REFLECTIONS IN K_2

BY

ØYVIND INDREBØ

THESIS FOR THE DEGREE OF

MASTER OF SCIENCE

(MASTER I MATEMATIKK)

DEPARTMENT OF MATHEMATICS
FACULTY OF MATHEMATICS AND NATURAL SCIENCES
UNIVERSITY OF OSLO

NOVEMBER 2011

Abstract

In this thesis we show a reflection theorem for K_2. We compare the 3-rank of $K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{D})})$ to the 3-rank of $K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{-3D})})$ and find that they differ by at most 2. We also show by examples that the formula we obtain is optimal. Introductions to algebraic number theory and classical algebraic K-theory are provided. A proof by Washington of Scholz's Reflection Theorem is given, and we discuss in detail results from Moore, Keune and Tate that describe the structure of $K_2(\mathcal{O}_F)$ of a number field F.

Contents

Introduction

In 1932, Arnold Scholz wrote a paper *Über die Beziehung der Klassenzahlen quadratizcher Körper zueinander*, in which he states and proves the following theorem:

Satz. *Hat von den beiden Körpern $P(\sqrt{\delta})$ und $P(\sqrt{-3\delta})$ die Klassengruppe des imaginären Körpers r Basisklassen und die des reellen Körpers s Basisklassen von Dreierpotenzordnung (also $3^r - 1$ bezw. $3^s - 1$ Idealklassen der Ordnung 3), so gilt:*

$$s \leq r \leq s + 1.$$

In modern terms this would be:

Theorem. *Let D be a positive square free number, and consider the quadratic number fields $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt{-3D})$. Let s be the 3-rank of $\mathrm{Cl}(\mathbb{Q}(\sqrt{D}))$ and r the 3-rank of $\mathrm{Cl}(\mathbb{Q}(\sqrt{-3D}))$. Then*

$$s \leq r \leq s + 1.$$

This theorem is known as the Reflection Theorem and has since Scholz's time been generalized by many authors. Most notably, Leopold's Spigelungssatz ([12]) and Georges Grass' $T - S$-Reflection Theorem ([8]).

In this thesis, we will "extend" the reflection theorem to K_2. We will, by using the same techniques as Lawrence C. Washington used to prove Scholz's theorem in [24], prove the following reflection theorem for K_2.

Theorem. *Let D be a positive square free integer. Then*

$$\mathrm{rk}_3(K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{-3D})})) - \mathrm{rk}_3(K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{D})})) = \begin{cases} 1, 0, -1 & \text{if } d \equiv 1 \bmod 3 \\ 0, -1, -2 & \text{if } d \equiv 6 \bmod 9 \\ 0, -1 & \text{otherwise.} \end{cases}$$

We will also find examples of all the 8 different cases of the theorem above. Most of the examples have been computed by the free computer algebra system PARI/GP ([23]).

The group $K_2(\mathcal{O}_F)$ was first studied as the kernel of the direct sum of the Tame symbol maps

$$\tau : K_2(F) \xrightarrow{\oplus \tau_P} \bigoplus_P k_P^\times.$$

The map τ was first shown to be surjective by Calvin Moore as a consequence of his Reciprocity Theorem, in 1968 [16], which lead Bass, Milnor and Tate among others to study the Tame kernel $\ker \tau$. The next big breakthrough came when Howard Garland proved that the Tame kernel is finite, when F is a number field in [7], 1971. The finiteness of $\ker \tau$ was later extended to function fields by Bass and Tate. For a very nice summary of what was known about the Tame kernel before Garland's Finiteness Theorem see [21]. The Tame kernel was identified with $K_2(\mathcal{O}_F)$ as a consequence of Daniel Quillen's localization sequence for higher K-theory published in [20],

1973. Quillen's paper became the foundation of higher algebraic K-theory. In 1976, John Tate published a paper *Relations between K_2 and Galois cohomology*, [22], where he proves that

$$K_2(F)/n \approx {}_nBr(F),$$

for a global field F, that contains a primitive nth root of unity. Here ${}_nBr(F)$ denotes the subgroup of elements of order dividing n, in the Brauer group $Br(F)$. This result was later extended to all fields by Merkurjev and Suslin, in [14]. Also in the paper by Merkurjev and Suslin is Hilbert's 90 for K_2 proved.

Organization of the sections

Section 1 is a basic introduction to algebraic number theory with an emphasis on quadratic number fields. We will define the ring of integers, ideal class group and discuss ideal decompositions in a Galois extension. For quadratic number fields, we will determine the rings of integers and the ideal decomposition of a prime number p in $\mathbb{Q}(\sqrt{D})$.

In Section 2 we state and prove Scholz's Reflection Theorem. The proof we give is a slightly more detailed version of Washington's proof in [24]. We will later in Section 4 use some of the same techniques to prove the reflection theorem for K_2. In addition to the theory developed in Section 1, we will need results from Kummer theory and class field theory. The observant reader may also notice that we make use of the Norm Residue symbol in the proof of Scholz's Reflection Theorem, without mentioning it. Since the Norm Residue symbol is closely related to the Hilbert symbol, which is crucial in the study of the structure of $K_2(\mathcal{O}_F)$ for a number field F, it might be possible to find a more direct proof of reflection in K_2.

Section 3 is divided into three parts. The first one is an introduction to Classical Algebraic K-theory, where the functors K_0, K_1 and K_2 are defined and discussed. In the second part, we use Matsumoto's description of $K_2(F)$ for a field F, to define Steinberg symbols. The Steinberg symbols will be used to describe the structure of $K_2(F)$ and $K_2(\mathcal{O}_F)$ when F is a number field. The third part shows two "structure" theorems for $K_2(\mathcal{O}_F)/p$. These results are consequences of Tate's work in [22], but the presentation is the same as in [11].

In Section 4, we prove the reflection theorem for K_2, using the theory developed in the previous sections.

In Section 5,we give, for each of the different cases of the theorem in Section 4, an example of a D such that $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt{-3D})$ satisfies that case. Most of the examples are computed by the computer algebra system PARI/GP. We have included the code needed to check the first example with an explanation of what the different functions do, and how to interpret their output. We prove the reflection theorem for K_2 using the theory developed in the previous sections. The examples show that our theorem in section 4 is optimal.

Acknowledgments

I would like to thank my adviser Paul Arne Østvær for giving me such a nice problem for my thesis. I would also like to thank Roman Linneberg Eliassen, Nina Holden, Kristian Jonsson Moi, Elin Røse and Sigurd Segtnan for proof reading and valuable feedback. Finally, I would like to

thank all the students on the sixth floor of Nils Henrik Abels hus for good companionship, and the math department at UC Berkeley for hosting me in the Fall 2010 and Spring 2011.

1 Basic Number Theory

In this section we will review the basic theory of our main object of study, namely quadratic number fields. All rings in this section are assumed to be commutative with a unit element.

1.1 Rings of Integers in algebraic number fields

A number field is a finite extension of the rational numbers $\mathbb{Q}$ contained in the complex numbers $\mathbb{C}$. In other words a field L is a number field if it is finite as a $\mathbb{Q}$-algebra. We can therefore give L a finite dimensional $\mathbb{Q}$-vector space structure. A quadratic number field $L = \mathbb{Q}(\sqrt{D})$ is for example a two dimensional $\mathbb{Q}$-vector space spanned by $\{1, \sqrt{D}\}$, where D is assumed to be squarefree.

If K is a number field and L is a finite field extension of K, then L is a number field, and hence finite dimensional as a $\mathbb{Q}$-vector space. We will write L/K for finite extensions $K \hookrightarrow L$.

Definition 1.1. Let $A \subset B$ be an extension of rings[1]. An element $x \in B$ is said to be integral over A if it is a zero of a monic polynomial with coefficients in A, i.e. $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ where $a_i \in A$.

The set $C \subset B$ consisting of all A-integral elements forms a ring and is called the integral closure of A in B.

The ring of integers $\mathcal{O}_L$ of a number field L plays the same role as $\mathbb{Z}$ does for $\mathbb{Q}$, in the sense that $\mathcal{O}_L$ is the smallest integrally closed subdomain of L such that L is the fraction field of $\mathcal{O}_L$.

If A is a domain and the integral closure of A in its fraction field is equal to A, then we say that A is integrally closed.

Since multiplication distributes over addition, we get a correspondence between elements $a \in L$ and the linear transformation given by $T_a : x \mapsto ax$. By choosing a basis for L, this correspondence yields a ring homomorphism from L to the center of the non-commutative ring $Gl_n(K)$. Each of these matrices has a determinant and a trace.

Definition 1.2. Let L/K be an extension of number fields, and $\alpha = \{\alpha_1, \ldots, \alpha_n\}$ be a basis of L as a K-vector space. The trace and norm functions from L to K are defined by

$$\text{Trace}_{L/K,\alpha}(x) = \text{tr}\, T_x \text{ and } \text{Norm}_{L/K,\alpha}(x) = \det T_x,$$

where $T_x : L \to L$ is the matrix corresponding to multiplication by x.

The trace and the norm can be defined independently of a basis in the following way:

Lemma 1.3. *For an extension of number fields L/K, let S denote the set of K-embeddings of L in $\mathbb{C}$, then*

$$\text{Trace}_{L/K}(x) = \sum_{\sigma \in S} \sigma x \text{ and } \text{Norm}_{L/K}(x) = \prod_{\sigma \in S} \sigma x.$$

Proof. See [17, p. 9] for a proof. □

[1] Recall our assumption about rings.

The next proposition will show why the norm and trace are useful tools in the study of integral elements.

Proposition 1.4. *If $x \in \mathcal{O}_L$, then Trace$_{L/K}(x)$ and Norm$_{L/K}(x)$ is in $\mathcal{O}_K$. Furthermore, x is a unit in $\mathcal{O}_L$ if and only if Norm$_{L/K}(x)$ is a unit in $\mathcal{O}_K$.*

Proof. See [17, p. 12] for a proof. □

We have seen that a number field L can be given a finite dimensional $\mathbb{Q}$-vector space structure. What about the ring of integers $\mathcal{O}_L$, can it be described as a free $\mathbb{Z}$-module? The answer to this question is yes. In fact, the ring of integers $\mathcal{O}_L$ of an extension L/K is a free $\mathcal{O}_K$-module if $\mathcal{O}_K$ is a principal ideal domain.

Proposition & Definition 1.5. *If L/K is an extension of number fields and $\mathcal{O}_K$ is a principal ideal domain, then there exists a K-vector space basis $\{b_1, \ldots, b_n\}$ of L such that*

$$\mathcal{O}_L = \bigoplus_{i=1}^{n} \mathcal{O}_K\{b_i\}.$$

The basis $\{b_1, \ldots, b_n\}$ is called an integral basis.

Proof. See [17, p. 12-13] for a proof. □

Definition 1.6. Let $\{b_1, \ldots, b_n\}$ be an integral basis for K as a $\mathbb{Q}$-vector space. The number $\mathrm{d}(b_1, \ldots, b_n)$ defined by

$$\mathrm{d}(b_1, \ldots, b_n) = \det((\sigma_i b_j))^2,$$

where the σ_i's are the $\mathbb{Q}$-embedding of K in $\mathbb{C}$, is called the discriminant of K.

The discriminant turns out to be independent of the choice of integral basis (see [17, p. 14-15] for details). We will later see that the discriminant contains useful information about the "size" of the ring of integers, and also about the ramification of prime ideals in $\mathcal{O}_K$.

Proposition 1.7. *If $D \in \mathbb{Z}$ is square free, then the ring of integers of the quadratic number field $\mathbb{Q}(\sqrt{D})$ is*

$$\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \begin{cases} \mathbb{Z}[\frac{1+\sqrt{D}}{2}] & \text{if } D \equiv 1 \bmod 4 \\ \mathbb{Z}[\sqrt{D}] & \text{otherwise,} \end{cases}$$

and the discriminant

$$d_{\mathbb{Q}(\sqrt{D})} = \begin{cases} D & \text{if } D \equiv 1 \bmod 4 \\ 4D & \text{otherwise.} \end{cases}$$

Proof. For an elementary proof see [10, p. 189]. □

1.2 Ideal Class Group

One of the main goals of number theory is to determine which rings of integers have unique factorization in terms of prime (irreducible) elements. The classical example of a ring of integers without unique factorization is $\mathbb{Z}[\sqrt{-5}]$, where we can factor 6 as $2 \cdot 3$ and $(1+\sqrt{-5})(1-\sqrt{-5})$. Although unique factorization may fail for elements, it is in any noetherian ring possible to factor proper ideals into a unique finite intersections of primary ideals. See [1, p.83] for details. This leads to the notion of the ideal class group, which, loosely speaking, measures how far away a ring of integers is from having unique factorization.

Definition 1.8. An ideal I is said to be primary if $xy \in I$ implies that either $x \in I$ or $y^n \in I$ for some $n \in \mathbb{N}$.

Furthermore, for a class of rings called Dedekind domains, we can replace the finite intersection of primary ideals with a finite product of prime ideals.

Proposition 1.9. *Let A be a Dedekind domain and $I \subset A$ any ideal. Then there exist finitely many prime ideals $P_1, \ldots, P_n$ such that*

$$I = P_1^{e_1} \cdots P_n^{e_n}.$$

Proof. See [1, p.95] for a proof. □

A noetherian integral domain is called Dedekind if it has dimension 1 and is integrally closed in its field of fractions. The class of Dedekind domains provides a natural environment for the study of rings of integers.

Theorem 1.10. *The ring of integers in a number field is a Dedekind domain.*

Proof. See [1, p.96] for a proof. □

Definition 1.11. Let A be a Dedekind domain with fraction field K. A fractional ideal I is a non-zero finitely generated A-submodule of K. If I is generated by one element, i.e. $I = cA$ for some $c \in K$, we say that I is a principal fractional ideal.

Since all fractional ideals are A-submodules of K, it makes sense to multiply elements of two different fractional ideals. We can therefore define a multiplication of two fractional ideals I and J by defining IJ as the A-submodule of K consisting of all the products xy, where $x \in I$ and $y \in J$. If I is generated by (v_i) and J is generated by (w_j), then clearly IJ will be generated by $(v_i w_j)$.

Definition 1.12. Let I be a fractional ideal. The set $I^{-1} = \{x \in K | xI \subset A\}$ is called the inverse of I.

Lemma 1.13. *The inverse I^{-1} of a fractional ideal I is also a fractional ideal.*

Proof. Suppose that $a_1, \ldots, a_n$ generate I, and that $a_1, \ldots, a_k$ are the generators that are not in A. If all of the generators are in A, then clearly $A \subset I^{-1}$ and $I \neq \emptyset$. If not, let a_i be represented by the fraction r_i/s_i, and consider the element $c = s_1^{-1} \cdots s_k^{-1}$. It is clear that $cI \subset A$, hence that $c \in I^{-1}$. The inverse I^{-1} is therefore non-zero. It remains to show that I^{-1} is finitely generated as an A-module. Let $x \in I$ be non-zero. Clearly $xI^{-1} \subset A$. Since A is noetherian, we can conclude that xI^{-1} is finitely generated, and also that $x^{-1}xI^{-1} = I^{-1}$ is finitely generated. □

Let $\mathcal{J}_A$ denote the set of all fractional ideals of a Dedekind domain A.

Proposition 1.14. *The set $\mathcal{J}_A$ forms an abelian group under multiplication, with $A = (1)$ as the unit.*

Proof. Let I and J be fractional ideals. Clearly $IJ = JI$ is a fractional ideal and $(1)I = I(1) = I$. It therefore remains to show that $II^{-1} = A = (1)$.

By the definition of I^{-1}, it is clear that $II^{-1} \subset A$. Suppose that I is generated by $a_1, \ldots, a_n$, where $a_1, \ldots, a_k$ are the only generators that are not in A. Let $x = (a_1 \cdots a_r)^{-1}$. It is clear that $x \in I^{-1}$, and hence that $1 = a_1 \cdots a_r x \in II^{-1}$. □

Remark 1.15. For every fractional ideal I, there exists an element $c \in A$ such that $cI = (c)I \subset A$. By Proposition 1.9, $(c)I$ can be factored uniquely into a product of prime ideals, $(c)I = P_1^{e_1} \cdots P_n^{e_n}$. We can also factor (c) in a unique way as a product of prime ideals, $(c) = Q_1^{e'_1} \cdots Q_m^{e'_m}$. Hence

$$I = P_1^{e_1} \cdots P_n^{e_n} Q_1^{-e'_1} \cdots Q_m^{-e'_m}.$$

The factorization is also independent of the choice of c. We can therefore conclude that $\mathcal{J}_A$ is the free abelian group on the set of non-zero prime ideals.

The map $f : K^\times \to \mathcal{J}_A$ given by $x \mapsto (x)A$, is a group homomorphism with kernel $A^\times$, the units of A. The image of f is the subgroup of principal fractional ideals, denoted by $\mathcal{P}_A$.

Definition 1.16. The ideal class group $\mathrm{Cl}(A)$ is the quotient group $\mathcal{J}_A/\mathcal{P}_A$.

The class group is also the cokernel of f, and fits into the following exact sequence

$$1 \longrightarrow A^\times \longrightarrow K^\times \xrightarrow{f} \mathcal{J}_A \longrightarrow \mathrm{Cl}(A) \longrightarrow 1.$$

The sequence above shows us that the units $A^\times$ and the ideal class group $\mathrm{Cl}(A)$, measure how far off f is from being an isomorphism. In other words, they measure, respectively, what is "lost" and what one has to "add" when passing from elements (numbers) to ideals. For example A, is a unique factorization domain if and only if $\mathrm{Cl}(A) = 0$.

