UiO : Department of Mathematics
University of Oslo

Number Theoretic Symbols in K-theory and Motivic Homotopy Theory

Håkon Kolderup

Master's Thesis, Spring 2016

Abstract

We start out by reviewing the theory of symbols over number fields, emphasizing how this notion relates to classical reciprocity laws and algebraic K-theory. Then we compute the second algebraic K-group of the fields $\mathbf{Q}(\sqrt{-1})$ and $\mathbf{Q}(\sqrt{-3})$ based on Tate's technique for $K_2(\mathbf{Q})$, and relate the result for $\mathbf{Q}(\sqrt{-1})$ to the law of biquadratic reciprocity.

We then move into the realm of motivic homotopy theory, aiming to explain how symbols in number theory and relations in K-theory and Witt theory can be described as certain operations in stable motivic homotopy theory. We discuss Hu and Kriz' proof of the fact that the Steinberg relation holds in the ring $\pi_{*\alpha}\mathbf{1}$ of stable motivic homotopy groups of the sphere spectrum $\mathbf{1}$. Based on this result, Morel identified the ring $\pi_{*\alpha}\mathbf{1}$ as the Milnor-Witt K-theory $K_*^{MW}(F)$ of the ground field F. Our last aim is to compute this ring in a few basic examples.

Contents

Introduction

From reciprocity laws to K-theory

In number theory, one ubiquitous problem is that of solving equations over finite fields. In the case of quadratic equations, the problem led Legendre to introduce the symbols $(-/q)$ representing solvability of quadratic equations over $\mathbf{F}_q$. The pinnacle of theory is the quadratic reciprocity law of Gauss (Theorem 1.1) relating Legendre symbols over different primes.

Since the time of Gauss, the Legendre symbols have been generalized to arbitrary number fields, and to symbols representing solvability over finite fields of equations of any degree. Most notable are perhaps the Hilbert symbols $\left(\frac{-,-}{v}\right)$, which we will introduce in Chapter 1. These symbols satisfy properties like antisymmetry, bimultiplicativity and the relation

$$\left(\frac{x, 1-x}{v}\right) = 1. \tag{1}$$

This last property turned out to be very important. Indeed, Steinberg's work on central extensions led him to study certain bimultiplicative maps with values in an abelian group satisfying the relation (1) above [Tat76a]. Such maps are now called Steinberg symbols, and the relation (1) is called the Steinberg relation. Hilbert symbols provide important examples of Steinberg symbols.

By Matsumoto's description of the second K-group $K_2(F)$ of a field F, it turns out that $K_2(F)$ is the universal object with respect to Steinberg symbols. By formulating the classical law of quadratic reciprocity in terms of Hilbert symbols on $\mathbf{Q}$, this insight led Tate to the discovery that the structure theorem for $K_2(\mathbf{Q})$ is actually equivalent to quadratic reciprocity.

Classification problems and Milnor's conjecture

In every part of mathematics there are objects constructed for the purpose of classifying other mathematical objects. For example:

- In the machinery of algebraic K-theory, we have the group K_0 which classifies, e.g., isomorphism classes of finitely generated projective modules over a ring or classes of vector bundles on a scheme. The higher algebraic K-groups also take into account certain symmetry properties of the ground object of study.

- A classical problem that has been the subject of extensive study over the years is that of classifying quadratic forms over fields. The so-called Witt ring $W(F)$ of a field F evolved out of this problem, whose elements represents equivalence classes of quadratic spaces over F.

- Parallel to the story of the Witt ring is that of the Galois cohomology $H^*_{\mathrm{Gal}}(F; -)$. It is known for example that $H^2_{\mathrm{Gal}}(F; F^\times_{\mathrm{sep}})$—where F_{sep} is the separable closure of F—classifies equivalence classes of central simple algebras over the field F, while $H^1_{\mathrm{Gal}}(F; \mathbf{Z}/2)$ is the set of square classes of elements in $F^\times$.

The algebraic K-theory, the Witt ring and the Galois cohomology of a field F are clearly highly interesting invariants of F. What Milnor did in [Mil70] was to define a ring $K_*^M(F)$, purely in terms of generators and relations, which would serve as a sort of "best approximation" to the Witt theory and Galois cohomology of F [Dug04, 1.7]. The Milnor K-groups $K_n^M(F)$ agree with algebraic K-theory for n equal to 0, 1 and 2, but not generally in higher degrees. Letting $I(F)$ denote the fundamental ideal of the Witt ring $W(F)$, Milnor produced homomorphisms

$$\begin{array}{ccc} & K_n^M(F)/2K_n^M(F) & \\ \swarrow & & \searrow \\ I^n(F)/I^{n+1}(F) & & H^n_{\mathrm{Gal}}(F;\mathbf{Z}/2) \end{array}$$

and proved that these maps are isomorphisms in degrees 0, 1 and 2 as well as always being surjective. But it required the machinery of motivic homotopy theory—invented during the 1990s—to prove Milnor's conjecture that the maps are actually isomorphisms in every degree. More on this in Chapter 2.

The settlement of the Milnor conjecture shed a whole new light on the theory of quadratic forms over fields. For example, it made it possible to think about relations in both Witt theory and Milnor K-theory as operations in stable motivic homotopy theory. More precisely, further studies in motivic homotopy theory revealed that the stable motivic homotopy groups $\pi_{*\alpha}\mathbf{1}$ of the motivic sphere spectrum $\mathbf{1}$ could be described as the so-called Milnor-Witt K-theory $K_*^{MW}(F)$ of the ground field F. As the sphere spectrum is initial in the category of ring spectra, any homotopy group $\pi_{m+n\alpha}R$ of a ring spectrum R will inherit the relations in the group $\pi_{m+n\alpha}\mathbf{1}$ via the map $\pi_{m+n\alpha}\mathbf{1} \to \pi_{m+n\alpha}R$ induced by the unique unit map $\mathbf{1} \to R$. In this regard, Milnor-Witt K-theory is a fundamental object in stable motivic homotopy theory.

One prime at a time...

By the fundamental theorem of arithmetic, there is an isomorphism of abelian groups

$$\begin{aligned} \mathbf{Q}^\times &\xrightarrow{\cong} \mathbf{Z}/2 \oplus \bigoplus_{p \text{ prime}} \mathbf{Z} \\ x &\longmapsto (\mathrm{sgn}(x), \mathrm{ord}_2(x), \mathrm{ord}_3(x), \dots, \mathrm{ord}_p(x), \dots). \end{aligned}$$

Here $\mathrm{sgn}(x)$ is the sign of the rational number x, and $\mathrm{ord}_p(x)$ is the p-adic valuation of x. This isomorphism suggests that in order to solve a problem concerning the field $\mathbf{Q}$, it might be helpful to consider the problem in each completion $\mathbf{Q}_p$ of $\mathbf{Q}$, as well as in $\mathbf{R}$. In other words, one should consider one prime at a time. Hasse-Minkowski's local-global principle [MH73, Corollary 2.4, p.89] is a typical example of this, stating that a quadratic form defined over $\mathbf{Q}$ represents zero if and only if it represents zero in each completion $\mathbf{Q}_p$, as well as in $\mathbf{R}$. In fact, this local-global philosophy is used extensively in class field theory, as we will see examples of in Chapter 1.

Turning to the realm of K-theory, it was Tate who was the first one out to compute the group $K_2(\mathbf{Q})$. Using additive notation, the result is

$$K_2(\mathbf{Q}) \cong \mathbf{Z}/2 \oplus \bigoplus_{p \text{ prime}} K_1(\mathbf{F}_p).$$

Tate's method of computation consisted of defining a filtration of $K_2(\mathbf{Q})$ by subgroups indexed over the primes, and then analyzing each of these subgroups separately in order to "conclude globally". By Hilbert's formulation of the known reciprocity laws by means of considering one reciprocity symbol for each prime (see Theorem 1.55), Tate's computation made it possible to relate K-groups of number fields to reciprocity laws. More on all this in Chapter 3.

Tate's computation of $K_2(\mathbf{Q})$ inspired Milnor to give a new proof of the structure theorem for the Witt ring of $\mathbf{Q}$ [MH73, Theorem 2.1, p.88]:

$$W(\mathbf{Q}) \cong \mathbf{Z} \oplus \bigoplus_{p \text{ prime}} W(\mathbf{F}_p).$$

Again, the proof consists of defining a filtration of $W(\mathbf{Q})$, one subgroup for each prime, and considering one of these at a time.

In Chapter 5, we will see that this method also carries over to the case of Milnor-Witt K-theory. More precisely, for $n \geq 2$ we compute $K_n^{MW}(\mathbf{Q})$; the result being

$$K_n^{MW}(\mathbf{Q}) \cong \mathbf{Z} \oplus \bigoplus_{p \text{ prime}} K_{n-1}^{MW}(\mathbf{F}_p).$$

Outline

Chapter 1 provides background material for understanding number theoretic aspects of the K-theory we consider in Chapter 3. This chapter has two main themes: First we give a more or less detailed treatment of the properties of the number fields $\mathbf{Q}(\sqrt{-1})$ and $\mathbf{Q}(\sqrt{-3})$, which is needed later on. We then move on to discuss symbols over number fields and their relation to classical reciprocity laws. Number theoretic symbols are perhaps the main connection between number theory and classical algebraic K-theory, so we make an effort to introduce this concept thoroughly. In particular, we take a detour to visit class field theory and the origins of tame symbols. It is of course possible to take the formula in Proposition 1.52 as the definition of tame symbols and then move directly onto K-theory, but we find it illuminating to consider a more unified treatment of all the different number theoretic symbols, which is achieved by realizing these symbols as offspring of the local reciprocity map of local class field theory. As a motivation, we provide some background material on the history of reciprocity laws in the beginning of Chapter 1. We revisit classical reciprocity laws in new guises in Section 1.6, finishing the chapter by taking a closer look at biquadratic reciprocity.

Chapter 2 introduces some preliminary theory on classical algebraic K-theory. We also go through the definition and basic properties of Milnor K-theory and Witt theory. Finally, we briefly explain Milnor's conjecture relating Milnor K-theory, Witt theory and Galois cohomology.

Chapter 3 deals with some explicit calculations. Specifically, we compute the second K-group of the fields $\mathbf{Q}(\sqrt{-1})$ and $\mathbf{Q}(\sqrt{-3})$ based on Tate's technique for $K_2(\mathbf{Q})$. We hope to illustrate how the arithmetic of the given number field reveals itself in the K-group, e.g., by making use of previous results on units; the Euclidean algorithm; the structure of residue fields and the ramification and splitting behavior of primes in these number fields. In particular, we connect the result on $K_2(\mathbf{Q}(\sqrt{-1}))$ to the law of biquadratic reciprocity.

Chapter 4 is a brief introduction to motivic homotopy theory. The goal of this chapter is to provide background material and motivation for studying Milnor-Witt K-theory. The reader who wishes may therefore skip this chapter, as the definition of Milnor-Witt K-groups is purely algebraic and does not involve any motivic machinery. Note however that the defining generators and relations of Milnor-Witt K-theory have natural explanations as elements in stable motivic homotopy groups. Moreover, a few results from this chapter are used in the beginning of Chapter 5.

Chapter 5 aims to study how symbols in K-theory and Witt theory may be thought of as coming from operations in stable motivic homotopy theory. We start out by explaining Hu and Kriz' proof that the Steinberg relation holds in certain stable motivic homotopy groups, which was the starting point for Morel and Hopkins' discovery of Milnor-Witt K-theory. We take a brief look at how the ring spectrum map $\mathbf{1} \to \mathsf{KGL}$ behaves with respect to the well known symbols in K-theory. Then we proceed to study the properties of Milnor-Witt K-groups, and use similar methods as those of Chapter 3 to compute the Milnor-Witt K-theory of $\mathbf{Q}$ and $\mathbf{Q}(\sqrt{-1})$.

In Chapter 1, familiarity with some basic algebraic number theory is an advantage—for example a rough equivalent of the first two chapters of [Jan96]. However, we provide references to all the results we are using. In Chapter 4, we leave out background material on model categories, simplicial sets, sites and abstract homotopy theory. The interested reader may consult [DLØ+07] and [Hov99]. The remaining chapters should be fairly self-contained.

Acknowledgements

I would like to thank my advisor, Prof. Paul Arne Østvær, for his excellent guidance and patience throughout my work on this thesis. I thank Jonas for helpful discussions, proofreading and valuable suggestions, and Martin for proofreading and endless LaTeX-tips. Finally, I am grateful to Jarle for helpful discussions, and to the people at the sixth floor of the Abel building.

We exploit the opportunity to address a formal apology to Paul Arne in the wake of the author's reckless behavior in the Easter holiday, during which he—without notice—went fishing instead of showing up at the gym. It shall not happen again.

Conventions and notation

Throughout this text, the symbol F will denote a field.

By saying that a number field F is *Euclidean* we mean that the ring of integers $\mathcal{O}_F$ in F is Euclidean with respect to the norm map $\mathrm{Nm} : \mathcal{O}_F \to \mathbf{Z}$. By abuse of notation, we denote also by Nm the counting norm $\mathrm{Nm}(\mathfrak{a})$ defined on the set of integral ideals $\mathfrak{a}$ of $\mathcal{O}_F$, i.e., $\mathrm{Nm}(\mathfrak{a})$ is the *integer* $\#(\mathcal{O}_F/\mathfrak{a})$. Recall that, if $\mathfrak{a} = (a)$ is a principal ideal of $\mathcal{O}_F$, then $\mathrm{Nm}(a) = \mathrm{Nm}(\mathfrak{a})$ (see [Jan96, pp.42-45]).

We use the word "place" for an equivalence class of nontrivial absolute values on a number field. Note that the word "prime" is often used for the same concept in the literature.

Following Gras [Gra03], the word "ramification" is—as opposed to classical literature—used only in connection with finite places (i.e., the places corresponding to prime ideals in the ring of integers); the phenomenon of real infinite places becoming complex in some extension of number fields will instead be referred to as *complexification* (however, we shall rarely need to make use of this term. The important thing to note is that infinite places are not included when we speak about ramification).

When discussing algebraic K-theory of rings, we implicitly assume that all rings in consideration are commutative and unital. This is done because we only apply the K-theoretic machinery to such rings, and furthermore in order to avoid overstating the word *commutative.* Note however that several of the constructions of Chapter 2 apply to any associative ring.

When we consider the algebraic K-groups $K_n(F)$ of fields in Chapter 2 and Chapter 3, we will use multiplicative notation in order to keep in line with the notations of class field theory. In the context of Milnor K-theory, however, we switch to additive notation (e.g., compare $\{xy, z\} = \{x, z\}\{y, z\} \in K_2(F)$ and $\{xy, z\} = \{x, z\} + \{y, z\} \in K_2^M(F)$).

As we shall see in Chapter 4, we will denote by S^α the motivic sphere $\mathbf{G}_m$. Note however that the symbol S_t^1 is also often used in the literature (the t coming from the name "Tate circle"); this explains the notation $\Sigma_t := - \wedge S^\alpha$ used in Section 5.2 of Chapter 5.

CHAPTER 1

Results from Algebraic Number Theory

The history of reciprocity laws in number theory is impressively long and rich, to which several great names in mathematics have contributed. Below we start out by reviewing a tiny fraction of this story. From the time of Lagrange and Gauss, through the generalizations of Jacobi, Eisenstein, Hilbert and Artin we arrive at Tate and his discovery of the connection between reciprocity laws and K-theory. We then move on to study this connection in detail in the subsequent chapters.

1.1 Reciprocity laws

The famous *law of quadratic reciprocity* was stated in its complete form by Lagrange, but it was Gauss who first gave a full proof [Mil13b, vii]. Legendre introduced the symbols (p/q) for distinct odd primes p and q, demanding

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

The Legendre symbols allow for a compact formulation of the quadratic reciprocity law, which by now is the most common phrasing of the theorem:

Theorem 1.1 (Quadratic reciprocity [Lem00, p.vi])**.** *Let p and q be two distinct odd primes. Then*

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right). \tag{1.1}$$

Moreover, the following supplementary laws hold, for p an odd prime:

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

In other words, p is a square modulo q if and only if q is a square modulo p unless both p and q are congruent to 3 modulo 4, in which case p is a square modulo q if and only if q is a *nonsquare* modulo p.

There are several possible reasons as to why Gauss considered the quadratic reciprocity law worthy of the name “aureum theorema” (golden theorem). First of all, the very existence of a connection between two arbitrarily chosen prime numbers is quite astonishing in its own right. Quadratic reciprocity strengthens the philosophy that in order to understand an object, we should try to understand how it relates to other objects. In this case the objects are integers, and the reciprocity law states that there is indeed a rather mysterious connection between two prime numbers emanating as we turn to the “relative case”, i.e., look at their residue classes. This train of thought has of course been exploited to its full extent throughout modern mathematics. For example, it was the groundbreaking philosophy of Grothendieck that we should consider morphisms between objects rather than just the objects themselves, and the zeroth K-group in algebraic K-theory is an example of how we can understand a ring by understanding modules over the ring.

Furthermore, the quadratic reciprocity law solves a certain *inverse problem*. Given a prime number p, determining the integers that are quadratic residues modulo p is clearly a finite problem as one can simply check all elements in the finite group $\mathbf{Z}/p$. The inverse problem however, i.e., fixing an integer n and asking for which primes p is n a quadratic residue modulo p, is a question of seemingly an entirely different nature. It is now the strength of Formula 1.1 becomes apparent: The "infinite" inverse problem can be transformed into the finite direct problem of determining the quadratic residues modulo n.

To study quadratic residues modulo primes is to study quadratic polynomials over finite fields, and motivation for the latter is readily given by the Hasse-Minkowski theorem on the local-global principle for quadratic forms. For instance, if q is an odd prime number the polynomial $f(x) := x^2 - q$ splits in $\mathbf{F}_p[x]$ if and only if $(q/p) = 1$. Thus, the problem of determining the splitting of f modulo different primes is an example of an "inverse problem" as described above: Each time one changes the prime p and asks for the splitting behavior over $\mathbf{F}_p$ one has to compute a new Legendre symbol (q/p). Using quadratic reciprocity we convert the problem into computing (p/q) instead—a much more comfortable task, requiring only to check the q residue classes once and for all.

Example 1.2 ([Wym72, Example 1, p.573])**.** Let $f(x) := x^2 - 17$, and let us determine all primes p such that f splits over $\mathbf{F}_p$. A priori, we must compute $(17/p)$ for all p. However, quadratic reciprocity yields

$$\left(\frac{17}{p}\right) = \left(\frac{p}{17}\right)$$

since $17 \equiv 1 \pmod 4$. The quadratic residues modulo 17 are 1, 2, 4, 8, 9, 13, 15 and 16, hence f splits over $\mathbf{F}_p$ if and only if p is congruent modulo 17 to one of the listed numbers.

The splitting of quadratic polynomials over a number field F modulo different primes is closely related to the knowledge of the extension of F defined by the polynomial. In fact, knowing of the set of prime ideals that split in an extension L/F of number fields is enough to determine L [Mil13b, p.2]. Quadratic reciprocity is the key to determine which primes that split in quadratic extensions of $\mathbf{Q}$, and should therefore be considered the first step toward understanding the splitting of prime ideals in arbitrary extensions of number fields. In other words—as Milne notes in [Mil13b, p.3]—quadratic reciprocity should be viewed as the first result in class field theory.

Based on the following description of the Legendre symbol one generalizes it to n-th power residue symbols (see Definition 1.56 below):

Proposition 1.3. *The Legendre symbol satisfies* $(p/q) \equiv p^{\frac{q-1}{2}} \pmod q$.

Proof. The sequence

$$1 \longrightarrow \mu_2 \hookrightarrow \mathbf{F}_q^\times \xrightarrow{\alpha} \mathbf{F}_q^\times \xrightarrow{\beta} \mu_2 \longrightarrow 1$$

in which $\alpha(x) := x^2$ and $\beta(y) := y^{\frac{q-1}{2}}$ is clearly a complex by Fermat's little theorem. To show exactness at the second $\mathbf{F}_q^\times$, assume $x \in \mathbf{F}_q^\times$ is such that $x^{\frac{q-1}{2}} = 1$. Let ζ be a generator for the cyclic group $\mathbf{F}_q^\times$ with $x = \zeta^k$, then

$$x^{\frac{q-1}{2}} = \zeta^{k\frac{q-1}{2}} = 1,$$

hence $2 \mid k$, hence x is a square. Thus p is a square modulo q if and only if $p^{\frac{q-1}{2}} \equiv 1 \pmod q$. □

Gauss noticed that the ring of Gaussian integers $\mathbf{Z}[i]$, where $i^2 = -1$, was the appropriate setting for a formulation of a *biquadratic residue law* [Lem00, p.vi]:

Definition 1.4. Let π and τ be two distinct prime elements of $\mathbf{Z}[i]$ not dividing 2. The *biquadratic residue symbol* $(\pi/\tau)_4$ is the unique element in $\mu_4 = \{\pm 1, \pm i\}$ satisfying

$$\left(\frac{\pi}{\tau}\right)_4 \equiv \pi^{\frac{\mathrm{Nm}(\tau)-1}{4}} \pmod{\tau}.$$

We have $(\pi/\tau)_4 = 1$ if and only if $x^4 \equiv \pi \pmod{\tau}$ has a solution in the Gaussian integers.

Definition 1.5. A Gaussian integer α is *primary* if $\alpha \equiv 1 \pmod{(1+i)^3}$.

