UNIVERSITY
OF OSLO

Master's thesis

Weil Reciprocity and Number Theory

Investigating some reciprocity laws using algebraic K-theory

Nicolas Triantafilidis

Mathematics
60 ECTS study points

Department of Mathematics
Faculty of Mathematics and Natural Sciences

Spring 2023

Nicolas Triantafilidis

Weil Reciprocity and Number Theory

Investigating some reciprocity laws using algebraic K-theory

Supervisor:
Håkon Kolderup

Abstract

We begin with a treatment of classical algebraic number theory and algebraic K-theory. After introducing the notion of a (Steinberg) symbol, we use Tate's result on the structure of $K_2(\mathbb{Q})$ to prove quadratic reciprocity. In a similar manner we give an explicit computation of $K_2(\mathbb{Q}(\sqrt{-2}))$ and derive an analogous reciprocity law. We then shift our focus to exploring the relationship between three reciprocity laws: Artin reciprocity, Weil reciprocity and quadratic reciprocity, and show how the global Artin map can be used to derive both quadratic and Weil reciprocity. Finally, we show how one can use Weil reciprocity to prove quadratic reciprocity as well.

Contents

Introduction

The archetypal reciprocity law

In algebraic number theory, a common question to ask is whether, for a prime p, a polynomial $f(x)$, when reduced modulo p, splits into (distinct) linear factors. This question helps us determine how primes factorise in certain field extensions and can give us an insight into the arithmetic of the field. If we take the simplest case of a quadratic polynomial $f(x) = x^2 - q$, for some fixed prime q, we see that f splits modulo an odd prime p into the product of two distinct linear factors if and only if q is a square modulo p. With this in mind, we define the Legendre symbol as

$$\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{if } q \text{ is a square modulo } p; \\ -1 & \text{otherwise.} \end{cases}$$

Now, the problem of evaluating these symbols as p varies over infinitely many primes is not particularly easy. An easier problem is to evaluate $\left(\frac{p}{q}\right)$. Here, all we need to know is the value of p modulo our fixed prime q. That is to say, we only need to calculate q different symbols corresponding to the q residue classes. This gives us the notion, in some sense, of what we mean when we talk about reciprocity.

In fact, one of the most well-known results in algebraic number theory, the law of quadratic reciprocity, solves this problem completely. First formulated in full by Legendre, it was actually Gauss that provided the first proof[1].

With the notation above, we get the rather simple formulation of quadratic reciprocity as follows:

Theorem 0.1 (Quadratic reciprocity, [8, §5, Theorem 1])**.** *Let p and q be distinct odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Moreover, we have the following supplementary laws

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

[1] Milne's notes on Class Field Theory [14] provide a insight into the key characters in the world of algebraic number theory and class field theory.

Ireland and Rosen provide two different proofs in [8]: first, following Eisenstein's method and then using Gauss sums. One of the aims of this thesis is to provide two alternative proofs. First, we provide a proof from algebraic K-theory that follows Tate's computation of $K_2(\mathbb{Q})$. Second, we will demonstrate the power of the Artin map to provide a proof from class field theory.

Another aim of this thesis is to derive a reciprocity law for a quadratic extension of $\mathbb{Q}$ using algebraic K-theory. In establishing the isomorphism

$$K_2(\mathbb{Q}) \cong \{\pm 1\} \oplus \bigoplus_p (\mathbb{Z}/p\mathbb{Z})^*$$

Tate employed the Euclidean algorithm. Thus, in order to replicate his results for other number fields, their rings of integers must be Euclidean domains. We therefore choose $\mathbb{Q}(\sqrt{-2})$ as our quadratic extension and prove that

$$K_2(\mathbb{Q}(\sqrt{-2})) \cong \bigoplus_v k(v)^* \cong \bigoplus_{\substack{p \text{ prime} \\ p \equiv 1,3 (\mathrm{mod}\ 8)}} (\mathbb{F}_p^*)^2 \oplus \bigoplus_{\substack{p \text{ prime} \\ p \equiv 5,7 (\mathrm{mod}\ 8)}} \mathbb{F}_{p^2}^*.$$

Using the universal property of the K_2 functor, and a generalised reciprocity result (Theorem 3.10), we are then able to derive the reciprocity result

$$\left(\frac{x}{y}\right)_2 \left(\frac{y}{x}\right)_2^{-1} = \prod_{v \nmid 2} \left(\frac{x, y}{v}\right).$$

Finally, we make a seemingly unexpected connection between Weil reciprocity (a statement, that in essence is about the poles and zeros of a function) and quadratic reciprocity. In the more general form presented in Theorem 2.34, Weil reciprocity is as follows:

Theorem 0.2. *For any $f, g \in F(t)^*$, we have that*

$$\prod_v \mathrm{Nm}_{k(v)/F}(f, g)_v = 1, \tag{1}$$

where the product is taken over all discrete valuations on $F(t)$ that are trivial on F.

We will use this statement to prove a quadratic reciprocity-like result for polynomials over a finite field:

Theorem 0.3. *Let p be an odd prime, and $F, G \in \mathbb{F}_p[t]$ be two nonzero, irreducible, relatively prime, monic polynomials of degree m and n respectively. Then*

$$\left(\frac{F}{G}\right) \cdot \left(\frac{G}{F}\right) \cdot (-1)^{mn(p-1)/2} = 1.$$

Outline

Chapter 1 provides the reader with the necessary background material from algebraic number theory. Assuming very little, this chapter attempts to motivate the study of number fields and their rings of integers. It introduces the discriminant, provides an insight into primes that ramify, split or remain inert in extensions of a number field F and lists results specifically related to quadratic extensions of $\mathbb{Q}$. These are particularly useful in chapter 3 when calculating $K_2(\mathbb{Q}(\sqrt{-2}))$. The second half of chapter 1 is dedicated to class field theory. Both the local and global Artin maps are introduced, with the idèlic approach being favoured over the more classical ideal-theoretic construction. We finish the chapter with the Hasse product, which plays a role in chapter 3 and also in the proof that Artin reciprocity implies quadratic reciprocity in chapter 4.

Chapter 2 gives an insight into algebraic K-theory, specifically the functors K_1 and K_2. While we begin by defining these functors in terms of elementary matrices and Steinberg groups of order n, we are mostly interested in $K_2(F)$ for a field F. With that in mind, we invoke Matsumoto's Theorem, give some examples of symbols (most notably the tame symbol associated to a prime), and introduce the definition of Milnor K-theory. There are two big results in this chapter. First, a theorem due to Kato that helps us generalise our notion of Weil reciprocity as a special case (which we prove). Second, an exploration of Tate's construction of $K_2(\mathbb{Q})$ and how it is used to prove quadratic reciprocity.

Chapter 3 attempts to mimic Tate's construction of $K_2(\mathbb{Q})$ from chapter 2 on the field $\mathbb{Q}(\sqrt{-2})$. We are able to compute $K_2(\mathbb{Q}(\sqrt{-2})$ using our understanding of the structure of the residue fields at different primes, and derive a reciprocity result after generalising the quadratic Hilbert symbol mentioned in chapter 2.

Chapter 4 turns our attention to the second aim of this thesis. Namely, to explore the relationship between three reciprocity laws: Artin reciprocity, Weil reciprocity and quadratic reciprocity. We first prove that the generalised formulation of Weil reciprocity from chapter 2 follows from the global Artin map, where instead of a number field, we use the function field of a smooth, projective, irreducible curve over a finite field. This requires some background material on finite étale algebras that is introduced in the beginning of the chapter. Next, we prove the more well-known result that Artin reciprocity implies quadratic reciprocity and we finish off the thesis by proving that Weil reciprocity also implies quadratic reciprocity.

A Brief Note on Notation

As mentioned above, we will be looking at some problems in algebraic number theory through the lens of algebraic K-theory. When introducing the necessary results from classical algebraic number theory it seems most natural to follow established authors like Milne [13] and Neukirch [19] and denote fields by the

letter K. However, when transitioning to algebraic K-theory, we hope the reader agrees that, for example, the notation $K_2(K)$ just doesn't feel right. With $K_2(F)$ looking more satisfactory, we have made the decision throughout the entire thesis to let F denote a field[2].

We have also made the, somewhat arbitrary, decision to use *prime* instead of *place*[3] to denote an equivalence class of non-trivial valuations on F.

Acknowledgements

There are a lot of people to thank here! I'd like to start with my supervisor Håkon Kolderup for his unwavering support, guidance and enthusiasm during our weekly meetings. Thanks to Andreas for also taking MAT4250 and making class field theory more approachable. Thanks to Alexander and Aleksander, two of the smartest people I know, who I can go to with (trivial) problems at any time and they will help (I still don't know how to terminal)! Thanks also to Arne, Jakob, Ingeborg and Sasha for our great 'lesesal' vibes. Thank you to ('ma lucky charm') Leandros for introducing me to the importance of 'norsk julemat', Herman for all the chess, bouldering and 'rekesalat', and Are for being older than me. Thanks to Jon Pål for allowing me to use my skills to expand some brackets and count to six - a great insight into enumerative geometry!

And finally, thanks to Beate, my wife, for among everything else she does, encouraging me to take time out of my career to study again.

[2]There is one instance that may cause the reader mild irritation. Before Theorem 1.34, where, for an unramified extension, we give the isomorphism $\mathrm{Gal}(L/F) \cong \mathrm{Gal}(l/k)$, where l and k are the residue fields of L and F respectively. We hope that the reader agrees that f seems wrong here, and the normal notation for a residue field k seems acceptable in its place.

[3]The use of place in the previous footnote is not an attempt at a pun, I promise.

Chapter 1

Algebraic Number Theory

Perhaps one of the first motivations for studying algebraic number theory was to prove Fermat's Last Theorem. In 1847, the French mathematician, Gabriel Lamé, announced a proof at the Paris Academy. His proof relied on factorising the polynomial $X^p + Y^p$, for some prime p using p-th roots of unity. If ζ denotes a primitive p-th root of unity, then we have

$$X^p + Y^p = (X + Y)(X + \zeta Y) \dots (X + \zeta^{p-1} Y)$$

in the ring $\mathbb{Z}[\zeta]$.

Therefore, a solution (a, b, c) to Fermat's equation would satisfy

$$\prod_{i=0}^{p-1} (a + \zeta^i b) = c^p.$$

Lamé then showed that all the terms $a + \zeta^i b$ are relatively prime. Since the product is a p-th power, this then implies that each individual term is a p-th power. Lamé was then able to derive a contradiction, thus proving, in his mind, Fermat's Last Theorem[1].

However, the issue with this proof was that it relied on the rather subtle assumption that $\mathbb{Z}[\zeta]$ is a unique factorisation domain. Already for $p = 23$ this is not the case[2]. This leads to a very natural question about which rings do have unique factorisation.

The first three sections of this chapter are dedicated to some of the preliminary algebraic number theory used as motivation for the remarks above. This leads us to think about the factorisation of prime ideals in extensions of number fields, which then leads naturally into class field theory. We introduce both the local and global Artin maps in the final section of this chapter.

[1] For a more detailed account, see, for example [5].

[2] In fact, it is known that we only have unique factorisation for primes $p \leq 19$. See, for example [13, §6].

1.1 Introductory Algebraic Number Theory

A *number field* is a finite field extension of $\mathbb{Q}$, and the integral closure of $\mathbb{Z}$ in a number field F is called the *ring of integers*, denoted by $\mathcal{O}_F \subset F$.

Let d be a squarefree integer and let $F = \mathbb{Q}(\sqrt{d})$. Recall the following result, the proof of which can be found in, for example, [8, Proposition 13.1.1].

Proposition 1.1. *The ring of integers $\mathcal{O}_F$ in $F = \mathbb{Q}(\sqrt{d})$ is*

$$\mathcal{O}_F = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2, 3 \pmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

To illustrate when unique factorisation goes wrong, we state the following example.

Example 1.2. Consider $F = \mathbb{Q}(\sqrt{-14})$. By Proposition 1.1, we have that $\mathcal{O}_F = \mathbb{Z}[\sqrt{-14}]$ and that $\mathcal{O}_F$ is not a unique factorisation domain. In fact,

$$15 = 3 \times 5 = (1 + \sqrt{-14})(1 - \sqrt{-14}).$$

Using an argument involving norms, it is possible to verify that $3, 5, 1 + \sqrt{-14}$ and $1 - \sqrt{-14}$ are all irreducible in $\mathcal{O}_F$ and hence give rise to two distinct factorisations of 15 in $\mathcal{O}_F$.

Remark 1.3. The failure of unique factorisation in general paved the way for mathematicians like Kummer and Dedekind to shift away from factorisations of an integral *element* of a ring towards the possibility of unique factorisation of an *ideal* of that ring.

Consider the example above. While 15 does not factorise uniquely as an element of $\mathcal{O}_F$, we have that

$$(15) = (3)(5) = (1 + \sqrt{-14})(1 - \sqrt{-14}). \tag{1.1}$$

If we let $\mathfrak{p} = (3, 1 + \sqrt{-14})$ and $\mathfrak{q} = (5, 1 + \sqrt{-14})$, then eq. (1.1) becomes

$$(15) = \mathfrak{p}\overline{\mathfrak{p}}\mathfrak{q}\overline{\mathfrak{q}} = \mathfrak{p}\mathfrak{q}\overline{\mathfrak{p}}\overline{\mathfrak{q}},$$

and our issue of unique factorisation is resolved in this case.

More generally, unique factorisation of ideals exists in Dedekind domains (defined below) and the ring of integers $\mathcal{O}_F$ for a number field F is a Dedekind domain. The proofs of these statements can be found in [13, §3].

Definition 1.4. A *Dedekind domain* is an integral domain A such that

1. A is noetherian,
2. A is integrally closed, and
3. every nonzero prime ideal is maximal.

Theorem 1.5 ([13, Theorem 3.29])**.** *Let A be a Dedekind domain with field of fractions F, and let B be the integral closure of A in a finite separable extension L of F. Then B is a Dedekind domain.*

Remark 1.6. Since $\mathbb{Z}$ is a Dedekind domain, it follows immediately that the ring of integers $\mathcal{O}_F$ for a number field F is a Dedekind domain.

Theorem 1.7 ([13, Theorem 3.7])**.** *Let A be a Dedekind domain. Every proper, nonzero ideal $\mathfrak{a} \subset A$ can be written uniquely in the form*

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \dots \mathfrak{p}_n^{r_n},$$

where the $\mathfrak{p}_i$ are distinct prime ideals and each $r_i > 0$.

Remark 1.8. It is well-known that any principal ideal domain is a unique factorisation domain. In general, the converse is false. For example, given a field k, the polynomial ring $k[x, y]$ is a unique factorisation domain, but (x, y) is not a principal ideal. However, for a Dedekind domain, the converse is indeed true[3].

1.2 The class group of F

In the course of proving Theorem 1.7, one shows how to invert a nonzero prime ideal. The inverse is an $\mathcal{O}_F$-module that lies in F, but not in $\mathcal{O}_F$. For example, in $\mathbb{Q}$, the inverse of $2\mathbb{Z}$ is $(1/2)\mathbb{Z}$. This leads to the definition of *fractional ideals*, and it turns out that these ideals form a group.

Definition 1.9. Let A be a Dedekind domain. A *fractional ideal* of A is a nonzero A-submodule $\mathfrak{a}$ of F such that

$$c\mathfrak{a} = \{ca : a \in \mathfrak{a}\}$$

is contained in A for some nonzero $c \in A$.

Theorem 1.10 ([13, Theorem 3.20])**.** *The set* $\mathrm{Id}(A)$ *of fractional ideals is a group; in fact, it is the free abelian group on the set of nonzero prime ideals.*

To get a sense of how far away a ring is from being a unique factorisation domain, we can define the ideal class group as follows:

Definition 1.11. For a Dedekind domain A, the *ideal class group* of A, $\mathrm{Cl}(A)$, is given by

$$\mathrm{Cl}(A) = \mathrm{Id}(A)/\mathrm{P}(A),$$

where $\mathrm{P}(A) \subset \mathrm{Cl}(A)$ is the subgroup of principal ideals.

We now state two important results in the search for unique factorisation. Let $\mathfrak{a}$ be a nonzero ideal in $\mathcal{O}_F$. Recall that the numerical norm $\mathbb{N}(\mathfrak{a}) \coloneqq (\mathcal{O}_F : \mathfrak{a})$ is defined to be the index of $\mathfrak{a}$ in $\mathcal{O}_F$.

[3]For a proof of this statement, see, for example [13, Proposition 3.18].

Theorem 1.12 ([13, Theorem 4.3])**.** *Let F be a degree n field extension of $\mathbb{Q}$. Let Δ_F denote the discriminant of $F/\mathbb{Q}$. Let $2s$ be the number of nonreal complex embeddings of F. Then, there exists a set of representatives for the ideal class group of F consisting of ideals $\mathfrak{a}$ with*

$$\mathbb{N}(\mathfrak{a}) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s |\Delta_F|^{\frac{1}{2}}.$$

Remark 1.13. The bound above is commonly referred to as the Minkowski bound.

Definition 1.14. The *class number* of A is the order of $\mathrm{Cl}(A)$.

Remark 1.15. In the case that A is the ring of integers $\mathcal{O}_F$ for a number field F, it is common to refer to $\mathrm{Cl}(\mathcal{O}_F)$ as the *ideal class group* of F, and its order as the *class number* of F, denoted h_F.

Theorem 1.16 ([13, Theorem 4.4])**.** *The class number of F is finite.*

Example 1.17. Let $F = \mathbb{Q}(i)$. More elementary methods can be used to show that $\mathbb{Z}[i]$ is a principal ideal domain, but we apply Theorem 1.12 to prove this result. Note that there is one pair of complex embeddings, namely the identity and complex conjugation, giving $s = 1$. Furthermore, the discriminant $\Delta_F = -4$ and so the Minkowski bound becomes

$$\mathbb{N}(\mathfrak{a}) \leq \frac{2}{4}\left(\frac{4}{\pi}\right)|-4|^{\frac{1}{2}} < 1.27.$$

Since there are no such ideals other than $\mathbb{Z}[i]$ satisfying this bound, $\mathbb{Z}[i]$ is a principal ideal domain, and hence a unique factorisation domain.

Example 1.18. Motivated by the example above, we can find quadratic extensions F of $\mathbb{Q}$ for which the class group is trivial by checking when the Minkowski bound is less than 2. For a real quadratic extension, this is the case when $|\Delta_F| < 16$. For an imaginary quadratic extension, this happens when $|\Delta_F| < \pi^2$.

This tells us that the class number of $\mathbb{Q}(\sqrt{d})$ is 1 when $d = 2, 3, 5, 13, -1, -2, -3$ and -7. There are other quadratic extensions of $\mathbb{Q}$ for which the class number is 1, but the Minkowski bound is not less than 2, and so more work is required to prove that the class group is trivial.

Example 1.19. We now look at an example when the class group is not trivial. Let $F = \mathbb{Q}(\sqrt{-5})$. Here, $\mathbb{N}(\mathfrak{a}) \leq \frac{2}{4}\left(\frac{4}{\pi}\right)\sqrt{20} < 3$. Now, every ideal satisfying this bound must divide (2). In fact, $(2) = \mathfrak{p}^2$, where $\mathfrak{p} = (2, 1 + \sqrt{-5})$, and $\mathbb{N}(\mathfrak{p}^2) = \mathbb{N}(2) = 4$, so that $\mathbb{N}(\mathfrak{p}) = 2$. If $\mathfrak{p}$ were a principal ideal, then there would exist an element $\alpha = m + n\sqrt{-5}$ such that $\mathrm{Nm}(\alpha) = m^2 + 5n^2 = 2$. Since no such m and n exist, the ideals $\mathbb{Z}[\sqrt{-5}]$ and $\mathfrak{p}$ form a set of representatives for $\mathrm{Cl}(\mathbb{Z}[\sqrt{-5}])$ and $\mathrm{Cl}(\mathbb{Z}[\sqrt{-5}])$ has order 2.