From now on we will only be interested in the case where A is the ring of integers $\mathcal{O}_K$ of a number field K.

Definition 1.17. The absolute norm $N(I)$ of an ideal $I \subset \mathcal{O}_K$ is defined by

$$N(I) = |\mathcal{O}_K/I| \in \mathbb{N}_{>0},$$

and is a positive natural number.

If (a) is a principal ideal, then $N((a)) = |\mathrm{Norm}_{K/\mathbb{Q}}(a)|$. The absolute norm also distributes over products of ideals.

Proposition 1.18 (Minkowski Bound Theorem)**.** *Let L be a number field of degree n. Then for every fractional ideal I, there exists an ideal I' and an element a, such that $aI = I'$ and*

$$N(I') \leq \frac{n!}{n^n}\Big(\frac{4}{\pi}\Big)^s \sqrt{|d_L|},$$

where s is the number of pairs of complex embeddings of L.

Proof. See [17, p. 34] for a proof. □

The number $\frac{n!}{n^n}(\frac{4}{\pi})^s\sqrt{|\mathrm{d}_L|}$ is called the Minkowski Bound of L.

Theorem 1.19. *The ideal class group of a number field $\mathrm{Cl}(L)$ is finite.*

Proof. The result follows immediately from the Minkowski Bound Theorem. □

Remark 1.20. From the proof of Lemma 1.13 it is clear that every fractional ideal I can be written as a product $I = (a)I'$ of an ideal I' and a principal fractional ideal (a). We can therefore represent every class in the ideal class group by an ideal. The ideal classes to prime ideals with norm less than the Minkowski Bound, will therefore generate the ideal class group.

Example 1.21. Let $K = \mathbb{Q}(\sqrt{-5})$. The discriminant $d_K = -20$, which gives the Minkowski Bound

$$N(I) \leq \frac{2}{2^2}(\frac{4}{\pi})\sqrt{20} = \frac{4}{\pi}\sqrt{5} < 3.$$

We have seen that $\mathcal{O}_K$ is not a unique factorization domain, hence $\mathrm{Cl}(K) \neq 0$. From Remark 1.20 we can conclude that $\mathrm{Cl}(L)$ is generated by the prime ideals above 2. In the next chapter we will see that the prime number 2 ramifies in all quadratic extensions $\mathbb{Q}(\sqrt{D})$ when $D = 2, 3 \mod 4$, hence

$$\mathrm{Cl}(L) \approx \mathbb{Z}/2.$$

1.3 Galois Theory

We will mostly use Galois theory in the study of ideal factorization. Central to this scheme is the Hilbert ramification theory, but first some general theory will be presented.

Definition 1.22. An extension L/K of number fields is Galois if every embedding of $\sigma : L \hookrightarrow \mathbb{C}$, that is the identity on K, maps L onto itself.

Definition 1.23. If L/K is a Galois extension of number fields, we define the Galois group $\mathrm{Gal}(L/K)$ of L/K to be the group of automorphisms $\{\sigma : L \to L \mid \sigma_{|K} = \mathrm{id}_K\}$.

Proposition 1.24. *If $L/M/K$ is a tower of Galois extensions, we have the following relation between the Galois groups Gal(L/K), Gal(L/M) and Gal(M/K):*

$$\textit{Gal}(L/K)/\textit{Gal}(L/M) = \textit{Gal}(M/K).$$

Proof. See [6, p. 451] for a proof. □

Furthermore, if $N \subset \text{Gal}(L/K)$ is a normal subgroup then the fixpoints $L^N = \{x \in L | \sigma x = x \text{ for all } \sigma \in N\}$ is a Galois extension of K with Galois group $\text{Gal}(M/K)/N$. We have the following correspondence:

Proposition 1.25. *There is a one-to-one inclusion reserving correspondence between normal subgroups N of Gal(L/K) and Galois subfields $L \subset M \subset K$. The correspondence is given by*

$$N \mapsto L^N.$$

Proof. See [6, p. 451] for a proof. □

Suppose that a is an integral element in K. It is easy to check that σa is also an integral element in K for all $\sigma \in \text{Gal}(L/K)$. Furthermore, if $P \subset \mathcal{O}_K$ is a prime ideal, $\sigma(P)$ is also a prime ideal. We will therefore have well-defined group actions of the Galois group on both $\mathcal{O}_K$ and the set of prime ideals in $\mathcal{O}_K$. The latter action can easily be extended to the ideal class group.

Let L/K be an extension of number fields. Every prime ideal $P \subset \mathcal{O}_L$ lies above a unique prime ideal $p = \mathcal{O}_K \cap P$. The ideal $p\mathcal{O}_L$ factors as a product

$$p\mathcal{O}_L = P_1^{e_1} \cdots P_r^{e_r},$$

where the P_i's are the prime ideals above p. The number e_i is called the ramification index of P_i. By dividing out by p and P_i, we get a finite field extension

$$\begin{array}{c} \mathcal{O}_L/P_i \\ | \\ \mathcal{O}_K/p. \end{array}$$

The degree of this extension $f_i = [\mathcal{O}_L/P_i : \mathcal{O}_K/p]$ is called the inertia degree.

Proposition 1.26. *If L/K is a finite extension of degree n, and $p \subset \mathcal{O}_K$ is a prime ideal, then*

$$\sum_{i=1}^{r} e_i f_i = n.$$

Proof. See [17, p. 46] for a proof. □

Remark 1.27. In some cases we can explicitly find the factorization of a given prime ideal. Suppose that $L = K(\theta)$, where θ is a primitive element with minimal polynomial h. Also suppose that $p \subset \mathcal{O}_K$ is a prime ideal that is relatively prime to the conductor $\mathcal{F} = \{a \in \mathcal{O}_L \mid a\mathcal{O}_L \subset \mathcal{O}_K[\theta]\}$. Let

$$\bar{h} = \bar{h}_1^{e_1} \cdots \bar{h}_r^{e_r}$$

be the factorization of $\bar{h} = h \mod p \in (\mathcal{O}_K/p)[x]$. If we choose monic $h_i \in \mathcal{O}_K[x]$ such that $\bar{h}_i = h_i \mod p$, we can factorize

$$p = P_1^{e_1} \cdots P_r^{e_r},$$

where $P_i = (p, h_i(\theta))\mathcal{O}_L$. See [17, p. 47] for more details.

If $r = n = [L : K]$, we say that p is totally split. If $e_i \neq 1$ for some i, we say that p is ramified and in the case where $e_1 = n$, we say that it is totally ramified. If $r = 1$, $e_1 = 1$ and $f_1 = n$, we say that p is inert.

It turns out that there is only a finite number of prime ideals that ramify. Ramification is also totally controlled by the discriminant.

Proposition 1.28. *If L/K is an extension of number fields with discriminant $d_{L/K}$, then a prime ideal $p \subset \mathcal{O}_K$ ramifies if and only if it contains the principal ideal $(d_{L/K})\mathcal{O}_K$.*

Proof. See [17, p. 201-202] for a proof. □

Corollary 1.29. *In an extension of number fields, ramification occurs for only a finite number of prime ideals.*

Proof. There is only a finite number of primes that contain $(d_{L/K})\mathcal{O}_K$, so the result follows directly from Proposition 1.28. □

Let L/K be a Galois extension of number fields and $P \subset \mathcal{O}_L$ a prime above $p \subset \mathcal{O}_K$. Since $\sigma \in \text{Gal}(L/K)$ fixes K, it also fixes p, hence $\sigma(P)$ is above p for all $\sigma \in \text{Gal}(L/K)$. If $p = P_1^{e_1} \cdots P_k^{e_k}$, then $\text{Gal}(L/K)$ permutes the P_i transitively. Furthermore, if $\sigma \in \text{Gal}(L/K)$ maps P_i to P_j, it induces an isomorphism $\bar{\sigma} : \mathcal{O}_L/P_i \to \mathcal{O}_L/P_j$, so $e_i = e_j$ and $f_i = f_j$ for all i, j. We can therefore conclude that if L/K is a Galois extension, then the equation of Proposition 1.28 turns into

$$n = efr.$$

Definition 1.30. If P is a prime ideal of $\mathcal{O}_L$, then the subgroup

$$G_P = \{\sigma \in \text{Gal}(L/K) \mid \sigma P = P\}$$

of $\text{Gal}(L/K)$ is called the decomposition group of P. The field

$$Z_P = \{x \in L \mid \sigma x = x \text{ for all } \sigma \in G_P\}$$

is called the decomposition field of P.

A prime ideal $p \subset \mathcal{O}_K$ splits completely in $\mathcal{O}_{Z_P}$, and the prime ideal $P \cap \mathcal{O}_{Z_P}$ is the only prime ideal in $\mathcal{O}_{Z_P}$ that is below P, i.e. $[L : Z_P] = ef$.

The field extension $(\mathcal{O}_L/P)/(\mathcal{O}_K/p)$ is normal, and we get a surjective group homomorphism

$$\phi : \text{Gal}(L/K)_P \to \text{Gal}((\mathcal{O}_L/P)/(\mathcal{O}_K/p)).$$

For a more detailed description of the theory above, we refer the reader to [17, p. 55-56].

Definition 1.31. Let I_P denote the kernel of

$$\phi : \text{Gal}(L/K) \to \text{Gal}((\mathcal{O}_L/P)/(\mathcal{O}_K/p)).$$

The subgroup I_P is called the inertia group of P over K. The fixed field $T_P = \{x \in L \mid \sigma x = x \text{ for all } \sigma \in I_P\}$ is called the inertia field of P over K.

Theorem 1.32. *Let L/K be Galois and $P \subset \mathcal{O}_L$ prime above $p \subset \mathcal{O}_K$ with $n = efr$. Then the decomposition field and the inertia field fit into a tower of fields*

$$K \subset Z_P \subset T_P \subset L$$

with the following properties:

- *The degree $[Z_P : K] = r$, and p is totally split in Z_P*
- *The degree $[T_P : Z_P] = f$, and $P \cap Z_T$ is inert in T_P*
- *The degree $[L : T_P] = e$, and $P \cap T_P$ is totally ramified in L*

Proof. For a proof see [17, p. 56-58]. □

Example 1.33. Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{D})$, where D is squarefree. From Corollary 1.7, we know that the ring of integers $\mathcal{O}_L$ is given by

$$\mathcal{O}_L = \begin{cases} \mathbb{Z}[\sqrt{D}] & \text{if } D \equiv 2, 3 \bmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{D}}{2}] & \text{otherwise,} \end{cases}$$

and that the discriminant d_L is given by

$$d_L = \begin{cases} 4D & \text{if } D \equiv 2, 3 \bmod 4 \\ D & \text{otherwise.} \end{cases}$$

Since every quadratic number field is Galois and of degree two over $\mathbb{Q}$, there are three different ways in which we can factor a prime ideal. If $e = 2$, p will ramify completely. If $f = 2$, p will be inert, and if $r = 2$, p will split completely.

If $D \equiv 2, 3 \bmod 4$, the conductor equals (1). On the other hand, if $D \equiv 1 \bmod 4$, the conductor equals (2), so for odd primes p we get:

- p ramifies if and only if $p \mid D$
- p is inert if and only if $x^2 - D \bmod p$ is not solvable and $p \nmid D$
- p is totally split if and only if $x^2 - d \bmod p$ is solvable and $p \nmid D$

If $p = 2$, then p ramifies if and only if $D \equiv 2, 3 \bmod 4$. For the last cases, assume that $D \equiv 1 \bmod 4$. We will write $L = \mathbb{Q}(\frac{1+\sqrt{D}}{2})$. The primitive element $\frac{1+\sqrt{D}}{2}$ has a minimal polynomial $h = x^2 - x + \frac{1-D}{4}$, and the conductor is (1). The polynomial $h \bmod 2$ is solvable if and only if $\frac{1-D}{4} \equiv 0 \bmod 2$, which is equivalent to $D \equiv 1 \bmod 8$. Therefore, when $p = 2$, we find that:

- 2 ramifies if and only if $D \equiv 2, 3 \bmod 4$
- 2 is inert if and only if $D \equiv 5 \bmod 8$
- 2 splits if and only if $D \equiv 1 \bmod 8$

2 The Reflection Theorem

In 1932, Arnold Scholz published an article *Über die Beziehung der Klassenzahlen quadratizcher Körper zueinander* in *Journal für die reine und angewandte Mathematik 166*, in which he formulated and proved what would later be known as the reflection theorem.

Theorem 2.1 (The Reflection Theorem)**.** *If D is positive and squarefree, then the following formula holds:*

$$\mathrm{rk}_3\ \mathrm{Cl}(\mathbb{Q}(\sqrt{D})) \leq \mathrm{rk}_3\ \mathrm{Cl}(\mathbb{Q}(\sqrt{-3D})) \leq \mathrm{rk}_3\ \mathrm{Cl}(\mathbb{Q}(\sqrt{D})) + 1.$$

In this section we will go through the proof of the reflection theorem that is given in Lawrence C. Washington's *Introduction to Cyclotomic Fields*. The proof uses results from representation theory, class field theory and Kummer theory, in addition to the basic number theory that we went through in Section 1.

Recall that the p-rank $\mathrm{rk}_p G$ of a finite abelian group G is the vector space dimension of $\mathbb{F}_p \otimes_{\mathbb{Z}} G$ as a $\mathbb{F}_p$ vector space. The p-rank is also equal to the number of generators of the Sylow p-subgroup of G. If A is the p-Sylow subgroup of G, we have

$$\mathrm{rk}_p\ G = \mathrm{rk}_p\ A = \dim_{\mathbb{Z}/(p)}\ \mathbb{Z}/(p) \otimes_{\mathbb{Z}} A = \dim_{\mathbb{Z}/(p)}\ A/pA.$$

Let G be an abelian group, and let R be a ring. The group ring $R[G]$ consists of elements $\sum_{g\in G} a_i g_i$, $a_i \in R$, with only finitely many a_i different from 0. Multiplication and addition in the group ring $R[G]$ are defined in the obvious way.

If G is an abelian group, we will denote $\hat{G} = \mathrm{Hom}(G, \mathbb{C}^\times)$, the character group of G.

Definition 2.2. Let G be a finite abelian group and $\hat{G}$ the character group. The elements

$$\varepsilon_\phi = \frac{1}{|G|} \sum_{g\in G} \phi(g) g^{-1} \in \mathbb{C}[G],$$

where $\phi \in \hat{G}$, are called the orthogonal idempotents of the group ring $\mathbb{C}[G]$.

The name "orthogonal idempotents" stems from the following set of properties

Lemma 2.3. *The orthogonal idempotents satisfy*

(i) $\varepsilon_\phi^2 = \varepsilon_\phi$

(ii) $\varepsilon_\phi \varepsilon_\theta = 0$ *if* $\phi \neq \theta$

(iii) $1 = \sum_{\phi\in\hat{G}} \varepsilon_\phi$

(iv) $\varepsilon_\phi g = \phi(g)\varepsilon_\phi$ *for all* $g \in G$.

Proof. The properties (i), (ii), (iii) and (iv) are proved by straightforward calculations, and will therefore be left to the reader. □

Let R be a ring and G a group, such that $|G|^{-1} \in R$. Also suppose that there exists a subgroup $N \subset R^\times$ such that $\mathrm{Hom}(G, N) \approx \mathrm{Hom}(G, \mathbb{C}^\times)$. By letting $\hat{G} = \mathrm{Hom}(G, N)$, we can define orthogonal idempotents in $R[G]$ by the same recipe as for $\mathbb{C}[G]$. The properties of Lemma 2.3 will clearly hold in this more general setting.

If R is such a ring and M is an $R[G]$-module, we may from the properties (i), (ii) and (iii) decompose M as

$$M = \bigoplus_{\phi \in \hat{G}} \varepsilon_\phi M.$$

Example 2.4. Let $R = \mathbb{Z}_p$ be p-adic integers, and let $A \subset \mathrm{Cl}(\mathbb{Q}(\zeta_p))$ be the p-Sylow subgroup. Since $(A)^{p^k} = 1$ for $k >> 0$, we can consider A as a $\mathbb{Z}_p$-module. The module structure is given by the following multiplication: If $s = \sum a_i p^i \in \mathbb{Z}_p$ and $I \in A$, then

$$sI = I^{\sum a_i p^i} = I^{\sum_{i=0}^{k} a_i p^i}.$$

The Galois group $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p))$ also acts on A. We can therefore decompose

$$A = \bigoplus_{i=1}^{p-1} \epsilon_i A$$

as a $\mathbb{Z}_p[G]$-module.

A finite extension of number fields L/K is called unramified if every prime ideal $p \subset \mathcal{O}_K$ is unramified in $\mathcal{O}_L$. It is also called abelian if $\mathrm{Gal}(L/K)$ is abelian. Let K be a number field. The maximal unramified abelian field extension L/K, is called the Hilbert class field of K. The next well-known result belongs to class field theory.