Theorem 1.6 (Biquadratic reciprocity [Lem00, p.vii])**.** *Let π and τ be distinct primary Gaussian primes. Then*

$$\left(\frac{\pi}{\tau}\right)_4 = (-1)^{\frac{\mathrm{Nm}(\pi)-1}{4}\cdot\frac{\mathrm{Nm}(\tau)-1}{4}} \left(\frac{\tau}{\pi}\right)_4.$$

Moreover, the following supplementary laws hold:

$$\left(\frac{i}{\pi}\right)_4 = i^{\frac{\mathrm{Nm}(\pi)-1}{4}}, \qquad \left(\frac{1+i}{\pi}\right)_4 = i^{\nu-\mu},$$

where the integers μ and ν are determined as follows: By Proposition 1.23, the group $U_{1+i}/(U_{1+i}^4)$ of local units modulo fourth powers is isomorphic to $\mu_4 \oplus \langle\overline{3+2i}\rangle \oplus \langle\overline{5}\rangle$. Using this isomorphism, write $\pi \equiv i^k(3+2i)^\mu 5^\nu \pmod{(U_{1+i})^4}$ (see Section 1.3.1 and Section 1.5 for explanation of the notation).

Theorem 1.6 will be proved at the end of this chapter using power reciprocity. Later we will also consider how biquadratic reciprocity is connected to the second K-group of $\mathbf{Q}(i)$.

The biquadratic reciprocity theorem settles a reciprocity law for the cyclotomic extension $\mathbf{Q}(\zeta_4) = \mathbf{Q}(i)$, and it is natural to ask whether there is a reciprocity law for each cyclotomic field $\mathbf{Q}(\zeta_p)$. Jacobi led the search for such a general law, but the failure of unique factorization in these fields[1] led to serious obstacles. It was not until Kummer's invention of ideal numbers that progress was made possible, and eventually it was Eisenstein who succeeded in finding a reciprocity law for all odd primes [Lem00, p.vii]. In the following statement, we refer the reader to Definition 1.56 and the discussion following it for the meaning of the symbols $(-/\alpha)_n$.

Theorem 1.7 (Reciprocity at odd primes [Lem00, p.vii])**.** *Let p be an odd prime. We call an element $\alpha \in \mathbf{Z}[\zeta_p] = \mathcal{O}_{\mathbf{Q}(\zeta_p)}$* primary *if α is congruent to a rational integer modulo $(1-\zeta_p)^2$.*

If $\alpha \in \mathbf{Z}[\zeta_p]$ is primary, then

$$\left(\frac{\alpha}{a}\right)_p = \left(\frac{a}{\alpha}\right)_p$$

for all $a \in \mathbf{Z}$ prime to p.

The search for a complete generalization of quadratic reciprocity to arbitrary number fields is one of the main objectives of algebraic number theory. Indeed, this is the content of Hilbert's ninth problem. Hilbert discovered that the classical law of quadratic reciprocity could be phrased in terms of Hilbert symbols (see Definition 1.53) as a product formula

$$\prod_{v \in \mathrm{Pl}_{\mathbf{Q}}} \left(\frac{x, y}{v}\right) = 1 \tag{1.2}$$

for $x, y \in \mathbf{Q}^\times$, and conjectured that a similar formula should hold for any number field F [Lem00, p.viii]. This product formula was settled for abelian extensions of number fields by the breakthrough of class field theory and Artin's general reciprocity law, as we will see in Theorem 1.55 (in which the notations used in (1.2) are also explained). We shall also see explicitly that if we work over the number field $\mathbf{Q}(i)$, the corresponding product formula reduces to the biquadratic reciprocity law.

Artin's general reciprocity law will be stated in its idèlic form in Theorem 1.46 below, but for completeness we also mention the classical ideal group version:

[1] The class group of $\mathbf{Q}(\zeta_p)$ is trivial for $2 \leq p \leq 19$; the first instance of a cyclotomic field with nontrivial class group is $\mathbf{Q}(\zeta_{23})$, where $\mathrm{Cl}(\mathbf{Q}(\zeta_{23})) \cong \mathbf{Z}/3$ [Was82, p.353]. As p increases, the class number of $\mathbf{Q}(\zeta_p)$ grows exponentially [Was82, Theorem 4.20].

Theorem 1.8 (Artin's reciprocity law [Gra03, II 4.4])**.** *Let F be a number field and L/F a finite abelian extension. Let T be the set of ramified places in L/F and let $\mathfrak{m}$ be a modulus built from T. Then the Artin symbol $\alpha_{L/F} : I_T \to \mathrm{Gal}(L/F)$ induces a canonical isomorphism*

$$\frac{I_T}{P_{T,\mathfrak{m},\mathrm{pos}}\,\mathrm{Nm}_{L/F}(I_{L,T})} \xrightarrow[\alpha_{L/F}]{\cong} \mathrm{Gal}(L/F).$$

Here I_T is the group of fractional ideals of F prime to T, and $\mathfrak{m}$ is an integral ideal of the form $\mathfrak{m} := \prod_{v \in T} \mathfrak{p}_v^{n_v}$ for some $n_v \geq 0$, where $\mathfrak{p}_v$ is the maximal ideal corresponding to the finite place v. The group $P_{T,\mathfrak{m},\mathrm{pos}}$ is the group of principal fractional ideals (x) of F prime to T, with x totally positive and satisfying $\mathrm{ord}_v(x-1) \geq n_v$ for all $v \in T$, i.e., $x \equiv 1 \pmod{\mathfrak{m}}$.

Later Tate generalized the group isomorphism aspect of Artin's reciprocity law via the cohomological interpretation of class field theory. Specifically, Tate showed that—for L/F a finite Galois extension—cup product with the fundamental class

$$u_{L/F} \in \widehat{H}^2(\mathrm{Gal}(L/F), C_L)$$

induces a canonical isomorphism

$$x \mapsto x \smile u_{L/F} : \widehat{H}^r(\mathrm{Gal}(L/F); \mathbf{Z}) \xrightarrow{\cong} \widehat{H}^{r+2}(\mathrm{Gal}(L/F); C_L)$$

for all $r \in \mathbf{Z}$; see [Gra03, p.109]. Here the $\widehat{H}^r$ are Tate's modified cohomology groups (see, e.g., [Wei94, Definition 6.2.4]), and C_L is the idèle class group of L, defined in Definition 1.39. Tate was also the first to discover the connection between the second algebraic K-group and reciprocity laws—more precisely, he computed the group $K_2(\mathbf{Q})$ and noticed that the method was very similar to the formal part of Gauss' first proof of quadratic reciprocity [Tat76a, p.318]. It involved induction over the primes and use of the Euclidean algorithm; we will return to this in Chapter 3. It is this K-theoretic view on classical number theory we shall keep in mind in the subsequent chapters.

As a final remark we mention that the story of the general reciprocity law is far from over: Although class field theory solves Hilbert's ninth problem in the case of abelian extensions of number fields, the general case remains unsolved to this date.

1.2 Preliminary results on quadratic fields

Let d be a squarefree integer, and consider the field $F := \mathbf{Q}(\sqrt{d})$. Recall the following result, whose proof can be found in, e.g., [IR90, Proposition 13.1.1].

Proposition 1.9. *The ring of integers $\mathcal{O}_F$ in $F = \mathbf{Q}(\sqrt{d})$ equals*

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

Note that, by the fundamental identity [Mil13a, Theorem 3.34], if a rational prime p is ramified in a quadratic extension $F/\mathbf{Q}$, it is totally ramified, and similarly if p splits, it is totally split.

Proposition 1.10. *Consider the field $F = \mathbf{Q}(\sqrt{d})$ where d is a squarefree integer. Let $p \in \mathbf{Z}$ be a rational prime. Assume first that $p > 2$, then*

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

For the prime 2, we have the following.

- 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. Write $\mathcal{O}_F = \mathbf{Z}[\theta]$. From Proposition 1.9 we see that the minimal polynomial f of θ is either $x^2 - d$ or $x^2 - x - (d-1)/4$ according as $d \equiv 2, 3 \pmod 4$ or $d \equiv 1 \pmod 4$. Hence the discriminant $\delta_{F/\mathbf{Q}}$ is either $4d$ or d, so the odd prime p ramifies if and only if $p \mid d$ (cf. [Jan96, I Theorem 7.3]). If $p \nmid d$, we have

$$\frac{\mathcal{O}_F}{p\mathcal{O}_F} \cong \frac{\mathbf{Z}[x]}{(p, f)} \cong \frac{\mathbf{F}_p[x]}{(\overline{f})},$$

where $\overline{f}$ is the reduction of f modulo p. Thus, if f splits modulo p we have $\mathcal{O}_F/p\mathcal{O}_F \cong \mathbf{F}_p \oplus \mathbf{F}_p$ by the Chinese remainder theorem; if f is irreducible modulo p we have $\mathcal{O}_F/p\mathcal{O}_F \cong \mathbf{F}_{p^2}$—the finite field with p^2 elements. In the first case p splits; in the second case, p is inert. But f splits modulo p if and only if $(d/p) = 1$, so this finishes the case when p is odd.

We turn to the case $p = 2$. We have seen that $2 \mid \delta_{F/\mathbf{Q}}$ if and only if $d \equiv 2, 3 \pmod 4$, in which case 2 ramifies. If $d \equiv 1 \pmod 4$, the minimal polynomial $f(x) = x^2 - x - (d-1)/4$ of the extension $F/\mathbf{Q}$ is irreducible modulo 2 if and only if $(d-1)/4 \equiv 1 \pmod 2$, which is equivalent to $d \equiv 5 \pmod 8$. Similarly, f splits modulo 2 if and only if $(d-1)/4 \equiv 0 \pmod 2$, which happens if and only if $d \equiv 1 \pmod 8$. □

Note that these results also give some information about the structure of the residue fields at the different prime ideals. We record this as a proposition for future reference.

Proposition 1.11. *If F is a number field and $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_F$ is a nonzero prime ideal above the prime $p \in \mathbf{Z}$, then*

$$k(\mathfrak{p}) \cong \mathbf{F}_{\operatorname{Nm} \mathfrak{p}},$$

where $k(\mathfrak{p}) := \mathcal{O}_F/\mathfrak{p}$ is the residue field of $\mathfrak{p}$.

In particular, if $F = \mathbf{Q}(\sqrt{d})$ is a quadratic number field, we have the following description of $k(\mathfrak{p})$:

- *If p ramifies or splits, then $k(\mathfrak{p}) \cong \mathbf{F}_p$.*
- *If p is inert, $k(\mathfrak{p}) \cong \mathbf{F}_{p^2}$.*

Proof. We have $k(\mathfrak{p}) \cong \mathbf{F}_{\operatorname{Nm} \mathfrak{p}}$ by the definition of the counting norm $\operatorname{Nm} \mathfrak{p}$ as the number of elements in $k(\mathfrak{p})$.

In the case when F is a quadratic number field, write $p\mathcal{O}_F = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_s^{e_s}$ for $\mathfrak{P}_j \in \operatorname{Spec} \mathcal{O}_F$. By the fundamental identity we have

$$\sum_{j=1}^{s} e_j f_j = [F : \mathbf{Q}] = 2,$$

where $f_j := [k(\mathfrak{P}_j) : \mathbf{F}_p]$ are the local degrees. We have $\mathfrak{P}_j = \mathfrak{p}$ for some j by assumption, and since the extension $F/\mathbf{Q}$ is Galois, all the local degrees are equal [Lan70, Corollary 2, p.26]. Thus we can apply the results above to deduce the following:

- If p ramifies, then $s = 1$ and $e_1 = 2$, thus $f_1 = 1$. Hence $k(\mathfrak{p})$ is a degree 1 extension of $\mathbf{F}_p$, in other words isomorphic to $\mathbf{F}_p$.
- If p splits, we get $s = 2$ and $f_j = e_j = 1$ $(j = 1, 2)$. Hence $k(\mathfrak{p}) \cong \mathbf{F}_p$.
- That p is inert means that $s = 1$ and $e_1 = 1$, thus $f_1 = 2$. In other words, $k(\mathfrak{p})$ is a degree 2 extension of $\mathbf{F}_p$. Hence $k(\mathfrak{p}) \cong \mathbf{F}_{p^2}$. □

$\delta_{\mathbf{Q}(\sqrt{d})/\mathbf{Q}}$	-3	-4	-7	-8	-11	-15
$M(\mathbf{Q}(\sqrt{d}))$	$\frac{1}{3}$	$\frac{1}{2}$	$\frac{4}{7}$	$\frac{3}{4}$	$\frac{9}{11}$	$\frac{16}{15}$

Table 1.1: Euclidean minima for the first six imaginary quadratic number fields.

The existence of a Euclidean algorithm on a number field simplifies certain K-theoretic questions; we shall make use of this in Chapter 3. In the case of imaginary quadratic number fields there are five instances for which there exists a Euclidean algorithm.

Proposition 1.12 ([Lem95, Proposition 4.2])**.** *Let $d < 0$ be a squarefree integer and consider the imaginary quadratic number field $F := \mathbf{Q}(\sqrt{d})$. Let D denote the maximum distance from a point in $\mathbf{C}$ to a lattice point of $\mathcal{O}_F$ and let $M(F) := D^2$ be the Euclidean minimum (cf. [Lem95, 3.1]). Then*

$$M(F) = \begin{cases} \dfrac{|d|+1}{4} & \text{if } d \equiv 2, 3 \pmod 4; \\ \dfrac{(|d|+1)^2}{16|d|} & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Remark 1.13. In Chapter 3, Lemma 3.1, we will essentially prove this proposition in the case when $d \not\equiv 1 \pmod 4$.

Table 1.1 shows the values of $M(\mathbf{Q}(\sqrt{d}))$ for the first six imaginary quadratic number fields, ordered by their discriminant.

Proposition 1.14 ([BT73, p.432])**.** *A number field F is Euclidean if $M(F) < 1$. Hence, by Proposition 1.12, $\mathbf{Q}(\sqrt{-d})$ is Euclidean for*

$$d \in \{1, 2, 3, 7, 11\}.$$

1.3 The Gaussian integers

We consider the degree two extension $F := \mathbf{Q}(i)$ of $\mathbf{Q}$, whose ring of integers $\mathcal{O}_F$ in F is the Gaussian integers $\mathbf{Z}[i]$ (which follows from, e.g., Proposition 1.9).

Proposition 1.15. *The ring of Gaussian integers is a principal ideal domain.*

Proof. Note that the discriminant of $\mathbf{Q}(i)/\mathbf{Q}$ is $\delta_{\mathbf{Q}(i)/\mathbf{Q}} = -4$, and since there is exactly one pair of complex conjugate embeddings of $\mathbf{Q}(i)$ into $\mathbf{C}$, the Minkowski bound for the extension becomes

$$M = \frac{2}{2^2} \cdot \frac{4}{\pi} \sqrt{|\delta_{\mathbf{Q}(i)/\mathbf{Q}}|} = \frac{4}{\pi}.$$

By the Minkowski bound theorem ([Jan96, I Theorem 13.7]), any class in the ideal class group $\mathrm{Cl}(\mathbf{Z}[i])$ is represented by a nonzero integral ideal $\mathfrak{a}$ whose counting norm $\mathrm{Nm}(\mathfrak{a})$ is bounded by M. Since $M < 2$, we must have that $\mathrm{Nm}(\mathfrak{a}) = 1$, i.e., $\mathfrak{a} = \mathbf{Z}[i]$, and thus the ideal class group is trivial. □

Remark 1.16. The above result follows of course also from the fact that $\mathbf{Z}[i]$ is Euclidean.

Remark 1.17. The field $\mathbf{Q}(i)$ is one of the in total nine imaginary quadratic number fields with class number one; the other ones are $\mathbf{Q}(\sqrt{-d})$ for

$$d \in \{2, 3, 7, 11, 19, 43, 67, 167\}.$$

Proposition 1.18. *We have $\mathbf{Z}[i]^\times = \mu(\mathbf{Q}(i)) = \mu_4$.*

Proof. This follows directly from Dirichlet's unit theorem ([Jan96, I Theorem 13.12]):

$$\mathbf{Z}[i]^\times \cong \mu(\mathbf{Q}(i)) \times \mathbf{Z}^{r+c-1} = \mu(\mathbf{Q}(i)),$$

where r and c denotes respectively the number of real embeddings of $\mathbf{Q}(i)$, and the number of complex conjugate pairs of embeddings. □

To introduce some geometry to the picture, let us take a look at the fibers over the closed points of $\operatorname{Spec}\mathbf{Z}$ of the morphism $X := \operatorname{Spec}\mathbf{Z}[i] \to \operatorname{Spec}\mathbf{Z}$ induced by the inclusion $\mathbf{Z} \hookrightarrow \mathbf{Z}[i]$. Let p be a rational prime, then the fiber

$$\begin{aligned} X_{(p)} &= \operatorname{Spec}\mathbf{Z}[i] \times_{\operatorname{Spec}\mathbf{Z}} \operatorname{Spec}\mathbf{F}_p \\ &= \operatorname{Spec}(\mathbf{Z}[x]/(x^2+1) \otimes_{\mathbf{Z}} \mathbf{F}_p) \\ &= \operatorname{Spec}(\mathbf{F}_p[x]/(x^2+1)). \end{aligned}$$

Thus we see that determining the fibers $X_{(p)}$ is the same as determining the splitting of the prime p in the extension $\mathbf{Q}(i)/\mathbf{Q}$. From Proposition 1.10 we have the following.

1. The prime 2 ramifies. Here we can also see at once that $\mathbf{F}_2[x]/(x^2+1) = \mathbf{F}_2[x]/(x+1)^2$, and by the correspondence $x \mapsto i$ we get that $2\mathbf{Z}[i] = (2, i+1)^2 = (i+1)^2$. Geometrically, the fiber is a nonreduced one-point scheme.

2. Assume $p \equiv 1 \pmod 4$. By the first supplementary law of quadratic reciprocity we then obtain
$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1.$$
Hence p splits, and the fiber consists of two points.

3. If $p \equiv 3 \pmod 4$ then $(-1/p) = -1$, hence p is inert in the extension and the fiber consists of one closed point.

Point 2 above illustrates a classical theorem of Fermat, namely that a rational prime p is the sum of two squares if and only if $p \equiv 1 \pmod 4$. Indeed, let $\operatorname{Nm} := \operatorname{Nm}_{\mathbf{Q}(i)/\mathbf{Q}} : \mathbf{Z}[i] \to \mathbf{Z}$ be the norm map $a + ib \mapsto a^2 + b^2$, so that p is a sum of two squares if and only if p lies in the image of the norm map. If p splits, i.e., $p = \alpha\beta$ in $\mathbf{Z}[i]$, then $\operatorname{Nm}(p) = p^2 = \operatorname{Nm}(\alpha)\operatorname{Nm}(\beta)$, and since we assume neither α nor β is a unit we must have $p = \operatorname{Nm}(\alpha) = \operatorname{Nm}(\beta)$. Hence p is a sum of two squares. But by the above discussion, p splits if and only if $p \equiv 1 \pmod 4$.

Let us summarize the results above.

Proposition 1.19. *The nonzero prime ideals of* $\mathbf{Z}[i]$ *are of the following forms:*

- $(1+i)$ *lying above* 2.
- $(a+ib)$*, which lies above the prime* $p \equiv 1 \pmod 4$ *such that* $p = a^2 + b^2$.
- (p)*, for* p *a rational prime congruent to* 3 *modulo* 4.

By Proposition 1.11 we obtain the following result:

Proposition 1.20. *Let* $\mathfrak{p}$ *be a nonzero prime ideal of* $\mathbf{Z}[i]$ *above the prime* $p \in \mathbf{Z}$. *Then the residue field* $k(\mathfrak{p}) := \mathbf{Z}[i]/\mathfrak{p}$ *is of the following form:*

$$k(\mathfrak{p}) \cong \mathbf{F}_{\operatorname{Nm}\mathfrak{p}} = \begin{cases} \mathbf{F}_p & \text{if } p = 2 \text{ or } p \equiv 1 \pmod 4; \\ \mathbf{F}_{p^2} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Figure 1.1 depicts the analogy with Riemann surfaces: One thinks of the morphism

$$\operatorname{Spec}\mathbf{Z}[i] \longrightarrow \operatorname{Spec}\mathbf{Z}$$

as a two sheeted covering, ramified only above (2). In general, given a number field $F \neq \mathbf{Q}$, let δ_F denote its discriminant. By Minkowski's theorem [Jan96, I Theorem 13.9], the extension

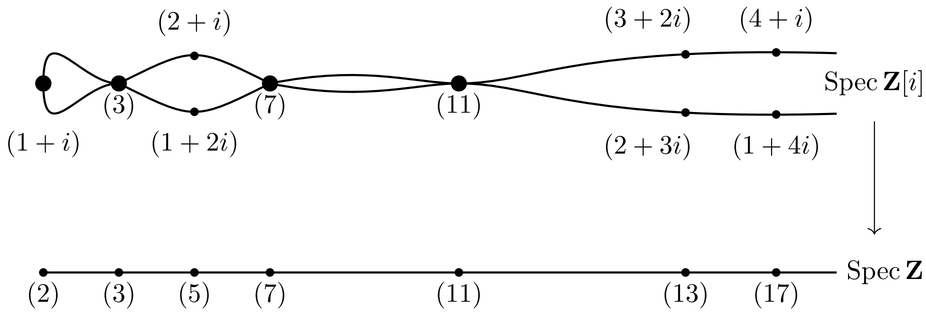


Figure 1.1: The closed points of Spec $\mathbf{Z}[i]$, viewed as a two-sheeted covering of Spec $\mathbf{Z}$.

$F/\mathbf{Q}$ is ramified, and the ramified prime ideals of $\mathcal{O}_F$ are exactly those lying above a rational prime p dividing δ_F. Let S be the set consisting of the infinite places of F together with the finite places corresponding to the ramified primes, and let

$$\mathcal{O}_{F,S} := \{x \in F : \mathrm{ord}_v(x) \geq 0 \text{ for all } v \notin S\}$$

denote the ring of S-integers. Then

$$\operatorname{Spec} \mathcal{O}_{F,S} = \operatorname{Spec}(\mathcal{O}_F[1/\delta_F]) \longrightarrow \operatorname{Spec} \mathbf{Z}$$

is a finite étale covering. The fact that there are no unramified algebraic extensions of $\mathbf{Q}$ implies that Spec $\mathbf{Z}$ is simply connected in the sense of étale fundamental groups: $\pi_1^{\text{ét}}(\operatorname{Spec} \mathbf{Z}) = 0$ [Mor12b, p.36]. In this language, class field theory describes the maximal abelian quotient of the étale fundamental group of the arithmetic scheme Spec $\mathcal{O}_F$ in terms of the arithmetic of the number field F itself.

