(u)$ is the same as the one generated by $(\overline{j}_1(u))^{(p-1)/2}$. Hence $\overline{j}_1(E_{M^+}) \subseteq \overline{j}_1(E_K)$. But $E_K \subset E_{M^+}$. Therefore $\overline{j}_1(E_{M^+}) = \overline{j}_1(E_K)$. □

In general, the behaviour of the fundamental unit of K under the map $\overline{j}_1$ is fairly random; in some cases it generates the entire group $(\mathcal{O}_K/p\mathcal{O}_K)^\times/(\mathbb{Z}/p\mathbb{Z})^\times$ and hence

determines completely the image of $\overline{j}_1$ while in others it maps to the identity element and so gives no clue as to the order of $\overline{j}_1(E_{M^+})$. If, for example, $K = \mathbb{Q}(\sqrt{2})$ then the fundamental unit is $1 + \alpha$ which, for $p = 7$, generates the entire group. On the other extreme, if $K = \mathbb{Q}(\sqrt{19})$ then the fundamental unit is $170 + 39\alpha$ which for $p = 3$ or 13 maps to 1.

We now return to the index Q_M which, as we can see from theorem (2.2), in the case when K is quadratic imaginary, has a direct bearing on the order of $D(\mathcal{O}_K G)$. In the next section we will attempt to calculate this index.

3. The calculation of Q_M

We continue to use the earlier notation except that K now is quadratic imaginary and the prime p is unramified in K. As before, we will write K as $\mathbb{Q}(\sqrt{-d})$; d now is positive. The ring of integers $\mathcal{O}_K$ in K is $\mathbb{Z}[\alpha]$ where α is $\sqrt{-d}$ or $(1+\sqrt{-d})/2$ depending on whether $d \not\equiv 3 \bmod (4)$ or $d \equiv 3 \bmod (4)$.

The problem here is to calculate the index $Q_M = [E_M : W_M E_{M^+}]$ for $M = K(\zeta_p)$. This index in the case when $K = \mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$ was calculated in the last section. So here we will assume that K is a field other than $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$.

(3.1) PROPOSITION. *The index Q_M is 2 if and only if there exists a unit $u \in E_M$ such that $u^c = -u$.*

Proof. The group, W_M, of roots of unity in M is generated by -1 and ζ_p; W_M^2 is generated by ζ_p. Therefore

$$\frac{W_M}{W_M^2} = \langle [-1] \rangle.$$

By (2.9), $Q_M = 2$ if and only if the map $E_M \to W_M/W_M^2$, $u \mapsto [u/u^c]$, is surjective, which is the case if and only if there exists a unit $v \in E_M$ such that $[v/v^c] = [-1]$ or $v = -\zeta^2 v^c$ for some $\zeta \in W_M$. Setting $u = \zeta^{-1} v$ gives $u = -u^c$. □

The extension N/N^+ (recall that $N = \mathbb{Q}(\zeta_p)$) is ramified at p and as $N^+ \subset N \subset M$, M/N^+ is ramified at p. Since $M = M^+(\sqrt{-d})$ and p does not divide d, M/M^+ is unramified at p. Therefore M^+/N^+ must be ramified at p. The degree of M^+ over N^+ is 2 and so M^+/N^+ is fully ramified. In terms of ideals we have

$$\begin{aligned} p\mathcal{O}_{N^+} &= P_{N^+}^{(p-1)/2}, \\ p\mathcal{O}_{M^+} &= P_{M^+}^{(p-1)}, \\ P_{N^+}\mathcal{O}_{M^+} &= P_{M^+}^2, \end{aligned}$$

where P_{N^+} and P_{M^+} respectively are prime ideals of $\mathcal{O}_{N^+}$ and $\mathcal{O}_{M^+}$ which lie above the rational prime p. The prime ideal P_{N^+} is principal—for a generator we can take $\mathrm{norm}_{N/N^+}(1-\zeta_p)$. So the ideal P_{M^+} has order at most 2 in $Cl(\mathcal{O}_{M^+})$. The absolute norm of P_{M^+} is p, and so P_{M^+} is principal if and only if there exists an element $x \in \mathcal{O}_{M^+}$ of absolute norm $\pm p$. The problem of determining whether P_{M^+} is principal is equivalent to calculating the index Q_M as the following theorem shows.

(3.2) THEOREM. *The index Q_M is 2 if and only if the prime ideal of M^+ lying above p is principal.*

Before we could prove the above theorem we need the following lemma.

(3.3) LEMMA. *An arbitrary element x of $\mathcal{O}_{M^+}$ can be expressed as*

$$x = a + \alpha(\zeta_p - \zeta_p^{-1})b,$$

where $a, b \in \mathcal{O}_{N^+}$ if $\alpha = \sqrt{-d}$, or $a \in \mathcal{O}_N$, $b \in \mathcal{O}_{N^+}$, $a^c = a + (\zeta_p - \zeta_p^{-1})b$ if $\alpha = (1 + \sqrt{-d})/2$.

Proof. For an element $x \in \mathcal{O}_M$ to lie in $\mathcal{O}_{M^+}$, one must have $x^c = x$. Writing x as $r + s\alpha$, $r, s \in \mathcal{O}_N$, and requiring $x^c = x$ gives $r \in \mathcal{O}_{N^+}$, $s^c = -s$ if $\alpha = \sqrt{-d}$, or $r^c = r + s$, $s^c = -s$ if $\alpha = (1 + \sqrt{-d})/2$. Since $s \in \mathcal{O}_N$ and $s^c = -s$, s must have the form

$$s = \sum_{i=1}^{(p-1)/2} s_i(\zeta_p^i - \zeta_p^{-i}), \qquad s_i \in \mathbb{Z}.$$

But $\zeta_p^i - \zeta_p^{-i}$ generates the same prime ideal of M as the element $\zeta_p - \zeta_p^{-1}$. Therefore $\zeta_p^i - \zeta_p^{-i}$ is an associate of $\zeta_p - \zeta_p^{-1}$, and $(\zeta_p^i - \zeta_p^{-i})/(\zeta_p - \zeta_p^{-1})$ is a unit which, one can easily check, lies in $\mathcal{O}_{M^+}$. So s can be expressed as

$$s = (\zeta_p - \zeta_p^{-1}) \sum_{i=1}^{(p-1)/2} s_i u_i,$$

where $u_i = (\zeta_p^i - \zeta_p^{-i})/(\zeta_p - \zeta_p^{-1})$. Therefore $s \in (\zeta_p - \zeta_p^{-1})\mathcal{O}_{N^+}$. The statement of the lemma is now obvious. □

Proof of (3.2). First assume that $Q_M = 2$. There therefore exists a unit $u \in E_M$ such that $u^c = -u$. Let $x = u(\zeta_p - \zeta_p^{-1})$. The element x is an integer of M which is fixed under complex conjugation. Therefore $x \in \mathcal{O}_{M^+}$. Taking the norm from M^+ to N^+ gives

$$\mathrm{norm}_{M^+/N^+}(x) = (\zeta_p - \zeta_p^{-1})^2 \mathrm{norm}_{M/N}(u).$$

Now $\mathrm{norm}_{M/N}(u)$ is a unit in $\mathcal{O}_N$. Since $[\mathrm{norm}_{M/N}(u)]^c = \mathrm{norm}_{M/N}(u)$, the element $\mathrm{norm}_{M/N}(u)$ is a unit in $\mathcal{O}_{N^+}$. The element $(\zeta_p - \zeta_p^{-1})^2$ generates the prime of $\mathcal{O}_{N^+}$ lying above p and so the prime of $\mathcal{O}_{M^+}$ lying above p is principal.

Conversely assume that the prime of $\mathcal{O}_{M^+}$ lying above p is principal. This means that we can find an element $x \in \mathcal{O}_{M^+}$ such that

$$\text{norm}_{M^+/N^+}(x) = v(\zeta_p - \zeta_p^{-1})^2,$$

where $v \in E_{N^+}$. Now if $\alpha = \sqrt{-d}$ then, by (3.3), any element of $\mathcal{O}_{M^+}$ can be written as $a + \alpha(\zeta_p - \zeta_p^{-1})b$ where $a, b \in \mathcal{O}_{N^+}$. Writing x in this form and then taking norm from M^+ to N^+ gives

$$a^2 + d(\zeta_p - \zeta_p^{-1})^2 b^2 = v(\zeta_p - \zeta_p^{-1})^2.$$

This shows that a^2 lies in $(\zeta_p - \zeta_p^{-1})^2\mathcal{O}_{N^+}$. Since $(\zeta_p - \zeta_p^{-1})^2\mathcal{O}_{N^+}$ is a prime ideal and $a \in \mathcal{O}_{N^+}$, it follows that $a \in (\zeta_p - \zeta_p^{-1})^2\mathcal{O}_{N^+}$. If we write $a = (\zeta_p - \zeta_p^{-1})^2 a'$, where $a' \in \mathcal{O}_{N^+}$, then x can be written as

$$x = (\zeta_p - \zeta_p^{-1})[(\zeta_p - \zeta_p^{-1})a' + \alpha b].$$

Let $u = (\zeta_p - \zeta_p^{-1})a' + \alpha b$. Then $u \in \mathcal{O}_M$ and $u^c = -u$. Since

$$\begin{aligned} \text{norm}_{M^+/N^+}(x) &= (\zeta_p - \zeta_p^{-1})^2 \text{norm}_{M/N}(u), \\ &= v(\zeta_p - \zeta_p^{-1})^2, \end{aligned}$$

it follows that $\text{norm}_{M/N}(u) = v$, and therefore u is a unit. So we have succeeded in constructing a unit u in $\mathcal{O}_M$ which satisfies $u^c = -u$. Therefore $Q_M = 2$.

On the other hand if $\alpha = (1 + \sqrt{-d})/2$ then, by (3.3), x can be written as $x = a + \alpha(\zeta_p - \zeta_p^{-1})b$ where $a \in \mathcal{O}_N$, $b \in \mathcal{O}_{N^+}$ and $a^c = a + (\zeta_p - \zeta_p^{-1})b$. Taking norm of x from M^+ to N^+ gives

$$a^2 + (\zeta_p - \zeta_p^{-1})ab + \left(\frac{1+d}{4}\right)(\zeta_p - \zeta_p^{-1})^2 b^2 = v(\zeta_p - \zeta_p^{-1})^2.$$

Replacing $a^2 + (\zeta_p - \zeta_p^{-1})ab$ by aa^c gives

$$aa^c + \left(\frac{1+d}{4}\right)(\zeta_p - \zeta_p^{-1})^2 b^2 = v(\zeta_p - \zeta_p^{-1})^2,$$

from which we see that $aa^c \in (\zeta_p - \zeta_p^{-1})^2\mathcal{O}_{N^+}$ or $a \in (\zeta_p - \zeta_p^{-1})\mathcal{O}_N$. Let $a = (\zeta_p - \zeta_p^{-1})a'$, where $a' \in \mathcal{O}_N$ and $a'^c = -(a' + b)$, and

$$u = \frac{x}{(\zeta_p - \zeta_p^{-1})} = a' + \alpha b.$$

Then $u^c = -u$ and, since $\text{norm}_{M/N}(u) = v$, u is a unit. Therefore $Q_M = 2$. □

The above theorem is useful in that it establishes a link between the index Q_M and the class group $Cl(\mathcal{O}_{M^+})$, but it does not really aid the calculation of Q_M. Of course if $Cl(\mathcal{O}_{M^+})$ is known to be of odd order, the theorem will then give $Q_M = 2$. But in practice it will be more difficult to calculate the order of $Cl(\mathcal{O}_{M^+})$ than to calculate Q_M. Also the order of $Cl(\mathcal{O}_{M^+})$ determines Q_M only if it is odd—the class group $Cl(\mathcal{O}_{M^+})$ can have elements of order 2 and still Q_M can have either of its two possible values.

Next we investigate more practical methods for calculating Q_M. We begin with a theorem which will enable us to calculate Q_M for a large number of fields.

(3.4) THEOREM. *If $Q_M = 2$, then either*

$$\left(\frac{d}{p}\right) = 1, \qquad \left(\frac{(-1)^t p}{q}\right) = 1, \qquad \text{for all } q|d,$$

or

$$\left(\frac{d}{p}\right) = -1, \qquad \left(\frac{(-1)^{t+1} p}{q}\right) = 1, \qquad \text{for all } q|d,$$

where q denotes a prime divisor of d and $t = (p-1)/2$ is the degree of N^+ over $\mathbb{Q}$.

Proof. Assume $Q_M = 2$. Let u be a unit in E_M such that $u^c = -u$. Let us first assume that $\alpha = \sqrt{-d}$. Then u can be written as $u = a + b\alpha$ where $a, b \in \mathcal{O}_N$ and $a^c = -a$, $b^c = b$. Since u is a unit, $\mathrm{norm}_M(u) = \pm 1$. We can write $\mathrm{norm}_M(u)$ as

$$\begin{aligned} \mathrm{norm}_M(u) &= \mathrm{norm}_N(a^2 + db^2), \\ &= [\mathrm{norm}_{N^+}(a^2 + db^2)]^2. \end{aligned}$$

Equating this to ± 1 gives $[\mathrm{norm}_{N^+}(a^2 + db^2)]^2 = \pm 1$. But $\mathrm{norm}_{N^+}(a^2 + db^2) \in \mathbb{Z}$. Therefore

$$\mathrm{norm}_{N^+}(a^2 + db^2) = \pm 1. \tag{3.5}$$

Since $a^c = -a$, a can be written as $a = (\zeta_p - \zeta_p^{-1})a'$ where $a' \in \mathcal{O}_{N^+}$. Reducing (3.5) mod (p) gives $d^t \overline{b}^{2t} \equiv \pm 1 \bmod (p)$ where $\overline{b} \in (\mathbb{Z}/p\mathbb{Z})^\times$ and $\overline{b} \equiv b \bmod (\zeta_p - \zeta_p^{-1})$. Solving for d gives $d\overline{b}^2 \equiv z^{2k} \bmod (p)$ if $d^t \overline{b}^{2t} \equiv 1 \bmod (p)$ or $d\overline{b}^2 \equiv z^{2k+1} \bmod (p)$ if $d^t \overline{b}^{2t} \equiv -1 \bmod (p)$ where z is a generator for $(\mathbb{Z}/p\mathbb{Z})^\times$ and k is an integer. These congruences show that

$$\left(\frac{d}{p}\right) = \begin{cases} +1, & \text{if } \mathrm{norm}_{N^+}(a^2 + db^2) = 1, \\ -1, & \text{if } \mathrm{norm}_{N^+}(a^2 + db^2) = -1. \end{cases}$$

Let q be a prime divisor of d. Reducing $\mathrm{norm}_{N^+}(a^2 + db^2) = 1 \bmod (q)$ gives $\mathrm{norm}_{N^+}(a^2) \equiv 1 \bmod (q)$. Now $\mathrm{norm}_{N^+}(a^2) = (-1)^t \mathrm{norm}_N(a)$. Substituting for

$a = (\zeta_p - \zeta_p^{-1})a'$ gives

$$\begin{aligned}\text{norm}_{N^+}(a^2) &= (-1)^t \text{norm}_N((\zeta_p - \zeta_p^{-1})a'),\\ &= (-1)^t p[\text{norm}_{N^+}(a')]^2,\\ &\equiv 1 \bmod (q),\end{aligned}$$

and therefore $(-1)^t p$ is a square mod (q) for all q, that is,

$$\left(\frac{(-1)^t p}{q}\right) = 1, \qquad \text{for all } q|d.$$

Similarly reducing $\text{norm}_{N^+}(a^2 + db^2) = -1 \bmod (q)$ leads to

$$\left(\frac{(-1)^{t+1} p}{q}\right) = 1, \qquad \text{for all } q|d.$$

This completes the proof in the case when $\alpha = \sqrt{-d}$.

If $\alpha = (1 + \sqrt{-d})/2$, then u can be written as $u = a + b\alpha$ where $a \in \mathcal{O}_N$, $b \in \mathcal{O}_{N^+}$ and $a^c = -(a + b)$. Taking the norm of u from M to $\mathbb{Q}$ gives

$$\begin{aligned}\text{norm}_M(u) &= \text{norm}_N(a^2 + ab + b^2(1 + d)/4),\\ &= [\text{norm}_{N^+}(a^2 + ab + b^2(1 + d)/4)]^2,\\ &= \pm 1.\end{aligned}$$

Therefore

$$\text{norm}_{N^+}(a^2 + ab + b^2(1 + d)/4) = \pm 1,$$

or

$$\text{norm}_{N^+}(((2a + b)^2 + db^2)/4) = \pm 1. \tag{3.6}$$

Since $(2a + b)^c = -(2a + b)$, we can write $2a + b$ as $(\zeta_p - \zeta_p^{-1})a'$ where $a' \in \mathcal{O}_{N^+}$. Reducing (3.6) mod (p) and mod (q), respectively, proves the theorem in the case when $\alpha = (1 + \sqrt{-d})/2$. □

If we solve the conditions of (3.4) for d we obtain

(3.7) THEOREM. *If $Q_M = 2$, then either d is a product of primes where each*

prime is a square mod (p), *or* d *has the form* $d = 2^{\delta} q_1 \cdots q_l r_1 \cdots r_m$ *where* $\delta = 0$ *or* 1,

$$q_i \equiv 1 \bmod (4), \qquad \left(\frac{q_i}{p}\right) = 1, \qquad 1 \le i \le l,$$

$$r_i \equiv 3 \bmod (4), \qquad \left(\frac{r_i}{p}\right) = -1, \qquad 1 \le i \le m,$$

and

$$\delta \frac{(p^2-1)}{8} + m \equiv 1 \bmod (2).$$

Proof. We have to prove that the conditions on d given here are equivalent to those given in (3.4).

Let us then assume that

$$\left(\frac{d}{p}\right) = 1, \qquad \left(\frac{(-1)^t p}{q}\right) = 1, \qquad \text{for all } q|d.$$

Let q be an odd prime divisor of d. Then

$$\left(\frac{(-1)^t p}{q}\right) = \begin{cases} (\frac{p}{q}), & \text{if } p \equiv 1 \bmod (4), \\ (\frac{-p}{q}), & \text{if } p \equiv 3 \bmod (4), \end{cases}$$

$$= \begin{cases} (\frac{q}{p}), & \text{if } p \equiv 1 \bmod (4), \\ (\frac{-1}{q})(\frac{p}{q}), & \text{if } p \equiv 3 \bmod (4). \end{cases}$$

Now

$$\left(\frac{-1}{q}\right) = \begin{cases} 1, & \text{if } q \equiv 1 \bmod (4), \\ -1, & \text{if } q \equiv 3 \bmod (4), \end{cases}$$

and, for $p \equiv 3 \bmod (4)$,

$$\left(\frac{p}{q}\right) = \begin{cases} (\frac{q}{p}), & \text{if } q \equiv 1 \bmod (4), \\ -(\frac{q}{p}), & \text{if } q \equiv 3 \bmod (4). \end{cases}$$

Therefore, for $p \equiv 3 \bmod (4)$,

$$\left(\frac{-1}{q}\right)\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right),$$

and so, for any p,

$$\left(\frac{(-1)^t p}{q}\right) = \left(\frac{q}{p}\right) = 1,$$

that is, each odd prime divisor of d is a square mod (p). But since $(\frac{d}{p}) = 1$, it follows that 2, if it is a divisor of d, is also a square mod (p), and therefore each prime divisor of d is a square mod (p).

Conversely if we assume that each prime divisor of d is a square mod (p) then it is obvious that

$$\left(\frac{d}{p}\right) = 1, \qquad \left(\frac{(-1)^t p}{q}\right) = 1, \qquad \text{for all } q|d.$$

We now assume that

$$\left(\frac{d}{p}\right) = -1, \qquad \left(\frac{(-1)^{t+1} p}{q}\right) = 1, \qquad \text{for all } q|d.$$

Let q be an odd prime divisor of d. Then

$$\left(\frac{(-1)^{t+1} p}{q}\right) = \begin{cases} (\frac{-p}{q}), & \text{if } p \equiv 1 \bmod (4), \\ (\frac{p}{q}), & \text{if } p \equiv 3 \bmod (4). \end{cases}$$

Now, for $p \equiv 1 \bmod (4)$,

$$\left(\frac{-p}{q}\right) = \begin{cases} (\frac{q}{p}), & \text{if } q \equiv 1 \bmod (4), \\ -(\frac{q}{p}), & \text{if } q \equiv 3 \bmod (4), \end{cases}$$

and, for $p \equiv 3 \bmod (4)$,

$$\left(\frac{p}{q}\right) = \begin{cases} (\frac{q}{p}), & \text{if } q \equiv 1 \bmod (4), \\ -(\frac{q}{p}), & \text{if } q \equiv 3 \bmod (4). \end{cases}$$

Therefore

$$\left(\frac{(-1)^{t+1} p}{q}\right) = \begin{cases} (\frac{q}{p}), & \text{if } q \equiv 1 \bmod (4), \\ -(\frac{q}{p}), & \text{if } q \equiv 3 \bmod (4), \end{cases}$$

and so

$$\left(\frac{q}{p}\right) = \begin{cases} 1, & \text{if } q \equiv 1 \bmod (4), \\ -1, & \text{if } q \equiv 3 \bmod (4). \end{cases}$$

Let $d = 2^\delta q_1 \cdots q_l r_1 \cdots r_m$ with $q_i \equiv 1 \bmod (4)$ and $r_i \equiv 3 \bmod (4)$. Then

$$\begin{aligned} \left(\frac{d}{p}\right) &= \left(\frac{2}{p}\right)^\delta (-1)^m, \\ &= (-1)^{\delta((p^2-1)/8)+m}. \end{aligned}$$

Equating this to -1 gives $\delta((p^2-1)/8) + m \equiv 1 \bmod (2)$.

Conversely if we assume the conditions on d given in (3.7) then we can readily obtain

$$\left(\frac{d}{p}\right) = -1, \qquad \left(\frac{(-1)^{t+1} p}{q}\right) = 1, \qquad \text{for all } q|d.$$

□

Because of the strong conditions in (3.7) which d must satisfy if Q_M is to be 2, a large proportion of all the possible values for d, for a given p, fail to satisfy these conditions and, consequently, for these values of d one gets $Q_M = 1$. If, for example, $p = 3$ then there are 45 possible values for d less than 100. Out of these 45 values, 24 fail to satisfy the conditions of (3.7) and so for these values we immediately obtain $Q_M = 1$. For $p = 5$ there are 50 values for $d < 100$ and only 22 of them satisfy (3.7).

Next we prove a result which will allow us to calculate Q_M for $M = \mathbb{Q}(\sqrt{-q}, \zeta_p)$ where q is a prime congruent to 3 mod (4).

(3.8) THEOREM. *Let L be an abelian extension of $\mathbb{Q}$ which contains M or is a subfield of M. If the degree of L over M or M over L, whichever is applicable, is odd then $Q_L = Q_M$.*

Proof. Let us first assume L contains M. The group, W_L, of roots of unity in L can be written as $\langle \zeta_a, \zeta_b \rangle$ where a is a power of 2 and b is an odd integer. If the degree of L over M is odd then a can not be greater then 2. The group W_L is therefore generated by -1 and ζ_b. The group W_L^2 is generated by ζ_b, and so W_L/W_L^2 is generated by -1.

Assume $Q_L = 2$. Then, by (2.9), there exists a unit $u \in E_L$ such that $u^c = -u$. Taking norm of $u^c = -u$ from L to M gives

$$\begin{aligned} \mathrm{norm}_{L/M}(u^c) &= \mathrm{norm}_{L/M}(-u), \\ &= (-1)^{[L:M]}\mathrm{norm}_{L/M}(u), \\ &= -\mathrm{norm}_{L/M}(u), \end{aligned}$$

since $[L : M]$ is odd. As L is an abelian extension of $\mathbb{Q}$, complex conjugation commutes with all the other automorphisms; we obtain

$$[\mathrm{norm}_{L/M}(u)]^c = -\mathrm{norm}_{L/M}(u).$$

Since u is a unit in $\mathcal{O}_L$, $\mathrm{norm}_{L/M}(u)$ is a unit in $\mathcal{O}_M$. So there exists a unit $v = \mathrm{norm}_{L/M}(u)$ in E_M such that $v^c = -v$, and therefore $Q_M = 2$.

Conversely assume that $Q_M = 2$. Then we can find a u in E_M such that $u^c = -u$. Treating u as an element of E_L gives $Q_L = 2$.

The proof when L is a subfield of M is similar and so we omit it. □

(3.9) COROLLARY. *If $M = \mathbb{Q}(\sqrt{-q}, \zeta_p)$, where q is a prime congruent to 3 mod (4), then $Q_M = 2$.*

Proof. Let $L = \mathbb{Q}(\zeta_q, \zeta_p)$. Then L contains M and the degree of L over M is $(q-1)/2$ which is odd since $q \equiv 3 \bmod (4)$. The group W_L is generated by -1 and ζ_{pq}, and W_L/W_L^2 is generated by -1. The element $1 - \zeta_{pq}$ is a unit in L, and

$$(1 - \zeta_{pq})^c = -\zeta_{pq}^{-1}(1 - \zeta_{pq}).$$

Now ζ_{pq} lies in W_L^2 but -1 does not. Therefore $Q_L = 2$. Using (3.8) now gives $Q_M = 2$. □

Theorem (3.8) has another useful application. If M has a subfield L with $[M : L]$ odd and whose degree over $\mathbb{Q}$ is small then it may be easier to calculate Q_L (and hence Q_M) than calculating Q_M directly. We now explore this possibility for calculating Q_M.

Our success in obtaining Q_M through calculating Q_L will depend on the degree of L over $\mathbb{Q}$ being small. This degree is smallest when $p \equiv 3 \bmod (4)$, and so in the following we will restrict our considerations to the case when $p \equiv 3 \bmod (4)$ only.

So let us assume that $p \equiv 3 \bmod (4)$. Then $L = \mathbb{Q}(\alpha, \beta)$ where $\beta = (1 + \sqrt{-p})/2$. The group, W_L, of roots of unity in L is $\langle -1 \rangle$ unless $p = 3$ in which case $W_L = \langle -1, \zeta_3 \rangle$. In any case we have $W_L/W_L^2 = \langle -1 \rangle$, and so $Q_L = 2$ if and only if there exists a unit $u \in E_L$ such that $u^c = -u$.

Now any element $x \in \mathcal{O}_L$ satisfying $x^c = -x$ can be written as

$$x = \begin{cases} a\sqrt{-d} + b\sqrt{-p}, & \text{if } d \not\equiv 3 \bmod (4), \\ \frac{1}{2}(a\sqrt{-d} + b\sqrt{-p}), & \text{if } d \equiv 3 \bmod (4), \end{cases}$$

where $a, b \in \mathbb{Z}$ and, in the case $d \equiv 3 \bmod (4)$, $a + b \equiv 0 \bmod (2)$. So if x is a unit satisfying $x^c = -x$ then

$$\mathrm{norm}_{L/K}(x) = \begin{cases} -da^2 + pb^2, & \text{if } d \not\equiv 3 \bmod (4), \\ \frac{1}{4}(-da^2 + pb^2), & \text{if } d \equiv 3 \bmod (4), \end{cases}$$

must be a unit in $\mathcal{O}_K$. Since the only units in $\mathcal{O}_K$ are ± 1, we conclude that $Q_L = 2$ if and only if the equation

$$da^2 - pb^2 = \begin{cases} \pm 1, & \text{if } d \not\equiv 3 \bmod (4), \\ \pm 4, & \text{if } d \equiv 3 \bmod (4), \end{cases}$$

has an integer solution. Multiplying this equation by p or d, whichever is the smaller

of two, allows us to write this equation as

$$x^2 - pdy^2 = \delta k, \tag{3.10}$$

where $\delta = \pm 1$ and

$$k = \begin{cases} \min\{p, d\}, & \text{if } d \not\equiv 3 \bmod (4), \\ 4 \min\{p, d\}, & \text{if } d \equiv 3 \bmod (4). \end{cases}$$

So whether $Q_M = 2$ or 1 depends on whether or not (3.10), a generalized Pell's equation, is soluble. This equation, fortunately for us, belongs to a family of equations for which it is possible to settle the question of solubility in any particular case. In the following we will show how to determine whether (3.10) is soluble.

Consider the equation

$$x^2 - pdy^2 = \delta k', \tag{3.11}$$

where

$$k' = \begin{cases} k, & \text{if } d \not\equiv 3 \bmod (4), \\ k/4, & \text{if } d \equiv 3 \bmod (4). \end{cases}$$

The equation (3.10) is clearly soluble if (3.11) is. So let us first discuss (3.11). This is one of the standard equations which one encounters when studying quadratic indeterminate equations. A treatment of this equation can be found in, for example, [7]. In the following we will only state the main theorem on the solubility of (3.11) without the proof.