1.3 Factorising prime ideals in extensions

Throughout this section, we take F to be a number field and $\mathcal{O}_F$ be the ring of integers of F. By Theorem 1.7, any prime ideal $\mathfrak{p}$ factors in an extension L of F as

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g},$$

where $e_i \geq 1$, and $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ are the prime ideals of $\mathcal{O}_L$ lying above $\mathfrak{p}$.

If any of the e_i are strictly greater than 1, then we say that $\mathfrak{P}_i$ is *ramified* in L. The number e_i is called the *ramification index*. We write f_i for the degree of the field extension $[\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_F/\mathfrak{p}]$ and call this the *residue class degree*. A prime $\mathfrak{p}$ *splits* in L if $e_i = f_i = 1$ for all i, and is *inert* in L if $\mathfrak{p}\mathcal{O}_L$ is a prime ideal (that is, $g = e = 1$).

Here, we let $k(\mathfrak{p}) \coloneqq \mathcal{O}_F/\mathfrak{p}$ denote the residue field at $\mathfrak{p}$.

Example 1.20. Take $F = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{-2})$. Then, in $\mathbb{Z}[\sqrt{-2}]$, $(2) = (\sqrt{-2})^2$, so (2) is ramified with ramification index 2. The ideal (3) splits as the product of two prime ideals $(3) = (1 + \sqrt{-2})(1 - \sqrt{-2})$, while the ideal (5) is inert with residue field $\mathbb{Z}[\sqrt{-2}]/(5)$ and residue class degree 2.

We state two results that are useful in determining which primes ramify. For proofs of these statements, see [13, §3].

Theorem 1.21 ([13, Theorem 3.34])**.** *Let n be the degree of a field extension L over a number field F and let $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ be the prime ideals dividing $\mathfrak{p}$. Then,*

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

Furthermore, if L is Galois over F, then all the ramification numbers are equal and all of the residue class degrees are equal, so that

$$efg = n.$$

Theorem 1.22 ([13, Theorem 3.35])**.** *A prime ideal $\mathfrak{p} = (p)$ in $\mathbb{Z}$ ramifies in $\mathcal{O}_F$ if and only if $p \mid \Delta_F$, where, as in the previous section, Δ_F denotes the discriminant of F.*

From this, we have the useful result that:

Corollary 1.23. *Only a finite number of primes $p \in \mathbb{Z}$ ramify in $\mathcal{O}_F$.*

While it is useful to know which primes ramify, it may also be useful to know when a prime splits or is inert. The following theorem provides us with an approach.

Theorem 1.24 ([13, Theorem 3.41])**.** *Let L be a finite field extension of F and let $\mathfrak{p}$ be a prime in $\mathcal{O}_F$. Choose $\alpha \in \mathcal{O}_L$ such that $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = (\mathcal{O}_F/\mathfrak{p})[\bar{\alpha}]$, where $\bar{\alpha}$ denotes the image of α mod $\mathfrak{p}$. Let $f(X) \in \mathcal{O}_F[X]$ be the minimal polynomial of α and assume that*

$$f(X) = \prod_{i=1}^{g} g_i(X)^{e_i} \pmod{\mathfrak{p}\mathcal{O}_F[X]},$$

where $e_i \geq 1$ and the $g_i(X)$ are distinct monic polynomials whose images are irreducible in $(\mathcal{O}_F/\mathfrak{p})[X]$. Then we have the prime decomposition

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} (\mathfrak{p}, g_i(\alpha))^{e_i}.$$

Moreover, the residue class degree f_i is equal to the degree of g_i.

We will spend time in the later chapters considering quadratic extensions and so it will be of particular use to reformulate the above results for quadratic extensions. In doing so, we also characterise when primes are split and inert and describe the residue fields in each case.

Proposition 1.25. *Let d be a squarefree integer and consider $F = \mathbb{Q}(\sqrt{d})$. Let $p \in \mathbb{Z}$ be an odd prime. Then*

- *p ramifies $\iff p \mid d$;*
- *p is inert $\iff \left(\frac{d}{p}\right) = -1$;*
- *p splits $\iff \left(\frac{d}{p}\right) = 1$.*

If $p = 2$, then

- *2 ramifies $\iff d \equiv 2, 3 \pmod 4$;*
- *2 is inert $\iff d \equiv 5 \pmod 8$;*
- *2 splits $\iff d \equiv 1 \pmod 8$.*

Proof. Let $\mathcal{O}_F = \mathbb{Z}[\alpha]$, where, by Proposition 1.1, α is $\sqrt{d}$ or $\frac{1+\sqrt{d}}{2}$ depending on whether $d \equiv 2, 3 \pmod 4$ or $d \equiv 1 \pmod 4$. The minimal polynomial f of α is therefore either $x^2 - d$ or $x^2 - x - \frac{d-1}{4}$, and so the discriminant Δ_F is either $4d$ or d. By Theorem 1.22, it follows that an odd prime p ramifies if and only if $p \mid d$.

Now, if $p \nmid d$, we use Theorem 1.24 to see that p splits if and only if f has distinct roots modulo p. If $f(x) = (x-a)(x-b)$ for some distinct $a, b \in \mathbb{Z}/p\mathbb{Z}$, then $\Delta_F = (a-b)^2 \pmod p$, which is equivalent[4] to saying d is a square modulo p, i.e. $\left(\frac{d}{p}\right) = 1$. Conversely, if $\left(\frac{d}{p}\right) = 1$, then we can write $d \equiv m^2 \pmod p$, where $p \nmid m$. Then, if $d \equiv 1 \pmod 4$, it is easy to see that $(1 \pm m)/2$ are two distinct roots of f and so p splits. In the case $d \equiv 2, 3 \pmod 4$, the distinct roots are $\pm m$.

[4]This works for both $\Delta_F = d$ and $\Delta_F = 4d$.

If $p = 2$, then Proposition 1.1 says that p ramifies if and only if $d \equiv 2, 3 \pmod 4$. In the case $d \equiv 1 \pmod 4$, it is easy to check that $f(x) = x^2 - x - \frac{d-1}{4}$ has distinct roots modulo 2, i.e. 2 splits, if and only if $\frac{d-1}{4} \equiv 0 \pmod 2$ and this happens if and only if $d \equiv 1 \pmod 8$. Similarly, one can check that 2 is inert if and only if $\frac{d-1}{4} = 1 \pmod 2$ which happens if and only if $d \equiv 5 \pmod 4$.

□

The results above give us an indication of what the residue fields of a quadratic number field look like at different prime ideals.

Proposition 1.26. *Let d be a squarefree integer and let $F = \mathbb{Q}(\sqrt{d})$ be a quadratic number field. Then, for a prime p, we have the following:*

1. *If p ramifies, then $k(\mathfrak{p}) \cong \mathbb{F}_p$;*
2. *If p splits, then $k(\mathfrak{p}) \cong \mathbb{F}_p$;*
3. *If p is inert, then $k(\mathfrak{p}) \cong \mathbb{F}_{p^2}$;*

Proof. Let p be a prime number and suppose we have the decomposition $p\mathcal{O}_F = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}$, where each $\mathfrak{P}_i$ is a prime ideal of $\mathcal{O}_F$ lying above p. Then, by Theorem 1.21, we have

$$\sum_{i=1}^{g} e_i f_i = 2.$$

1. If p ramifies, then $g = 1$ and $e_1 = 2$, giving $f_1 = 1$. Hence $k(\mathfrak{p})$ is a degree 1 extension of $\mathbb{F}_p$, i.e. it is isomorphic to $\mathbb{F}_p$.
2. If p splits, then $g = 2$ and $f_i = e_i = 1$ for $i = 1, 2$. Again, this implies that $k(\mathfrak{p}) \cong \mathbb{F}_p$.
3. Finally, if p is inert, then $g = 1$, $e_1 = 1$ and so $f_1 = 2$. That is to say, $k(\mathfrak{p})$ is a degree 2 extension of $\mathbb{F}_p$, i.e. $k(\mathfrak{p}) \cong \mathbb{F}_{p^2}$.

□

We end this section with one final result that will be used later on.

Proposition 1.27 ([13, Proposition 4.1])**.** *Let A be a Dedekind domain with field of fractions F and let B be the integral closure of A in a finite separable extension L. Suppose that L is Galois over F and let $\mathfrak{P}$ be a nonzero prime ideal of B lying above $\mathfrak{p} \subset A$. Then*

$$\mathrm{Nm}_{L/F}\mathfrak{P} \cdot B = \prod_{\sigma \in \mathrm{Gal}(L/F)} \sigma\mathfrak{b}.$$

1.4 Local and global class field theory

The main goal of class field theory is to describe the Galois extensions of a local or global field in terms of the arithmetic of the field itself[5]. By 1930, the theory had been developed for abelian extensions[6] by Hilbert, Furtwängler, Takagi and others. In 1967, a letter from Langlands to Weil gave an indication of how the theory for nonabelian extensions should progress. We shall focus only on abelian extensions and in this section introduce the notion of symbols over number fields which serve as one of the links between number theory and algebraic K-theory. In our treatment of global class field theory, rather than using ideals, we take the more modern idèlic approach, which has the advantage of making the connection to local class field theory more transparent[7].

We begin by fixing some notation, for the most part following [13] and [14]. Let F be a field, either local or global. By a *prime*[8], we mean an equivalence class of non-trivial valuations on F. By Ostrowski's Theorem [13, Theorem 7.14], there is exactly one prime for each nonzero prime ideal in $\mathcal{O}_F$, for each real embedding $F \hookrightarrow \mathbb{R}$ and for each conjugate pair of nonreal embeddings $F \hookrightarrow \mathbb{C}$. We call these primes finite, real infinite and complex infinite respectively. A real prime is said to split in an extension L/F if every prime lying over it is real, otherwise it ramifies in L.

Example 1.28. Let $F = \mathbb{Q}$ and $L = \mathbb{Q}[\sqrt{-5}]$. Then the primes that ramify in L are precisely $(2) = (2, 1 + \sqrt{-5})^2$, $(5) = (\sqrt{-5})^2$ and the real embedding, which we denote by ∞.

Definition 1.29. Let v be a prime of F. We will denote by[9]:

- F^{ab} the union of all finite abelian extensions of F in some fixed algebraic closure of F;
- F_v the completion of F at v, with valuation ring[10] $\mathcal{O}_v$;
- π_v a uniformizer of F_v, that is, a generator of the maximal ideal $\mathfrak{p}_v$ of $\mathcal{O}_v$ for v finite;
- $k(v) \coloneqq \mathcal{O}_v/\mathfrak{p}_v$ the residue field, for v finite;
- $q_v \coloneqq \#k(v)$;
- $U_v \coloneqq \mathcal{O}_v^*$ the unit group, where we set $U_v \coloneqq \mathbb{R}_{>0}$ when v is real infinite;
- $U_v^1 \coloneqq 1 + \mathfrak{p}_v$, for v finite;

[5] For a Galois extension L of F, this typically means studying the primes in $\mathcal{O}_F$ that split in $\mathcal{O}_L$.

[6] By abelian extensions, we mean that the Galois group $\mathrm{Gal}(L/F)$ is abelian.

[7] In fact, we shall see the global Artin map defined as a product of local Artin maps.

[8] As mentioned in the introduction, some authors use the terminology *place* instead.

[9] Similar notation follows naturally for an extension L of F with a prime w lying over v.

[10] Here, we only have that it is a ring when v is a finite prime.

- $m \coloneqq \mu(F), m_v \coloneqq \mu(F_v)$ the groups of roots of unity of F and F_v respectively;
- $i_v : F \hookrightarrow F_v$ the embedding of F into its completion F_v at v.

Definition 1.30. Let v be a prime of F. We denote by ord_v the corresponding valuation, which takes the following forms:

- if v is a finite prime, $\mathrm{ord}_v : F^* \to \mathbb{Z}$ is the $\mathfrak{p}_v$-adic valuation.
- if v is a real infinite prime, the valuation $\mathrm{ord}_v : F^* \to \mathbb{Z}/2$ is defined as:

$$\mathrm{ord}_v(x) \coloneqq \begin{cases} 0 & \text{if } i_v(x) > 0 \\ 1 & \text{if } i_v(x) < 0. \end{cases}$$

- if v is a complex infinite prime, we set $\mathrm{ord}_v \coloneqq 0$.

Before defining the local and global Artin maps, we give a brief introduction to idèles.

The *restricted product* $\prod'_{i\in I} G_i$ of a family of locally compact topological groups $\{G_i\}_{i\in I}$ is, by definition, the subset of $\prod_{i\in I} G_i$ consisting of all elements $(g_i)_{i\in I}$ for which $g_i \in F_i$ for almost all i, where F_i is some compact subgroup of G_i. Thus, the restricted product is a locally compact group, and it is given a topology whose basis elements are of the form $\prod_i A_i$, where $A_i \subset G_i$ is open in G_i for all i and $A_i = F_i$ for almost all i.

Definition 1.31. For a number field F, the group of idèles is

$$\begin{aligned} \mathbb{I}_F &= \prod_v{}' F_v^* \\ &= \Big\{(a_v)_v \in \prod_v F_v^* : a_v \in U_v \text{ for almost all } v\Big\}. \end{aligned}$$

Remark 1.32. For a finite set of primes S, which contain the infinite primes, one may also define $\mathbb{I}_F$ as the colimit

$$\mathbb{I}_F = \varinjlim_S \mathbb{I}_S.$$

Here, we have that $\mathbb{I}_S = \prod_{v\in S} F_v^* \times \prod_{v\notin S} U_v$.

Remark 1.33. There is a natural 'diagonal' embedding

$$\begin{aligned} i\colon F^* &\longrightarrow \mathbb{I}_F \\ a &\longmapsto (i_v(a))_v. \end{aligned}$$

It is worth noting that this is a well defined map since a is a unit almost everywhere. For the sake of brevity, we will often write F^* instead of $i(F^*)$ and g instead of $i(g)$.

For each prime v, we can also embed the local field F_v into the idèle group $\mathbb{I}_F$ via the map

$$\begin{aligned} F_v^* &\longrightarrow \mathbb{I}_F \\ a &\longmapsto (1, 1, \ldots, 1, a, 1, 1, \ldots). \end{aligned}$$

where a appears at the vth coordinate.

For the remainder of this section, we assume that L/F is an abelian extension of F, i.e. that $G = \mathrm{Gal}(L/F)$ is abelian. Let v be a prime of F and $w|v$ a prime of L lying above v.

As proved in [13, Proposition 7.50], if L is unramified over F, then the action of $\mathrm{Gal}(L/F)$ on $\mathcal{O}_L$ gives an isomorphism $\mathrm{Gal}(L/F) \cong \mathrm{Gal}(l/k)$, where l and k are the residue fields of L and F respectively. Therefore, $\mathrm{Gal}(L/F)$ is cyclic, generated by the unique element σ such that for all $x \in \mathcal{O}_L$, $\sigma(x) = x^{q_v} \pmod{\mathfrak{p}_w}$. This element σ is called the *Frobenius element* of $\mathrm{Gal}(L/F)$ and is denoted by $\mathrm{Frob}_{L/F}$.

Theorem 1.34 ([14, Theorem 1.1])**.** *For every nonarchimedean local field F, there exists a unique homomorphism*

$$\phi_F \colon F^* \longrightarrow \mathrm{Gal}(F^{\mathrm{ab}}/F)$$

such that:

1. *For every prime element $\pi \in F$ and every finite unramified extension L of F, $\phi_F(\pi)$ acts on L as $\mathrm{Frob}_{L/F}$.*
2. *For every finite abelian extension L of F, $\mathrm{Nm}_{L/F}(L^*)$ is contained in the kernel of the restriction $\phi_F|_L$. Furthermore, ϕ_F induces an isomorphism*

$$\phi_{L/F} \colon F^*/\mathrm{Nm}_{L/F}(L^*) \longrightarrow \mathrm{Gal}(L/F).$$

In particular,

$$(F^* : \mathrm{Nm}_{L/F}(L^*)) = [L : F].$$

Remark 1.35. The second statement in Theorem 1.34 says that, for every finite abelian extension L of F, the following diagram commutes:

$$\begin{array}{ccc} F^* & \xrightarrow{\phi_F} & \mathrm{Gal}(F^{\mathrm{ab}}/F) \\ \downarrow & & \downarrow{\scriptstyle \tau \mapsto \tau|_L} \\ F^*/\mathrm{Nm}_{L/F}(L^*) & \xrightarrow{\phi_{L/F}} & \mathrm{Gal}(L/F). \end{array}$$

We call $\phi_{L/F}$ the *local Artin map.*

Remark 1.36. To make the connection later on to global class field theory more clear, we simplify the above diagram slightly. Let Φ_F denote the composition of ϕ_F followed by the map $\tau \mapsto \tau|_L$. Then the commutative diagram becomes

$$\begin{array}{ccc} F^* & \xrightarrow{\Phi_F} & \mathrm{Gal}(L/F) \\ \downarrow & \nearrow_{\phi_{L/F}} & \\ F^*/\mathrm{Nm}_{L/F}(L^*). & & \end{array}$$

Corollary 1.37 ([14, Corollary 1.2])**.** *Let F be a nonarchimedean local field, and assume there exists a homomorphism $\phi\colon F \to \mathrm{Gal}(F^{\mathrm{ab}}/F)$ satisfying the two conditions of Theorem 1.34. Then*

1. *The map $L \mapsto \mathrm{Nm}_{L/F}(L^*)$ is a bijection from the set of finite abelian extensions of F onto the set of norm groups in F^*;*
2. *$L \subset L' \iff \mathrm{Nm}_{L/F}(L^*) \supset \mathrm{Nm}_{L/F}(L'^*)$;*
3. *$\mathrm{Nm}_{L/F}((L \cdot L')^*) = \mathrm{Nm}_{L/F}(L^*) \cap \mathrm{Nm}_{L/F}(L'^*)$;*
4. *$\mathrm{Nm}_{L/F}((L \cap L')^*) = \mathrm{Nm}_{L/F}(L^*) \cdot \mathrm{Nm}_{L/F}(L'^*)$;*
5. *Every subgroup of F^* containing a norm group is itself a norm group.*

We state one final result which provides a useful application of the local Artin map.

Theorem 1.38 ([14, Theorem 1.4])**.** *The norm groups in F^* are precisely the open subgroups of finite index.*

Example 1.39. Let p be an odd prime[11]. By Theorem 1.38 and Corollary 1.37, we have a one-to-one correspondence between quadratic extensions of $\mathbb{Q}_p$ and index 2 subgroups of $\mathbb{Q}_p^*$.

It is a well-known fact[12] that

$$\mathbb{Q}_p^* \cong \langle p \rangle \oplus \langle \zeta \rangle \oplus U_p^1,$$

where $\langle \zeta \rangle = \mu_{p-1}$ is the group of $(p-1)$-th roots of unity and $U_p^1 = (1 + p\mathbb{Z}_p)$. It follows[13] that

$$\mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z},$$

with representatives $\{1, p, \zeta, \zeta p\}$. Thus, the quadratic extensions of $\mathbb{Q}_p$ are

$$\mathbb{Q}_p(\sqrt{p}),\ \ \mathbb{Q}_p(\sqrt{\zeta}),\ \ \mathbb{Q}_p(\sqrt{\zeta p}).$$

[11] A similar computation can be done for the case $p = 2$. See, for example, [7, Exercise 1.6.5].

[12] The argument here relies on applying Hensel's Lemma ([6, Theorem 3.4.1] to the polynomial $f(x) = x^{p-1} - 1$. We note here that it is also possible to generalise this statement to arbitrary global number fields F. Indeed, Proposition 1.35 in [10] says that $F_v^* \cong \pi_v^{\mathbb{Z}} \oplus \mu_{q_v - 1} \oplus U_v^1$.

[13] See, for example, [6, Corollary 3.4.4] for another application of Hensel's Lemma to compute squares in $\mathbb{Q}_p^*$.