1.3.1 Local structure

In this subsection we will make use of a few lemmas whose statement we defer until Section 1.5.1 after general notation has been introduced. The reader may therefore skip this at the first reading and rather return when needed.

Later on we will need a few results on the structure of the local field $\mathbf{Q}(i)_v$ for v a place of $\mathbf{Q}(i)$—in particular the place corresponding to the prime $1+i$. First of all, recall that if v is a finite place of $\mathbf{Q}(i)$ lying above a rational prime p, then $\mathbf{Q}(i)_v = \mathbf{Q}_p(i)$ (see [Gra03, p.13]). In particular, $\mathbf{Q}(i)_{(1+i)} = \mathbf{Q}_2(i)$ and thus $\mathbf{Z}[i]_{(1+i)} = \mathbf{Z}_2[i]$. Let $U_{1+i} := \mathbf{Z}_2[i]^\times$, and let $U_{1+i}^n := 1 + (1+i)^n \mathbf{Z}_2[i]$ denote the higher unit groups (cf. Definition 1.28).

Lemma 1.21. *If α is a Gaussian integer relatively prime to $1+i$, then α has a primary associate. In other words, α becomes primary after multiplication by a suitable power of i.*

Proof. Since we assume α is coprime to $1+i$, $\overline{\alpha}$ is a unit in $\mathbf{Z}[i]/(1+i)^3$. Now

$$\#(\mathbf{Z}[i]/(1+i)^3)^\times = \varphi((1+i)^3) = \mathrm{Nm}(1+i)^2(\mathrm{Nm}(1+i) - 1) = 4,$$

where φ is the Euler totient function on $\mathbf{Z}[i]$. Thus there are 4 units, and we can take μ_4 as a system of representatives for $(\mathbf{Z}[i]/(1+i)^3)^\times$ since the powers of i are different modulo $(1+i)^3$. Hence $\overline{\alpha} = \overline{i^k}$ for some $k \in \{0,1,2,3\}$, and the statement follows. □

Proposition 1.22. *We have $\mathbf{Q}_2(i)^\times \cong (1+i)^{\mathbf{Z}} \oplus \mu_4 \oplus U_{1+i}^3$. Consequently $U_{1+i} \cong \mu_4 \oplus U_{1+i}^3$.*

Proof. Let v denote the place corresponding to $(1+i)$. Note that any element $\alpha \in U_v$ can be written as a power series

$$\alpha = a_0 + a_1(1+i) + a_2(1+i)^2 + \cdots$$

where $a_n \in \{0, 1\}$ and $a_0 \neq 0$. Hence $U_v = U_v^1$.

By Proposition 1.35 it is enough to show that $U_v^1 \cong \mu_4 \oplus U_v^3$. Since

$$\frac{\mathbf{Z}_2[i]}{(1+i)^3\mathbf{Z}_2[i]} \cong \frac{\mathbf{Z}[i]}{(1+i)^3},$$

the result of Lemma 1.21 holds also for U_v^1, hence any $\alpha \in U_v^1$ can be written as

$$\alpha = i^{4-k}(i^k\alpha) \in \mu_4 \oplus U_v^3$$

for some k. Since the powers of i are different modulo $(1+i)^3$ we have $U_v^3 \cap \mu_4 = 1$, yielding $U_v^1 \cong \mu_4 \oplus U_v^3$. □

Proposition 1.23. *Let $(U_{1+i})^4$ be the group of fourth powers in $\mathbf{Z}_2[i]^\times$. Then*

1. *the group $U_{1+i}/(U_{1+i})^4$ has order 64;*
2. *$(U_{1+i})^4 = U_{1+i}^7$;*
3. *$U_{1+i}/(U_{1+i})^4 \cong \mu_4 \oplus \langle 3+2i \rangle \oplus \langle 5 \rangle$.*

Proof. To ease the notation let v denote the place corresponding to $(1+i)$ and put $\pi := 1+i$.

1. Since $4 = -\pi^4$ we have $\mathrm{ord}_v(4) = 4$, so Lemma 1.34 yields

$$(U_v : (U_v)^4) = \frac{\#\mu_4(\mathbf{Q}_2(i))}{|4|_v} = \frac{4}{\mathrm{Nm}(\pi)^{-\mathrm{ord}_v(4)}} = 2^6.$$

2. To show that $(U_v)^4 \subseteq U_v^7$, take an $\alpha \in U_v$. Note that by the proof of Proposition 1.22, we may assume $i^k\alpha$ is primary for some $k \in \{0, 1, 2, 3\}$, say

$$i^k\alpha = 1 + \pi^3\beta$$

for some $\beta \in \mathbf{Z}_2[i]$. Then

$$\begin{aligned} \alpha^4 = (i^k\alpha)^4 &= 1 + 4\beta\pi^3 + 6\beta^2\pi^6 + 4\beta^3\pi^9 + \beta^4\pi^{12} \\ &\equiv 1 + 4\beta\pi^3 + 6\beta^2\pi^6 \pmod{\pi^7} \end{aligned}$$

Writing $4 = -\pi^4$ and $2 = (-i)\pi^2$ we get

$$\alpha^4 \equiv 1 - \beta\pi^7 - 3i\beta^2\pi^8 \equiv 1 \pmod{\pi^7}.$$

Hence $(U_v)^4 \subseteq U_v^7$. Since $(U_v : U_v^7) = q_v^6(q_v - 1) = 2^6$ by Lemma 1.33 below (and the notations used there), we have by 1 that $(U_v : U_v^7) = (U_v : (U_v)^4)$, hence $(U_v)^4 = U_v^7$.

3. Again by Lemma 1.33 we have

$$\frac{U_v^1}{U_v^7} \cong \left(\frac{\mathbf{Z}_2[i]}{\pi^7\mathbf{Z}_2[i]}\right)^\times \cong \left(\frac{\mathbf{Z}[i]}{\pi^7\mathbf{Z}[i]}\right)^\times.$$

Choosing $3+2i \in U_v^3$, $5 \in U_v^4$ and $i \in U_v$ as generators for $(\mathbf{Z}[i]/\pi^7)^\times$ yields the result. □

1.4 The Eisenstein integers

Now we turn to the case $F = \mathbf{Q}(\sqrt{-3})$. Since $-3 \equiv 1 \pmod 4$, the ring of integers $\mathcal{O}_F$ equals $\mathbf{Z}[\omega]$, where $\omega := (-1+\sqrt{-3})/2$. The elements of $\mathbf{Z}[\omega]$ are called the *Eisenstein integers*. Note that ω is a primitive third root of unity, and that $\mathbf{Z}[\omega] = \mathbf{Z}[\zeta_6]$, where ζ_6 is a primitive sixth root of unity. The discriminant of the extension $\mathbf{Q}(\sqrt{-3})/\mathbf{Q}$ equals -3, so the same reasoning as in Proposition 1.15 shows that $\mathbf{Z}[\omega]$ is a principal ideal domain.

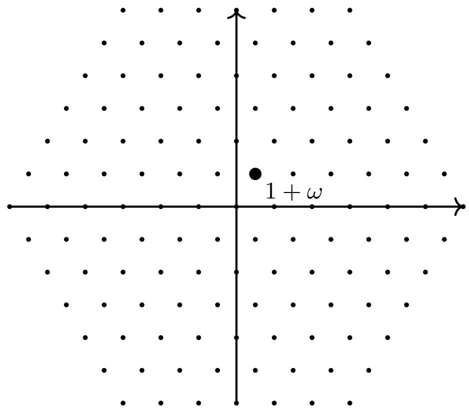


Figure 1.2: Part of the lattice of integers in $\mathbf{Q}(\sqrt{-3})$.

Proposition 1.24. *The ring of Eisenstein integers is a principal ideal domain, and the units are*

$$\mathbf{Z}[\omega]^\times = \mu_6 = \{\pm 1, \pm\omega, \pm\omega^2\}.$$

Proposition 1.25. *The norm of an Eisenstein integer $a + b\omega \in \mathbf{Z}[\omega]$ is given by* $\mathrm{Nm}(a + b\omega) = a^2 - ab + b^2$.

Proof. Let $\alpha := a + b\omega \in \mathbf{Z}[\omega]$ be an Eisenstein integer. If $b = 0$ we have $\mathrm{Nm}(\alpha) = \mathrm{Nm}(a) = a^2$, so the statement is true in this case. If $b \neq 0$, a straightforward computation shows that the minimal polynomial over $\mathbf{Q}$ of α is

$$x^2 - (2a - b)x + (a^2 - ab + b^2),$$

and the norm $\mathrm{Nm}(\alpha)$ is the constant term of the minimal polynomial. □

Proposition 1.26. *Consider the extension $\mathbf{Q}(\sqrt{-3})/\mathbf{Q}$. If $p \in \mathbf{Z}$ is a rational prime, then*

- *p ramifies $\iff$ $p = 3$;*
- *p splits $\iff$ $p \equiv 1 \pmod 3$;*
- *p is inert $\iff$ $p \equiv 2 \pmod 3$.*

Thus, the nonzero prime ideals of $\mathbf{Z}[\omega]$ are of the following forms:

- *$(2 + \omega)$ lying above $3 \in \mathbf{Z}$;*
- *$(a + b\omega)$ lying above the rational prime $p \equiv 1 \pmod 3$ such that $p = a^2 - ab + b^2$;*
- *(p), which lies above the prime $p \in \mathbf{Z}$ such that $p \equiv 2 \pmod 3$.*

Hence the Diophantine equation $x^2 - xy + y^2 = p$ has a solution if and only if $p = 3$ or $p \equiv 1 \pmod 3$.

Proof. By Proposition 1.10, only 3 ramifies. By Proposition 1.25 we have

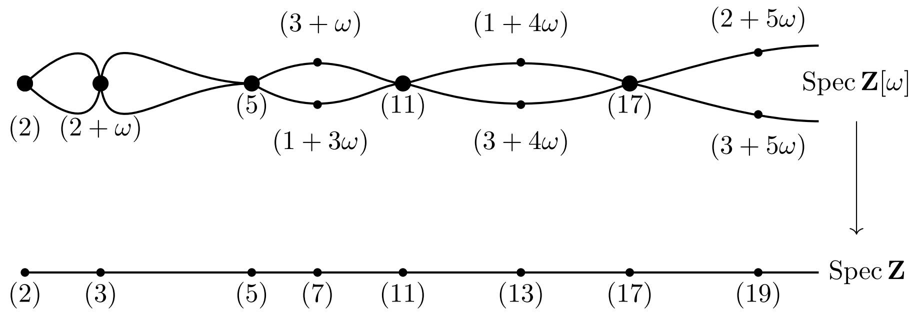
$$\mathrm{Nm}(2 + \omega) = 3,$$

so the ideal $(2 + \omega)$ lies above (3), hence $3\mathbf{Z}[\omega] = (2 + \omega)^2$.

Furthermore, we know by Proposition 1.10 that the prime 2 is inert. To show the rest of the statement for $p \neq 2$, all we need is quadratic reciprocity. By Proposition 1.10, a rational odd prime $p \neq 3$ splits in the extension if and only if $(-3/p) = 1$. By multiplicativity of Legendre symbols,

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right).$$

We consider two cases.



- If $p \equiv 1 \pmod 4$, $(3/p) = (p/3)$ by quadratic reciprocity. Hence
$$\left(\frac{-3}{p}\right) \equiv (-1)^{\frac{p-1}{2}} p \equiv p \pmod 3,$$
i.e., $(-3/p) = 1$ if and only if $p \equiv 1 \pmod 3$.
- If $p \equiv 3 \pmod 4$ we have $(3/p) = -(p/3)$, so
$$\left(\frac{-3}{p}\right) \equiv -(-1)^{\frac{p-1}{2}} p \equiv p \pmod 3,$$
so also in this case we get that $(-3/p) = 1$ if and only if $p \equiv 1 \pmod 3$.

Thus p splits if and only if $p \equiv 1 \pmod 3$. □

Proposition 1.27. *Let $\mathfrak{p} \in \operatorname{Spec} \mathbf{Z}[\omega]$ be a nonzero prime ideal. Then the residue field $k(\mathfrak{p})$ is given by*
$$k(\mathfrak{p}) \cong \begin{cases} \mathbf{F}_p & \text{if } p = 3 \text{ or } p \equiv 1 \pmod 3; \\ \mathbf{F}_{p^2} & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

1.5 Class field theory

We state some of the main results of local and global class field theory. From here we introduce the notion of symbols over number fields, which serves as one of the first links between number theory and algebraic K-theory. This section will also help to fix notations, of which we mostly follow [Gra03].

Let F be a global number field, and let Pl_F denote the set of places of F. By Ostrowski's theorem [Gra03, I Theorem 1.2], Pl_F decomposes as a disjoint union
$$\mathrm{Pl}_F = \mathrm{Pl}_0 \cup \mathrm{Pl}_\infty$$
of finite and infinite places, respectively. Occasionally we will be interested in considering only noncomplex places of F, the set of which will be denoted by $\mathrm{Pl}_F^{\mathrm{nc}}$.

Definition 1.28. Let v be a place of F. We will denote by:

- F_v the completion of F at v, with valuation ring $\mathcal{O}_v$;
- π_v a uniformizer of F_v, i.e., a generator of the maximal ideal $\mathfrak{p}_v$ of $\mathcal{O}_v$ (for v finite);
- $k(v) := \mathcal{O}_v/\mathfrak{p}_v$ the residue field (for v finite);
- $q_v := \#k(v)$ (for v finite);
- $U_v := \mathcal{O}_v^\times$ the unit group, where we set $U_v := \mathbf{R}_{>0}$ when v is infinite real;
- $U_v^n := 1 + \mathfrak{p}_v^n$ $(n \geq 1)$ the higher unit groups (for v finite);

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

For each place $v \in \mathrm{Pl}_F$ we shall make use of the corresponding valuation on $F^\times$. It is clear that when v is a finite place, the corresponding valuation is just the $\mathfrak{p}_v$-adic valuation. However, it is convenient to also have a similar notion when v is infinite:

Definition 1.29. Let $v \in \mathrm{Pl}$ be a place of F. We denote the corresponding valuation by ord_v, and it takes the following forms:

- If $v \in \mathrm{Pl}_0$ is a finite place, $\mathrm{ord}_v : F^\times \to \mathbf{Z}$ is the $\mathfrak{p}_v$-adic valuation.
- If v is an infinite real place, the valuation $\mathrm{ord}_v : F^\times \to \mathbf{Z}/2$ is defined by:

$$\mathrm{ord}_v(x) := \begin{cases} 0, & i_v(x) > 0 \\ 1, & i_v(x) < 0. \end{cases}$$

- If v is an infinite complex place, we set $\mathrm{ord}_v := 0$.

1.5.1 On the higher unit groups

The higher unit groups U_v^n of the local field F_v form a filtration

$$U_v \supseteq U_v^1 \supseteq \cdots \supseteq U_v^n \supseteq \cdots$$

of the unit group U_v, whose filtration coefficients U_v^n/U_v^{n+1} are all finite. They allow us to express U_v as the limit $U_v = \varprojlim_n U_v/U_v^n$, hence U_v is a profinite group.

Proposition 1.30. *The group U_v contains the $(q_v - 1)$-roots of unity μ_{q_v-1}.*

Proof. By the general Fermat's little theorem, the polynomial

$$f(x) := x^{q_v-1} - 1$$

when reduced modulo $\mathfrak{p}_v$ has $q_v - 1$ distinct roots in $k(v)^\times \cong \mu_{q_v-1}$. By Hensel's lemma, these roots lift uniquely to $q_v - 1$ distinct roots of f in U_v. □

Remark 1.31. The map $k(v)^\times \hookrightarrow U_v$ which sends an element to its unique lift in U_v provided by Hensel's lemma is called the *Teichmüller lift.*

Lemma 1.32 ([Ser79, Proposition 6, p.66])**.** *For any finite place $v \in \mathrm{Pl}_F$ we have a canonical isomorphism $U_v/U_v^1 \cong \mu_{q_v-1} \cong k(v)^\times$, and for each $n \geq 1$ a noncanonical isomorphism $U_v^n/U_v^{n+1} \cong k(v)$.*

Lemma 1.33. *Given $v \in \mathrm{Pl}_0$ and any $n \geq 1$, let φ be the generalized Euler function, where $\varphi(\mathfrak{p}_v^n) = q_v^{n-1}(q_v - 1)$. Then $(U_v : U_v^n) = \varphi(\mathfrak{p}_v^n)$, and*

$$U_v/U_v^n \cong (\mathcal{O}_v/\mathfrak{p}_v^n)^\times.$$

Proof. Note that we have exact sequences

$$1 \longrightarrow U_v^n/U_v^{n+1} \longrightarrow U_v/U_v^{n+1} \longrightarrow U_v/U_v^n \longrightarrow 1$$

for all n, i.e., $(U_v : U_v^{n+1}) = (U_v : U_v^n)(U_v^n : U_v^{n+1})$. When $n = 1$, this reads $(U_v : U_v^2) = q_v(q_v - 1)$ by Lemma 1.32; the general case follows by induction.

The second statement follows from the fact that the canonical surjective homomorphism

$$\begin{aligned} U_v &\longrightarrow (\mathcal{O}_v/\mathfrak{p}_v^n)^\times \\ u &\longmapsto u \pmod{\mathfrak{p}_v^n} \end{aligned}$$

has kernel U_v^n. □

Lemma 1.34 ([Lan70, Proposition 6, p.47]). *Let v be a finite place of F. For any $n \geq 1$, let $(U_v)^n$ denote the group of n-th powers in U_v. Then*

$$(U_v : (U_v)^n) = \frac{\#\mu_n(F_v)}{|n|_v},$$

where $\mu_n(F_v)$ is the group of n-th roots of unity contained in F_v, and $|\cdot|_v$ is the v-adic absolute value on F_v.

Proposition 1.35. *For v a finite place of F, there is a decomposition*

$$F_v^\times \cong \pi_v^{\mathbf{Z}} \oplus \mu_{q_v-1} \oplus U_v^1.$$

Proof. Any $x \in F_v^\times$ can be written $x = \pi_v^{\mathrm{ord}_v(x)} u$ with $u \in U_v$. Since $U_v/U_v^1 \cong \mu_{q_v-1}$ we have an exact sequence

$$1 \longrightarrow U_v^1 \longrightarrow U_v \longrightarrow \mu_{q_v-1} \longrightarrow 1,$$

which splits by the Teichmüller lift $\mu_{q_v-1} \cong k(v)^\times \hookrightarrow U_v$. $\square$

Example 1.36. Let us show that any element of $U_p^1 = 1 + p\mathbf{Z}_p$ is in fact a square whenever p is an odd rational prime. Indeed, for any $x \in 1 + p\mathbf{Z}_p$, write $x = 1 + py$ where $y \in \mathbf{Z}_p$. Then we have the series expansion

$$x^{1/2} = (1+py)^{1/2} = 1 + \frac{y}{2}p - \frac{y^2}{8}p^2 + \frac{y^3}{16}p^3 - \cdots$$

which converges p-adically. The denominators are all powers of 2, hence invertible in $\mathbf{Z}_p$, so the series converges to an element in $1 + p\mathbf{Z}_p$. Thus x has a square root in $1 + p\mathbf{Z}_p$. From this and Proposition 1.35 above we can conclude for example that $\mathbf{Z}_p^\times$ has only one subgroup of index 2, namely $\mu_{p-1}^2 \oplus (1 + p\mathbf{Z}_p) = (\mathbf{Z}_p^\times)^2$.

1.5.2 Frobenius

Recall that if L/F is an extension of number fields and w a place of L above a finite place v of F, there is a canonical isomorphism $\mathrm{Gal}(L_w/F_v) \cong D_w$ [Mil13a, Proposition 8.10] where D_w is the *decomposition group* of w:

$$D_w := \{\sigma \in \mathrm{Gal}(L/F) : \sigma w = w\},$$

where the action of $\mathrm{Gal}(L/F)$ on Pl_L is defined by

$$|x|_{\sigma w'} := |\sigma^{-1}(x)|_{w'}$$

for any $w' \in \mathrm{Pl}_L$. There is a surjective homomorphism $D_w \to \mathrm{Gal}(k(w)/k(v))$ defined by $\sigma \mapsto \overline{\sigma}$, where

$$\overline{\sigma}(y + \mathfrak{p}_w) := \sigma(y) + \mathfrak{p}_w.$$

Its kernel is called the *inertia group* of w, and is denoted by I_w. If L_w/F_v is unramified, the inertia group is trivial and thus we have an isomorphism $\mathrm{Gal}(L_w/F_v) \cong \mathrm{Gal}(k(w)/k(v))$ in this case. Now $\mathrm{Gal}(k(w)/k(v))$ is a finite cyclic group, with a canonical generator which sends $\overline{y} \in k(w)$ to $\overline{y}^{q_v}$.

Definition 1.37. Suppose L_w/F_v is an unramified extension of local fields. The image in $\mathrm{Gal}(L_w/F_v)$ of the canonical generator of $\mathrm{Gal}(k(w)/k(v))$ under the isomorphism $\mathrm{Gal}(L_w/F_v) \cong \mathrm{Gal}(k(w)/k(v))$ is called the *local Frobenius*, and is denoted by

$$(L_w/F_v).$$

The image of (L_w/F_v) in $\mathrm{Gal}(L/F)$ under the isomorphism $\mathrm{Gal}(L_w/F_v) \cong D_w \subseteq \mathrm{Gal}(L/F)$ is called the *global Frobenius at w*, and is denoted by

$$\left(\frac{L/F}{w}\right).$$

Remark 1.38. If w and w' are two places above v, then the global Frobenius at w and w' are conjugate to each other [Jan96, p.126]. Hence they are equal if L/F is an abelian extension, i.e., if $\mathrm{Gal}(L/F)$ is abelian. In this case we will therefore denote by $\left(\frac{L/F}{v}\right)$ the Frobenius at any place above v.