The method of solution for (3.11) involves the continued fractions expansion of $\sqrt{pd}$. Let $A_0 = \sqrt{pd}$ and let a_0 be the integer part of A_0. For $i \geq 1$, define

$$A_i = (A_{i-1} - a_{i-1})^{-1}.$$

Set a_i equal to the integer part of A_i. The sequence of integers $[a_0, a_1, \ldots]$ represents the continued fractions expansion of $\sqrt{pd}$. This representation is periodic, i.e., we can find integers r and s such that $a_i = a_{i+s}$ for $i \geq r$. To indicate this the continued fractions expansion of $\sqrt{pd}$ is written as $[a_0, a_1, \ldots, \dot{a}_r, \ldots, \dot{a}_{r+s-1}]$.

The constants A_i can be expressed as

$$A_i = \frac{\sqrt{pd} + P_i}{Q_i},$$

where $P_0 = 0$, $Q_0 = 1$, and, for $i \geq 1$,

$$P_i = a_{i-1}Q_{i-1} - P_{i-1},$$
$$Q_i = \frac{pd - (a_{i-1}Q_{i-1} - P_{i-1})^2}{Q_{i-1}}.$$

Both P_i and Q_i are integers. To prove this we use induction. Assume $A_i = (\sqrt{pd} + P_i)/Q_i$. Then

$$\begin{aligned} A_{i+1} &= \left(\frac{\sqrt{pd} + P_i}{Q_i} - a_i\right)^{-1}, \\ &= \frac{Q_i}{\sqrt{pd} + P_i - a_i Q_i}, \\ &= \frac{\sqrt{pd} + a_i Q_i - P_i}{(pd - (a_i Q_i - P_i)^2)/Q_i}, \end{aligned}$$

which can be seen to have the form $(\sqrt{pd} + P_{i+1})/Q_{i+1}$. To prove that P_i and Q_i are integers we note that if P_i and Q_i are integers for all $i \leq j$ then $P_{j+1} = a_j Q_j - P_j$ is also an integer, and

$$\begin{aligned} pd - (a_j Q_j - P_j)^2 &\equiv pd - P_j^2 \bmod (Q_j), \\ &\equiv Q_{j-1} Q_j \bmod (Q_j), \end{aligned}$$

and therefore Q_{j+1} is also an integer. Hence P_i and Q_i are integers for all i.

Because of the periodicity of a_i's the set of distinct values which P_i and Q_i can take is finite. In fact, $P_i = P_{i+s}$, and $Q_i = Q_{i+s}$ for $i \geq r$. Let $p_0 = a_0$, $q_0 = 1$, $p_1 = a_0 a_1 + 1$, $q_1 = a_1$, and

$$\begin{aligned} p_{i+1} &= a_{i+1} p_i + p_{i-1}, \qquad i \geq 1, \\ q_{i+1} &= a_{i+1} q_i + q_{i-1}, \qquad i \geq 1. \end{aligned}$$

The following theorem which has been taken from [7], §10.8, deals with the question of solubility of (3.11) conclusively.

(3.12) THEOREM. *Let l be an integer with $l^2 < pd$. The equation*

$$x^2 - pdy^2 = l$$

is soluble if and only if $l = (-1)^i Q_i$ for some i. If this is the case then any solution x, y can be written as $x = \pm p_{j-1}$, $y = \pm q_{j-1}$ where $l = (-1)^j Q_j$. □

In (3.11) $k'^2 < pd$ and so we can use the above theorem to decide whether (3.11) is soluble. If (3.11) is soluble then $Q_L = 2$, and, since $Q_M = Q_L$, Q_M will also be 2. But if (3.11) is not soluble then, in the case $d \equiv 3 \bmod (4)$, the equation (3.10) may still have a solution.

Let us assume that (3.11) is not soluble and $d \equiv 3 \bmod (4)$. We want to determine whether (3.10) has a solution. In the following we will show that any solution to (3.10) arises from a proper solution (x, y are relatively coprime) to

$$x^2 - pdy^2 = \eta l, \tag{3.13}$$

where $\eta = \pm 1$ and l is a positive integer with $l^2 < pd$. By using (3.12), we can then proceed to obtain all the solutions to (3.13), that is, if they exist. Once all the solutions to (3.13) have been obtained, by checking whether any of these gives rise to a solution to (3.10) we will be able to decide whether or not (3.10) is soluble.

Let

$$l = \begin{cases} k, & \text{if } 16p < d, \\ (d-p)/4, & \text{if } p < d,\ 16p > d, \\ k, & \text{if } 16d < p, \\ (p-d)/4, & \text{if } d < p,\ 16d > p. \end{cases}$$

Then l is a positive integer with $l^2 < pd$. Let $\eta = \pm 1$.

(3.14) PROPOSITION. *Any solution to $x^2 - pdy^2 = \delta k$ arises from a proper solution to $r^2 - pds^2 = \eta l$.*

Proof. If $l = k$ then there is nothing to prove. Assume $l = (d-p)/4$. Let x, y be a solution to $x^2 - pdy^2 = \delta k$. Then we claim that

$$\begin{aligned} x &= \frac{1}{\eta l}(\delta' pr - \delta pds), \\ y &= \frac{1}{\eta l}(\delta' ps - \delta r), \end{aligned} \tag{3.15}$$

where $\delta' = \pm 1$ and r, s are integers satisfying $r^2 - pds^2 = \eta l$. To prove this, observe that $(x, y)^2$, the square of the highest common factor of x and y, divides k. Since k is $4p$ or $4d$ and d is square-free, $(x, y) = 1$ or 2. But $(x, y) \neq 2$, for otherwise (3.11) will be soluble. So $(x, y) = 1$. Let r, s be integers such that

$$xs - yr = \delta. \tag{3.16}$$

If r_0, s_0 is a particular solution to (3.16) then r, s can be written as

$$\begin{aligned} r &= r_0 + mx, \\ s &= s_0 + my, \end{aligned}$$

where m is an integer. Multiplying $x^2 - pdy^2 = \delta k$ by $(r^2 - pds^2)$ gives

$$(r^2 - pds^2)(x^2 - pdy^2) = (r^2 - pds^2)\delta k,$$
$$(rx - pdsy)^2 - pd(xs - yr)^2 = (r^2 - pds^2)\delta k,$$

or

$$(rx - pdsy)^2 - pd = (r^2 - pds^2)\delta k. \tag{3.17}$$

Now

$$\begin{aligned} rx - pdsy &= (r_0 + mx)x - pd(s_0 + my)y, \\ &= r_0x - pds_0y + m(x^2 - pdy^2), \\ &= r_0x - pds_0y + m\delta k. \end{aligned}$$

Choose m such that

$$|rx - pdsy| \leq k/2 = 2p.$$

Since

$$(rx - pdsy)^2 - pd \equiv 0 \bmod (4p),$$

we have

$$rx - pdsy = \delta' p. \tag{3.18}$$

Substituting for $rx - pdsy = \delta' p$ in (3.17) gives

$$p^2 - pd = (r^2 - pds^2)\delta k,$$

or

$$r^2 - pds^2 = \eta l.$$

Equations (3.16) and (3.18) can now be solved for x, y to give (3.15).

The proof for the case $l = (p - d)/4$ is similar to the one given above and so we omit it. □

So in order to determine whether (3.10) is soluble we first, using (3.12), solve (3.13). If we find that (3.13) has a proper solution r, s for which x, y in (3.15) are integers then (3.10) is soluble and $Q_M = Q_L = 2$. If (3.13) has no such solution then (3.10) is insoluble and $Q_M = Q_L = 1$.

Let us consider a few examples. Let $p = 19$ and $d = 51$. Then $Q_L = 2$ if and only if the equation $x^2 - 969y^2 = \pm 76$ has an integer solution. We first consider the equation

$$x^2 - 969y^2 = \pm 19.$$

The continued fractions expansion of $\sqrt{969}$ is $[31, \dot{7}, 1, 3, 3, 1, 1, 1, 2, 1, 1, 1, 3, 3, 1, 7, \dot{6}\dot{2}]$. The above equation has a solution if and only if there exists an i such that $Q_i = \pm 19$. The constants Q_i's are given by $[\dot{1}, 8, 43, 15, 16, 33, 25, 32, 19, 32, 25, 33, 16, 15, 43, \dot{8}]$. Since $Q_8 = 19$, the above equation is soluble. For a solution we can take $p_7 = 11362$, $q_7 = 365$:

$$11362^2 - 969 \cdot 365^2 = 19.$$

Hence $Q_L = 2$.

Let $p = 31$ and $d = 39$. The equation we have to solve now is $x^2 - 1209y^2 = \pm 124$. But first we consider

$$x^2 - 1209y^2 = \pm 31.$$

The continued fractions expansion of $\sqrt{1209}$ is $[34, \dot{1}, 3, 2, 1, 3, 2, 1, 1, 22, 1, 1, 2, 3, 1, 2, 3, 1, \dot{6}\dot{8}]$. For the constants Q_i's we get $[\dot{1}, 53, 16, 23, 40, 17, 25, 29, 40, 3, 40, 29, 25, 17, 40, 23, 16, \dot{5}\dot{3}]$. Since for no value of i is $Q_i = \pm 31$, the above equation is insoluble. We now consider $x^2 - 1209y^2 = \pm 124$. By (3.14), any solution to this equation arises from a solution to

$$x^2 - 1209y^2 = \pm 2.$$

But again for no value of i is $Q_i = \pm 2$. Therefore the above equation is insoluble and hence $Q_L = 1$.

4. $D(\mathcal{O}_K G)$, p ramified in K

Our task here is to calculate the group $D(\mathcal{O}_K G)$ in the case when p is ramified in K. We will prove

(4.1) THEOREM. *If $d(K/\mathbb{Q}) = p\mathbb{Z}$, then the kernel group $D(\mathcal{O}_K G)$ is given by the exact sequence*

$$1 \to \mathrm{Coker}(j_1) \to D(\mathcal{O}_K G) \to \mathrm{Coker}(j_1') \to 1,$$

where

$$j_1 : (\mathcal{O}_K G/J)^\times \to (\mathcal{O}_K/p\mathcal{O}_K)^\times,$$
$$g \mapsto 1,$$

$J = (1 + g + \cdots + g^{p-1})\mathcal{O}_K G$, and $j_1' : \mathcal{O}_N^\times \to (\mathcal{O}_N/P_N^{(p-1)/2})^\times$ is induced by the ring homomorphism

$$\mathcal{O}_N \to \mathcal{O}_N/P_N^{(p-1)/2}.$$

Here $P_N = (1 - \zeta_p)\mathcal{O}_N$ is the prime ideal of $N = \mathbb{Q}(\zeta_p)$ lying above p.

(4.2) THEOREM. *If K is real, $d(K/\mathbb{Q}) \neq p\mathbb{Z}$, $b \not\equiv 0 \bmod (p)$, where $u = a + b\alpha$ is the fundamental unit in K, and p does not divide the class number h_M of $M = K(\zeta_p)$, then*

$$D(\mathcal{O}_K G) \simeq \underbrace{C_p \times \cdots \times C_p}_{n \text{ factors}} \times C_{|D(\mathcal{O}_{K'} G)|},$$

where

$$n = \begin{cases} (p-1)/4, & \text{if } p \equiv 1 \bmod (4), \\ (p-3)/4, & \text{if } p \equiv 3 \bmod (4), \end{cases}$$

$K' = \mathbb{Q}(\sqrt{-d'})$, $d' = \delta d/p$, $\delta = +1$ if $p \equiv 1 \bmod (4)$, or $\delta = -1$ if $p \equiv 3 \bmod (4)$.

(4.3) THEOREM. *If K is imaginary, $d(K/\mathbb{Q}) \neq p\mathbb{Z}$, and p does not divide the class number h_M of $M = K(\zeta_p)$, then $D(\mathcal{O}_K G)$ is given by the exact sequence*

$$1 \to C_p \to D(\mathcal{O}_K G) \to \underbrace{C_p \times \cdots \times C_p}_{n \text{ factors}} \times C_{|D(\mathcal{O}_{K'} G)|} \to 1,$$

where

$$n = \begin{cases} (p-5)/4, & \text{if } p \equiv 1 \bmod (4), \\ (p-3)/4, & \text{if } p \equiv 3 \bmod (4), \end{cases}$$

$K' = \mathbb{Q}(\sqrt{-d'})$, $d' = \delta d/p$, $\delta = +1$ if $p \equiv 1 \bmod (4)$, or $\delta = -1$ if $p \equiv 3 \bmod (4)$, and

$D(\mathcal{O}_K G)$ has order $p^{n+1}|D(\mathcal{O}_{K'}G)|$.

Proof of (4.1). Let $I = (1-g)\mathcal{O}_K G$, and $J = (1+g+\cdots+g^{p-1})\mathcal{O}_K G$. Then the following is a cartesian square.

$$\begin{array}{ccc} \mathcal{O}_K G/(I\cap J) & \xrightarrow{i_1} & \mathcal{O}_K G/J \\ \downarrow i_2 & & \downarrow j_1 \\ \mathcal{O}_K G/I & \xrightarrow{j_2} & \mathcal{O}_K G/(I+J) \end{array} \tag{4.4}$$

The map $g \to x$ sets up an isomorphism

$$\mathcal{O}_K G \simeq \frac{\mathcal{O}_K[x]}{\langle x^p-1\rangle},$$

and this isomorphism allows the following identification:

$$I \simeq (1-x)\frac{\mathcal{O}_K[x]}{\langle x^p-1\rangle},$$
$$J \simeq (1+x+\cdots+x^{p-1})\frac{\mathcal{O}_K[x]}{\langle x^p-1\rangle}.$$

We can now simplify the rings which appear in (4.4). The ideals I and J have trivial intersection and therefore

$$\frac{\mathcal{O}_K G}{I\cap J} \simeq \mathcal{O}_K G.$$

This follows from the fact that the factors $1-x$ and $1+x+\cdots+x^{p-1}$ of x^p-1 are relatively coprime and therefore

$$I\cap J \simeq (1-x)\frac{\mathcal{O}_K[x]}{\langle x^p-1\rangle} \cap (1+x+\cdots+x^{p-1})\frac{\mathcal{O}_K[x]}{\langle x^p-1\rangle} = 0.$$

The other rings in (4.4) simplify to

$$\frac{\mathcal{O}_K G}{I} \simeq \mathcal{O}_K,$$
$$\frac{\mathcal{O}_K G}{J} \simeq \frac{\mathcal{O}_K[x]}{\langle 1+x+\cdots+x^{p-1}\rangle},$$
$$\frac{\mathcal{O}_K G}{I+J} \simeq \frac{\mathcal{O}_K}{p\mathcal{O}_K}.$$

The square (4.4) can now be written as

$$\begin{array}{ccc} \mathcal{O}_K G & \xrightarrow{i_1} & \mathcal{O}_K G/J \\ \downarrow i_2 & & \downarrow j_1 \\ \mathcal{O}_K & \xrightarrow{j_2} & \mathcal{O}_K/p\mathcal{O}_K \end{array}$$

The action of various maps on g is given by

$$\begin{array}{ccc} g & \xrightarrow{i_1} & [g] \\ \downarrow{\scriptstyle i_2} & & \downarrow{\scriptstyle j_1} \\ 1 & \xrightarrow{j_2} & [1] \end{array}$$

Both j_1 and j_2 are surjective. The Mayer-Vietoris sequence attached to the above square is

$$\begin{aligned} 1 \to j_1((\mathcal{O}_K G/J)^\times) \times j_2(\mathcal{O}_K^\times) &\to (\mathcal{O}_K/p\mathcal{O}_K)^\times \\ &\to D(\mathcal{O}_K G) \to D(\mathcal{O}_K G/J) \times D(\mathcal{O}_K) \to 1. \end{aligned}$$

Since $\mathcal{O}_K$ is the maximal order in K, the kernel group $D(\mathcal{O}_K)$ is trivial. The group $\mathcal{O}_K^\times$ lies in $(\mathcal{O}_K G/J)^\times$. We can rewrite the above sequence as

$$1 \to j_1((\mathcal{O}_K G/J)^\times) \to (\mathcal{O}_K/p\mathcal{O}_K)^\times \to D(\mathcal{O}_K G) \to D(\mathcal{O}_K G/J) \to 1. \tag{4.5}$$

This sequence shows that in order to calculate $D(\mathcal{O}_K G)$ we need to find $D(\mathcal{O}_K G/J)$. Let

$$\Lambda = \frac{\mathcal{O}_K G}{J} \simeq \frac{\mathcal{O}_K[x]}{\langle 1 + x + \cdots + x^{p-1} \rangle}.$$

The polynomial $m(x) = 1 + x + \cdots + x^{p-1}$ splits into two irreducible factors in $\mathcal{O}_K[x]$. We denote these factors by $m_1(x)$ and $m_2(x)$. We can assume that $m_1(\zeta_p) = 0$. The two factors $m_1(x)$ and $m_2(x)$ are relatively coprime. We therefore have

$$\begin{aligned} \frac{K[x]}{\langle 1 + x + \cdots + x^{p-1} \rangle} &\simeq \frac{K[x]}{\langle m_1(x) \rangle} \times \frac{K[x]}{\langle m_2(x) \rangle}, \\ &\simeq K(\zeta_p) \times K(\sigma(\zeta_p)), \\ &\simeq N \times N, \end{aligned} \tag{4.6}$$

where σ is the non-trivial element of $Gal(N/\mathbb{Q})/Gal(N/K) \simeq Gal(K/\mathbb{Q})$. The isomorphism (4.6) allows us to embed Λ in $\mathcal{O}_N \times \mathcal{O}_N$:

$$\begin{aligned} \Lambda = \frac{\mathcal{O}_K G}{J} &\to \mathcal{O}_N \times \mathcal{O}_N, \\ g &\mapsto (\zeta_p, \sigma(\zeta_p)). \end{aligned}$$

Let $I' = m_1(g)\Lambda$, $J' = m_2(g)\Lambda$. Then the diagram

$$\begin{array}{ccc} \Lambda/(I' \cap J') & \longrightarrow & \Lambda/J' \\ \downarrow & & \downarrow \\ \Lambda/I' & \longrightarrow & \Lambda/(I' + J') \end{array} \tag{4.7}$$

is a cartesian square. Since $m_1(x)$ and $m_2(x)$ are relatively coprime, the ideals I' and

J' have trivial intersection and therefore $\Lambda/(I' \cap J') \simeq \Lambda$. For the ring Λ/I' we have

$$\frac{\Lambda}{I'} \simeq \frac{\mathcal{O}_K[x]}{\langle m_1(x) \rangle} \simeq \mathcal{O}_K[\zeta_p].$$

Since K is a subfield of $N = \mathbb{Q}(\zeta_p)$, $\mathcal{O}_K[\zeta_p] = \mathbb{Z}[\zeta_p] = \mathcal{O}_N$. Therefore $\Lambda/I' \simeq \mathcal{O}_N$. The ring Λ/J' is also isomorphic to $\mathcal{O}_N$. For $\Lambda/(I' + J')$ we get

$$\begin{aligned} \frac{\Lambda}{I' + J'} &\simeq \frac{\mathcal{O}_K[x]}{\langle m_1(x), m_2(x) \rangle}, \\ &\simeq \frac{\mathcal{O}_K[\zeta_p]}{\langle m_2(\zeta_p) \rangle}, \\ &\simeq \frac{\mathcal{O}_N}{\langle m_2(\zeta_p) \rangle}. \end{aligned}$$

The polynomial $m_2(x)$ can be written as

$$m_2(x) = \prod_a (x - \sigma(\zeta_p)^a),$$

where the product is over the elements of $Gal(N/K)$. Therefore

$$m_2(\zeta_p) = \prod_a (\zeta_p - \sigma(\zeta_p)^a).$$

For each $a \in Gal(N/K)$ the element $\zeta_p - \sigma(\zeta_p)^a$ generates the prime ideal $P_N = (1 - \zeta_p)\mathcal{O}_N$ of N lying above p. Therefore

$$m_2(\zeta_p)\mathcal{O}_N = P_N^{(p-1)/2},$$

and hence

$$\frac{\Lambda}{I' + J'} \simeq \frac{\mathcal{O}_N}{P_N^{(p-1)/2}}.$$

The square (4.7) can now be written as

$$\begin{array}{ccc} \mathcal{O}_K G/J & \xrightarrow{i'_1} & \mathcal{O}_N \\ \downarrow i'_2 & & \downarrow j'_1 \\ \mathcal{O}_N & \xrightarrow{j'_2} & \mathcal{O}_N/P_N^{(p-1)/2} \end{array} \tag{4.8}$$

The maps i''s and j''s are given by

$$\begin{array}{ccc} [g] & \xrightarrow{i'_1} & \sigma(\zeta_p) \\ \downarrow i'_2 & & \downarrow j'_1 \\ \zeta_p & \xrightarrow{j'_2} & [\zeta_p] \end{array}$$

The above square gives the exact sequance:

$$1 \to j_1'(\mathcal{O}_N^\times) \to (\mathcal{O}_N/P_N^{(p-1)/2})^\times \to D(\mathcal{O}_K G/J) \to 1.$$

Here we have used the fact that $D(\mathcal{O}_N) = 1$. This sequence together with the sequence (4.5) proves the theorem. □

Next we attempt to calculate the groups $\mathrm{Coker}(j_1)$ and $\mathrm{Coker}(j_1')$ which appear in (4.1).

(4.9) PROPOSITION. *The cokernel of the map*

$$j_1 : (\mathcal{O}_K G/J)^\times \to (\mathcal{O}_K/p\mathcal{O}_K)^\times,$$
$$g \mapsto 1,$$

is either trivial or it is isomorphic to a cyclic group of order p.

Proof. A subring of $\mathcal{O}_K G/J$ is $\mathbb{Z}G/\langle 1 + g + \cdots + g^{p-1}\rangle$ which is isomorphic to $\mathcal{O}_N = \mathbb{Z}[\zeta_p]$. The image of $\mathcal{O}_N^\times$ under j_1 is $(\mathbb{Z}/p\mathbb{Z})^\times$. In fact, the cyclotomic units in $\mathcal{O}_N^\times$ alone are enough to give $(\mathbb{Z}/p\mathbb{Z})^\times$. Therefore $\mathrm{Coker}(j_1) \simeq \mathrm{Coker}(\bar{j}_1)$ where

$$\bar{j}_1 : \left(\frac{\mathcal{O}_K G}{J}\right)^\times \to \frac{(\mathcal{O}_K/p\mathcal{O}_K)^\times}{(\mathbb{Z}/p\mathbb{Z})^\times} \tag{4.10}$$

is induced by j_1. The ideal $p\mathcal{O}_K$ ramifies in K: $p\mathcal{O}_K = P_K^2$. The ring $\mathcal{O}_K/p\mathcal{O}_K$ is therefore a local ring with the unique maximal ideal $P_K/p\mathcal{O}_K$. The group of units in $\mathcal{O}_K/p\mathcal{O}_K$ is given by

$$1 \to 1 + \frac{P_K}{p\mathcal{O}_K} \to \left(\frac{\mathcal{O}_K}{p\mathcal{O}_K}\right)^\times \to \left(\frac{\mathcal{O}_K}{P_K}\right)^\times \to 1.$$

The order of $1 + P_K/p\mathcal{O}_K$ is p and $(\mathcal{O}_K/P_K)^\times \simeq \mathrm{GF}(p)^\times$. Therefore $(\mathcal{O}_K/p\mathcal{O}_K)^\times \simeq C_p \times C_{p-1}$. Going back to (4.10), we see that

$$\frac{(\mathcal{O}_K/p\mathcal{O}_K)^\times}{(\mathbb{Z}/p\mathbb{Z})^\times} \simeq C_p,$$

and therefore $\mathrm{Coker}(\bar{j}_1) \simeq 1$ or C_p. □

(4.11) THEOREM. *If K is imaginary, i.e., $p \equiv 3 \bmod (4)$, then the cokernel of the map*

$$j_1 : (\mathcal{O}_K G/J)^\times \to (\mathcal{O}_K/p\mathcal{O}_K)^\times$$

is isomorphic to a cyclic group of order p unless $K = \mathbb{Q}(\sqrt{-3})$, in which case it is trivial.

Proof. Since $\mathrm{Coker}(j_1) \simeq \mathrm{Coker}(\bar{j}_1)$ where

$$\bar{j}_1 : \left(\frac{\mathcal{O}_K G}{J}\right)^\times \to \frac{(\mathcal{O}_K/p\mathcal{O}_K)^\times}{(\mathbb{Z}/p\mathbb{Z})^\times}$$

is induced by j_1, we consider the map $\bar{j}_1$.

By (4.8), we have an isomorphism

$$k : (\mathcal{O}_K G/J)^\times \to A = \left\{(a,b) \in \mathcal{O}_N^\times \times \mathcal{O}_N^\times \mid a \equiv \sigma^{-1}(b) \bmod (P_N^{(p-1)/2})\right\}$$

given by $g \mapsto (\zeta_p, \sigma(\zeta_p))$. The inverse map $k^{-1} : A \to (\mathcal{O}_K G/J)^\times$ is given by

$$k^{-1}(a,b) = x_1 g + \cdots + x_{p-1} g^{p-1}$$

where $x_i \in \mathcal{O}_K$, and

$$\begin{aligned} a &= x_1\zeta_p + \cdots + x_{p-1}\zeta_p^{p-1}, \\ b &= x_1\sigma(\zeta_p) + \cdots + x_{p-1}\sigma(\zeta_p^{p-1}). \end{aligned}$$

The above equations are soluble for x_i, $1 \le i \le p-1$. To prove this, let $x_i = r_i + s_i\alpha$, $r_i, s_i \in \mathbb{Z}$. Since $a \equiv \sigma^{-1}(b) \bmod (P_N^{(p-1)/2})$, we can find $\sum_i c_i\zeta_p^i \in \mathcal{O}_N$ such that $a - \sigma^{-1}(b) = (2\alpha - 1)\sum_i c_i\zeta_p^i$. But

$$\begin{aligned} a - \sigma^{-1}(b) &= \sum_{i=1}^{p-1}(x_i - \sigma^{-1}(x_i))\zeta_p^i, \\ &= (2\alpha - 1)\sum_{i=1}^{p-1} s_i\zeta_p^i. \end{aligned}$$

Therefore $s_i = c_i$, $1 \le i \le p-1$. The integers r_i, $1 \le i \le p-1$, can now be determined by using the equation $a = x_1\zeta_p + \cdots + x_{p-1}\zeta_p^{p-1}$, or

$$\sum_{i=1}^{p-1} r_i\zeta_p^i = a - \alpha\sum_{i=1}^{p-1} s_i\zeta_p^i.$$

Let

$$k' : A \to \frac{(\mathcal{O}_K/p\mathcal{O}_K)^\times}{(\mathbb{Z}/p\mathbb{Z})^\times}$$

denote the composite map $\bar{j}_1 k^{-1}$. Then the cokernel of $\bar{j}_1$ is isomorphic to $\mathrm{Coker}(k')$. The group $\mathrm{Coker}(k')$ is trivial if there exists an element in A whose image under k'

is non-trivial; otherwise $\mathrm{Coker}(k') \simeq C_p$. Now, for an element $(a,b) \in A$, we have

$$k'(a,b) = \bar{j}_1 \left(\sum_{i=1}^{p-1} (r_i + s_i\alpha) g^i \right), \qquad r_i, s_i \in \mathbb{Z},$$
$$= \sum_{i=1}^{p-1} (2r_i + s_i) + (2\alpha - 1) \sum_{i=1}^{p-1} s_i,$$

since $2 \in (\mathbb{Z}/p\mathbb{Z})^\times$. The element $\sum_{i=1}^{p-1}(2r_i + s_i)$ lies in $(\mathbb{Z}/p\mathbb{Z})^\times$ and therefore we can express $k'(a,b)$ as

$$k'(a,b) = 1 + (2\alpha - 1) \frac{\sum_{i=1}^{p-1} s_i}{\sum_{i=1}^{p-1}(2r_i + s_i)}.$$

But

$$\sum_{i=1}^{p-1} (2r_i + s_i) = t(a + \sigma^{-1}(b)),$$
$$\sum_{i=1}^{p-1} s_i = t\left(\frac{a - \sigma^{-1}(b)}{2\alpha - 1} \right),$$

where $t : \mathcal{O}_N \to \mathcal{O}_N/P_N$ denotes reduction mod (P_N). Hence

$$k'(a,b) = 1 + (2\alpha - 1) t \left(\frac{a - \sigma^{-1}(b)}{2\alpha - 1} \cdot \frac{1}{a + \sigma^{-1}(b)} \right).$$

Since, for any element $(a,b) \in A$,

$$(a,b) = (a, \sigma(a))(1, \sigma(a)^{-1} b),$$

and

$$k'(a, \sigma(a)) = 1,$$

it follows that $k'(A) = k'(B)$ where B is the subgroup of A consisting of elements of A of the form $(1,a)$. The group B is clearly isomorphic to

$$E_N^{((p-1)/2)} = \{ x \in E_N \mid x \equiv 1 \bmod (P_N^{(p-1)/2}) \}.$$

E_N, of course, is the group of units in $\mathcal{O}_N$. Let

$$k'' : E_N^{((p-1)/2)} \to \frac{(\mathcal{O}_K/p\mathcal{O}_K)^\times}{(\mathbb{Z}/p\mathbb{Z})^\times}$$

denote the map induced by the isomorphism

$$E_N^{((p-1)/2)} \to B,$$
$$a \mapsto (1, \sigma(a)).$$

Then $\mathrm{Coker}(\bar{j}_1) \simeq \mathrm{Coker}(k'')$.