Now, it is not too hard to see that the index 2 subgroups of $\mathbb{Q}_p^*$ are given by

$$\begin{aligned} N_1 &\coloneqq \langle p^2 \rangle \oplus \langle \zeta \rangle \oplus U_p^1, \\ N_2 &\coloneqq \langle p \rangle \oplus \langle \zeta^2 \rangle \oplus U_p^1, \\ N_3 &\coloneqq \langle \zeta p \rangle \oplus \langle \zeta^2 \rangle \oplus U_p^1. \end{aligned}$$

Since N_1 contains the group of units $\mathbb{Z}_p^*$, it corresponds to the unramified extension[14], $\mathbb{Q}(\sqrt{\zeta})$. Before we associate N_2 and N_3 to quadratic extensions, we note that p is a norm in $\mathbb{Q}_p(\sqrt{-p})$ and ζp is a norm in $\mathbb{Q}_p(\sqrt{-\zeta p})$. Therefore, it seems almost more natural to write the remaining two quadratic extensions as $\mathbb{Q}_p(\sqrt{-p})$ and $\mathbb{Q}_p(\sqrt{-\zeta p})$. In doing this, it becomes clear that they correspond to N_2 and N_3 respectively. A small calculation[15] shows that, for $p \equiv 1 \pmod 4$,

$$\mathbb{Q}_p(\sqrt{-p}) = \mathbb{Q}_p(\sqrt{p}) \text{ and } \mathbb{Q}_p(\sqrt{-\zeta p}) = \mathbb{Q}_p(\sqrt{\zeta p}).$$

If, however, $p \equiv 3 \pmod 4$, then the extensions on the right must be swapped with one another.

Remark 1.40. In the archimedean case, there is also a local Artin map. The abelian extensions of $F = \mathbb{R}$ are $\mathbb{R}$ and $\mathbb{C}$ and their norm groups are $\mathbb{R}^*$ and $\mathbb{R}_{>0}$ respectively. In the case $L = \mathbb{R}$, the map $\phi_{L/F}$ is trivial, while for $L = \mathbb{C}$ we have

$$\begin{aligned} \phi_{\mathbb{R}} \colon \mathbb{R}^*/\mathbb{R}_{>0} &\longrightarrow \mathrm{Gal}(\mathbb{C}/\mathbb{R}) \\ x &\longmapsto \sigma^{\mathrm{ord}_\infty(x)} \end{aligned}$$

where, as in Definition 1.30,

$$\mathrm{ord}_\infty(x) \coloneqq \begin{cases} 0 & \text{if } x > 0 \\ 1 & \text{if } x < 0 \end{cases}$$

and σ acts as complex conjugation. Since $\mathrm{Nm}_{\mathbb{C}/\mathbb{R}}(\mathbb{C}^*) = \mathbb{R}_{>0}$, we have a natural isomorphism

$$\mathbb{R}^*/\mathbb{R}_{>0} \cong \mathbb{Z}/2\mathbb{Z} \cong \mathrm{Gal}(\mathbb{C}/\mathbb{R}).$$

As mentioned at the beginning of this section, it is possible to define a global Artin map in terms of idèles. There are two main benefits over the more classical ideal-theoretic construction. First, we shall see the global Artin map defined as a product of the local maps. Second, we get a unified treatment of the embeddings of F into its completion at all primes, including the infinite ones.

Proposition 1.41 ([14, Proposition 5.2])**.** *For a global field F, there exists a unique continuous homomorphism $\rho_F \colon \mathbb{I}_F \to \mathrm{Gal}(F^{\mathrm{ab}}/F)$ such that the following diagram commutes*

[14]More generally, for an unramified extension L/F, the group of units $\mathcal{O}_F^*$ is contained in $\ker \phi_{L/F} = \mathrm{Nm}_{L/F}(L^*)$. An explanation of this is given in paragraph 1.8 of [13].

[15]Essentially, this boils down to showing that $i = \sqrt{-1} \in \mu_{p-1}$ if and only if $p \equiv 1 \pmod 4$, which is straightforward.

$$\begin{array}{ccc} \mathbb{I}_F & \xrightarrow{\hat{\rho}_F} & \mathrm{Gal}(L/F) \\ \uparrow & & \uparrow \\ F_v^* & \xrightarrow{\Phi_{F_v}} & \mathrm{Gal}(L_w/F_v). \end{array}$$

Here, as in Remark 1.36, $\hat{\rho}_F$ is given by the composition of ρ_F followed by the map $\tau \mapsto \tau|_L$ for some element $\tau \in \mathrm{Gal}(F^{\mathrm{ab}}/F)$. Furthermore, for an element $\mathbf{a} = (a_v)_v \in \mathbb{I}_F$, we have that $\hat{\rho}_F(\mathbf{a}) = \prod_v \Phi_{F_v}(a_v)$.

As in the local case, we expect an isomorphism between the Galois group $\mathrm{Gal}(L/F)$ and a quotient of the group of idèles by some norm group, which we must first define. We recall from [13, Proposition 8.2] the isomorphism

$$L \otimes_F F_v \xrightarrow{\cong} \prod_{w|v} L_w.$$

It follows for any $\alpha \in L$ that

$$\mathrm{Nm}_{L/F}(\alpha) = \prod_{w|v} \mathrm{Nm}_{L_w/F_v}(\alpha).$$

For an idèle $\mathbf{a} = (a_w)_w \in \mathbb{I}_L$, we can define $\mathrm{Nm}_{L/F}(\mathbf{a})$ to be the idèle $\mathbf{b} \in \mathbb{I}_F$ such that $b_v = \prod_{w|v} \mathrm{Nm}_{L_w/F_v}(a_w)$. This gives us the following commutative diagram

$$\begin{array}{ccc} L^* & \hookrightarrow & \mathbb{I}_L \\ \downarrow{\scriptstyle \mathrm{Nm}_{L/F}} & & \downarrow{\scriptstyle \mathrm{Nm}_{L/F}} \\ F^* & \hookrightarrow & \mathbb{I}_F. \end{array}$$

The following theorem gives us a global Artin map, in a similar manner to the local case.

Theorem 1.42 ([14, Theorem 5.3])**.** *The map $\rho_F \colon \mathbb{I}_F \to \mathrm{Gal}(F^{\mathrm{ab}}/F)$ is surjective and satisfies the following properties:*

1. *$F^* \subseteq \ker \rho_F$;*
2. *for every finite abelian extension L of F, $\hat{\rho}_F$ defines an isomorphism*

$$\rho_{L/F} \colon \mathbb{I}_F / F^* \cdot \mathrm{Nm}_{L/F}(\mathbb{I}_L) \longrightarrow \mathrm{Gal}(L/F).$$

Remark 1.43. The local and global Artin maps are also commonly referred to as local and global reciprocity maps.

We state here one final result which will be used to prove quadratic reciprocity in chapter 3. In fact, it is one of the main results in class field theory and is considered to be the generalisation of quadratic reciprocity to arbitrary abelian extensions of number fields. The theorem below follows immediately from Theorem 1.42.

Definition 1.44. For a prime v, the *Hasse symbols* $\left(\frac{-,L/F}{v}\right)$ are defined on F^* as

$$\begin{aligned}\left(\frac{-,L/F}{v}\right)\colon F^* &\longrightarrow \mathrm{Gal}(L/F)\\ x &\longmapsto [\Phi_{F_v}(x)],\end{aligned}$$

where $[\Phi_{F_v}(x)]$ denotes the image of $\Phi_{F_v}(x)$ in $\mathrm{Gal}(L/F)$.

Theorem 1.45. *For any $x \in F^*$,*

$$\prod_v \left(\frac{x,L/F}{v}\right) = 1.$$

Chapter 2

Algebraic and Milnor K-theory

The aim of this chapter is to formulate and prove Weil Reciprocity using Milnor K-theory. We motivate our study with a simpler formulation of Weil Reciprocity and then introduce the necessary tools from algebraic K-theory to generalise the statement in terms of the norm map on Milnor K-groups.

2.1 First formulation of Weil Reciprocity

To begin with, let X be a connected, compact Riemann surface and let $\mathbb{C}(X)$ denote the field of meromorphic functions on X. Let $\mathbb{C}(X)^* = \mathbb{C}(X) \setminus \{0\}$. We denote by (f) the set of zeroes and poles of $f \in \mathbb{C}(X)^*$ and we let $v_P(h)$ be the order of $h \in \mathbb{C}(X)^*$ at $P \in X$. This will be positive if P is a zero, negative if P is a pole and 0 if P is neither a zero, nor a pole. Then Weil Reciprocity can be formulated as:

Theorem 2.1. *Let $f, g \in \mathbb{C}(X)^*$ be two meromorphic functions such that $(f) \cap (g) = \emptyset$. Then*

$$\prod_{P \in X} f(P)^{v_P(g)} = \prod_{P \in X} g(P)^{v_P(f)}.$$

In fact, a stronger version, which removes the requirement that (f) and (g) are disjoint, is:

Theorem 2.2. *Let $f, g \in \mathbb{C}(X)^*$ be two meromorphic functions. Then*

$$\prod_{P \in X} (f, g)_P = 1$$

where $(f, g)_P \coloneqq (-1)^{v_P(f)v_P(g)} f^{v_P(g)}(P) g^{-v_P(f)}(P)$.

The proofs of these statements can be found in [18].

2.2 K_1 of a ring A

In order to generalise the statement above, we need to introduce algebraic K-theory. We begin with a classical treatment of the functors K_1 and K_2 of a ring A, then look at the special case when $A = F$ is a field, before turning to Milnor K-theory. A key result in what follows will be Matsumoto's theorem, which allows us to view $K_2(F)$ as the universal object with respect to the Steinberg symbols. A more thorough treatment of the following can be found in [12] and [22].

Let A be a ring. We recall the definition of GL(A), the *general linear group*, as the colimit of the directed system

$$\mathrm{GL}_1(A) \hookrightarrow \mathrm{GL}_2(A) \hookrightarrow \dots$$

where the inclusion of $\mathrm{GL}_n(A)$ into $\mathrm{GL}_{n+1}(A)$ is given by $M \mapsto \begin{pmatrix} M & 0 \\ 0 & 1 \end{pmatrix}$. Let $e_{i,j}(a)$ denote the matrix which differs from the identity matrix only by having a in the (i,j)-th position, where $i \neq j$. We call this an elementary matrix and note that the elementary $n \times n$ matrices generate a subgroup $E_n(A) \subset \mathrm{GL}_n(A)$. Just as above, we have inclusions $E_n(A) \hookrightarrow E_{n+1}(A)$ and the colimit of this directed system is denoted by $E(A)$. We also recall that the commutator subgroup of a group G is generated by its commutators $[g,h] = ghg^{-1}h^{-1}$.

Lemma 2.3 ([12, Lemma 9.7])**.** *The group $E(A)$ is the commutator subgroup of $GL(A)$.*

Definition 2.4. The *first algebraic K-group* of a ring A is:

$$K_1(A) \coloneqq \mathrm{GL}(A)/E(A).$$

Now, a ring map $A \to B$ naturally induces a map $\mathrm{GL}(A) \to \mathrm{GL}(B)$ which preserves elementary matrices, and hence a map $K_1(A) \to K_1(B)$. This means that K_1 is a covariant functor on the category of rings.

There is also a determinant map $\det\colon \mathrm{GL}(A) \to A^*$, which induces a map $K_1(A) \to A^*$. Let $SL(A)$ denote the kernel of the determinant map and let $SK_1(A) \coloneqq SL(A)/E(A)$. Writing $\mathrm{GL}_1(A)$ as A^*, which maps into A, we obtain a split exact sequence

$$1 \longrightarrow SK_1(A) \longrightarrow K_1(A) \longrightarrow A^* \longrightarrow 1.$$

Example 2.5. It is known that $SK_1(A)$ is trivial when A is a local ring [22, Lemma 1.4] or the ring of integers in a number field [2]. Hence, in this case,

$$K_1(A) \cong A^*.$$

2.3 K_2 of a ring A

We turn our focus briefly to central extensions and perfect groups.

Definition 2.6. A *central extension* of a group G by an abelian group A is a short exact sequence

$$1 \longrightarrow A \longrightarrow E \xrightarrow{\phi} G \longrightarrow 1,$$

where E is a group containing A as a central subgroup. A central extension is denoted by (E, ϕ).

The central extensions of a group G form a category, where a morphism $\psi : (E, \phi) \to (E', \phi')$ is a homomorphism $\psi : E \to E'$ over G, giving the following commutative diagram

$$\begin{array}{ccc} E & \xrightarrow{\psi} & E' \\ & \searrow^{\phi} & \downarrow{\scriptstyle \phi'} \\ & & G \end{array}$$

Thus, we can define a central extension (E, ϕ) to be *universal* if it is initial in the category of central extensions of G.

Recall that a group is *perfect* if it equals its commutator subgroup.

In order to define $K_2(A)$, we return to our study of elementary matrices. There are two immediate properties that are worth stating. First, for any $i, j \in \mathbb{N}$,

$$e_{ij}(a)e_{ij}(b) = e_{ij}(a + b).$$

Second, for any $i, j, k, l \in \mathbb{N}$, the commutator of two elementary matrices satisfies

$$[e_{ij}(a), e_{kl}(b)] = \begin{cases} 1 & \text{if } j \neq k, i \neq l \\ e_{il}(ab) & \text{if } j = k, i \neq l \\ e_{kj}(-ab) & \text{if } j \neq k, i = l. \end{cases}$$

Using these properties as motivation, we make the following definition:

Definition 2.7. Let A be a ring. For $n \geq 3$, we define $\mathrm{St}_n(A)$, *the Steinberg group of order n over A*, to be the free group generated by symbols $x_{ij}(a)$, $i \neq j$, $1 \leq i, j \leq n$, $a \in A$, subject to the following relations

1. $x_{ij}(a)x_{ij}(b) = x_{ij}(a + b)$;
2. $[x_{ij}(a), x_{kl}(b)] = x_{il}(ab)$ if $i \neq l$;
3. $[x_{ij}(a), x_{kl}(b)] = 1$ if $j \neq k$, $i \neq l$.

For every n, there are natural maps $\mathrm{St}_n(A) \to \mathrm{St}_{n+1}(A)$, and we let $\mathrm{St}(A)$ denote the colimit of the directed system. Given a ring map $f : A \to B$, we get an induced map on the free groups generated by $\{x_{ij}(a) : a \in A\}$ and $\{x_{ij} : b \in B\}$ by mapping $x_{ij}(a)$ to $x_{ij}(f(a))$. This is compatible with the relations in $\mathrm{St}(A)$ and so factors through a map $\mathrm{St}(A) \to \mathrm{St}(B)$, giving us a well-defined functor $\mathrm{St}(-)$ on the category of rings. There are also natural maps $\phi_n \colon \mathrm{St}_n(A) \to \mathrm{GL}_n(A)$ for any n, given by $x_{ij}(a) \mapsto e_{ij}(a)$. We note that the image of this map is precisely the group $E_n(A)$. Passing to the colimit, we get a map $\phi \colon \mathrm{St}(A) \to E(A)$.

Definition 2.8. The second algebraic K-group, $K_2(A)$ of a ring A is defined as the kernel of the map $\phi \colon \mathrm{St}(A) \to E(A)$.

We note that the functoriality of $\mathrm{St}(-)$ and $E(-)$ tell us that K_2 is a functor. Following the definition of K_2, we have the exact sequence

$$1 \longrightarrow K_2(A) \longrightarrow \mathrm{St}(A) \xrightarrow{\phi} E(A) \longrightarrow 1.$$

The following theorem shows that the exact sequence above is in fact a central extension of the group $E(A)$. Thus, in particular, $K_2(A)$ is an abelian group.

Theorem 2.9 ([20, Theorem 4.2.4])**.** *The group $K_2(A)$ is the center of the Steinberg group $\mathrm{St}(A)$.*

Before moving on to studying K_2 of a field, it is worth mentioning one example that will play a role later on.

Example 2.10. Let A be any ring and let

$$x = (x_{12}(1)x_{21}(-1)x_{12}(1))^4.$$

Then,

$$\begin{aligned} \phi(x) &= \left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right)^4 \\ &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^4 \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

Thus $x \in K_2(A)$. This element x appears later in Example 2.13 as the only non-trivial element of $K_2(\mathbb{Z})$.

2.4 K_2 of a field F

As we shall see later on, for a number field F, $K_2(F)$ contains information about the arithmetic of F. By this, we mean that $K_2(F)$ reveals the structure of the residue fields and how primes in F split or ramify. In order to explicitly calculate anything about $K_2(F)$ we use a simplification in our definition due to Matsumoto

[17, §12]. To formulate Matsumoto's theorem, we first look at the general case involving rings and specialise to fields later on.

We can explicitly construct elements of $K_2(A)$ for a given ring A. Let $a, b \in E(A)$ such that the commutator $[a, b] = 1$. Let x and y denote representatives for $\phi^{-1}(a)$ and $\phi^{-1}(b)$ respectively. Then $[x, y] = xyx^{-1}y^{-1} \in \mathrm{St}(A)$ and $\phi([x, y]) = 1$, so that $[x, y] \in K_2(A)$.

We must check that the element $[x, y]$ is well-defined. Suppose x' is another representative for $\phi^{-1}(a)$. Then x' and x differ by an element of $\ker(\phi) = K_2(A)$. But the theorem above tells us that $K_2(A)$ is the center of $\mathrm{St}(A)$, so we can write $x' = xz$ for some z in the center of $\mathrm{St}(A)$. Then, upon noting that z commutes with every element of $\mathrm{St}(A)$, we see that

$$\begin{aligned} [x', y] &= x'yx'^{-1}y^{-1} \\ &= xzyz^{-1}x^{-1}y^{-1} \\ &= xyx^{-1}y^{-1} \\ &= [x, y]. \end{aligned}$$

We therefore let $[\phi^{-1}(a), \phi^{-1}(b)]$ denote the element $[x, y] \in K_2(A)$, where x and y are representatives for $\phi^{-1}(a)$ and $\phi^{-1}(b)$ respectively.

Definition 2.11. Let A be a ring and $u, v \in A^*$. We define[1] the *Steinberg symbol* $\{u, v\}$ to be the element $[\phi^{-1}(d_{12}(u)), \phi^{-1}(d_{13}(v))] \in K_2(A)$, where

$$d_{12}(u) = \begin{pmatrix} u & 0 & 0 \\ 0 & u^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad d_{13}(v) = \begin{pmatrix} v & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & v^{-1} \end{pmatrix}.$$

The following result, found in [20, Lemmas 4.2.14 and 4.2.17] is straightforward to prove but requires keeping rigorous track of symbols and commutators.

Lemma 2.12. *The Steinberg symbol map*

$$\{-, -\} \colon A^* \times A^* \to K_2(A)$$

satisfies

(1) $\{u, v\} = \{v, u\}^{-1}$ *(antisymmetry);*

(2) $\{u_1u_2, v\} = \{u_1, v\}\{u_2, v\}$ *(bilinearity);*

(3) $\{u, -u\} = 1$ *for* $u \in A^*$*;*

(4) $\{u, 1 - u\} = 1$ *for* $u, 1 - u \in A^*$.

[1] We hope that, from context, it is sufficiently clear when we use $\{a, b\}$ to denote the symbol in $K_2(A)$ and when we use it to denote the set containing elements a and b.

Example 2.13. If $A = \mathbb{Z}$, then $\mathbb{Z}^* = \{\pm 1\}$ has only two elements. Milnor proves in chapter 10 of [17] that $\{-1,-1\}$ has order 2 and is therefore the only non-trivial symbol[2] on $K_2(\mathbb{Z})$. It is also possible to show[3] that the element $x = (x_{12}(1)x_{21}(-1)x_{12}(1))^4$, from Example 2.10, must be $\{-1,-1\}$.

Let F be a field. The following result allows us to view $K_2(F)$ in terms of the symbols $\{u,v\}$.

Theorem 2.14 (Matsumoto's Theorem, [17, §12])**.** *The group $K_2(F)$ is the abelian group generated by the set of Steinberg symbols $\{u,v\}$, where $u,v \in F^*$, subject to the relations*

(1) $\{u_1u_2, v\} = \{u_1,v\}\{u_2,v\}$;

(2) $\{u, v_1v_2\} = \{u,v_1\}\{u,v_2\}$;

(3) $\{u, 1-u\} = 1$ *for any* $u \neq 1$.