1.5.3 Local and global class field theory

All the number theoretic symbols we shall consider in Section 1.6 are offspring of the *local reciprocity map*, which will be introduced shortly in the discussion on local class field theory (see Theorem 1.41). The treatment of global class field theory will be idèlic, i.e., we define the global reciprocity map on the idèle group of the global field in consideration, as opposed to the more classical ideal-theoretic definition. The idèle group, first introduced by Chevalley [Mil13b, p.viii], is an object attached to a global field allowing for a unified treatment of the different embeddings of the field into its completion at all places, including the infinite ones. We start off by a brief introduction to the idèles before we move on to the local and global reciprocity maps.

The *restricted product* $\coprod_{i\in I} G_i$ 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 $g_i \in K_i$ for almost all i, where K_i is some fixed compact subgroup of G_i. The restricted product is then a locally compact group, and we provide it with a topology whose basis elements are of the form $\prod_i A_i$ where $A_i \subseteq G_i$ is open in G_i for all i and $A_i = K_i$ for almost all i.

Definition 1.39. The *idèle group* of the number field F is the restricted product of the groups $F_v^\times$ with respect to the compact subgroups U_v:

$$\mathbf{J}_F := \coprod_{v\in \mathrm{Pl}_F} F_v^\times = \{(x_v)_{v\in\mathrm{Pl}_F} : x_v \in F_v^\times, x_v \in U_v \text{ for almost all } v\}.$$

An element $\mathbf{x}$ of $\mathbf{J}_F$ is called an *idèle.* We define the *idèle class group* C_F as

$$C_F := \mathbf{J}_F / i(F^\times),$$

where $i : F^\times \to \prod_{v\in\mathrm{Pl}} F_v^\times$ is the injective map sending $x \in F^\times$ to $(i_v(x))_v$.

We sometimes abbreviate $\mathbf{J}_F$ and C_F to $\mathbf{J}$ and C. By abuse of notation we may also write simply $F^\times$ for the image $i(F^\times)$ when it is clear from context that we consider the subset of $\mathbf{J}_F$ and not of F.

As in the general case mentioned above, the idèles $\mathbf{J}_F$ are endowed with a topology whose basis elements are of the form

$$\prod_{v\in\mathrm{Pl}} V_v,$$

where V_v is open in $F_v^\times$ for all v and $V_v = U_v$ for almost all v. With this topology, the image of $F^\times$ in $\mathbf{J}$ under the diagonal embedding i becomes discrete.

Remark 1.40. Alternatively, one may define $\mathbf{J}_F$ as the colimit

$$\mathbf{J}_F = \varinjlim_{S\subseteq \mathrm{Pl}_F} \mathbf{J}_F(S),$$

where S varies over all finite subsets of Pl_F containing the infinite places, and

$$\mathbf{J}_F(S) := \prod_{v\in S} F_v^\times \times \prod_{v\notin S} U_v.$$

Yet another definition is to put $\mathbf{J}_F := \mathbf{A}_F^\times$, where $\mathbf{A}_F$ is the adèle ring of F. However, due to the multiplicative nature of class field theory, we shall not need to introduce adèles for our purposes.

For any idèle $\mathbf{x} = (x_v)_v \in \mathbf{J}$, define the *volume* of $\mathbf{x}$ as

$$|\mathbf{x}| := \prod_v |x_v|_v,$$

where $|\cdot|_v$ is the absolute value on F_v. The volume map $|\cdot| : \mathbf{J}_F \to \mathbf{R}_{>0}$ is then continuous. If we let $\mathbf{J}^1$ denote the kernel of the volume map, i.e., $\mathbf{J}^1 := \{\mathbf{x} \in \mathbf{J} : |\mathbf{x}| = 1\}$, then $F^\times$ is contained in $\mathbf{J}^1$ by the product formula for absolute values [Jan96, II Theorem 6.4] and the quotient $\mathbf{J}^1/F^\times$ is compact [Lan70, Theorem 4, p.142]. This compactness result is an equivalent formulation of the finiteness of the ideal class group and Dirichlet's unit theorem.

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

Theorem 1.41 (Local Reciprocity Law [Gra03, II Theorem 1.4])**.** *There exists a unique canonical homomorphism*

$$(-, L_w/F_v) : F_v^\times \longrightarrow \mathrm{Gal}(L_w/F_v),$$

called the local reciprocity map*, or the* local Artin map*, satisfying the following properties.*

1. *The kernel of $(-, L_w/F_v)$ is equal to the norm group*

$$\mathrm{Nm}_{L_w/F_v}(L_w^\times) = \{\mathrm{Nm}_{L_w/F_v}(x) : x \in L_w^\times\},$$

and we have an exact sequence

$$1 \longrightarrow \mathrm{Nm}_{L_w/F_v}(L_w^\times) \longrightarrow F_v^\times \xrightarrow{(-,L_w/F_v)} \mathrm{Gal}(L_w/F_v) \longrightarrow 1.$$

2. *If L_w/F_v is unramified, then*

$$(x, L_w/F_v) = (L_w/F_v)^{\mathrm{ord}_v(x)}$$

for all $x \in F_v^\times$.

3. *The image of the unit group U_v under $(-, L_w/F_v)$ is equal to the inertia group I_w, and we have the exact sequence*

$$1 \longrightarrow \mathrm{Nm}_{L_w/F_v}(U_w) \longrightarrow U_v \longrightarrow I_w \longrightarrow 1.$$

Theorem 1.42 ([Gra03, II Theorem 1.5])**.** *For any subgroup N of $F_v^\times$ of finite index there exists a finite abelian extension M of F_v such that* $\mathrm{Nm}_{M/F_v}(M^\times) = N$*. The map $M \mapsto \mathrm{Nm}_{M/F_v}(M^\times)$ is a bijection between the set of finite abelian extensions of F_v and subgroups of F_v of finite index. This bijection has the following properties, where the field extensions M_1, M_2 correspond respectively to the groups N_1 and N_2:*

1. *$M_1 \subseteq M_2$ if and only if $N_1 \supseteq N_2$;*
2. *M_1M_2 corresponds to $N_1 \cap N_2$;*
3. *$M_1 \cap M_2$ corresponds to N_1N_2;*
4. *if $M_1 \subseteq M_2$ then* $\mathrm{Gal}(M_2/M_1) \cong N_1/N_2$.

Example 1.43 ([Mil13b, 1.6, p.22], [Gra03, II Remark 1.4.6])**.** Suppose $F = \mathbf{Q}$, $L = \mathbf{Q}(i)$, and let v be the infinite real place of F, so that $F_v = \mathbf{R}$. If w is a place of L above v, then $L_w = \mathbf{C}$. The local reciprocity map $(-, L_w/F_v) = (-, \mathbf{C}/\mathbf{R})$ is then given by

$$(x, \mathbf{C}/\mathbf{R}) = c^{\mathrm{ord}_v(x)}$$

for $x \in \mathbf{R}^\times$, where $c \in \mathrm{Gal}(\mathbf{C}/\mathbf{R})$ is complex conjugation. Note that

$$\mathrm{Nm}_{\mathbf{C}/\mathbf{R}}(\mathbf{C}^\times) = \mathbf{R}_{>0} = \ker(-, \mathbf{C}/\mathbf{R})$$

(remember Definition 1.29). Finally, any subgroup N of $\mathbf{R}^\times$ of finite index is equal to either $\mathbf{R}^\times$ or $\mathbf{R}_{>0}$. Indeed, N contains $\mathbf{R}^{\times n}$ for some n, and by the intermediate value theorem one has $\mathbf{R}^{\times n} = \mathbf{R}^\times$ if n is odd; $\mathbf{R}^{\times n} = \mathbf{R}_{>0}$ if n is even.

The local compactness of the idèle group makes it possible to define a *global reciprocity map* whose components are the local reciprocity maps:

Definition 1.44. The *global reciprocity map*—or *global Artin map*—is defined for the extension L/F as the map

$$\begin{aligned}\rho_{L/F} : \mathbf{J}_F &\longrightarrow \mathrm{Gal}(L/F)\\ \mathbf{x} = (x_v)_v &\longmapsto \prod_{v \in \mathrm{Pl}_F} \left(\frac{x_v, L/F}{v}\right),\end{aligned}$$

where $\left(\frac{x_v, L/F}{v}\right)$ is the image of $(x_v, L_v/F_v) \in \mathrm{Gal}(L_v/F_v)$ in $\mathrm{Gal}(L/F)$ under the isomorphism $\mathrm{Gal}(L_v/F_v) \cong D_v \subseteq \mathrm{Gal}(L/F)$.

Note that for an idèle $(x_v)_v \in \mathbf{J}$, since $x_v \in U_v$ for almost all v and only finitely many places v are ramified in L/F, property 2 of Theorem 1.41 tells us that $\left(\frac{x_v, L/F}{v}\right) = 1$ for almost all v, so $\rho_{L/F}$ is well defined.

Definition 1.45. Given any place $v \in \mathrm{Pl}_F$, the *Hasse symbols* $\left(\frac{-, L/F}{v}\right)$ are defined on $F^\times$ as:

$$\begin{aligned}\left(\frac{-, L/F}{v}\right) : F^\times &\longrightarrow \mathrm{Gal}(L/F)\\ x &\longmapsto \left(\frac{i_v(x), L/F}{v}\right).\end{aligned}$$

The following theorem—which states in terms of Hasse symbols that the diagonal embedding $i(F^\times)$ of $F^\times$ in $\mathbf{J}_F$ is contained in the kernel of the global reciprocity map—is one of the main results of class field theory, and is considered as the generalization of the quadratic reciprocity law of Gauss to arbitrary abelian extensions of number fields. This constitutes a partial solution to Hilbert's ninth problem.

Theorem 1.46 ([Gra03, II Theorem 3.4.1])**.** *Let L/F be a finite abelian extension of number fields. For any $x \in F^\times$, the following product formula holds:*

$$\prod_{v \in \mathrm{Pl}_F} \left(\frac{x, L/F}{v}\right) = 1.$$

Example 1.47 ([Gra03, II Example 3.4.2])**.** We calculate some Hasse symbols and illustrate how Gauss' quadratic reciprocity law is obtained from the product formula. Let p be an odd prime number and take $F = \mathbf{Q}$. We consider the extension $L = \mathbf{Q}(\sqrt{p^*})$ where $p^* := (-1)^{(p-1)/2}p$. Write $\mathrm{Gal}(L/\mathbf{Q}) = \{\pm 1\}$. We shall compute the Hasse symbols

$$\left(\frac{-1, L/\mathbf{Q}}{v}\right) \text{ and } \left(\frac{q, L/\mathbf{Q}}{v}\right),$$

where q is a rational prime and v runs through all places of $\mathbf{Q}$. Now there is exactly one archimedean place of $\mathbf{Q}$, which we denote by ∞, and otherwise all the nonarchimedean places correspond to prime numbers $\ell \in \mathbf{Q}$.

First of all, we have that the extension $L/\mathbf{Q}$ is ramified only at p. Indeed, since $p^* \equiv 1 \pmod 4$, we know from the proof of Proposition 1.10 that the discriminant $\delta_{L/\mathbf{Q}} = p^*$. Thus, only p ramifies in $L/\mathbf{Q}$.

By Theorem 1.41 (2) we know that if we are given an $x \in \mathbf{Q}^\times$ and a place v of $\mathbf{Q}$ unramified in $L/\mathbf{Q}$ which satisfies $\mathrm{ord}_v(x) = 0$, then $\left(\frac{x, L/\mathbf{Q}}{v}\right) = 1$.

- Consider first $\left(\frac{-1, L/\mathbf{Q}}{v}\right)$. We have $\mathrm{ord}_v(x) = 0$ for any $v \neq \infty$, hence the only exceptional places are p and ∞ in this case. The product formula yields

$$\prod_v \left(\frac{-1, L/\mathbf{Q}}{v}\right) = \left(\frac{-1, L/\mathbf{Q}}{p}\right)\left(\frac{-1, L/\mathbf{Q}}{\infty}\right) = 1,$$

i.e., $\left(\frac{-1,L/\mathbf{Q}}{p}\right) = \left(\frac{-1,L/\mathbf{Q}}{\infty}\right)$. We must examine the extension of local fields

$$L_\infty/\mathbf{Q}_\infty = \mathbf{R}(\sqrt{p^*})/\mathbf{R}.$$

If $p \equiv 1 \pmod 4$, then $p^* = p$ and the extension is trivial. Thus $\left(\frac{-1,L/\mathbf{Q}}{\infty}\right) = 1$ in this case. If $p \equiv 3 \pmod 4$, then $L_\infty = \mathbf{C}$, and thus (again by property 2 of Theorem 1.41):

$$\left(\frac{-1,L/\mathbf{Q}}{\infty}\right) = (-1)^{\mathrm{ord}_\infty(-1)} = -1$$

(here we write $\mathrm{Gal}(\mathbf{C}/\mathbf{R}) = \{\pm 1\}$). Combining these two cases we get

$$\left(\frac{-1,L/\mathbf{Q}}{p}\right) = \left(\frac{-1,L/\mathbf{Q}}{\infty}\right) = (-1)^{\frac{p-1}{2}}.$$

- Now consider $\left(\frac{q,L/\mathbf{Q}}{v}\right)$, which is equal to 1 except perhaps for $v \in \{p,q\}$. First, if $q = p$ we have $\left(\frac{p,L/\mathbf{Q}}{v}\right) = 1$ for all $v \neq p$. But then the product formula is reduced to

$$\left(\frac{p,L/\mathbf{Q}}{p}\right) = 1.$$

  We may therefore assume $q \neq p$ in the following.

- For $v = p$, to compute $\left(\frac{q,L/\mathbf{Q}}{p}\right)$ we must understand $(q, L_p/\mathbf{Q}_p)$. Now since $q \neq p$ we have $q \in U_p = \mathbf{Z}_p^\times$. Furthermore, the extension $L_p/\mathbf{Q}_p$ is ramified, so we can only conclude by property 1 in Theorem 1.41 that $(q, L_p/\mathbf{Q}_p) = 1$ if and only if $q \in \mathrm{Nm}_{L_p/\mathbf{Q}_p}(L_p^\times)$. But we know that since $L_p/\mathbf{Q}_p$ is ramified, the inertia group I_p has order 2, and hence by property 3 in Theorem 1.41, the quotient group

$$U_p/(U_p \cap \mathrm{Nm}_{L_p/\mathbf{Q}_p}(L_p^\times)) \cong I_p$$

  has order 2. Thus $U_p \cap \mathrm{Nm}_{L_p/\mathbf{Q}_p}(L_p^\times)$ has index 2 in $U_p = \mathbf{Z}_p^\times$. Hence $(q, L_p/\mathbf{Q}_p) = 1$ if and only if q belongs to a subgroup of index 2 of $\mathbf{Z}_p^\times$. But by Example 1.36, the only subgroup of index 2 of $U_p = \mathbf{Z}_p^\times$ is

$$\mu_{p-1}^2 \oplus U_p^1 = (U_p)^2.$$

  Therefore $(q, L_p/\mathbf{Q}_p) = 1$ if and only if $q \in (U_p)^2$, which happens if and only if $\overline{q} \in \mathbf{F}_p^{\times 2}$, i.e., if and only if q is a square modulo p. Thus we have that

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

- For $v = q$, since the extension $L_q/\mathbf{Q}_q$ is unramified, we can use property 2 of Theorem 1.41 to get

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

  This Frobenius is trivial if and only if the extension $L_q/\mathbf{Q}_q = \mathbf{Q}_q(\sqrt{p^*})/\mathbf{Q}_q$ is trivial, which happens if and only if p^* is a square modulo q. In other words,

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

  where (p^*/q) is the Kronecker symbol, which is the same as the Legendre symbol for $q \neq 2$, and for $q = 2$ it is defined as

$$\left(\frac{a}{2}\right) = \begin{cases} 1 & \text{if } a \equiv 1 \pmod 8; \\ -1 & \text{otherwise.} \end{cases}$$

$p \pmod 8$	p^*	$\left(\frac{p^*}{2}\right)$	$(-1)^{\frac{p^2-1}{8}}$
1	p	1	1
3	$-p$	-1	-1
5	p	-1	-1
7	$-p$	1	1

Table 1.2: $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Thus the product formula yields

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

Finally, for p and q odd primes, the formulation of quadratic reciprocity in Theorem 1.1 is obtained from the above by using the multiplicativity of the Legendre symbols:

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

yielding

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

For $q = 2$ and p odd we get $(2/p) = (p^*/2)$, but here we cannot use multiplicativity of the symbols as above, since e.g., $(3/2) = (5/2) = (15/2) = -1$. Instead we check all possible values for $p \pmod 8$ (see Table 1.2), and find

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

Thus we have also obtained the supplementary law of quadratic reciprocity.

1.6 Symbols over number fields

We now turn to the notion of symbols over number fields which we later will connect to algebraic K-theory. We mostly follow Gras' presentation [Gra03, II §7]. As before, F denotes a number field and $v \in \mathrm{Pl}^{\mathrm{nc}}$ a place of F.

In this section we will disregard all infinite complex places. There are several reasons for this exclusion. First, by our Definition 1.29, all infinite complex places have trivial valuation. Secondly, we will repeatedly consider the group of roots of unity $\mu(F_v)$ of the local field F_v, which is finite cyclic whenever $v \in \mathrm{Pl}_F^{\mathrm{nc}}$, but infinite if $F_v = \mathbf{C}$. Finally, Moore has shown that any continuous Steinberg symbol (see Definition 2.16) on $\mathbf{C}$ is in fact trivial (cf. [Mil71, Corollary A.2]).

Definition 1.48. The *local Hilbert symbol at v* is the map

$$(-,-)_v : F_v^\times \times F_v^\times \longrightarrow \mu(F_v)$$

defined by

$$(x,y)_v := \frac{(y, F_v(\sqrt[m_v]{x})/F_v)(\sqrt[m_v]{x})}{\sqrt[m_v]{x}}.$$

Here $(y, F_v(\sqrt[m_v]{x})/F_v)$ is the local reciprocity symbol for the cyclic extension $F_v(\sqrt[m_v]{x})/F_v$ evaluated at $y \in F_v^\times$. It is an element of the Galois group $\mathrm{Gal}(F_v(\sqrt[m_v]{x})/F_v)$ and therefore permutes the different m_v-roots of x. Hence $(y, F_v(\sqrt[m_v]{x})/F_v)(\sqrt[m_v]{x})$ and $\sqrt[m_v]{x}$ differ by a root of unity.

Proposition 1.49 ([Gra03, II Proposition 7.1.1]). *The local Hilbert symbol is* $\mathbf{Z}$*-bilinear, and nondegenerate as a map on* $F_v^\times/F_v^{\times m_v} \times F_v^\times/F_v^{\times m_v}$*. Furthermore, it satisfies the following relations:*

- $(x, 1-x)_v = 1$ *for all* $x \in F_v^\times$, $x \neq 1$ *(Steinberg relation);*
- $(x, -x)_v = 1$*;*
- $(x, y)_v = (y, x)_v^{-1}$*, for all* $x, y \in F_v^\times$*.*

Proof (following [Gra03]). We only show the Steinberg relation. Antisymmetry and the relation $(x, -x)_v = 1$ follow from the Steinberg relation; see Lemma 2.17.

To this end, by Theorem 1.41 it is enough to show that for $x \in F^\times$, the element $1 - x$ is a norm in the extension M/F_v, where $M := F_v(\sqrt[m_v]{x})$. Let $d := [M : F_v]$, so that $d \mid m_v$. By Kummer theory (see e.g., [Gra03, I §6]) there is a $t \in F_v^\times$ such that $M = F_v(\sqrt[d]{t})$ and $x = t^{m_v/d}$. Note that for any $\xi \in \mu(F_v)$ we have

$$\begin{aligned}\mathrm{Nm}_{M/F_v}(1 - \xi\sqrt[d]{t}) &= \prod_{\sigma \in \mathrm{Gal}(M/F_v)} \sigma(1 - \xi\sqrt[d]{t}) \\ &= \prod_{j=1}^{d} (1 - \zeta_d^j \xi \sqrt[d]{t}) \\ &= 1 - \xi^d t\end{aligned}$$

where ζ_d is a primitive d-th root of unity.

Now let ζ_v denote a generator for $\mu(F_v)$. We claim that the element

$$\prod_{j=1}^{\frac{m_v}{d}} (1 - \zeta_v^j \sqrt[d]{t}) \in M^\times$$

has norm equal to $1 - x$:

$$\begin{aligned}\mathrm{Nm}_{M/F_v}\left(\prod_{j=1}^{\frac{m_v}{d}} (1 - \zeta_v^j \sqrt[d]{t})\right) &= \prod_{j=1}^{\frac{m_v}{d}} \mathrm{Nm}_{M/F_v}(1 - \zeta_v^j \sqrt[d]{t}) \\ &= \prod_{j=1}^{\frac{m_v}{d}} (1 - \zeta_v^{dj} t) \\ &= 1 - \zeta_v^{m_v} t^{\frac{m_v}{d}} = 1 - x,\end{aligned}$$

as desired. □

For a finite place $v \in \mathrm{Pl}_0$, let ℓ denote the characteristic of the residue field $k(v) = \mathcal{O}_v/\mathfrak{p}_v$. By Proposition 1.35 there is a decomposition $F_v^\times \cong \pi_v^{\mathbf{Z}} \oplus \mu_{q_v-1} \oplus U_v^1$. This yields a decomposition

$$\mu(F_v) = \mu_{q_v-1} \oplus \mu(U_v^1)$$

where $\mu(U_v^1)$ denotes the torsion part of U_v^1, whose order is a power of ℓ. With this decomposition in mind we will from now on instead denote the group μ_{q_v-1} by $\mu(F_v)^{\mathrm{reg}}$ and $\mu(U_v^1)$ by $\mu(F_v)^1$. If v is a real place at infinity, we will set $\mu(F_v)^{\mathrm{reg}} := \mu_2$ and $\mu(F_v)^1 := 1$. Here we do not consider complex places at infinity since $\mathrm{ord}_v(x) = 0$ for all $x \in F_v$ for such a place. We write

$$m_v^1 := \#\mu(F_v)^1.$$

There are only finitely many places v for which $\mu(F_v)^1 \neq 1$, and such places will be referred to as *irregular* places. The places v with $\mu(F_v) = 1$ are called *regular*.