Assume $K = \mathbb{Q}(\sqrt{-3})$. Then $E_N = \langle -1, \zeta_3 \rangle$, and $E_N^{(1)} = \langle \zeta_3 \rangle$. The image of ζ_3 under k'' is non-trivial. This follows from the fact that

$$k''(\zeta_3) = 1 + (2\alpha - 1)t\left(\frac{1-\zeta_3}{2\alpha - 1} \cdot \frac{1}{1+\zeta_3}\right),$$

and $(1-\zeta_3)/(2\alpha-1) = \zeta_3^2$ which is a unit. Therefore $\mathrm{Coker}(k'') = 1$ and hence $\mathrm{Coker}(\bar{j}_1) = 1$.

Now assume $K \neq \mathbb{Q}(\sqrt{-3})$. Then p is a prime greater than 3 which is congruent to 3 mod (4). Let $x \in E_N^{((p-1)/2)}$. Then, since $E_N = W_N E_{N^+}$, where $W_N = \langle -1, \zeta_p \rangle$ is the group of roots of unity in $\mathcal{O}_N$ and E_{N^+} is the group of units in $\mathcal{O}_{N^+}$, x can be written as $x = \zeta_p^i u$ where $1 \leq i \leq p$ and $u \in E_{N^+}$. As x is congruent to 1 mod $(P_N^{(p-1)/2})$, it can also be written as $1 + (2\alpha - 1)y$ where $y \in \mathcal{O}_N$. Applying the complex conjugation to the equation $x = \zeta_p^i u = 1 + (2\alpha - 1)y$ gives

$$x^c = \zeta_p^{-i} u = 1 - (2\alpha - 1)y^c.$$

Substituting for $u = \zeta_p^{-i}(1 + (2\alpha - 1)y)$ gives

$$1 - \zeta_p^{-2i} = (2\alpha - 1)(\zeta_p^{-2i} y + y^c).$$

If $i \neq p$ then $(1 - \zeta_p^{-2i})\mathcal{O}_N = P_N$. Since $(2\alpha - 1)\mathcal{O}_N = P_N^{(p-1)/2}$ and $(p-1)/2$ is greater than 1, the above equation is valid if and only if $i = p$. Therefore $y^c = -y$. The subset of $\mathcal{O}_N$ consisting of elements which satisfy $y^c = -y$ is $(\zeta_p - \zeta_p^{-1})\mathcal{O}_{N^+}$. Therefore any $x \in E_N^{((p-1)/2)}$ can be written as $x = 1 + (2\alpha - 1)(\zeta_p - \zeta_p^{-1})y$ where $y \in \mathcal{O}_{N^+}$. Since $t((1-x)/(2\alpha-1)) = 0$, applying k'' to x gives 1, and therefore $\mathrm{Coker}(k'') \simeq C_p$. Hence $\mathrm{Coker}(\bar{j}_1) \simeq C_p$ as required. □

The situation is markedly different in the case when K is real.

(4.12) THEOREM. *If K is real, then $\mathrm{Coker}(j_1)$ is trivial if $b \not\equiv 0 \bmod (p)$, where $u = a + b\alpha$ is the fundamental unit of K. If $b \equiv 0 \bmod (p)$ then $\mathrm{Coker}(j_1) \simeq C_p$.*

Proof. If $b \not\equiv 0 \bmod (p)$ then the image of u under $\bar{j}_1$ is non-trivial and therefore Coker($\bar{j}_1$)=1. Since Coker(j_1) $\simeq$ Coker($\bar{j}_1$), we obtain Coker(j_1) = 1.

Now assume $b \equiv 0 \bmod (p)$. In the proof of (4.11) we saw that Coker(j_1) $\simeq$ Coker(k'') where

$$k'' : E_N^{((p-1)/2)} \to \frac{(\mathcal{O}_K/p\mathcal{O}_K)^\times}{(\mathbb{Z}/p\mathbb{Z})^\times},$$
$$x \mapsto 1 + (2\alpha - 1)t\left(\frac{1-x}{2\alpha-1} \cdot \frac{1}{1+x}\right).$$

Suppose Coker(k'') = 1. Let $x \in E_N^{((p-1)/2)}$ be a unit whose image under k'' is non-trivial. Then $x = 1 + (2\alpha - 1)y$ where $y \in \mathcal{O}_N$ and $t(y) \in (\mathbb{Z}/p\mathbb{Z})^\times$. Taking the norm of x from N to K gives a unit in $\mathcal{O}_K$ which satisfies

$$\mathrm{norm}_{N/K}(x) \equiv 1 + (2\alpha - 1)\mathrm{tr}_{N/K}(y) \bmod (p\mathcal{O}_K).$$

For $\mathrm{tr}_{N/K}(y)$ we have

$$\mathrm{tr}_{N/K}(y) \equiv \frac{p-1}{2}t(y) \bmod ((2\alpha - 1)\mathcal{O}_K),$$

and therefore

$$\mathrm{tr}_{N/K}(y) = \frac{p-1}{2}t(y) + (2\alpha - 1)y', \qquad y' \in \mathcal{O}_K.$$

Hence

$$\mathrm{norm}_{N/K}(x) \equiv 1 + (2\alpha - 1)\left(\frac{p-1}{2}\right)t(y) \bmod (p\mathcal{O}_K).$$

So we have a unit $r + s\alpha$ in $\mathcal{O}_K$ such that $s \not\equiv 0 \bmod (p)$. But this contradicts the fact that, mod $(p\mathcal{O}_K)$, the fundamental unit lies in $(\mathbb{Z}/p\mathbb{Z})^\times$. Therefore Coker($k''$) $\simeq C_p$ and hence Coker(j_1) $\simeq C_p$. □

The above theorem shows that in order to calculate Coker(j_1) all one has to do is obtain the image of the fundamental unit of K under the map

$$\mathcal{O}_K^\times \to \frac{(\mathcal{O}_K/p\mathcal{O}_K)^\times}{(\mathbb{Z}/p\mathbb{Z})^\times}.$$

If this image is non-trivial then Coker(j_1) = 1; otherwise Coker(j_1) $\simeq C_p$. It is of course an interesting question to ask whether there exist primes p for which the fundamental unit in K fails to generate $(\mathcal{O}_K/p\mathcal{O}_K)^\times/(\mathbb{Z}/p\mathbb{Z})^\times$.

Next we consider the map

$$j_1' : \mathcal{O}_N^\times \to \left(\frac{\mathcal{O}_N}{P_N^{(p-1)/2}}\right)^\times$$

and its cokernel. This is the second of the maps whose cokernel appears in (4.1). The group $(\mathcal{O}_N/P_N^{(p-1)/2})^\times$ is given by the exact sequence

$$1 \to 1 + \frac{P_N}{P_N^{(p-1)/2}} \to \left(\frac{\mathcal{O}_N}{P_N^{(p-1)/2}}\right)^\times \to \left(\frac{\mathcal{O}_N}{P_N}\right)^\times \to 1.$$

The group $1 + P_N/P_N^{(p-1)/2}$ is isomorphic to $(p-3)/2$ copies of C_p and $(\mathcal{O}_N/P_N)^\times$ is isomorphic to C_{p-1}. Since the order of $1 + P_N/P_N^{(p-1)/2}$ is coprime to the order of $(\mathcal{O}_N/P_N)^\times$, it follows that

$$\left(\frac{\mathcal{O}_N}{P_N^{(p-1)/2}}\right)^\times \simeq C_{p-1} \times \underbrace{C_p \times \cdots \times C_p}_{(p-3)/2 \text{ factors}}.$$

If we let $\lambda = 1 - \zeta_p$ then $(\mathcal{O}_N/P_N^{(p-1)/2})^\times$ can be written as

$$\left(\frac{\mathcal{O}_N}{P_N^{(p-1)/2}}\right)^\times = \left\langle z, 1-\lambda, 1-\lambda^2, \ldots, 1-\lambda^{(p-3)/2} \right\rangle,$$

where z is a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$.

Since the map $\mathcal{O}_N^\times \to (\mathcal{O}_N/P_N)^\times \simeq (\mathbb{Z}/p\mathbb{Z})^\times = \langle z \rangle$ is surjective, we can find a unit u in $\mathcal{O}_N^\times$ such that $u \equiv z \bmod (P_N)$, and hence $u^p \equiv z^p \equiv z \bmod (p\mathcal{O}_N)$. The ideal $P_N^{(p-1)/2}$ divides $p\mathcal{O}_N$ and therefore $u^p \equiv z \bmod (P_N^{(p-1)/2})$. This shows that $(\mathbb{Z}/p\mathbb{Z})^\times$ lies in the image of j_1'. Also, $\zeta_p = 1 - \lambda$ and therefore the element $1 - \lambda$ and the subgroup of $(\mathcal{O}_N/P_N^{(p-1)/2})^\times$ which it generates also lies in the image of j_1'.

To advance further with our calculation of $\mathrm{Im}(j_1')$ we have to make an assumption about the class number of $N = \mathbb{Q}(\zeta_p)$. If we assume that p is regular then there exist real units of the form

$$\begin{aligned} u_1 &\equiv 1 + a_1\lambda^2 \bmod (\lambda^3\mathcal{O}_N), \\ u_2 &\equiv 1 + a_2\lambda^4 \bmod (\lambda^5\mathcal{O}_N), \\ &\vdots \\ u_{(p-3)/2} &\equiv 1 + a_{(p-3)/2}\lambda^{p-3} \bmod (\lambda^{p-2}\mathcal{O}_N), \end{aligned}$$

where $a_i \in (\mathbb{Z}/p\mathbb{Z})^\times$ for all i, which generate a subgroup E'_{N^+} of E_{N^+} of index prime to p (see [5]). E_{N^+} of course is the group of units in the maximal real subfield N^+

of N. The index of $W_N E'_{N+}$ in $W_N E_{N+}$ is prime to p and, since $E_N = W_N E_{N+}$, the image of j'_1 is the subgroup of $(\mathcal{O}_N/P_N^{(p-1)/2})^\times$ generated by z and the image of $W_N E'_{N+}$ under j'_1.

Let, for $i \geq 1$,

$$j_i : E'_{N+} \to (\mathcal{O}_N/P_N^i)^\times.$$

Then $\mathrm{Im}(j_1) = 1$ and the image of j_i for $i \geq 2$ is isomorphic to $\mathrm{Im}(k_i) \times \mathrm{Im}(j_{i-1})$ where

$$k_i : E'_{N+} \to \frac{(\mathcal{O}_N/P_N^i)^\times}{(\mathcal{O}_N/P_N^{i-1})^\times}$$

is the map induced by j_i. Hence

$$\mathrm{Im}(j_i) \simeq \mathrm{Im}(k_i) \times \cdots \times \mathrm{Im}(k_2) \times \mathrm{Im}(j_1).$$

The group $(\mathcal{O}_N/P_N^i)^\times/(\mathcal{O}_N/P_N^{i-1})^\times$ is generated by $1 - \lambda^{i-1}$ and is isomorphic to C_p. Therefore $\mathrm{Im}(k_i) = 1$ or C_p. If we apply k_i to u_l, $1 \leq l \leq (p-3)/2$, we find $\mathrm{Im}(k_i)$ is trivial if i is even or $\mathrm{Im}(k_i) \simeq C_p$ if i is odd. Hence $\mathrm{Im}(j_i)$ is isomorphic to n copies of C_p where n is the number of odd indices in $\{2, 3, \ldots, i\}$. In particular, $j'_1(E'_{N+}) = \mathrm{Im}(j_{(p-1)/2})$ is isomorphic to n copies of C_p where $n = (p-5)/4$ if $p \equiv 1 \bmod (4)$, or $n = (p-3)/4$ if $p \equiv 3 \bmod (4)$. We can now obtain $j'_1(W_N E'_{N+})$ and therefore $\mathrm{Im}(j'_1)$. We find $\mathrm{Im}(j'_1) \simeq C_{p-1}$ if $p = 3$, and if $p > 3$ then

$$\mathrm{Im}(j'_1) \simeq C_{p-1} \times \underbrace{C_p \times \cdots \times C_p}_{n \text{ factors}},$$

where $n = (p-1)/4$ if $p \equiv 1 \bmod (4)$, or $n = (p+1)/4$ if $p \equiv 3 \bmod (4)$. It is now straightforward to prove

(4.13) THEOREM. *If p is regular, then the cokernel of the map*

$$j'_1 : \mathcal{O}_N^\times \to (\mathcal{O}_N/P_N^{(p-1)/2})^\times$$

is trivial if $p = 3$. Otherwise it is isomorphic to n copies of C_p where $n = (p-5)/4$ if $p \equiv 1$ mod (4), or $n = (p-7)/4$ if $p \equiv 3$ mod (4). □

We now prepare the ground for proving (4.2) and (4.3). Let us assume $d(K/\mathbb{Q}) \neq p\mathbb{Z}$. The polynomial $1 - x^p$ splits into two irreducible factors $1 - x$ and $1 + x + \cdots + x^{p-1}$

in K which are relatively coprime. Let $I = (1-g)\mathcal{O}_K G$, and $J = (1+g+\cdots+g^{p-1})\mathcal{O}_K G$. Then

$$\begin{array}{ccc} \mathcal{O}_K G/(I\cap J) & \xrightarrow{i_1} & \mathcal{O}_K G/J \\ \downarrow i_2 & & \downarrow j_1 \\ \mathcal{O}_K G/I & \xrightarrow{j_2} & \mathcal{O}_K G/(I+J) \end{array}$$

is a cartesian square. The rings in the above square simplify as

$$\begin{aligned} \mathcal{O}_K G/(I\cap J) &\simeq \mathcal{O}_K G, \\ \mathcal{O}_K G/I &\simeq \mathcal{O}_K, \\ \mathcal{O}_K G/J &\simeq \mathcal{O}_K[\zeta_p], \\ \mathcal{O}_K G/(I+J) &\simeq \mathcal{O}_K/p\mathcal{O}_K, \end{aligned}$$

and so the above square can be written as

$$\begin{array}{ccc} \mathcal{O}_K G & \xrightarrow{i_1} & \mathcal{O}_K[\zeta_p] \\ \downarrow i_2 & & \downarrow j_1 \\ \mathcal{O}_K & \xrightarrow{j_2} & \mathcal{O}_K/p\mathcal{O}_K \end{array}$$

Both j_1 and j_2 are surjective. The above square gives the exact sequence:

$$1 \to j_1(\mathcal{O}_K[\zeta_p]^\times) \to (\mathcal{O}_K/p\mathcal{O}_K)^\times \to D(\mathcal{O}_K G) \to D(\mathcal{O}_K[\zeta_p]) \to 1. \qquad (4.14)$$

In writing the above sequence we have omitted $j_2(\mathcal{O}_K^\times)$ and $D(\mathcal{O}_K)$; the reason being $j_2(\mathcal{O}_K^\times) \subset j_1(\mathcal{O}_K[\zeta_p]^\times)$, and $D(\mathcal{O}_K) = 1$. In the above sequence we can not set $D(\mathcal{O}_K[\zeta_p])$ to 1 as $\mathcal{O}_K[\zeta_p]$ is not the maximal order in M. The maximal order in M is $\mathcal{O}_M$ and $\mathcal{O}_K[\zeta_p]$ is a proper subring of $\mathcal{O}_M$. In fact we have

(4.15) PROPOSITION. *As an abelian subgroup of $\mathcal{O}_M$, the $\mathbb{Z}$-index of $\mathcal{O}_K[\zeta_p]$ in $\mathcal{O}_M$ is given by*

$$(\mathcal{O}_M : \mathcal{O}_K[\zeta_p]) = p^{(p-1)/2}.$$

Before we prove the above proposition we need to introduce some notation. Let $d' = \delta d/p$ where $\delta = +1$ if $p \equiv 1 \bmod (4)$, and $\delta = -1$ if $p \equiv 3 \bmod (4)$. Let $K' = \mathbb{Q}(\sqrt{-d'})$. Then $d \equiv d' \bmod (4)$ and the two discriminants $d(K/\mathbb{Q})$ and $d(K'/\mathbb{Q})$ are related by $d(K/\mathbb{Q}) = p\,d(K'/\mathbb{Q})$. For the field M we have $M = K'N$ where $N = \mathbb{Q}(\zeta_p)$. Since $N/\mathbb{Q}$ is ramified at p only and p does not divide $d(K'/\mathbb{Q})$, K' and N have discriminants which are relatively coprime. The ring of integers in M is

therefore a compositum of the rings of integers in K' and N, that is $\mathcal{O}_M = \mathcal{O}_{K'}\mathcal{O}_N$. Since $\mathcal{O}_{K'} = \mathbb{Z}[\beta]$ where

$$\beta = \begin{cases} \sqrt{-d'}, & \text{if } d' \not\equiv 3 \bmod (4), \\ (1+\sqrt{-d'})/2, & \text{if } d' \equiv 3 \bmod (4), \end{cases}$$

it follows that $\mathcal{O}_M = \mathbb{Z}[\beta, \zeta_p]$.

Proof of (4.15). The index $(\mathcal{O}_M : \mathcal{O}_K[\zeta_p])$ is given by

$$(\mathcal{O}_M : \mathcal{O}_K[\zeta_p])^2 = \frac{\Delta_M(\mathcal{O}_K[\zeta_p])}{\Delta_M(\mathcal{O}_M)}. \tag{4.16}$$

The ring $\mathcal{O}_K[\zeta_p]$ is a compositum of $\mathcal{O}_K$ and $\mathcal{O}_N$, and therefore

$$\Delta_M(\mathcal{O}_K[\zeta_p]) = \Delta_K(\mathcal{O}_K)^{p-1}\Delta_N(\mathcal{O}_N)^2.$$

For the ring $\mathcal{O}_M$ we have $\mathcal{O}_M = \mathcal{O}_{K'}\mathcal{O}_N$ and so

$$\Delta_M(\mathcal{O}_M) = \Delta_{K'}(\mathcal{O}_{K'})^{p-1}\Delta_N(\mathcal{O}_N)^2.$$

Substituting for $\Delta_M(\mathcal{O}_K[\zeta_p])$ and $\Delta_M(\mathcal{O}_M)$ in (4.16) gives

$$(\mathcal{O}_M : \mathcal{O}_K[\zeta_p]) = \left(\frac{\Delta_K(\mathcal{O}_K)}{\Delta_{K'}(\mathcal{O}_{K'})}\right)^{(p-1)/2}.$$

Using $\Delta_K(\mathcal{O}_K) = p\Delta_{K'}(\mathcal{O}_{K'})$ now gives the required result. □

So before we can proceed any further with our calculation for $D(\mathcal{O}_K G)$ we need to calculate $D(\mathcal{O}_K[\zeta_p])$, and for that we need to find a cartesian square which describes $\mathcal{O}_K[\zeta_p]$. Let us, as a first step to obtaining a cartesian square for $\mathcal{O}_K[\zeta_p]$, prove that $p\mathcal{O}_M$ is an ideal of $\mathcal{O}_K[\zeta_p]$. $p\mathcal{O}_M$ clearly is a module over $\mathcal{O}_K[\zeta_p]$. To show that it is an ideal of $\mathcal{O}_K[\zeta_p]$ we need to show that $p\mathcal{O}_M = p\mathbb{Z}[\beta, \zeta_p] \subset \mathcal{O}_K[\zeta_p]$. It is obvious that $p\zeta_p \in \mathcal{O}_K[\zeta_p]$. For $p\beta$ we have

$$p\beta = \begin{cases} \delta\sqrt{\delta p}\alpha, & \text{if } d' \not\equiv 3 \bmod (4), \\ \delta\sqrt{\delta p}((-1+\sqrt{\delta p})/2 + \alpha), & \text{if } d' \equiv 3 \bmod (4). \end{cases}$$

Both $\sqrt{\delta p}$ and $(-1+\sqrt{\delta p})/2$ lie in $\mathbb{Z}[\zeta_p]$. Therefore $p\beta \in \mathcal{O}_K[\zeta_p]$.

The following can now be seen to be a cartesian square.

$$\begin{array}{ccc} \mathcal{O}_K[\zeta_p] & \longrightarrow & \mathcal{O}_M \\ \downarrow & & \downarrow \\ \mathcal{O}_K[\zeta_p]/p\mathcal{O}_M & \longrightarrow & \mathcal{O}_M/p\mathcal{O}_M \end{array}$$

Since $\mathcal{O}_K[\zeta_p]/p\mathcal{O}_M$ is not an $\mathcal{O}_K$-order contained in some K-algebra A, the exact sequence attached to the above square has the form (1.2) rather than (1.1). The

exact sequence is

$$1 \to (\mathcal{O}_K[\zeta_p])^\times \to \mathcal{O}_M^\times \times (\mathcal{O}_K[\zeta_p]/p\mathcal{O}_M)^\times \to (\mathcal{O}_M/p\mathcal{O}_M)^\times$$
$$\to \mathrm{Pic}(\mathcal{O}_K[\zeta_p]) \to \mathrm{Pic}(\mathcal{O}_M) \times \mathrm{Pic}(\mathcal{O}_K[\zeta_p]/p\mathcal{O}_M) \to \mathrm{Pic}(\mathcal{O}_M/p\mathcal{O}_M).$$

But for a finite ring Λ, $\mathrm{Pic}(\Lambda) = 1$, and for an integral domain Λ, $\mathrm{Pic}(\Lambda) = Cl(\Lambda)$. So we can rewrite the above sequence as

$$1 \to \mathcal{O}_K[\zeta_p]^\times \to \mathcal{O}_M^\times \times (\mathcal{O}_K[\zeta_p]/p\mathcal{O}_M)^\times$$
$$\to (\mathcal{O}_M/p\mathcal{O}_M)^\times \to Cl(\mathcal{O}_K[\zeta_p]) \to Cl(\mathcal{O}_M) \to 1.$$

Since $\mathcal{O}_M$ is the maximal order in M, we get

$$1 \to \mathcal{O}_K[\zeta_p]^\times \to \mathcal{O}_M^\times \times (\mathcal{O}_K[\zeta_p]/p\mathcal{O}_M)^\times \to (\mathcal{O}_M/p\mathcal{O}_M)^\times \to D(\mathcal{O}_K[\zeta_p]) \to 1. \quad (4.17)$$

Combining (4.14) and (4.17) gives

(4.18) THEOREM. *If $d(K/\mathbb{Q}) \neq p\mathbb{Z}$, then the kernel group $D(\mathcal{O}_K G)$ is given by the exact sequence*

$$1 \to \mathrm{Coker}(j_1) \to D(\mathcal{O}_K G) \to \mathrm{Coker}(j_1') \to 1,$$

where

$$j_1 : \mathcal{O}_K[\zeta_p]^\times \to (\mathcal{O}_K/p\mathcal{O}_K)^\times,$$
$$\zeta_p \mapsto 1,$$

and

$$j_1' : \mathcal{O}_M^\times \to \frac{(\mathcal{O}_M/p\mathcal{O}_M)^\times}{(\mathcal{O}_K[\zeta_p]/p\mathcal{O}_M)^\times}$$

is induced by the ring homomorphism $\mathcal{O}_M \to \mathcal{O}_M/p\mathcal{O}_M$. □

Next we calculate $\mathrm{Coker}(j_1)$.

Let $W_{\mathcal{O}_K[\zeta_p]}$ be the subgroup of $\mathcal{O}_K[\zeta_p]^\times$ consisting of roots of unity, and

$$\mathcal{O}_K[\zeta_p]^+ = \{x \in \mathcal{O}_K[\zeta_p] \mid x^c = x\}.$$

(4.19) LEMMA. *If the map*

$$\overline{\psi} : \mathcal{O}_K[\zeta_p]^\times \to \frac{W_{\mathcal{O}_K[\zeta_p]}}{W_{\mathcal{O}_K[\zeta_p]}^2},$$
$$x \mapsto x/x^c,$$

is surjective, then the index of $W_{\mathcal{O}_K[\zeta_p]}(\mathcal{O}_K[\zeta_p]^+)^\times$ in $\mathcal{O}_K[\zeta_p]^\times$ is 2; otherwise it is 1.

Proof. The sequence

$$1 \to W_{\mathcal{O}_K[\zeta_p]}(\mathcal{O}_K[\zeta_p]^+)^\times \to \mathcal{O}_K[\zeta_p]^\times \xrightarrow{\overline{\psi}} \frac{W_{\mathcal{O}_K[\zeta_p]}}{W^2_{\mathcal{O}_K[\zeta_p]}}$$

is exact; the proof of this is similar to the one given in (2.9). Since $W_{\mathcal{O}_K[\zeta_p]} = \langle -1, \zeta_p \rangle$ and $W^2_{\mathcal{O}_K[\zeta_p]} = \langle \zeta_p \rangle$, the group $W_{\mathcal{O}_K[\zeta_p]}/W^2_{\mathcal{O}_K[\zeta_p]}$ is generated by -1. If $\overline{\psi}$ is surjective then

$$\frac{\mathcal{O}_K[\zeta_p]^\times}{W_{\mathcal{O}_K[\zeta_p]}(\mathcal{O}_K[\zeta_p]^+)^\times} \simeq \frac{W_{\mathcal{O}_K[\zeta_p]}}{W^2_{\mathcal{O}_K[\zeta_p]}} \simeq C_2,$$

and $[\mathcal{O}_K[\zeta_p]^\times : W_{\mathcal{O}_K[\zeta_p]}(\mathcal{O}_K[\zeta_p]^+)^\times] = 2$; otherwise

$$\frac{\mathcal{O}_K[\zeta_p]^\times}{W_{\mathcal{O}_K[\zeta_p]}(\mathcal{O}_K[\zeta_p]^+)^\times} = 1,$$

and $[\mathcal{O}_K[\zeta_p]^\times : W_{\mathcal{O}_K[\zeta_p]}(\mathcal{O}_K[\zeta_p]^+)^\times] = 1$. □

(4.20) LEMMA. *If K is quadratic imaginary, then cokernel of*

$$j_1 : \mathcal{O}_K[\zeta_p]^\times \to (\mathcal{O}_K/p\mathcal{O}_K)^\times$$

is a cyclic group of order p.

Proof. Since $\mathbb{Z}[\zeta_p] \subset \mathcal{O}_K[\zeta_p]$, $\mathcal{O}_K[\zeta_p]^\times$ contains units of the form

$$\xi_a = \frac{1-\zeta_p^a}{1-\zeta_p}, \qquad 1 \le a \le p-1.$$

The image of ξ_a's under j_1 is $(\mathbb{Z}/p\mathbb{Z})^\times$, and therefore $\mathrm{Coker}(j_1) \simeq \mathrm{Coker}(\overline{j}_1)$ where

$$\overline{j}_1 : \mathcal{O}_K[\zeta_p]^\times \to \frac{(\mathcal{O}_K/p\mathcal{O}_K)^\times}{(\mathbb{Z}/p\mathbb{Z})^\times}$$

is induced by j_1.