Property *(3)* is commonly referred to as the *Steinberg identity.*

Since a field is a local ring, Lemma 2.12 and Example 2.5 give us:

Theorem 2.15. *There is an antisymmetric, bilinear map*

$$K_1(F) \times K_1(F) \longrightarrow K_2(F)$$

mapping $(a,b) \in K_1(F) \times K_1(F) \cong F^* \times F^*$ *to* $\{a,b\} \in K_2(F)$.

It turns out that $K_2(F)$ satisfies a certain universal property which we will take advantage of later on to derive some well known reciprocity laws. To describe this universal property, we require a definition. Our definition of the Steinberg symbol $\{-,-\}$ above should generalise in the following sense:

Definition 2.16. Let F be a field and G be an abelian group, written multiplicatively. A *(G-valued Steinberg) symbol on F* is a bilinear map

$$(-,-)\colon F^* \times F^* \longrightarrow G$$

such that $(x, 1-x) = 1$ whenever $x \in F^* \setminus \{1\}$.

Now, Matsumoto's theorem tells us that any symbol $(-,-)\colon F^* \times F^* \to G$ gives rise to a commutative diagram

$$\begin{array}{ccc} F^* \times F^* & \xrightarrow{\{-,-\}} & K_2(F) \\ & \searrow^{(-,-)} & \downarrow{\scriptstyle \exists!} \\ & & G \end{array}$$

[2]This is clear by the lemma above, since $\{1,-1\} = \{-1,1\} = \{1,1\} = 1$.

[3]This calculation is not too difficult, but it relies on introducing new notation and probably takes up more space than is necessary. For details, see, for example, Example 4.2.19 in [20].

Put differently, $K_2(F)$ is the universal object with respect to symbols on F with values in an abelian group G, and the corresponding symbol $\{-,-\}$ is the universal symbol on F.

We prove a result for symbols with values in an abelian group, similar to that of Lemma 2.12.

Lemma 2.17. *Let $(-,-)\colon F^*\times F^* \to G$ be a symbol on F. Then, for all $x, y \in F^*$, we have*

(1) $(x,-x) = 1$;

(2) $(x,y)^{-1} = (y,x)$;

(3) $(x,1) = (1,x) = 1$;

(4) $(x,x) = (x,-1)$.

Proof. (1) We start by writing $-x = (1-x)/(1-x^{-1})$ for $x \neq 1$. Then, using bilinearity,

$$\begin{aligned}(x,-x) &= (x,1-x)\cdot(x,(1-x^{-1})^{-1}) \\ &= (x,1-x^{-1})^{-1} \\ &= (x^{-1},1-x^{-1}) \\ &= 1,\end{aligned}$$

where in the second and final equalities we use the Steinberg identity.

To finish the proof of (1), we need to consider the case $x = 1$. But, in that case, bilinearity gives us $(1,-1) = (1,-1)\cdot(1,-1)$ and so $(1,-1) = 1$ after cancelling[4].

(2) Antisymmetry follows because

$$\begin{aligned}(x,y)\cdot(y,x) &= (x,-x)\cdot(x,y)\cdot(y,x)\cdot(y,-y) \\ &= (x,-xy)\cdot(y,-xy) \\ &= (xy,-xy) \\ &= 1.\end{aligned}$$

(3) This follows immediately from the bilinearity of a symbol. Indeed, $(x,1) = (x,1\cdot 1) = (x,1)(x,1)$. Antisymmetry then gives $(1,x) = 1$.

(4) Finally,

$$(x,x) = (x,-x)\cdot(x,-1) = (x,-1).$$

□

[4]In fact, this same argument shows that $(x,1) = 1$ for any $x \in F^*$

Theorem 2.18. *For a finite field F, $K_2(F)$ is the trivial group.*

Proof. Suppose $F = \mathbb{F}_q$ is a finite field with q elements. Let ζ denote a generator of the cyclic group $\mathbb{F}_q^*$. For any elements $x, y \in \mathbb{F}_q^*$, write $x = \zeta^m$, $y = \zeta^n$. Then $\{x, y\} = \{\zeta^m, \zeta^n\} = \{\zeta, \zeta\}^{mn}$, so it suffices to show that $\{\zeta, \zeta\} = 1$.

By antisymmetry, $\{\zeta, \zeta\} = \{\zeta, \zeta\}^{-1}$ and so $\{\zeta, \zeta\}$ has order at most 2. If q is a power of 2, then $\mathrm{char}(F) = 2$ which implies that $-1 = 1$ in $\mathbb{F}_q$ and so $\{\zeta, \zeta\} = \{\zeta, -\zeta\} = 1$. If, however, q is odd, then bilinearity, together with (1) from Lemma 2.17 gives us

$$\{\zeta, \zeta\} = \{\zeta, -\zeta\} \cdot \{\zeta, -1\} = \{\zeta, -1\} = \{\zeta, \zeta^{\frac{q-1}{2}}\} = \{\zeta, \zeta\}^{\frac{q-1}{2}}.$$

So if $(q-1)/2$ is even[5], we can see that $\{\zeta, \zeta\} = 1$. If $(q-1)/2$ is odd, then, in $\mathbb{F}_q$, -1 is not a perfect square[6]. Suppose we can choose $u \in \mathbb{F}_q$ such that neither u nor $1-u$ is a perfect square in $\mathbb{F}_q$. Recalling that $\{u, 1-u\} = 1$, and noting that u and $1-u$ are both odd powers of ζ, we see that $\{u, 1-u\}$ is an odd power of $\{\zeta, \zeta\}$. Thus $\{\zeta, \zeta\} = 1$.

It therefore remains to show that such a u exists. Since -1 is not a perfect square in $\mathbb{F}_q$, showing such a u exists is the same as showing that there exists a u, not a perfect square, such that $u - 1 = -1(1-u)$ is a perfect square. But this must be true, otherwise adding 1 to a perfect square would always give us a perfect square. Thus, every element of $\mathbb{F}_q^*$ would be a perfect square, clearly a contradiction. □

Before moving on to Milnor K-theory, we briefly discuss some symbols that will appear later on.

Example 2.19. Let $F = \mathbb{R}$ and $G = \{\pm 1\}$. Let

$$(x, y)_\infty = \begin{cases} -1 & \text{if and only if } x, y < 0; \\ 1 & \text{otherwise.} \end{cases}$$

Then, it is straightforward to verify that this is indeed a symbol.

Example 2.20. Let p be an odd prime and take $F = \mathbb{Q}_p$, $G = \mathbb{F}_p^*$. If we let $v_p : \mathbb{Q}_p^* \to \mathbb{Z}$ denote the p-adic valuation, then it is clear that the element

$$(-1)^{v_p(x)v_p(y)} x^{v_p(y)} y^{-v_p(x)}$$

belongs to $\mathbb{Z}_p^*$ for every $x, y \in \mathbb{Q}_p^*$. Fairly routine calculations show that its image in $\mathbb{F}_p^*$ is indeed a symbol, which is commonly referred to as the *tame symbol* associated to v_p. This will be generalised in the next section.

[5] If the order of $\{\zeta, \zeta\}$ was in fact 2 and not 1, then it would divide $\frac{q-1}{2}$ leading to a contradiction.

[6] To see this, argue by contradiction and show that $-1 = 1$.

2.5 Milnor K-theory

Motivated by Matsumoto's characterisation of $K_2(F)$, in this section we introduce the Milnor K-groups of a field F and state some basic properties. We mention the transfer, or norm map, associated to finite field extensions of F and the split exact sequence that will help us prove quadratic recirpocity and establish an equivalence between the transfer map, and Weil Reciprocity.

Let F be a field and for any $n \geq 0$, let $(F^*)^{\otimes n} \coloneqq F^* \underbrace{\otimes_{\mathbb{Z}} \dots \otimes_{\mathbb{Z}}}_{n\text{-times}} F^*$ be the n-fold tensor product of F^*. Here, we define $(F^*)^{\otimes 0} \coloneqq \mathbb{Z}$.

Definition 2.21. Let $n \geq 0$. The *n-th Milnor K-group* $K_n^M(F)$ of a field F is the group

$$K_n^M(F) \coloneqq (F^*)^{\otimes n}/(x_1 \otimes \dots \otimes x_n : x_i \in F^*, x_i + x_{i+1} = 1 \text{ for some } i).$$

We write $\{x_1, \dots, x_n\}$ for the image of $x_1 \otimes \dots \otimes x_n \in (F^*)^{\otimes n}$ in $K_n^M(F)$.

The *Milnor K-theory* $K_*^M(F)$ of F is the graded ring $K_*^M(F) \coloneqq \bigoplus_{n \geq 0} K_n^M(F)$, where $K_n^M(F)$ consists of the homogeneous elements of degree n.

Remark 2.22. By Example 2.5 and Matsumoto's Theorem (Theorem 2.14), we see that $K_n^M(F)$ and $K_n(F)$ agree for $n = 1, 2$. While we have not mentioned the functor K_0 here, it turns out[7] that $K_0(F) = \mathbb{Z}$, so the two groups also agree for $n = 0$. We also note here, out of interest, that Theorem 2.18 tells us that $K_n^M(F) = 0$ for any finite field F and any $n \geq 2$.

In what follows, as in chapter 1, if v is a discrete valuation on a field F, with valuation ring $\mathcal{O}_v$ and maximal ideal $\mathfrak{p}_v$, we let $k(v) = \mathcal{O}_v/\mathfrak{p}_v$ denote the *residue field* of F.

Definition 2.23. Suppose v is a discrete valuation on a field F. The *tame symbol* associated to v is the map

$$\begin{aligned} \overline{\tau_v} \colon F^* \times F^* &\longrightarrow k(v)^* \\ (x, y) &\longmapsto (-1)^{v(x)v(y)} x^{v(y)} y^{-v(x)} \pmod{\mathfrak{p}_v}. \end{aligned}$$

This gives an *(induced) tame symbol*[8]

$$\begin{aligned} \tau_v \colon K_2^M(F) &\longrightarrow k(v)^* \\ \{x, y\} &\longmapsto \overline{\tau_v}(x, y). \end{aligned}$$

We can use the tame symbol to describe $K_2^M(\mathbb{Q})$.

[7] See, for example, chapter 2, section 2 of [22].

[8] We will drop the use of *induced* when mentioning the more commonly used tame symbol τ_v rather than $\overline{\tau_v}$.

Example 2.24. Suppose p is a prime and $v = v_p$ is the p-adic valuation on $\mathbb{Q}$. We have that $k(v) \cong \mathbb{Z}/p\mathbb{Z}$. So, if x is a non-zero integer such that $|x| < p$, we can follow the map τ_v by this isomorphism to get a map

$$\begin{aligned} \tau_p \colon K_2^M(\mathbb{Q}) &\longrightarrow (\mathbb{Z}/p\mathbb{Z})^* \\ \{x, p\} &\longmapsto x \pmod{p}. \end{aligned}$$

We can then define a group homomorphism

$$\begin{aligned} \tau : K_2^M(\mathbb{Q}) &\longrightarrow \bigoplus_p (\mathbb{Z}/p\mathbb{Z})^* \\ \alpha &\longmapsto (\tau_2(\alpha), \tau_3(\alpha), \tau_5(\alpha), \ldots), \end{aligned}$$

and Tate [12, Theorem 14.56] was able to show that there exists a split exact sequence

$$1 \longrightarrow \{\pm 1\} \xrightarrow{i_\infty} K_2^M(\mathbb{Q}) \xrightarrow{\tau} \bigoplus_p (\mathbb{Z}/p\mathbb{Z})^* \longrightarrow 1. \tag{2.1}$$

Thus,

$$K_2^M(\mathbb{Q}) \cong \{\pm 1\} \oplus \bigoplus_p (\mathbb{Z}/p\mathbb{Z})^*.$$

Remark 2.25. We note here that the map $i_\infty \colon \{\pm 1\} \to K_2^M(\mathbb{Q})$, which sends -1 to $\{-1, -1\}$, has left inverse given by the real symbol $(-,-)_\infty$. We could just as easily have used something called the 2-adic symbol to get a similar left inverse. In fact, that is how Tate originally described $K_2^M(\mathbb{Q})$ and we will define and use this variation in the next section to prove quadratic reciprocity.

Motivated by the exact sequence in (2.1), Milnor [12, Definition 14.58] defines an extension of the tame symbol $\tau_v : K_2^M(F) \to k(v)^* \cong K_1^M(k(v))$ to a map

$$\partial_v \colon K_n^M(F) \longrightarrow K_{n-1}^M(k(v))$$

for each $n \geq 1$.

Theorem 2.26 ([16, Lemma 2.1])**.** *Let F be a field. For every $n \geq 1$ and any discrete valuation v on F, there exists a unique homomorphism*

$$\partial_v \colon K_n^M(F) \longrightarrow K_{n-1}^M(k(v)).$$

For all units $u_1, \ldots, u_{n-1} \in \mathcal{O}_v^*$,

$$\partial_v(\{u_1, \ldots, u_{n-1}, x\}) = v(x)\{\overline{u_1}, \ldots, \overline{u_n}\} \in K_{n-1}^M(k(v)),$$

where $\overline{u_i}$ is the class of u_i in $k(v)^*$.

Remark 2.27. We call the map ∂_v the extended tame symbol on v.

Remark 2.28. As a special case, we note that $\partial_v : K_1^M(F) \to K_0^M(k(v)) \cong \mathbb{Z}$ maps $\{x\}$ to $v(x)$. It is also not too difficult to see that $\partial_v : K_2^M(F) \to K_1^M(k(v))$ maps $\{x, y\}$ to $\{\tau_v(\{x, y\})\}$.

In a similar manner to proving the split exactness of the sequence in (2.1), Milnor was able to prove the following:

Theorem 2.29 ([16, Theorem 2.3])**.** *Let F be a field. The extended tame symbols ∂_v, for the p-adic valuations $v = v_p$ on $F(t)$, combine to give a map ∂ in a split exact sequence*

$$0 \longrightarrow K_n^M(F) \longrightarrow K_n^M(F(t)) \xrightarrow{\partial} \bigoplus_p K_{n-1}^M(k(v_p)) \longrightarrow 0,$$

where p ranges over all monic irreducibles in $F[t]$.

Example 2.30. Imitating the proof of Theorem 2.29, we can get a split exact sequence

$$0 \longrightarrow K_n^M(\mathbb{Z}) \longrightarrow K_n^M(\mathbb{Q}) \longrightarrow \bigoplus_p K_{n-1}^M(\mathbb{Z}/p\mathbb{Z}) \longrightarrow 0, \tag{2.2}$$

where p ranges over all primes in $\mathbb{Z}$.

Since $\mathbb{Z}/p\mathbb{Z}$ is a finite field, Theorem 2.18 implies that $K_{n-1}^M(\mathbb{Z}/p\mathbb{Z}) = 0$ for $n > 2$. So (2.2) gives us an isomorphism $K_n^M(\mathbb{Z}) \cong K_n^M(\mathbb{Q})$ for $n > 2$. One can then show that $K_n^M(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$, generated by the element $\{-1, \ldots, -1\}$, for $n > 2$.

We state one last result, due to Kato [9, Theorem 3], which characterises the norm maps associated to a field extension. Let $F(t)$ be the field of rational functions in one variable over a field F. Then

$$v_\infty(f) = -\deg(f)$$

is a discrete valuation on $F(t)$ that is trivial on F and for which x^{-1} is a generator of the maximal ideal $\mathfrak{p}_{v_\infty}$. Every other discrete valuation v on $F(t)$ that is trivial on F is determined by a monic irreducible polynomial $p_v \in F[t]$ that is a generator of the maximal ideal $\mathfrak{p}_v$, and the residue field, $k(v) \cong F[t]/(p_v)$.

Theorem 2.31 ([9, Theorem 3])**.** *There exists a unique family of homomorphisms*

$$N_{F'/F} \colon K_n^M(F') \longrightarrow K_n^M(F) \tag{2.3}$$

associated with finite field extensions F'/F such that both $N_{F/F} = id$ and $\sum_v N_{k(v)/F} \circ \partial_v = 0$, where the sum ranges over all discrete valuations v of $F(t)$ that are trivial on F.

Remark 2.32. The norm map above is sometimes also referred to as the *transfer map.*

Remark 2.33. In the case $n = 0$, we must define $N_{F'/F}$ as multiplication by the index $[F' : F]$. Recall that $F[t]$ is a unique factorisation domain with quotient field $F(t)$. Therefore, every element $f \in F(t)^*$ can be written as

$$f = \mathrm{lead}(f) \cdot \prod_{v \neq v_\infty} p_v^{v(f)},$$

where $\mathrm{lead}(f) \in F$ is the leading coefficient of f. Therefore,

$$\sum_{v \neq v_\infty} [k(v) : F] \cdot v(f) = \sum_{v \neq v_\infty} \deg(p_v) \cdot v(f) = \deg(f),$$

and since $v_\infty(f) = -\deg(f)$ we see that

$$\sum_v [k(v) : F] \cdot v(f) = 0.$$

In the case $n = 1$, we must take $N_{F'/F}(\{x\}) = \{\mathrm{Nm}_{F'/F}(x)\}$, where on the right-hand side, $\mathrm{Nm}_{F'/F}$ is the usual norm map. This makes the following diagram commute:

$$\begin{array}{ccc} K_1^M(F') & \xrightarrow{N_{F'/F}} & K_1^M(F) \\ \downarrow \cong & & \downarrow \cong \\ F'^* & \xrightarrow{\mathrm{Nm}_{F'/F}} & F^* \end{array}$$

The theorem below, which is also called Weil reciprocity, is a generalisation of Theorem 2.2 and it is, in fact, precisely the summation formula in Theorem 2.31, written multiplicatively. In proving Weil reciprocity, we establish Theorem 2.31 for the case $n = 1$.

We will use $(-,-)_v$ to denote the tame symbol on $F(t)^*$, rather than $\overline{\tau_v}$.

Theorem 2.34 (Weil Reciprocity generalisation, [3, Theorem 5.6])**.** *For any $f, g \in F(t)^*$, we have that*

$$\prod_v \mathrm{Nm}_{k(v)/F}(f,g)_v = 1, \tag{2.4}$$

where the product is taken over all discrete valuations on $F(t)$ that are trivial on F.

Proof. Since $(f,g)_v$ is a symbol, the left-hand side of (2.4) is easily seen to be bilinear in (f,g) and we also have $(f,f)_v = (f,-1)_v$. Thus, it suffices only to verify (2.4) for f and g relatively prime polynomials in $F[t]$. In this case, $(f,g)_v = 1$ whenever $v(f) = v(g) = 0$, and so the left-hand side of (2.4) can be split up as

$$\begin{aligned} \prod_v \mathrm{Nm}_{k(v)/F}(f,g)_v &= (f,g)_{v_\infty} \cdot \prod_{v(g)>0} \mathrm{Nm}_{k(v)/F}((f,g)_v) \cdot \prod_{v(f)>0} \mathrm{Nm}_{k(v)/F}((f,g)_v) \\ &= (f,g)_{v_\infty} \left(\frac{f}{g}\right)\left(\frac{g}{f}\right)^{-1}, \end{aligned} \tag{2.5}$$

where

$$\left(\frac{f}{g}\right) = \prod_{v(g)>0} \mathrm{Nm}_{k(v)/F}((f,g)_v) = \prod_{g(\alpha_v)=0} \mathrm{Nm}_{k(v)/F}(f(\alpha_v)^{v(g)}).$$

Here, the second inequality following immediately from the definition of the tame symbol.

Now, let $\overline{F}$ be an algebraic closure of F. In $\overline{F}[t]$, we can write

$$f(t) = a(t-\alpha_1)\dots(t-\alpha_n) \text{ and } g(t) = b(t-\beta_1)\dots(t-\beta_m).$$

We then show that

$$\left(\frac{f}{g}\right) = \prod_{j=1}^{m} f(\beta_j) = a^m \prod_{j=1}^{m}\prod_{i=1}^{n}(\beta_j - \alpha_i). \tag{2.6}$$

The second equality follows immediately. For the first equality, we consider two cases. In the first case, we assume g is constant, in which case both the left and right-hand side of (2.6) are equal to 1. In the second case, $g = p_v$ for some irreducible p associated to a valuation v. Here,

$$\left(\frac{f}{p_v}\right) = \mathrm{Nm}_{k(\alpha_v)/F}(f(\alpha_v)),$$

where α_v is the image of t in $k(v) = F[t]/(p_v)$. Note that the images of α_v under the different embeddings of $k(v)$ in $\overline{F}$ are precisely $\beta_1, \dots, \beta_m$. This gives us the required result upon nothing that, for general g, $\left(\frac{f}{g}\right)$ defined above is multiplicative in the denominator.