Theorem 2.5. *Let L be the Hilbert class field of an number field K. Then*

$$\mathrm{Gal}(L/K) \approx \mathrm{Cl}(K).$$

Proof. See [17, p. 399] for a proof. □

Consider the Galois extension L/K, with Galois group $G = \mathrm{Gal}(L/K)$. Let M be the Hilbert class field of L. If $\tilde{\sigma} \in \mathrm{Gal}(M/K)$ is some extension of $\sigma \in G$, then

$$\tilde{\sigma}^{-1} \phi \tilde{\sigma} \in \mathrm{Gal}(M/L), \text{ for } \phi \in \mathrm{Gal}(M/L).$$

The automorphism $\tilde{\sigma}^{-1} \phi \tilde{\sigma}$ is also independent of the choice of the extension of σ. We can therefore act on $\mathrm{Gal}(M/L)$ by elements of G. This action makes $\mathrm{Gal}(M/L)$ into a $\mathbb{Z}[G]$-module, and the isomorphism in Theorem 2.5 into a $\mathbb{Z}[G]$-isomorphism ([24, p. 188]).

If L/K is a Galois extension of number fields and M is the Hilbert class field of L, then the subgroup $N = (\mathrm{Cl}(L))^p$ of $\mathrm{Cl}(L)$ corresponds to a subfield $L' \subset M$ by the fundamental theorem of Galois. This gives us a tower of fields

$$\mathbb{Q} \text{ —— } K \text{ —— } L \text{ —— } L' \text{ —— } M,$$

where $G = \text{Gal}(L/K)$, $(\text{Cl}(L))^p = \text{Gal}(M/L')$ and

$$\text{Gal}(L'/L) = \text{Cl}(L)/(\text{Cl}(L))^P \approx A/A^p,$$

where A is the p-Sylow subgroup of $\text{Cl}(L)$. The last group is not only a p-group, but is also elementary.

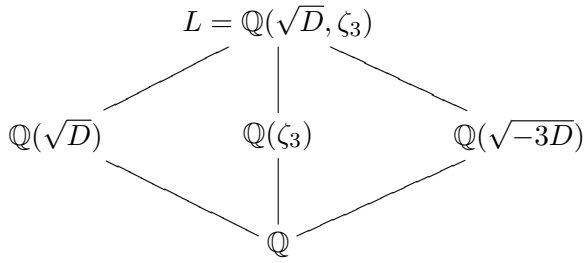
Definition 2.6. Let K be a number field, and suppose that a primitive n-th root of unity ζ_n is in K. The field extension L/K is called a Kummer extension if $\text{Gal}(L/K)$ is abelian with group exponent n.

Lemma 2.7. *Let L/K be a Kummer extension of exponent n. Then there exists a subgroup $B \subset K^\times/(K^\times)^n$ such that $L = K(\sqrt[n]{B})$.*

Proof. See [17, p. 278] for a proof. □

We are now ready to prove the Reflection Theorem.

Proof of the Reflection Theorem. Let $L = \mathbb{Q}(\sqrt{D}, \zeta_3)$ and $G = \text{Gal}(L/Q)$. The number field L has three quadratic subfields:



The first objective of the proof is to decompose the 3-Sylow subgroups A of $\text{Cl}(L)$ as a direct sum of the 3-Sylow subgroup $A_{\mathbb{Q}(\sqrt{D})}$ and $A_{\mathbb{Q}(\sqrt{-3D})}$ of $\text{Cl}(\mathbb{Q}(\sqrt{D}))$ and $\text{Cl}(\mathbb{Q}(\sqrt{-3D}))$, respectively.

Let

$$\begin{aligned} \{1, \tau\} &= \text{Gal}(L/\mathbb{Q}(\sqrt{D})), \\ \{1, \sigma\} &= \text{Gal}(L/\mathbb{Q}(\sqrt{-3D})) \text{ and} \\ \{1, \sigma\tau\} &= \text{Gal}(L/\mathbb{Q}(\zeta_3)). \end{aligned}$$

The elements of the character group $\hat{G}$ map G to the multiplicative group $\{\pm 1\} \subset \mathbb{C}^\times$. We can therefore decompose the identity element in the the group ring $\mathbb{Z}_3[G]$ as a sum of the orthogonal idempotents

$$1 = \varepsilon_1 + \varepsilon_2 + \varepsilon_3 + \varepsilon_4.$$

The orthogonal idempotents are

$$\begin{aligned}
\varepsilon_1 &= \Big(\frac{1+\tau}{2}\Big)\Big(\frac{1+\sigma}{2}\Big),\\
\varepsilon_2 &= \Big(\frac{1+\tau}{2}\Big)\Big(\frac{1-\sigma}{2}\Big),\\
\varepsilon_3 &= \Big(\frac{1-\tau}{2}\Big)\Big(\frac{1+\sigma}{2}\Big) \text{ and}\\
\varepsilon_4 &= \Big(\frac{1-\tau}{2}\Big)\Big(\frac{1-\sigma}{2}\Big).
\end{aligned}$$

Let A denote the 3-Sylow subgroup of the ideal class group of L. As in Example 2.4, we can make A into a $\mathbb{Z}_3[G]$-module and decompose it as $A = \oplus\varepsilon_i A$.

If $a \in A$ then $\varepsilon_1 a = \frac{1}{4}a\sigma(a)\tau(a)\sigma\tau(a) = \frac{1}{4}\text{Norm}_{L/\mathbb{Q}}(a)$, so $\varepsilon_1 A = 1$. Similarly, we see that

$$\begin{aligned}
\varepsilon_2 &= \frac{1}{4}(1-\sigma)\text{Norm}_{L/\mathbb{Q}(\sqrt{D})},\\
\varepsilon_3 &= \frac{1}{4}(1-\tau)\text{Norm}_{L/\mathbb{Q}(\sqrt{-3D})} \text{ and}\\
\varepsilon_4 &= \frac{1}{4}(1-\tau)\text{Norm}_{L/\mathbb{Q}(\zeta_3)}.
\end{aligned}$$

Since $\text{Cl}(\mathbb{Q}(\zeta_3)) = 1$, $\varepsilon_4 A = 1$ and

$$A = \varepsilon_2 A \oplus \varepsilon_3 A.$$

If we can show that $\varepsilon_2 A = A_{\mathbb{Q}(\sqrt{D})}$ and $\varepsilon_3 A = A_{\mathbb{Q}(\sqrt{-3D})}$, then our first objective will be achieved. Since $\varepsilon_2 = \frac{1}{4}(1-\sigma)\text{Norm}_{L/\mathbb{Q}(\sqrt{D})}$, the inclusion $\varepsilon_2 A \subset A_{\mathbb{Q}(\sqrt{D})}$ is clear. On the other hand, we may consider $A_{\mathbb{Q}(\sqrt{D})}$ as a subgroup of A. This gives us

$$\varepsilon_2 A = \varepsilon_2^2 A \subset \varepsilon_2 A_{\mathbb{Q}(\sqrt{D})} \subset \varepsilon_2 A.$$

If $I \in A_{\mathbb{Q}(\sqrt{D})}$, it is clear that $\tau I = I$ and $(1+\sigma)I = 1$. Thus $\sigma I = I^{-1}$ and

$$\frac{1}{4}(1-\sigma)(1+\tau)I = (I^4)^{\frac{1}{4}} = I.$$

We can therefore conclude that $\varepsilon_2 A_{\mathbb{Q}(\sqrt{D})} = A_{\mathbb{Q}(\sqrt{D})}$, and that

$$\varepsilon_2 A \subset A_{\mathbb{Q}(\sqrt{D})} \subset \varepsilon_2 A.$$

Similarly, it follows that $\varepsilon_3 A = A_{\mathbb{Q}(\sqrt{-3D}))}$.

We will now use Kummer theory in the form of Lemma 2.7 and Class Field theory in the form of Theorem 2.5 to compare the size of $A_{\mathbb{Q}(\sqrt{D})}$ and $A_{\mathbb{Q}(\sqrt{-3D})}$.

Let L' be the subfield of the Hilbert class field of L such that the Galois group

$$H = \text{Gal}(L'/L) \approx A/A^3.$$

Since L' is a Kummer extension of exponent 3, there exists a $\mathbb{Z}_3[G]$-submodule $B \subset L^\times/(L^\times)^3$ such that $L' = L(\sqrt[3]{B})$. Let $H \times B$ be the $\mathbb{Z}_3[G]$-module given by the diagonal action. Define

$$\phi : H \times B \to \mu_3,$$

where μ_3 is the group of 3-roots of unity, by

$$\phi(h, b) = \frac{h(\sqrt[3]{b})}{\sqrt[3]{b}}.$$

Since $\zeta_3 \in L$, G acts on μ_3, making it a $\mathbb{Z}_3[G]$-module. Consider $H \times B$ as a G-module equipped with the diagonal action. Note that

$$gb = g(\sqrt[3]{b})^3 = (\tilde{g}\sqrt[3]{b})^3,$$

where $\tilde{g}$ is some extension of g, so we get that

$$\sqrt[3]{gb} = \zeta_3^i \tilde{g}\sqrt[3]{b}$$

for some i. This gives us

$$\begin{aligned}
\phi(h^g, b^g) &= \frac{\tilde{g}h\tilde{g}^{-1}(\sqrt[3]{gb})}{(\sqrt[3]{gb})} \\
&= \frac{\tilde{g}h\tilde{g}^{-1}\zeta_3^i\tilde{g}\sqrt[3]{b}}{\zeta_3^i\tilde{g}\sqrt[3]{b}} \\
&= \frac{\zeta_3^i\tilde{g}h\tilde{g}^{-1}\tilde{g}\sqrt[3]{b}}{\zeta_3^i\tilde{g}\sqrt[3]{d}} \\
&= \frac{\tilde{g}h\sqrt[3]{b}}{\tilde{g}\sqrt[3]{b}} \\
&= g\Big(\frac{h\sqrt[3]{b}}{\sqrt[3]{b}}\Big),
\end{aligned}$$

and hence that ϕ is G-equivariant.

The map $b \mapsto \phi(-, b)$ from B to $\mathrm{Hom}(H, \mu_3) = \hat{H}$, is clearly injective. It is also surjective, since for every i, there is an h such that $h(b^{\frac{1}{3}}) = \zeta_3^i b^{\frac{1}{3}}$. Hence ϕ is nondegenerate. This gives us isomorphisms

$$B \approx \hat{H} \approx H \approx A/A^3,$$

where the second isomorphism is neither G-linear nor canonical. Since the last isomorphism is G-linear,

$$\varepsilon_i H \approx \varepsilon_i A/A^3$$

for all i. In particular, $\varepsilon_1 H = \varepsilon_4 H = 1$ so

$$\phi(\varepsilon_i H, \varepsilon_j B) = 1, \text{ for } i = 1, 4.$$

Let $h \in \varepsilon_2 H$, and let $I \in \varepsilon_2(A/A^3)$ be the image of h under the isomorphism $\varepsilon_2 H \approx \varepsilon_2 A/(A)^3$. Since $\varepsilon_2 A = A_{\mathbb{Q}(\sqrt{D})}$, we can consider I as an element of $A_{\mathbb{Q}(\sqrt{D})}/(A_{\mathbb{Q}(\sqrt{D})})^3$. It follows that $\sigma I = I^{-1}$ and $\tau I = I$, so $\sigma h = h^{-1}$ and $\tau h = h$. Similarly, if $h \in \varepsilon_3 H$, then $\sigma h = h$ and $\tau h = h^{-1}$.

If b is in $\varepsilon_1 B$, then b is also in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^3$, and $\sigma b = \tau b = b$. On the other hand, if b is in $\varepsilon_2 B$, we only know that $\tau b = b$. Similarly, we know that $\sigma a = a$ and $\sigma\tau b = b$ for $a \in \varepsilon_3 B$ and $b \in \varepsilon_4 B$, respectively.

Assume that $h \in \varepsilon_2 H$, $b \in \varepsilon_1 B$. Since $\tau h = h$ and $\tau b = b$,

$$\phi(h, b) = \phi(\tau h, \tau b) = \tau\phi(h, b).$$

On the other hand, τ does not act trivially on $\mathbb{Q}(\zeta_3)$ so $\phi(h, b) = 1$. Similar arguments show that

$$\phi(h, b) = 1$$

when $h \in \varepsilon_i H$ and $b \in \varepsilon_j B$ for pairs

$$(i, j) \in \{(2, 2), (3, 1), (3, 3), (3, 4)\}.$$

For $i = 2, 3$, $h \in \varepsilon_i H$ and $b \in \varepsilon_4 B$, we see that

$$\phi(h, b)^{-1} = \phi(h^{-1}, b) = \phi(\sigma\tau h, \sigma\tau b) = \sigma\tau\phi(h, b) = \phi(h, b),$$

and hence $\phi(h, b) = 1$. It is therefore clear that

$$\phi(\varepsilon_i H, \varepsilon_j B) = 1,$$

unless $(i, j) = (2, 3), (3, 2)$. Since $\phi : H \times B \to \mu_3$ is nondegenerate,

$$\phi : \varepsilon_2 H \times \varepsilon_3 B \to \mu_3 \text{ and } \phi : \varepsilon_3 H \times \varepsilon_2 B \to \mu_3,$$

have to be nondegenerate as well.

The field $L(\sqrt[3]{b})$ is an unramified extension of L. We can therefore find an ideal I such that $I^3 = (b)$ in $\mathcal{O}_L$ (see exercise 9.1 in [24, p. 182]). Sending each $b \in B$ to the ideal class of the corresponding I, defines a map $\psi : B \to A$. It is welldefined since, if $x^3 \in (L^\times)^3$, then $(x^3 b) = (xI)^3$ and $(x)I$ is in the same ideal class as I. Since $g(b) = (gb) = (gI)^3$, the map is clearly G-linear. Suppose that $\psi(b) = (1)$. Then $(b) = (a)^3$ for some $a \in L$, and hence $b = ua^3$, where u is a unit in $\mathcal{O}_L$, so

$$\ker\psi \subset \mathcal{O}_L^\times/(\mathcal{O}_L^\times)^3.$$

Since ψ is G-linear we, get maps

$$\psi|_{\varepsilon_2 B} : \varepsilon_2 B \to \varepsilon_2 A,$$

$$\psi|_{\varepsilon_3 B} : \varepsilon_3 B \to \varepsilon_3 A,$$

and $\ker\psi \cap \varepsilon_2 B$ is a subgroup of $\varepsilon_2(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^3)$. Similarly, $\ker\psi \cap \varepsilon_3 B$ is a subgroup of $\varepsilon_3(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^3)$. It is clear that $\varepsilon_2(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^3)$ is contained in $\mathcal{O}^\times_{\mathbb{Q}(\sqrt{D})}/(\mathcal{O}^\times_{\mathbb{Q}(\sqrt{D})})^3$. By the Dirichlet unit Theorem (see for example [17, p. 42]), we can conclude that

$$\varepsilon_2(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^3) \approx 0 \text{ or } \mathbb{Z}/3.$$

Since $\mathbb{Q}(\sqrt{-3D}) \neq \mathbb{Q}(\zeta_3)$ for $D \neq 1$, we get

$$\varepsilon_3(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^3) = 0.$$

Putting the above together, we get

$$\begin{aligned}
\mathrm{rk}_3\,\mathrm{Cl}(\mathbb{Q}(\sqrt{D})) &= \mathrm{rk}_3\varepsilon_2 A \\
&= \mathrm{rk}_3\,\varepsilon_2 H \\
&= \mathrm{rk}_3\,\varepsilon_3 B \\
&\leq \mathrm{rk}_3\,\varepsilon_3(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^3) + \mathrm{rk}_3\,\varepsilon_3 A \\
&= 0 + \mathrm{rk}_3\,\mathrm{Cl}(\mathbb{Q}(\sqrt{-3D})),
\end{aligned}$$

and

$$\begin{aligned}
\mathrm{rk}_3\,\mathrm{Cl}(\mathbb{Q}(\sqrt{-3D})) &= \mathrm{rk}_3\,\varepsilon_3 A \\
&= \mathrm{rk}_3\,\varepsilon_3 H \\
&= \mathrm{rk}_3\,\varepsilon_2 B \\
&\leq \mathrm{rk}_3\,\varepsilon_2(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^3) + \mathrm{rk}_3\,\varepsilon_2 A \\
&\leq 1 + \mathrm{rk}_3\,\mathrm{Cl}(\mathbb{Q}(\sqrt{D})).
\end{aligned}$$

□

There are examples of both the case where $\mathrm{rk}_3\,\mathrm{Cl}(\mathbb{Q}(\sqrt{D})) = \mathrm{rk}_3\,\mathrm{Cl}(\mathbb{Q}(\sqrt{-3D}))$, and the case where $\mathrm{rk}_3\,\mathrm{Cl}(\mathbb{Q}(\sqrt{D})) + 1 = \mathrm{rk}_3\,\mathrm{Cl}(\mathbb{Q}(\sqrt{-3D}))$.

Example 2.8. By using the computer algebra system PARI/GP (see Section 5), one can easily verify that $D = 79$ is an example where

$$\mathrm{rk}_3\,\mathrm{Cl}\,\mathbb{Q}(\sqrt{79}) = \mathrm{rk}_3\,\mathrm{Cl}\,\mathbb{Q}(\sqrt{-237}) = 1.$$

One can also use PARI/GP to show that $D = 69$ is an example of the case where

$$\mathrm{rk}_3\,\mathrm{Cl}\,\mathbb{Q}(\sqrt{69}) = 0 \text{ but } \mathrm{rk}_3\,\mathrm{Cl}\,\mathbb{Q}(\sqrt{-13}) = 1.$$

3 Classical Algebraic K-theory

Classical algebraic K-theory usually refers to the study of the three functors K_0, K_1 and K_2 from the category of associative rings with multiplicative unit, $Rings$, to the category of abelian groups, Ab. As we will see, there are several equivalent, but different, ways to define the K-functors. It is also not immediately clear how the different K-functors relate to each other. All of this may lead the reader to question the intrinsic value of Algebraic K-theory. On the other hand, there is a big picture theory usually referred to as "higher algebraic K-theory" that generalizes the three classical K-functors. The two most important generalizations are Quillen's Q-construction and Waldhausen's $S_\bullet$-construction. Both of these constructions make it clear how the different K_i's are related and also what type of information they give.