Definition 1.50. Let v be a noncomplex place of the number field F. The *regular*, or *tame* Hilbert symbol at v, $(-,-)_v^{\mathrm{reg}}$, is the map on $F_v^\times \times F_v^\times$ defined by

$$(x,y)_v^{\mathrm{reg}} := \frac{(y, F_v(\sqrt[q_v-1]{x})/F_v)(\sqrt[q_v-1]{x})}{\sqrt[q_v-1]{x}}.$$

Remark 1.51. The regular Hilbert symbol is nothing more than a power of the local Hilbert symbol at v:

$$(x,y)_v^{\mathrm{reg}} = (x,y)_v^{m_v^1} = (x^{m_v^1}, y)_v.$$

Thus the results of Proposition 1.49 also hold for the regular Hilbert symbol.

Proposition 1.52 ([Gra03, II Proposition 7.1.5])**.** *For any $x, y \in F_v^\times$ the following formula for $(x,y)_v^{\mathrm{reg}}$ holds:*

$$(x,y)_v^{\mathrm{reg}} = \begin{cases} (-1)^{\mathrm{ord}_v(x)\,\mathrm{ord}_v(y)} x^{\mathrm{ord}_v(y)} y^{-\mathrm{ord}_v(x)} + \mathfrak{p}_v, & v \text{ finite;} \\ (-1)^{\mathrm{ord}_v(x)\,\mathrm{ord}_v(y)}, & v \text{ infinite real,} \end{cases}$$

where we in the finite case identify $\mu(F_v)^{\mathrm{reg}}$ with $k(v)^\times$.

Proof (following [Gra03]). First assume v is an infinite real place. Then, since $\mu(F_v^\times) = \mu_2$ we have

$$(x,y)_v^{\mathrm{reg}} = \frac{(y, F_v(\sqrt{x})/F_v)(\sqrt{x})}{\sqrt{x}}.$$

If $i_v(x) > 0$, or in other words $\mathrm{ord}_v(x) = 0$, we have $F_v(\sqrt{x}) = F_v = \mathbf{R}$. Therefore $(y, F_v(\sqrt{x})/F_v) = 1$, and hence

$$(x,y)_v^{\mathrm{reg}} = 1 = (-1)^{\mathrm{ord}_v(x)\,\mathrm{ord}_v(y)}.$$

If $i_v(x) < 0$ so that $\mathrm{ord}_v(x) = 1$ we have $F_v(\sqrt{x})/F_v = \mathbf{C}/\mathbf{R}$, and thus, as we saw in Example 1.43, $(y, \mathbf{C}/\mathbf{R}) = c^{\mathrm{ord}_v(y)}$ where c is complex conjugation. Hence

$$(x,y)_v^{\mathrm{reg}} = (-1)^{\mathrm{ord}_v(y)} = (-1)^{\mathrm{ord}_v(x)\,\mathrm{ord}_v(y)}.$$

Now assume v is a finite place of F. For any $x \in F_v^\times$ we may write $x = \pi_v^n u$ for some $u \in U_v$ and $n = \mathrm{ord}_v(x)$. By bilinearity and antisymmetry of the Hilbert symbol it is therefore enough to compute

$$(u,u')_v^{\mathrm{reg}}, \quad (u,\pi)_v^{\mathrm{reg}}, \quad (\pi,\pi)_v^{\mathrm{reg}},$$

where $u, u' \in U_v$ and where π_v is abbreviated by π.

- The extension $F_v(\sqrt[q_v-1]{u})/F_v$ is unramified, hence

$$(u,u')_v^{\mathrm{reg}} = \frac{(u', F_v(\sqrt[q_v-1]{u})/F_v)(\sqrt[q_v-1]{u})}{\sqrt[q_v-1]{u}} = \left(F_v(\sqrt[q_v-1]{u})/F_v\right)^{\mathrm{ord}_v(u')} = 1$$

  since $\mathrm{ord}_v(u') = 0$.

- For the symbol $(u,\pi)_v^{\mathrm{reg}}$ we again use that $F_v(\sqrt[q_v-1]{u})/F_v$ is unramified. We have

$$(\pi, F_v(\sqrt[q_v-1]{u})/F_v) = \left(F_v(\sqrt[q_v-1]{u})/F_v\right)^{\mathrm{ord}_v(\pi)} = \left(F_v(\sqrt[q_v-1]{u})/F_v\right)$$

  since $\mathrm{ord}_v(\pi) = 1$. Let σ denote the Frobenius $(F_v(\sqrt[q_v-1]{u})/F_v)$. Then

$$(u,\pi)_v^{\mathrm{reg}} = \frac{\sigma(\sqrt[q_v-1]{u})}{\sqrt[q_v-1]{u}} \equiv \frac{(\sqrt[q_v-1]{u})^{q_v}}{\sqrt[q_v-1]{u}} \equiv u \pmod{\mathfrak{p}_v}$$

  by the properties of the Frobenius automorphism. Thus

$$(u,\pi)_v^{\mathrm{reg}} \equiv u = (-1)^{\mathrm{ord}_v(u)\,\mathrm{ord}_v(\pi)} u^{\mathrm{ord}_v(\pi)} \pi^{-\mathrm{ord}_v(u)} \pmod{\mathfrak{p}_v}.$$

- Finally, to compute $(\pi,\pi)_v^{\mathrm{reg}}$ we make use of the properties in Proposition 1.49. We have
$$(\pi,-\pi)_v^{\mathrm{reg}} = 1 = (\pi,\pi)_v^{\mathrm{reg}}(\pi,-1)_v^{\mathrm{reg}},$$
hence $(\pi,\pi)_v^{\mathrm{reg}} = (-1,\pi)_v^{\mathrm{reg}}$ by antisymmetry. By the previous result with $u=-1$ we get
$$(\pi,\pi)_v^{\mathrm{reg}} \equiv -1 = (-1)^{\mathrm{ord}_v(\pi)^2}\pi^{\mathrm{ord}_v(\pi)}\pi^{-\mathrm{ord}_v(\pi)} \pmod{\mathfrak{p}_v}.$$

By bilinearity, this concludes the proof. □

Definition 1.53 (Hilbert symbols)**.** For $x,y\in F^\times$ and v a place of F, the *Hilbert symbol at v of order $m=\#\mu(F)$* is defined as
$$\left(\frac{x,y}{v}\right) := \frac{\sigma_v(\sqrt[m]{x})}{\sqrt[m]{x}} \in \mu(F),$$
where
$$\sigma_v = \left(\frac{y, F(\sqrt[m]{x})/F}{v}\right)$$
is the Hasse symbol at v.

For any divisor n of m, we also define the *Hilbert symbol of order n* as
$$\left(\frac{-,-}{v}\right)_n := \left(\frac{-,-}{v}\right)^{\frac{m}{n}}.$$

Example 1.54. For $F=\mathbf{Q}$ and $v\in\mathrm{Pl}_{\mathbf{Q}}$, the Hilbert symbol $\left(\frac{-,-}{v}\right)$ is given by
$$\left(\frac{a,b}{v}\right) = \begin{cases} 1 & \text{if } ax^2+by^2=z^2 \text{ has a nontrivial solution in } \mathbf{Q}_v; \\ -1 & \text{otherwise,}\end{cases}$$
for any $a,b\in\mathbf{Q}^\times$ [Dal06].

Theorem 1.55 (Product formula for Hilbert symbols)**.** *For any $x,y\in F^\times$ and any $n\mid m=\#\mu(F)$, the following product formula holds:*
$$\prod_{v\in\mathrm{Pl}_F}\left(\frac{x,y}{v}\right)_n = 1.$$

Proof. The conclusion follows from the product formula for Hasse symbols (Theorem 1.46) and the fact that if $\{\sigma_i\}_{i=1}^N$ is a finite set of automorphisms in the Galois group of some abelian extension L of F containing an n-th root z of an element $x\in F^\times$, we have
$$\frac{(\prod_{i=1}^N\sigma_i)(z)}{z} = \prod_{i=1}^N\frac{\sigma_i(z)}{z}\in\mu(F).$$

Indeed, let $\sigma,\tau\in\mathrm{Gal}(L/F)$. Then
$$\begin{aligned}\frac{(\sigma\tau)(z)}{z} &= \frac{\sigma(\tau(z))}{z}\cdot\frac{\tau(z)}{\tau(z)} \\ &= \frac{\tau(\sigma(z))}{\tau(z)}\cdot\frac{\tau(z)}{z} \\ &= \tau\left(\frac{\sigma(z)}{z}\right)\cdot\frac{\tau(z)}{z} \\ &= \frac{\sigma(z)}{z}\cdot\frac{\tau(z)}{z},\end{aligned}$$
where the second equality holds because the extension is abelian, and the last equality holds since τ acts trivially on F and $\mu_n\subseteq F^\times$. The general case follows by induction. □

Definition 1.56. Let $n > 1$ be a natural number. For any $x \in F^\times$ and any $v \in \mathrm{Pl}_0$ not ramified in $F(\sqrt[n]{x})/F$, we define the *n-th power residue symbol* as

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

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 $y \in F^\times$ such that all $v \mid y$ is unramified in $F(\sqrt[n]{x})/F$, we define

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

where the product runs over all places $v \mid y$ and all infinite real places.

Write $\sigma = \left(\frac{F(\sqrt[n]{x})/F}{v}\right)$ for the global Frobenius at the finite place v, and let $\mathfrak{p}$ denote the prime ideal corresponding to v. Recall that, modulo $\mathfrak{p}$, σ raises elements to the power of $q_v = \mathrm{Nm}(\mathfrak{p})$. Hence

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

so the n-th power reciprocity symbol is a direct generalization of the Legendre symbol $(p/q) \equiv p^{\frac{q-1}{2}} \pmod{q}$.

Proposition 1.57 ([Gra03, pp.204-205])**.** *The n-th power residue symbols satisfy the following properties (for any place v such that the given residue symbol is defined):*

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

   In particular,

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

Theorem 1.58 (The n-th power reciprocity law [Gra03, II Theorem 7.4.4])**.** *Let n be a divisor of $m = \#\mu(F)$. Suppose $x, y \in F^\times$ are such that* $\mathrm{ord}_v(x)\,\mathrm{ord}_v(y) = 0$ *for any $v \in \mathrm{Pl}_F$ (i.e., x and y are coprime), and* $\mathrm{ord}_v(x) = \mathrm{ord}_v(y) = 0$ *for all places v dividing n. Then*

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

Proof (following [Gra03]). By definition we have

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

since $\mathrm{ord}_v(x) = \mathrm{ord}_v(y) = 0$ for all $v \mid n$.

Since

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

we have

$$\begin{aligned}\left(\frac{y}{x}\right)_n\left(\frac{x}{y}\right)_n^{-1} &= \prod_{\substack{v\nmid n\\ \mathrm{ord}_v(x)\neq 0}}\left(\frac{y,x}{v}\right)_n \prod_{\substack{v\nmid n\\ \mathrm{ord}_v(y)\neq 0}}\left(\frac{x,y}{v}\right)_n^{-1}\\ &= \prod_{\substack{v\nmid n\\ \mathrm{ord}_v(xy)\neq 0}}\left(\frac{y,x}{v}\right)_n = \prod_{v\nmid n}\left(\frac{y,x}{v}\right)_n,\end{aligned}$$

where the last two equalities follow since by assumption $\mathrm{ord}_v(xy)\neq 0 \iff \mathrm{ord}_v(x)\neq 0$ or $\mathrm{ord}_v(y)\neq 0$. By the product formula for Hilbert symbols this equals

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

so this concludes the proof. □

Let us return to the Gaussian integers. Recall the statement of biquadratic reciprocity (Theorem 1.6): For distinct primary Gaussian primes π, τ, we have

$$\left(\frac{\tau}{\pi}\right)_4 = (-1)^{\frac{\mathrm{Nm}(\pi)-1}{4}\cdot\frac{\mathrm{Nm}(\tau)-1}{4}}\left(\frac{\pi}{\tau}\right)_4.$$

Proof of Theorem 1.6. The following argument is due to Lenstra and Stevenhagen.

Since $\mathbf{Q}(i)$ only has complex places at infinity, and since $(1+i)$ is the only place dividing $n=4$, power reciprocity states that

$$\left(\frac{\tau}{\pi}\right)_4\left(\frac{\pi}{\tau}\right)_4^{-1} = \left(\frac{\pi,\tau}{(1+i)}\right)_4,$$

where the right hand side is the Hilbert symbol of order 4 at $(1+i)$. Thus we want to show

$$\left(\frac{\pi,\tau}{(1+i)}\right)_4 = (-1)^{\frac{\mathrm{Nm}(\pi)-1}{4}\cdot\frac{\mathrm{Nm}(\tau)-1}{4}}. \tag{1.3}$$

Let v denote the place corresponding to $(1+i)$. Note that for a primary Gaussian prime α we have $\alpha\in U_v^3$ by definition (here we identify α with its image $i_v(\alpha)$ in U_v). Thus α has component 1 on μ_4 in the decomposition of $\mathbf{Z}_2[i]^\times$ of Proposition 1.22, and by Proposition 1.23 the same holds for the residue class of α in

$$U_v/(U_v)^4 \cong \mu_4\oplus\langle\overline{3+2i}\rangle\oplus\langle\overline{5}\rangle.$$

We must therefore compute the Hilbert symbols $\left(\frac{\pi,\tau}{v}\right)_4$ for π and τ in the congruence classes of $3+2i$ and 5 modulo $(U_v)^4$. According to the right hand side of Equation (1.3) we must show that

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

If α, $\beta\in\mathbf{Z}[i]$ satisfy $\mathrm{ord}_v(\alpha\beta)\geq 7$, then by Proposition 1.23 (3) we have $1-\alpha\beta\in(U_v)^4$. Using this we will show that $\left(\frac{1+\alpha,1+\beta}{v}\right)_4 = 1$.

First, note that

$$\left(\frac{1+\alpha,-\alpha}{v}\right)_4 = 1$$

by the Steinberg relation (cf. Proposition 1.49). Hence, using bilinearity, we get

$$\left(\frac{1+\alpha,1+\beta}{v}\right)_4 = \left(\frac{1+\alpha,1+\beta}{v}\right)_4\left(\frac{1+\alpha,-\alpha}{v}\right)_4 = \left(\frac{1+\alpha,-\alpha(1+\beta)}{v}\right)_4.$$

Since $1-\alpha\beta \in (U_v)^4$, we have

$$\left(\frac{-\alpha(1+\beta), 1-\alpha\beta}{v}\right)_4 = 1 = \left(\frac{(1-\alpha\beta)^{-1}, -\alpha(1+\beta)}{v}\right)_4.$$

Thus

$$\begin{aligned}\left(\frac{1+\alpha, -\alpha(1+\beta)}{v}\right)_4 &= \left(\frac{1+\alpha, -\alpha(1+\beta)}{v}\right)_4 \left(\frac{(1-\alpha\beta)^{-1}, -\alpha(1+\beta)}{v}\right)_4 \\ &= \left(\frac{\frac{1+\alpha}{1-\alpha\beta}, -\alpha(1+\beta)}{v}\right)_4.\end{aligned}$$

Multiplying similarly in the second slot we obtain

$$\begin{aligned}\left(\frac{1+\alpha, 1+\beta}{v}\right)_4 &= \left(\frac{1+\alpha, -\alpha(1+\beta)}{v}\right)_4 \\ &= \left(\frac{\frac{1+\alpha}{1-\alpha\beta}, \frac{-\alpha(1+\beta)}{1-\alpha\beta}}{v}\right)_4 \\ &= \left(\frac{\frac{1+\alpha}{1-\alpha\beta}, 1-\frac{1+\alpha}{1-\alpha\beta}}{v}\right)_4 = 1.\end{aligned}$$

Since $\mathrm{ord}_v(4) = 4$, this finishes the case where at least one of π or τ is congruent to 5 modulo $(U_v)^4$. For if $\pi = 5$ while τ equals 5 or $3+2i$, then we can write $\pi = 1+\alpha$, $\tau = 1+\beta$ where $\mathrm{ord}_v(\alpha\beta) \geq 7$.

For the remaining case we shall show that

$$\left(\frac{1+\alpha}{1+\beta}\right)_4 \left(\frac{1+\beta}{1+\alpha}\right)_4^{-1} = -1$$

for some $\alpha, \beta \in \mathbf{Z}[i]$ with $\mathrm{ord}_v(\alpha) = \mathrm{ord}_v(\beta) = 3$, i.e., $1+\alpha, 1+\beta \in U_v^3 \backslash U_v^4$. Put $\alpha = (-i)(1+i)^3$ and $\beta = -(1+i)^3$. Using that

$$1+\alpha = 3+2i \equiv 1-i \pmod{3-2i},$$

we get $\left(\frac{3+2i}{3-2i}\right)_4 = \left(\frac{1-i}{3-2i}\right)_4$. However,

$$(1-i)^{\frac{\mathrm{Nm}(3-2i)-1}{4}} = (1-i)^3 = -2-2i \equiv i \pmod{3-2i},$$

hence

$$\left(\frac{1+\alpha}{1+\beta}\right)_4 = i.$$

Since $1+\beta$ is the complex conjugate of $1+\alpha$ we then have

$$\left(\frac{1+\beta}{1+\alpha}\right)_4 = \overline{\left(\frac{1+\alpha}{1+\beta}\right)_4} = -i,$$

where the bar denotes complex conjugation. Hence we end up with

$$\left(\frac{1+\alpha}{1+\beta}\right)_4 \left(\frac{1+\beta}{1+\alpha}\right)_4^{-1} = -1.$$

We now turn to the supplementary laws stated in Theorem 1.6. The identity $(i/\pi)_4 = i^{(\mathrm{Nm}(\pi)-1)/4}$ is true by definition, so we need only concern ourselves with the symbol $((1+i)/\pi)_4$. As noted in Theorem 1.6, we use the isomorphism

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

to write $\pi \equiv i^k(3+2i)^\mu 5^\nu \pmod{(U_{1+i})^4}$. Multiplicativity of residue symbols yields

$$\left(\frac{1+i}{\pi}\right)_4 = \left(\frac{1+i}{3+2i}\right)_4^\mu \left(\frac{1+i}{2+i}\right)_4^\nu \left(\frac{1+i}{2-i}\right)_4^\nu.$$

We compute[2]:

$$\begin{aligned}
\left(\frac{1+i}{3+2i}\right)_4 &\equiv (1+i)^{\frac{\mathrm{Nm}(3+2i)-1}{4}} \equiv (1+i)^3 \equiv -i \pmod{3+2i};\\
\left(\frac{1+i}{2+i}\right)_4 &\equiv 1+i \equiv -1 \pmod{2+i};\\
\left(\frac{1+i}{2-i}\right)_4 &\equiv -i \pmod{2-1}.
\end{aligned}$$

Hence

$$\left(\frac{1+i}{\pi}\right)_4 = (-i)^\mu(-1)^\nu(-i)^\nu = i^{\nu-\mu},$$

as desired. □

[2]To solve congruences of Gaussian integers it can often be helpful to draw the lattice spanned by unit multiples of the given Gaussian prime, and look at Gaussian integers relative to this lattice; see Figure 3.1 in Chapter 3.

CHAPTER 2

Algebraic K-theory

The zeroth algebraic K-group originated in Grothendieck's work on his formulation of the generalized Riemann-Roch theorem [Dal06]. Through his need to work on sheaves over a scheme X there arose two definitions of algebraic K-groups, either of which is referred to as the Grothendieck group of X: He defined $K_0(X)$ as a certain group built from isomorphism classes of locally free sheaves of finite rank over X, and similarly a group $G_0(X)$ of classes of coherent sheaves over X. If X is a regular variety, the two definitions coincide. If X is the spectrum of a ring A, we have an alternate definition of the K-group of X. We consider the monoid M consisting of isomorphism classes of finitely generated projective modules over A, keeping in mind that such modules may be regarded as locally free $\mathcal{O}_X$-modules. Then $K_0(X)$ is defined as the universal object with respect to monoid homomorphisms of M into various abelian groups.

The functor K_0 is the starting point for the definition of a series of functors attaching important invariants to a ring. As a starter, we shall see in Example 2.4 that the torsion part of $K_0(A)$ is precisely the ideal class group $\mathrm{Cl}(A)$ when A is the ring of integers in a number field.

2.1 Classical K-theory of rings

There is a forgetful functor

$$U : \mathrm{Ab} \longrightarrow \mathrm{CMon}$$

from the category of abelian groups to the category of commutative monoids, which admits a left adjoint—a "group completion functor"

$$(-)^+ : \mathrm{CMon} \longrightarrow \mathrm{Ab}.$$

For a given commutative monoid M, the group M^+ is called the *Grothendieck group*, or the *group completion* of M. Thus, the Grothendieck group of M is a group M^+ together with a map $i : M \to M^+$ (not necessarily an injection) such that the following universal property is satisfied. Given any abelian group G with a monoid map $f : M \to G$, there is a unique map of abelian groups $\overline{f} : M^+ \to G$ such that the following diagram commutes:

$$\begin{array}{ccc} M & \xrightarrow{\;i\;} & M^+ \\ {\scriptstyle f}\big\downarrow & \swarrow{\scriptstyle \exists!\overline{f}} & \\ G & & \end{array}$$

One constructs M^+ by adding formal differences as follows [Ros94, Theorem 1.1.3]. Define the equivalence relation $\sim$ on $M \times M$ by letting $(x_1, y_1) \sim (x_2, y_2)$ if and only if there is a $t \in M$ such that

$$x_1 + y_2 + t = x_2 + y_1 + t.$$

Then $M^+ = M \times M/\sim$.