It then follows from (2.6) that

$$\left(\frac{f}{g}\right)\cdot\left(\frac{g}{f}\right)^{-1} = (-1)^{mn}\frac{a^m}{b^n}.$$

Since $v_\infty(f) = -n$ and $v_\infty(g) = -m$, we also have that

$$(f,g)_{v_\infty} = (-1)^{mn}\frac{a^{-m}}{b^{-n}},$$

which, together with (2.5), proves Weil Reciprocity.

□

2.6 Quadratic Hilbert symbols and quadratic reciprocity

In this section, we aim to prove quadratic reciprocity using the variation on the exact sequence (2.1), mentioned in Remark 2.25. In order to do this, we need to define the *quadratic Hilbert symbol* on a field F, which is done using norms. We introduce some preliminary results to motivate the definition. Recall the norm

$$\begin{aligned}\mathrm{Nm}_{\mathbb{C}/\mathbb{R}}\colon \mathbb{C} &\longrightarrow \mathbb{R}\\ a+bi &\longmapsto (a+bi)(a-bi) = a^2+b^2.\end{aligned}$$

We can express the real symbol

$$(x,y)_\infty = \begin{cases} -1 & \text{if and only if } x,y < 0; \\ 1 & \text{otherwise,} \end{cases}$$

in terms of this norm as follows:

Lemma 2.35. *For any $a, b \in \mathbb{R}^*$, $(a,b)_\infty = 1$ if, and only if, b is a norm from $\mathbb{R}(\sqrt{a})$.*

Proof. Suppose $a > 0$. Then $(a,b)_\infty = 1$, and $\mathbb{R}(\sqrt{a}) = \mathbb{R}$, so that $b = \mathrm{Nm}_{\mathbb{R}/\mathbb{R}}(b)$. If, however, $a < 0$, then $\mathbb{R}(\sqrt{a}) = \mathbb{C}$ and b is a norm from $\mathbb{C}$ if and only if $b > 0$, in which case $(a,b)_\infty = 1$. □

We can actually express this norm condition in terms of quadratic forms.

Lemma 2.36. *Suppose F is a field and $a, b \in F^*$. Then b is a norm from $F(\sqrt{a})$ if, and only if, $ax^2 + by^2 = z^2$ has a non-zero solution $(x,y,z) \in F^3$.*

Proof. We start by choosing a root $\sqrt{a}$ of $x^2 - a$ in an algebraic closure of F, and we let $E = F(\sqrt{a})$.

If $a = c^2$, for some $c \in F$, then $\sqrt{a} = \pm c$ and so $E = F$. In this case, we obviously have $b = \mathrm{Nm}_{E/F}(b)$ and also $a \cdot (c^{-1})^2 + b \cdot 0^2 = 1^2$.

On the other hand, suppose that a is not a square in F. If b is a norm from $F(\sqrt{a})$, then we can write $b = \mathrm{Nm}_{E/F}(c + d\sqrt{a}) = c^2 - ad^2$, for some $c, d \in F$. Then, $a \cdot d^2 + b \cdot 1^2 = c^2$ giving us a non-zero solution $(d, 1, c)$. For the converse, assume that there exists a non-zero solution $(x,y,z) \in F^3$ to $ax^2 + by^2 = z^2$. Since a is not a square, we must have $y \neq 0$. Therefore, after rearranging, $b = (z/y)^2 - a(x/y)^2 = \mathrm{Nm}_{E/F}((z/y) + (x/y)\sqrt{a})$.

□

Hilbert generalised the real symbol to other fields F by defining a map $(-,-)_F \colon F^* \times F^* \longrightarrow \mathbb{Z}^*$ which sends a pair (a,b) to[9]

$$(a,b)_F = \begin{cases} 1 & \text{if } \ b \in \mathrm{Nm}_{F(\sqrt{a})/F}(F(\sqrt{a})^*); \\ -1 & \text{otherwise.} \end{cases}$$

If we take $x = y = z = 1$ in Lemma 2.36, then $(a,b)_F = 1$ whenever $a + b = 1$. Also, $(a,b)_F = (b,a)_F$, so $(a,b)_F$ is multiplicative in a if and only if it is multiplicative in b. Now, suppose that $N = \mathrm{Nm}_{F(\sqrt{a})/F}(F(\sqrt{a})^*)$ has index 1 or 2 in F^*. Then, $b_1 b_2 \in N$ if, and only if, b_1 and b_2 are both in N or both not in N. Therefore, for all $a, b_1, b_2 \in F^*$ we have that

$$(a, b_1 b_2)_F = (a, b_1)_F \cdot (a, b_2)_F.$$

If, however, we suppose that N has index greater than 2, we can find cosets $b_1 N \neq N$, $b_2 N \neq N$ so that $(a, b_1 b_2)_F = (a, b_1)_F = (a, b_2)_F = -1$. This gives us the following result:

[9] By Lemma 2.36, we could also send the pair (a,b) to 1 or -1 subject to there being a non-zero solution $(x,y,z) \in F^3$ to the equation $ax^2 + by^2 = z^2$. This is a common equivalent way of defining the quadratic Hilbert symbol.

Proposition 2.37. *Suppose F is a field. The following are equivalent:*

1. *For $a \in F$ and $E = F(\sqrt{a})$, the subgroup $N = \mathrm{Nm}_{E/F}(E^*)$ has index 1 or 2 in F^*.*

2. *The map $(-,-)_F \colon F^* \times F^* \longrightarrow \{\pm 1\}$ is bilinear.*

3. *The map $(-,-)_F \colon F^* \times F^* \longrightarrow \{\pm 1\}$ is a symbol, which induces a homomorphism $K_2(F) \to \{\pm 1\}$, sending $\{a,b\}$ to $(a,b)_F$.*

Remark 2.38. If $(-,-)_F$ is a symbol map, then we call it a *quadratic Hilbert symbol* on F. It is worth noting here that the real symbol $(-,-)_\infty$ is a quadratic Hilbert symbol relies on the fact that $\mathrm{Nm}_{\mathbb{C}/\mathbb{R}}(\mathbb{C}^*)$ has index 2 in $\mathbb{R}^*$.

Remark 2.39. There is also a quadratic Hilbert symbol on each algebraically closed field F, since then $F(\sqrt{a}) = F$ and $\mathrm{Nm}_{F/F}(F^*)$ has index 1 in F^*. But in this case, $(a,b)_F = 1$ for all a, b and the induced homomorphism is trivial, so this doesn't tell us much.

Example 2.40. There is no quadratic Hilbert symbol on $\mathbb{Q}$. By Proposition 2.37, we need only show that the index of $\mathrm{Nm}_{\mathbb{Q}(i)/\mathbb{Q}}(\mathbb{Q}(i)^*)$ is not 1 or 2, but our proof will actually show that the index is infinite. To see why[10], recall that the primes $p \in \mathbb{Z}$ which remain prime in $\mathbb{Z}[i]$ are precisely those which are congruent to 3 (mod 4). For any such prime p and any $a + bi \in \mathbb{Z}[i]$, we have that[11] $v_p(a+bi) = v_p(a-bi)$. This implies that $v_p(a^2+b^2) = v_p(\mathrm{Nm}_{\mathbb{Q}(i)/\mathbb{Q}}(a+bi))$ must be even. If q is any integer not divisible by p, then there do not exist $a, b, c \in \mathbb{Z}$ such that

$$\frac{p}{q} = \mathrm{Nm}_{\mathbb{Q}(i)/\mathbb{Q}}\left(\frac{a}{c} + \frac{b}{c}i\right) = \frac{a^2+b^2}{c^2},$$

since $v_p(pc^2)$ is odd and $v_p(q(a^2+b^2))$ is even. Thus, no two primes $p, q \equiv \pmod 3$ are congruent modulo norms from $\mathbb{Q}(i)^*$. Since there are infinitely many primes which are congruent to 3 (mod 4), this shows that $\mathrm{Nm}_{\mathbb{Q}(i)/\mathbb{Q}}(\mathbb{Q}(i)^*)$ has infinite index in $\mathbb{Q}^*$.

In order to reformulate quadratic reciprocity, we need quadratic Hilbert symbols on $\mathbb{Q}_p$ for primes p. When p is an odd prime, this is done by following the tame symbol map $\mathbb{Q}_p^* \times \mathbb{Q}_p^* \to (\mathbb{Z}/p\mathbb{Z})^*$ by the map $a \mapsto a^{(p-1)/2}$. When $p = 2$, the problem of $(\mathbb{Z}/2\mathbb{Z})^*$ being the trivial group arises, and so a quadratic Hilbert symbol must be constructed directly. We are interested in how Tate's description of $K_2(\mathbb{Q})$ leads to quadratic reciprocity and as a result, omit the proofs for the constructions of these symbols. For a full proof, see, for example, [12, §15].

Proposition 2.41.

[10] See, for example [13, Example 3.44]

[11] A simple argument proceeds as follows: If $v_p(a+bi) = k$, then $a + bi = p^k \cdot \alpha$ for some $\alpha \in \mathbb{Z}[i]$. Taking conjugates yields $a - bi = p^k \cdot \overline{\alpha}$ and so $v_p(a-bi) = k$. The other direction is identical.

1. *Let p be an odd prime and $a, b \in \mathbb{Q}_p^*$. Then, there is a quadratic Hilbert symbol $(-,-)_p$ on $\mathbb{Q}_p$, given by*

$$(a,b)_p = \overline{\tau_p}(a,b)^{(p-1)/2}, \tag{2.7}$$

where $\overline{\tau_p} : \mathbb{Q}_p^* \times \mathbb{Q}_p^* \to k(v)^* \cong (\mathbb{Z}/p\mathbb{Z})^*$ is the tame symbol defined in Definition 2.23.

2. *Let $a, b \in \mathbb{Q}_2^*$. Then a, b can be written in the form $a = 2^i \cdot (-1)^j \cdot 5^k \cdot s$ and $b = 2^I \cdot (-1)^J \cdot 5^K \cdot t$, where $s, t \in 1 + 8\mathbb{Z}_2$. Furthermore, there is a quadratic Hilbert symbol $(-,-)_2$ on $\mathbb{Q}_2$, given by*

$$(a,b)_2 = (-1)^{iK+jJ+kI}. \tag{2.8}$$

While there is no quadratic Hilbert symbol on $\mathbb{Q}$, for each prime p, we can restrict the p-adic symbol $(-,-)_p$ to a map

$$(-,-)_p \colon \mathbb{Q}^* \times \mathbb{Q}^* \longrightarrow \mathbb{Z}^*$$

which is bilinear and satisfies $(a,b)_p = 1$ for all $a, b \in \mathbb{Q}^*$ such that $a + b = 1$. Hence, for each prime p, we get an induced map

$$K_2(\mathbb{Q}) \to \mathbb{Z}^*, \{a,b\} \mapsto (a,b)_p.$$

For the rest of this section let $\mathcal{P}$ denote the set of *odd* primes.

Remark 2.42. In Remark 2.25, we mentioned that Tate originally described $K_2^M(\mathbb{Q})$ slightly differently. While he kept the tame symbols at odd primes, he used the 2-adic symbol $(-,-)_2$ instead of $(-,-)_\infty$ to get a split exact sequence

$$1 \longrightarrow \{\pm 1\} \xrightarrow{i_2} K_2^M(\mathbb{Q}) \xrightarrow{\tau} \bigoplus_{p \in \mathcal{P}} (\mathbb{Z}/p\mathbb{Z})^* \longrightarrow 1. \tag{2.9}$$

Here, the map i_2 is the same map as i_∞. Noting that $(-1,-1)_2 = -1$, we see that the 2-adic symbol $(-,-)_2$, also induces a left inverse (which we denote by h_2 below), hence the minor change of notation.

As before, this gives us an isomorphism

$$\begin{aligned} K_2(\mathbb{Q}) &\cong \{\pm 1\} \oplus \bigoplus_{p \in \mathcal{P}} \left(\mathbb{Z}/p\mathbb{Z}\right)^* \\ \{a,b\} &\mapsto ((a,b)_2, \tau_3(a,b), \tau_5(a,b), \ldots) \end{aligned}$$

this time involving the 2-adic symbol instead. The question guiding us towards quadratic reciprocity is, how does the real symbol fit into this description?

If we compose the above isomorphism with projection and inclusion maps, we see that there are homomorphisms

$$K_2(\mathbb{Q}) \underset{i_2}{\overset{h_2}{\rightleftarrows}} \{\pm 1\} \quad \text{and} \quad K_2(\mathbb{Q}) \underset{i_p}{\overset{\tau_p}{\rightleftarrows}} (\mathbb{Z}/p\mathbb{Z})^*$$

Written multiplicatively, the map $i_2 \circ h_2 \cdot \prod(i_p \circ \tau_p)$ acts as the identity on $K_2(\mathbb{Q})$. If $r\colon K_2(\mathbb{Q}) \to \{\pm 1\}$ is induced by the real symbol, then we see that

$$\begin{aligned} r &= r \circ \left(i_2 \circ h_2 \cdot \prod (i_p \circ \tau_p) \right) \\ &= (r \circ i_2) \circ h_2 \cdot \prod (r \circ i_p) \circ \tau_p. \end{aligned}$$

It is straightforward to see that $r \circ i_2\colon \{\pm 1\} \to \{\pm 1\}$ is the identity map. In addition, each homomorphism $r \circ i_p\colon (\mathbb{Z}/p\mathbb{Z})^* \to \{\pm 1\}$ is completely determined by where it maps a generator of $(\mathbb{Z}/p\mathbb{Z})^*$. It is therefore[12] given by the map that sends an element x to $x^{n(p)}$, where $n(p) = (p-1)/2$ or $p-1$. Therefore, for $a, b \in \mathbb{Q}^*$, we have

$$(a,b)_\infty = (a,b)_2 \prod_{p \in \mathcal{P}} (a,b)_p^{m(p)}, \tag{2.10}$$

where $m(p)$ is either 1 or 2.

In proving quadratic reciprocity follows from the formula above, we require a result due to Gauss.

Lemma 2.43 ([12, Lemma 15.33])**.** *If p is a prime such that $p \equiv 1 \pmod 8$, then there is a prime $q < \sqrt{p}$ such that p is not a square modulo q.*

Theorem 2.44 (Quadratic reciprocity)**.** *For all $a, b \in \mathbb{Q}^*$,*

$$(a,b)_\infty = (a,b)_2 \prod_{p \in \mathcal{P}} (a,b)_p. \tag{2.11}$$

Therefore, for all odd primes $p \neq q$,

$$1 = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot \left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right).$$

Proof. Let p and q be two distinct odd primes. Before we begin, we note three things that will help to prove both statements of the theorem. Namely, that $(p,q)_\infty = 1$ and for any prime $r \neq p, q$, we have that $(p,q)_r = 1$. Also, working modulo 8, we can write $p \equiv (-1)^j 5^k \pmod 8$ and $q \equiv (-1)^J 5^K \pmod 8$.

To prove (2.11) we must show that $m(p) = 1$ for all primes $p \in \mathcal{P}$ in (2.10). To do this, we consider a few different cases.

1. Suppose first that $p \in \mathcal{P}$ and $p \equiv -1, -5 \pmod 8$. Then Proposition 2.41, combined with the note made at the beginning of the proof, says that $(p,p)_2 = -1$. Letting $a = b = p$ in (2.10) gives

   $$1 = (-1) \cdot (p,p)_p^{m(p)}$$

   and so $m(p) = 1$.

[12] While this is a well-known result, a proof will be given in Lemma 3.19.

2. Next, suppose that $p \in \mathcal{P}$ and $p \equiv 5 \pmod 8$. Then, using the same reasoning as above, we can see that $(2,p)_2 = -1$. Taking $a = 2, b = p$ in (2.10) gives
$$1 = (-1) \cdot (2,p)_p^{m(p)}$$
and so we conclude, again, that $m(p) = 1$.

3. The final case, $p \equiv 1 \pmod 8$, is slightly more involved. The problem here is that $(p,a)_2 = 1$ for all $a \in \mathbb{Q}^*$. Therefore, suppose, for contradiction, that the theorem is not true. Let p be the smallest prime such that $m(p) = 2$. For each odd prime $q < p$, we have that $m(q) = 1$. Substituting $a = p, b = q$ in (2.10) gives
$$\begin{aligned} 1 &= (p,q)_q \cdot (p,q)_p^2 \\ &= (p,q)_q \\ &= p^{(q-1)/2} \pmod q \\ &= \left(\frac{p}{q}\right), \end{aligned}$$
where in the final line we have used Euler's criterion. This tells us that p is a square modulo all primes $q < p$, which contradicts Lemma 2.43.

Having verified that $m(p) = 1$ for all primes p, we have established (2.11).

For the second statement, we substitute odd primes p, q into (2.11). Using the statement made at the beginning of the proof, it is straightforward to verify that
$$\begin{aligned} (p,q)_2 &= \begin{cases} 1 & \text{if } p \text{ or } q \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv q \equiv 3 \pmod 4. \end{cases} \\ &= (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}. \end{aligned}$$

Therefore, the only contributions to the right-hand side of (2.11) come from the two primes p and q and the 2-adic symbol $(p,q)_2$. Using the tame symbol definition, we have that
$$(p,q)_p = \left((-1)^{0 \cdot 1} \cdot p^0 \cdot q^1\right)^{\frac{p-1}{2}} \equiv q^{\frac{p-1}{2}} \pmod p$$

Recalling that $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$, for any prime p and $a \in \mathbb{Z}$, we have that
$$\begin{aligned} 1 &= (p,q)_2 \cdot (p,q)_p \cdot (p,q)_q \\ &= (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot \left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right), \end{aligned}$$
as required.

□

Chapter 3

Further Symbols and Their Relationship to $K_2(\mathbb{Q}(\sqrt{-2}))$

In the previous chapter we saw how Tate's computation of $K_2(\mathbb{Q})$ led to a rather neat derivation of quadratic reciprocity. To see this, we had to introduce quadratic Hilbert symbols and, for $a, b \in \mathbb{Q}^*$, derive the product formula

$$(a,b)_\infty = (a,b)_2 \prod_{p \in \mathcal{P}} (a,b)_p.$$

Our aim in this chapter is to generalise quadratic Hilbert symbols and mimic Tate's construction of $K_2(\mathbb{Q})$) to get a similar reciprocity result for $K_2(\mathbb{Q}(\sqrt{-2})$. It is worth noting that in proving the split exactness of the sequence

$$1 \longrightarrow \{\pm 1\} \longrightarrow K_2(\mathbb{Q}) \longrightarrow \bigoplus_p (\mathbb{Z}/p\mathbb{Z})^* \longrightarrow 1$$

Tate used the Euclidean algorithm. Thus, to have any hope of replicating this construction, the ring of integers of our quadratic number field must be a Euclidean domain. It is well-known[1] that $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$ is a Euclidean domain for $d \in \{1, 2, 3, 7, 11\}$. The cases $d = 1, 3$ have been discussed in [10], and so it seems only natural to consider the case when $d = 2$.

We take the opportunity in this chapter to generalise the quadratic Hilbert symbol to Hilbert symbols of order m and make a connection between them and the so-called n-th power residue symbols. We will prove a product formula and state a powerful result due to Moore that says such a relation between Hilbert symbols is unique. This combines to give a reciprocity law for $K_2(\mathbb{Q}(\sqrt{-2}))$.

3.1 Generalising the quadratic Hilbert symbol

Throughout this section, we let F be a field and v be a prime. Recall that we defined the quadratic Hilbert symbol to be the symbol $(-,-)_F \colon F^* \times F^* \longrightarrow \mathbb{Z}^*$ that sends a pair (a, b) to

$$(a,b)_F = \begin{cases} 1 & \text{if } \ b \in \mathrm{Nm}_{F(\sqrt{a})/F}(F(\sqrt{a})^*); \\ -1 & \text{otherwise.} \end{cases}$$

[1] See, for example, page 432 in [3].