In this section we will define the classical K-functors and study in more detail the structure of $K_2(\mathcal{O}_K)$ for a number field K. The main theorem in the last section is central in our proof of the reflection theorem for K_2.

3.1 The functors K_0, K_1 and K_2

Let R be an associative ring with a multiplicative identity, and denote by $Proj(R)$ the category of finitely generated projective left R-modules. The isomorphism classes of objects in $Proj(R)$ form a set $[Proj(R)]$, and for an R-module M, let $[M]$ be its isomorphism class. We can define a summation $\oplus$ on the set of isomorphism classes by

$$[M] \oplus [N] = [M \oplus N].$$

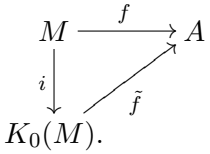
This summation makes the set of isomorphism classes into a commutative monoid with identity the zero module.

Let M be a commutative monoid. The Grothendieck group of M, $K_0(M)$, is the group completion of M. It can be constructed as a quotient

$$K_0(M) = M \times M/\sim,$$

where $(m_1, m_2) \sim (n_1, n_2)$ if there exists a $k \in M$ such that $m_1 + n_2 + k = n_1 + m_2 + k$. The Grothendieck group has the following universal property:

There exists a monoid homomorphism $i : M \to K_0(M)$ such that for every monoid homomorphism $f : M \to A$, where A is an abelian group, there is a unique group homomorphism $\tilde{f} : K_0(M) \to A$, such that the following diagram commutes



Definition 3.1. Let R be an associative ring with a multiplicative identity. The group completion of $[Proj(R)]$ is called the Grothendieck group of R, and is denoted by $K_0(R)$, i.e.

$$K_0(R) = K_0([Proj(R)]).$$

The functor $K_0 : Rings \to Ab$ sends a ring R to the abelian group $K_0(R)$, and a ring homomorphism $f : R \to R'$ to the group homomorphism $K_0(f)$ given on generators by

$$[P] \mapsto [R' \otimes_R P],$$

where $[P]$ is a finitely generated projective left R-module.

Example 3.2. Let F be a field. Since all projective F-modules are free, we get an isomorphism between the monoid $[Proj(F)]$ and $\mathbb{N}$ by mapping $[P]$ to $\dim_F P$. By group completing both the monoids, it is clear that

$$K_0(F) \approx \mathbb{Z}.$$

Remark 3.3. Although $K_0(R)$ contains a lot of information about the "additive" structure of the category $Proj(R)$, it also forgets most of the mapping structure of the same category. Consider for example the two fields $\mathbb{R}$ and $\mathbb{F}_2$. Both $K_0(\mathbb{R})$ and $K_0(\mathbb{F}_2)$ are isomorphic to $\mathbb{Z}$. But the vector space $(\mathbb{F}_2)^2$ is only isomorphic to itself in 6 different ways, while on the other hand $\mathbb{R}^2$ is isomorphic to itself in uncountably many ways.

Let $Aut(Proj(R))$ be the category whose objects are pairs (M, α), where M is an object in $Proj(R)$, and $\alpha : M \to M$ is a isomorphism. A morphism $f : (M, \alpha) \to (N, \beta)$ in $Aut(Proj(R))$ is a morphism $f : M \to N$ in $Proj(R)$ such that $\beta \circ f = f \circ \alpha$.

Definition 3.4. The Bass group $K_1(Proj(R))$ of $Aut(Proj(R))$ is defined as the abelian group with isomorphism classes, $[M, \alpha]$, of $Aut(Proj(R))$ as generators, and subject to the following relations:

$$[M, \alpha] + [N, \beta] = [M \oplus N, \alpha \oplus \beta],$$
$$[M, \alpha] + [M, \alpha\prime] = [M, \alpha \circ \alpha\prime].$$

There is a description of $K_1(Proj(R))$ using the general linear group $GL_n(R)$. We can embed $GL_n(R)$ into $GL_{n+1}(R)$ by mapping a matrix P to the matrix

$$\begin{bmatrix} P & 0 \\ 0 & 1 \end{bmatrix}.$$

This gives us a directed system

$$GL_1(R) \to GL_2(R) \to \cdots GL_n(R) \to \cdots,$$

whose colimit is denoted by $GL(R)$. A matrix m in $GL(R)$ is called elementary if it has only one off-diagonal entry different from 0.

A well known theorem by Whitehead states that

Theorem 3.5. *The subgroup $E(R)$ generated by elementary matrices is the commutator subgroup of $GL(R)$.*

Proof. See [15, §4] for a nice proof. □

Definition 3.6. The first algebraic K-group of R is defined as

$$K_1(R) = GL(R)/E(R) = GL(R)_{ab}.$$

Hyman Bass shows in his *Algebraic K-theory* ([3]) that there is a natural isomorphism between $K_1(Proj(R))$ and $K_1(R)$.

In the case where R is a ring of integers for some number field, both $K_0(R)$ and $K_1(R)$ correspond to classical invariants:

$$K_0(R) \approx \mathbb{Z} \oplus Cl(R) \text{ and}$$

$$K_1(R) \approx R^{\times}.$$

The first isomorphism follows from a result of Steinitz (see [15, p. 9-18]), which says that each finitely generated projective module M is isomorphic to $R^n \oplus I$, where I is a fractional ideal, and is true in general for all Dedekind domains. The second isomorphism is given by the determinant map det : $GL(R) \to R^{\times}$, which was shown to be an isomorphism for rings of integers in number fields by Bass, Milnor and Serre in [2].

Let $e^a_{i,j}$, be the elementary matrix with entry a in the (i,j)-th place. Then

$$e^a_{i,j} e^b_{i,j} = e^{a+b}_{i,j},$$

and for the commutators we have the relations

$$[e^a_{i,j}, e^b_{k,l}] = \begin{cases} 1 & \text{if } j \neq k, i \neq l \\ e^{ab}_{i,l} & \text{if } j = k, i \neq l \\ e^{-ba}_{k,j} & \text{if } j \neq k, i = l. \end{cases}$$

Definition 3.7. For $n \geq 3$, we will define the Steinberg group $St(n,R)$ of R as the group generated by formal symbols $x^a_{i,j}$, $1 \leq i, j, n$ and $a \in R$, subject to the following relations:

(1) $x^a_{i,j} x^b_{i,j} = x^{a+b}_{i,j}$

(2) $[x^a_{i,j}, x^b_{j,l}] = x^{ab}_{i,l}$ for $i \neq l$

(3) $[x^a_{i,j}, x^b_{k,l}] = 1$ if $j \neq k, i \neq l$

We can define a canonical homomorphism

$$\phi_n : St(n,R) \to GL_n(R)$$

for every n, by mapping $x^a_{i,j}$ to $e^a_{i,j}$. By passing to the colimit, we obtain the map

$$\phi = \text{colim } \phi_n : St(R) \to GL(R).$$

Note that $\phi(St(R)) = E(R)$.

Definition 3.8. The kernel of the homomorphism $\phi : St(R) \to GL(R)$ will be called $K_2(R)$.

Theorem 3.9. *The group $K_2(R)$ is the center of the Steinberg group $St(R)$.*

Proof. See [15, §5] for a proof. □

The abelian group K_2 fits into the exact sequence

$$0 \longrightarrow K_2(R) \longrightarrow St(R) \longrightarrow GL(R) \longrightarrow K_1(R) \longrightarrow 0.$$

As Milnor explains in [15, §5], the intuition you should have in mind, is that $K_2(R)$ forms the set of nontrivial relations between elementary matrices, i.e. relations not of the form (1), (2) and (3). In fact, any relation

$$e^{a_1}_{i_1,j_1} e^{a_2}_{i_2,j_2} \cdots e^{a_r}_{i_r,j_r} = I$$

gives rise to an element $x^{a_1}_{i_1,j_1} x^{a_2}_{i_2,j_2} \cdots x^{a_r}_{i_r,j_r}$ in $K_2(R)$ and every element in $K_2(R)$, can be obtained in this way.

Example 3.10. The matrix

$$e^1_{1,2} e^{-1}_{2,1} e^1_{1,2} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

in $E_2(\mathbb{Z})$ represents a 90 degree rotation, and has order 4. This gives rise to an element $(x^1_{1,2} x^{-1}_{2,1} x^1_{1,2})^4$ in $K_2(\mathbb{Z})$. It turns out that

$$K_2(\mathbb{Z}) \approx \mathbb{Z}/2,$$

and generated by $(x^1_{1,2} x^{-1}_{2,1} x^1_{1,2})^4$. See [15, §10] for the complete computation.

There is also another interesting definition of the Steinberg group which is more closely related to group homology.

Definition 3.11. A central extension of a group G consists of a pair (E, ψ), where E is a group and $\psi : E \to G$ is a surjective homomorphism such that $\ker(\psi)$ is a central subgroup of E.

A morphism of central extension (E, ψ) to (E', ψ') is a homomorphism from E to E' over G.

Definition 3.12. A central extension of G is called the universal central extension if it is the initial object in the category of all central extensions of G.

Definition 3.13. A group G is called perfect if $[G, G] = G$.

Since $[G, G] = G$ for a perfect group, $G_{ab} = 1$, and hence the first homology group $H_1(G; \mathbb{Z})$ vanishes.

Proposition 3.14. *A group G admits a universal central extension if and only if G is perfect.*

Proposition 3.15. *There is a canonical isomorphism between the kernel $\ker \psi : E \to G$ of the universal central extension of G, to the second homology group $H_2(G; \mathbb{Z})$.*

The proofs of Propositions 3.14 and 3.15 can be found in [15, p. 45-46].

Since $E(R)$ is a perfect group, and its universal central extension is the Steinberg group (see [15, p. 47-48]), we get that

$$K_2(R) = H_2(E(R); \mathbb{Z}).$$

3.2 Steinberg Symbols and K_2

Let R be a commutative ring. Suppose that $A, B \in E(R)$ are matrices that commute. If $a, b \in St(R)$ are representatives of A and B, respectively, i.e. $\phi(a) = A$ and $\phi(b) = B$, then the commutator $[a, b] = aba^{-1}b^{-1}$ is in $K_2(R)$, since $\phi([a, b]) = ABA^{-1}B^{-1} = I$. The commutator $[a, b]$ will be denoted by

$$A \star B.$$

To see that $A \star B$ is independent of the choice of representatives, consider another representative a' of A. Since $\phi(a) = \phi(a')$, $ac = a'$, where c is in the center of $St(R)$, we get

$$[a', b] = a'ba' - 1b^{-1} = acbc^{-1}a^{-1}b^{-1} = aba^{-1}b^{-1} = [a, b].$$

This way of producing elements of $K_2(R)$, will give rise to a skew-symmetric bimultiplicative paring

$$\{-,-\} : K_1(R) \otimes K_1(R) \to K_2(R), \tag{1}$$

see [15, §8] for more details.

In the case $R = F$ is a field, we have that $K_1(F) \approx F^\times$, and hence a pairing

$$\{-,-\} : F^\times \otimes F^\times \to K_2(F).$$

It turns out that $K_2(F)$ is generated by the symbols $\{x, y\}$, where $x, y \in F^\times$. Furthermore, H. Matsumoto identified the kernel of this pairing in his thesis [13].

Theorem 3.16 (Matsumoto)**.** *The abelian group $K_2(F)$ can be viewed as the abelian group generated by symbols $\{x, y\}$, with $x, y \in F^\times$ subject to the following relations and their consequences:*

(1) $\{x, 1 - x\} = 1$ *for* $x \neq 0, 1$

(2) $\{x_1x_2, y\} = \{x_1, y\}\{x_2, y\}$

(3) $\{x, y_1y_2\} = \{x, y_1\}\{x, y_2\}$

Proof. For a complete proof of Matsumotos theorem, see [15, §12]. □

Consider a bimultiplicative map

$$(-,-) : F^\times \times F^\times \to A,$$

where A is an abelian group, that satifies $(x, 1 - x) = 1$, for $x \neq 1$. Such a map will be called a Steinberg symbol. And Matsumoto's theorem is equivalent to the following proposition:

Proposition 3.17. *Given any Steinberg Symbol $(-,-) : F^\times \times F^\times \to A$, there exists one unique map $\alpha : K_2(F) \to A$ such that the diagram*

$$\begin{array}{ccc} F^\times \times F^\times & \xrightarrow{(-,-)} & A \\ & \searrow^{\{-,-\}} & \uparrow \alpha \\ & & K_2(F), \end{array}$$

commutes.

Proof. See [15, p. 94] for a proof of the equivalence of Theorem 3.16 and Proposition 3.17. □

Recall that a discrete valuation v on F is a homomorphism from the multiplicative group $F^\times$ to the additive group of integers, such that $v(x+y) \geq \min(v(x), v(y))$. The discrete valuation ring $\mathcal{O}_v$ consisting of all the elements x such that $v(x) \geq 0$, is called the associated valuation ring of v. The ring $\mathcal{O}_v$ is a local ring, with maximal ideal $m_v = \{x \in F \mid v(x) > 0\}$. The residue field of v, k_v, is the quotient $\mathcal{O}_v/m_v$.

If F is a number field, then every non-zero prime ideal P in $\mathcal{O}_F$ will give rise to a discrete valuation ring $(\mathcal{O}_F)_P$, and hence a discrete valuation v such that $(\mathcal{O}_F)_P = \mathcal{O}_v$. Conversely, for every discrete valuation v on F, $\mathcal{O}_v = (\mathcal{O}_F)_P$ for some prime ideal P.

Let x, y be in $F^\times$ and v be a discrete valuation on F. The formula

$$f_v(x,y) = (-1)^{v(x)v(y)} x^{v(y)} y^{-v(x)} \tag{2}$$

gives rise to a bimultiplicative map from $F^\times \times F^\times$ to $F^\times$. It is clear that $v(f_v(x,y)) = 0$ for all x, y, so $f_v(x,y) \in \mathcal{O}_v^\times$.

Consider the Steinberg symbol

$$\tau_v : F^\times \times F^\times \to k_v^\times,$$

where τ_v is the composition of f_v and the quotient map $q : \mathcal{O}_v \to k_v$. Formally,

$$\tau_v(x,y) = q(f(x,y)) = (-1)^{v(x)v(y)} x^{v(y)} y^{-v(x)} \bmod m_v.$$

From Proposition 3.17, we know that τ_v factors through $K_2(F)$. We will abuse the notation and denote the induced map from $K_2(F)$ to $k_v^\times$ by τ_v as well.

Let T be the set of the non-zero prime ideals of $\mathcal{O}_F$. We get tame symbols

$$\tau_P : K_2(F) \to k_P^\times,$$

for every prime P in T. Consider the product of the tame symbols

$$\tau = \prod \tau_P : K_2(F) \to \prod_{P \in T} k_P^\times.$$

We can replace the product with a direct sum, since $\tau_P(a,b) = 1$ for all but finitely many prime ideals P.

The kernel of τ is called the tame kernel of F, and can be identified with $K_2(\mathcal{O}_F)$.

Lemma 3.18. *The map τ fits into a short exact sequence:*

$$0 \longrightarrow K_2(\mathcal{O}_F) \longrightarrow K_2(F) \xrightarrow{\tau} \bigoplus_P k_P^\times \longrightarrow 0,$$

where $K_2(\mathcal{O}_F)$ has been identified with the tame kernel.

Proof. Quillen's localization sequence [20, Thm. 5] gives us the following long exact sequences:

$$\longrightarrow \bigoplus_P K_2(k_P) \xrightarrow{i^*} K_2(\mathcal{O}_F) \xrightarrow{i_*} K_2(F) \xrightarrow{\partial} \bigoplus_P k_P^\times \xrightarrow{i^*} \mathcal{O}_F^\times \xrightarrow{i} F^\times \longrightarrow \cdots \longrightarrow 0.$$

Clearly the inclusion $i : \mathcal{O}_F^\times \to F^\times$ is injective. Quillen also shows in [19] that $K_{2i}(k) = 0$ for all finite fields k and $i > 0$. Consider the commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K_2(\mathcal{O}_F) & \xrightarrow{i_*} & K_2(F) & \xrightarrow{\partial} & \bigoplus_P k_P^\times & \longrightarrow & 0 \\ & & \downarrow & & \downarrow \text{id} & & \downarrow & & \\ 0 & \longrightarrow & \ker(\tau) & \longrightarrow & K_2(F) & \xrightarrow{\tau} & \bigoplus_P k_P^\times & \longrightarrow & \operatorname{coker}(\tau) \longrightarrow 0, \end{array}$$

where the top sequence comes from Quillen's localization sequence, and the lower sequence is the exact sequence associated with the map τ. If $a, b \in \mathcal{O}_F^\times$, then $\tau_P(\{a, b\}) = 1$ for all primes P. This gives us the vertical map $K_2(\mathcal{O}_F) \to \ker(\tau)$. The vertical map $\bigoplus_P k_P^\times \to \bigoplus_P k_P^\times$ is just the induced map.