The ideal $p\mathcal{O}_K$ ramifies in K: $p\mathcal{O}_K = P_K^2$ where P_K is the prime of K lying above p. The ring $\mathcal{O}_K/p\mathcal{O}_K$ is therefore a local ring with the unique maximal ideal $P_K/p\mathcal{O}_K$. The group of units in $\mathcal{O}_K/p\mathcal{O}_K$ is $\mathcal{O}_K/p\mathcal{O}_K$ minus $P_K/p\mathcal{O}_K$. Now $|\mathcal{O}_K/p\mathcal{O}_K| = p^2$, and $|P_K/p\mathcal{O}_K| = p$. Therefore $|(\mathcal{O}_K/p\mathcal{O}_K)^\times| = p(p-1)$, and so

$$\frac{(\mathcal{O}_K/p\mathcal{O}_K)^\times}{(\mathbb{Z}/p\mathbb{Z})^\times} \simeq C_p,$$

a cyclic group of order p. The cokernel of $\overline{j}_1$ is, therefore, either 1 or C_p. Let us assume that $\mathrm{Coker}(\overline{j}_1) = 1$. Then $|\overline{j}_1(\mathcal{O}_K[\zeta_p]^\times)| = p$, and, since $[\mathcal{O}_K[\zeta_p]^\times :$

$W_{\mathcal{O}_K[\zeta_p]}(\mathcal{O}_K[\zeta_p]^+)^\times] \leq 2$ by (4.19), $|\bar{j}_1(W_{\mathcal{O}_K[\zeta_p]}(\mathcal{O}_K[\zeta_p]^+)^\times)| = p$. But from $W_{\mathcal{O}_K[\zeta_p]} = \langle -1, \zeta_p \rangle$ and

$$\mathcal{O}_K[\zeta_p]^+ = \langle \zeta_p + \zeta_p^{-1}, \ldots, \zeta_p^{(p-1)/2} + \zeta_p^{-(p-1)/2}, \alpha(\zeta_p - \zeta_p^{-1}), \ldots, \alpha(\zeta_p^{(p-1)/2} - \zeta_p^{-(p-1)/2}) \rangle_{\mathbb{Z}}, \qquad \text{if } d \not\equiv 3 \bmod (4),$$

or

$$\mathcal{O}_K[\zeta_p]^+ = \langle \zeta_p + \zeta_p^{-1}, \ldots, \zeta_p^{(p-1)/2} + \zeta_p^{-(p-1)/2}, \zeta_p^{-1} + \alpha(\zeta_p - \zeta_p^{-1}), \ldots, \zeta_p^{-(p-1)/2} + \alpha(\zeta_p^{(p-1)/2} - \zeta_p^{-(p-1)/2}) \rangle_{\mathbb{Z}}, \qquad \text{if } d \equiv 3 \bmod (4),$$

we have $\bar{j}_1(W_{\mathcal{O}_K[\zeta_p]}(\mathcal{O}_K[\zeta_p]^+)^\times) = 1$ which contradicts $|\bar{j}_1(W_{\mathcal{O}_K[\zeta_p]}(\mathcal{O}_K[\zeta_p]^+)^\times)| = p$. Therefore $\mathrm{Coker}(\bar{j}_1) \simeq C_p$, and so our lemma is proved. □

(4.21) LEMMA. *If K is quadratic real and $b \not\equiv 0$ mod (p) where $u = a + b\alpha$ is the fundamental unit in K, then* $\mathrm{Coker}(j_1)$ *is trivial. Otherwise* $\mathrm{Coker}(j_1) \simeq C_p$.

Proof. From the proof of (4.20) we know that $\mathrm{Coker}(j_1) \simeq \mathrm{Coker}(\bar{j}_1)$, and $\mathrm{Coker}(\bar{j}_1)$ is either 1 or C_p. If $b \not\equiv 0 \bmod (p)$ then the image of the fundamental unit u under $\bar{j}_1$ is non-trivial and therefore $\mathrm{Coker}(\bar{j}_1) = 1$.

If $b \equiv 0 \bmod (p)$, then $\mathrm{Coker}(\bar{j}_1) = 1$ or C_p. Assume $\mathrm{Coker}(\bar{j}_1) = 1$. Let x be a unit in $\mathcal{O}_K[\zeta_p]^\times$ whose image under $\bar{j}_1$ generates $(\mathcal{O}_K/p\mathcal{O}_K)^\times/(\mathbb{Z}/p\mathbb{Z})^\times$. Then $\mathrm{norm}_{M/K}(x)$ is a unit in K whose image under the map

$$\mathcal{O}_K^\times \to \frac{(\mathcal{O}_K/p\mathcal{O}_K)^\times}{(\mathbb{Z}/p\mathbb{Z})^\times}$$

generates $(\mathcal{O}_K/p\mathcal{O}_K)^\times/(\mathbb{Z}/p\mathbb{Z})^\times$. But, since $b \equiv 0 \bmod (p)$, this is not possible. Therefore $\mathrm{Coker}(\bar{j}_1) \simeq C_p$. □

We now turn our attention to $\mathrm{Coker}(j_1')$.

(4.22) LEMMA. *The kernel of the map*

$$j_1' : \mathcal{O}_M^\times \to \frac{(\mathcal{O}_M/p\mathcal{O}_M)^\times}{(\mathcal{O}_K[\zeta_p]/p\mathcal{O}_M)^\times}$$

is $\mathcal{O}_K[\zeta_p]^\times$.

Proof. It is obvious that

$$\mathcal{O}_M^\times \cap \mathcal{O}_K[\zeta_p] \subseteq \mathrm{Ker}(j_1').$$

To show that $\mathrm{Ker}(j_1') \subseteq \mathcal{O}_M^\times \cap \mathcal{O}_K[\zeta_p]$, let $x \in \mathrm{Ker}(j_1')$. Then $x = a + pb$ where $a \in \mathcal{O}_K[\zeta_p]$ and $b \in \mathcal{O}_M$. But $p\mathcal{O}_M \subset \mathcal{O}_K[\zeta_p]$. Therefore $x \in \mathcal{O}_K[\zeta_p]$, and so $\mathrm{Ker}(j_1') \subseteq \mathcal{O}_M^\times \cap \mathcal{O}_K[\zeta_p]$. Since $\mathcal{O}_K[\zeta_p]$ is closed under the action of $Gal(M/\mathbb{Q})$, $\mathcal{O}_M^\times \cap \mathcal{O}_K[\zeta_p] = \mathcal{O}_K[\zeta_p]^\times$. □

The cokernel of j_1' is

$$\mathrm{Coker}(j_1') = \frac{(\mathcal{O}_M/p\mathcal{O}_M)^\times/(\mathcal{O}_K[\zeta_p]/p\mathcal{O}_M)^\times}{\mathrm{Im}(j_1')},$$

and, by (4.22),

$$\mathrm{Im}(j_1') \simeq \frac{\mathcal{O}_M^\times}{\mathcal{O}_K[\zeta_p]^\times}.$$

So in order to calculate $\mathrm{Coker}(j_1')$ we need to work out the structure of

$$\frac{(\mathcal{O}_M/p\mathcal{O}_M)^\times}{(\mathcal{O}_K[\zeta_p]/p\mathcal{O}_M)^\times}$$

and $\mathcal{O}_M^\times/\mathcal{O}_K[\zeta_p]^\times$. We begin with $(\mathcal{O}_M/p\mathcal{O}_M)^\times/(\mathcal{O}_K[\zeta_p]/p\mathcal{O}_M)^\times$.

(4.23) LEMMA.

$$\left(\frac{\mathcal{O}_M}{p\mathcal{O}_M}\right)^\times \simeq \underbrace{C_p \times \cdots \times C_p}_{2(p-2)\text{ factors}} \times \left(\frac{\mathcal{O}_{K'}}{p\mathcal{O}_{K'}}\right)^\times.$$

Proof. Let $\mathrm{rad}(\mathcal{O}_M/p\mathcal{O}_M)$ denote the radical of $\mathcal{O}_M/p\mathcal{O}_M$; $\mathrm{rad}(\mathcal{O}_M/p\mathcal{O}_M)$ is the intersection of all the maximal ideals of $\mathcal{O}_M/p\mathcal{O}_M$. Then the sequence

$$1 \to 1 + \mathrm{rad}\left(\frac{\mathcal{O}_M}{p\mathcal{O}_M}\right) \to \left(\frac{\mathcal{O}_M}{p\mathcal{O}_M}\right)^\times \to \left(\frac{\mathcal{O}_M/p\mathcal{O}_M}{\mathrm{rad}(\mathcal{O}_M/p\mathcal{O}_M)}\right)^\times \to 1 \qquad (4.24)$$

is exact. The ideal $\mathrm{rad}(\mathcal{O}_M/p\mathcal{O}_M)$ is given by

$$\mathrm{rad}\left(\frac{\mathcal{O}_M}{p\mathcal{O}_M}\right) = \frac{\prod P_M}{p\mathcal{O}_M},$$

where the product is taken over primes of M lying above p. There is only one prime of N which lies above p, namely $(1-\zeta_p)\mathcal{O}_N$. Since p does not divide $d(M/N)$, the

extension of $(1-\zeta_p)\mathcal{O}_N$ to M is either a prime or it is a product of two distinct primes. In any case the product of primes of M lying above p is $(1-\zeta_p)\mathcal{O}_M$. So we can rewrite the sequence (4.24) as

$$1 \to 1 + \frac{(1-\zeta_p)\mathcal{O}_M}{p\mathcal{O}_M} \to \left(\frac{\mathcal{O}_M}{p\mathcal{O}_M}\right)^\times \to \left(\frac{\mathcal{O}_M}{(1-\zeta_p)\mathcal{O}_M}\right)^\times \to 1. \tag{4.25}$$

Since $|\mathcal{O}_M/p\mathcal{O}_M| = p^{2(p-1)}$ and $|\mathcal{O}_M/(1-\zeta_p)\mathcal{O}_M| = p^2$, it follows that

$$\left|1 + \frac{(1-\zeta_p)\mathcal{O}_M}{p\mathcal{O}_M}\right| = \left|\frac{(1-\zeta_p)\mathcal{O}_M}{p\mathcal{O}_M}\right| = p^{2(p-2)}. \tag{4.26}$$

To find the structure of $1 + (1-\zeta_p)\mathcal{O}_M/p\mathcal{O}_M$, let $x \in 1 + (1-\zeta_p)\mathcal{O}_M/p\mathcal{O}_M$. Then $x = 1 + (1-\zeta_p)y$, $y \in (\mathcal{O}_M/p\mathcal{O}_M)$, and

$$\begin{aligned} x^p &= (1 + (1-\zeta_p)y)^p, \\ &\equiv 1 + (1-\zeta_p)^p y^p \bmod (p\mathcal{O}_M), \\ &\equiv 1 \bmod (p\mathcal{O}_M). \end{aligned}$$

This shows that $1 + (1-\zeta_p)\mathcal{O}_M/p\mathcal{O}_M$ is an elementary p-group, and so, by (4.26),

$$1 + \frac{(1-\zeta_p)\mathcal{O}_M}{p\mathcal{O}_M} \simeq \underbrace{C_p \times \cdots \times C_p}_{2(p-2) \text{ factors}}.$$

To find $(\mathcal{O}_M/(1-\zeta_p)\mathcal{O}_M)^\times$, we note that

$$\frac{\mathcal{O}_M}{(1-\zeta_p)\mathcal{O}_M} \simeq \frac{\mathcal{O}_{K'}}{p\mathcal{O}_{K'}};$$

the isomorphism is induced by $\zeta_p \mapsto 1$. Substituting for $1 + (1-\zeta_p)\mathcal{O}_M/p\mathcal{O}_M$ and $(\mathcal{O}_M/(1-\zeta_p)\mathcal{O}_M)^\times$ in (4.25) gives

$$1 \to C_p \times \cdots \times C_p \to \left(\frac{\mathcal{O}_M}{p\mathcal{O}_M}\right)^\times \to \left(\frac{\mathcal{O}_{K'}}{p\mathcal{O}_{K'}}\right)^\times \to 1.$$

Since p does not divide $d(K'/\mathbb{Q})$, p is either inert in K' or it splits. In any case the order of $(\mathcal{O}_{K'}/p\mathcal{O}_{K'})^\times$ is coprime to p. The end groups in the above exact sequence, therefore, have orders which are relatively coprime, and so

$$\left(\frac{\mathcal{O}_M}{p\mathcal{O}_M}\right)^\times \simeq \underbrace{C_p \times \cdots \times C_p}_{2(p-2) \text{ factors}} \times \left(\frac{\mathcal{O}_{K'}}{p\mathcal{O}_{K'}}\right)^\times.$$

□

(4.27) LEMMA.

$$\left(\frac{\mathcal{O}_K[\zeta_p]}{p\mathcal{O}_M}\right)^\times \simeq \underbrace{C_p \times \cdots \times C_p}_{(3p-5)/2 \text{ factors}} \times \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times.$$

Proof. As in (4.23), the sequence

$$1 \to 1 + \operatorname{rad}\left(\frac{\mathcal{O}_K[\zeta_p]}{p\mathcal{O}_M}\right) \to \left(\frac{\mathcal{O}_K[\zeta_p]}{p\mathcal{O}_M}\right)^\times \to \left(\frac{\mathcal{O}_K[\zeta_p]/p\mathcal{O}_M}{\operatorname{rad}(\mathcal{O}_K[\zeta_p]/p\mathcal{O}_M)}\right)^\times \to 1 \qquad (4.28)$$

is exact.

To find $\operatorname{rad}(\mathcal{O}_K[\zeta_p]/p\mathcal{O}_M)$, we note that for a finite commutative ring R,

$$\operatorname{rad}(R) = \{x \in R \mid x^n = 0 \text{ for some integer } n\},$$

and if S is a subring of R then $\operatorname{rad}(S) = \operatorname{rad}(R) \cap S$. Applying this argument to $\mathcal{O}_M/p\mathcal{O}_M$ and $\mathcal{O}_K[\zeta_p]/p\mathcal{O}_M$ gives

$$\begin{aligned}\operatorname{rad}\left(\frac{\mathcal{O}_K[\zeta_p]}{p\mathcal{O}_M}\right) &= \operatorname{rad}\left(\frac{\mathcal{O}_M}{p\mathcal{O}_M}\right) \cap \frac{\mathcal{O}_K[\zeta_p]}{p\mathcal{O}_M}, \\ &= \frac{(1-\zeta_p)\mathcal{O}_M}{p\mathcal{O}_M} \cap \frac{\mathcal{O}_K[\zeta_p]}{p\mathcal{O}_M}, \\ &= \frac{(1-\zeta_p)\mathcal{O}_M \cap \mathcal{O}_K[\zeta_p]}{p\mathcal{O}_M}.\end{aligned}$$

Let

$$T = \{x \in \mathcal{O}_M \mid (1-\zeta_p)x \in \mathcal{O}_K[\zeta_p]\}.$$

Then

$$\operatorname{rad}\left(\frac{\mathcal{O}_K[\zeta_p]}{p\mathcal{O}_M}\right) = \frac{(1-\zeta_p)T}{p\mathcal{O}_M},$$

and (4.28) now gives

$$1 \to 1 + \left(\frac{(1-\zeta_p)T}{p\mathcal{O}_M}\right) \to \left(\frac{\mathcal{O}_K[\zeta_p]}{p\mathcal{O}_M}\right)^\times \to \left(\frac{\mathcal{O}_K[\zeta_p]}{(1-\zeta_p)T}\right)^\times \to 1. \qquad (4.29)$$

Now $(1-\zeta_p)T$ is an ideal of $\mathcal{O}_K[\zeta_p]$ which contains $(1-\zeta_p)\mathcal{O}_K[\zeta_p]$:

$$(1-\zeta_p)\mathcal{O}_K[\zeta_p] \subset (1-\zeta_p)T \subset \mathcal{O}_K[\zeta_p]. \qquad (4.30)$$

The $\mathbb{Z}$-index of $(1-\zeta_p)\mathcal{O}_K[\zeta_p]$ in $\mathcal{O}_K[\zeta_p]$ is given by

$$(\mathcal{O}_K[\zeta_p] : (1-\zeta_p)\mathcal{O}_K[\zeta_p]) = \frac{(\mathcal{O}_M : (1-\zeta_p)\mathcal{O}_K[\zeta_p])}{(\mathcal{O}_M : \mathcal{O}_K[\zeta_p])}.$$

Since

$$(\mathcal{O}_M : (1-\zeta_p)\mathcal{O}_K[\zeta_p]) = \mathrm{norm}_M(1-\zeta_p)\cdot(\mathcal{O}_M : \mathcal{O}_K[\zeta_p]),$$

we obtain

$$(\mathcal{O}_K[\zeta_p] : (1-\zeta_p)\mathcal{O}_K[\zeta_p]) = p^2.$$

In (4.30) $(1-\zeta_p)T \neq \mathcal{O}_K[\zeta_p]$ and, since the element $(1-\zeta_p)^{(p-3)/2}\beta$ lies in T but not in $\mathcal{O}_K[\zeta_p]$, $(1-\zeta_p)\mathcal{O}_K[\zeta_p] \neq (1-\zeta_p)T$. Therefore $(\mathcal{O}_K[\zeta_p] : (1-\zeta_p)T) = p$. This implies that $(1-\zeta_p)T$ is a maximal $\mathcal{O}_K[\zeta_p]$-ideal, and therefore

$$\frac{\mathcal{O}_K[\zeta_p]}{(1-\zeta_p)T} \simeq \frac{\mathbb{Z}}{p\mathbb{Z}}.$$

Next we calculate the order of the group $1+(1-\zeta_p)T/p\mathcal{O}_M$. We have

$$\begin{aligned}(\mathcal{O}_K[\zeta_p] : p\mathcal{O}_M) &= \frac{(\mathcal{O}_M : p\mathcal{O}_M)}{(\mathcal{O}_M : \mathcal{O}_K[\zeta_p])},\\ &= \frac{p^{2(p-1)}}{p^{(p-1)/2}},\\ &= p^{3(p-1)/2}.\end{aligned}$$

But

$$(\mathcal{O}_K[\zeta_p] : p\mathcal{O}_M) = (\mathcal{O}_K[\zeta_p] : (1-\zeta_p)T)((1-\zeta_p)T : p\mathcal{O}_M).$$

Therefore

$$\begin{aligned}((1-\zeta_p)T : p\mathcal{O}_M) &= \frac{(\mathcal{O}_K[\zeta_p] : p\mathcal{O}_M)}{(\mathcal{O}_K[\zeta_p] : (1-\zeta_p)T)},\\ &= p^{(3p-5)/2}.\end{aligned}$$

This gives us the order of $1+(1-\zeta_p)T/p\mathcal{O}_M$. If we now use the fact that $1+(1-\zeta_p)T/p\mathcal{O}_M$ is a subgroup of $1+(1-\zeta_p)\mathcal{O}_M/p\mathcal{O}_M$ and $1+(1-\zeta_p)\mathcal{O}_M/p\mathcal{O}_M$ is an elementary p-group, we obtain

$$1+(1-\zeta_p)T/p\mathcal{O}_M \simeq \underbrace{C_p \times \cdots \times C_p}_{(3p-5)/2 \text{ factors}}.$$

Substituting for $1+(1-\zeta_p)T/p\mathcal{O}_M$ and $\mathcal{O}_K[\zeta_p]/(1-\zeta_p)T$ in (4.29) gives

$$1 \to C_p \times \cdots \times C_p \to \left(\frac{\mathcal{O}_K[\zeta_p]}{p\mathcal{O}_M}\right)^{\times} \to \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^{\times} \to 1,$$

and therefore

$$\left(\frac{\mathcal{O}_K[\zeta_p]}{p\mathcal{O}_M}\right)^\times \simeq \underbrace{C_p \times \cdots \times C_p}_{(3p-5)/2 \text{ factors}} \times \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times.$$

□

We are now in a position to prove the following.

(4.31) THEOREM.

$$\frac{(\mathcal{O}_M/p\mathcal{O}_M)^\times}{(\mathcal{O}_K[\zeta_p]/p\mathcal{O}_M)^\times} \simeq \underbrace{C_p \times \cdots \times C_p}_{(p-3)/2 \text{ factors}} \times C_{p^*},$$

where

$$p^* = \begin{cases} p+1, & \text{if } p \text{ is inert in } K', \\ p-1, & \text{if } p \text{ splits in } K'. \end{cases}$$

Proof. From (4.23) and (4.27) we have

$$\frac{(\mathcal{O}_M/p\mathcal{O}_M)^\times}{(\mathcal{O}_K[\zeta_p]/p\mathcal{O}_M)^\times} \simeq \underbrace{C_p \times \cdots \times C_p}_{(p-3)/2 \text{ factors}} \times \frac{(\mathcal{O}_{K'}/p\mathcal{O}_{K'})^\times}{(\mathbb{Z}/p\mathbb{Z})^\times}.$$

Since $p\mathcal{O}_{K'}$ is either a prime or it is a product of two primes,

$$\frac{\mathcal{O}_{K'}}{p\mathcal{O}_{K'}} \simeq \begin{cases} \mathrm{GF}(p^2), & \text{if } p \text{ is inert in } K', \\ \mathrm{GF}(p) \times \mathrm{GF}(p), & \text{if } p \text{ splits in } K'. \end{cases}$$

Therefore

$$\left(\frac{\mathcal{O}_{K'}}{p\mathcal{O}_{K'}}\right)^\times \simeq \begin{cases} C_{p^2-1}, & \text{if } p \text{ is inert in } K', \\ C_{p-1} \times C_{p-1}, & \text{if } p \text{ splits in } K'. \end{cases}$$

The rest is obvious. □

Having obtained the structure of $(\mathcal{O}_M/p\mathcal{O}_M)^\times/(\mathcal{O}_K[\zeta_p]/p\mathcal{O}_M)^\times$, we now calculate $\mathcal{O}_M^\times/\mathcal{O}_K[\zeta_p]^\times$.

By (4.22), $\mathcal{O}_M^\times/\mathcal{O}_K[\zeta_p]^\times$ is isomorphic to a subgroup of

$$\frac{(\mathcal{O}_M/p\mathcal{O}_M)^\times}{(\mathcal{O}_K[\zeta_p]/p\mathcal{O}_M)^\times}$$

and, since we know the structure of this group, we can at once write

$$\frac{\mathcal{O}_M^\times}{\mathcal{O}_K[\zeta_p]^\times} \simeq \underbrace{C_p \times \cdots \times C_p}_{n \text{ factors}} \times C_a,$$

where $[\mathcal{O}_M^\times : \mathcal{O}_K[\zeta_p]^\times] = p^n a$, and a is a divisor of p^*. So if we knew the integers n

and a we will know the structure of $\mathcal{O}_M^\times/\mathcal{O}_K[\zeta_p]^\times$.

Let $\lambda_i = (1-\zeta_p)^i$, $0 \le i \le p-1$, and $\mathcal{O}_i = \mathcal{O}_N[\lambda_i\beta]$. Then we have the following chain of rings:

$$\mathcal{O}_{p-1} \subset \mathcal{O}_{p-2} \subset \cdots \subset \mathcal{O}_1 \subset \mathcal{O}_0.$$

In the above chain, each ring properly contains the preceding ring.

(4.32) LEMMA.

$$(\mathcal{O}_i : \mathcal{O}_{i+1}) = p, \qquad 0 \le i \le p-2.$$

Proof. We have

$$\mathcal{O}_0 = \langle \zeta_p, \ldots \zeta_p^{p-1}, \beta\zeta_p, \ldots, \beta\zeta_p^{p-1} \rangle_{\mathbb{Z}},$$
$$\mathcal{O}_{p-1} = \langle \zeta_p, \ldots, \zeta_p^{p-1}, p\beta\zeta_p, \ldots, p\beta\zeta_p^{p-1} \rangle_{\mathbb{Z}},$$

and therefore $(\mathcal{O}_0 : \mathcal{O}_{p-1}) = p^{p-1}$. But

$$(\mathcal{O}_0 : \mathcal{O}_{p-1}) = \prod_{i=0}^{p-2} (\mathcal{O}_i : \mathcal{O}_{i+1}).$$

So each index $(\mathcal{O}_i : \mathcal{O}_{i+1})$ must be a power of p. Since $\mathcal{O}_i$ properly contains $\mathcal{O}_{i+1}$, $(\mathcal{O}_i : \mathcal{O}_{i+1}) \ge p$. As there are $p-1$ factors in the above product, $(\mathcal{O}_i : \mathcal{O}_{i+1}) = p$. □

In the above notation, $\mathcal{O}_M = \mathcal{O}_0$, $\mathcal{O}_K[\zeta_p] = \mathcal{O}_{(p-1)/2}$ and, by (4.32), $(\mathcal{O}_0 : \mathcal{O}_{(p-1)/2}) = p^{(p-1)/2}$ which is consistent with (4.15).

The $\mathcal{O}_0$-ideal $p\mathcal{O}_0$ lies in $\mathcal{O}_{p-1}$, and therefore it is an $\mathcal{O}_i$-ideal for all $0 \le i \le p-1$.

(4.33) LEMMA.

$$\left(\frac{\mathcal{O}_i}{p\mathcal{O}_0}\right)^\times \simeq \underbrace{C_p \times \cdots \times C_p}_{2p-3-i \text{ factors}} \times C_{p-1}, \qquad 1 \le i \le p-1.$$

Proof. The proof is similar to the one given in (4.27). We start with the exact sequence

$$1 \to 1 + \mathrm{rad}\left(\frac{\mathcal{O}_i}{p\mathcal{O}_0}\right) \to \left(\frac{\mathcal{O}_i}{p\mathcal{O}_0}\right)^\times \to \left(\frac{\mathcal{O}_i/p\mathcal{O}_0}{\mathrm{rad}(\mathcal{O}_i/p\mathcal{O}_0)}\right)^\times \to 1.$$

For $1 \leq i \leq p-1$, $\mathrm{rad}(\mathcal{O}_i/p\mathcal{O}_0)$ is given by

$$\begin{aligned}\mathrm{rad}\left(\frac{\mathcal{O}_i}{p\mathcal{O}_0}\right) &= \mathrm{rad}\left(\frac{\mathcal{O}_0}{p\mathcal{O}_0}\right) \cap \frac{\mathcal{O}_i}{p\mathcal{O}_0}, \\ &= \frac{(1-\zeta_p)\mathcal{O}_0}{p\mathcal{O}_0} \cap \frac{\mathcal{O}_i}{p\mathcal{O}_0}, \\ &= \frac{(1-\zeta_p)\mathcal{O}_{i-1}}{p\mathcal{O}_0}.\end{aligned}$$

Now $(1-\zeta_p)\mathcal{O}_{i-1}$, one can easily show, is a maximal $\mathcal{O}_i$-ideal, and

$$\begin{aligned}(\mathcal{O}_i : (1-\zeta_p)\mathcal{O}_{i-1}) &= p, \\ ((1-\zeta_p)\mathcal{O}_{i-1} : p\mathcal{O}_0) &= p^{2p-3-i}.\end{aligned}$$

Therefore

$$\begin{aligned}\left|\left(\frac{\mathcal{O}_i}{p\mathcal{O}_0}\right)^\times\right| &= \left|1 + \frac{(1-\zeta_p)\mathcal{O}_{i-1}}{p\mathcal{O}_0}\right| \cdot \left|\left(\frac{\mathcal{O}_i}{(1-\zeta_p)\mathcal{O}_{i-1}}\right)^\times\right|, \\ &= p^{2p-3-i}(p-1).\end{aligned}$$

If we now use (4.23) and the fact that $(\mathcal{O}_i/p\mathcal{O}_0)^\times$ is a subgroup of $(\mathcal{O}_0/p\mathcal{O}_0)^\times$, we obtain the required result. □

Let $\mathcal{O}_i^+$ be the maximal real subring of $\mathcal{O}_i$, $U_i = \mathcal{O}_i^\times$, and $U_i^+ = (\mathcal{O}_i^+)^\times$. Then

$$\begin{aligned}[\mathcal{O}_M^\times : \mathcal{O}_K[\zeta_p]^\times] &= [U_0 : U_{(p-1)/2}], \\ &= \prod_{i=0}^{(p-3)/2} [U_i : U_{i+1}].\end{aligned}$$

The following result takes us a step closer to calculating the index $[\mathcal{O}_M^\times : \mathcal{O}_K[\zeta_p]^\times]$.

(4.34) LEMMA.

$$\begin{aligned}[U_0 : U_1] &= p^*/|D(\mathcal{O}_{K'}G)|, \\ [U_i : U_{i+1}] &= 1 \text{ or } p, \qquad 1 \leq i \leq p-2.\end{aligned}$$

Proof. Let

$$k : U_i \to \frac{(\mathcal{O}_i/p\mathcal{O}_0)^\times}{(\mathcal{O}_{i+1}/p\mathcal{O}_0)^\times}$$

be the map induced by $\mathcal{O}_i \to \mathcal{O}_i/p\mathcal{O}_0$. Then $\mathrm{Ker}(k) = U_{i+1}$, and therefore U_i/U_{i+1} is isomorphic to a subgroup of $(\mathcal{O}_i/p\mathcal{O}_0)^\times/(\mathcal{O}_{i+1}/p\mathcal{O}_0)^\times$. By (4.33),

$$\left|\frac{(\mathcal{O}_i/p\mathcal{O}_0)^\times}{(\mathcal{O}_{i+1}/p\mathcal{O}_0)^\times}\right| = p, \qquad 1 \leq i \leq p-2,$$

and therefore, for $1 \leq i \leq p-2$, $[U_i : U_{i+1}] = 1$ or p.