Also recall from Definition 1.44 the Hasse symbol on F^* for some field extension L of a global field F is defined as

$$\begin{aligned}\left(\frac{-, L/F}{v}\right)\colon F^* &\longrightarrow \mathrm{Gal}(L/F)\\ x &\longmapsto [\Phi_{F_v}(x)],\end{aligned}$$

where $[\Phi_{F_v}(x)]$ denotes the image of $\Phi_{F_v}(x)$ in $\mathrm{Gal}(L/F)$.

Definition 3.1. For $x, y \in F^*$, the *Hilbert symbol of order* $m = \#\mu(F)$ at v is defined as

$$\left(\frac{x, y}{v}\right) := \frac{\sigma_v(\sqrt[m]{x})}{\sqrt[m]{x}} \in \mu(F),$$

where, to simplify notation, we let

$$\sigma_v = \left(\frac{y, F(\sqrt[m]{x})/F}{v}\right)$$

denote the Hasse symbol on F^* at v.

For any divisor n of m, we also define the *Hilbert symbol of order* n as

$$\left(\frac{-, -}{v}\right)_n := \left(\frac{-, -}{v}\right)^{\frac{m}{n}}.$$

Remark 3.2. If we replace F by F_v, m by m_v and instead let $\sigma_v = \phi_{F_v(\sqrt[m_v]{x})/F_v}$ denote the local Artin map in the definition above we get the *local Hilbert symbol* at v of order m_v.

We make note of this here as it will come in use later when defining the map used in Moore's Theorem.

Remark 3.3. Taking $m = n = 2$, we see that the Hilbert symbol of order 2 is given by

$$\left(\frac{x, y}{v}\right) = \frac{\sigma_v(\sqrt{x})}{\sqrt{x}} \in \{\pm 1\}.$$

This takes value $+1$ if and only if $\sigma_v(\sqrt{x}) = \sqrt{x}$, which is equivalent to saying that y lies in the kernel of the local Artin map. By Theorem 1.34, this happens if and only if $y \in \mathrm{Nm}_{F(\sqrt{x})/F}(F(\sqrt{x})^*)$, which is precisely the definition of the quadratic symbol given above.

More specifically, let p be a prime number and v be the associated valuation. For $F = \mathbb{Q}_p$, Proposition 2.41 then tells us that

$$\left(\frac{x, y}{v}\right) = (x, y)_p.$$

Now, in order to prove the product formula for Hilbert symbols, we need the following result:

Lemma 3.4. *Let L be a finite abelian extension of F containing an n-th root z of an element $x \in F^*$. Let $\{\sigma_i\}_{i=1}^M$ be a finite set of automorphisms in the Galois group* $\mathrm{Gal}(L/F)$*. Then*

$$\frac{\left(\prod_{i=1}^M \sigma_i\right)(z)}{z} = \prod_{i=1}^M \frac{\sigma_i(z)}{z} \in \mu(F).$$

Proof. We prove this statement by induction. Let $\sigma, \tau \in \mathrm{Gal}(L/F)$. Then

$$\begin{aligned}\frac{(\sigma\tau)(z)}{z} &= \frac{(\sigma(\tau(z))}{z} \cdot \frac{\tau(z)}{z} \\ &= \frac{\tau(\sigma(z))}{\tau(z)} \cdot \frac{\tau(z)}{z} \\ &= \tau\left(\frac{\sigma(z)}{z}\right) \cdot \frac{\tau(z)}{z} \\ &= \frac{\sigma(z)}{z} \cdot \frac{\tau(z)}{z}.\end{aligned}$$

Here, the second equality follows from the fact that the extension is abelian and then final equality follows from the fact that τ acts trivially on $\mu(F) \subset F$. The lemma then follows by induction.

□

Theorem 3.5. *For any $x, y \in F^*$ and any n dividing $m = \#\mu(F)$, we have the following product formula:*

$$\prod_v \left(\frac{x, y}{v}\right)_n = 1.$$

Proof. The product formula follows immediately using Lemma 3.4 and Theorem 1.45. □

Definition 3.6. Let $n > 1$ be a natural number, $x \in F^*$ and v a finite prime that is not ramified in $F(\sqrt[n]{x})/F$. We define the *n-th power residue symbol* as

$$\left(\frac{x}{v}\right)_n := \frac{\left(\frac{F(\sqrt[n]{x})/F}{v}\right)(\sqrt[n]{x})}{\sqrt[n]{x}},$$

where we use $\left(\frac{F(\sqrt[n]{x})/F}{v}\right)$ to denote the Frobenius element in $\mathrm{Gal}(F(\sqrt[n]{x})/F)$.

If $\mathfrak{p}$ is the prime ideal corresponding to v, we also write

$$\left(\frac{x}{\mathfrak{p}}\right)_n := \left(\frac{x}{v}\right)_n.$$

Finally, for $y \in F^*$ such that all $v|y$ are unramified in $F(\sqrt[n]{x})/F$, we define

$$\left(\frac{x}{y}\right)_n := \prod_v \left(\frac{x}{v}\right)_n^{\mathrm{ord}_v(y)},$$

where the product runs over all primes v dividing y and all real infinite places.

Remark 3.7. In a similar style to the notation above, we will write $\sigma = \left(\frac{F(\sqrt[n]{x})/F}{v}\right)$ for the Frobenius element at the prime v, and we let $\mathfrak{p}$ be the prime corresponding to v. Recalling that the Frobenius acts as raising elements to the power $q_v = \mathrm{Nm}(\mathfrak{p})$ modulo $\mathfrak{p}$, we see that

$$\left(\frac{x}{\mathfrak{p}}\right)_n = \frac{\sigma(\sqrt[n]{x})}{\sqrt[n]{x}} \equiv x^{\frac{q_v-1}{n}} \pmod{\mathfrak{p}}.$$

Thus, we see that the n-th power reciprocity symbol is a generalisation of the Legendre symbol.

The following proposition is used to prove an n-th power reciprocity law.

Proposition 3.8 ([7, Proposition 7.4.3])**.** *The n-th power residue symbols satisfy the following properties:*

1. $\left(\frac{x}{v}\right)_n = 1$ *if and only if* $i_v(x)$ *is an n-th power in* F_v^**;*
2. $\left(\frac{x}{v}\right)_n \left(\frac{y}{v}\right)_n = \left(\frac{xy}{v}\right)_n$ *;*
3. $\left(\frac{x,y}{v}\right)_n = \left(\frac{x}{v}\right)_n^{ord_v(y)}$.

Remark 3.9. We note that, in particular, the last result of the proposition above implies that

$$\left(\frac{x, \pi_v}{v}\right)_n = \left(\frac{x}{v}\right)_n.$$

Theorem 3.10 (The n-th power reciprocity law [7, Theorem 7.4.4])**.** *Let n be a divisor of $m = \#\mu(F)$. Let $x, y \in F^*$ such that for any prime v we have $\mathrm{ord}_v(x) = 0$ or $\mathrm{ord}_v(y) = 0$, and for any prime v dividing n we have $\mathrm{ord}_v(x) = \mathrm{ord}_v(y) = 0$. Then*

$$\left(\frac{x}{y}\right)_n \left(\frac{y}{x}\right)_n^{-1} = \prod_{v|n} \left(\frac{y, x}{v}\right)_n.$$

Proof. By definition

$$\left(\frac{x}{y}\right)_n \left(\frac{y}{x}\right)_n^{-1} = \prod_{v \nmid n} \left(\frac{x}{v}\right)_n^{\mathrm{ord}_v(y)} \prod_{v \nmid n} \left(\frac{y}{v}\right)_n^{-\mathrm{ord}_v(x)},$$

since $\mathrm{ord}_n(x) = \mathrm{ord}_n(y) = 0$ for all $v|n$. Hence, using Proposition 3.8 we see that

$$\begin{aligned}\left(\frac{x}{y}\right)_n \left(\frac{y}{x}\right)_n^{-1} &= \prod_{v \nmid n} \left(\frac{x, y}{v}\right)_n \prod_{v \nmid n} \left(\frac{y, x}{v}\right)_n^{-1} \\ &= \prod_{v \nmid n} \left(\frac{x, y}{n}\right)_n.\end{aligned}$$

In the last equality, we use the antisymmetry property of a symbol. Now, Hilbert's product formula in Theorem 3.5 says that

$$\prod_{v\nmid n}\left(\frac{x,y}{n}\right)_n = \prod_{v|n}\left(\frac{x,y}{n}\right)_n^{-1} = \prod_{v|n}\left(\frac{y,x}{n}\right)_n,$$

where we once again have used the antisymmetry property in the final equality. Putting this all together, we arrive at the required result. □

Remark 3.11. The case $n = m = 2$ and $F = \mathbb{Q}$ corresponds to quadratic reciprocity and the reader can compare the equivalence between this formulation and the one made in Theorem 2.44.

3.2 Calculating $K_2(\mathbb{Q}(\sqrt{-2}))$

Throughout this section, we consider $F = \mathbb{Q}(\sqrt{-2})$. Recall from Proposition 1.1 that the ring of integers $\mathcal{O}_F = \mathbb{Z}[\sqrt{-2}]$ and the discriminant, Δ_F, of $F/\mathbb{Q}$ is -8. Thus, Theorem 1.22 tells us that the only prime that ramifies in $\mathcal{O}_F$ is 2. To find the primes that split, Proposition 1.25 tells us that we can look for those that satisfy $\left(\frac{-2}{p}\right) = 1$. Using the multiplicativity of the Legendre symbol, this is equivalent to finding the primes that satisfy $\left(\frac{2}{p}\right)\left(\frac{-1}{p}\right) = 1$.

The supplementary laws of quadratic reciprocity from Theorem 2.44 tell us that

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4; \\ -1 & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

and that

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod 8; \\ -1 & \text{if } p \equiv 3, 5 \pmod 8. \end{cases}$$

Thus, a prime splits precisely when $p \equiv 1, 3 \pmod 8$, leaving $p \equiv 5, 7 \pmod 8$ as the inert primes.

Our aim in this section is to establish, for non-complex primes v, the isomorphism[2]

$$K_2(\mathbb{Q}(\sqrt{-2})) \cong \bigoplus_v k(v)^* \cong \bigoplus_{\substack{p \text{ prime} \\ p\equiv 1,3 (\text{mod } 8)}} (\mathbb{F}_p^*)^2 \oplus \bigoplus_{\substack{p \text{ prime} \\ p\equiv 5,7 (\text{mod } 8)}} \mathbb{F}_{p^2}^*.$$

Here the terms in the direct sum come from the residue fields (see Proposition 1.26) at each prime p, according to its residue class modulo 8. It is worth highlighting that the residue field for the prime 2 does not appear explicitly since it is trivial.

[2]Notice the similarity between the isomorphism given here and that used in Tate's computation of $K_2(\mathbb{Q})$ in Example 2.24.

In constructing $K_2(\mathbb{Q})$, Tate used a filtration

$$M_2 \subset M_3 \subset M_5 \subset \ldots \subset M_p \subset \ldots \subset K_2(\mathbb{Q}),$$

where, for each prime p,

$$M_p \coloneqq \langle \{x, y\} : x, y \in \mathbb{Z} \setminus \{0\}, 1 \leq |x|, |y| \leq p \rangle.$$

We aim to do something similar, with some minor changes, that require a few preliminary results. In the lemma below, $|a|$ is the standard absolute value that satisfies $|a|^2 = \mathrm{Nm}(a)$.

Lemma 3.12. *For any finite prime v of $\mathbb{Q}(\sqrt{-2})$, there is a complete system of representatives $\{\alpha_j\}_{j=1,\ldots,\mathrm{Nm}(\pi_v)}$ for $k(v)$ such that $|\alpha_j| \leq \frac{\sqrt{3}}{2}|\pi_v|$ for each j.*

Proof. Let π be a prime element and $\alpha \in \mathbb{Z}[\sqrt{-2}] \setminus \{0\}$. Geometrically, what one should picture is the lattice spanned by integer multiples of π. Then α lies in one of the rectangles of the lattice with distance at most $\frac{\sqrt{3}}{2}|\pi|$ away from a corner $\gamma\pi$. If we let $\beta = \alpha - \gamma\pi$ then $\beta \equiv \alpha \pmod{\pi}$ and $|\beta| \leq \frac{\sqrt{3}}{2}|\pi|$. □

Lemma 3.13. *The group $K_2(\mathbb{Q}(\sqrt{-2}))$ is generated by elements $\{a, b\}$ where $a, b \in \mathbb{Z}[\sqrt{-2}] \setminus \{0\}$.*

Proof. Let $\{x, y\} \in K_2(\mathbb{Q}(\sqrt{-2}))$. We can write $x = a/b$ and $y = a'/b'$ where $a, a', b, b' \in \mathbb{Z}[\sqrt{-2}] \setminus \{0\}$. Using bilinearity and the properties in Lemma 2.17, we see that

$$\begin{aligned} \{x, y\} &= \{ab^{-1}, a'b'^{-1}\} \\ &= \{a, a'\}\{a, b'^{-1}\}\{b^{-1}, a'\}\{b^{-1}, b'^{-1}\} \\ &= \{a, a'\}\{b', a\}\{a', b\}\{b, b'\}. \end{aligned}$$

□

Lemma 3.14. *In $K_2(\mathbb{Q}(\sqrt{-2}))$, the symbols $\{-1, -1\}$ and $\{\sqrt{-2}, \sqrt{-2}\}$ are both trivial.*

Proof. We begin by recalling here, for ease of use, the necessary properties of symbols[3]:

(a) For all $x \neq 1$, the Steinberg relation says that $\{x, 1 - x\} = 1$;

(b) $\{x, y\}^{-1} = \{y, x\}$;

(c) $\{x, x\} = \{x, -1\}$;

(d) $\{x, 1\} = \{1, x\} = 1$.

(e) $\{x, x\}^2 = \{x, -1\}^2 = \{x, 1\} = 1$.

[3]These come from Definition 2.16 and Lemma 2.17.

We shall prove the triviality of both symbols in four steps.

1. Since $(-1)+(-1)(\sqrt{-2})^2 = 1$, the Steinberg relation implies that

$$\begin{aligned} 1 &= \{-1, (-1)(\sqrt{-2})^2\} \\ &= \{-1,-1\}\{-1,\sqrt{-2}\}^2 \\ &= \{-1,-1\}, \end{aligned}$$

   where the second equality uses bilinearity, and the final equality uses (e).

2. Since $(-1)(\sqrt{-2})+(1+\sqrt{-2}) = 1$, the Steinberg relation also implies that

$$\begin{aligned} 1 &= \{(-1)(\sqrt{-2}), 1+\sqrt{-2}\} \\ &= \{-1, 1+\sqrt{-2}\}\{\sqrt{-2}, 1+\sqrt{-2}\} \\ &= \{1+\sqrt{-2}, 1+\sqrt{-2}\}\{\sqrt{-2}, 1+\sqrt{-2}\}, \end{aligned}$$

   where the second equality follows from bilinearity and the final equality follows from (c).

   This implies that $\{1+\sqrt{-2}, 1+\sqrt{-2}\}^{-1} = \{\sqrt{-2}, 1+\sqrt{-2}\}$, which, by (b) gives

$$\{1+\sqrt{-2}, 1+\sqrt{-2}\} = \{\sqrt{-2}, 1+\sqrt{-2}\}.$$

3. Once again, since $\frac{(-1)(1+\sqrt{-2})}{(\sqrt{-2})^2} + \frac{(-1)(1-\sqrt{-2})}{(\sqrt{-2})^2} = 1$, the Steinberg relation implies that

$$\begin{aligned} 1 =& \left\{ \frac{(-1)(1+\sqrt{-2})}{(\sqrt{-2})^2}, \frac{(-1)(1-\sqrt{-2})}{(\sqrt{-2})^2} \right\} \\ &= \{-1,-1\}\{-1,1-\sqrt{-2}\}\{-1,\sqrt{-2}\}^{-2}\{1+\sqrt{-2},-1\}\{1+\sqrt{-2},1-\sqrt{-2}\} \\ &\quad \{1+\sqrt{-2},\sqrt{-2}\}^{-2}\{\sqrt{-2},-1\}^{-2}\{\sqrt{-2},1-\sqrt{-2}\}^{-2}\{\sqrt{-2},\sqrt{-2}\}^4 \\ &= \{-1,1-\sqrt{-2}\}\{1+\sqrt{-2},-1\}\{1+\sqrt{-2},1-\sqrt{-2}\}\{\sqrt{-2},1+\sqrt{-2}\}^2 \\ &= \{1-\sqrt{-2},1-\sqrt{-2}\}\{1+\sqrt{-2},1+\sqrt{-2}\}\{1+\sqrt{-2},1-\sqrt{-2}\}\{1+\sqrt{-2},1+\sqrt{-2}\}^2 \\ &= \{1-\sqrt{-2},1-\sqrt{-2}\}\{1+\sqrt{-2},1+\sqrt{-2}\}\{1+\sqrt{-2},1-\sqrt{-2}\}. \end{aligned}$$

   In this rather long and daunting calculation, the third equality uses 1. to eliminate $\{-1,-1\}$, bilinearity and (d) to eliminate the third and seventh symbols, the Steinberg relation to eliminate the eighth symbol, and (c) to eliminate the ninth symbol. The fourth equality uses (c) and 2. The final equality uses (e).

   Rearranging this equation gives us

$$\{1-\sqrt{-2},1-\sqrt{-2}\}\{1+\sqrt{-2},1+\sqrt{-2}\} = \{1-\sqrt{-2},1+\sqrt{-2}\}.$$

4. We invoke the Steinberg relation one last time. Note that $(-1)(1-\sqrt{-2})+(-1)(\sqrt{-2})(1+\sqrt{-2})=1$, so

$$\begin{aligned}1 &= \{(-1)(1-\sqrt{-2}),(-1)(\sqrt{-2})(1+\sqrt{-2})\}\\ &= \{-1,-1\}\{-1,\sqrt{-2}\}\{-1,1+\sqrt{-2}\}\{1-\sqrt{-2},-1\}\\ &\quad \{1-\sqrt{-2},\sqrt{-2}\}\{1-\sqrt{-2},1+\sqrt{-2}\}\\ &= \{-1,\sqrt{-2}\}\{-1,1+\sqrt{-2}\}\{1-\sqrt{-2},-1\}\{1-\sqrt{-2},1+\sqrt{-2}\}.\end{aligned}$$

But, using the result from 3. together with (c), we see that

$$\begin{aligned}1 &= \{\sqrt{-2},\sqrt{-2}\}\{1+\sqrt{-2},1+\sqrt{-2}\}^2\{1-\sqrt{-2},1-\sqrt{-2}\}^2\\ &= \{\sqrt{-2},\sqrt{-2}\},\end{aligned}$$

where the last equality uses (e).

□

Now, to define our filtration of $K_2(\mathbb{Q}(\sqrt{-2}))$ we list the finite primes of $\mathbb{Q}(\sqrt{-2})$ in order of increasing norm:

$$\mathrm{P}_0 = \{v_1, v_2, \ldots : \mathrm{Nm}(\pi_{v_n}) \leq \mathrm{Nm}(\pi_{v_{n+1}}) \text{ for all } n \in \mathbb{N}\}.$$

Definition 3.15. Let P_0 be defined as above. For all $n \geq 1$, let

$$S_n \coloneqq \{v_1, v_2, \ldots, v_n\} \subset \mathrm{P}_0.$$

Using the notation of Tate in [3], we define, as a subgroup of $K_2(\mathbb{Q}(\sqrt{-2}))$,

$$K_2^{S_n}(\mathbb{Q}(\sqrt{-2})) \coloneqq \langle \{\alpha,\beta\} \in K_2(\mathbb{Q}(\sqrt{-2})) : \alpha,\beta \in \mathbb{Z}[\sqrt{-2}]^*_{S_n}\rangle,$$

where

$$\mathbb{Z}[\sqrt{-2}]_{S_n} = \mathbb{Z}\left[\sqrt{-2}, \frac{1}{\pi_{v_1}}, \ldots, \frac{1}{\pi_{v_n}}\right].$$

The groups $K_2^{S_n}(\mathbb{Q}(\sqrt{-2}))$ form a filtered system, and passing to the colimit, we see that $K_2(\mathbb{Q}(\sqrt{-2})) = \varinjlim_n K_2^{S_n}(\mathbb{Q}(\sqrt{-2}))$.