The Snake Lemma gives us that $K_2(\mathcal{O}_F) \approx \ker(\tau)$. A theorem of Bass [4, Thm. 6] shows that in the more general setting, where R is a Dedekind Domain with countably many maximal ideals, $\operatorname{coker}(\tau) = SL(R)/E(R)$, where $SL(R)$ is the special linear group. By a theorem of Bass, Milnor and Serre, $SL(R)/E(R)$ vanishes when R is the ring of integers of some number field ([2]). □

Let F be a number field. A valuation on F is a function $|\ | : F \to \mathbb{R}$, such that the following is satisfied:

- $|x| \geq 0$, and $|x| = 0$ if and only if $x = 0$
- $|xy| = |x||y|$
- $|x + y| \leq |x| + |y|$

We will disregard the trivial valuation $|\ |$, which satisfies $|x| = 1$ for all $x \in F^\times$. Every valuation defines a norm on F, and hence induces a topology on F. We will say that two valuations are equivalent if they define the same topology.

There are two kinds of valuations, archimedean and nonarchimedean. The nonarchimedean valuations, in addition to satisfy the axioms above, also adhere to the strong triangle inequality:

$$|x + y| \leq \max\{|x|, |y|\}.$$

We have seen that for every non-zero prime ideal, there exists a discrete valuation. Moreover, every discrete valuation v gives rise to a nonarchimedean valuations $|\ |_v$ (see [17, Ch. II] for details). In fact, for a number field F, every equivalence class of a nonarchimedean valuation can be represented by a valuation $|\ |_v$ with v a discrete valuation.

The equivalence classes of archimedean valuations can be represented by valuations $|\ |_\tau$ given by

$$|x|_\tau = |\tau(x)|,$$

where τ is either a complex or real embedding of F.

Definition 3.19. A place v of a number field F is an equivalence class of valuations on F. The nonarchimedean equivalence classes will be called finite places, and the archimedean ones will be called infinite places.

Let F be a nonarchimedean local field of characteristic 0, i.e. it is complete with respect to a nonarchimedean valuation $|\ |_P$, where P is the corresponding ideal of the valuation ring. Suppose that F contains the n-th roots of unity μ_n. We then get a Steinberg symbol

$$\left(\frac{\cdot,}{P}\right)_n : F^\times \times F^\times \to \mu_n,$$

called the Hilbert symbol of order n. For a complete definition of the Hilbert symbol see [17, Ch. V]. We will only give an explicit definition for some of the cases.

Example 3.20. Let (F, v) be a local nonarchimedean field of characteristic 0 that contains the n-th roots of units μ_n. Consider the formula (2) for the tame symbol

$$f_v(x, y) = (-1)^{v(x)v(y)} y^{v(x)} x^{-v(y)}.$$

It defines a bimultiplicative homomorphism from $F^\times \times F^\times$ to $\mathcal{O}_v^\times$. Assume that the residue field k has order q and characteristic p. The field F must contain the $(q-1)$-th roots of unity, so $n \mid (q-1)$. Suppose now that the residue characteristic p of F does not divide n. The units $\mathcal{O}_F^\times$ of F can be written as a product

$$u = \pi^k h(u) g(u)$$

in a unique way, where π is a prime element, $h(u) \in \mu_{q-1}$ a $(q-1)$-th root of unity and $g(u) \in 1 + m_v$ is an element of the group of principal units (see [17, p. 136]). We can compose f_v and h, this gives us a map from $F^\times \times F^\times$ to μ_{q-1}, which we can map onto the subgroup μ_n. Denote the new map by λ_v. We then have

$$\lambda_v(x, y) = (h((-1)^{v(x)v(y)} y^{v(x)} x^{-v(y)}))^{q-1/n}.$$

The λ_v defines a Steinberg symbol on F to the cyclic group of n elements μ_n. In the case above, λ_v is equal to the Hilbert symbol on F, and is therefore often called the tame Hilbert symbol of order n.

If $F = \mathbb{R}$ and $n = 2$, we get a Hilbert symbol $\left(\frac{\cdot,}{\infty}\right)_2$, defined by

$$\left(\frac{a, b}{\infty}\right)_2 = (-1)^{\frac{\mathrm{sgn}a-1}{2} \cdot \frac{\mathrm{sgn}b-1}{2}}.$$

If $F = \mathbb{C}$, the Hilbert symbols will be trivial.

Now consider a number field F. For every finite and real infinite place v, we have a completion $F \subset F_v$. For some general field L, let $\mu(L)$ denote the complete group of roots of unity contained in L. Let $m = |\mu(F)|$ and $m_v = |\mu(F_v)|$. We can then define Steinberg symbols

$$\lambda_v : F^\times \times F^\times \longrightarrow F_v^\times \times F_v^\times \longrightarrow \mu(F_v),$$

where the first map is the inclusion, and the second is the Hilbert symbol $\left(\frac{\cdot}{v}\right)_{m_v}$ of order m_v.

Theorem 3.21. *Let F be a number field, with $\mu_n \subset F^\times$. We have the following product formula for the Hilbert symbols*

$$\prod (\lambda_v(x, y))^{m_v/n} = 1,$$

where the product is taken over all finite and real infinite places v if $n = 2$, and over all finite places when $n > 2$.

Proof. See [17, p. 414] for a proof. □

The Steinberg symbols λ_v will again induce maps

$$\lambda_v : K_2(F) \to \mu(F_v),$$

which we can combine to get a map

$$\lambda = \oplus \lambda_v : K_2(F) \to \bigoplus \mu(F_v).$$

By the product formula of Theorem 3.21, it is clear that the different λ_v-s are linearly dependent. Conversely, a theorem of Calvin Moore [16, Thm. 7.4] states that the product formula is the only relation between the different λ_v-s, so we get the following theorem:

Theorem 3.22. *The sequence*

$$K_2(F) \xrightarrow{\lambda} \bigoplus \mu(F_v) \xrightarrow{c} \mu(F) \longrightarrow 0,$$

is exact when $c((x_v)) = \prod (x_v)^{m_v/m}$.

Proof. See [16, p. 39] for the original proof. There is also a direct proof in [5]. □

The kernel W of λ is called the wild kernel. Let S be the set of all finite and real-infinite places. Consider the commutative diagram

$$\begin{array}{ccc} K_2(F) & \xrightarrow{\lambda} & \bigoplus_{v \in S} \mu(F_v) \\ \downarrow{\scriptstyle \tau} & \swarrow & \\ \bigoplus_{v \text{ finite}} k_v^\times & & \end{array}$$

The ker-coker sequence of this triangle relates the wild kernel to $K_2(\mathcal{O}_F)$ in the following way:

$$0 \longrightarrow W(F) \longrightarrow K_2(\mathcal{O}_F) \longrightarrow \bigoplus \ker(\mu(F_v) \longrightarrow k_v^\times) \longrightarrow \mu(F) \longrightarrow 0.$$

It will be useful to let

$$\lambda_n : K_2(F) \to \bigoplus \mu_n$$

denote the map given by

$$\{a, b\} \mapsto \bigoplus \lambda_v(a, b)^{m_v/n},$$

where the sum is taken over all finite places for $n > 2$, and over all finite and real infinite places for $n = 2$. Note that

$$\lambda_n = \oplus \Big(\frac{\cdot}{v} \Big)_n.$$

The last Steinberg symbol we will look at relates K_2 to Brauer groups.

Definition 3.23. Let A be an finite dimensional F-algebra. The algebra A is called central simple over F if A is simple, i.e. it has no two-sided ideals other than 0 and itself, and the center of A, $Z(A)$ is F.

Let A and B be central simple algebras over F. The tensor product $A \otimes_F B$ is also a central simple algebra over F, so it turns the set $C(F)$ of isomorphism classes of central simple algebras into a multiplicative monoid with identity F. By the Artin-Webberburn Theorem, every central simple algebra is determined up to isomorphism in the following way.

Proposition 3.24. *Let A be a central simple algebra over F. Then there exists a natural number n and a division algebra D over F, such that*

$$A \approx M_n(D),$$

where $M_n(D)$ is the algebra of $n \times n$ matrices over D.

Proof. This is a special case of the Artin-Webberburn Theorem that is stated and proved in [18, p. 49]. □

We can therefore represent each isomorphism class of central simple F-algebras by the pair (n, D). The division ring D is called the basic algebra, and is a representation of its isomorphism class. Note that the tensor product of two division rings is not necessarily a division ring.

Define the relation $\sim$ by

$$(n_1, D_1) \sim (n_2, D_2),$$

if and only if $D_1 \approx D_2$.

Proposition 3.25. *The relation $\sim$ is an equivalence relation, and $C(F)/\sim$ is a group with respect to the tensor product.*

Proof. For a complete proof see [18, p. 228]. □

Let $[A]$ denote the equivalence class of A in $C(F)$. The identity element is given by $[F]$, and $[A][B] = [A \otimes_F B]$. Since $A \otimes_F A^{op} \approx M_m(F)$, where A^{op} is the opposite ring of A with the same algebra structure as A, it is clear that $[A]^{-1} = [A^{op}]$.

Definition 3.26. The group $Br(F) = C(F)/\sim$ is called the Brauer group.

Let F be a number field that contains a primitive n-th root of unity ζ_n. For $a, b \in F^\times$ consider the algebra $A_{\zeta_n}(a,b)$ over F that is the unital associative algebra of dimension n^2 generated by the formal symbols X, Y, subject to the following relations:

$$X^n = a,\ Y^n = b \text{ and } XY = \zeta_n YX.$$

Proposition 3.27. *The algebra $A_{\zeta_n}(a,b)$ is central simple, and the map*

$$\psi_{\zeta_n} : F^\times \times F^\times \to {}_nBr(F)$$

given by

$$(a,b) \mapsto [A_{\zeta_N}(a,b)],$$

defines a Steinberg symbol on F. Here ${}_nBr(F)$ denotes the subgroup of $Br(F)$ generated by all elements with order dividing n.

Proof. See [15, p. 144] for a complete proof. □

A natural question to ask, is how the symbol depends on the choice of ζ_n. It turns out that if you consider another primitive n-th root ζ such that $\zeta = \zeta_n^i$, then

$$\psi_\zeta(a,b)^i = \psi_{\zeta_n}(a,b).$$

On the other hand, if $i \mid n$, we get that

$$\psi_\zeta(a,b) = \psi_{\zeta_n}(a,b)^i.$$

For detailed computations see [15, p. 148].

This dependence can be fixed by tensoring with ζ, i.e., consider the Steinberg symbol

$$\zeta \otimes \psi_\zeta : F^\times \times F^\times \to \mu_n \otimes {}_nBr(F),$$

which sends (a,b) to the element $\zeta \otimes \psi_\zeta(a,b)$. This symbol is independent of the choice of primitive n-th root ζ, since if i is relative prime to n,

$$\zeta^i \otimes \psi_{\zeta^i}(a,b) = \zeta \otimes (\psi_{\zeta^i}(a,b))^i = \zeta \otimes \psi_\zeta(a,b).$$

John Tate proved in [22, Thm. 5.1] that the induced map

$$\zeta \otimes \psi : K_2(F)/n \to \mu \otimes {}_nBr(F),$$

is an isomorphism for the case where F is a number field or a global function field. It was later proved by A. S. Merkurjev and A. A. Suslin that the result holds in general for all fields ([14]).

When F is a local field, the subgroup ${}_nBr(F)$ of all the elements in $Br(F)$ that has order dividing n is cyclic. This follows from the classical result

$$Br(F) \approx \mathbb{Q}/\mathbb{Z},$$

when F is local, see [18, p. 338]. On the other hand, if F is a number field, the Brauer group fits into the following short exact sequence

$$0 \longrightarrow Br(F) \longrightarrow \bigoplus_P Br(F_P) \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0.$$

We can use this sequence to prove the next proposition, but first we should recall what is meant by the ring of S-integers of a number field F.

Definition 3.28. Let S be a set of places containing the infinite places of a number field F. The ring of S-integers denoted by $\mathcal{O}_{F,S}$ is the ring

$$\mathcal{O}_{F,S} = \{x \in F \mid v(x) \geq 0 \text{ for all } v \notin S\}.$$

Proposition 3.29. *Let F be a number field containing the n-th roots of unity μ_n. Then the following sequence is exact*

$$0 \longrightarrow K_2(F)/n \xrightarrow{\lambda_n} \bigoplus_v \mu_n \xrightarrow{c} \mu_n \longrightarrow 0,$$

where for $n > 2$, the sum is taken over all finite places v, and for $n = 2$, the sum is taken over all finite and real infinite places.

Proof. See [11, Prop. 3.2] for a detailed proof. □

Proposition 3.30. *Let F be a number field that contains the n-th roots of unity, μ_n, and let S be an arbitrary set of places that contains the infinite places and the primes dividing n. Then the following sequence is exact*

$${}_nK_2(F) \xrightarrow{\tau} \bigoplus_{P \notin S} \mu_n \xrightarrow{f} \mu_n \otimes \mathrm{Cl}(\mathcal{O}_{F,S}) \longrightarrow 0,$$

where $\tau : {}_nK_2(F) \to \bigoplus_v {}_nk_v^\times = \bigoplus_v \mu_n$ is the tame symbol and f the map given by

$$(n)_v \mapsto \zeta_n \otimes [\prod P_v^{n_v}],$$

where P_v is the prime ideal corresponding to the finite place v.

Proof. Consider the exact sequence

$$F^\times \longrightarrow \bigoplus_{P \notin S} \mathbb{Z} \longrightarrow \mathrm{Cl}(\mathcal{O}_{F,S}) \longrightarrow 0.$$

The first map is given by the direct sum $\oplus v_P$ of the valuation maps v_P, $P \notin S$, and the second is f as defined in the proposition. It is clear that this sequence is exact from the definition of the ideal class group of $\mathcal{O}_{F,S}$. If we tensor the sequence above with μ_n, we get another exact sequence:

$$\mu_n \otimes F^\times \longrightarrow \bigoplus_{P \notin S} \mu_n \longrightarrow \mu_n \otimes \mathrm{Cl}(\mathcal{O}_{F,S}) \longrightarrow 0.$$

Since the tensor product commutes with direct products, we can decompose the first map as $\bigoplus(id \otimes v_P)$. Each component $id \otimes v_P$ maps $\zeta \otimes a$ to $\zeta \otimes v_P(a)$, which we can identify with $\zeta^{v_P(a)}$ in μ_n. Now consider the weak Steinberg symbol restricted to $\mu_n \otimes F^\times$, $\tau_P : \mu_n \otimes F^\times \to \mu_n$. Recall that the weak symbol is given by the following formula:

$$a \otimes b \mapsto (-1)^{v_P(a)v_P(b)} b^{v_P(a)} a^{-v_P(b)} \mod P.$$

For $a = \zeta \in \mu_n$, we get that

$$\tau_P(\zeta \otimes b) = (-1)^{v_P(\zeta)v_P(b)} b^{v_P(\zeta)} \zeta^{-v_P(b)} \mod P = \zeta^{v_P(b)},$$

and hence that the two maps τ_P and $id \otimes v_P$ agree. We can therefore factor the map through ${}_nK_2(F)$ to get the result. □

3.3 Structure of $K_2(\mathcal{O}_K)/p$

In this section, we will show two "structure" theorems for $K_2(\mathcal{O}_F)/p$.

Theorem 3.31. *Let F be a number field containing a primitive p-th root of unity, and let S_0 be the set of finite places above p. (If $p = 2$, S_0 has to include all the real infinite places as well). The following sequence is exact*

$$0 \longrightarrow \mu_p \otimes \mathrm{Cl}(\mathcal{O}_F[\tfrac{1}{p}]) \xrightarrow{l} K_2(\mathcal{O}_F[\tfrac{1}{p}])/p \xrightarrow{\lambda'} \bigoplus_{v \in S_0} \mu_p \xrightarrow{c} \mu_p \longrightarrow 0,$$

where λ' is induced by the Hilbert symbol of order p, and c is the codiagonal map. The map l is a boundary map, defined by

$$l(\zeta \otimes [I]) = x^p \mod pK_2(\mathcal{O}_{F,S})),$$

if $x \in K_2(F)$ such that $\tau_P(x) = \zeta^{v_P(I)} \mod P$ for all prime ideals P not containing p.