If $i = 0$, then

$$\frac{(\mathcal{O}_0/p\mathcal{O}_0)^\times}{(\mathcal{O}_1/p\mathcal{O}_0)^\times} \simeq \frac{(\mathcal{O}_{K'}/p\mathcal{O}_{K'})^\times}{(\mathbb{Z}/p\mathbb{Z})^\times} \simeq C_{p^*}.$$

The isomorphism is induced by $\zeta_p \to 1$. Let k' be k followed by reduction mod $(1-\zeta_p)$. Then $\mathrm{Coker}(k') \simeq D(\mathcal{O}_{K'}G)$, and so $|k'(U_0)| = p^*/|D(\mathcal{O}_{K'}G)|$. Since $U_0/U_1 \simeq k'(U_0)$, $[U_0 : U_1] = p^*/|D(\mathcal{O}_{K'}G)|$. □

(4.35) LEMMA. *For $1 \le i \le p-1$, let Q_i be the index of $W_iU_i^+$ in U_i. Then $Q_i = 1$ or 2, and $Q_i = Q_1$ for all $1 \le i \le p-1$.*

Proof. There is an exact sequence:

$$1 \to W_iU_i^+ \to U_i \xrightarrow{\overline{\psi}} W_i/W_i^2,$$

where $\overline{\psi}$ sends a unit u to $[u/u^c]$. The group W_i/W_i^2 is generated by -1. If $\overline{\psi}$ is surjective then $Q_i = 2$; otherwise $Q_i = 1$.

To prove the second part, we note that $U_i/W_iU_i^+$ is isomorphic to a subgroup of $U_1/W_1U_1^+$ and therefore Q_i divides Q_1. If $Q_1 = 1$ then $Q_i = 1$. Let us assume $Q_1 = 2$. Let u be the unit that lies in U_1 but not in $W_1U_1^+$. We can assume $u^c = -u$. By (4.34), $[U_1 : U_i] = p^r$. Therefore $u^{p^r} \in U_i$, and $(u^{p^r})^c = -u^{p^r}$. So $\overline{\psi} : U_i \to W_i/W_i^2$ is surjective, i.e., $Q_i = 2$. □

(4.36) LEMMA.

$$[U_i : U_{i+1}] = [U_i^+ : U_{i+1}^+], \qquad 1 \le i \le p-2.$$

Proof. We can express the index $[U_i : U_{i+1}^+]$ as

$$[U_i : U_{i+1}^+] = [U_i : U_{i+1}][U_{i+1} : U_{i+1}^+], \tag{4.37}$$

or

$$[U_i : U_{i+1}^+] = [U_i : U_i^+][U_i^+ : U_{i+1}^+]. \tag{4.38}$$

By (4.35), $[U_i : W_iU_i^+] = Q_1$, $1 \le i \le p-1$, or

$$[U_i : U_i^+] = Q_1 p, \tag{4.39}$$

since $[W_iU_i^+ : U_i^+] = p$. Equating (4.37) and (4.38), and using (4.39) proves the lemma. □

(4.40) LEMMA. *If K' is real, then, for odd i,*

$$[U_i^+ : U_{i+1}^+] = 1, \qquad 1 \le i \le p-2,$$

and if K' is imaginary, then, for even i,

$$[U_i^+ : U_{i+1}^+] = 1, \qquad 1 \le i \le p-2.$$

Proof. Let us assume K' is real, and, for an odd i, $[U_i^+ : U_{i+1}^+] \neq 1$. Let u be the unit that lies in U_i^+ but not in U_{i+1}^+. Then $u = a + \lambda_i \beta b$, $a, b \in \mathcal{O}_N$, and $b \notin (1-\zeta_p)\mathcal{O}_N$. Since u is real, $u^c = u$. But

$$u^c = a^c + (-1)^i \zeta_p^{-i} \lambda_i \beta b^c.$$

Therefore

$$(a + \lambda_i \beta b) - (a^c + (-1)^i \zeta_p^{-i} \lambda_i \beta b^c) = 0,$$

and so $a - a^c = 0$, and

$$\lambda_i b - (-1)^i \zeta_p^{-i} \lambda_i b^c = 0. \tag{4.41}$$

The above equation gives $b + \zeta_p^{-i} b^c = 0$, since i is odd. This implies $1 + \zeta_p^{-i} \equiv 0 \bmod (1-\zeta_p)$ which clearly is not true.

The proof of the second part is similar except that we obtain

$$\lambda_i b + (-1)^i \zeta_p^{-i} \lambda_i b^c = 0$$

instead of (4.41). Since i is even now, this again leads to $1 + \zeta_p^{-i} \equiv 0 \bmod (1-\zeta_p)$. □

(4.42) LEMMA. *If p does not divide h_M, the class number of M, then, for K' real and i even and for K' imaginary and i odd,*

$$[U_i^+ : U_{i+1}^+] = p, \qquad 1 \le i \le p-2.$$

Proof. The lemma will follow at once if we allow ourselves the following (see [6]): if p does not divide h_M, then there are units in U_0^+ which satisfy, for K' real,

$$\begin{aligned} u_1 &\equiv 1 + a_1 \lambda_2 \bmod (\lambda_3), \\ u_2 &\equiv 1 + a_2 \lambda_4 \bmod (\lambda_5), \\ &\vdots \\ u_{(p-3)/2} &\equiv 1 + a_{(p-3)/2} \lambda_{p-3} \bmod (\lambda_{p-2}), \end{aligned}$$

$$v_1 \equiv 1 + b_1\lambda_2 \bmod (\lambda_3),$$
$$v_2 \equiv 1 + b_2\lambda_4 \bmod (\lambda_5),$$
$$\vdots$$
$$v_{(p-1)/2} \equiv 1 + b_{(p-1)/2}\lambda_{p-1} \bmod (\lambda_p),$$

where $a_i, b_i \in \mathcal{O}_{K'}$ and, for each $1 \leq i \leq (p-3)/2$,

$$\frac{\mathcal{O}_{K'}}{p\mathcal{O}_{K'}} = \langle a_i, b_i \rangle \frac{\mathbb{Z}}{p\mathbb{Z}},$$

and, for K' imaginary,

$$u_1 \equiv 1 + \lambda_2 \bmod (\lambda_3),$$
$$u_2 \equiv 1 + \lambda_4 \bmod (\lambda_5),$$
$$\vdots$$
$$u_{(p-3)/2} \equiv 1 + \lambda_{p-3} \bmod (\lambda_{p-2}),$$

$$v_1 \equiv 1 + \sqrt{-d'}\lambda_1 \bmod (\lambda_2),$$
$$v_2 \equiv 1 + \sqrt{-d'}\lambda_3 \bmod (\lambda_4),$$
$$\vdots$$
$$v_{(p-1)/2} \equiv 1 + \sqrt{-d'}\lambda_{p-2} \bmod (\lambda_{p-1}).$$

In the K' real case, for a given $1 \leq i \leq (p-3)/2$, $u_i, v_i \in U_{2i}^+$. The units u_i, v_i cannot both lie in U_{2i+1}^+, for otherwise a_i, b_i will fail to be a basis for $\mathcal{O}_{K'}/p\mathcal{O}_{K'}$ over $\mathbb{Z}/p\mathbb{Z}$. Therefore $[U_{2i}^+ : U_{2i+1}^+] > 1$. But, by (4.34) and (4.36), $[U_{2i}^+ : U_{2i+1}^+] = 1$ or p. Therefore $[U_{2i}^+ : U_{2i+1}^+] = p$.

In the K' imaginary case, $v_i \in U_{2i-1}^+$ but v_i clearly does not lie in U_{2i}^+, and so $[U_{2i-1}^+ : U_{2i}^+] > 1$. Using (4.34) and (4.36) gives $[U_{2i-1}^+ : U_{2i}^+] = p$. □

Combining the results of last several lemmas we obtain

(4.43) THEOREM. *If p does not divide h_M, then*

$$\frac{\mathcal{O}_M^\times}{\mathcal{O}_K[\zeta_p]^\times} \simeq \underbrace{C_p \times \cdots \times C_p}_{n \text{ factors}} \times C_a,$$

where $a = p^*/|D(\mathcal{O}_{K'}G)|$ and, if K' is real,

$$n = \begin{cases} (p-5)/4, & \text{if } p \equiv 1 \bmod (4), \\ (p-3)/4, & \text{if } p \equiv 3 \bmod (4), \end{cases}$$

and if K' is imaginary,

$$n = \begin{cases} (p-1)/4, & \text{if } p \equiv 1 \bmod (4), \\ (p-3)/4, & \text{if } p \equiv 3 \bmod (4). \end{cases}$$

Proof. The proof is a straightforward matter of obtaining the number of even indices in $1 \leq i \leq (p-3)/2$ in the K' real case, and the number of odd indices in $1 \leq i \leq (p-3)/2$ in the K' imaginary case. Using (4.42) will then give the order of $\mathcal{O}_M^\times/\mathcal{O}_K[\zeta_p]^\times$ at p.

The order of $\mathcal{O}_M^\times/\mathcal{O}_K[\zeta_p]^\times$ away from p was calculated in (4.34). □

We can now prove (4.2) and (4.3).

Proof of (4.2). By (4.18), the kernel group $D(\mathcal{O}_K G)$ is given by

$$1 \to \text{Coker}(j_1) \to D(\mathcal{O}_K G) \to \text{Coker}(j_1') \to 1.$$

But, by (4.21), $\text{Coker}(j_1) = 1$. The group $\text{Coker}(j_1')$ is given by

$$\text{Coker}(j_1') \simeq \frac{(\mathcal{O}_M/p\mathcal{O}_M)^\times/(\mathcal{O}_K[\zeta_p]/p\mathcal{O}_M)^\times}{\mathcal{O}_M^\times/\mathcal{O}_K[\zeta_p]^\times}.$$

Using (4.31) and (4.43) now proves the theorem. □

Proof of (4.3). The proof, as in the case of (4.2), is a straightforward matter of putting (4.18), (4.20), (4.31), and (4.43) together. □

5. $R(\mathcal{O}_K G)$ — the group of realizable classes

We now turn to the problem of calculating the group, $R(\mathcal{O}_K G)$, of realizable classes in $Cl(\mathcal{O}_K G)$ where K is a quadratic imaginary number field. In the following we will calculate $R(\mathcal{O}_K G)$ subject to G being a cyclic group of prime order p and the class number of $M = K(\zeta_p)$ being trivial. We will also, given a tame extension L of K with $Gal(L/K) \simeq G$, obtain invariants of L which will completely determine the class of $\mathcal{O}_L$ in $R(\mathcal{O}_K G)$.

Just to confirm our notation, we will continue to write K as $\mathbb{Q}(\sqrt{-d})$ and $\mathcal{O}_K$ as $\mathbb{Z}[\alpha]$. The values of d are now restricted to positive square-free integers.

Our starting point is the description of $R(\mathcal{O}_K G)$ given in [9] which goes as follows.

Let $\Delta = \mathrm{Aut}(G)$, the group of automorphisms of G. Then, since G is cyclic of order p, $\Delta \simeq (\mathbb{Z}/p\mathbb{Z})^\times$. We can take Δ to be

$$\Delta = \{\delta_i \mid 1 \leq i \leq p-1\},$$

where the action of δ_i on G is defined as $\delta_i(g) = g^i$. For $\delta \in \Delta$ and $(C) \in Cl(\mathcal{O}_K G)$, let (C^δ) be the class in $Cl(\mathcal{O}_K G)$ where C^δ is isomorphic to C as an abelian group but with G-action $gx^\delta = (\delta(g)x)^\delta$. Then under the multiplication

$$\begin{aligned} \Delta \times Cl(\mathcal{O}_K G) &\to Cl(\mathcal{O}_K G), \\ (\delta, (C)) &\mapsto (C^\delta), \end{aligned}$$

$Cl(\mathcal{O}_K G)$ is a $\mathbb{Z}\Delta$-module. Let

$$\theta' = \sum_{a=1}^{p-1} a\delta_a^{-1},$$

and

$$J = \mathbb{Z}\Delta \cap (\theta'/p)\mathbb{Z}\Delta,$$

the Stickelberger ideal. Then the group of realizable classes is given by

$$R(\mathcal{O}_K G) = Cl^0(\mathcal{O}_K G)^J,$$

where

$$Cl^0(\mathcal{O}_K G) = \mathrm{Ker}(Cl(\mathcal{O}_K G) \to Cl(\mathcal{O}_K)).$$

$Cl^0(\mathcal{O}_K G)^J$ is the subgroup of $Cl^0(\mathcal{O}_K G)$ generated by (C^j) for (C) in $Cl^0(\mathcal{O}_K G)$ and j in J.

We can now proceed with the calculation of $R(\mathcal{O}_K G)$. In the next section we will calculate $R(\mathcal{O}_K G)$ for p an odd prime, but here we obtain $R(\mathcal{O}_K G)$ in the case when $p = 2$.

(5.1) THEOREM. *If $G \simeq C_2$ and M has class number 1, then*

$$R(\mathcal{O}_K G) \simeq \begin{cases} 1, & \text{if } K = \mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{-3}),\ \text{or } \mathbb{Q}(\sqrt{-7}), \\ C_2, & \text{if } K = \mathbb{Q}(\sqrt{-2}), \\ C_3, & \text{otherwise.} \end{cases}$$

Proof. For $G \simeq C_2$, the Stickelberger ideal J is $\mathbb{Z}$ and therefore

$$R(\mathcal{O}_K G) = Cl^0(\mathcal{O}_K G)^J = Cl^0(\mathcal{O}_K G).$$

The maximal order in KG is $\mathcal{O}_K \times \mathcal{O}_K$, and so we have an exact sequence

$$1 \to D(\mathcal{O}_K G) \to Cl(\mathcal{O}_K G) \to Cl(\mathcal{O}_K) \times Cl(\mathcal{O}_K) \to 1.$$

Since the class number of $M = K(\zeta_2) = K$ is 1, $Cl(\mathcal{O}_K) = 1$ and therefore

$$Cl^0(\mathcal{O}_K G) = Cl(\mathcal{O}_K G) = D(\mathcal{O}_K G).$$

To calculate $D(\mathcal{O}_K G)$, we note that the diagram

$$\begin{array}{ccc} \mathcal{O}_K G & \xrightarrow{i_1} & \mathcal{O}_K \\ \downarrow i_2 & & \downarrow j_1 \\ \mathcal{O}_K & \xrightarrow{j_2} & \mathcal{O}_K/2\mathcal{O}_K \end{array}$$

is a cartesian square. The various maps are given by

$$\begin{array}{ccc} g & \xrightarrow{i_1} & -1 \\ \downarrow i_2 & & \downarrow j_1 \\ 1 & \xrightarrow{j_2} & [1] \end{array}$$

The Mayer-Vietoris sequence attached to the above square gives

$$j_1(\mathcal{O}_K^\times) \times j_2(\mathcal{O}_K^\times) \to (\mathcal{O}_K/2\mathcal{O}_K)^\times \to D(\mathcal{O}_K G) \to D(\mathcal{O}_K) \times D(\mathcal{O}_K) \to 1.$$

But $j_2(\mathcal{O}_K^\times) \subseteq j_1(\mathcal{O}_K^\times)$, and $D(\mathcal{O}_K) = 1$. Therefore $D(\mathcal{O}_K G) \simeq \mathrm{Coker}(j_1)$ where

$$j_1 : \mathcal{O}_K^\times \to (\mathcal{O}_K/2\mathcal{O}_K)^\times.$$

The group, $\mathcal{O}_K^\times$, of units is

$$\mathcal{O}_K^\times = \begin{cases} \langle \zeta_4 \rangle, & \text{if } K = \mathbb{Q}(\sqrt{-1}), \\ \langle -1, \zeta_3 \rangle, & \text{if } K = \mathbb{Q}(\sqrt{-3}), \\ \langle -1 \rangle, & \text{otherwise.} \end{cases}$$

Now 2 ramifies in $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-2})$, and so, for these fields, $(\mathcal{O}_K/2\mathcal{O}_K)^\times \simeq C_2$. If $K = \mathbb{Q}(\sqrt{-1})$, then $(\mathcal{O}_K/2\mathcal{O}_K)^\times = \langle \zeta_4 \rangle$, and j_1 is surjective, which means, $D(\mathcal{O}_K G) = 1$. If $K = \mathbb{Q}(\sqrt{-2})$, then $(\mathcal{O}_K/2\mathcal{O}_K)^\times = \langle 1 + \alpha \rangle$, and $D(\mathcal{O}_K G) \simeq C_2$.

If $K = \mathbb{Q}(\sqrt{-7})$, then 2 splits in K and $(\mathcal{O}_K/2\mathcal{O}_K)^\times = 1$. So we obtain $D(\mathcal{O}_K G) = 1$ for $K = \mathbb{Q}(\sqrt{-7})$.

For the rest of the fields, 2 is inert and so $(\mathcal{O}_K/2\mathcal{O}_K)^\times \simeq C_3$. If $K = \mathbb{Q}(\sqrt{-3})$, then $D(\mathcal{O}_K G) = 1$; otherwise $D(\mathcal{O}_K G) \simeq C_3$. □

(5.2) COROLLARY. *If $K = \mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-3})$ or $\mathbb{Q}(\sqrt{-7})$, then any tame quadratic extension of K has a normal integral basis.*

Proof. Obvious from the theorem. □

Next, for a tame quadratic extension L of K with $Gal(L/K) \simeq G$, we identify the class of $\mathcal{O}_L$ in $R(\mathcal{O}_K G)$. Because of (5.2) we can assume that K is a field other than $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-3})$, or $\mathbb{Q}(\sqrt{-7})$. We continue to assume that M, which for $p = 2$ is K, has class number 1.

Let L be a quadratic extension of K. Then $L = K(\beta)$ where $\beta = \sqrt{l}$, $l \in \mathcal{O}_K$. Since $h_K = 1$, we can assume l is square-free.

(5.3) THEOREM. *L is a tame extension of K if and only if $l \equiv a^2 \bmod (4\mathcal{O}_K)$ where $a \in (\mathcal{O}_K/2\mathcal{O}_K)^\times$;*

$$\left(\frac{\mathcal{O}_K}{2\mathcal{O}_K}\right)^\times = \begin{cases} \{1, 1+\alpha\}, & \text{if } K = \mathbb{Q}(\sqrt{-2}), \\ \{1, \alpha, 1+\alpha\}, & \text{otherwise.} \end{cases}$$

The class of $\mathcal{O}_L$ in

$$R(\mathcal{O}_K G) \simeq \begin{cases} C_2, & \text{if } K = \mathbb{Q}(\sqrt{-2}), \\ C_3, & \text{otherwise,} \end{cases}$$

is trivial if $l \equiv 1 \bmod (4\mathcal{O}_K)$, and it generates $R(\mathcal{O}_K G)$ if $l \not\equiv 1 \bmod (4\mathcal{O}_K)$.

Proof. Since $[L : K] = 2$ and K is complex, L will be tame over K as long as 2 doesn't ramify in L. A prime of K ramifies in L if and only if it divides $d(L/K)$. Therefore, for tameness, we require $(d(L/K), 2\mathcal{O}_K) = \mathcal{O}_K$.

Now $4l\mathcal{O}_K \subseteq d(L/K) \subseteq l\mathcal{O}_K$, and so L/K is tame if and only if $d(L/K) = l\mathcal{O}_K$ and $(l\mathcal{O}_K, 2\mathcal{O}_K) = \mathcal{O}_K$.

If $d(L/K) = l\mathcal{O}_K$, then there must be an integer x in $\mathcal{O}_L$ of the form $x = (r+s\beta)/2$ where $r, s \in (\mathcal{O}_K/2\mathcal{O}_K)^\times$. Taking the norm of x from L to K gives

$$r^2 - s^2 l \equiv 0 \bmod (4\mathcal{O}_K),$$

and therefore

$$l \equiv (r/s)^2 \bmod (4\mathcal{O}_K).$$

Let $l \equiv a^2 \bmod (4\mathcal{O}_K)$ where $a \in (\mathcal{O}_K/2\mathcal{O}_K)^\times$. Then $\theta = (a+\beta)/2$ is an integer in $\mathcal{O}_L$, and $\mathcal{O}_L = \langle 1, \theta \rangle_{\mathcal{O}_K}$. Let us assume that $\mathcal{O}_L$ is a free $\mathcal{O}_K G$-module with the element $r + s\theta \in \mathcal{O}_L$, $r, s \in \mathcal{O}_K$, generating a normal integral basis for L over K. Then

$$\begin{aligned} d(L/K) &= \Delta_{L/K}[g_1(r+s\theta), g_2(r+s\theta)]\mathcal{O}_K, \\ &= \det \begin{pmatrix} r+sa & -s \\ r & s \end{pmatrix}^2 \Delta_{L/K}[1, \theta]\mathcal{O}_K, \\ &= (2rs + s^2 a)^2 d(L/K), \end{aligned}$$

and therefore $2rs + s^2 a = u$ where $u \in \mathcal{O}_K^\times = \{\pm 1\}$. Since $2rs + s^2 a$ is divisible by s, $s \in \mathcal{O}_K^\times$. Therefore $s = \pm 1$ and $s^2 = 1$. The equation $2rs + s^2 a = u$ now gives $u - a \equiv 0 \bmod (2\mathcal{O}_K)$ which is soluble for u if and only if $a = 1$. So L has a normal integral basis over K if and only if $l \equiv 1 \bmod (4\mathcal{O}_K)$. If $l \equiv 1 \bmod (4\mathcal{O}_K)$, then the element $\theta = (1+\beta)/2$ generates one such basis. □

6. $R(\mathcal{O}_K G)$, p an odd prime

We now consider the case when p is an odd prime which is unramified in K. We make a further assumption that the index Q_M of $W_M E_{M^+}$ in E_M is 2. (By (3.9), there are infinitely many cases where this index is 2.)

Our main results in this section are:

(6.1)THEOREM. *If M has class number 1 and p is inert in K, then $R(\mathcal{O}_K G) \simeq$ Coker(j), where the map*

$$j : \mathcal{O}_M^\times \to \left(\frac{\mathcal{O}_M}{(1-\zeta_p)\mathcal{O}_M}\right)^\times$$

is induced by reduction mod $((1-\zeta_p)\mathcal{O}_M)$, and the class of $\mathcal{O}_L$ for a tame extension L of K with $Gal(L/K) \simeq G$ and discriminant $d(L/K) = l^{p-1}\mathcal{O}_K$, $l \in \mathcal{O}_K$, corresponds to the element $[x] \in$ Coker(j) where $x^2 \equiv l$ mod $(p\mathcal{O}_K)$.

(6.2) THEOREM. *If M has class number 1 and p splits in K, then $R(\mathcal{O}_K G) = 1$, that is, every tame extension L of K with $Gal(L/K) \simeq G$ has a normal integral basis.*

We will also prove the following results which are specific quadratic imaginary number fields which have class number 1.

(6.3) THEOREM. *If $p = 3$, then $R(\mathcal{O}_K G)$ is trivial if $K = \mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, or $\mathbb{Q}(\sqrt{-11})$, and $R(\mathcal{O}_K G)$ is cyclic of order 2 if $K = \mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-19})$, $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$, or $\mathbb{Q}(\sqrt{-163})$. In cases where $R(\mathcal{O}_K G)$ is non-trivial, a tame extension L of K with $Gal(L/K) \simeq G$ and discriminant $d(L/K) = l^2\mathcal{O}_K$ has a normal integral basis if and only if l mod $(3\mathcal{O}_K)$ lies in $(\mathbb{Z}/3\mathbb{Z})^\times$.*

(6.4) THEOREM. *If $p = 5$, then $R(\mathcal{O}_K G)$ is trivial if $K = \mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$, and $R(\mathcal{O}_K G)$ is cyclic of order 3 if $K = \mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{-7})$. If $K = \mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{-7})$, then a tame extension L of K with $Gal(L/K) \simeq G$ and discriminant $d(L/K) = l^4\mathcal{O}_K$ has a normal integral basis if and only if l mod $(5\mathcal{O}_K)$ lies in $(\mathbb{Z}/5\mathbb{Z})^\times$.*

We begin with a few preliminary calculations. Let us assume that M has class number 1. In the following this assumption will continuously be in effect unless it is

explicitly removed. A consequence of this assumption is that $Cl^0(\mathcal{O}_K G)$ is the entire kernel group $D(\mathcal{O}_K G)$. This follows from the exact sequence

$$1 \to D(\mathcal{O}_K G) \to Cl(\mathcal{O}_K G) \to Cl(\mathcal{O}_K) \times Cl(\mathcal{O}_M) \to 1.$$

The group $Cl(\mathcal{O}_M)$ is trivial and so $Cl^0(\mathcal{O}_K G) = D(\mathcal{O}_K G)$. By the proof of (2.1), the group $D(\mathcal{O}_K G)$ is given by

$$D(\mathcal{O}_K G) \simeq \text{Coker}(j),$$

where

$$j : \mathcal{O}_M^\times \to \left(\frac{\mathcal{O}_M}{(1-\zeta_p)\mathcal{O}_M}\right)^\times$$

is the map induced by reduction mod $((1-\zeta_p)\mathcal{O}_M)$. We will write an element of $\text{Coker}(j)$ as $[x]$ where $x \in M$ with x coprime to $1-\zeta_p$. Let $[x] \in \text{Coker}(j)$, then the element $(C(x))$ of $D(\mathcal{O}_K G)$ which corresponds to $[x]$ under the above isomorphism is described by the diagram:

$$\begin{array}{ccc} C(x) & \longrightarrow & \mathcal{O}_M \\ \downarrow & & \downarrow j_1 \\ \mathcal{O}_K & \xrightarrow{j_2} & \mathcal{O}_M/(1-\zeta_p)\mathcal{O}_M \end{array}$$

where j_1 is multiplication by x followed by reduction mod $((1-\zeta_p)\mathcal{O}_M)$ and j_2 is reduction mod $(p\mathcal{O}_K)$. We can write $C(x)$ as

$$C(x) = \{(a,b) \in \mathcal{O}_K \times \mathcal{O}_M \mid a \equiv xb \bmod ((1-\zeta_p)\mathcal{O}_M)\}.$$

The action of G on $C(x)$ is induced from the action on $KG \simeq K \times M$:

$$g(a,b) = (a, \zeta_p b).$$

The group $\Delta = \text{Aut}(G)$ acts on $D(\mathcal{O}_K G)$. For $\delta \in \Delta$ and $(C(x)) \in D(\mathcal{O}_K G)$, $[x] \in \text{Coker}(j)$, $(C(x))^\delta = (C(x)^\delta)$ where $C(x)^\delta$ is same as $C(x)$ as an abelian group, but the G-action on $C(x)^\delta$ is defined as $g(a,b)^\delta = (\delta(g)(a,b))^\delta$.

(6.5) LEMMA. *$D(\mathcal{O}_K G)$ is a trivial Δ-module.*

Proof. We need to show that, for $\delta_i \in \Delta$ and $(C(x)) \in D(\mathcal{O}_K G)$, $C(x)^{\delta_i}$ is isomorphic to $C(x)$.

Since $\Delta \simeq Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, elements of Δ act on ζ_p by $\delta_i(\zeta_p) = \zeta_p^i$. As a result, Δ acts on $\mathcal{O}_M$. Define

$$\begin{aligned} f : C(x)^{\delta_i} &\longrightarrow C(x), \\ (a,b)^{\delta_i} &\mapsto (a, {\delta_i}^{-1}(b)). \end{aligned}$$

For $b \in \mathcal{O}_M$, we obtain ${\delta_i}^{-1}(b)$ from b by replacing ζ_p by an appropriate conjugate of ζ_p. Therefore, on reduction mod $((1-\zeta_p)\mathcal{O}_M)$, $b \equiv {\delta_i}^{-1}(b)$. So the image of f lies in $C(x)$. The map f clearly is an isomorphism of abelian groups. It also respects the action of G as the following shows.

$$\begin{aligned} f(g(a,b)^{\delta_i}) &= f((g^i(a,b))^{\delta_i}), \\ &= f((a,\zeta_p^i b)^{\delta_i}), \\ &= (a, {\delta_i}^{-1}(\zeta_p^i b)), \\ &= (a, \zeta_p {\delta_i}^{-1}(b)), \\ &= gf(a,b)^{\delta_i}. \end{aligned}$$

The map f is therefore an $\mathcal{O}_K G$-isomorphism. □

A consequence of the above lemma is that for $a \in \mathbb{Z}\Delta$ and $(C(x)) \in D(\mathcal{O}_K G)$,

$$C(x)^a \simeq C(x)^{\varepsilon(a)},$$

where $\varepsilon : \mathbb{Z}\Delta \to \mathbb{Z}$ is the augmentation map.

We are now set to calculate $R(\mathcal{O}_K G)$, the group of realizable classes in $Cl(\mathcal{O}_K G)$.