Now let $(\mathscr{C}, \square)$ be a symmetric monoidal category (see [ML98, p.184] for a definition), and assume that the isomorphism classes of objects of $\mathscr{C}$ form a *set*, which we denote by $\mathscr{C}^{\text{iso}}$. The set $\mathscr{C}^{\text{iso}}$ is then a commutative monoid with addition given by

$$[C] + [C'] := [C \square C'],$$

where we write $C \square C' := \square(C, C')$ for any $C, C' \in \mathscr{C}$. The Grothendieck group of $\mathscr{C}$ is then defined as

$$K_0^{\square}(\mathscr{C}) := (\mathscr{C}^{\text{iso}})^+,$$

and is often abbreviated to $K_0(\mathscr{C})$ if no confusion is likely to arise (although confusion will occur in the case of K_0 of schemes—see below).

To define K_0 of a ring A, we take as our symmetric monoidal category the category $\mathscr{P}(A)$ of finitely generated projective A-modules, with direct sum as the associated bifunctor.

Definition 2.1. The *zeroth algebraic K-group* $K_0(A)$ of the ring A is the Grothendieck group of $(\mathscr{P}(A), \oplus)$:

$$K_0(A) := K_0^{\oplus}(\mathscr{P}(A)).$$

Moreover, tensor product over A induces a ring structure on $K_0(A)$.

Example 2.2. If A is a principal ideal domain or a local ring, any finitely generated projective A-module is free ([Ros94, Theorem 1.3.1], [Wei13, Lemma 2.2, p.11]). Since the rank is well defined up to isomorphism, the map $\mathscr{P}(A)^{\text{iso}} \to \mathbf{Z}_{\geq 0}$ defined by $[A^n] \mapsto n$ is an isomorphism. By group completing the two monoids we obtain an isomorphism $K_0(A) \cong \mathbf{Z}$.

To generalize the definition of K_0 of a ring to arbitrary schemes, we consider the category $\text{VB}(X)$ of vector bundles over a scheme X. It turns out that the most satisfactory way of defining K_0 of X is to set

$$K_0(X) := K_0(\text{VB}(X)),$$

where the right hand side means K_0 of $\text{VB}(X)$ viewed as an *exact category*, and not as a symmetric monoidal category. See [Wei13, II Ch.7] for details on K_0 of an exact category. Since $\text{VB}(X)$ is not always a split exact category[1], we have $K_0(X) \ncong K_0^{\oplus}(X)$ in general. On the other hand, if $X = \operatorname{Spec} A$ is an affine scheme, there is an equivalence of categories $\mathscr{P}(A) \cong \text{VB}(\operatorname{Spec} A)$ [Wei13, p.51], hence $K_0(A) = K_0(\operatorname{Spec} A)$.

For any scheme X there is a rank map

$$\text{rank} : K_0(X) \longrightarrow H^0(X, \underline{\mathbf{Z}})$$

induced by taking the rank of vector bundles, whose kernel $\widetilde{K}_0(X)$ is called the *reduced K-theory* of X. Here $\underline{\mathbf{Z}}$ is the constant sheaf on X with group $\mathbf{Z}$, and $H^0(X, \underline{\mathbf{Z}})$ is viewed as a subring of $K_0(X)$. Similarly, there is a determinant map

$$\det : K_0(X) \longrightarrow \operatorname{Pic}(X)$$

induced by the determinant map on vector bundles sending a locally free rank n bundle $\mathscr{F}$ to the line bundle $\det \mathscr{F} = \bigwedge^n \mathscr{F}$. The map $\text{rank} \oplus \det$ is a surjective ring homomorphism [Wei13, Theorem 8.1, p.158].

Theorem 2.3 ([Wei13, Proposition 8.2.1, p.159])**.** *If X is a 1-dimensional separated, regular noetherian scheme, the map* $\text{rank} \oplus \det$ *yields an isomorphism*

$$K_0(X) \cong H^0(X, \underline{\mathbf{Z}}) \oplus \operatorname{Pic}(X).$$

Example 2.4. Let A be a Dedekind ring. Then the Picard group of $\operatorname{Spec} A$ is the ideal class group $\operatorname{Cl}(A)$ [Har77, II Example 6.3.2], and since $\operatorname{Spec} A$ is connected we have $H^0(\operatorname{Spec} A, \underline{\mathbf{Z}}) = \mathbf{Z}$. Hence the theorem above yields

$$K_0(A) \cong \mathbf{Z} \oplus \operatorname{Cl}(A),$$

i.e., $\widetilde{K}_0(A) \cong \operatorname{Cl} A$.

[1] E.g., taking $X = \mathbf{P}^1_{\mathbf{C}}$, the exact sequence $0 \to \mathscr{O}_X(-2) \to \mathscr{O}_X(-1)^{\oplus 2} \to \mathscr{O}_X \to 0$ does not split.

2.1.1 The functors K_1 and K_2

Let A be a ring. Recall the definition of the *general linear group* $\mathrm{GL}(A)$ as the colimit of the directed system

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

where the injections of $\mathrm{GL}_n(A)$ into $\mathrm{GL}_{n+1}(A)$ are defined by $M \mapsto \left(\begin{smallmatrix} M & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Let $e_{ij}(a)$ denote the matrix which coincides with the identity matrix except having a in the (i,j)-position, where $i \neq j$. Such a matrix is called an *elementary matrix*, and the elementary $n \times n$-matrices generate a subgroup $E_n(A)$ of $\mathrm{GL}_n(A)$. As in the above sequence we have maps $E_n(A) \to E_{n+1}(A)$ for each n, and the colimit of this system is denoted by $E(A)$.

Lemma 2.5 (Whitehead)**.** *The group $E(A)$ is the commutator subgroup of $\mathrm{GL}(A)$.*

Whitehead's lemma tells us that $\mathrm{GL}(A)/E(A)$ is the maximal abelian quotient $\mathrm{GL}(A)^{\mathrm{ab}}$ of $\mathrm{GL}(A)$. This group was recognized by Bass to be the correct definition of $K_1(A)$:

Definition 2.6. The first algebraic K-group of the ring A is defined as

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

A ring map $A \to B$ induces a map $\mathrm{GL}(A) \to \mathrm{GL}(B)$ preserving elementary matrices, and hence a map $K_1(A) \to K_1(B)$. Thus K_1 is a covariant functor on the category of rings.

There is a determinant map $\det : \mathrm{GL}(A) \to A^\times$, which induces a map $K_1(A) \to A^\times$. Denote by $\mathrm{SL}(A)$ the kernel of the determinant map, and let $SK_1(A) := \mathrm{SL}(A)/E(A)$. By realizing $A^\times$ as $\mathrm{GL}_1(A)$, which then maps into $\mathrm{GL}(A)$, we obtain a split exact sequence

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

Example 2.7. The kernel $SK_1(A)$ is known to be trivial for example when A is a local ring [Wei13, III Lemma 1.4] or the ring of integers in a number field [BMS67]. In other words, we get an isomorphism

$$K_1(A) \cong A^\times$$

in this case.

Definition 2.8. 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 G form a category where a morphism $\psi : (E,\phi) \to (E',\phi')$ is a homomorphism $\psi : E \to E'$ over G, i.e., a commutative diagram

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

We may therefore define a central extension (E,ϕ) of G to be *universal* if (E,ϕ) is initial in the category of central extensions of G.

Recall that a group G is *perfect* if it equals its commutator subgroup $[G,G]$. In other words, a group is perfect if it has trivial abelianization, which is equivalent to the vanishing of the first group homology $H_1(G,\mathbf{Z})$.

Theorem 2.9 ([Ros94, Theorem 4.1.3])**.** *A group admits a universal central extension if and only if it is perfect.*

We turn back to a quick study of the elementary matrices over a ring A. There are a few evident relations satisfied by such matrices. First we have

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

Secondly, the commutator of two elementary matrices satisfies

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

With this in mind, we define the Steinberg group as the group generated by symbols satisfying the analog of the relations given above:

Definition 2.10. Let A be a ring and $n \geq 3$ a natural number. The *Steinberg group* $\mathrm{St}_n(A)$ of order n over A is defined as the free group generated by symbols $x_{ij}(a), 1 \leq i, j \leq n$, $i \neq j$, $a \in A$, modulo the 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 homomorphism $f : A \to B$ we get an induced map on the free groups generated by the $\{x_{ij}(a) : a \in A\}$ and $\{x_{ij}(b) : b \in B\}$ by sending $x_{ij}(a)$ to $x_{ij}(f(a))$. This is compatible with the relations in $\mathrm{St}(A)$ and therefore factors through a map $\mathrm{St}(A) \to \mathrm{St}(B)$. Hence the formation of Steinberg groups is functorial. Additionally there are maps $\phi_n : \mathrm{St}_n(A) \to \mathrm{GL}_n(A)$ for any n, given by $x_{ij}(a) \mapsto e_{ij}(a)$; clearly its image is precisely the group $E_n(A)$ generated by elementary $n \times n$-matrices. Passing to the colimit, we obtain a map $\phi : \mathrm{St}(A) \to E(A)$.

Definition 2.11. The second algebraic K-group $K_2(A)$ of the ring A is defined as the kernel of the map $\phi : \mathrm{St}(A) \to E(A)$.

That K_2 is a functor is a consequence of the functoriality of $\mathrm{St}(-)$ and $E(-)$. From 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 this exact sequence is in fact a central extension of the group $E(A)$. In particular, $K_2(A)$ is an abelian group.

Theorem 2.12 ([Mil71, Theorem 5.10])**.** *The group $K_2(A)$ is the center of the Steinberg group $\mathrm{St}(A)$.*

2.2 K_2 of fields

The group $K_2(F)$ for F a field has been extensively studied since the beginning of algebraic K-theory. If F is a number field, $K_2(F)$ contains much information about the arithmetic of F. Later on we will see a few examples of this.

When it comes to computational questions on $K_2(F)$, one rarely operates with the original Definition 2.11. The first vast simplification on the description of $K_2(F)$ is due to Matsumoto (see Theorem 2.14), which allows for the computation of K_2 of finite fields as well as K_2 of some number fields. In the computations in Chapter 3, we use only Matsumoto's theorem along with some number theory. To formulate Matsumoto's theorem, we first look at the general case of K_2 of a ring A and later specialize to the case of a field.

In order to construct elements of $K_2(A)$ for a given ring A, consider two elements $a, b \in E(A)$ such that the commutator $[a, b] = 1$. Let x, y denote representatives for $\phi^{-1}(a), \phi^{-1}(b)$, respectively. Then $[x, y] = xyx^{-1}y^{-1}$ lies in $\mathrm{St}(A)$, and by definition $\phi([x, y]) = 1$, so that $[x, y]$ is an element of $K_2(A)$. To see that the element $[x, y]$ is well defined, note that if x' is another representative for $\phi^{-1}(a)$, then $x' = xz$ for some z lying in the center of $\mathrm{St}(A)$. But then

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

since z commutes with every element of $\mathrm{St}(A)$. We therefore let $[\phi^{-1}(a), \phi^{-1}(b)]$ denote the element $[x, y]$ of $K_2(A)$ where x and y are any representatives for respectively $\phi^{-1}(a)$ and $\phi^{-1}(b)$.

Definition 2.13. Let A be a ring and $u, v \in A^\times$. We define 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 Steinberg symbols give rise to an antisymmetric bilinear map

$$\{-, -\} : A^\times \times A^\times \longrightarrow K_2(A),$$

satisfying the relation

$$\{u, 1-u\} = 1 \text{ for all } u \in A^\times \text{ with } 1 - u \in A^\times$$

[Ros94, Lemma 4.2.14, Theorem 4.2.17]. When we restrict our attention to a field F, it turns out that the group $K_2(F)$ is generated by the symbols $\{u, v\}$:

Theorem 2.14 (Matsumoto [Mil71, §12])**.** *The group $K_2(F)$ is the free abelian group on the generators $\{x, y\}$, where $x, y \in F^\times$, subject only to the following relations:*

1. *$\{x, 1 - x\} = 1$ for any $x \neq 1$;*
2. *$\{x_1x_2, y\} = \{x_1, y\}\{x_2, y\}$;*
3. *$\{x, y_1y_2\} = \{x, y_1\}\{x, y_2\}$.*

Theorem 2.15 ([Mil71, Theorem 8.8])**.** *There is an antisymmetric, bilinear pairing*

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

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

Let us proceed to describe the universal property of $K_2(F)$.

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

$$(-, -) : F^\times \times F^\times \longrightarrow G$$

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

By Matsumoto's theorem, any symbol $(-, -) : F^\times \times F^\times \to G$ gives rise to a commutative diagram

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

In other words, $K_2(F)$ is the universal object with respect to symbols on F with values in abelian groups, and the corresponding Steinberg symbol $\{-, -\}$ is the universal symbol on F.

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

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

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

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

Proof. First, note that $(1, x) = (1, x)(1, x)$ for any $x \in F^\times$ by bilinearity, hence $(1, x) = 1$. In particular, $(1, -1) = 1$ so that property (i) holds for $x = 1$. Therefore, assume that $x \neq 1$ and write $-x = (1-x)(1-x^{-1})^{-1}$. We then have

$$
\begin{aligned}
(x, -x) &= (x, 1-x)(x, (1-x^{-1})^{-1}) &(2.1)\\
&= (x, (1-x^{-1})^{-1}) &(2.2)\\
&= (x, 1-x^{-1})^{-1} &(2.3)\\
&= (x^{-1}, 1-x^{-1}) = 1, &(2.4)
\end{aligned}
$$

where the equality at (2.3) holds since $(x, 1-x^{-1})(x, (1-x^{-1})^{-1}) = (x, 1) = 1$. A similar computation shows that $(x, 1-x^{-1})^{-1} = (x^{-1}, 1-x^{-1})$.

The antisymmetry follows from (i):

$$1 = (xy, -xy) = (x, -x)(x, y)(y, x)(y, -y) = (x, y)(y, x).$$

Similarly we get property (iii):

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

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

Proof. Let u denote a generator of the cyclic group $F^\times$. If $x, y \in F^\times$, write $x = u^n$, $y = u^m$. Then in $K_2(F)$ we have

$$\{x, y\} = \{u^n, u^m\} = \{u, u\}^{nm},$$

hence it suffices to show that $\{u, u\} = 1$.

If the characteristic $\operatorname{char} F = 2$ we have $u = -u$, hence $\{u, u\} = \{u, -u\} = 1$ by Lemma 2.17 (i). We may therefore assume $\operatorname{char} F \neq 2$.

Suppose that F has order q, where q is a power of an odd prime. The set

$$A := F^\times \setminus F^{\times 2}$$

of nonsquares of $F^\times$ contains $(q-1)/2$ elements and is in bijection with the set

$$B := \{1 - v : v \in A\}.$$

Suppose that $A \cap B = \varnothing$. Since both A and B contain $(q-1)/2$ elements we can then write $F^\times$ as the disjoint union of A and B. But since 1 is a square, $1 \notin A$, and since $0 \notin A$ we have that $1 \notin B$. Hence $1 \notin A \cup B$, which contradicts the assumption that $F^\times = A \cup B$. We can therefore conclude that there are odd integers i, j such that $u^j = 1 - u^i$, and thus $1 = \{u^i, u^j\} = \{u, u\}^{ij}$. Writing $ij = 2k+1$ for k an integer we therefore get that

$$1 = \{u, u\}^{2k+1} = \{u, u\}^{2k}\{u, u\} = \{u, u\},$$

since $\{u, u\}^2 = 1$ by the antisymmetry. □

We now return to the number theoretic setting. Let F denote an algebraic number field and v a place of F. Proposition 1.49 tells us that the local Hilbert symbol at v, defined in 1.48, is in fact a symbol in the sense of Definition 2.16. Thus the same holds for the regular Hilbert symbol of Definition 1.50.

Definition 2.19. The *global regular Hilbert symbol*

$$(-,-)^{\mathrm{reg}} : F^\times \times F^\times \longrightarrow \bigoplus_{v \in \mathrm{Pl}^{\mathrm{nc}}} \mu(F_v)^{\mathrm{reg}}$$

is defined via the regular Hilbert symbols at the different places v as

$$(x, y)^{\mathrm{reg}} := ((i_v(x), i_v(y))_v^{\mathrm{reg}})_{v \in \mathrm{Pl}^{\mathrm{nc}}},$$

where v runs over all noncomplex places of F.

Note that $(x, y)^{\mathrm{reg}}$ indeed takes values in the direct sum, as $(i_v(x), i_v(y))_v^{\mathrm{reg}} = 1$ for almost all v.

With this definition $(-,-)^{\mathrm{reg}}$ becomes a symbol on $F^\times$, and it therefore factors through $K_2(F)$. We denote by h^{reg} the induced map $h^{\mathrm{reg}} : K_2(F) \to \bigoplus_v \mu(F_v)^{\mathrm{reg}}$:

$$\begin{array}{ccc} F^\times \times F^\times & \xrightarrow{\{-,-\}} & K_2(F) \\ {\scriptstyle (-,-)^{\mathrm{reg}}}\big\downarrow & \swarrow {\scriptstyle h^{\mathrm{reg}}} & \\ \bigoplus_v \mu(F_v)^{\mathrm{reg}} & & \end{array}$$

In a completely analogous manner we obtain the *global Hilbert symbol*,

$$F^\times \times F^\times \ni (x, y) \longmapsto ((i_v(x), i_v(y))_v)_{v \in \mathrm{Pl}^{\mathrm{nc}}} \in \bigoplus_{v \in \mathrm{Pl}^{\mathrm{nc}}} \mu(F_v),$$

inducing a map

$$h : K_2(F) \longrightarrow \bigoplus_{v \in \mathrm{Pl}^{\mathrm{nc}}} \mu(F_v).$$

We aim to compare the maps h and h^{reg}. To this end, we start out with a small observation before moving on to Moore's theorem.

Observation 2.20. *The Hilbert symbol can be described as*

$$\left(\frac{x, y}{v}\right) = i_v^{-1}\left((i_v(x), i_v(y))_v^{\frac{m_v}{m}}\right).$$

Proof. We have $(i_v(x), i_v(y))_v^{m_v/m} = (i_v(x)^{m_v/m}, i_v(y))_v$ by bilinearity, and

$$\left(i_v(y), F_v\left(\sqrt[m_v]{i_v(x^{m_v/m})}\right)/F_v\right) = \left(i_v(y), F_v\left(\sqrt[m]{i_v(x)}\right)/F_v\right);$$

the right hand side being the image under the local reciprocity map in L_v/F_v, where $L := F(\sqrt[m]{i_v(x)})$. Hence, letting σ denote the Hasse symbol $\sigma := \left(\frac{y, F(\sqrt[m]{x})/F}{v}\right)$, we get

$$i_v^{-1}\left((i_v(x), i_v(y))_v^{m_v/m}\right) = \frac{\sigma(\sqrt[m]{x})}{\sqrt[m]{x}} = \left(\frac{x, y}{v}\right). \qquad \square$$

Now define a map

$$\pi : \bigoplus_{v \in \mathrm{Pl}^{\mathrm{nc}}} \mu(F_v) \longrightarrow \mu(F)$$

by

$$\pi((\zeta_v)_v) := \prod_v i_v^{-1}\left(\zeta_v^{\frac{m_v}{m}}\right).$$

The above observation together with the product formula for Hilbert symbols shows that the sequence

$$K_2(F) \xrightarrow{\;h\;} \bigoplus_{v \in \mathrm{Pl}^{\mathrm{nc}}} \mu(F_v) \xrightarrow{\;\pi\;} \mu(F) \longrightarrow 1$$

is a complex. That the sequence is in fact exact is the statement of Moore's theorem, which is also known as the *reciprocity uniqueness theorem.* It says that the relation $\prod_v \left(\frac{x,y}{v}\right) = 1$ is the *only* relation between the Hilbert symbols.

Theorem 2.21 (Moore [Gra03, II Theorem 7.6]). *The sequence*

$$K_2(F) \xrightarrow{h} \bigoplus_{v \in \mathrm{Pl}^{\mathrm{nc}}} \mu(F_v) \xrightarrow{\pi} \mu(F) \longrightarrow 1$$

is exact.

Definition 2.22 ([Gra03, II 7.6.2]). The kernel of

$$h : K_2(F) \to \bigoplus_{v \in \mathrm{Pl}^{\mathrm{nc}}} \mu(F_v)$$

is called the *wild kernel*, and is denoted $WK_2(F)$. The kernel of h^{reg} is called the *regular*, or *tame* kernel, and is denoted by $R_2^{\mathrm{ord}}(F)$.

Clearly we have $WK_2(F) \subseteq R_2^{\mathrm{ord}}(F)$. In the notations of Moore's theorem we have a commutative diagram [Gra03, II Theorem 7.6]

$$\begin{array}{ccccccccccc}
1 & \longrightarrow & WK_2(F) & \longrightarrow & K_2(F) & \xrightarrow{h} & \bigoplus_{v \in \mathrm{Pl}^{\mathrm{nc}}} \mu(F_v) & \xrightarrow{\pi} & \mu(F) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow{=} & & \downarrow{\oplus m_v^1} & & \downarrow{m} & & \\
1 & \longrightarrow & R_2^{\mathrm{ord}}(F) & \longrightarrow & K_2(F) & \xrightarrow{h^{\mathrm{reg}}} & \bigoplus_{v \in \mathrm{Pl}^{\mathrm{nc}}} \mu(F)^{\mathrm{reg}} & \longrightarrow & 1 & &
\end{array}$$

Nontriviality of the regular kernel occurs for example when the prime 2 splits in the extension $F/\mathbf{Q}$. This is due to the existence of a so-called "wild" 2-adic Hilbert symbol on such a field; see Example 3.14. On the other hand, nontriviality of the wild kernel means that there are symbols on F which do not come from Hilbert symbols—i.e., symbols that are detected by global, but not by local class field theory. This means that there are global symbols defined on F which cannot be expressed in terms of the Hilbert symbols $\left(\frac{x,y}{v}\right)$ at different places v. Such symbols are called *exotic* symbols. As Gras notes in [Gra03, p.214], at the present time no one has managed to describe such a symbol explicitly. We will briefly revisit regular and wild kernels in Chapter 3.