Proof. Compare [11, Thm. 3.5]. Let S be the set of places containing the infinite places and the finite places above p. Recall, that we identified $K_2(\mathcal{O}_F, S)$ with the kernel of $\tau : K_2(F) \to \bigoplus_{v \notin S} k_v^\times$. Consider the commutative diagram with exact rows

$$\begin{array}{ccccccccc}
0 & \longrightarrow & K_2(\mathcal{O}_{F,S}) & \longrightarrow & K_2(F) & \xrightarrow{\tau} & \bigoplus_{v \notin S} k_v^\times & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \cdot p} & & \downarrow{\scriptstyle \cdot p} & & \downarrow{\scriptstyle \cdot p} & & \\
0 & \longrightarrow & K_2(\mathcal{O}_{F,S}) & \longrightarrow & K_2(F) & \xrightarrow{\tau} & \bigoplus_{v \notin S} k_v^\times & \longrightarrow & 0.
\end{array}$$

The Snake Lemma gives us the following exact sequence

$$0 \longrightarrow {}_pK_2(\mathcal{O}_{F,S}) \longrightarrow {}_pK_2(F) \xrightarrow{\tau} \bigoplus_{v\notin S} \mu_p \longrightarrow K_2(\mathcal{O}_{F,S})/p \longrightarrow K_2(F)/p \xrightarrow{\lambda'} \bigoplus_{v\notin S} \mu_p \longrightarrow 0.$$

Note that the penultimate map is obtained from the composition of the quotient map

$$\bigoplus_{v\notin S} k_v^\times \to \bigoplus_{v\notin S} \mu_p, \text{ and } \tau : K_2(F) \to \bigoplus_{v\notin S} k_v^\times,$$

which is equal to λ', where

$$\lambda' = \underset{v\notin S}{\oplus} (\lambda_v)^{m_v/p}.$$

From Proposition 3.30 we have that the cokernel of τ is $\mu_p \otimes \mathrm{Cl}(\mathcal{O}_{F,S})$. We can therefore shorten the exact sequence to

$$0 \longrightarrow \mu_p \otimes \mathrm{Cl}(\mathcal{O}_{F,S}) \xrightarrow{l} K_2(\mathcal{O}_{F,S})/p \longrightarrow K_2(F)/p \xrightarrow{\lambda'} \bigoplus_{v\notin S} \mu_p \longrightarrow 0,$$

where l is the map described in the theorem. Recall from Proposition 3.29 that there is an exact sequence

$$0 \longrightarrow K_2(F)/p \xrightarrow{\lambda_p} \bigoplus_{v\notin(S-S_0)} \mu_p \xrightarrow{c} \mu_p \longrightarrow 0.$$

In lack of a better name, we denote the map from $K_2(\mathcal{O}_{F,S})/p \to K_2(F)/p$ by f. Now consider the composition $\lambda_p \circ f : K_2(\mathcal{O}_{F,S}) \to \oplus\mu_p$. Since λ_p is injective, $\ker(\lambda_p \circ f) = \ker f$, and hence it gives us an alternative ending of the exact sequence. Now since $\lambda' \circ f = 0$, it is clear that $\lambda \circ f = \underset{v\in S_0}{\oplus} (\lambda_v)^{m_v/n}$, which only hits elements in $\underset{v\in S_0}{\oplus} \mu_p$. Moore's Reciprocity Theorem (Theorem 3.22) tells us that the cokernel is given by the codiagonal map c, so we get the exact sequence

$$0 \longrightarrow \mu_p \otimes \mathrm{Cl}(\mathcal{O}_{F,S}) \xrightarrow{l} K_2(\mathcal{O}_{F,S})/p \xrightarrow{\lambda'} \bigoplus_{v\in S_0} \mu_p \xrightarrow{c} \mu_p \longrightarrow 0. \qquad \square$$

In [11], Theorem 3.31 is stated and proved also for the case where p is a natural number not necessarily a prime. We are on the other hand only interested in the case where p is prime, and will therefore refer the interested reader to [11] for the more general case.

The second structure theorem can also be found in ([11, Thm 5.4]).

Theorem 3.32. *Let p be an odd prime, F a number field, ζ_p a primitive pth root of unity, and suppose $\zeta_p \notin F$. Then we have a short exact sequence*

$$0 \longrightarrow (\mu_p \otimes \mathrm{Cl}(\mathcal{O}_{F(\zeta_p)}[\tfrac{1}{p}]))^G \longrightarrow K_2(\mathcal{O}_F)/p \longrightarrow \bigoplus_s \mu_p \longrightarrow 0,$$

where $G = Gal(F(\zeta_p)/F)$ acts diagonally on $\mu_p \otimes \mathrm{Cl}(\mathcal{O}_{F(\zeta_p)}[\frac{1}{3}])$, and s is the number of p-adic primes of F that split completely in $F(\zeta_p)$.

Theorem 3.31 and Theorem 3.32 together give a description of $K_2(\mathcal{O}_F/p)$ both when μ_p is contained in F and when it is not. Theorem 3.32 will in particular be very useful in Section 4 where we prove a reflection theorem for K_2.

In order to prove Theorem 3.32, we need to develop some more theory. In particular we will have to make use of transfer homomorphism $i^* : K_i(E) \to K_i(F)$ for a field extension E/F.

Let $A \subset B$ be rings such that B is a finitely generated left A-module. The inclusion $i : A \to B$ induces a map on K-groups

$$i_* : K_j(A) \to K_j(B),$$

for $j = 0, 1$ or 2, by the functoriality of K_j. We can also define transfer maps

$$i^* : K_j(B) \to K_j(A),$$

see [15, §14].

Let A be a number field F or its ring of integers $\mathcal{O}_F$, and let B be correspondingly either an extension E of F or the ring of integers $\mathcal{O}_E$.

- The zero transfer map $i^* : K_0(B) \to K_0(A)$ is given by restriction of scalars.
- The first transfer map $i^* : K_1(B) \to K_1(A)$ can be identified with the norm map

  $$\mathrm{Norm}_{E/F} : B^\times \approx K_1(B) \to K_1(A) \approx A^\times,$$

  (see [15, p. 139] for details).

The second transfer map $i^* : K_2(B) \to K_2(A)$ is hard to describe explicitly, but it satisfies the projection formula of Theorem 3.33.

Theorem 3.33. *Let $A \subset B$ be commutative rings such that B is a finitely generated A-module. For every $a \in K_1(A)$ and $b \in K_1(B)$, the following formula holds*

$$i^*(\{b, i_*(a)\}) = \{i^*(b), a\},$$

where $\{\ ,\ \}$ is the product from 1.

Proof. See [15, §14] for a proof. □

Lemma 3.34. *Let F be a number field and E a finite Galois extension of F, with Galois group $G = Gal(E/F)$. Then the compositions $i^*i_* : K_2(F) \to K_2(F)$ and $i_*i^* : K_2(E) \to K_2(E)$ are given by*

$$i^*i_*(\{x, y\}) = deg(E/F)\{x, y\},$$
$$i_*i^*(\{x, y\}) = \prod_{\sigma \in G} \{\sigma x, \sigma y\}.$$

Proof. Let $\{x, y\} \in K_2(E)$, and suppose that $x, y \in F^\times$, i.e. $\{x, y\}$ is in the image of i_*. From Theorem (3.33), we get

$$i^*\{x, y\} = \{\text{Norm}_{E/F}(x), y\} = \{x^n, y\} = \{x, y\}^n,$$

where $n = \deg(E/F)$.

The second composition is harder to prove. We will therefore refer the reader to [9, p. 6] for a complete proof, and only remark that in the case $y \in F^\times$, we get the result from the Projection formula by the following computation:

$$i^*\{x, y\} = \{\prod \sigma x, y\} = \prod \{\sigma x, \sigma y\}. \qquad \square$$

Lemma 3.35. *Let E/F be an extension of number fields. Let S be a set of places in K containing the infinite places and let T be the set of places in L that lie above the places in S. Then the following diagram with exact rows commutes*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K_2(\mathcal{O}_{E,T}) & \longrightarrow & K_2(E) & \xrightarrow{\tau} & \bigoplus k_v^\times & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle i^*} & & \downarrow{\scriptstyle i^*} & & \downarrow{\scriptstyle N} & & \\ 0 & \longrightarrow & K_2(\mathcal{O}_{F,S}) & \longrightarrow & K_2(F) & \xrightarrow{\tau} & \bigoplus k_v^\times & \longrightarrow & 0, \end{array}$$

where the map $N = \oplus(\prod \text{Norm}_{k_w/k_v})$.

If E/F is a Galois extension with Galois group $G = Gal(E/F)$, then the diagram is a commutative diagram of G-modules with G-homomorphisms.

Proof. The transfer homomorphism $i^* : K_2(\mathcal{O}_{E,T}) \to K_2(\mathcal{O}_{F,S})$ coincides with the restriction, so it is only necessary to prove commutativity of the last square. Consider the following diagram

$$\begin{array}{ccc} K_2(E) & \xrightarrow{\oplus_{w|v} \tau_w} & \bigoplus_{w|v} k_v^\times \\ \downarrow{\scriptstyle i^*} & & \downarrow{\scriptstyle \prod \text{Norm}_{k_w/k_v}} \\ K_2(F) & \xrightarrow{\tau_v} & k_v^\times \\ \downarrow{\scriptstyle i_*} & & \downarrow{\scriptstyle \oplus i} \\ K_2(E) & \xrightarrow{\oplus_{w|v} \tau_w} & \bigoplus_{w|v} k_v^\times. \end{array}$$

The lower square is clearly commutative. Since $i^*i_*\{x, y\} = \prod_{\sigma \in G}\{\sigma x, \sigma y\}$, from Lemma 3.34, we see that the outer square is also commutative. Since $\oplus i : k_v \to \bigoplus k_w$ is injective, we can conclude that the upper square is commutative, which completes the proof. $\square$

Another consequence of Lemma 3.34 is the following:

Proposition 3.36. *For a Galois extension E/F, with Galois group $G = Gal(E/F)$ and an integer n, the map i_* induces homomorphisms*

$$i_* : K_2(F)/n \to (K_2(E)/n)^G$$

and

$$i_* : K_2(\mathcal{O}_{F,S})/n \to (K_2(\mathcal{O}_{E,T})/n)^G.$$

Moreover, both are isomorphisms when n is relatively prime to $|G|$.

Proof. Consider the maps

$$i_* : K_2(F)/n \to (K_2(E)/n)^G \text{ and } i^* : (K_2(E)/n)^G \to K_2(F)/n.$$

It is clear that both i^*i_* and i_*i^* are multiplications by $|G|$. So if $|G|$ and n are relatively prime, both i^*i_* and i_*i^* are isomorphisms. Since i^*i_* is an isomorphism, i_* is injective, and since i_*i^* is an isomorphism, i_* is surjective.

The same argument follows through for

$$i_* : K_2(\mathcal{O}_{F,S})/n \to (K_2(\mathcal{O}_{E,T})/n)^G.$$ □

Proof of Theorem 3.32. Let p be an odd prime. From Theorem 3.31, we have an exact sequence

$$0 \longrightarrow \mu_p \otimes \mathrm{Cl}(\mathcal{O}_{F(\zeta_p)}[\tfrac{1}{p}]) \xrightarrow{l} K_2(\mathcal{O}_{F(\zeta_p)}[\tfrac{1}{p}])/p \xrightarrow{\lambda'} \bigoplus_{v \in S_0} \mu_p \xrightarrow{c} \mu_p \longrightarrow 0.$$

Since p is odd, S_0 consists of all the finite places above p, and

$$\lambda'(\{x, y\}) = \bigoplus_{P|p} \Big(\frac{x, y}{P}\Big)_p.$$

We will first show that the exact sequence from Theorem 3.31 can be made into an exact sequence of G-modules.

Let $\sigma \in G$ act on $\mu_p \otimes \mathrm{Cl}(\mathcal{O}_{F(\zeta_p)}[\frac{1}{p}])$ diagonally, i.e. $\sigma(\zeta \otimes I) = (\sigma\zeta \otimes \sigma I)$. Recall the definition of $l : \mu_p \otimes \mathrm{Cl}(\mathcal{O}_{F(\zeta_p)}[\frac{1}{p}]) \to K_2(\mathcal{O}_F[\frac{1}{p}])/p$ in Theorem 3.31. Suppose that $l(\zeta \otimes I) = x^p$ for some x with

$$\tau_p(x) = \zeta^{v_P(I)} \bmod P$$

for all prime ideals P not dividing p. We need to show that $\tau_P(\sigma x) = (\sigma\zeta)^{v_P(\sigma I)} \mod P$ for all P not dividing p. If $\sigma Q = P$, then

$$\tau_P \sigma x = \tau_{\sigma Q} \sigma x = (\sigma\zeta)^{v_{\sigma Q}(\sigma I)} = (\sigma\zeta)^{v_P(\sigma I)},$$

and $\sigma l(\zeta \otimes I) = l(\sigma\zeta \otimes \sigma I)$.

Define a G-action on $\bigoplus_{P \in S_0} \mu_p$ by

$$(\sum \zeta[P])^\sigma = \sum \sigma(\zeta)[\zeta(P)],$$

i.e. the diagonal action followed by a permutation.

Observe that

$$\sigma\Big(\frac{x,y}{P}\Big)_p = \Big(\frac{\sigma x,\sigma y}{\sigma P}\Big)_p.$$

Clearly, the G-action we defined on $\bigoplus_{P\in S_0}\mu_p$ makes λ' into a G-module homomorphism, which makes the sequence into an exact sequence of G-modules.

Taking cohomology of the sequence of G-modules yields an exact sequence

$$0\longrightarrow(\mu_p\otimes \mathrm{Cl}(\mathcal{O}_{F(\zeta_p)}[\tfrac{1}{p}]))^G \xrightarrow{l'} (K_2(\mathcal{O}_{F(\zeta_p)}[\tfrac{1}{p}])/p)^G \xrightarrow{\lambda''} \Big(\bigoplus_{v\in S_0}\mu_p\Big)^G \xrightarrow{c'} \mu_p^G,$$

where l', λ'' and c' are just the restrictions of the original maps. It is clear that $\mu_p^G = 0$, and from Proposition 3.36

$$i_*: K_2(\mathcal{O}_F[\tfrac{1}{p}])/p \longrightarrow (K_2(\mathcal{O}_{F(\zeta_p)}[\tfrac{1}{p}])/p)^G$$

is an isomorphism. We can therefore rewrite the sequence as

$$0\longrightarrow(\mu_p\otimes \mathrm{Cl}(\mathcal{O}_{F(\zeta_p)}[\tfrac{1}{p}]))^G \xrightarrow{l'} (K_2(\mathcal{O}_{F(\zeta)}[\tfrac{1}{p}])/p)^G \xrightarrow{\lambda''} \Big(\bigoplus_{v\in S_0}\mu_p\Big)^G \xrightarrow{c'} 0.$$

Let T_0 be the set of p-adic primes in F. We can decompose

$$\bigoplus_{P\in S_0}\mu_p = \bigoplus_{Q\in T_0}\Big(\bigoplus_{P|Q}\mu_p\Big).$$

Let σ be the generator of G, and suppose that $Q = P_1^e\cdots P_r^e$. Since $\sigma P_i = P_j$ for some $j\neq i$, we get that

$$\Big(\bigoplus_{P\in S_0}\mu_p\Big)^G = \bigoplus_{Q\in T_0}\Big(\bigoplus_{P|Q}\mu_p\Big)^G.$$

How can we describe $\Big(\bigoplus_{P|Q}\mu_p\Big)^G$? Let

$$(\zeta_1,\ldots,\zeta_{i_r})\in(\mu_p)\oplus\cdots\oplus(\mu_p).$$

We may assume that

$$\sigma(\zeta_1,\ldots,\zeta_r) = (\sigma\zeta_r,\sigma\zeta_1,\ldots,\sigma\zeta_{r-1}),$$

so if $(\zeta_1,\ldots,\zeta_{i_r})\in((\mu_p)\oplus\cdots\oplus(\mu_p))^G$, then $\zeta_i = \sigma^{i-1}\zeta_1$. In particular, $\zeta_1 = \zeta_{r+1} = \sigma^r\zeta_1$, which implies that $r = p-1$. We can therefore conclude that

$$\Big(\bigoplus_{P|Q}\mu_p\Big)^G \approx \begin{cases}\mu_p & \text{if } Q \text{ splits completely in } E,\\ 0 & \text{otherwise.}\end{cases}$$

From Quillen's localization sequence, we have that the sequence

$$0 \longrightarrow K_2(\mathcal{O}_F) \longrightarrow K_2(\mathcal{O}_F[\tfrac{1}{p}]) \longrightarrow \bigoplus_{P|p} k_P^{\times} \longrightarrow 0$$

is exact. Since $\mu_p \not\subset F^{\times}$, $|k_P^{\times}|$ is relatively prime to p, hence

$$K_2(\mathcal{O}_F) \longrightarrow K_2(\mathcal{O}_F[\tfrac{1}{p}])$$

is an isomorphism.

This gives us the exact sequence

$$0 \longrightarrow (\mu_p \otimes \mathrm{Cl}(\mathcal{O}_{F(\zeta_p)}[\tfrac{1}{3}]))^G \longrightarrow K_2(\mathcal{O}_F)/p \longrightarrow \bigoplus_{s} \mu_p \longrightarrow 0,$$

which completes the proof. □

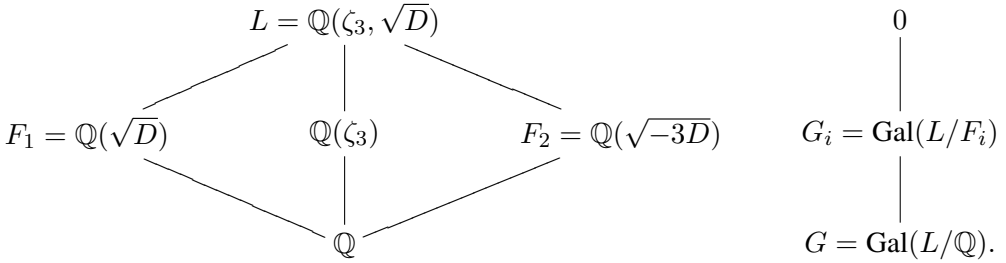
4 Reflection in K_2

In this section we will make use of the theory developed in the previous sections to prove a reflection theorem for K_2.