(6.6) THEOREM.

$$R(\mathcal{O}_K G) = \begin{cases} D(\mathcal{O}_K G), & \text{if } p \text{ is inert in } K, \\ 1, & \text{if } p \text{ splits in } K. \end{cases}$$

Proof. The group $R(\mathcal{O}_K G)$ is given by

$$R(\mathcal{O}_K G) = D(\mathcal{O}_K G)^J,$$

where $J = \mathbb{Z}\Delta \cap (\theta'/p)\mathbb{Z}\Delta$ is the Stickelberger ideal and $\theta' = \sum_{a=1}^{p-1} a\delta_a^{-1}$, of course, is the Stickelberger element. Since the action of Δ on $D(\mathcal{O}_K G)$ is trivial,

$$\begin{aligned} R(\mathcal{O}_K G) &= D(\mathcal{O}_K G)^J, \\ &= D(\mathcal{O}_K G)^{\varepsilon(J)}, \\ &= D(\mathcal{O}_K G)^{(p-1)/2}, \end{aligned}$$

where we have used the fact that $\varepsilon(J) = ((p-1)/2)\mathbb{Z}$. By (2.2), the order of $D(\mathcal{O}_K G)$ divides $(p+1)/Q_M$ if p is inert in K or it divides $(p-1)/Q_M$ if p splits in K. Q_M, of

course, is the index of $W_M E_{M^+}$ in E_M which we are assuming to be 2. So the order of $D(\mathcal{O}_K G)$ divides $(p+1)/2$ if p is inert in K or it divides $(p-1)/2$ if p splits in K. Since $(p+1)/2$ and $(p-1)/2$ are relatively coprime, we obtain

$$D(\mathcal{O}_K G)^{(p-1)/2} = \begin{cases} D(\mathcal{O}_K G), & \text{if } p \text{ is inert in } K, \\ 1, & \text{if } p \text{ splits in } K. \end{cases}$$

□

Proof of (6.2). Immediate from the above theorem. □

Having calculated $R(\mathcal{O}_K G)$ we can now proceed with the business of identifying the class of $\mathcal{O}_L$ in $R(\mathcal{O}_K G)$ where L is a tame extension of K with $Gal(L/K) \simeq G$. Since, by (6.2), there is not anything further to prove in the case when p splits in K, we only need to consider the case when p is inert in K.

Let $\theta \in \mathcal{O}_L$ be an element which generates a normal basis for L over K, that is, an element whose conjugates form a basis for L as a vector space over K:

$$L = \langle g_1(\theta), \ldots, g_p(\theta) \rangle_K.$$

We can assume that $\mathrm{tr}_{L/K}(\theta) = 1$. The element θ sets up an isomorphism between the KG-modules L and KG:

$$\begin{aligned} \phi : L &\to KG, \\ x &\mapsto \phi(x), \end{aligned}$$

where $\phi(x)(\theta) = x$. The map ϕ allows us to embed $\mathcal{O}_L$ in KG. The K-algebra KG splits as $K \times M$. Let π_1 be the projection of KG into the first factor, and π_2 into the second. We take the action of (π_1, π_2) on KG to be

$$(\pi_1, \pi_2)(g) = (1, \zeta_p)\ .$$

The combined map $(\pi_1, \pi_2)\phi$ induces an injective $\mathcal{O}_K G$-homomorphism:

$$(\pi_1, \pi_2)\phi : \mathcal{O}_L \to K \times M.$$

Because of our choice of θ, the map $\pi_1\phi : \mathcal{O}_L \to K$ is the ordinary trace map from L to K. Therefore $\pi_1\phi(\mathcal{O}_L) \subseteq \mathcal{O}_K$. Since L/K is tame, there exists in $\mathcal{O}_L$ an element of trace 1 and, consequently, $\pi_1\phi(\mathcal{O}_L) = \mathcal{O}_K$. The image of $\mathcal{O}_L$ under $\pi_2\phi$ will not in general be $\mathcal{O}_M$. It will be a fractional ideal of $\mathcal{O}_M$. Because of our assumption that $Cl(\mathcal{O}_M) = 1$, $\pi_2\phi(\mathcal{O}_L)$ will be a principal fractional ideal. Let $\pi_2\phi(\mathcal{O}_L) = y\mathcal{O}_M$ with $y \in M$. The element y uniquely determines the class of $\mathcal{O}_L$ in $R(\mathcal{O}_K G)$ as the following theorem shows.

(6.7) THEOREM. *The class of $\mathcal{O}_L$ in $R(\mathcal{O}_K G)$ is $(C(y))$.*

Proof. Let $y^{-1}\pi_2\phi : \mathcal{O}_L \to \mathcal{O}_M$ be the homomorphism obtained by combining $\pi_2\phi$ with multiplication by y^{-1}. Then $y^{-1}\pi_2\phi$ is a surjective $\mathcal{O}_K G$-homomorphism. The map $\pi_1\phi : \mathcal{O}_L \to \mathcal{O}_K$ is also a surjective $\mathcal{O}_K G$-homomorphism into $\mathcal{O}_K$. We can use these maps to construct a square of $\mathcal{O}_K G$-modules:

$$\begin{array}{ccc} \mathcal{O}_L & \xrightarrow{y^{-1}\pi_2\phi} & \mathcal{O}_M \\ \downarrow{\scriptstyle \pi_1\phi} & & \downarrow{\scriptstyle j_1} \\ \mathcal{O}_K & \xrightarrow{j_2} & \mathcal{O}_M/(1-\zeta_p)\mathcal{O}_M \end{array} \tag{6.8}$$

where j_1 is multiplication by y followed by reduction mod $((1-\zeta_p)\mathcal{O}_M)$ and j_2 is reduction mod $(p\mathcal{O}_K)$. The above square is commutative. To show this, let $x \in \mathcal{O}_L$. Then

$$\phi(x) = x_1 g_1 + \cdots + x_p g_p, \qquad x_i \in K,$$

and

$$\begin{aligned} \pi_1\phi(x) &= x_1 + \cdots + x_p, \\ \pi_2\phi(x) &= x_1\zeta_p + \cdots + x_p\zeta_p^p. \end{aligned}$$

Reducing $\pi_2\phi(x)$ mod $((1-\zeta_p)\mathcal{O}_M)$ gives $x_1 + \cdots + x_p$ mod $(p\mathcal{O}_K)$ which is same as $\pi_1\phi(x)$ mod $(p\mathcal{O}_K)$.

Since $\mathcal{O}_M/(1-\zeta_p)\mathcal{O}_M \simeq \mathcal{O}_K/p\mathcal{O}_K$, the map j_2 is surjective, and, as the square is commutative, j_1 is also surjective. As $(\pi_1, y^{-1}\pi_2)\phi : \mathcal{O}_L \to \mathcal{O}_K \times \mathcal{O}_M$ is injective, (6.8) is cartesian. The square (6.8) is exactly how we had previously defined $C(y)$. Therefore $\mathcal{O}_L \simeq C(y)$, and $(\mathcal{O}_L) = (C(y))$. □

The above theorem shows that in order to determine the class of $\mathcal{O}_L$ in $R(\mathcal{O}_K G)$ we need to calculate the element $y \in M$ which generates $\pi_2\phi(\mathcal{O}_L)$ over $\mathcal{O}_M$. Actually, it is the coset of y in

$$\mathrm{Coker}(j) \simeq \frac{(\mathcal{O}_M/(1-\zeta_p)\mathcal{O}_M)^\times}{j(\mathcal{O}_M^\times)}$$

that we need to calculate, for the class $(C(y))$ of $\mathcal{O}_L$ depends on $[y]$ rather than y. It is proper that the class of $\mathcal{O}_L$ should depend on $[y]$ instead of y. The value of y depends on our choice of θ used to define the isomorphism $\phi : L \to KG$, and, as there is not any canonical way of defining this isomorphism, there is not any unique value for y. In the following we will see that different values of θ may lead to different values of y but they all define the same coset in $\mathrm{Coker}(j)$. This is consistent with the

fact that the class of $\mathcal{O}_L$ in $R(\mathcal{O}_K G)$ is independent of how we choose to represent the isomorphism $L \simeq KG$.

We begin our calculation of $[y]$ by computing the discriminant $d(L/K)$ of L over K. The discriminant $d(L/K)$, we will see below, is central to the calculation of $[y]$.

(6.9) LEMMA. *The discriminant $d(L/K)$ is a $(p-1)$th power of an ideal of $\mathcal{O}_K$, i.e., $d(L/K) = H^{p-1}$ where H is an ideal of $\mathcal{O}_K$.*

Proof. Let $\mathcal{D}(L/K)$ be the different. Then, since L/K is tame and the ramification index of any prime which ramifies in L is p, we have

$$\mathcal{D}(L/K) = \prod_Q Q^{p-1}.$$

The product is over the primes which ramify. The discrminant is

$$\begin{aligned} d(L/K) &= \mathrm{norm}_{L/K}(\mathcal{D}(L/K)), \\ &= \prod_Q \mathrm{norm}_{L/K}(Q)^{p-1}. \end{aligned}$$

Since $\mathrm{norm}_{L/K}(Q)$, for each Q, is an ideal of $\mathcal{O}_K$, the discriminant $d(L/K)$ is a $(p-1)$th power of the product of prime ideals of $\mathcal{O}_K$ which ramify in L. □

The product of prime ideals of $\mathcal{O}_K$ which ramify in L will not in general be a principal ideal. For cases where it is, we have the following result.

(6.10) LEMMA. *If $d(L/K) = l^{p-1}\mathcal{O}_K$, $l \in \mathcal{O}_K$, then l is a square in $(\mathcal{O}_K/p\mathcal{O}_K)^\times$, i.e., the congruence*

$$l \equiv k^2 \ mod \ (p\mathcal{O}_K)$$

is soluble for $k \in (\mathcal{O}_K/p\mathcal{O}_K)^\times$.

Proof. Let P be a prime of K which divides $l\mathcal{O}_K$. Let Q be the prime of L lying above P, and K_P and L_Q denote the completions at the indicated primes. Then $P\mathcal{O}_L = Q^p$ and $Gal(L_Q/K_P) \simeq G$. The local Artin map $K_P^\times \to Gal(L_Q/K_P)$, induces an isomorphism

$$\frac{E_P}{\mathrm{norm}_{Q/P}(E_Q)} \simeq Gal(L_Q/K_P),$$

where E_P and E_Q, respectively, are groups of units in K_P and L_Q, and $\mathrm{norm}_{Q/P}$ is the norm mapping from L_Q to K_P. Since L/K is tame, the subgroup E_P^1 of E_P

consisting of units congruent to 1 mod $(P\mathcal{O}_P)$ lies in $\mathrm{norm}_{Q/P}(E_Q)$ (see [2]) and consequently the order of $Gal(L_Q/K_P)$ divides the order of E_P/E_P^1. The order of $Gal(L_Q/K_P)$ is p. To find the order of E_P/E_P^1 we note that

$$\frac{E_P}{E_P^1} \simeq \left(\frac{\mathcal{O}_P}{P\mathcal{O}_P}\right)^\times \simeq \left(\frac{\mathcal{O}_K}{P}\right)^\times.$$

The order of the group $(\mathcal{O}_K/P)^\times$ is $\mathrm{norm}_K(P) - 1$. Hence $\mathrm{norm}_K(P) \equiv 1 \bmod (p)$. Since norm_K is multiplicative, $\mathrm{norm}_K(l) \equiv 1 \bmod (p)$. So l lies in the kernel of the map

$$\left(\frac{\mathcal{O}_K}{p\mathcal{O}_K}\right)^\times \to \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times$$

induced by $\mathrm{norm}_K : \mathcal{O}_K \to \mathbb{Z}$. Since p is inert in K, $(\mathcal{O}_K/p\mathcal{O}_K)^\times$ is a cyclic group of order $p^2 - 1$. The kernel of the above map is $((\mathcal{O}_K/p\mathcal{O}_K)^\times)^{p-1}$. So l, in fact, is not just a square but a $(p-1)$th power in $(\mathcal{O}_K/p\mathcal{O}_K)^\times$. □

Next We define an object $\det_\theta(\mathcal{O}_L)$ which will link $[y]$ with the discriminant $d(L/K)$ of L over K.

Assume that the discriminant $d(L/K)$ has the form $l^{p-1}\mathcal{O}_K$. Then since $d(L/K)$ is principal, $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module (—in general, to determine the class of $\mathcal{O}_L$ in $Cl(\mathcal{O}_K)$, one has to consider the square root of the discriminant $d(L/K)$ but in our case, since $p-1$ is even, such considerations are irrelevant). Let us fix an $\mathcal{O}_K$-basis for $\mathcal{O}_L$:

$$\mathcal{O}_L = \langle e_1, \ldots, e_p \rangle_{\mathcal{O}_K}.$$

The image of $\mathcal{O}_L$ under ϕ can be written as

$$\phi(\mathcal{O}_L) = \langle \phi(e_1), \ldots, \phi(e_p) \rangle_{\mathcal{O}_K},$$

where

$$\phi(e_i) = \sum_{j=1}^{p} E_{ij} g_j, \qquad E_{ij} \in K.$$

Define $\det_\theta(\mathcal{O}_L) = \det(E)$. The θ in $\det_\theta(\mathcal{O}_L)$ signifies $\det_\theta(\mathcal{O}_L)$'s dependence on the choice of θ.

(6.11) LEMMA.

$$\det_\theta(\mathcal{O}_L) \equiv u k^{p-1} \ mod\ (p\mathcal{O}_K),$$

where $u \in \mathcal{O}_K^\times$ *and* $k^2 \equiv l \ mod\ (p\mathcal{O}_K)$.

Proof. Let $A_{ij} = g_i(e_j)$ and $B_{ij} = g_i(g_j(\theta))$. Then, since

$$\begin{aligned} A_{ij} &= g_i\left(\sum_{k=1}^{p} E_{jk} g_k(\theta)\right), \\ &= \sum_{k=1}^{p} E_{jk} g_k(g_i(\theta)), \\ &= \sum_{k=1}^{p} E_{jk} B_{ki}, \\ &= (EB)^T_{ij}, \end{aligned}$$

where $(EB)^T$ denotes the transpose of the matrix EB, $A = (EB)^T$ and therefore $\det(A) = \det(E)\det(B)$. But $\det(E) = \det_\theta(\mathcal{O}_L)$. Hence

$$\det(A) = \det_\theta(\mathcal{O}_L)\det(B). \tag{6.12}$$

Now $\det(A) \in \mathcal{O}_K$. To prove this, we note that $\det(A) \in \mathcal{O}_L$ and $g(\det(A)) = \det(g(A))$ where $g(A) = (g(A_{ij}))$. By interchanging rows in $g(A)$ we can transform $g(A)$ to A. The number of interchanges required is $p-1$ and therefore $\det(g(A)) = (-1)^{p-1}\det(A) = \det(A)$. So the element $\det(A) \in \mathcal{O}_L$ is fixed under G and therefore it lies in $\mathcal{O}_K$.

The discriminant of the basis e_i, $1 \le i \le p$, is

$$\begin{aligned} \Delta_{L/K}[e_1, \ldots, e_p] &= \det(g_i(e_j))^2, \\ &= \det(A)^2. \end{aligned}$$

But $d(L/K) = \Delta_{L/K}[e_1, \ldots, e_p]\mathcal{O}_K = l^{p-1}\mathcal{O}_K$. Therefore $\det(A) = vl^{(p-1)/2}$ where $v \in \mathcal{O}_K^\times$, or $\det(A) \equiv vk^{p-1} \bmod (p\mathcal{O}_K)$ where $k^2 \equiv l \bmod (p\mathcal{O}_K)$.

The determinant of the matrix B, on reduction mod $(p\mathcal{O}_K)$, gives

$$\begin{aligned} \det(B) &\equiv (-1)^{(p-1)/2}(g_1(\theta) + \cdots + g_p(\theta))^p \bmod (p\mathcal{O}_K), \\ &\equiv (-1)^{(p-1)/2}\mathrm{tr}_{L/K}(\theta)^p \bmod (p\mathcal{O}_K), \\ &\equiv (-1)^{(p-1)/2} \bmod (p\mathcal{O}_K), \end{aligned}$$

since $\mathrm{tr}_{L/K}(\theta) = 1$.

Returning to (6.12), we find

$$vk^{p-1} \equiv (-1)^{(p-1)/2}\det_\theta(\mathcal{O}_L) \bmod (p\mathcal{O}_K),$$

or $\det_\theta(\mathcal{O}_L) \equiv uk^{p-1} \bmod (p\mathcal{O}_K)$ as required. □

Having related $\det_\theta(\mathcal{O}_L)$ to $d(L/K)$, we now relate it to y where $\pi_2\phi(\mathcal{O}_L) = y\mathcal{O}_M$.

(6.13) LEMMA.

$$\det_\theta(\mathcal{O}_L) \equiv uy^{p-1} \bmod ((1-\zeta_p)\mathcal{O}_M), \qquad u \in \mathcal{O}_K^\times.$$

Proof. The image of $\phi(\mathcal{O}_L)$ under (π_1, π_2) is

$$(\pi_1, \pi_2)(\phi(\mathcal{O}_L)) = \{(a, b) \in \mathcal{O}_K \times y\mathcal{O}_M \mid a \equiv b \bmod ((1-\zeta_p)\mathcal{O}_M)\}.$$

Let $x \in \mathcal{O}_K$ be such that $x \equiv y \bmod ((1-\zeta_p)\mathcal{O}_M)$. Then

$$(\pi_1, \pi_2)(\phi(\mathcal{O}_L)) = \langle (x, y\zeta_p), \ldots, (x, y\zeta_p^{p-1}), (p, 0)\rangle_{\mathcal{O}_K},$$

and

$$\phi(\mathcal{O}_L) = (\pi_1, \pi_2)^{-1}\langle (x, y\zeta_p), \ldots, (x, y\zeta_p^{p-1}), (p, 0)\rangle_{\mathcal{O}_K}.$$

But

$$(\pi_1, \pi_2)^{-1}\langle (x, y\zeta_p), \ldots, (x, y\zeta_p^{p-1}), (p, 0)\rangle_{\mathcal{O}_K} = \langle f_1, \ldots, f_p\rangle_{\mathcal{O}_K},$$

where

$$f_i = \sum_{j=1}^{p} F_{ij} g_j, \qquad F_{ij} \in K,$$

and

$$\sum_{j=1}^{p} F_{ij} = x, \qquad 1 \le i \le p-1,$$

$$\sum_{j=1}^{p} F_{ij}\zeta_p^j = y\zeta_p^i, \qquad 1 \le i \le p-1,$$

$$F_{pj} = 1, \quad 1 \le j \le p.$$

But previously we had $\phi(\mathcal{O}_L) = \langle \phi(e_1), \ldots, \phi(e_p)\rangle_{\mathcal{O}_K}$, where $\phi(e_i) = \sum_{j=1}^{p} E_{ij} g_j$, $E_{ij} \in K$. Therefore

$$E_{ik} = \sum_{j=1}^{p} T_{ij} F_{jk},$$

where $T_{ij} \in \mathcal{O}_K$ with $\det(T) \in \mathcal{O}_K^\times$, and $\det_\theta(\mathcal{O}_L) = \det(E) = v\det(F)$, $v \in \mathcal{O}_K^\times$.

In the matrix (F_{ij}), if we subtract the pth column from the ith for all $1 \leq i \leq p-1$ and denote the resulting matrix by (F'_{ij}), then $\det(F)$ is unchanged by the operation $(F_{ij}) \rightarrow (F'_{ij})$, and so $\det(F) = \det(F')$. But $\det(F') = \det(F'')$ where $F''_{ij} = F_{ij} - F_{ip}$ is a $p-1 \times p-1$ matrix. For $1 \leq i \leq p-1$,

$$\begin{aligned}\sum_{j=1}^{p-1} F''_{ij}\zeta_p^j &= \sum_{j=1}^{p-1}(F_{ij} - F_{ip})\zeta_p^j, \\ &= \sum_{j=1}^{p-1} F_{ij}\zeta_p^j + F_{ip}\zeta_p^p, \\ &= y\zeta_p^i,\end{aligned}$$

and so, for $1 \leq i \leq p-1$, the elements $\sum_{j=1}^{p-1} F''_{ij}\zeta_p^j$ generate $y\mathcal{O}_M$ over $\mathcal{O}_K$. As a result,

$$\det(F''_{ij}) = w\mathrm{norm}_{M/K}(y), \qquad w \in \mathcal{O}_K^\times.$$

We therefore have $\det_\theta(\mathcal{O}_L) = vw\mathrm{norm}_{M/K}(y)$, or

$$\det_\theta(\mathcal{O}_L) \equiv vwy^{p-1} \bmod ((1-\zeta_p)\mathcal{O}_M).$$

□

We are now in a position to prove (6.1).

Proof of (6.1). We have already proved in our earlier discussions that if p is inert in K then $R(\mathcal{O}_K G) \simeq \mathrm{Coker}(j)$ where $j : \mathcal{O}_M^\times \rightarrow (\mathcal{O}_M/(1-\zeta_p)\mathcal{O}_M)^\times$. It only remains to identify the class of $\mathcal{O}_L$ in $R(\mathcal{O}_K G)$.

By (6.7), the class of $\mathcal{O}_L$ is $(C(y))$ where $[y] \in \mathrm{Coker}(j)$ and, by (6.11) and (6.13),

$$y^{p-1} \equiv uk^{p-1} \bmod ((1-\zeta_p)\mathcal{O}_M),$$

where $u \in \mathcal{O}_K^\times$, $k^2 \equiv l \bmod (p\mathcal{O}_K)$, and $d(L/K) = l^{p-1}\mathcal{O}_K$ is the discriminant. Since p is inert in K, the group $(\mathcal{O}_M/(1-\zeta_p)\mathcal{O}_M)^\times$ which is isomorphic to $(\mathcal{O}_K/p\mathcal{O}_K)^\times$ is cyclic of order p^2-1. Let z be a generator of $(\mathcal{O}_M/(1-\zeta_p)\mathcal{O}_M)^\times$. The subgroup of $(\mathcal{O}_M/(1-\zeta_p)\mathcal{O}_M)^\times$ generated by $\mathcal{O}_K^\times$ is $\langle z^{(p^2-1)/t}\rangle$ where t is 4 if $K = \mathbb{Q}(\sqrt{-1})$, 6 if $K = \mathbb{Q}(\sqrt{-3})$, or 2 if $K \neq \mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-3})$. If we let $y/k = z^x$ then the above congruence can be written as

$$z^{x(p-1)} \equiv z^{a(p^2-1)/t} \bmod ((1-\zeta_p)\mathcal{O}_M),$$

where $1 \leq a \leq t$. This implies $x(p-1) \equiv a(p^2-1)/t \bmod (p^2-1)$. Since the image of $j : \mathcal{O}_M^\times \rightarrow (\mathcal{O}_M/(1-\zeta_p)\mathcal{O}_M)^\times$ is generated by $z^{(p+1)/t}$, it follows that $p+1 \equiv$

0 mod (t). We therefore have $x \equiv a(p+1)/t \bmod (p+1)$, or $x = a(p+1)/t + b(p+1)$, $b \in \mathbb{Z}$. Hence $y = z^{a(p+1)/t} z^{b(p+1)} k$. The elements $z^{a(p+1)/t}$ and $z^{b(p+1)}$ lie in $j(\mathcal{O}_M^\times)$. Therefore, in $\mathrm{Coker}(j)$, $[y] = [k]$. □

Although theorem (6.1) can be used to determine the class of $\mathcal{O}_L$ for a tame extension L of K with $Gal(L/K) \simeq G$ and $d(L/K) = l^{p-1}\mathcal{O}_K$, it does not, of course, establish the existence of such extensions. Next we prove a result which will show that there indeed exist extensions of K to which (6.1) is applicable.

In (6.9) and in the proof of (6.10) we saw that if L is a tame extension of K with $Gal(L/K) \simeq G$ then the discriminant $d(L/K)$ has the form H^{p-1} where $H = \prod_h h$ is the product of primes of K which ramify in L and, for each h, $\mathrm{norm}_K(h) \equiv 1 \bmod (p)$. We now consider the question whether for a given product $H = \prod_h h$ of primes of K with $\mathrm{norm}_K(h) \equiv 1 \bmod (p)$ for each h there exists a tame extension L of K with $Gal(L/K) \simeq G$ whose discriminant $d(L/K)$ is H^{p-1}. The following theorem answers this question in the case where only one single prime h of K is involved.

(6.14) THEOREM. *Let h be a prime of K with $\mathrm{norm}_K(h) \equiv 1$ mod (p). Then there is a unique tame extension L of K with $Gal(L/K) \simeq G$ and discriminant $d(L/K) = h^{p-1}$.*

Proof. The proof is a straightforward exercise in class field theory. Let I_h be the group of fractional ideals of $\mathcal{O}_K$ which are relatively prime to h. Let P_h denote the subgroup of I_h consisting of principal fractional ideals and let P_h^1 be the subgroup of P_h consisting of ideals which have generators congruent to 1 mod (h). Under the map induced by $P_h \to (\mathcal{O}_K/h)^\times$, $x\mathcal{O}_K \mapsto [x]$, P_h/P_h^1 is isomorphic to $(\mathcal{O}_K/h)^\times$ modulo the subgroup of $(\mathcal{O}_K/h)^\times$ generated by $\mathcal{O}_K^\times$. The order of $(\mathcal{O}_K/h)^\times$ is $\mathrm{norm}_K(h)-1$ which is divisible by p. The group $\mathcal{O}_K^\times$ is $\langle\zeta_4\rangle$ if $K = \mathbb{Q}(\sqrt{-1})$, $\langle\zeta_6\rangle$ if $K = \mathbb{Q}(\sqrt{-3})$, or $\langle -1\rangle$ otherwise. The order of the subgroup generated by $\mathcal{O}_K^\times$ is, therefore, relatively prime to p. Hence p divides the index $(P_h : P_h^1)$ and, consequently, p divides $(I_h : P_h^1)$. Let Q, $P_h^1 \subset Q \subset I_h$, be the unique subgroup whose index in I_h is p. Then the classfield of Q is the unique tame extension L of K with $Gal(L/K) \simeq G$ and $d(L/K) = h^{p-1}$ whose existence we are trying to prove. The Galois group of the class field over K is isomorphic to I_h/Q, the isomorphism being induced by the Artin map. The group I_h/Q is cyclic of order p and therefore isomorphic to G. □

The above theorem basically is a recipe for generating tame extensions L of K with $Gal(L/K) \simeq G$ and discriminant $d(L/K) = H^{p-1}$ where $H = \prod_h h$, $\mathrm{norm}_K(h) \equiv$

1 mod (p), is an arbitrary product of primes of K. Stating with a product $H = \prod_{i=1}^{n} h_i$, $\mathrm{norm}_K(h_i) \equiv 1 \bmod (p)$, of primes of K we denote by L_i the extension of K guaranteed by (6.14) which is ramified at h_i only. The compositum $\prod_{i=1}^{n} L_i$ then is a tame extension of K ramified at primes dividing H only with Galois group consisting of n copies of G. The field $\prod_{i=1}^{n} L_i$ has a whole series of subfields L which are tame over K with $Gal(L/K) \simeq G$ and $d(L/K) = H^{p-1}$. In fact any tame extension L of K with $Gal(L/K) \simeq G$ and $d(L/K) = H^{p-1}$ arises in this manner. If $H = l\mathcal{O}_K$ is principal then we have a whole string of tame extensions of K to which (6.1) can be applied.

Next we prepare the ground for proving (6.3) and (6.4). We assume K is a quadratic imaginary number field with class number 1. The values of d are now restricted to $1, 2, 3, 7, 11, 19, 43, 67$, and 163.

(6.15) THEOREM. *If $p = 3$, then $Cl(\mathcal{O}_M) = 1$ for all K. If $p = 5$, then $Cl(\mathcal{O}_M) = 1$ for $K = \mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$, and $\mathbb{Q}(\sqrt{-7})$.*

Proof. Let h_M be the class number of M and h_{M^+} the class number of M^+. Then, by [16], theorem (4.17),

$$\frac{h_M}{h_{M^+}} = Q_M |W_M| \prod_{\varphi \text{ odd}} \left(-\frac{1}{2} B_\varphi\right), \tag{6.16}$$

where the product is over odd Dirichlet characters of M, Q_M is the index of $W_M E_{M^+}$ in E_M, and, for a character φ with conductor f_φ,

$$B_\varphi = \frac{1}{f_\varphi} \sum_a \varphi(a) a,$$

where the sum is over the elements of $(\mathbb{Z}/f_\varphi\mathbb{Z})^\times$.

Let us first calculate the index Q_M. From (2.10) we have $Q_M = 2$ for $K = \mathbb{Q}(\sqrt{-1})$ and $K = \mathbb{Q}(\sqrt{-3})$. If $K = \mathbb{Q}(\sqrt{-2})$, then the element $1 - \zeta_8\zeta_p$ is a unit in $\mathbb{Q}(\zeta_8, \zeta_p)$. Taking the norm of $1 - \zeta_8\zeta_p$ from $\mathbb{Q}(\zeta_8, \zeta_p)$ to $M = \mathbb{Q}(\sqrt{-2}, \zeta_p)$ gives

$$u = (1 - \zeta_8\zeta_p)(1 - \zeta_8^3\zeta_p) \in E_M,$$

and $u/u^c = -\zeta_p^2 \notin W_M^2$. Hence, by (2.9), $Q_M = 2$.