Remark 2.23. The regular kernel $R_2^{\mathrm{ord}}(F)$ was identified by Quillen as $K_2(\mathcal{O}_F)$. The lower exact sequence in the diagram above is a special case of the localization sequence in higher algebraic K-theory [Qui73, p.29]

$$\cdots \longrightarrow K_{n+1}(F) \longrightarrow \bigoplus_{\mathfrak{p} \in \mathrm{Spec}(A) \setminus \{0\}} K_n(k(\mathfrak{p})) \longrightarrow K_n(A) \longrightarrow K_n(F) \longrightarrow \cdots$$

for A a Dedekind ring and F the field of fractions of A.

2.3 Milnor K-groups and Witt theory

In Chapter 5 we will discuss the motivic homotopy groups $\pi_{*\alpha}\mathbf{1}$ of the sphere spectrum. These groups were identified by Morel in [Mor04a] as the so-called Milnor-Witt K-groups (defined in Definition 5.6), introduced by Morel in the same article. Milnor-Witt K-theory is in some sense a blend of Milnor K-theory and Witt theory, so let us here briefly review the definition and basic properties of these objects.

Let F be a field. The Milnor K-groups were first defined in Milnor's seminal paper [Mil70], inspired by Matsumoto's description of $K_2(F)$.

For any $n \geq 0$, let $(F^\times)^{\otimes n} := F^\times \otimes_{\mathbf{Z}} \cdots \otimes_{\mathbf{Z}} F^\times$ be the n-fold tensor product of $F^\times$, where we define $(F^\times)^{\otimes 0} := \mathbf{Z}$.

Definition 2.24. Let $n \geq 0$. The *n-th Milnor K-group* $K_n^M(F)$ of F is the group

$$K_n^M(F) := (F^\times)^{\otimes n}/\langle a_1 \otimes \cdots \otimes a_n : a_j \in F^\times, a_j + a_{j+1} = 1 \text{ for some } j\rangle.$$

We write $\{a_1, \ldots, a_n\}$ for the image of $a_1 \otimes \cdots \otimes a_n \in (F^\times)^{\otimes n}$ in $K_n^M(F)$.

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

Example 2.25. Theorem 2.18 shows that $K_n^M(\mathbf{F}_q) = 0$ for any $n \geq 2$.

By Example 2.2 and Example 2.7, $K_n^M(F)$ agrees with the algebraic K-theory $K_n(F)$ for $n = 0, 1, 2$.

In [Mil70], Milnor establishes an analog of the regular map $h^{\mathrm{reg}} : K_2(F) \to \bigoplus_{v\in \mathrm{Pl}_F^{\mathrm{nc}}} k(v)^\times$ in Milnor K-theory (recall that $k(v)^\times \cong K_1(k(v))$):

Theorem 2.26 ([Mil70, Lemma 2.1])**.** *Let F be field. For each discrete valuation v on F and each $n \geq 1$ there exists a unique homomorphism*

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

such that

$$\partial_v(\{\pi_v, u_2, \ldots, u_n\}) = \{\overline{u}_2, \ldots, \overline{u}_n\} \in K_{n-1}^M(k(v))$$

and

$$\partial_v(\{u_1, u_2, \ldots, u_n\}) = 0$$

for all units $u_i \in \mathcal{O}_v^\times$.

Using these maps, Milnor showed in [Mil70] that there are split exact sequences

$$0 \longrightarrow K_n^M(F) \longrightarrow K_n^M(F(t)) \xrightarrow{\bigoplus_{\mathfrak{p}} \partial_{\mathfrak{p}}} \bigoplus_{\mathfrak{p}\in \mathrm{Spec}(F[t])\setminus\{0\}} K_{n-1}^M(F[t]/\mathfrak{p}) \longrightarrow 0,$$

where the direct sum ranges over all nonzero prime ideals of $F[t]$. Again, the method of computation is attributed to Tate.

2.3.1 The Witt ring

The following is based on [MH73, Sch85, Wei13]. Let A be a ring and let M be an A-module. A *symmetric bilinear form over A* is an A-bilinear map

$$\beta : M \times M \longrightarrow A$$

such that $\beta(x, y) = \beta(y, x)$ for all $x, y \in M$. The pair (M, β) is called a *symmetric inner product space* over A if in addition the following conditions are satisfied:

- M is finitely generated and projective over A;
- the maps $M \to M^* = \mathrm{Hom}_A(M, R)$ given by $x \mapsto \beta(x, -)$ and $y \mapsto \beta(-, y)$ are bijective (i.e., the form is nondegenerate).

A map $f : (M, \beta) \to (M', \beta')$ of inner product spaces over A is an A-module map $f : M \to M'$ such that $\beta'(f(x), f(y)) = \beta(x, y)$. Thus we can form the category $\mathrm{SBil}(A)$ of inner product spaces over A. An isomorphism in $\mathrm{SBil}(A)$ is called an *isometry*.

The category $\mathrm{SBil}(F)$ becomes symmetric monoidal under orthogonal sum defined by

$$(M, \beta) \oplus (M', \beta') := (M \oplus M', \beta \oplus \beta'),$$

where $(\beta \oplus \beta')(x \oplus x', y \oplus y') := \beta(x, y) + \beta'(x', y')$. Moreover, tensor product over A provides $\mathrm{SBil}(A)^{\mathrm{iso}}$ with the structure of a semiring. Hence the Grothendieck group $K_0\mathrm{SBil}(A)$ becomes a ring, called the *Grothendieck-Witt ring* of A. We write

$$GW(A) := K_0\mathrm{SBil}(A).$$

If $M \in \mathscr{P}(A)$, the associated *hyperbolic space* is defined as

$$\mathbf{H}(M) := (M \oplus M^*, \mathbf{h}_M),$$

where

$$\mathbf{h}_M((x,\alpha),(y,\beta)) := \beta(x) + \alpha(y).$$

The adjoint map $\widehat{\mathbf{h}}_M : M \oplus M^* \to M^* \oplus M$ of $\mathbf{h}$ is then given by $\begin{pmatrix} 0 & \mathrm{id}_{M^*} \\ \mathrm{id}_M & 0 \end{pmatrix}$.

Definition 2.27. The *Witt ring* $W(A)$ of A is the quotient of $GW(A)$ by the ideal generated by hyperbolic spaces.

There is an augmentation $\epsilon : GW(A) \to \mathbf{Z}$; this is simply the rank map. We let $\widehat{I}$ denote the kernel of ϵ. The augmentation map induces a map on the Witt ring

$$\epsilon_{\mathbf{Z}/2} : W(A) \longrightarrow \mathbf{Z}/2;$$

its kernel $I(A)$ is called the *fundamental ideal*. It is the ideal of even-dimensional forms. We have $I(A) \cong \widehat{I}$ as abelian groups, and the following diagram summarizes the situation:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \widehat{I} & \longrightarrow & GW(A) & \xrightarrow{\epsilon} & \mathbf{Z} & \longrightarrow & 0 \\ & & \downarrow{\cong} & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & I(A) & \longrightarrow & W(A) & \xrightarrow{\epsilon_{\mathbf{Z}/2}} & \mathbf{Z}/2 & \longrightarrow & 0 \end{array}$$

Example 2.28. The case when A is a field F of characteristic not 2 is perhaps the most studied. Any element $u \in F^\times$ gives rise to a symmetric inner product space $\langle u \rangle$, where $V = F$ is the underlying vector space and $\beta(x,y) := uxy$ is the bilinear form. We have $\langle u \rangle \cong \langle u' \rangle$ if and only if $u' = a^2 u$ for some $a \in F^\times$. We will write $\langle u, u' \rangle$ for the sum $\langle u \rangle \oplus \langle u' \rangle$, and we have $\langle u \rangle \otimes \langle u' \rangle = \langle uu' \rangle$.

The *hyperbolic plane* $\mathbf{H}$ is the inner product space (F^2, β), where β is given by the matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. By diagonalizing we have $\mathbf{H} = \langle 1 \rangle \oplus \langle -1 \rangle$. The hyperbolic plane generates an ideal $\langle \mathbf{H} \rangle$, which is in fact equal to $\mathbf{Z} \cdot \mathbf{H}$. The ideal $\langle \mathbf{H} \rangle$ is the ideal of hyperbolic spaces, and we have $W(F) = GW(F)/\langle \mathbf{H} \rangle$.

The need to consider Witt rings of arbitrary rings becomes apparent shortly: We shall see in Example 2.35 and Theorem 2.36 that in order to describe the Witt ring of number fields, we are forced to consider the Witt ring of the ring of integers as well as $W(\mathbf{F}_q)$ for q even.

The rings $GW(F)$ and $W(F)$ can be described by generators and relations as follows:

Theorem 2.29 ([Lam05, II Theorem 4.1])**.** *The Grothendieck-Witt ring is the free abelian group generated by symbols $\langle u \rangle$ for $u \in F^\times$, subject to the following relations.*

1. $\langle 1 \rangle = 1$,
2. $\langle u \rangle \langle v \rangle = \langle uv \rangle$,
3. $\langle u \rangle + \langle v \rangle = \langle u + v \rangle (1 + \langle uv \rangle)$

whenever they make sense. Requiring the additional relation

4. $1 + \langle -1 \rangle = 0$

one recovers the Witt ring.

The so-called *Pfister forms* are elements of the Witt ring of particular interest.

Definition 2.30. Let $a_1, \ldots, a_n \in F^\times$. The corresponding *$n$-fold Pfister form* is the 2^n-dimensional form

$$\langle\langle a_1, \ldots, a_n \rangle\rangle := \prod_{i=1}^{n} \langle 1, -a_i \rangle = (\langle 1 \rangle - \langle a_1 \rangle) \cdots (\langle 1 \rangle - \langle a_n \rangle).$$

q	$W(\mathbf{F}_q)$	$I(\mathbf{F}_q)$	$I^2(\mathbf{F}_q)$
even	$\mathbf{Z}/2$	0	0
$\equiv 1 \pmod 4$	$\mathbf{Z}/2 \oplus \mathbf{Z}/2$	$\mathbf{Z}/2$	0
$\equiv 3 \pmod 4$	$\mathbf{Z}/4$	$\mathbf{Z}/2$	0

Table 2.1: The Witt ring and the fundamental ideal of finite fields.

Proposition 2.31 ([Lam05, X Proposition 1.2])**.** *The n-th power $I^n(F)$ of the fundamental ideal of F is generated as an abelian group by all n-fold Pfister forms.*

There is a group homomorphism $F^\times/F^{\times 2} \to I(F)/I^2(F)$ induced by $u \mapsto \langle\langle u\rangle\rangle$; Pfister showed that this is an isomorphism:

Theorem 2.32 (Pfister [MH73, Theorem 5.2])**.** *There is a canonical isomorphism $F^\times/F^{\times 2} \cong I(F)/I^2(F)$.*

Example 2.33. The Witt ring of a finite field $\mathbf{F}_q$ is described in [MH73, p.87]; see Table 2.1. In particular, we have $I^2(\mathbf{F}_q) = 0$ for any prime power q.

Example 2.34. Let us consider the case of ordered fields F. Recall the inertia theorem of Jacobi and Sylvester [MH73, p.61], which says that any inner product space X over an ordered field F is isomorphic to an orthogonal sum

$$X \cong X^+ \oplus X^-,$$

where X^+ is positive definite (i.e., $x \cdot x$ is positive for all nonzero $x \in X^+$), and X^- is negative definite. Moreover, the ranks of X^+ and X^- are invariants up to isomorphism.

Suppose P is an ordering in F. In light of the inertia theorem one defines the *signature* $\sigma_P(X)$ of the inner product space X at P as the integer

$$\sigma_P(X) := \mathrm{rk}(X^+) - \mathrm{rk}(X^-).$$

For the rank 1 inner product space $\langle u\rangle$—where $u \in F^\times$—we have $\sigma_P(\langle u\rangle) = \mathrm{sgn}(u)$, the sign of u. One can show that the signature induces a well defined homomorphism on the Witt ring, and that if F is an ordered field in which all positive elements are squares, then $\sigma_P : W(F) \to \mathbf{Z}$ is an isomorphism (see [MH73, p.63]). In particular, we have $W(\mathbf{R}) \cong \mathbf{Z}$.

Example 2.35. We have the following description of the Witt ring of $\mathbf{Q}$:

$$W(\mathbf{Q}) \cong W(\mathbf{Z}) \oplus \bigoplus_{p \text{ prime}} W(\mathbf{F}_p).$$

The original proof uses the Hasse-Minkowski theorem for quadratic forms over $\mathbf{Q}$. In [MH73, pp.88–89], Milnor gives an alternative proof not making use of the Hasse-Minkowski principle. This proof is quite similar to Tate's computation of $K_2(\mathbf{Q})$, which we will come back to in Chapter 3.

There are analogs of the tame symbols also in Witt theory: If F is a number field, each finite place $v \in \mathrm{Pl}_F$ and each choice of uniformizer π_v gives rise to an additive homomorphism

$$\partial_v^{\pi_v} : W(F) \longrightarrow W(k(v))$$

sending a generator $\langle u\pi_v^n\rangle$ of $W(F)$ to either $\langle \overline{u}\rangle$ or 0 according as $n \equiv 1 \pmod 2$ or $n \equiv 0 \pmod 2$. The map $\partial_v^{\pi_v}$ is unique up to choice of uniformizer π_v.

Theorem 2.36 ([MH73, IV Corollary 3.3])**.** *If F is a number field, there is an exact sequence*

$$0 \longrightarrow W(\mathcal{O}_F) \longrightarrow W(F) \xrightarrow{\bigoplus_v \partial_v^{\pi_v}} \bigoplus_{v \in \mathrm{Pl}_0} W(k(v)).$$

The extent to which $\partial := \bigoplus_v \partial_v^{\pi_v}$ fails to be surjective is measured by the ideal class group:

Proposition 2.37 ([MH73, p.94])**.** *There is an exact sequence*

$$W(F) \xrightarrow{\partial} \bigoplus_{v\in \mathrm{Pl}_0} W(k(v)) \longrightarrow \mathrm{Cl}(F)/\,\mathrm{Cl}(F)^2 \longrightarrow 0,$$

where the map $\bigoplus_v W(k(v)) \to \mathrm{Cl}(F)/\,\mathrm{Cl}(F)^2$ *is defined by sending each generator* $\langle \overline{u}\rangle$ *of* $W(k(v))$ *to the ideal class of* $\mathfrak{p}_v$ *modulo* $\mathrm{Cl}(F)^2$*.*

Example 2.38. If F equals $\mathbf{Q}(i)$ or $\mathbf{Q}(\sqrt{-3})$ then $\mathrm{Cl}(F) = 0$, hence we have exact sequences

$$0 \longrightarrow W(\mathcal{O}_F) \longrightarrow W(F) \xrightarrow{\partial} \bigoplus_{v\in \mathrm{Pl}_0} W(k(v)) \longrightarrow 0.$$

In [MH73, p.96], Milnor and Husemoller describe the groups $W(\mathcal{O}_{\mathbf{Q}(\sqrt{-d})})$ for $d = 1, 2, \ldots, 15$. In our case, the result is

$$W(\mathbf{Z}[i]) \cong \mathbf{Z}/2 \oplus \mathbf{Z}/2; \qquad W(\mathbf{Z}[\omega]) \cong \mathbf{Z}/4.$$

2.3.2 Relation to Milnor K-theory

Let $k_n^M(F)$ denote the mod 2 Milnor K-theory

$$k_n^M(F) := K_n^M(F)/2K_n^M(F).$$

Thus we have $k_0^M(F) = \mathbf{Z}/2$ and $k_1^M(F) = F^\times/F^{\times 2}$, the square classes of elements in $F^\times$. By definition of the fundamental ideal we have $W(F)/I(F) \cong k_0^M(F)$, and by Pfister's Theorem 2.32 we have $I(F)/I^2(F) \cong k_1^M(F)$.

In [Mil70], Milnor establishes a unique homomorphism

$$s_n : k_n^M(F) \longrightarrow I^n(F)/I^{n+1}(F)$$

for each $n \geq 0$, induced by

$$\{a_1, \ldots, a_n\} \longmapsto \langle\!\langle a_1, \ldots, a_n \rangle\!\rangle \pmod{I^{n+1}(F)}.$$

He proved that s_n is surjective for all values of n and announced the famous *Milnor conjecture*, asking whether s_n is always bijective.

Before Milnor's article [Mil70], Bass and Tate had discovered some connections between K_2 and Galois cohomology [Tat76b]. Let F be a field of characteristic not 2, and let F_{sep} denote its separable closure. We then have the Kummer sequence

$$1 \longrightarrow \mu_2 \longrightarrow F_{\mathrm{sep}}^\times \xrightarrow{(-)^2} F_{\mathrm{sep}}^\times \longrightarrow 1.$$

The start of the corresponding long exact sequence in Galois cohomology takes the form

$$0 \longrightarrow \mathbf{Z}/2 \longrightarrow F^\times \xrightarrow{\cdot 2} F^\times \xrightarrow{\delta} H^1_{\mathrm{Gal}}(F; \mathbf{Z}/2) \longrightarrow 0.$$

Here $H^n_{\mathrm{Gal}}(F; M) := H^n(\mathrm{Gal}(F_{\mathrm{sep}}/F); M) = H^n_{\text{ét}}(F; M)$, and $H^1_{\mathrm{Gal}}(F; F_{\mathrm{sep}}^\times) = 0$ by the Hilbert-Speiser-Noether Theorem 90 [Ser79, Ch.X]. Hence there is an isomorphism

$$k_1^M(F) \cong H^1_{\mathrm{Gal}}(F; \mathbf{Z}/2).$$

Theorem 2.39 ([Tat76b, Theorem 3.1])**.** *The isomorphism*

$$\{a\} \mapsto \delta(a) : k_1^M(F) \longrightarrow H^1_{\mathrm{Gal}}(F; \mathbf{Z}/2)$$

extends uniquely to a ring homomorphism

$$h_F : k_*^M(F) \longrightarrow H^*_{\mathrm{Gal}}(F; \mathbf{Z}/2)$$

satisfying $h_F(\{a, b\}) = \delta(a) \smile \delta(b)$*.*

In 1996—by the advent of motivic homotopy theory—Orlov-Vishik-Voevodsky brought clarity to all the connections mentioned above. Indeed, they settled the Milnor conjecture by showing that s_* as well as h_* are graded ring isomorphisms [OVV07]

$$\begin{array}{ccc} & k^M_*(F) & \\ {\scriptstyle s_*}\swarrow\cong & & \cong\searrow{\scriptstyle h_*} \\ \mathrm{Gr}_I(W(F)) & \longrightarrow & H^*_{\mathrm{Gal}}(F;\mathbf{Z}/2) \end{array}$$

where $\mathrm{Gr}_I(W(F)) := W(F)/I(F) \oplus I(F)/I^2(F) \oplus \cdots$ is the associated graded Witt ring. Every known proof of this fact uses motivic homotopy theory.

CHAPTER 3

On K_2 of Some Imaginary Quadratic Number Fields

In this chapter we look at the K-theory of the two imaginary quadratic number fields $\mathbf{Q}(\sqrt{-1})$ and $\mathbf{Q}(\sqrt{-3})$. Specifically, we compute K_2 of these fields and look at how the result for $\mathbf{Q}(\sqrt{-1})$ is connected with the law of biquadratic reciprocity.

In Tate's computation of $K_2(\mathbf{Q})$ he defined a filtration

$$L_2 \subseteq L_3 \subseteq L_5 \subseteq \cdots \subseteq L_p \subseteq \cdots \subseteq K_2(\mathbf{Q})$$

of $K_2(\mathbf{Q})$, where for each prime p,

$$L_p := \langle \{x, y\} : x, y \in \mathbf{Z} \setminus \{0\}, 1 \leq |x|, |y| \leq p \rangle.$$

Tate used induction and the Euclidean algorithm to show that $L_p \cong \mu_2 \bigoplus_{2<\ell\leq p} \mathbf{F}_\ell^\times$, yielding

$$K_2(\mathbf{Q}) \cong \mu_2 \oplus \bigoplus_{p\neq 2} \mathbf{F}_p^\times.$$

We aim to follow the same technique, only with slight modifications. In particular, the filtration has to be defined differently due to the fact that there may be two primes with the same norm in these number fields. Since we want to consider each prime separately, the norm is not sufficient to distinguish between them.

Now the groups $K_2(\mathbf{Q}(\sqrt{-1}))$ and $K_2(\mathbf{Q}(\sqrt{-3}))$ are of course known, e.g., from [BT73, p.429] where Tate computes the second K-group of the first six imaginary quadratic number fields (ordered by their discriminants). Tate's method of computation is based on a few general results; here we will instead—as mentioned—give a direct computation based on the calculation of $K_2\mathbf{Q}$ mentioned above. This approach should work for all Euclidean imaginary quadratic number fields, but not in general because of the need of an Euclidean algorithm. However, the computation exemplifies how the arithmetic of the number field reveals itself in the K-group.

3.1 The group $K_2(\mathbf{Q}(\sqrt{-1}))$

Recall the situation from Chapter 2 for the global regular Hilbert symbol:

$$\begin{array}{ccc} F^\times \times F^\times & \xrightarrow{\{-,-\}} & K_2(F) \\ {\scriptstyle (-,-)^{\mathrm{reg}}}\downarrow & \swarrow{\scriptstyle h^{\mathrm{reg}}} & \\ \bigoplus_v \mu(F_v)^{\mathrm{reg}} & & \end{array}$$

Here we specialize to the case when $F = \mathbf{Q}(i)$, where $i^2 = -1$. Thus we have $\mathcal{O}_{\mathbf{Q}(i)} = \mathbf{Z}[i]$, the Gaussian integers. The map $h^{\mathrm{reg}} : K_2(\mathbf{Q}(i)) \to \bigoplus_v \mu(\mathbf{Q}(i)_v)^{\mathrm{reg}}$ will be our primary object of study.