Theorem 4.1. *Let D be a positive squarefree integer. Then*

$$\mathrm{rk}_3(K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{-3D})})) - \mathrm{rk}_3(K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{D})})) = \begin{cases} 1, 0, -1 & \text{if } D \equiv 1 \bmod 3 \\ 0, -1, -2 & \text{if } D \equiv 6 \bmod 9 \\ 0, -1 & \text{otherwise.} \end{cases}$$

Let $L = \mathbb{Q}(\zeta_3, \sqrt{D})$, $F_1 = \mathbb{Q}(\sqrt{D})$, and $F_2 = \mathbb{Q}(\sqrt{-3D})$. In the rest of this section one should keep the following picture in mind:



Recall from Theorem 3.32 that we have a short exact sequence

$$0 \longrightarrow (\mu_3 \otimes \mathrm{Cl}\,\mathcal{O}_L[\tfrac{1}{3}])^{G_i} \longrightarrow K_2(\mathcal{O}_{F_i})/p \longrightarrow \bigoplus_{s_i} \mu_3 \longrightarrow 0,$$

where $G_i = \mathrm{Gal}(L/F_i)$ and s_i is the number of 3-adic primes in F_i that split completely in L. Since all the groups in the above sequence are elementary 3-groups,

$$\mathrm{rk}_3 K_2(\mathcal{O}_{F_i}) = s_i + \mathrm{rk}_3(\mu_3 \otimes \mathrm{Cl}\,\mathcal{O}_L[\tfrac{1}{3}])^{G_i}.$$

Corollary 4.2. *We can write the difference $\mathrm{rk}_3(K_2(\mathcal{O}_{F_2})) - \mathrm{rk}_3(K_2(\mathcal{O}_{F_1}))$, as $s + t$, where*

$$s = s_2 - s_1,$$

and

$$t = \mathrm{rk}_3(\mu_3 \otimes \mathrm{Cl}\,\mathcal{O}_L[\tfrac{1}{3}])^{G_2} - \mathrm{rk}_3(\mu_3 \otimes \mathrm{Cl}\,\mathcal{O}_L[\tfrac{1}{3}])^{G_1}.$$

Since $L/\mathbb{Q}$ is Galois, we can use Hilbert's ramification theory to factorize (3) in L.

Lemma 4.3. *If s_1 is the number of 3-adic primes in $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ that split in $\mathcal{O}_L$, and s_2 the number of 3-adic primes in $\mathcal{O}_{\mathbb{Q}(\sqrt{-3D})}$ that split in L, then we have*

$$s = s_2 - s_1 = \begin{cases} 1 & \text{if} D \equiv 1 \bmod 3 \\ -1 & \text{if} D \equiv 6 \bmod 9 \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Since $d_{\mathbb{Q}(\sqrt{-3})} = -3$ and 3 divides -3, the prime ideal (3) will ramify in $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$. The prime 3 will therefore neither split totally, nor be completely inert in L. We also want to eliminate the case where 3 is totally ramified in L.

Assume for contradiction that (3) is totally ramified in L. By Proposition 1.28, 3 has to divide both $d_{\mathbb{Q}(\sqrt{D})}$ and $d_{\mathbb{Q}(\sqrt{-3D})}$. But

$$d_{\mathbb{Q}(\sqrt{D})} = \begin{cases} 4D & \text{if } D \equiv 2, 3 \bmod 4 \\ D & \text{otherwise,} \end{cases}$$

so 3 must divide D. Furthermore, since $3|D$, $\mathbb{Q}(\sqrt{-3D}) = \mathbb{Q}(\sqrt{-\frac{D}{3}})$, which by the same argument as above, implies that 3 divides $\frac{D}{3}$. This contradicts the assumption that D is squarefree. We can therefore conclude that there are only two possible ways of factoring 3 in L. In other words,

$$(3) = \begin{cases} P^2 \\ P_1^2 P_2^2, \end{cases}$$

for some prime ideals P, P_1 and P_2 in L. We also know that 3 ramifies in either $\mathbb{Q}(\sqrt{D})$ or $\mathbb{Q}(\sqrt{-3D})$, but not in both.

Assume that 3 ramifies in $\mathbb{Q}(\sqrt{D})$. Then 3 will either split or be inert in $\mathbb{Q}(\sqrt{-3D})$, and correspondingly the 3-adic prime of $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ will split or be inert in L. The prime 3 splits in $\mathbb{Q}(\sqrt{-3D})$ if and only if $x^2 + \frac{D}{3}$ is solvable modulo 3 (see Example 1.33). The equation $x^2 + \frac{D}{3}$ is solvable if $D \equiv 0 \bmod 9$ or $D \equiv 6 \bmod 9$. We can disregard the first case since D is assumed to be square free, which leaves us with

$$s_1 = \begin{cases} 1 & \text{if } D \equiv 6 \bmod 9 \\ 0 & \text{otherwise.} \end{cases}$$

Similarly, we get that

$$s_2 = \begin{cases} 1 & \text{if } D \equiv 1 \bmod 3 \\ 0 & \text{otherwise,} \end{cases}$$

and hence the result. □

In order to compute the difference

$$t = \mathrm{rk}_3(\mu_3 \otimes \mathrm{Cl}\,\mathcal{O}_L[\tfrac{1}{3}])^{G_2} - \mathrm{rk}_3(\mu_3 \otimes \mathrm{Cl}\,\mathcal{O}_L[\tfrac{1}{3}])^{G_1},$$

we will adapt some of the techniques used in the proof of Scholz's Reflection Theorem 1.18.

Lemma 4.4. *Let A be the 3-Sylow subgroup of $\mathrm{Cl}(\mathcal{O}_L[\frac{1}{3}])$, and assume that $\langle \sigma_i \rangle = G_i$. Then*

$$(\mu_3 \otimes \mathrm{Cl}\,\mathcal{O}_L[\tfrac{1}{3}])^{G_i} = \mu_3 \otimes \ker(1 + \sigma_i : A \to A).$$

Proof. It is clear that $\mu_3 \otimes \mathrm{Cl}\,\mathcal{O}_L[\frac{1}{3}] = \mu_3 \otimes A$. Consider elements of the form $\zeta_3^i \otimes I$, where $I \in A$, generate $\mu_3 \otimes A$. Moreover, since $\zeta_3^i \otimes I = \zeta_3 \otimes I^i$, we can write every generator as $\zeta_3 \otimes I'$, for some $I' \in A$. Consider an element $\sum(\zeta_3 \otimes I)$ in $\mu_3 \otimes A$. Clearly

$$\sum(\zeta_3 \otimes I) = \zeta_3 \otimes \Big(\prod I\Big).$$

We can therefore write any element in $\mu_3 \otimes A$ as $\zeta_3 \otimes I''$, for some I'' in A.

Since $\zeta_3^{\sigma_i} = \zeta_3^{-1}$, we get that

$$(\zeta_3 \otimes I)^{\sigma_i} = \zeta_3^{\sigma_i} \otimes I^{\sigma_i} = \zeta_3^{-1} \otimes I^{\sigma_i} = \zeta_3 \otimes I^{-\sigma_i}.$$

The fixed points $(\mu_3 \otimes A)^{G_i}$ are the elements $\zeta_3 \otimes I$ where $-\sigma I = I$, i.e. $(1+\sigma)I = 0$. □

Recall from Section 2 that every $\mathbb{Z}_3[G]$-module M can be decomposed as

$$M = \varepsilon_1 M \oplus \varepsilon_2 M \oplus \varepsilon_3 M \oplus \varepsilon_4 M,$$

where

$$\begin{aligned}
\varepsilon_1 &= \Big(\frac{1+\sigma_1}{2}\Big)\Big(\frac{1+\sigma_2}{2}\Big),\\
\varepsilon_2 &= \Big(\frac{1+\sigma_1}{2}\Big)\Big(\frac{1-\sigma_2}{2}\Big),\\
\varepsilon_3 &= \Big(\frac{1-\sigma_1}{2}\Big)\Big(\frac{1+\sigma_2}{2}\Big),\\
\varepsilon_4 &= \Big(\frac{1-\sigma_1}{2}\Big)\Big(\frac{1-\sigma_2}{2}\Big).
\end{aligned}$$

In particular,

$$A = \varepsilon_1 A \oplus \varepsilon_2 A \oplus \varepsilon_3 A \oplus \varepsilon_4 A.$$

In the proof of Scholz's Reflection Theorem, we showed that

$$\varepsilon_1 = \frac{1}{4}\,\mathrm{Norm}_{L/\mathbb{Q}} \text{ and } \varepsilon_4 = \Big(\frac{1-\sigma_1}{4}\Big)\,\mathrm{Norm}_{L/\mathbb{Q}(\zeta_3)},$$

and hence the subgroup $\varepsilon_1\ {}_3\mathrm{Cl}\,(L) = \varepsilon_4\ {}_3\mathrm{Cl}\,(L) = 0$. The same argument applies to A, i.e. $\varepsilon_1 A = \varepsilon_4 A = 0$. Later in the proof of Scholz's Reflection Theorem, we showed that

$$\begin{aligned}
\varepsilon_2\ {}_3\mathrm{Cl}\,(L) &= {}_3\mathrm{Cl}\,(\mathbb{Q}(\sqrt{D})),\\
\varepsilon_3\ {}_3\mathrm{Cl}\,(L) &= {}_3\mathrm{Cl}\,(\mathbb{Q}(\sqrt{-3D})).
\end{aligned}$$

Let A_1 denote the 3-Sylow subgroup ${}_3\mathrm{Cl}\,(\mathcal{O}_{\mathbb{Q}(\sqrt{D})}[\frac{1}{3}])$ of $\mathrm{Cl}(\mathcal{O}_{\mathbb{Q}(\sqrt{D})})$, and A_2 the 3-Sylow subgroup ${}_3\mathrm{Cl}\,(\mathcal{O}_{\mathbb{Q}(\sqrt{-3D})}[\frac{1}{3}])$ of $\mathrm{Cl}(\mathcal{O}_{\mathbb{Q}(\sqrt{-3D})})$. Let $I \subset {}_3\,\mathrm{Cl}(L)$ be the subgroup generated by the 3-adic primes of order a power of 3, then $A = {}_3\,\mathrm{Cl}(L)/I$. Let $\phi :\ {}_3\,\mathrm{Cl}(L) \to A$ be the quotient map. It is clearly a G-module map, hence

$$\varepsilon_2 A = A_1$$

and

$$\varepsilon_3 A = A_2.$$

Lemma 4.5. *The kernel of* $1+\sigma_1 : A \to A$ *is equal to the subgroup* $A_2 = {}_3Cl\,(\mathcal{O}_{\mathbb{Q}(\sqrt{-3D})}[\frac{1}{3}])$, *and* $\ker(1+\sigma_2 : A \to A)$ *is equal to* $A_1 = {}_3Cl\,(\mathcal{O}_{\mathbb{Q}(\sqrt{D})}[\frac{1}{3}])$.

Proof. We have that $A = \varepsilon_2 A \oplus \varepsilon_3 A = (\frac{1+\sigma_1}{2})(\frac{1-\sigma_2}{2})A \oplus (\frac{1-\sigma_1}{2})(\frac{1+\sigma_2}{2})A$. Since

$$\begin{aligned}(1+\sigma_1)(\frac{1+\sigma_1}{2})(\frac{1-\sigma_2}{2})A &= (\frac{1+2\sigma_1+1}{2})(\frac{1-\sigma_2}{2})A \\ &= 2A_1 \\ &= A_1,\end{aligned}$$

and

$$\begin{aligned}(1+\sigma_1)(\frac{1-\sigma_1}{2})(\frac{1+\sigma_2}{2})A &= (\frac{1-1}{2})(\frac{1-\sigma_2}{2})A \\ &= 0,\end{aligned}$$

we get that $\ker(1+\sigma_1 : A \to A) = A_2$. Similarly, it follows that $\ker(1+\sigma_2 : A \to A) = A_1$. □

We can now write the sequence from Theorem 3.32 as

$$0 \longrightarrow \mu_3 \otimes A_2 \longrightarrow K_2(\mathcal{O}_{F_1})/p \longrightarrow \bigoplus_{s_1} \mu_3 \longrightarrow 0,$$

and

$$0 \longrightarrow \mu_3 \otimes A_1 \longrightarrow K_2(\mathcal{O}_{F_2})/p \longrightarrow \bigoplus_{s_2} \mu_3 \longrightarrow 0.$$

Lemma 4.6. *We can write the* t *from Corollary 4.2 as*

$$t = \mathrm{rk}_3 A_1 - \mathrm{rk}_3 A_2 = \begin{cases} 0, -1, -2 & \text{if} D = 1 \mod 3 \\ 1, 0, -1 & \text{if} D = 6 \mod 9 \\ 0, -1 & \text{otherwise.} \end{cases}$$

Proof. Let $t_1 = \mathrm{rk}_3 A_1$ and $t_2 = \mathrm{rk}_3 A_2$. If $t_1' = \mathrm{rk}_3\,\mathrm{Cl}(\mathbb{Q}(\sqrt{D}))$, and $t_2' = \mathrm{rk}_3\,\mathrm{Cl}(\mathbb{Q}(\sqrt{-3D}))$, then by Scholz's Reflection Theorem 1.18

$$t_2' - t_1' = 1, 0.$$

The 3-Sylow subgroup $A_1 \subset \mathrm{Cl}(\mathcal{O}_{\mathbb{Q}(\sqrt{D})}[\frac{1}{3}])$ is the quotient of ${}_3\mathrm{Cl}\,(\mathbb{Q}(\sqrt{D}))$ by the 3-adic primes of order a power of 3. The prime 3 can either split totally, ramify totally or be inert in $\mathbb{Q}(\sqrt{D})$. If 3 is inert, i.e (3) is a prime ideal in $\mathbb{Q}(\sqrt{D})$, then it is also principal, and hence $A_1 = {}_3\mathrm{Cl}\,(\mathbb{Q}(\sqrt{D}))$. If 3 ramifies, the 3-adic prime has order two, which also implies that $A_1 = {}_3\mathrm{Cl}\,(\mathbb{Q}(\sqrt{D}))$. The only case where the 3-adic primes can have order a power of 3, is when 3 splits (we will give examples of this in the next section). Suppose that $(3) = P_1 P_2$ in $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$. Since (3) is principal, the ideal classes of P_1 and P_2 are mutually inverses of each other, hence there is at most one 3-adic generator of ${}_3\mathrm{Cl}\,(\mathbb{Q}(\sqrt{D}))$.

The prime 3 splits in $\mathbb{Q}(\sqrt{D})$ if and only if $D \equiv 1 \bmod 3$, so

$$t_1' - t_1 = \begin{cases} 1, 0 & \text{if } D \equiv 1 \bmod 3 \\ 0 & \text{otherwise.} \end{cases}$$

Similarly, we get that

$$t_2' - t_2 = \begin{cases} 1, 0 & \text{If } D \equiv 6 \bmod 9 \\ 0 & \text{otherwise.} \end{cases}$$

We can write the difference

$$\begin{aligned} t = t_1 - t_2 &= t_1' - t_2' + (t_1 - t_1') - (t_2 - t_2') \\ &= 0, -1 + \begin{cases} 0, -1 & \text{if } D \equiv 1 \bmod 3 \\ 0 & \text{otherwise} \end{cases} + \begin{cases} 1, 0 & \text{If } D \equiv 6 \bmod 9 \\ 0 & \text{otherwise} \end{cases} \\ &= \begin{cases} 0, -1, -2 & \text{if } D \equiv 1 \bmod 3 \\ 1, 0, -1 & \text{if } D \equiv 6 \bmod 9 \\ 0, -1 & \text{otherwise.} \end{cases} \end{aligned}$$

□

We can now easily prove the Reflection Theorem for K_2.

Proof of theorem 4.1. If we put Lemma 4.3 together with Lemma 4.6, we get by Corollary 4.2 that

$$\mathrm{rk}_3\, K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{-3D})}) - \mathrm{rk}_3\, K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{D})}) = s + t = \begin{cases} 1, 0, -1 & \text{if } D \equiv 1 \bmod 3 \\ 0, -1, -2 & \text{if } D \equiv 6 \bmod 9 \\ 0, -1 & \text{otherwise.} \end{cases}$$

□

5 Examples

In this section we will present examples of the eight different cases of Theorem 4.1. All of our computations (except for the easiest ones) have been done with the computer algebra system PARI/GP, first developed by Henri Cohen and his co-workers at Université Bordeaux I. It is now maintained by Karim Belabas [23]. The first example will be followed by a block of GP code that computes the integral basis and the class group of a number field. The code is followed by its output when run through the GP calculator. The rest of the examples can be computed in a similar way, by slightly modifying the input in the function **bnfinit()**.