For the rest of K's, M has the form $\mathbb{Q}(\sqrt{-q}, \zeta_p)$ where q is a prime congruent to 3 mod (4). By (3.9), we at once obtain $Q_M = 2$ for these fields.

Let $p = 3$. Then $M = K(\zeta_3)$. If $K = \mathbb{Q}(\sqrt{-3})$, then $M = K(\zeta_3) = \mathbb{Q}(\sqrt{-3})$, and the class number of M is 1 (M is one of the quadratic imaginary number fields with class number 1).

Assume K is a field other than $\mathbb{Q}(\sqrt{-3})$. The group W_M of roots of unity in M is

$$W_M = \begin{cases} \langle \zeta_4, \zeta_3 \rangle, & \text{if } K = \mathbb{Q}(\sqrt{-1}), \\ \langle -1, \zeta_3 \rangle, & \text{otherwise,} \end{cases}$$

and so $|W_M| = 12$ if $K = \mathbb{Q}(\sqrt{-1})$; 6 otherwise.

The character group $X(M)$ of M is a subgroup of the character group for $\mathbb{Q}(\zeta_D, \zeta_3)$ where D is the smallest positive integer such that $M \subseteq \mathbb{Q}(\zeta_D, \zeta_3)$ which is the same thing as the positive generator for the discriminant $d(K/\mathbb{Q})$. We have

$$X(M) = \langle \chi, \psi \mid \chi^2 = \psi^2 = 1 \rangle,$$

where χ is a character of $\mathbb{Q}(\zeta_D)$ and ψ is the non-trivial character of $\mathbb{Q}(\zeta_3)$. The action of ψ on $Gal(\mathbb{Q}(\zeta_3)/\mathbb{Q}) \simeq (\mathbb{Z}/3\mathbb{Z})^\times$ is clear; it sends the generator of $(\mathbb{Z}/3\mathbb{Z})^\times$ to -1. The action of χ on $Gal(\mathbb{Q}(\zeta_D)/\mathbb{Q}) \simeq (\mathbb{Z}/D\mathbb{Z})^\times$ depends on the value of D. If $K = \mathbb{Q}(\sqrt{-1})$, then $D = 4$ and $\chi(1) = 1$, $\chi(3) = -1$. If $K = \mathbb{Q}(\sqrt{-2})$, then $D = 8$ and $\chi(1) = \chi(3) = 1$, $\chi(5) = \chi(7) = -1$. For the rest of the K's, D is an odd prime and

$$\chi(a) = \left(\frac{a}{D}\right), \qquad a \in \left(\frac{\mathbb{Z}}{D\mathbb{Z}}\right)^\times.$$

To find the odd characters of M we recall that a character is odd if it sends -1, i.e. complex conjugation, to -1 (and even if it sends it to 1). Now χ is clearly odd if $K = \mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-2})$. For the other fields, D is a prime congruent to 3 mod (4), and therefore -1 is not a square mod D, and hence $\chi(-1) = -1$. So χ is an odd character for all K. The character ψ is also odd. The set of odd characters of M, therefore, consists of χ and ψ. The conductor of χ is D whereas it is 3 for ψ.

Now that we have the set of odd characters of M, computing B_φ for each odd character φ gives, for χ,

$$B_\chi = \begin{cases} -1/2, & \text{if } K = \mathbb{Q}(\sqrt{-1}), \\ -1, & \text{otherwise,} \end{cases}$$

and, for ψ, $B_\psi = -1/3$.

Evaluating the quotient in (6.16) now gives $h_M/h_{M^+} = 1$, or $h_M = h_{M^+}$. The field M^+ is a real quadratic number field. From the table given in [1] on the class

numbers of real quadratic number fields we get $h_{M^+} = 1$ for all M^+, and therefore $h_M = 1$ for all K.

Now assume $p = 5$. Then $M = K(\zeta_5)$. The group W_M of roots of unity in M is

$$W_M = \begin{cases} \langle \zeta_4, \zeta_5 \rangle, & \text{if } K = \mathbb{Q}(\sqrt{-1}), \\ \langle -1, \zeta_3, \zeta_5 \rangle, & \text{if } K = \mathbb{Q}(\sqrt{-3}), \\ \langle -1, \zeta_5 \rangle, & \text{otherwise.} \end{cases}$$

The order of W_M is 20 if $K = \mathbb{Q}(\sqrt{-1})$, 30 if $K = \mathbb{Q}(\sqrt{-3})$, and 10 otherwise.

The character group $X(M)$ is given by

$$X(M) = \langle \chi, \psi \mid \chi^2 = \psi^4 = 1 \rangle,$$

where χ is a character of $\mathbb{Q}(\zeta_D)$ which is defined in the same way as in the $p = 3$ case and ψ generates the character group for $\mathbb{Q}(\zeta_5)$. We define the action of ψ on $Gal(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \simeq (\mathbb{Z}/5\mathbb{Z})^\times$ as $\psi(2) = \zeta_4$. Since 2 generates $(\mathbb{Z}/5\mathbb{Z})^\times$, the action of ψ on the other elements of $(\mathbb{Z}/5\mathbb{Z})^\times$ can be obtained from the action of ψ on 2.

The set of odd characters of M consists of χ, $\chi\psi^2$, ψ^3, and ψ. The conductors are: $f_\chi = D$, $f_{\chi\psi^2} = 5D$, $f_{\psi^3} = 5$, $f_\psi = 5$. Calculating B_φ for each odd character φ gives

$$B_\chi = \begin{cases} -1/2, & \text{if } K = \mathbb{Q}(\sqrt{-1}), \\ -1/3, & \text{if } K = \mathbb{Q}(\sqrt{-3}), \\ -1, & \text{otherwise,} \end{cases}$$

$$B_{\chi\psi^2} = \begin{cases} -2, & \text{if } K = \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3}), \text{ or } \mathbb{Q}(\sqrt{-7}), \\ -4, & \text{if } K = \mathbb{Q}(\sqrt{-11}), \\ -8, & \text{if } K = \mathbb{Q}(\sqrt{-19}), \\ -14, & \text{if } K = \mathbb{Q}(\sqrt{-43}), \\ -18, & \text{if } K = \mathbb{Q}(\sqrt{-67}), \\ -30, & \text{if } K = \mathbb{Q}(\sqrt{-163}), \end{cases}$$

$$B_{\psi^3} = -\frac{1}{5}(3 - \zeta_4),$$

$$B_\psi = -\frac{1}{5}(3 + \zeta_4).$$

Substituting for Q_M, $|W_M|$, and B_φ in (6.16) gives

$$\frac{h_M}{h_{M^+}} = \begin{cases} 1, & \text{if } K = \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3}), \text{ or } \mathbb{Q}(\sqrt{-7}), \\ 2, & \text{if } K = \mathbb{Q}(\sqrt{-11}), \\ 4, & \text{if } K = \mathbb{Q}(\sqrt{-19}), \\ 7, & \text{if } K = \mathbb{Q}(\sqrt{-43}), \\ 9, & \text{if } K = \mathbb{Q}(\sqrt{-67}), \\ 15, & \text{if } K = \mathbb{Q}(\sqrt{-163}), \end{cases}$$

which shows that, for $K = \mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$, and $\mathbb{Q}(\sqrt{-7})$, $h_M = h_{M^+}$, and, since h_{M^+} is an integer, $h_M > 1$ for $K = \mathbb{Q}(\sqrt{-11})$, $\mathbb{Q}(\sqrt{-19})$, $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$, and $\mathbb{Q}(\sqrt{-163})$.

Next we show that, for $K = \mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$, and $\mathbb{Q}(\sqrt{-7})$, $h_{M^+} = 1$. We use Minkowski bound method for calculating h_{M^+}.

If we write K as $\mathbb{Q}(\sqrt{-d})$ then M^+ can be written as $\mathbb{Q}(\beta, \gamma)$ where $\beta = (1 + \sqrt{5})/2$, and $\gamma = \sqrt{d(\beta+2)}$ if $d \not\equiv 3 \bmod (4)$ or $\gamma = (1 + \beta + \sqrt{d(\beta+2)})/2$ if $d \equiv 3 \bmod (4)$. The ring of integers in M^+ is

$$\mathcal{O}_{M^+} = \langle 1, \beta, \gamma, \beta\gamma \rangle_{\mathbb{Z}}.$$

The discriminant $d(M^+/\mathbb{Q})$ of M^+ over $\mathbb{Q}$ is $5^3 d(K/\mathbb{Q})^2$.

If $K = \mathbb{Q}(\sqrt{-1})$, then $d(M^+/\mathbb{Q}) = 2^4 5^3 \mathbb{Z}$ and the Minkowski bound for M^+ is 4. The rational prime 2 is inert in $\mathbb{Q}(\beta)$ but it ramifies in M^+. The prime of M^+ lying above 2 is generated by $1 + \beta + \gamma$ and therefore is principal. The prime 3 is inert in $\mathbb{Q}(\beta)$, so there is no ideal of norm 3. Every ideal with norm ≤ 4 is principal; M^+ has class number 1.

If $K = \mathbb{Q}(\sqrt{-2})$, then $d(M^+/\mathbb{Q}) = 2^6 5^3 \mathbb{Z}$ and the Minkowski bound for M^+ is 8. There is only one prime ideal of M^+ lying above 2 and it is generated by $2 + \gamma$. As 3 is inert in $\mathbb{Q}(\beta)$, there is no ideal of norm 3. The prime 5 ramifies in $\mathbb{Q}(\beta)$ and it ramifies further in M^+. The prime of M^+ lying above 5 is generated by $1 - 2\beta - \gamma$. The prime 7 is inert in $\mathbb{Q}(\beta)$. The class number of M^+ is therefore 1.

If $K = \mathbb{Q}(\sqrt{-3})$, then $d(M^+/\mathbb{Q}) = 3^2 5^3 \mathbb{Z}$. The Minkowski bound for M^+ is 3. Both 2 and 3 are inert in $\mathbb{Q}(\beta)$. So there is no ideal of norm ≤ 3.

If $K = \mathbb{Q}(\sqrt{-7})$, then $d(M^+/\mathbb{Q}) = 7^2 5^3 \mathbb{Z}$ and the Minkowski bound for M^+ is 7. There is only one ideal with norm ≤ 7 and it is the one which lies above 5 and is generated by $1 - \beta\gamma$. The class number of M^+ is therefore 1.

So, for $K = \mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$, and $\mathbb{Q}(\sqrt{-7})$, $h_{M^+} = 1$. □

Proof of (6.3). If $K = \mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{-11})$, then 3 splits and therefore, for these fields, $R(\mathcal{O}_K G) = 1$. For the remaining fields 3 is inert and the order of $R(\mathcal{O}_K G)$ is 1 if $K = \mathbb{Q}(\sqrt{-1})$ or 2 otherwise.

Let K be a field such that $R(\mathcal{O}_K G)$ is non-trivial. Then, by (6.1), the class of $\mathcal{O}_L$ in $R(\mathcal{O}_K G)$ is trivial if and only if $x \in j(\mathcal{O}_M^\times)$ where $x^2 \equiv l \bmod (3\mathcal{O}_K)$. The group $(\mathcal{O}_K/3\mathcal{O}_K)^\times$ is generated by α. The image of $\mathcal{O}_M^\times$ under j is the subgroup of $(\mathcal{O}_K/3\mathcal{O}_K)^\times$ generated by α^2. Therefore $j(\mathcal{O}_M^\times)^2 = \langle \alpha^4 \rangle = \{\pm 1\}$. Hence L has a normal integral basis if and only if $l \equiv \pm 1 \bmod (3\mathcal{O}_K)$. □

Proof of (6.4). If $K = \mathbb{Q}(\sqrt{-1})$, then 5 splits and therefore $R(\mathcal{O}_K G) = 1$. If $K = \mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$ or $\mathbb{Q}(\sqrt{-7})$, then 5 is inert. The order of $R(\mathcal{O}_K G)$ is 1 if $K = \mathbb{Q}(\sqrt{-3})$ or 3 otherwise.

Let $K = \mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{-7})$. Then, by (6.1), the class of $\mathcal{O}_L$ in $R(\mathcal{O}_K G)$ is trivial if and only if $x \in j(\mathcal{O}_M^\times)$ where $x^2 \equiv l \bmod (5\mathcal{O}_K)$. If $K = \mathbb{Q}(\sqrt{-2})$, then $(\mathcal{O}_K/5\mathcal{O}_K)^\times = \langle \alpha + 1 \rangle$, $j(\mathcal{O}_M^\times) = \langle (\alpha+1)^3 \rangle = \langle \alpha \rangle$, and $j(\mathcal{O}_M^\times)^2 = \langle 3 \rangle$. Therefore L has a normal integral basis if and only if $l \bmod (5\mathcal{O}_K)$ lies in $(\mathbb{Z}/5\mathbb{Z})^\times$. If $K = \mathbb{Q}(\sqrt{-7})$, then we obtain $j(\mathcal{O}_M^\times)^2 = \langle 2 \rangle$ and so L has a normal integral basis if and only if $l \bmod (5\mathcal{O}_K) \in (\mathbb{Z}/5\mathbb{Z})^\times$. □

7. $R'(\mathcal{O}_K G)$ — a subgroup of $R(\mathcal{O}_K G)$

Let K be an imaginary quadratic number field with class number 1. In this section we consider the subgroup $R'(\mathcal{O}_K G)$ of $R(\mathcal{O}_K G)$ generated by classes of the form $(\mathcal{O}_L)$ where L is a tame Galois extension of K with $Gal(L/K)$ isomorphic to G which is also a Galois extension of $\mathbb{Q}$. As in the last section, we assume that p is unramified in K but, unlike the last section, we do not impose the condition $Cl(\mathcal{O}_M) = 1$.

Let L be a tame extension of K with $Gal(L/K) \simeq G$ which is also a Galois extension of $\mathbb{Q}$. The group $Gal(L/\mathbb{Q})$, then, is either cyclic or it is isomorphic to the dihedral group D_{2p} of order $2p$. Let us first consider the case when $Gal(L/\mathbb{Q})$ is cyclic. The group $Gal(L/\mathbb{Q})$ has a unique subgroup whose index in $Gal(L/\mathbb{Q})$ is 2; let F be the corresponding subfield of L. Then F is a tame Galois extension of $\mathbb{Q}$ with the Galois group $Gal(F/\mathbb{Q})$ isomorphic to G and $L = KF$.

(7.1) LEMMA. *If the discriminants $d(K/\mathbb{Q})$ and $d(F/\mathbb{Q})$ are relatively coprime, then L has a normal integral basis, i.e., the class of $\mathcal{O}_L$ in $R'(\mathcal{O}_K G)$ is trivial.*

Proof. Assume that the discriminants $d(K/\mathbb{Q})$ and $d(F/\mathbb{Q})$ are relatively coprime. Then, since $L = KF$, the ring $\mathcal{O}_L$ of integers in L is a compositum of the rings $\mathcal{O}_K$ and $\mathcal{O}_F$ of integers in K and F, i.e., $\mathcal{O}_L = \mathcal{O}_K \mathcal{O}_F$. Since F is a tame Galois extension of $\mathbb{Q}$ with $Gal(F/\mathbb{Q}) \simeq G$ which is abelian, by Taylor's proof [15] of Fröhlich's conjecture, F has a normal integral basis over $\mathbb{Q}$. This means that $\mathcal{O}_F \simeq \mathbb{Z}G$ and therefore $\mathcal{O}_L \simeq \mathcal{O}_K G$. The element of $\mathcal{O}_F$ which generates a normal integral basis for F over $\mathbb{Q}$ also generates a normal integral basis for L over K. □

Next, for each K, we identify cases where $d(K/\mathbb{Q})$ and $d(F/\mathbb{Q})$ can have a common factor. We will need the following lemma.

(7.2) LEMMA. *Let r be a prime integer which divides $d(F/\mathbb{Q})$. Then $r \equiv 1 \bmod (p)$.*

Proof. Let R be the prime of F which lies above $r\mathbb{Z}$. Let $\mathbb{Q}_r$ and F_R denote completions of $\mathbb{Q}$ and F at r and R respectively. Then $r\mathcal{O}_F = R^p$ and $Gal(F_R/\mathbb{Q}_r) \simeq G$. Since the inertia subgroup of $Gal(F_R/\mathbb{Q}_r)$ is the entire group $Gal(F_R/\mathbb{Q}_r)$, the local Artin map

$$\mathbb{Q}_r^{\times} \to Gal(F_R/\mathbb{Q}_r)$$

induces an isomorphism

$$\frac{E_r}{\mathrm{norm}_{R/r}(E_R)} \simeq Gal(F_R/\mathbb{Q}_r),$$

where E_r and E_R denote the groups of units in $\mathbb{Q}_r$ and F_R respectively, and $\mathrm{norm}_{R/r}$ is the norm mapping from F_R to $\mathbb{Q}_r$. Let $E_r^{(0)} = E_r$ and, for a positive integer a, $E_r^{(a)}$ be the subgroup of E_r consisting of units congruent to 1 mod $(r^a\mathcal{O}_r)$. Then, by the class field theory, we can find an integer a such that

$$E_r^{(a)} \subseteq \mathrm{norm}_{R/r}(E_R).$$

Let a be the smallest such integer. Then, since $E_r^{(0)}$ does not lie in $\mathrm{norm}_{R/r}(E_R)$, we can assume $a \geq 1$. Since $Gal(F_R/\mathbb{Q}_r)$ is cyclic whose order is a prime integer, under the local Artin map, $E_r^{(a-1)}$ will map onto $Gal(F_R/\mathbb{Q}_r)$ with $E_r^{(a)}$ lying in the kernel. Therefore the order of $Gal(F_R/\mathbb{Q}_r)$ divides the index of $E_r^{(a)}$ in $E_r^{(a-1)}$. If $a = 1$, then

$$\frac{E_r^{(0)}}{E_r^{(1)}} \simeq \left(\frac{\mathcal{O}_r}{r\mathcal{O}_r}\right)^{\times} \simeq \left(\frac{\mathbb{Z}}{r\mathbb{Z}}\right)^{\times},$$

and the index of $E_r^{(1)}$ in $E_r^{(0)}$ is $r-1$. If $a > 1$, then

$$\frac{E_r^{(a-1)}}{E_r^{(a)}} \simeq \frac{r^{a-1}\mathcal{O}_r}{r^a\mathcal{O}_r} \simeq \frac{\mathbb{Z}}{r\mathbb{Z}}, \qquad \text{(additive group)},$$

and the index of $E_r^{(a)}$ in $E_r^{(a-1)}$ is r. So the order of $Gal(F_R/\mathbb{Q}_r)$, which is p, divides $r-1$ or it divides r. But p does not divide r; r is a prime distinct from p. Therefore p divides $r-1$ or, equivalently, $r \equiv 1 \bmod (p)$. □

In the process of proving (7.2), we have proved, keeping in mind that F is a real field and therefore there is no possibility of the infinite prime of $\mathbb{Q}$ ramifying in F,

(7.3) LEMMA. *Let l be the product of finite primes of $\mathbb{Q}$ which ramify in F. Then the conductor $f(F/\mathbb{Q})$ of F over $\mathbb{Q}$ is simply $l\mathbb{Z}$.* □

(7.4) THEOREM. *If $K = \mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, or $\mathbb{Q}(\sqrt{-3})$, then the class of $\mathcal{O}_L$ in $R'(\mathcal{O}_K G)$ is trivial.*

Proof. Let $K = \mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, or $\mathbb{Q}(\sqrt{-3})$. Then $d(K/\mathbb{Q}) = 4\mathbb{Z}$, $8\mathbb{Z}$, or $3\mathbb{Z}$. By (7.2), there does not exist an abelian extension F of $\mathbb{Q}$ of degree p such that 2 or 3 divides the discriminant $d(F/\mathbb{Q})$. Therefore, for any abelian extension F of $\mathbb{Q}$ of degree p, $d(K/\mathbb{Q})$ and $d(F/\mathbb{Q})$ are relatively coprime. Applying (7.1) now immediately proves the theorem. □

Since, by (7.4), there is nothing else to be said about the case when K is $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{-3})$, let us assume that K is a field other than $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{-3})$. We can write K as $\mathbb{Q}(\sqrt{-q})$ where q is a prime congruent to 3 mod (4). The discriminant $d(K/\mathbb{Q})$ of K over $\mathbb{Q}$ is $q\mathbb{Z}$. The discriminant $d(F/\mathbb{Q})$ of F over $\mathbb{Q}$ is $l^{p-1}\mathbb{Z}$ where l is the product of prime integers of $\mathbb{Q}$ which ramify in F. This follows easily from the fact that

$$d(F/\mathbb{Q}) = \mathrm{norm}_F(\mathcal{D}(F/\mathbb{Q})),$$

where the different $\mathcal{D}(F/\mathbb{Q})$ is the product of ramified primes of F raised to the power $p-1$. There are three distinct possibilities for the prime factors of l:

a) $l = q$, i.e., F is ramified at q only,
b) $l = m$, $(q,m) = 1$, i.e., F is ramified at primes other than q, and
c) $l = qm$, $(q,m) = 1$, i.e., F is ramified at q as well as at primes other than q.

To indicate F's ramification, we will write F as F_q, F_m, or F_{qm} representing the above three possibilities. The associated field L will be written as L_q, L_m, or L_{qm}. In the following we will determine the class of $\mathcal{O}_L$ in $R'(\mathcal{O}_K G)$ in each of the three cases $L = L_q$, L_m, and L_{qm}. We begin with $L = L_m$ which is the easiest to deal with.

(7.5) THEOREM. *If $L = L_m$, then the class of $\mathcal{O}_L$ in $R'(\mathcal{O}_K G)$ is trivial.*

Proof. This is a straightforward case of applying (7.1). The discriminants $d(K/\mathbb{Q})$ and $d(F/\mathbb{Q})$ are relatively coprime and therefore L has a normal integral basis over K, and hence the class of $\mathcal{O}_L$ in $R'(\mathcal{O}_K G)$ is trivial. □

Let $\mathcal{O}_q$ and $\mathcal{O}_{qm}$, respectively, be the rings of integers in L_q and L_{qm}. The next result links the class of $\mathcal{O}_{qm}$ to the class of $\mathcal{O}_q$.

(7.6) THEOREM. *In $R'(\mathcal{O}_K G)$, $(\mathcal{O}_{qm}) = (\mathcal{O}_q)$, i.e., as an $\mathcal{O}_K G$-module, $\mathcal{O}_{qm}$ is isomorphic to $\mathcal{O}_q$.*

Before we could prove the above theorem, we need a number of auxiliary results. First of all, we note that the extension L_q is unique. To prove this we observe that the extension L_q is a compositum of K with F_q where F_q is an abelian extension of $\mathbb{Q}$ whose conductor, by (7.3), is $q\mathbb{Z}$. The smallest cyclotomic field containing F_q is, therefore, $\mathbb{Q}(\zeta_q)$. The Galois group $Gal(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/q\mathbb{Z})^\times$ which is cyclic of order $q-1$. Since p divides $q-1$, $Gal(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ has a unique subgroup

whose index in $Gal(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ is p. Therefore, by Galois correspondance, $\mathbb{Q}(\zeta_q)$ has a unique subfield whose degree over $\mathbb{Q}$ is p. Since F_q lies in $\mathbb{Q}(\zeta_q)$ and its degree over $\mathbb{Q}$ is p, F_q must be that field.

Next we indicate how extensions of the form F_m and F_{qm} can arise. Let us first consider F_m. The conductor of F_m is $m\mathbb{Z}$ and therefore $F_m \subset \mathbb{Q}(\zeta_m)$. If $m = \prod_{i=1}^{n} r_i$ is the factorization of m into prime integers, then

$$Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \simeq \left(\frac{\mathbb{Z}}{r_1\mathbb{Z}}\right)^{\times} \times \cdots \times \left(\frac{\mathbb{Z}}{r_n\mathbb{Z}}\right)^{\times}.$$

Since $r_i \equiv 1 \bmod (p)$, each group $(\mathbb{Z}/r_i\mathbb{Z})^{\times}$ has a subgroup whose index in $(\mathbb{Z}/r_i\mathbb{Z})^{\times}$ is p. Consequently $Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ has a whole string of subgroups with indices p in $Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. As a result, $\mathbb{Q}(\zeta_m)$ has an entire family of subfields with degree p over $\mathbb{Q}$ and discriminants which divide $m^{p-1}\mathbb{Z}$. The field F_m is one such field. Extensions of the form F_{qm} also arise in this manner.

Given an extension F_m, there is a quicker way of generating extensions of the form F_{qm}. It involves forming the compositum F_qF_m of F_m with F_q and then fixing under a subgroup of $Gal(F_qF_m/\mathbb{Q})$. The group $Gal(F_qF_m/\mathbb{Q})$ is isomorphic to $Gal(F_q/\mathbb{Q}) \times Gal(F_m/\mathbb{Q})$ where each factor is cyclic of order p. There are $p+1$ subgroups of $Gal(F_qF_m/\mathbb{Q})$ with indices p in $Gal(F_qF_m/\mathbb{Q})$. So there are $p+1$ subfields of F_qF_m with degree p over $\mathbb{Q}$. Out of these $p+1$ subfields, 2 correspond to F_q and F_m. The remaining $p-1$ subfields are of the form F_{qm}. The following result proves that any extension of the form F_{qm} can be generated in this manner.

(7.7) LEMMA. *For any extension F_{qm} there exists a unique extension F_m such that F_{qm} is a subfield of the compositum F_qF_m.*

Proof. The compositum F_qF_{qm} lies in $\mathbb{Q}(\zeta_{qm})$ and contains a unique extension F_m of $\mathbb{Q}$ of degree p which is ramified at primes dividing m only. The degree of F_qF_m over $\mathbb{Q}$ is p^2 which is the same as the degree of F_qF_{qm} over $\mathbb{Q}$. Therefore $F_qF_{qm} = F_qF_m$ and hence $F_{qm} \subset F_qF_m$.

The Galois group $Gal(F_qF_m/\mathbb{Q})$ is isomorphic to $Gal(F_q/\mathbb{Q}) \times Gal(F_m/\mathbb{Q})$. Let g_q and g_m, respectively, be generators of $Gal(F_q/\mathbb{Q})$ and $Gal(F_m/\mathbb{Q})$. Then the subgroups of $Gal(F_qF_m/\mathbb{Q})$ with indices p in $Gal(F_qF_m/\mathbb{Q})$ are $\langle g_q \rangle$, $\langle g_m \rangle$, and $\langle g_q^a g_m \rangle$, $1 \leq a \leq p-1$. The fixed fields of $\langle g_q \rangle$ and $\langle g_m \rangle$ are F_m and F_q respectively. Fixed fields of $\langle g_q^a g_m \rangle$ correspond to extensions which are ramified at q as well as at primes

dividing m. Therefore

$$F_{qm} = (F_q F_m)^{\langle g_q^a g_m \rangle},$$

for some $1 \leq a \leq p-1$. □

Proof of (7.6). By (7.7), there exists an extension F_m and an integer a, $1 \leq a \leq p-1$, such that F_{qm} is a subfield of $F_q F_m$ fixed under the subgroup of $Gal(F_q/\mathbb{Q}) \times Gal(F_m/\mathbb{Q})$ generated by $g_q^a g_m$. For the fields L_q, L_m and L_{qm} this implies

$$L_{qm} = (L_q L_m)^{\langle g_q^a g_m \rangle},$$

where $Gal(L_q/K) \simeq Gal(F_q/\mathbb{Q})$ and $Gal(L_m/K) \simeq Gal(F_m/\mathbb{Q})$.

The ring of integers in $L_q L_m$ is $\mathcal{O}_q \mathcal{O}_m$. This follows from the fact that $L_q L_m$ can written as $L_q F_m$. The discriminants $d(L_q/\mathbb{Q})$ and $d(F_m/\mathbb{Q})$ are relatively coprime and therefore the ring of integers in $L_q F_m$ is $\mathcal{O}_q \mathcal{O}'_m$ where $\mathcal{O}'_m$ is the ring of integers in F_m. Since $\mathcal{O}_K \subset \mathcal{O}_q$, it follows that $\mathcal{O}_q \mathcal{O}'_m = \mathcal{O}_q \mathcal{O}_K \mathcal{O}'_m$. But $\mathcal{O}_K \mathcal{O}'_m$ is the ring $\mathcal{O}_m$ of integers in $L_m = K F_m$. Therefore the ring of integers in $L_q F_m$ is $\mathcal{O}_q \mathcal{O}_m$.