Lemma 3.16. *For any $n \geq 3$, the quotient group $K_2^{S_{n+1}}(\mathbb{Q}(\sqrt{-2}))/K_2^{S_n}(\mathbb{Q}(\sqrt{-2}))$ is isomorphic to $k(v_{n+1})^*$.*

Proof. For $\pi \coloneqq \pi_{v_{n+1}}$, we define a map

$$\phi\colon k(v_{n+1})^* \longrightarrow K_2^{S_{n+1}}(\mathbb{Q}(\sqrt{-2}))/K_2^{S_n}(\mathbb{Q}(\sqrt{-2}))$$

by

$$\bar{\alpha} \longmapsto \{\alpha,\pi\} \pmod{K_2^{S_n}(\mathbb{Q}(\sqrt{-2}))}.$$

By Lemma 3.12, we may assume that $\mathrm{Nm}(\alpha) \leq \frac{3}{4}\mathrm{Nm}(\pi)$. We must show that ϕ is a well-defined homomorphism. To this end, assume that $\alpha\beta \equiv \gamma \pmod{\pi}$. That is to say, write $\alpha\beta = \gamma + \delta\pi$, where $|\alpha|, |\beta|, |\gamma| \leq \frac{\sqrt{3}}{2}|\pi|$. Then

$$|\delta\pi| \leq |\alpha\beta| + |\gamma| \leq \frac{3}{4}|\pi|^2 + \frac{\sqrt{3}}{2}|\pi|,$$

and so

$$|\delta| \leq \frac{3}{4}|\pi| + \frac{\sqrt{3}}{2}.$$

Since $n \geq 3$, one readily checks that this is less than $|\pi|$. This, in turn, implies that $\mathrm{Nm}(\delta) < \mathrm{Nm}(\pi)$ and so $\bar{\delta} \in k(v_{n+1})^*$. Now, using the Steinberg relation we see that

$$\begin{aligned}
1 &= \{\frac{\gamma}{\alpha\beta}, 1 - \frac{\gamma}{\alpha\beta}\} \\
&= \{\frac{\gamma}{\alpha\beta}, \frac{\delta\pi}{\alpha\beta}\} \\
&= \{\gamma, \delta\}\{\gamma, \pi\}\{\alpha\beta, \gamma\}\{\delta, \alpha\beta\}\{\pi, \alpha\beta\}\{\alpha\beta, \alpha\beta\} \\
&\equiv \{\gamma, \pi\}\{\pi, \alpha\beta\} \pmod{K_2^{S_n}(\mathbb{Q}(\sqrt{-2}))}.
\end{aligned}$$

Here, the last equality since all of α, β, γ and δ have norms less than $\mathrm{Nm}(\pi)$ and thus belong to $K_2^{S_n}(\mathbb{Q}(\sqrt{-2}))$. Modulo $K_2^{S_n}(\mathbb{Q}(\sqrt{-2}))$, the above working out shows that $\{\alpha\beta, \pi\} = \{\gamma, \pi\}$, which proves both that ϕ is multiplicative and well-defined by taking $\beta = 1$.

To prove that ϕ is surjective, we note that the group $K_2^{S_{n+1}}(\mathbb{Q}(\sqrt{-2}))$ is generated by the elements of $K_2^{S_n}(\mathbb{Q}(\sqrt{-2}))$ together with symbols[4] of the form $\{\alpha, \pi\}$, where $\alpha \in \mathbb{Z}[\sqrt{-2}]^*_{S_n}$. This means that $\bar{\alpha} \in k(v_{n+1})^*$ and $\phi(\bar{\alpha}) = \{\alpha, \pi\}$ and so ϕ is surjective and also $\#(K_2^{S_{n+1}}(\mathbb{Q}(\sqrt{-2}))/K_2^{S_n}(\mathbb{Q}(\sqrt{-2}))) \leq \mathrm{Nm}(\pi) - 1$.

Now, let $\bar{\zeta}$ be a generator of the cyclic group $k(v_{n+1})^*$. Recalling the definition of the tame symbol in Definition 2.23, we have that

$$\overline{\tau}_{v_{n+1}}(\zeta, \pi) = \bar{\zeta} \in k(v_{n+1})^*.$$

But, by the universal property of K_2 mentioned in Definition 2.16, there exists a unique map $\psi\colon K_2(\mathbb{Q}(\sqrt{-2})) \to k(v_{n+1})^*$ such that

$$\overline{\tau}_{v_{n+1}}(\zeta, \pi) = \psi(\{\zeta, \pi\}),$$

and so $\{\zeta, \pi\}$ has order $\mathrm{Nm}(\pi)-1$. Thus, the group $K_2^{S_{n+1}}(\mathbb{Q}(\sqrt{-2}))/K_2^{S_n}(\mathbb{Q}(\sqrt{-2}))$ has order at least $\mathrm{Nm}(\pi) - 1$. By the inequality above, this means that the order is exactly $\mathrm{Nm}(\pi) - 1$, and so ϕ is an isomorphism.

□

[4]By bilinearity, we are reduced to considering symbols of the form $\{\alpha, \beta\}$, $\{\pi, \pi\}$ and $\{\alpha, \pi\}$. However, the first is an element of $K_2^{S_n}(\mathbb{Q}(\sqrt{-2}))$ and $\{\pi, \pi\} = \{-1, \pi\}$, so neither of these need be considered as separate cases.

Remark 3.17. In [10], a similar result to the lemma above is established for $K_2(\mathbb{Q}(i))$ and $n \geq 1$. Unfortunately, the bound given in Lemma 3.12 only allows us to establish the result for $n \geq 3$. This leads to the somewhat problematic primes with 3 or 11 as their norm[5]. Our aim is to prove the theorem below by induction and the base case, as we shall see, follows quite easily from Lemma 3.14. However, we must 'skip' over the cases $n = 2, 3$ if we wish make use of Lemma 3.16, which may seem dubious at first glance. We won't include the details here, as it takes us too far away from our main goal, but rest assured, this issue has been dealt with in [3] - see Proposition 1 and Lemma 2 of the Appendix.

Theorem 3.18. *For non-complex primes v, we have the following isomorphism*

$$\Phi\colon K_2(\mathbb{Q}(\sqrt{-2})) \xrightarrow{\cong} \bigoplus_v k(v)^* \cong \bigoplus_{\substack{p \text{ prime} \\ p\equiv 1,3 \pmod 8}} (\mathbb{F}_p^*)^2 \oplus \bigoplus_{\substack{p \text{ prime} \\ p\equiv 5,7 \pmod 8}} \mathbb{F}_{p^2}^*.$$

Proof. Our aim, similar to [10, Theorem 3.7], is to prove that the restriction of Φ to the subgroups $K_2^{S_n}(\mathbb{Q}(\sqrt{-2}))$ gives an isomorphism $K_2^{S_n}(\mathbb{Q}(\sqrt{-2})) \cong \bigoplus_{i=1}^n k(v_i)^*$. The result will then follow after passing to the colimit.

We begin by considering the base case $n = 1$. Here, $S_1 = \{v_1\}$ where v_1 is the prime above $2 \in \mathbb{Z}$, and $\mathbb{Z}[\sqrt{-2}]^*_{S_1}$ comprises a torsion part μ_2 and a free part generated by $\sqrt{-2}$. Using bilinearity and the relation $\{x, x\} = \{x, -1\}$, we need only consider the symbols $\{-1, -1\}$ and $\{\sqrt{-2}, \sqrt{-2}\}$. But Lemma 3.14 shows that both of these are trivial and so $K_2^{S_1}(\mathbb{Q}(\sqrt{-2}))$ is trivial, and hence isomorphic to $k(v_1)^*$ as required.

As mentioned in Remark 3.17, the cases $n = 2, 3$ have been proved in [3]. So, for $n \geq 3$, we assume, by induction that $K_2^{S_n}(\mathbb{Q}(\sqrt{-2})) \cong \bigoplus_{i=1}^n k(v_i)^*$ via Φ. We want to show that Φ induces an isomorphism

$$K_2^{S_{n+1}}(\mathbb{Q}(\sqrt{-2})) \cong \bigoplus_{i=1}^{n+1} k(v_i)^*.$$

By Lemma 3.16, if Φ maps an element $x \in K_2^{S_{n+1}}(\mathbb{Q}(\sqrt{-2}))$ to 1, then $x \in K_2^{S_n}(\mathbb{Q}(\sqrt{-2}))$, and, arguing inductively yields $x = 1$. This establishes the injectivity of Φ. Now, if $u = (u_i)_{i=1}^{n+1} \in \bigoplus_{i=1}^{n+1} k(v_i)^*$, then Lemma 3.16 gives us an element from $K_2^{S_{n+1}}(\mathbb{Q}(\sqrt{-2}))$ that maps to u_{n+1}. By the inductive hypothesis above, there is an element in $K_2^{S_n}(\mathbb{Q}(\sqrt{-2}))$ that maps to $(u_i)_{i=1}^n$ and so the product of these elements gives us the relevant preimage of u, establishing the surjectivity of Φ.

□

3.3 Deriving a reciprocity result

In this section we show how $K_2(\mathbb{Q}(\sqrt{-2}))$ gives a product formula in a similar manner to the derivation of quadratic reciprocity in Theorem 2.44. We let $\overline{\tau} = \bigoplus_v \overline{\tau}_v$ be the map defined by the tame symbols at each prime v.

[5]Note that the norm of an element $a + b\sqrt{-2}$ in $\mathbb{Z}[\sqrt{-2}]$ is given by $a^2 + 2b^2$ and so the primes 5 and 7 are inert. This means that, in the context of $S_n \subset \mathrm{P}_0$, the primes in order of increasing norm start $2, 3, 11 \ldots$.

For all $v \nmid 2$, Theorem 3.18 says that there exist maps $\psi_v \colon k(v)^* \to \mu_2$ such that the following diagram commutes:

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{-2})^* \times \mathbb{Q}(\sqrt{-2})^* & \xrightarrow{\overline{\tau}} & \bigoplus_{v \nmid 2} k(v)^* \\ & \searrow^{\left(\frac{-,-}{\sqrt{-2}}\right)} & \downarrow \prod \psi_v \\ & & \mu_2 \end{array}$$

Simply put, this says that for all $x, y \in \mathbb{Q}(\sqrt{-2})^*$,

$$\left(\frac{x, y}{\sqrt{-2}}\right) = \prod_{v \nmid 2} \psi_v(\overline{\tau}_v(x, y)).$$

Lemma 3.19. *Let v be a finite prime of $\mathbb{Q}(\sqrt{-2})$ not lying above 2 and let $q_v = \mathrm{Nm}(\mathfrak{p}_v)$. Suppose $f \colon k(v)^* \longrightarrow \mu_2$ is a homomorphism. Then f satisfies*

$$f(x) \equiv x^{\frac{q_v - 1}{2}\delta} \pmod{\mathfrak{p}_v}$$

where $\delta \in \{0, 1\}$.

Proof. In what follows, we simplify notation by writing $q = q_v$, and we identify elements x with their image in $k(v)^*$, hopefully without causing confusion.

The map f is completely determined by where it sends a generator, ζ of the cyclic group $k(v)^*$. For ζ to be a generator, we note that $\zeta^{\frac{q-1}{2}} = -1$, otherwise ζ would be a square. There are then two cases to consider:

1. if $f(\zeta) = 1$, then $f \equiv 1$ and so $f(x) \equiv x^{\frac{q-1}{2} \cdot 0} \pmod{\mathfrak{p}_v}$;
2. if $f(\zeta) = -1$, then $f(x) \equiv x^{\frac{q-1}{2} \cdot 1} \pmod{\mathfrak{p}_v}$, since their action on the generator agrees.

□

Applying the above lemma, we see that[6]:

$$\left(\frac{x, y}{\sqrt{-2}}\right) = \prod_{v \nmid 2} \psi_v(\overline{\tau}_v(x, y)) = \prod_{v \nmid 2} \overline{\tau}_v(x, y)^{\frac{q_v - 1}{2}\delta_v} = \prod_{v \nmid 2} \left(\frac{x, y}{v}\right)^{\delta_v},$$

where $\delta_v \in \{0, 1\}$ for all $v \nmid 2$, and $x, y \in \mathbb{Q}(\sqrt{-2})^*$.

To obtain a reciprocity law, we'd like to show that $\delta_v = 1$ for all primes v. We will invoke a theorem, due to Moore, which says that the relation among Hilbert symbols given in Theorem 3.5 is unique. Before stating the theorem, we make two remarks. In both cases, and in Moore's theorem, the direct sum is taken over all non-complex primes.

[6]Here, the final equality follows from a result which essentially generalises Proposition 2.41 to an arbitrary number field F. In doing so, it uses the notion of regular local Hilbert symbols and it goes somewhat beyond the requirements of this chapter to introduce these concepts purely to establish the necessary result. We instead refer the reader to [7, II. §7] for further reading.

1. Let $x, y \in F^*$ and let v be a non-complex prime. After embedding x and y into the completion F_v of F with respect to v, and applying the local Hilbert symbol from Remark 3.2, we get a map

$$F^* \times F^* \longrightarrow \mu(F_v).$$

Taking a direct sum over all non-complex primes v then gives us a symbol[7],

$$F^* \times F^* \longrightarrow \bigoplus_v \mu(F_v).$$

It is worth noting that this map is well-defined, since the local Hilbert symbol will take the value 1 for almost all v. Now, applying the universal property of K_2, gives us an induced map

$$h\colon K_2(F) \longrightarrow \bigoplus_v \mu(F_v).$$

2. If $\zeta_v \in \mu(F_v)$, then $\zeta_v^{m_v/m}$ is an m-th root of unity, and thus an element of $\mu(F)$. This gives a map

$$\begin{aligned} \phi\colon \bigoplus_v \mu(F_v) &\longrightarrow \mu(F) \\ (\zeta_v)_v &\longmapsto \prod_v \zeta_v^{m_v/m}. \end{aligned}$$

Theorem 3.20 (Moore's Theorem, [4])**.** *The sequence*

$$K_2(F) \xrightarrow{h} \bigoplus_v \mu(F_v) \xrightarrow{\phi} \mu(F) \longrightarrow 1,$$

is exact.

Now, invoking Moore's theorem, which says that there is *only one* relation of Hilbert symbols, we must have $\delta_v = 1$ for all primes v. This yields, for all $x, y \in \mathbb{Q}(\sqrt{-2})^*$,

$$\left(\frac{x, y}{\sqrt{-2}}\right) = \prod_{v \nmid 2} \left(\frac{x, y}{v}\right).$$

Finally, using Theorem 3.10 and noting that the only prime v dividing $n = 2$ is $v = \sqrt{-2}$, we see that

$$\left(\frac{x}{y}\right)_2 \left(\frac{y}{x}\right)_2^{-1} = \prod_{v \nmid 2} \left(\frac{x, y}{v}\right),$$

giving a reciprocity law for $\mathbb{Q}(\sqrt{-2})$.

[7] This map is often called the *global Hilbert symbol*.

Chapter 4

The Relationship Between Some Well-Known Reciprocity Laws

Written in the introduction to Milne's *Class Field Theory* [14] is a quote from Emil Artin about the power of (what is now called) the Artin map:

> I will tell you about the Reciprocity Law. After my thesis, I had the idea to define L-series for non-abelian extensions. But for them to agree with the L-series for abelian extensions, a certain ismorphism had to be true. I could show it implied all the standard reciprocity laws. So I called it the General Reciprocity Law and tried to prove it but couldn't, even after many tries [...] Then one afternoon I had nothing special to do, so I said, "Well, I try to prove the Reciprocity Law again." So I went out and sat down in the garden. You see, from the very beginning I had the idea to use the cyclotomic fields, but they never worked, and now I suddenly saw that all this time I had been using them in the wrong way - and in half an hour I had it.
>
> - Emil Artin, as recalled by Mattuck (in Recountings: Conversations with MIT Mathematicians 2009).

In explicitly demonstrating the power of the Artin map, the main goal of this thesis, which will be achieved in this chapter, is to prove that the Weil reciprocity generalisation follows from Artin reciprocity. As an added bonus, we will further explore the relationship between Artin, Weil and quadratic reciprocity by proving Artin implies quadratic and Weil implies quadratic.

4.1 Artin implies Weil

Our setup now will be slightly different to most other treatments of class field theory - instead of using an algebraic number field as our global field, we instead need to consider the case where we have a function field in one variable over a finite field[1].

[1]This can take one into the world of geometric (abelian) class field theory. Instead of mapping into $\mathrm{Gal}(F^{\mathrm{ab}}/F)$, one must consider the étale fundamental group of a scheme X. We choose not to go down this pathway - but the curious reader will find both [11] and [21] valuable resources.

4.1.1 Finite étale algebras and a categorical anti-equivalence

Before we begin our proof, we require a few preliminary results. We will introduce the notion of (finite) étale F-algebras and give a criterion to help classify them. We then give a categorical anti-equivalence between finite étale F-algebras and a category involving the absolute Galois group (defined below).

Definition 4.1. Let F be a field. A *(finite) étale F-algebra*[2] is an F-algebra that is isomorphic to a (finite) product of finite, separable[3] field extensions of F.

Proposition 4.2. *Let F be a field and let $f \in F[X]$. Then $A = F[X]/(f)$ is a finite étale algebra if and only if f is separable.*

Proof. Let $f = \prod f_i^{m_i}$, where the f_i are irreducible and distinct. By the Chinese Remainder Theorem we have

$$A \cong \prod F[X]/(f_i^{m_i}).$$

Now, the F-algebra $F[X]/(f_i^{m_i})$ is a field if and only if $m_i = 1$, and so it is a separable extension of F if and only if each f_i is separable.

□

In order to establish the separability of a polynomial we recall the following well-known result:

Proposition 4.3. *[15, Proposition 2.21] Let F be a field and $f \in F[X]$ a nonzero polynomial. Then, the following are equivalent:*

1. *f is separable;*
2. *$\gcd(f, f') = 1$ in $F[X]$.*

With F-algebra homorphisms as the morphisms between finite étale F-algebras, we can define the category of finite étale F-algebras, $\mathbf{EAlg}_F$. To establish the other category we will use in our categorical anti-equivalence, we need the notion of an absolute Galois group, G, and a corresponding G-set.

Definition 4.4. Let F be a field and $\bar{F}$ be some fixed algebraic closure of F. Then, the *separable closure* F_s of F is given by:

$$F_s = \{x \in \bar{F} : x \text{ is separable over } F\}.$$

The extension F_s/F is Galois, and we call the Galois group $\mathrm{Gal}(F_s/F)$ the *absolute Galois group* of F.

[2]This is also commonly referred to as a separable F-algebra.

[3]Recall that $f \in F[X]$ is a separable polynomial if and only if it has no repeated roots in every extension of F.

Definition 4.5. Let G be the absolute Galois group of a field F, given a fixed separable closure F_s. A *G-set* is a set E equipped with a continuous action of G on E, where G has the Krull topology and E has the discrete topology[4].

Definition 4.6. A *morphism* from a G-set E to a G-set E' is a map $f\colon E \to E'$ such that $f(\sigma e) = \sigma f(e)$ for all $\sigma \in G$ and $e \in E$.

Remark 4.7. The notion of a morphism of G-sets allows us to speak of the category of G-sets, which we denote **G-sets.**

The following result will enable us to use the Artin map to prove Weil reciprocity:

Theorem 4.8 ([11, Theorem 2.9])**.** *Let F be a field and G its absolute Galois group. Then, the categories $\boldsymbol{EAlg}_F$ of finite étale F-algebras, and G-**sets** of finite sets with a continuous action of G are anti-equivalent.*

4.1.2 Proof that Artin implies Weil

We begin by recalling the statements of Weil reciprocity, Theorem 2.34, and global Artin reciprocity, Theorem 1.42.