Recall from Section 4 that

- $L = \mathbb{Q}(\sqrt{D}, \zeta_3)$, $F_1 = \mathbb{Q}(\sqrt{D})$ and $F_2 = \mathbb{Q}(\sqrt{-3D})$
- $G_1 = \mathrm{Gal}(\mathbb{Q}(\sqrt{D})/\mathbb{Q})$ and $G_2 = \mathrm{Gal}(\mathbb{Q}(\sqrt{-3D})/\mathbb{Q})$
- s_i is the number of 3-adic primes in F_i that split completely in L
- $s = s_2 - s_1$
- $t = \mathrm{rk}_3(\mu_3 \otimes \mathrm{Cl}\,\mathcal{O}_L[\frac{1}{3}])^{G_2} - \mathrm{rk}_3(\mu_3 \otimes \mathrm{Cl}\,\mathcal{O}_L[\frac{1}{3}])^{G_1}$
- $\mathrm{rk}_3(K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{-3D})})) - \mathrm{rk}_3(K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{D})})) = s + t$

The formula in the Reflection Theorem 4.1 states that

$$\mathrm{rk}_3(K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{-3D})})) - \mathrm{rk}_3(K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{D})})) = \begin{cases} 1, 0, -1 & \text{if } D \equiv 1 \bmod 3 \\ 0, -1, -2 & \text{if } D \equiv 6 \bmod 9 \\ 0, -1 & \text{otherwise.} \end{cases} \tag{3}$$

5.1 For $D \equiv 1 \bmod 3$

If $D \equiv 1 \bmod 3$, we have from Lemma 4.3 that the 3-adic prime in $\mathbb{Q}(\sqrt{-3D})$ will split completely in L, so $s = 1$. We also know from the proof of Lemma 4.6 that $\mathrm{rk}_3\,\mathrm{Cl}(\mathcal{O}_{\mathbb{Q}(\sqrt{-3D})}[\frac{1}{3}]) = \mathrm{rk}_3\,\mathrm{Cl}(\mathcal{O}_{\mathbb{Q}(\sqrt{-3D})})$.

If $t = 0$, the right hand side of formula (3) will be 1. This happens for example if the 3-Sylow subgroups of $\mathrm{Cl}(\mathbb{Q}(\sqrt{D}))$ and $\mathrm{Cl}(\mathbb{Q}(\sqrt{-3D}))$ are trivial. So let $D = 7$. The Minkowski bound of $\mathbb{Q}(\sqrt{7})$ is

$$\frac{2!}{2^2}\left(\frac{4}{\pi}\right)^s \sqrt{|\mathrm{d}_{\mathbb{Q}(\sqrt{7})}|} = \sqrt{7} < 3.$$

By Remark 1.20 we get that the 2-adic primes will generate $\mathrm{Cl}(\mathbb{Q}(\sqrt{7}))$. Since (2) ramifies in $\mathbb{Q}(\sqrt{7})$, it is clear that the 3-Sylow subgroup of $\mathrm{Cl}(\mathcal{O}_{\mathbb{Q}(\sqrt{7})})$ will be trivial.

An easy calculation in PARI/GP shows that the ideal class group

$$\mathrm{Cl}(\mathcal{O}_{\mathbb{Q}(\sqrt{-3D})}) = \mathrm{Cl}(\mathcal{O}_{\mathbb{Q}(\sqrt{-21})}) \approx \mathbb{Z}/2 \oplus \mathbb{Z}/2,$$

and it is generated by the class of the prime ideals $(5, 2 + \sqrt{7}), (2, 1 + \sqrt{7})$. So if $D = 7$, we have

$$\mathrm{rk}_3 K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{-3D})}) - \mathrm{rk}_3 K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{D})}) = 1.$$

```
setrand(1);
//sets the random seed

bnf = bnfinit(x^2+21);
//creates the number field object Q(\sqrt(-21))

bnf.zk
//prints the integral basis of bnf

bnf.clgp
//prints the class group

bnfcertify(bnf)
//checks if the result is correct
```

```
//Reads the code from the file example.gp
? \r{example.gp}

//output of bnf.zk is an array where the elements form an
//integral basis for the given number field. Here x denotes the
//quotient class of x in Q(x)/x^2+21
%1 = [1, x]

//output of bnf.clgp is a 3 array where the first element is
//the class number, the second is a vector that describes the
//cyclic decoposition of the class group, in this case it is
//Z/2xZ/2. The last element is an array of matrices on Hermite
//Normal Form, that describes the ideals with respect to the
//integral basis given by bnf.zk, that generate the ideal class
//group.
%2 = [4, [2, 2], [[5, 2; 0, 1], [2, 1; 0, 1]]]

//bnfinit() assumes GRH, we therefore have to verify our
//results by using bnfcertify(). If the output is 1 we are
//safe.
%3 = 1
```

The right hand side of formula (3) will be 0 when $t = -1$. This will happen if, for example,

$$\mathrm{rk}_3 \operatorname{Cl}(\mathcal{O}_{\mathbb{Q}(\sqrt{-3D})}[\tfrac{1}{3}]) = \mathrm{rk}_3 \operatorname{Cl} \mathcal{O}_{\mathbb{Q}(\sqrt{-3D})} = 1 + \mathrm{rk}_3 \operatorname{Cl} \mathcal{O}_{\mathbb{Q}(\sqrt{D})} = 1 + \mathrm{rk}_3 \operatorname{Cl}(\mathcal{O}_{\mathbb{Q}(\sqrt{D})}[\tfrac{1}{3}]).$$

If $D = 58$, then $-3D = -174$, and we get isomorphisms

$$\operatorname{Cl} \mathcal{O}_{\mathbb{Q}(\sqrt{D})} \approx \mathbb{Z}/2,$$
$$\operatorname{Cl} \mathcal{O}_{\mathbb{Q}(\sqrt{-3D})} \approx \mathbb{Z}/6 \oplus \mathbb{Z}/2.$$

The ideal class groups are generated by $\{[(3, 1 + \sqrt{58})]\}$ and $\{[(5, 4 + \sqrt{-174})], [(3, \sqrt{-174})]\}$, respectively. Thus inverting 3 in $\mathcal{O}_{\mathbb{Q}(\sqrt{-3D})}$ will not change the 3-sylow subgroup of the ideal class group. So, if $D = 58$, we get

$$\mathrm{rk}_3 K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{-3D})}) - \mathrm{rk}_3 K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{D})}) = 0.$$

The last example will satisfy

$$\mathrm{rk}_3 K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{-3D})}) - \mathrm{rk}_3 K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{D})}) = -1.$$

In other words, we need to find a D such that $t = -2$ and

$$\mathrm{rk}_3 \mathrm{Cl}(\mathcal{O}_{\mathbb{Q}(\sqrt{-3D})}[\tfrac{1}{3}]) = \mathrm{rk}_3 \mathrm{Cl}\,\mathcal{O}_{\mathbb{Q}(\sqrt{-3D})} = 1 + \mathrm{rk}_3 \mathrm{Cl}\,\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = 2 + \mathrm{rk}_3 \mathrm{Cl}(\mathcal{O}_{\mathbb{Q}(\sqrt{D})}[\tfrac{1}{3}]).$$

The smallest D that satisfies the equation above is $D = 2917$ so $-3D = -8751$, whence

$$\begin{aligned} \mathrm{Cl}\,\mathcal{O}_{\mathbb{Q}(\sqrt{D})} &\approx \mathbb{Z}/3, \\ \mathrm{Cl}\,\mathcal{O}_{\mathbb{Q}(\sqrt{D})}\Big[\frac{1}{3}\Big] &\approx 0 \text{ and}, \\ \mathrm{Cl}\,\mathcal{O}_{\mathbb{Q}(\sqrt{-3D})} &\approx \mathbb{Z}/24 \oplus \mathbb{Z}/3. \end{aligned}$$

The class group $\mathrm{Cl}\,\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ is generated by $[(3, \frac{1+\sqrt{2917}}{2})]$ and the class group $\mathrm{Cl}\,\mathcal{O}_{\mathbb{Q}(\sqrt{-3D})}$ is generated by $\{[(2, \frac{1+\sqrt{-8751}}{2})], [(46, \frac{83+\sqrt{-8751}}{2})]\}$. Note that $(46, \frac{83+\sqrt{-8751}}{2})$ is not a prime ideal, but a product of a 2-adic prime ideal and a 23-adic prime ideal.

5.2 For $D \equiv 6 \bmod 9$

If $D \equiv 6 \bmod 3$, we have from Lemma 4.3 that the 3-adic prime in $\mathbb{Q}(\sqrt{D})$ will split completely in L, so $s = -1$. We also know from the proof of Lemma 4.6 that

$$\mathrm{rk}_3 \mathrm{Cl}(\mathcal{O}_{\mathbb{Q}(\sqrt{D})}[\frac{1}{3}]) = \mathrm{rk}_3 \mathrm{Cl}(\mathcal{O}_{\mathbb{Q}(\sqrt{D})}).$$

Note also that $\mathbb{Q}(\sqrt{-3D}) = \mathbb{Q}\Big(\sqrt{-\frac{D}{3}}\Big)$.

As we saw for $D \equiv 1 \bmod 3$, the different cases will correspond to different values of t. The case where

$$\mathrm{rk}_3 K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{-\frac{D}{3}})}) - \mathrm{rk}_3 K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{D})}) = 0,$$

corresponds to $t = 1$. In other words, we need to find an example where

$$\mathrm{rk}_3 \mathrm{Cl}(\mathcal{O}_{\mathbb{Q}(\sqrt{-\frac{D}{3}})}[\frac{1}{3}]) + 1 = \mathrm{rk}_3 \mathrm{Cl}\,\mathcal{O}_{\mathbb{Q}(\sqrt{-\frac{D}{3}})} = \mathrm{rk}_3 \mathrm{Cl}\,\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \mathrm{rk}_3 \mathrm{Cl}(\mathcal{O}_{\mathbb{Q}(\sqrt{D})}[\frac{1}{3}]).$$

If $D = 321$, then $-\frac{D}{3} = -107$, and we get

$$\begin{aligned} \mathrm{Cl}\,\mathcal{O}_{\mathbb{Q}(\sqrt{D})} &\approx \mathbb{Z}/3, \\ \mathrm{Cl}(\mathcal{O}_{\mathbb{Q}(\sqrt{-\frac{D}{3}})}) &\approx \mathbb{Z}/3. \end{aligned}$$

The ideal class groups are generated by $\{[(2, \frac{1+\sqrt{321}}{2})]\}$ and $\{[(3, \frac{1+\sqrt{-107}}{2})]\}$, hence

$$\mathrm{Cl}(\mathcal{O}_{\mathbb{Q}(\sqrt{-\frac{D}{3}})}[\tfrac{1}{3}]) = 0.$$

So for $D = 321$,

$$\mathrm{rk}_3 K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{-\frac{D}{3}})}) - \mathrm{rk}_3 K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{D})}) = 0.$$

We can easily find an example of the case where $t = 0$. Let $D = 6$, so $-\frac{D}{3} = -2$. The Minkowski Bound of $\mathbb{Q}(\sqrt{D})$ is less than 3, and the Minkowski Bound of $\mathbb{Q}(\sqrt{-\frac{D}{3}})$ is $\frac{4}{\pi} < 2$, so both $\mathrm{rk}_3 \mathrm{Cl}\,\mathbb{Q}(\sqrt{D})$ and $\mathrm{rk}_3 \mathrm{Cl}\,\mathbb{Q}(\sqrt{-\frac{D}{3}})$ are zero, since 2 ramifies in $\mathbb{Q}(\sqrt{D})$. Thus

$$\mathrm{rk}_3 K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{-\frac{D}{3}})}) - \mathrm{rk}_3 K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{D})}) = -1.$$

The last case corresponds to $t = -1$. In other words, we should have

$$\mathrm{rk}_3 \mathrm{Cl}(\mathcal{O}_{\mathbb{Q}(\sqrt{-\frac{D}{3}})}[\tfrac{1}{3}]) = \mathrm{rk}_3 \mathrm{Cl}\,\mathcal{O}_{\mathbb{Q}(\sqrt{-\frac{D}{3}})} = 1 + \mathrm{rk}_3 \mathrm{Cl}\,\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = 1 + \mathrm{rk}_3 \mathrm{Cl}(\mathcal{O}_{\mathbb{Q}(\sqrt{D})}[\tfrac{1}{3}]).$$

If $D = 69$, then $-\frac{D}{3} = -23$, and we get that

$$\mathrm{Cl}\,\mathcal{O}_{\mathbb{Q}(\sqrt{D})} \approx 0,$$
$$\mathrm{Cl}(\mathcal{O}_{\mathbb{Q}(\sqrt{-\frac{D}{3}})}) \approx \mathbb{Z}/3,$$

and we can conclude that

$$\mathrm{rk}_3 K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{-\frac{D}{3}})}) - \mathrm{rk}_3 K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{D})}) = -2.$$

5.3 Neither $D \equiv 1 \bmod 3$ nor $D \equiv 6 \bmod 9$

In the two last examples, (3) will be inert in either $\mathbb{Q}(\sqrt{D})$ or $\mathbb{Q}(\sqrt{-3D})$ and ramify in the other. Since it will neither split in $\mathbb{Q}(\sqrt{D})$ or in $\mathbb{Q}(\sqrt{-3D})$, $s = 0$. Furthermore, since (3) is inert or totally ramified, the 3-adic primes will have order 1 or 2 in the class group. The 3-rank of the ideal classes will therefore be unaffected when we invert 3. So t is either 1 or 0.

If $D = 2$, the Minkowski Bound of $\mathbb{Q}(\sqrt{D})$ will be $\sqrt{2} < 2$, so $\mathrm{Cl}\,\mathbb{Q}(\sqrt{D}) = 0$. The Minkowski bound on $\mathbb{Q}(\sqrt{-3D})$ is less than 3. Since 2 ramifies, $\mathrm{rk}_3 \mathrm{Cl}\,\mathbb{Q}(\sqrt{-3D}) = 0$. So for $D = 2$, we get

$$\mathrm{rk}_3 K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{-3D})}) - \mathrm{rk}_3 K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{D})}) = 0.$$

On the other hand, if $D = 29$, then $\mathrm{Cl}\,\mathbb{Q}(\sqrt{D}) = 0$ and $\mathrm{Cl}\,\mathbb{Q}(\sqrt{-3D}) \approx \mathbb{Z}/6$. So

$$\mathrm{rk}_3 K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{-3D})}) - \mathrm{rk}_3 K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{D})}) = -1.$$

We see from the examples given in this section that our reflection theorem for K_2 is optimal in the sense that there are examples of all the different cases.

References

[1] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[2] H. Bass, J. Milnor, and J.-P. Serre. Solution of the congruence subgroup problem for SL_n $(n \geq 3)$ and Sp_{2n} $(n \geq 2)$. *Inst. Hautes Études Sci. Publ. Math.*, (33):59–137, 1967.

[3] Hyman Bass. *Algebraic K-theory*. W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[4] Hyman Bass. K_2 des corps globaux (d'après Tate, Garland). In *Seminar on Modern Methods in Number Theory (Inst. Statist. Math., Tokyo, 1971), Paper No. 1*, page 23. Inst. Statist. Math., Tokyo, 1971.

[5] Stephen U. Chase and William C. Waterhouse. Moore's theorem on uniqueness of reciprocity laws. *Invent. Math.*, 16:267–270, 1972.

[6] John B. Fraleigh. *A first course in abstract algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1967.

[7] Howard Garland. A finiteness theorem for K_2 of a number field. *Ann. of Math. (2)*, 94:534–548, 1971.

[8] Georges Gras. *Class field theory*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2003. From theory to practice, Translated from the French manuscript by Henri Cohen.

[9] B. Harris and J. Stasheff. Suspension, automorphisms, and division algebras. In *Algebraic K-theory, II: "Classical" algebraic K-theory and connections with arithmetic (Proc. Conf., Battelle Seattle Res. Center, Seattle, Wash., 1972)*, pages 337–346. Lecture Notes in Math., Vol. 342. Springer, Berlin, 1973.

[10] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[11] Frans Keune. On the structure of the K_2 of the ring of integers in a number field. In *Proceedings of Research Symposium on K-Theory and its Applications (Ibadan, 1987)*, volume 2, pages 625–645, 1989.

[12] Heinrich-Wolfgang Leopoldt. Zur Struktur der l-Klassengruppe galoisscher Zahlkörper. *J. Reine Angew. Math.*, 199:165–174, 1958.

[13] H. Matsumoto. *Sur les sous-groupes arithmétiques des groupes semi-simples déployés*. Gauthier-Villars, 1969.

[14] A. S. Merkur′ev and A. A. Suslin. K-cohomology of Severi-Brauer varieties and the norm residue homomorphism. *Izv. Akad. Nauk SSSR Ser. Mat.*, 46(5):1011–1046, 1135–1136, 1982.

[15] John Milnor. *Introduction to algebraic K-theory*. Princeton University Press, Princeton, N.J., 1971. Annals of Mathematics Studies, No. 72.

[16] Calvin C. Moore. Group extensions of p-adic and adelic linear groups. *Inst. Hautes Études Sci. Publ. Math.*, (35):157–222, 1968.

[17] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[18] Richard S. Pierce. *Associative algebras*, volume 88 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1982. Studies in the History of Modern Science, 9.

[19] Daniel Quillen. On the cohomology and K-theory of the general linear groups over a finite field. *Ann. of Math. (2)*, 96:552–586, 1972.

[20] Daniel Quillen. Higher algebraic K-theory. I. In *Algebraic K-theory, I: Higher K-theories (Proc. Conf., Battelle Memorial Inst., Seattle, Wash., 1972)*, pages 85–147. Lecture Notes in Math., Vol. 341. Springer, Berlin, 1973.

[21] John Tate. Symbols in arithmetic. In *Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 1*, pages 201–211. Gauthier-Villars, Paris, 1971.

[22] John Tate. Relations between K_2 and Galois cohomology. *Invent. Math.*, 36:257–274, 1976.

[23] The PARI Group, Bordeaux. *PARI/GP, version* `2.5.0`, 2011. available from `http://pari.math.u-bordeaux.fr/`.

[24] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.