By (7.5), L_m has a normal integral basis. Let $\theta \in \mathcal{O}_m$ be an element which generates a normal integral basis for L_m over K. Then $\mathcal{O}_m = \mathcal{O}_K Gal(L_m/K)(\theta)$ and $\mathcal{O}_q \mathcal{O}_m = \mathcal{O}_q Gal(L_m/K)(\theta)$. Each element of $\mathcal{O}_q \mathcal{O}_m$ can be uniquely written as $x_1 g_m^1(\theta) + \cdots + x_p g_m^p(\theta)$, $x_i \in \mathcal{O}_q$.

To find the ring $\mathcal{O}_{qm}$ of integers in L_{qm}, we note that an element $\sum_{i=1}^p x_i g_m^i(\theta)$, $x_i \in \mathcal{O}_q$, of $\mathcal{O}_q \mathcal{O}_m$ lies in $\mathcal{O}_{qm}$ if an only if

$$g_q^a g_m \left(\sum_{i=1}^p x_i g_m^i(\theta) \right) = \sum_{i=1}^p x_i g_m^i(\theta).$$

This gives $x_i = g_q^{ai}(x_p)$. Therefore

$$\mathcal{O}_{qm} = \left\{ \sum_{i=1}^p g_q^{ai}(x) g_m^i(\theta) \mid x \in \mathcal{O}_q \right\}.$$

It is now straightforward to check that the map

$$\begin{aligned} \mathcal{O}_q &\to \mathcal{O}_{qm}, \\ x &\mapsto \sum_{i=1}^p g_q^{ai}(x) g_m^i(\theta), \end{aligned}$$

is an isomorphism of $\mathcal{O}_K G$-modules. □

We had set ourselves the task of identifying the class of $\mathcal{O}_L$ in $R'(\mathcal{O}_K G)$ for $L = L_q$, L_m, and L_{qm}. We have shown that $(\mathcal{O}_m)$ is trivial and $(\mathcal{O}_{qm}) = (\mathcal{O}_q)$. So, to complete the task, all there remains for us to do is to determine the class of $\mathcal{O}_q$ in $R'(\mathcal{O}_K G)$. This we now do.

(7.8) LEMMA. *The class of $\mathcal{O}_q$ lies in the kernel group $D(\mathcal{O}_K G)$.*

Proof. Since

$$1 \to D(\mathcal{O}_K G) \to Cl(\mathcal{O}_K G) \to Cl(\mathcal{O}_K) \times Cl(\mathcal{O}_M) \to 1,$$

and the class number of K is 1, the proof involves showing that $\mathcal{O}_q$ corresponds to a principal ideal in $Cl(\mathcal{O}_M)$. More concretely, we need to show that, under the map

$$\pi_2 \phi : L_q \to M,$$

where

$$\begin{aligned} \phi : L_q &\to KG, \\ x &\mapsto \phi(x), \end{aligned}$$

$\phi(x)(\theta) = x$, θ is an element of $\mathcal{O}_q$ which generates a normal basis for L_q over K and π_2 is the projection of the algebra KG, which splits as $K \times M$, into M, the image of $\mathcal{O}_q$ is a principal ideal.

If $q = 7$, then p must be 3, for only then $q - 1 \equiv 0 \bmod (p)$ and an extension F_q which is ramified at q exists. But, by (6.15), M has class number 1 and therefore all ideals of M are principal.

If $q = 11$, then p is 5 and L_{11} is the unique extension contained in $\mathbb{Q}(\zeta_{11})$ whose degree over K is 5. Since the degree of $\mathbb{Q}(\zeta_{11})$ over K is 5, $L_{11} = \mathbb{Q}(\zeta_{11})$. Let $\theta = \zeta_{11}$. Then θ generates a normal integral basis for L_{11} over $\mathbb{Q}$, i.e.,

$$\mathcal{O}_{11} = \mathbb{Z}Gal(L_{11}/\mathbb{Q})(\theta).$$

Let $\sigma \in Gal(K/\mathbb{Q})$ be the non-trivial element. Then

$$\begin{aligned} \mathcal{O}_{11} &= \mathbb{Z}Gal(L_{11}/K)(\theta, \sigma(\theta)), \\ &= \mathbb{Z}G(\theta, \sigma(\theta)), \end{aligned}$$

where the action of G on $\theta = \zeta_{11}$ is defined as $g(\zeta_{11}) = \zeta_{11}^3$. Let $\phi : L_{11} \to KG$ be the isomorphism induced by θ. Then

$$\phi(\mathcal{O}_{11}) = \mathbb{Z}G(1, \phi(\sigma(\theta))).$$

To find $\phi(\sigma(\theta))$, we note that $\beta\theta = (x + \sigma y)(\theta)$, where β is the trace of ζ_{11} from L_{11}

to K, and $x = g^3 + g^4$ and $y + 1 + g^2 + g^3$ are elements of KG. The element $\sigma(\theta)$ can be written as $\sigma(\theta) = ((-x + \beta)/y)(\theta)$, and therefore

$$\phi(\mathcal{O}_{11}) = \mathbb{Z}G\left(1, \frac{1}{y}(-x + \beta)\right).$$

Applying $\pi_2 : KG \to M$, $g \mapsto \zeta_5$, gives

$$\pi_2\phi(\mathcal{O}_{11}) = \left\langle 1, \frac{1}{\pi_2(y)}(-\pi_2(x) + \beta)\right\rangle_{\mathcal{O}_M}.$$

But $\pi_2(y) = 1 + \zeta_5^2 + \zeta_5^3 = (1 - \sqrt{5})/2$ is a unit in $\mathcal{O}_M$. Therefore $\pi_2\phi(\mathcal{O}_{11}) = \mathcal{O}_M$. So $\pi_2\phi(\mathcal{O}_{11})$ indeed is principal and hence $(\mathcal{O}_{11}) \in D(\mathcal{O}_K G)$.

If $q = 19$, then $p = 3$. By (6.15), $Cl(\mathcal{O}_M) = 1$ and therefore every ideal is principal.

If $q = 43$, then $p = 3$ or 7. If $p = 3$ then, by (6.15), $Cl(\mathcal{O}_M) = 1$. Assume $p = 7$. Then L_{43} is the unique subfield of $\mathbb{Q}(\zeta_{43})$ whose degree over K is 7. Let θ be the trace of ζ_{43} from $\mathbb{Q}(\zeta_{43})$ to L_{43}. Then

$$\theta = \zeta_{43} + \zeta_{43}^6 + \zeta_{43}^{36},$$

and

$$\mathcal{O}_{43} = \mathbb{Z}Gal(L_{43}/\mathbb{Q})(\theta),$$

or

$$\mathcal{O}_{43} = \mathbb{Z}G(\theta, \sigma(\theta)),$$

where $\sigma \in Gal(K/\mathbb{Q})$ is the non-trivial element and the action of G on θ is induced from $g(\zeta_{43}) = \zeta_{43}^9$. Let $\phi : L \to KG$ be the isomorphism induced by θ. Then

$$\phi(\mathcal{O}_{43}) = \mathbb{Z}G(1, \phi(\sigma(\theta))).$$

To find $\phi(\sigma(\theta))$, we need to express $\sigma(\theta)$ as $z(\theta)$ where $z \in KG$. We have $\beta\theta = (x + \sigma y)(\theta)$, where β is the trace of ζ_{43} from $\mathbb{Q}(\zeta_{43})$ to K, $x = 1 + g + 2g^3 + g^4 + 3g^5 + 2g^6$ and $y = 3 + g + g^2 + 2g^3 + 2g^4 + g^5 + g^6$, and therefore

$$\phi(\mathcal{O}_{43}) = \mathbb{Z}G\left(1, \frac{1}{y}(-x + \beta)\right).$$

Applying $\pi_2 : KG \to M$, $g \mapsto \zeta_7$, gives

$$\pi_2\phi(\mathcal{O}_{43}) = \left\langle 1, \frac{1}{\pi_2(y)}(-\pi_2(x) + \beta)\right\rangle_{\mathcal{O}_M}.$$

But the norm of the element

$$\pi_2(y) = -(2\zeta_7 + 2\zeta_7^2 + \zeta_7^3 + \zeta_7^4 + 2\zeta_7^5 + 2\zeta_7^6)$$

is 1 and therefore it is a unit. Hence $\pi_2\phi(\mathcal{O}_{43}) = \mathcal{O}_M$.

If $q = 67$, then $p = 3$ or 11. If $p = 3$ then, by (6.15), $Cl(\mathcal{O}_M) = 1$ and so $(\mathcal{O}_q) \in D(\mathcal{O}_K G)$. Assume $p = 11$. Then $L_{67} \subset \mathbb{Q}(\zeta_{67})$ and

$$\mathcal{O}_{67} = \mathbb{Z}Gal(L_{67}/\mathbb{Q})(\theta),$$

where $\theta = \zeta_{67} + \zeta_{67}^{29} + \zeta_{67}^{37}$ is the trace of ζ_{67} from $\mathbb{Q}(\zeta_{67})$ to L_{67}. We can write $\mathcal{O}_{67}$ as

$$\mathcal{O}_{67} = \mathbb{Z}G(\theta, \sigma(\theta)),$$

where σ is the non-trivial element of $Gal(K/\mathbb{Q})$, and the action of G on θ is induced from $g(\zeta_{67}) = \zeta_{67}^4$. Let $\phi : L_{67} \to KG$ be the isomorphism induced by θ. Then

$$\phi(\mathcal{O}_{67}) = \mathbb{Z}G\left(1, \frac{1}{y}(-x + \beta)\right),$$

where β is the trace of ζ_{67} from $\mathbb{Q}(\zeta_{67})$ to K, and

$$x = 1 + 2g^2 + g^3 + 2g^4 + g^5 + 2g^6 + g^7 + 2g^8 + g^9 + 3g^{10},$$
$$y = 3 + 2g + 2g^2 + g^3 + 2g^5 + 2g^6 + g^8 + 2g^9 + 2g^{10}.$$

Applying $\pi_2 : KG \to M$, $g \mapsto \zeta_{11}$, to $\phi(\mathcal{O}_{67})$ gives

$$\pi_2\phi(\mathcal{O}_{67}) = \left\langle 1, \frac{1}{\pi_2(y)}(-\pi_2(x) + \beta) \right\rangle_{\mathcal{O}_M}.$$

Unlike the previous cases, the norm of the element

$$\pi_2(y) = -(\zeta_{11} + \zeta_{11}^2 + 2\zeta_{11}^3 + 3\zeta_{11}^4 + \zeta_{11}^5 + \zeta_{11}^6 + 3\zeta_{11}^7 + 2\zeta_{11}^8 + \zeta_{11}^9 + \zeta_{11}^{10})$$

from $N = \mathbb{Q}(\zeta_{11})$ to $\mathbb{Q}$ is not 1 or -1 and therefore it is not a unit. The norm of the element $\pi_2(y)$ from N to $\mathbb{Q}$ is 89^2. The prime 89 splits completely in N. Let A_i, $1 \leq i \leq 10$, denote primes of N lying above 89. Then

$$A_i = \langle 89, \zeta_{11} - 2^i \rangle_{\mathcal{O}_N}, \qquad 1 \leq i \leq 10.$$

By subjecting $\pi_2(y)$ to the maps, one for each i,

$$\mathcal{O}_N \to \frac{\mathcal{O}_N}{A_i},$$

we can find the primes which occur in the factorization of $\pi_2(y)\mathcal{O}_N$. We obtain $\pi_2(y) = A_2A_9$.

Now each of the primes A_i, $1 \leq i \leq 10$, splits further in M. This is due to the fact that 89 splits in K. Let B_1 and B_2 be the primes of K lying above 89. Then, we can assume, $B_1 = \langle 8 + \alpha \rangle_{\mathcal{O}_K}$ and $B_2 = \langle 9 - \alpha \rangle_{\mathcal{O}_K}$. We can now write down the primes of M lying above 89. They are

$$C_{ij} = \langle A_i, B_j \rangle_{\mathcal{O}_M}, \qquad 1 \leq i \leq 10,\ 1 \leq j \leq 2.$$

The factorization of $\pi_2(y)\mathcal{O}_M$ in M is therefore given by

$$\pi_2(y)\mathcal{O}_M = C_{21}C_{22}C_{91}C_{92}.$$

To obtain the factorization of $(-\pi_2(x)+\beta)\mathcal{O}_M$, we note that the norm of $-\pi_2(x)+\beta$ form M to N is ${\pi_2}^2(x) + \pi_2(x) + 17$. By using a method similiar to the one for $\pi_2(y)\mathcal{O}_N$, we can show that $({\pi_2}^2(x) + \pi_2(x) + 17)\mathcal{O}_N = A_2^2 A_9^2$. Under the maps

$$\mathcal{O}_M \rightarrow \frac{\mathcal{O}_M}{C_{ij}}, \qquad 1 \leq i \leq 10,\ 1 \leq j \leq 2,$$

$-\pi_2(x) + \beta$ lies in the kernel if and only if $i = 2$, $j = 1$ or $i = 9$, $j = 2$. Therefore

$$(-\pi_2(x) + \beta)\mathcal{O}_M = C_{21}^2 C_{92}^2,$$

since the norm from M to N is $A_2^2 A_9^2$.

Returning to the ideal $\pi_2\phi(\mathcal{O}_{67})$, we find

$$\begin{aligned} \pi_2\phi(\mathcal{O}_{67}) &= \left\langle 1, \frac{C_{21}^2 C_{92}^2}{C_{21}C_{22}C_{91}C_{92}} \right\rangle_{\mathcal{O}_M}, \\ &= \frac{1}{C_{22}C_{91}}. \end{aligned}$$

To prove that $\pi_2\phi(\mathcal{O}_{67})$ is principal and hence $(\mathcal{O}_{67}) \in D(\mathcal{O}_K G)$, we need to show that the ideal $C_{22}C_{91}$ is principal. The ideal $C_{22}C_{91}$ is fixed under complex conjugation. Complex conjugation sends A_i to A_{11-i} and B_1 to B_2, and therefore

$$(C_{22})^c = \langle A_2, B_2 \rangle_{\mathcal{O}_M}^c = \langle A_9, B_1 \rangle_{\mathcal{O}_M} = C_{91}.$$

So the ideal $C_{22}C_{91}$ basically is a prime ideal of M^+ extended to M. From this we conclude that $\pi_2\phi(\mathcal{O}_{67})$ is principal if the primes of M^+ lying above 89 are principal.

The primes of M^+ lying above 89 are principal. In fact, the class number of M^+ is 1. To give the generators for the primes dividing 89, let us write M^+ as $\mathbb{Q}(\nu)$ where

ν is a zero of the polynomial

$$p(x) = x^{10} - x^9 - 186(x^8 - x^7) + 12530(x^6 - x^5) - 365771(x^4 - x^3) + 4227884(x^2 - x) - 11390543.$$

The primes dividing 89 are then generated by the element

$$\frac{1}{331057}(-8\nu^9 - 10\nu^8 + 961\nu^7 + 1058\nu^6 - 37042\nu^5 - 41119\nu^4 + 504190\nu^3 + 607692\nu^2 - 1708239\nu - 4787272)$$

and its $Gal(M^+/\mathbb{Q})$-conjugates. The ideal $\pi_2\phi(\mathcal{O}_{67})$ is therefore principal, and so $(\mathcal{O}_{67}) \in D(\mathcal{O}_K G)$.

Lastly, if $q = 163$ then $p = 3$, and, by (6.15), the class number of M is 1. Hence $(\mathcal{O}_q) \in D(\mathcal{O}_K G)$. □

The next result completes our calculations to determine the class of $\mathcal{O}_q$.

(7.9) LEMMA. *The class of $\mathcal{O}_q$ in $R'(\mathcal{O}_K G)$ is non-trivial; its order is 2.*

Proof. By (7.8), $(\mathcal{O}_q)$ lies in the kernel group $D(\mathcal{O}_K G)$. In the last section we saw that $D(\mathcal{O}_K G) \simeq \mathrm{Coker}(j)$, where the map

$$j : \mathcal{O}_M^\times \to \left(\frac{\mathcal{O}_M}{(1-\zeta_p)\mathcal{O}_M}\right)^\times$$

is induced by reduction mod $((1-\zeta_p)\mathcal{O}_M)$, and, for an element $[x] \in \mathrm{Coker}(j)$, the corresponding class $(C(x))$ in $D(\mathcal{O}_K G)$ is defined by the diagram:

$$\begin{array}{ccc} C(x) & \longrightarrow & \mathcal{O}_M \\ \downarrow & & \downarrow j_1 \\ \mathcal{O}_K & \xrightarrow{j_2} & \mathcal{O}_M/(1-\zeta_p)\mathcal{O}_M \end{array}$$

where j_1 is multiplication by x followed by reduction mod $((1-\zeta_p)\mathcal{O}_M)$ and j_2 is reduction mod $(p\mathcal{O}_K)$.

On the other hand, given a class in $D(\mathcal{O}_K G)$ in the form of a ring $\mathcal{O}_L$ of integers in a tame extension L over K with $Gal(L/K) \simeq G$, the way we determine the corresponding element in $\mathrm{Coker}(j)$ is to subject $\mathcal{O}_L$ to the map

$$(\pi_1, \pi_2)\phi : L \to K \times M,$$

where $\phi : L \to KG$ is an isomorphism and $\pi_1(g) = 1$, $\pi_2(g) = \zeta_p$, and obtain the images, say, $x\mathcal{O}_K$ and $y\mathcal{O}_M$ in K and M respectively. These images, as has been

indicated, are principal ideals since it is known that $(\mathcal{O}_L) \in D(\mathcal{O}_K G)$. The class $(\mathcal{O}_L)$ can then be described by the diagram:

$$\begin{array}{ccc} \mathcal{O}_L & \overset{y^{-1}\pi_2\phi}{\longrightarrow} & \mathcal{O}_M \\ \downarrow{\scriptstyle x^{-1}\pi_1\phi} & & \downarrow{\scriptstyle j_1} \\ \mathcal{O}_K & \overset{j_2}{\longrightarrow} & \mathcal{O}_M/(1-\zeta_p)\mathcal{O}_M \end{array}$$

where j_1 is multiplication by y/x followed by reduction mod $((1-\zeta_p)\mathcal{O}_M)$ and j_2 is reduction mod $(p\mathcal{O}_K)$. But this square defines $(C(y/x))$. Therefore $(\mathcal{O}_L) = (C(y/x))$ and the element of Coker(j) corresponding to $(\mathcal{O}_L)$ is $[y/x]$.

To prove the lemma, we have two distinct cases to consider: p is inert in K, or p splits in K. Assume p splits in K. Then there is only one instance of this which occurs when $q = 11$ and $p = 5$. In the proof of (7.8) we saw that if $\phi : L_{11} \to KG$ is the isomorphism induced by ζ_{11} then $\pi_2\phi(\mathcal{O}_{11}) = \mathcal{O}_M$. To calculate $\pi_1\phi(\mathcal{O}_{11})$, we note that the map $\pi_1\phi$ is the familiar trace from L_{11} to K composed with multiplication by $1/\mathrm{tr}_{L/K}(\zeta_{11})$. Therefore

$$\pi_1\phi(\mathcal{O}_{11}) = \frac{\mathrm{tr}_{L/K}(\mathcal{O}_{11})}{\mathrm{tr}_{L/K}(\zeta_{11})}.$$

Since L_{11} is a tame extension of K, there is an element in $\mathcal{O}_{11}$ with trace 1. Consequently, $\mathrm{tr}_{L/K}(\mathcal{O}_{11}) = \mathcal{O}_K$. The trace of ζ_{11} is $\alpha - 1$. Therefore $\pi_1\phi(\mathcal{O}_{11}) = (1/\alpha - 1)\mathcal{O}_K$ and hence $(\mathcal{O}_{11}) = (C(\alpha - 1))$.

The structure and the order of the group Coker(j) was calculated in section 2. For the case under consideration, it is a cyclic group of order 2 generated by $[\alpha]$. Since $[\alpha - 1] = [\alpha]$, $(\mathcal{O}_{11}) = (C(\alpha))$, and hence the order of $(\mathcal{O}_{11})$ in $D(\mathcal{O}_K G)$ is 2. In fact, $(\mathcal{O}_{11})$ generates $D(\mathcal{O}_K G)$.

If p is inert in K, then by using an argument similar to the one for (6.1) we can show that the class of $(\mathcal{O}_q)$ is $(C(x))$ where $x^2 \equiv l \bmod (p\mathcal{O}_K)$ and $d(L_q/K) = l^{p-1}\mathcal{O}_K$ is the discriminant. The only prime of K which ramifies in L_q/K is the one lying above $q\mathbb{Z}$. The rational prime $q\mathbb{Z}$ ramifies in K: $q\mathcal{O}_K = (\sqrt{-q})^2\mathcal{O}_K = (2\alpha - 1)^2\mathcal{O}_K$. Therefore $d(L_q/K) = (2\alpha - 1)^{p-1}\mathcal{O}_K$. The group $(\mathcal{O}_K/p\mathcal{O}_K)^\times$ is cyclic of order $p^2 - 1$. Let z be a generator for $(\mathcal{O}_K/p\mathcal{O}_K)^\times$. Then the image of j is generated by $z^{(p+1)/2}$ and Coker(j) is a cyclic group of order $(p+1)/2$. Solving the congruence $x^2 \equiv l \bmod (p\mathcal{O}_K)$ in $(\mathcal{O}_K/p\mathcal{O}_K)^\times$ gives

$$x \equiv \pm z^{(p+1)/4} \bmod (p\mathcal{O}_K),$$

which shows that $x \notin \mathrm{Im}(j)$ and therefore, in Coker(j), $[x] \neq 1$. This proves that the class of $\mathcal{O}_q$ is non-trivial. Since $[x]^2 = 1$, the order of $(\mathcal{O}_q)$ in $R'(\mathcal{O}_K G)$ is 2. □

This concludes our discussion of the case when $Gal(L/\mathbb{Q})$ ia abelian. We have proved

(7.10) THEOREM. *If L is a tame extension of K with $Gal(L/K) \simeq G$ which is also an abelian extension of $\mathbb{Q}$, then the class of $\mathcal{O}_L$ lies in $D(\mathcal{O}_K G)$ and has order at most 2.* □

Next we consider the case when $Gal(L/\mathbb{Q})$ is isomorphic to D_{2p}.

(7.11) THEOREM. *Let L be a tame extension of K with $Gal(L/K) \simeq G$ and $Gal(L/\mathbb{Q}) \simeq D_{2p}$. If $(\mathcal{O}_L) \in D(\mathcal{O}_K G)$ and p is inert in K then $\mathcal{O}_L$ is a free $\mathcal{O}_K G$-module.*

Proof. Let us recall that the kernel group $D(\mathcal{O}_K G)$ is isomorphic to the cokernel of the map $j : \mathcal{O}_M^\times \to (\mathcal{O}_M/(1-\zeta_p)\mathcal{O}_M)^\times$. For $[x] \in \text{Coker}(j)$, the class in $D(\mathcal{O}_K G)$ which corresponds to $[x]$ is $(C(x))$ (see section 6 for the definition of $C(x)$).

Let $\theta \in \mathcal{O}_L$ with $\text{tr}_{L/K}(\theta) = 1$ be an element which generates a normal basis for L over K, let $\phi : L \to KG$ be the isomorphism of KG-modules defined by $x \mapsto \phi(x)$ where $\phi(x)(\theta) = x$, and let $(\pi_1, \pi_2) : KG \to K \times M$ be the map given by $(\pi_1, \pi_2)(g) = (1, \zeta_p)$. If $(\mathcal{O}_L) \in D(\mathcal{O}_K G)$, then, because of our choice of θ, $\pi_1\phi(\mathcal{O}_L)$ is $\mathcal{O}_K$, $\pi_2\phi(\mathcal{O}_L)$ is a principal fractional ideal, and $(\mathcal{O}_L) = (C(y))$ where $\pi_2\phi(\mathcal{O}_L) = y\mathcal{O}_M$. By using an argument similar to the one used to prove (6.1) we can show that

$$y^{p-1} \equiv uk^{p-1} \bmod ((1-\zeta_p)\mathcal{O}_M),$$

where $u \in \mathcal{O}_K^\times$, $k^2 \equiv l \bmod (p\mathcal{O}_K)$, and l is the product of primes of K which ramify in L. The above congruence can be solved to give, in $\text{Coker}(j)$, $[y] = [k]$. So the class of $\mathcal{O}_L$ is $(C(k))$ where $k^2 \equiv l \bmod (p\mathcal{O}_K)$.

Since L/K is a cyclic extension of degree prime p, any prime r of K which ramifies in L satisfies $\text{norm}_K(r) \equiv 1 \bmod (p)$. Therefore $\text{norm}_K(l) \equiv 1 \bmod (p)$. By considering ramification of rational primes in the maximal real subfield of L we can show that l has the form ul' where $u \in \mathcal{O}_K^\times$ and l' is a product of rational primes. The congruence $\text{norm}_K(l) \equiv 1 \bmod (p)$ now gives $l'^2 \equiv 1 \bmod (p)$, or $l' \in \langle z^{(p^2-1)/2} \rangle$ where z is a generator of $(\mathcal{O}_M/(1-\zeta_p)\mathcal{O}_M)^\times$ which is a cyclic group of order p^2-1. The group $\mathcal{O}_K^\times$ of units is $\langle \zeta_4 \rangle$ if $K = \mathbb{Q}(\sqrt{-1})$, $\langle \zeta_6 \rangle$ if $K = \mathbb{Q}(\sqrt{-3})$, or $\langle -1 \rangle$ if $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$. So any unit $u \in \mathcal{O}_K^\times$, on reduction mod $(p\mathcal{O}_K)$, lies in $\langle z^{(p^2-1)/t} \rangle$ where t is 4 if $K = \mathbb{Q}(\sqrt{-1})$, 6 if $K = \mathbb{Q}(\sqrt{-3})$, or 2 if $K \neq \mathbb{Q}(\sqrt{-1})$,

$\mathbb{Q}(\sqrt{-3})$. Therefore, on reduction mod $(p\mathcal{O}_K)$, l lies in $\langle z^{(t/2+1)(p^2-1)/t}\rangle$. Solving the congruence $k^2 \equiv l \bmod ((1-\zeta_p)\mathcal{O}_M)$ now shows that k lies in the subgroup generated by $z^{(p+1)/t}$. But by (2.2) the order of $D(\mathcal{O}_K G) \simeq \mathrm{Coker}(j)$ is $(p+1)/t$ and so the image of $j : \mathcal{O}_M^{\times} \to (\mathcal{O}_M/(1-\zeta_p)\mathcal{O}_M)^{\times}$ is generated by $z^{(p+1)/t}$. Therefore, in $\mathrm{Coker}(j)$, $[k] = 1$ and hence the class $(C(k))$ is trivial. □

The proof of the above theorem, as has been stated in the statement of the theorem, works only if p is inert in K. If p splits in K then the class of $\mathcal{O}_L$ is still determined by the element y where $\pi_2\phi(\mathcal{O}_L) = y\mathcal{O}_M$. But because, for any $x \in (\mathcal{O}_M/(1-\zeta_p)\mathcal{O}_M)^{\times}$, $x^{p-1} = 1$, we can not use a congruence of the form $y^{p-1} \equiv uk^{p-1} \bmod ((1-\zeta_p)\mathcal{O}_M)$ to calculate y.

References

[1] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, (1966).

[2] J. W. S. Cassels and A. Fröklich, *Algebraic Number Theory*, Academic Press, (1967).

[3] A. Fröhlich, *On the class group of integral group rings of finite abelian groups*, Mathematika **16** (1969), 143–152.

[4] A. Fröhlich, *Arithmetic and Galois module structure for tame extensions*, Crelle **286/287** (1976), 380–440.

[5] S. Galovich, *The class group of a cyclic p-group*, J. Algebra **30** (1974), 368–387.

[6] S. Homayouni, *Class groups of group rings over quadratic number fields*, thesis, King's college, (1982).

[7] Hua Loo-Keng, *Introduction to Number Theory*, Springer-Verlag, (1982).

[8] H. Jacobinski, *Genera and decomposition of lattices over orders*, Acta Math. **121** (1968), 1–29.

[9] L. R. McCulloh, *Galois Module Structure of Elementary Abelian Extensions*, J. Algebra **82** (1983), 102–134.

[10] L. R. McCulloh, *Galois module structure of abelian extensions*, Crelle **375/376** (1987), 259–306.

[11] I. Reiner, *Maximal Orders*, Academic Press (1975).

[12] I. Reiner and S. Ullom, *A Mayer-Vietoris sequence for class groups*, J. Algebra **31** (1974), 305–342.

[13] R. G. Swan, *Induced Representations of Projective Modules*, Ann. of Math. **71** (1960), 552–578.

[14] R. G. Swan, *The Grothendick Ring of a Finite Group*, Topology, **2** (1963), 85–110.

[15] M. J. Taylor, *On Fröhlich's conjecture for rings of integers of tame extensions*, Invent. Math. **63** (1981), 41–79

[16] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics, Springer-Verlag, (1982).