The more generalised formulation of Weil reciprocity says that, for any $f, g \in F(t)^*$, we have

$$\prod_v \mathrm{Nm}_{k(v)/F}(f,g)_v = 1,$$

where the product is taken over all discrete valuations on $F(t)$ that are trivial on F.

Recall also that global Artin reciprocity says that the map

$$\rho_F\colon \mathbb{I}_F \to \mathrm{Gal}(F^{\mathrm{ab}}/F)$$

is surjective and satisfies the following properties:

1. $F^* \subseteq \ker \rho_F$;
2. for every finite abelian extension L of F, $\hat{\rho}_F$ defines an isomorphism

$$\rho_{L/F}\colon \mathbb{I}_F/F^* \cdot \mathrm{Nm}_{L/F}(\mathbb{I}_L) \longrightarrow \mathrm{Gal}(L/F).$$

Since Artin reciprocity holds for global fields, the connection to Weil reciprocity happens in the setting of a function field over a finite field.

Let X be a smooth, projective, irreducible curve over a finite field $k = \mathbb{F}_q$. Let $F = k(X)$ be its function field and denote by $X^{(1)}$ the set of closed points of X. Let $f \in F^*$ and consider $L_f = F[t]/(t^{q-1} - f)$. Using Proposition 4.2 and Proposition 4.3, we see that this is indeed a finite étale F-algebra[5]. By the categorical anti-equivalence in Theorem 4.8, we can apply the global Artin map

[4] See, for example, chapter 8 of [15] for more detail.

[5] While this is somewhat implicitly done, the reader should be thinking of Definition 4.1 and how L_f can be written as a finite product of finite field extensions of F - all of which are separable.

from Theorem 1.42 to L_f. We will use the notation $\rho_{L_f/F}$ for the Artin map corresponding to the étale F-algebra L_f.

Letting $g \in F^*$, we seek to prove, as in the statement at the beginning of this section, that

$$\prod_{x \in X^{(1)}} \mathrm{Nm}_{k(x)/k}(f,g)_x = 1,$$

where we make the more natural choice to use $k(x)$ for the residue field instead of $k(v)$ from Theorem 2.34.

Since $g \in F^*$, Theorem 1.42 tells us that $\rho_{L_f/F}(g) = 1$. However, we also know that

$$\rho_{L_f/F}(g) = \prod_{x \in X^{(1)}} \mathrm{Frob}_x^{v_x(g)}.$$

So, we require to show that[6]

$$\mathrm{Frob}_x^{v_x(g)} = \mathrm{Nm}_{k(x)/k}(f,g)_x.$$

By weak approximation[7], we may assume that $f(x) \neq 0$. Then, $(f,g)_x = f^{v_x(g)}$, and our aim simplifies to showing

$$\mathrm{Frob}_x = \mathrm{Nm}_{k(x)/k}(f).$$

If we let d denote the degree of $k(x)$ over k, then, Proposition 1.27 tells us that

$$\begin{aligned} \mathrm{Nm}_{k(x)/k}(f) &= \prod_{\sigma \in \mathrm{Gal}(k(x)/k)} \sigma \cdot f \\ &= f^{1+q+\ldots+q^{d-1}}. \end{aligned}$$

Therefore, we calculate that

$$\begin{aligned} \mathrm{Frob}_x(t) &= t^{q^d} \\ &= t^{q^d-1} \cdot t \\ &= (t^{q-1})^{1+q+\ldots+q^{d-1}} \cdot t \\ &= f^{1+q+\ldots+q^{d-1}} \cdot t \\ &= \mathrm{Nm}_{k(x)/k}(f) \cdot t \end{aligned}$$

as required.

[6] In a slight abuse of notation, we mean that we seek to prove that the Frobenius map applied $v_x(g)$ times acts as multiplication by the norm $\mathrm{Nm}_{k(x)/k}(f,g)_x$.

[7] For reference, see Dustin Clausen's post in [1].

4.2 Artin implies quadratic

Recall the setup from chapter 1: for a finite abelian extension of number fields L/F and any $x \in F^*$, global Artin reciprocity gave us the product formula

$$\prod_v \left(\frac{x, L/F}{v}\right) = 1. \tag{4.1}$$

To prove quadratic reciprocity follows from this, we consider the special case $F = \mathbb{Q}$. Let p, q be distinct odd primes and $L = \mathbb{Q}(\sqrt{p^*})$, where $p^* = (-1)^{\frac{p-1}{2}} p$. We make this choice so that $p^* \equiv 1 \pmod 4$ and thus L/F is ramified only at p by Theorem 1.22. The aim is to show that $\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$ by computing the various Hasse symbols $\left(\frac{q, L/\mathbb{Q}}{v}\right)$.

We begin by noting that if v is unramified and $\mathrm{ord}_v(q) = 0$, then $\left(\frac{q, L/\mathbb{Q}}{v}\right) = 1$. Thus, $\left(\frac{q, L/\mathbb{Q}}{v}\right) = 1$ unless possibly $v \in \{p, q, \infty\}$. Let us consider each of these three cases:

- Let $v = \infty$. Then

  $$L_w/\mathbb{Q}_v = \mathbb{R}(\sqrt{p^*})/\mathbb{R}.$$

  If $p \equiv 1 \pmod 4$, then $p^* = p$ and the extension is trivial, giving $\left(\frac{q, L/\mathbb{Q}}{\infty}\right) = 1$. If, however, $p \equiv 3 \pmod 4$, then the extension becomes $\mathbb{C}/\mathbb{R}$. But then, by Definition 1.30, we have $\left(\frac{q, L/\mathbb{Q}}{\infty}\right) = q^{\mathrm{ord}_\infty(q)} = q^0 = 1$. In either case, we conclude that $v = \infty$ adds nothing nontrivial to (4.1).

- Let $v = q$. Then

  $$L_w/\mathbb{Q}_v = \mathbb{Q}_q(\sqrt{p^*})/\mathbb{Q}_q.$$

  This extension is unramified so $\left(\frac{q, L/\mathbb{Q}}{q}\right) = \mathrm{Frob}_q$. Note that Frob_q is trivial if and only if the extension $\mathbb{Q}_q(\sqrt{p^*})/\mathbb{Q}_q$ is trivial, which happens if and only if p^* is a square modulo q. That is to say,

  $$\left(\frac{q, L/\mathbb{Q}}{q}\right) = \left(\frac{p^*}{q}\right).$$

- Finally, let $v = p$. Then

  $$L_w/\mathbb{Q}_v = \mathbb{Q}_p(\sqrt{p^*})/\mathbb{Q}_p.$$

  This extension is ramified and, using the notation of Remark 1.36, we note that $\Phi_{F_v}(q) = 1$ if and only if $q \in \mathrm{Nm}_{L_p/\mathbb{Q}_p}(L_p^*)$. Now, $q \in \mathbb{Z}_p^*$ so $\Phi_{F_v}(q) = 1$ if and only if q is an element of the index 2 subgroup of $\mathbb{Z}_p^*$, which is precisely[8]

[8] The reader may find it helpful to recall the calculations done in Example 1.39.

the squares in $\mathbb{Z}_p^*$. Thus,

$$\begin{aligned}\Phi_{F_v}(q) = 1 &\iff q \text{ is a square in } \mathbb{Z}_p^* \\ &\iff q \text{ is a square in } (\mathbb{Z}/p\mathbb{Z})^* \\ &\iff \left(\frac{q}{p}\right) = 1.\end{aligned}$$

This gives us that:

$$\left(\frac{q, L/\mathbb{Q}}{p}\right) = \left(\frac{q}{p}\right).$$

Combining the above with (4.1), we see that

$$\left(\frac{p^*}{q}\right)\left(\frac{q}{p}\right) = 1. \tag{4.2}$$

Remark 4.9. We can use Euler's criterion and the multiplicativity of the Legendre symbol to make (4.2) look like quadratic reciprocity as it is most commonly formulated. Indeed,

$$\begin{aligned}\left(\frac{p^*}{q}\right)\cdot\left(\frac{q}{p}\right) &= \left(\frac{(-1)^{(p-1)/2}\cdot p}{q}\right)\cdot\left(\frac{q}{p}\right) \\ &= \left(\frac{(-1)^{(p-1)/2}}{q}\right)\cdot\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) \\ &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\cdot\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right).\end{aligned}$$

Putting it all together, we see that

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\cdot\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) = 1,$$

as required.

4.3 Weil implies quadratic

Let p be an odd prime, and $F, G \in \mathbb{F}_p[t]$ be two nonzero, irreducible, relatively prime, monic polynomials of degree m and n respectively. To demonstrate a quadratic reciprocity-like result, we aim to prove that

$$\left(\frac{F}{G}\right)\cdot\left(\frac{G}{F}\right)\cdot(-1)^{mn(p-1)/2} = 1.$$

Before we embark on our proof, we require a result that generalises Euler's criterion for determining whether or not an integer is a square modulo p, for some odd prime p. We also introduce a Legendre-like symbol on $\mathbb{F}_p[t]$.

Lemma 4.10. *Let $u \in \mathbb{F}_{p^r}^*$ for some positive integer r. Then*

$$u^{(p^r-1)/2} = \begin{cases} 1 & \text{if } u \text{ is a square in } \mathbb{F}_{p^r}; \\ -1 & \text{if } u \text{ is not a square in } \mathbb{F}_{p^r}. \end{cases}$$

Proof. If $u \neq 0$, then $0 = x^{p^r-1} - 1 = (x^{(p^r-1)/2} - 1)(x^{(p^r-1)/2} + 1)$. The map $\mathbb{F}_{p^r}^* \to \mathbb{F}_{p^r}^*$ given by $x \mapsto x^2$ is a homomorphism with kernel $\{\pm 1\}$. Thus, the image has order $(p^r-1)/2$ and so there are exactly $(p^r-1)/2$ squares - which are precisely the solutions to $x^{(p^r-1)/2} - 1 = 0$. □

Definition 4.11. Let p be an odd prime and let $f, g \in \mathbb{F}_p[t]^*$ be two irreducible polynomials with $\deg(g) = n$. We define the *Legendre symbol for* $\mathbb{F}_p[t]$ by[9]

$$\left(\frac{f}{g}\right) = \begin{cases} 1 & \text{if } f \text{ is a square in } \mathbb{F}_p[t]/(g) \cong \mathbb{F}_{p^n}; \\ -1 & \text{if } f \text{ is not a square in } \mathbb{F}_p[t]/(g) \cong \mathbb{F}_{p^n}. \end{cases}$$

Lemma 4.12. *Let p be an odd prime, $c \in \mathbb{F}_p^*$, and let $f \in \mathbb{F}_p[t]$ be irreducible of degree n. Then*

$$\left(\frac{c}{f}\right) = \left(\frac{c}{p}\right)^n. \tag{4.3}$$

Proof. Using Lemma 4.10 and Definition 4.11, we see that

$$\begin{aligned} \left(\frac{c}{f}\right) &= c^{(p^n-1)/2} \\ &= c^{(p-1)(1+p+\ldots+p^{n-1})/2} \\ &= (c^{(p-1)/2})^{1+p+\ldots+p^{n-1}}. \end{aligned}$$

Now, Euler's criterion tells us that $c^{(p-1)/2} = \pm 1$, so the n-term expression $1 + p + \ldots + p^{n-1}$ only matters modulo 2. Therefore, is it entirely determined by whether or not n is even or odd and it is straightforward to check that (4.3) holds in both cases.

□

Proof that Weil implies quadratic reciprocity: For a field F and $f, g \in F(t)^*$, we recall that the generalisation of Weil reciprocity (Theorem 2.34) states that

$$\prod_v \mathrm{Nm}_{k(v)/F}(f, g)_v = 1. \tag{4.4}$$

To prove quadratic reciprocity, we let p be an odd prime and $F = \mathbb{F}_p$ be the finite field of order p. We also let $f, g \in F[t]$ be two nonzero, irreducible, relatively prime polynomials of degree m and n respectively. Suppose further that the leading coefficients of f and g are a and b respectively. There are only three non-trivial valuations to consider:

[9] We choose to use the same notation as the Legendre symbol to illustrate the (surprising) connection with Weil reciprocity. In what follows, we hope it is clear from context when we are using the standard Legendre symbol and when we are using our newly defined extension to $\mathbb{F}_p[t]$.

(a) The valuation v_∞, where we recall that $v_\infty(h) = -\deg(h)$ for any $h \in F(t)$.

(b) The valuation v_f, which has associated residue field $k(v_f) = F[t]/(f) \cong \mathbb{F}_{p^m}$. Note that $v_f(f) = 1$ and $v_f(g) = 0$.

(c) The valuation v_g, which has associated residue field $k(v_g) = F[t]/(g) \cong \mathbb{F}_{p^n}$. Note that $v_g(g) = 1$ and $v_g(f) = 0$.

Using (b) and (c), we see[10] that $(f,g)_{v_f} = (-1)^{v_f(f)\cdot v_f(g)} f^{v_f(g)} g^{-v_f(f)} = g^{-1}$. In a similar manner, we calculate that $(f,g)_{v_g} = f$. Now, for any $r \in \mathbb{Z}^+$, the norm map $\mathbb{F}_{p^r}^* \to \mathbb{F}_p^*$ is given by $x \mapsto x^{(p^r-1)/(p-1)}$. Thus, (4.4) becomes

$$f^{(p^n-1)/(p-1)} \cdot g^{-(p^m-1)/(p-1)} \cdot (-1)^{mn} a^{-n} \cdot b^m = 1.$$

Raising both sides to the power $(p-1)/2$, this implies that

$$f^{(p^n-1)/2} \cdot g^{-(p^m-1)/2} \cdot (-1)^{mn(p-1)/2} a^{-n(p-1)/2} \cdot b^{m(p-1)/2} = 1. \tag{4.5}$$

Then (4.5) becomes

$$\left(\frac{f}{g}\right) \cdot \left(\frac{g}{f}\right) \cdot (-1)^{mn(p-1)/2} a^{-n(p-1)/2} \cdot b^{m(p-1)/2} = 1. \tag{4.6}$$

Write $f = aF$ and $g = bG$, so that F and G are monic. Then, using the multiplicativity of the Legendre symbol for $\mathbb{F}_p[t]$ together with Lemma 4.12 yields

$$\left(\frac{F}{G}\right) \cdot \left(\frac{G}{F}\right) \cdot (-1)^{mn(p-1)/2} = 1.$$

□

Remark 4.13. In demonstrating how one can arrive at something resembling quadratic reciprocity, we could have ended our proof at (4.6) with the additional terms still in there. However, much like when quadratic reciprocity for the Jacobi symbol is written using coprime *positive* integers, we chose to write our final statement using *monic*, irreducible polynomials.

[10] A slight abuse of notation sees us writing f and g when we really mean f modulo g and g modulo f respectively.

Final Remarks

While not usually included in written mathematics, it seems like a missed opportunity not to discuss the things that did not quite work out. In deriving the reciprocity result of section 3.3, the initial aim was to mimic the proof of Theorem 2.44 to show *directly* that $\delta_v = 1$ for all v, without having to rely on Moore's Theorem. One of the main barriers was trying to calculate the values of the symbol $\left(\frac{x,y}{\sqrt{-2}}\right)$. An attempt was made to employ the techniques found in chapter 1 of [10].

In that case, the author considered the field $F = \mathbb{Q}(i)$. Defining the higher unit groups $U_v^n := 1 + \mathfrak{p}_v^n$ for $n \geq 1$, the author was able to establish that $(U_{1+i})^4 \cong U_{1+i}^7$ and that

$$U_{1+i}/(U_{1+i})^4 \cong \mu_4 \oplus \langle \overline{3+2i} \rangle \oplus \langle \bar{5} \rangle,$$

where $(U_{1+i})^4$ denotes the 4^{th} powers in U_{1+i}.

They were able then to prove that

$$\left(\frac{\pi, \tau}{1+i}\right)_4 = \begin{cases} 1 & \text{if } \pi \text{ or } \tau \equiv 5 \pmod{(U_v)^4} \\ -1 & \text{if } \pi \equiv \tau \equiv 3+2i \pmod{(U_v)^4}. \end{cases}$$

This was all done in order to prove biquadratic reciprocity (hence the use of $(U_{1+i})^4$ and the Hilbert symbol of order 4).

For $F = \mathbb{Q}(\sqrt{-2})$, we would need to consider the set of squaresv $(U_v)^2$ for the prime v corresponding to $\sqrt{-2}$. Lemmas 1.33 and 1.34 of [10] tell us that we can only hope for a result like $(U_v)^2 \cong U_v^4$. Simply checking that $(1+\sqrt{-2})^2 \notin U_v^4$ is enough to show that no such result analogous to that of $\mathbb{Q}(i)$ exists.

An unsuccessful attempt was made at trying to directly find generators for $U_v/(U_v)^2$, in the hope that evaluating the right hand side of

$$\left(\frac{x, y}{\sqrt{-2}}\right) = \prod_{v \nmid 2} \left(\frac{x, y}{v}\right)$$

on these generators would imply that each $\delta_v = 1$.

Bibliography

[1] Dustin Clausen (https://mathoverflow.net/users/3931/dustin-clausen). *Weil reciprocity vs Artin reciprocity*. MathOverflow. URL:https://mathoverflow.net/q/96349 (version: 2012-05-08). URL: https://mathoverflow.net/q/96349.

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

[3] Hyman Bass and John Tate. 'The Milnor ring of a global field'. In: *"Classical" Algebraic K-Theory, and Connections with Arithmetic*. Springer Berlin Heidelberg, 1973, pp. 347–446.

[4] Stephen Chase and William Waterhouse. 'Moore's theorem on uniqueness of reciprocity laws'. In: *Inventiones mathematicae* 16 (1972), pp. 267–270.

[5] Harold M. Edwards. *Fermat's last theorem: a genetic introduction to algebraic number theory*. Vol. 50. Springer Science & Business Media, 1996.

[6] Fernando Gouvêa. *p-adic Numbers*. Universitext. Springer Berlin Heidelberg, 2003.

[7] Georges Gras. *Class Field Theory: from theory to practice*. Springer, 2003.

[8] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*. Vol. 84. Springer Science & Business Media, 1990.

[9] Kazuya Kato. 'A generalization of local class field theory by using K-groups. II'. In: *Journal of the Faculty of Science, the University of Tokyo. Sect. 1 A, Math.* 27 (1980), pp. 603–683.

[10] Håkon A. Kolderup. 'Number Theoretic Symbols in K-theory and Motivic Homotopy Theory'. MA thesis. 2016.

[11] Hendrik W. Lenstra. 'Galois theory for schemes'. In: 1985.

[12] Bruce A. Magurn. *An algebraic introduction to K-theory*. Vol. 87. Cambridge University Press, 2002.

[13] James S. Milne. *Algebraic Number Theory (v3.08)*. Available at www.jmilne.org/math/. 2020.

[14] James S. Milne. *Class Field Theory (v4.02)*. Available at www.jmilne.org/math/. 2013.

[15] James S. Milne. *Fields and Galois Theory (v5.10)*. Available at www.jmilne.org/math/. 2022.

[16] John Milnor. ‘Algebraic K-theory and quadratic forms’. In: *Invent. Math.* 9 (1970), pp. 318–344.

[17] John Milnor. *Introduction to algebraic K-theory*. 72. Princeton University Press, 1971.

[18] Eoin O. Murchadha. ‘Menelaus’ Theorem, Weil Reciprocity, and a Generalisation to Algebraic Curves’. In: (2012).

[19] Jürgen Neukirch. *Algebraic number theory*. Vol. 322. Springer Science & Business Media, 2013.

[20] Jonathan Rosenberg. *Algebraic K-theory and its applications*. Vol. 147. Springer-Verlag, New York, 2012.

[21] Pál P. Tóth. ‘Geometric Abelian Class Field Theory’. In: 2011.

[22] Charles A. Weibel. *The K-book: An introduction to algebraic K-theory*. Vol. 145. American Mathematical Society Providence, 2013.