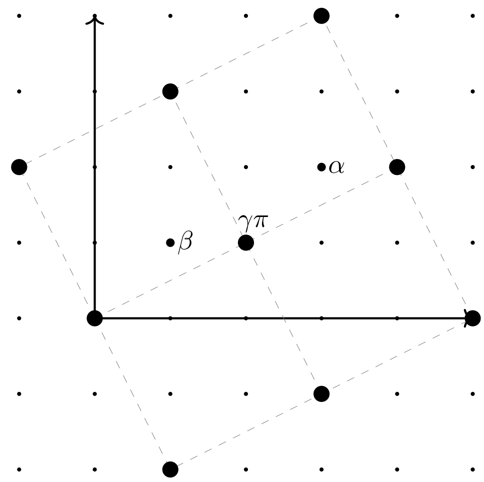


Figure 3.1: Gaussian integers lying in the same relative position in the squares defined by π are congruent modulo π.

First recall—as mentioned in Chapter 1—that if v is a finite place of $\mathbf{Q}(i)$ above a prime $p \in \mathbf{Z}$, then $\mathbf{Q}(i)_v = \mathbf{Q}_p(i)$. Secondly, recall that we in Proposition 1.20 have described the groups $(\mathbf{Z}[i]/\mathfrak{p}_v)^\times \cong k(v)^\times \cong \mu(\mathbf{Q}(i)_v)^{\mathrm{reg}}$, so that we have a map

$$h^{\mathrm{reg}} : K_2(\mathbf{Q}(i)) \longrightarrow \bigoplus_{\substack{p \text{ prime} \\ p \equiv 1 \ (\mathrm{mod}\ 4)}} \left(\mathbf{F}_p^\times\right)^2 \oplus \bigoplus_{\substack{p \text{ prime} \\ p \equiv 3 \ (\mathrm{mod}\ 4)}} \mathbf{F}_{p^2}^\times$$

induced by the global regular Hilbert symbol. We aim to show that this is an isomorphism. To begin with we need a few preliminary lemmas.

Lemma 3.1. *For any finite place v of $\mathbf{Q}(i)$, there is a complete system of representatives $\{\alpha_j\}_{j=1,\dots,\mathrm{Nm}(\pi_v)}$ for $k(v)$ such that $|\alpha_j| \le |\pi_v|/\sqrt{2}$ for each j (where $|\alpha|$ is the standard absolute value of α, satisfying $|\alpha|^2 = \mathrm{Nm}(\alpha)$).*

Proof. This is the Euclidean algorithm on the Gaussian integers and follows from Table 1.1 in Chapter 1, but we write out the details for convenience. Geometrically we can picture the situation as follows (see Figure 3.1): Given $\alpha \in \mathbf{Z}[i] \setminus \{0\}$ and π a prime element, consider the lattice spanned by unit multiples of π. Then α lies in one of the squares in the lattice, with distance at most $|\pi|/\sqrt{2}$ from a corner $\gamma\pi$. If $\beta := \alpha - \gamma\pi$ then $\beta \equiv \alpha \ (\mathrm{mod}\ \pi)$ and $|\beta| \le |\pi|/\sqrt{2}$. □

Lemma 3.2. *The group $K_2(\mathbf{Q}(i))$ is generated by elements $\{\alpha, \beta\}$ for which $\alpha, \beta \in \mathbf{Z}[i] \setminus \{0\}$.*

Proof. Let $\{x, y\} \in K_2(\mathbf{Q}(i))$, then we may write $x = \alpha/\beta$, $y = \alpha'/\beta'$ for $\alpha, \alpha', \beta, \beta' \in \mathbf{Z}[i]$ nonzero. Using the relations in Lemma 2.17 and bilinearity we then have

$$\begin{aligned}\{x, y\} &= \{\alpha\beta^{-1}, \alpha'\beta'^{-1}\} \\ &= \{\alpha, \alpha'\}\{\alpha, \beta'^{-1}\}\{\beta^{-1}, \alpha'\}\{\beta^{-1}, \beta'^{-1}\} \\ &= \{\alpha, \alpha'\}\{\beta', \alpha\}\{\alpha', \beta\}\{\beta, \beta'\},\end{aligned}$$

where we have used that $\{\gamma^{-1}, \delta\} = \{\gamma, \delta\}^{-1} = \{\delta, \gamma\}$. □

Remark 3.3. The same proof holds for $K_2(F)$ whenever F is the quotient field of some integral domain.

Definition 3.4. Let Λ_∞ denote the following subgroup of $K_2(\mathbf{Q}(i))$:

$$\Lambda_\infty := \langle \{u, v\} : u, v \in \mathbf{Z}[i]^\times = \mu_4 \rangle.$$

Lemma 3.5. *The group Λ_∞ is trivial.*

Proof. The generators of Λ_∞ are of the form $\{u, v\}$ with $u, v \in \mathbf{Z}[i]^\times$. First, note that if either $u = 1$ or $v = 1$, then $\{u, v\} = 1$ by the bilinearity. We consider the remaining cases:

- We already know that $\{i, -i\} = 1$ by the symbol properties. Therefore also $\{-i, i\} = \{i, -i\}^{-1} = 1$.
- Again by the relations in 2.17 we have $\{i, -1\} = \{i, i\}$. But $\{i, i\}\{i, i\} = \{i, -1\} = \{i, i\}$, hence $\{i, i\} = 1 = \{i, -1\}$ and also $\{-1, i\} = 1$.
- For the element $\{-1, -1\}$ we now get $\{-1, -1\} = \{i^2, -1\} = \{i, -1\}\{i, -1\} = 1$.
- Similarly as above we have that $\{-i, -1\} = \{-i, -i\}$ and

$$\{-i, -i\}\{-i, -i\} = \{-i, -1\} = \{-i, -i\},$$

hence $\{-i, -i\} = 1$ and therefore also $\{-i, -1\} = \{-1, -i\} = 1$. □

We aim to define a filtration of $K_2(\mathbf{Q}(i))$ indexed by the Gaussian primes. To start out, let us list the finite places of $\mathbf{Q}(i)$ by increasing norm:

$$\mathrm{Pl}_0 = \{v_1, v_2, \dots \mid \mathrm{Nm}(\pi_{v_n}) \leq \mathrm{Nm}(\pi_{v_{n+1}}) \quad \forall n\}.$$

Definition 3.6. Let Pl_0 be enumerated as above. For all $n \geq 1$, let

$$S_n := \{v_1, v_2, \dots, v_n\} \subseteq \mathrm{Pl}_0\,.$$

Following the notation of Tate in [BT73], let $K_2^{S_n}\mathbf{Q}(i)$ denote the following subgroup of $K_2\mathbf{Q}(i)$:

$$K_2^{S_n}\mathbf{Q}(i) := \left\langle \{\alpha, \beta\} \in K_2\mathbf{Q}(i) : \alpha, \beta \in \mathbf{Z}[i]_{S_n}^\times \right\rangle,$$

where

$$\mathbf{Z}[i]_{S_n} = \mathbf{Z}\left[i, \frac{1}{\pi_{v_1}}, \dots, \frac{1}{\pi_{v_n}}\right]$$

is the ring of Gaussian S_n-integers.

The groups $K_2^{S_n}\mathbf{Q}(i)$ then form a filtered system and thus we have $K_2\mathbf{Q}(i) = \varinjlim_n K_2^{S_n}\mathbf{Q}(i)$.

Theorem 3.7. *The global regular Hilbert symbol induces an isomorphism*

$$K_2(\mathbf{Q}(i)) \cong \bigoplus_{v \in \mathrm{Pl}^{\mathrm{nc}}_{\mathbf{Q}(i)}} k(v)^\times \cong \bigoplus_{\substack{p \text{ prime} \\ p \equiv 1 \ (\mathrm{mod}\ 4)}} \left(\mathbf{F}_p^\times\right)^2 \oplus \bigoplus_{\substack{p \text{ prime} \\ p \equiv 3 \ (\mathrm{mod}\ 4)}} \mathbf{F}_{p^2}^\times.$$

Proof. We will use induction to show that for any $n \geq 1$, the restriction of h^{reg} to $K_n^{S_n}\mathbf{Q}(i)$ yields an isomorphism $K_n^{S_n}\mathbf{Q}(i) \cong \bigoplus_{j=1}^n k(v_j)^\times$. To begin with we must show that $K_2^{S_1}\mathbf{Q}(i)$ is trivial. Note that $S_1 = \{v_1\}$, where v_1 is the place above $2 \in \mathbf{Z}$, and that the Gaussian S_1-units consist of the torsion part μ_4, and a free part generated by $1 + i$.

Using bilinearity, Lemma 3.5 and the relation $\{x, -1\} = \{x, x\}$, we need only consider the generating symbols $\{\alpha, \beta\} \in K_2^{S_1}\mathbf{Q}(i)$ where $\alpha, \beta = i, 1 + i$. From the proof of Lemma 3.5 we already know that $\{i, i\} = 1$, thus it remains to check the elements $\{1 + i, i\}$, $\{i, 1 + i\}$ and $\{1 + i, 1 + i\}$. But by the Steinberg relation we have

$$\{-i, 1 + i\} = 1.$$

Hence

$$1 = \{-i, 1 + i\} = \{-1, 1 + i\}\{i, 1 + i\},$$

and therefore

$$\{1 + i, i\} = \{-1, 1 + i\} = \{1 + i, 1 + i\}.$$

But then $\{1+i, i\} = \{i, 1+i\}$ and

$$\{i, 1+i\} = \{1+i, i\} = \{-1, 1+i\} = \{i, 1+i\}\{i, 1+i\},$$

hence $\{i, 1+i\} = 1$. In total we have

$$1 = \{i, 1+i\} = \{1+i, i\} = \{1+i, 1+i\},$$

so $K_2^{S_1}\mathbf{Q}(i)$ is trivial—in other words $K_2^{S_1}\mathbf{Q}(i) \cong k(v_1)^\times$.

Lemma 3.8. *For any $n \geq 1$, the quotient group $K_2^{S_{n+1}}\mathbf{Q}(i)/K_2^{S_n}\mathbf{Q}(i)$ is isomorphic to $k(v_{n+1})^\times$*

Proof. Define a map

$$\phi : k(v_{n+1})^\times \longrightarrow K_2^{S_{n+1}}\mathbf{Q}(i)/K_2^{S_n}\mathbf{Q}(i)$$

by

$$\overline{\alpha} \longmapsto \{\alpha, \pi\} \pmod{K_2^{S_n}\mathbf{Q}(i)},$$

where $\pi := \pi_{v_{n+1}}$, and where we may assume $\mathrm{Nm}(\alpha) \leq \mathrm{Nm}(\pi)/2$ by Lemma 3.1. To show that ϕ is a well defined homomorphism, assume $\alpha\beta \equiv \gamma \pmod{\pi}$, say $\alpha\beta = \gamma + \delta\pi$, where $|\alpha|, |\beta|, |\gamma| \leq |\pi|/\sqrt{2}$. Then

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

thus $|\delta| \leq |\pi|/2 + 1/\sqrt{2}$, which is less than $|\pi|$ since $\mathrm{Nm}(\pi) > 2$. Hence $\mathrm{Nm}(\delta) < \mathrm{Nm}(\pi)$, so that $\overline{\delta} \in k(v_{n+1})^\times$. Now compute

$$\begin{aligned} 1 &= \left\{\frac{\gamma}{\alpha\beta}, 1 - \frac{\gamma}{\alpha\beta}\right\} \\ &= \left\{\frac{\gamma}{\alpha\beta}, \frac{\delta\pi}{\alpha\beta}\right\} \\ &= \{\gamma, \delta\}\{\gamma, \pi\}\{\alpha\beta, \gamma\}\{\delta, \alpha\beta\}\{\pi, \alpha\beta\}\{\alpha\beta, \alpha\beta\} \\ &\equiv \{\gamma, \pi\}\{\pi, \alpha\beta\} \pmod{K_2^{S_n}\mathbf{Q}(i)}, \end{aligned}$$

where the last congruence holds since α, β, γ and δ all have norms bounded by $\mathrm{Nm}(\pi)$. Hence, modulo $K_2^{S_n}\mathbf{Q}(i)$ we have $\{\alpha\beta, \pi\} = \{\gamma, \pi\}$, which means that ϕ is multiplicative, and also well defined by taking $\beta = 1$.

Furthermore we have that ϕ is surjective. Indeed, the group $K_2^{S_{n+1}}\mathbf{Q}(i)$ is generated by the elements of $K_2^{S_n}\mathbf{Q}(i)$ in addition to the symbols $\{\alpha, \pi\}$ where α is a Gaussian S_n-unit (remember that $\{\pi, \pi\} = \{-1, \pi\}$). This means that $\overline{\alpha} \in k(v_{n+1})^\times$ and $\phi(\overline{\alpha}) = \{\alpha, \pi\}$, hence ϕ is surjective and $\#(K_2^{S_{n+1}}\mathbf{Q}(i)/K_2^{S_n}\mathbf{Q}(i)) \leq \mathrm{Nm}(\pi) - 1$.

Now let $\overline{\zeta}$ denote a generator for the cyclic group $k(v_{n+1})^\times$. By Proposition 1.52 we then have that

$$(\zeta, \pi)^{\mathrm{reg}}_{v_{n+1}} = \overline{\zeta} \in k(v_{n+1})^\times.$$

But

$$(\zeta, \pi)^{\mathrm{reg}} = h^{\mathrm{reg}}(\{\zeta, \pi\}),$$

hence $\{\zeta, \pi\}$ has order $\mathrm{Nm}(\pi)-1$ in $K_2^{S_{n+1}}\mathbf{Q}(i)/K_2^{S_n}\mathbf{Q}(i)$. Therefore the group $K_2^{S_{n+1}}\mathbf{Q}(i)/K_2^{S_n}\mathbf{Q}(i)$ also has order at least $\mathrm{Nm}(\pi)-1$. By the above inequality, its order must be exactly $\mathrm{Nm}(\pi)-1$, hence ϕ is an isomorphism. □

To conclude the proof, let $n \geq 1$ and assume by induction that $K_2^{S_n}\mathbf{Q}(i) \cong \bigoplus_{j=1}^{n} k(v_j)^\times$ via h^{reg}. We must show that h^{reg} yields an isomorphism

$$K_2^{S_{n+1}}\mathbf{Q}(i) \cong \bigoplus_{j=1}^{n+1} k(v_j)^\times.$$

If an element $x \in K_2^{S_{n+1}}\mathbf{Q}(i)$ maps to 1 under h^{reg}, Lemma 3.8 states that $x \in K_2^{S_n}\mathbf{Q}(i)$, and so $x = 1$ by induction. Similarly, if $u = (u_j)_{j=1}^{n+1} \in \bigoplus_{j=1}^{n+1} k(v_j)^\times$, we can find an element in $K_2^{S_{n+1}}\mathbf{Q}(i)$ mapping to u_{n+1} by Lemma 3.8. By the induction hypothesis there is an element in $K_2^{S_n}\mathbf{Q}(i)$ mapping to $(u_j)_{j=1}^{n}$, and so the product of these elements constitutes a suitable preimage of u. $\square$

3.1.1 Connection with biquadratic reciprocity

Let us show how the structure of $K_2(\mathbf{Q}(i))$ is related to the law of biquadratic reciprocity. By Theorem 3.7 there exist maps $\psi_v : k(v)^\times \to \mu_4$ for all $v \nmid 2$ such that the Hilbert symbol at the place $(1+i)$ factors through $\bigoplus_{v\nmid 2} k(v)^\times$ via these maps:

$$\begin{array}{ccc} \mathbf{Q}(i)^\times \times \mathbf{Q}(i)^\times & \xrightarrow{(-,-)^{\mathrm{reg}}} & \bigoplus_{v\nmid 2} k(v)^\times \\ \left(\frac{-,-}{(1+i)}\right)_4 \Big\downarrow & \swarrow \prod \psi_v & \\ \mu_4 & & \end{array}$$

In other words, for all $x, y \in \mathbf{Q}(i)^\times$ we have

$$\left(\frac{x,y}{(1+i)}\right)_4 = \prod_{v\nmid 2} \psi_v((x,y)_v^{\mathrm{reg}}).$$

Lemma 3.9. *Let v be a finite place of $\mathbf{Q}(i)$ not lying above 2. If f is a map $f : k(v)^\times \to \mu_4$, then f satisfies*

$$f(x) \equiv x^{\frac{q_v-1}{4}\delta} \pmod{\mathfrak{p}_v},$$

where $\delta \in \{0,1,2,3\}$ and $q_v = \mathrm{Nm}(\mathfrak{p}_v)$.

Proof. Write $q := q_v$. In the following, we abuse notation by identifying elements with their image in $k(v)^\times$.

The map f is determined by where a generator of the cyclic group $k(v)^\times$ is sent. If ζ denotes a generator for $k(v)^\times$, then clearly $\zeta^{\frac{q-1}{4}}$ equals i or $-i$, for if $\zeta^{\frac{q-1}{4}} \in \mu_2$ then ζ is a square or a fourth power.

Assume first that $f(\zeta) = i$. We consider two cases.

1. If $\zeta^{\frac{q-1}{4}} = i$, then $f(x) = x^{\frac{q-1}{4}}$ since their action on the generator coincide.
2. If $\zeta^{\frac{q-1}{4}} = -i$, then $\zeta^{3\frac{q_v-1}{4}} = i$, hence $f(x) = x^{3\frac{q-1}{4}}$.

Now if $f(\zeta) = i^\delta$, where $\delta \in \{0,1,2,3\}$, then in case 1 above we have $f(x) = x^{\frac{q-1}{4}\delta}$ for any $x \in k(v)^\times$, and in case 2 we get

$$f(x) = \left(x^{\frac{q-1}{4}}\right)^{3\delta} = x^{\frac{q-1}{4}\delta'}$$

for $\delta' \in \{0,1,2,3\}$ with $\delta' \equiv \delta \pmod 4$. $\square$

Note that, by Proposition 1.52 and Observation 2.20,

$$\left(\frac{a,b}{v}\right)_n \equiv ((a,b)_v^{\mathrm{reg}})^{\frac{q_v-1}{n}} \pmod{\mathfrak{p}_v}.$$

Thus, by applying the above lemma to the maps ψ_v above we get the relation of Hilbert symbols

$$\left(\frac{x,y}{(1+i)}\right)_4 = \prod_{v\nmid 2} ((x,y)_v^{\mathrm{reg}})^{\frac{q_v-1}{4}\delta_v} = \prod_{v\nmid 2} \left(\frac{x,y}{v}\right)_4^{\delta_v},$$

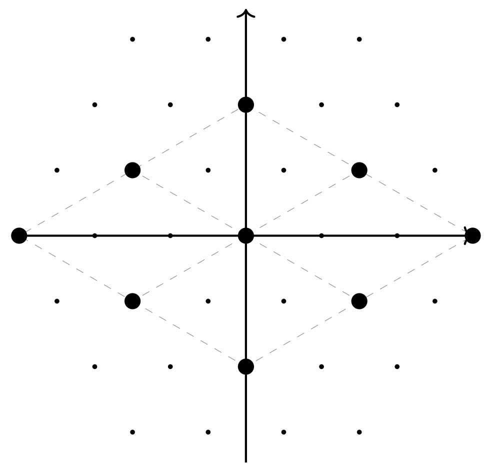


Figure 3.2: Lattice spanned by unit multiples of an Eisenstein prime.

where $\delta_v \in \{0, 1, 2, 3\}$ for all $v \nmid 2$. In other words, the structure of the group $K_2(\mathbf{Q}(i))$ *gives rise to a relation between Hilbert symbols of order* 4. But Moore's theorem says that there is only one relation of Hilbert symbols, hence we must have $\delta_v = 1$ for all $v \nmid 2$. Since $\left(\frac{x,y}{(1+i)}\right)_4$ takes values in $\{\pm 1\}$, we have thus obtained the product formula for Hilbert symbols

$$\prod_{v \in \mathrm{Pl}^{\mathrm{nc}}_{\mathbf{Q}(i)}} \left(\frac{x, y}{v}\right)_4 = 1,$$

which implies the biquadratic reciprocity law, as we have seen in Chapter 1.

3.2 The group $K_2(\mathbf{Q}(\sqrt{-3}))$

Now we turn to the case $F = \mathbf{Q}(\sqrt{-3}) = \mathbf{Q}(\omega)$, so that $\mathcal{O}_F = \mathbf{Z}[\omega]$, the Eisenstein integers. Here $\omega = \zeta_3 = (-1 + \sqrt{-3})/2$ is a primitive third root of unity. Again we consider the map

$$h^{\mathrm{reg}} : K_2\mathbf{Q}(\omega) \longrightarrow \bigoplus_{v \in \mathrm{Pl}^{\mathrm{nc}}_{\mathbf{Q}(\omega)}} k(v)^\times$$

induced by the global regular Hilbert symbol.

Definition 3.10. Let Λ_∞ denote the subgroup of $K_2\mathbf{Q}(\omega)$ generated by the elements $\{u, v\}$ for which $u, v \in \mathbf{Z}[\omega]^\times = \mu_6 = \{\pm 1, \pm\omega, \pm\omega^2\}$.

Lemma 3.11. *We have* $\Lambda_\infty = 1$.

Proof. Note that, by using bilinearity and the relations for Steinberg symbols, any element $\{u, v\}$ for which $u, v \in \{-1, \pm\omega, \pm\omega^2\}$ is a product of the symbols $\{\omega, \omega\}$, $\{-1, -1\}$. We check that these are trivial. Recall that $\omega^{-1} = \omega^2$ and that $1 + \omega + \omega^2 = 0$ in the following.

- We have
$$\{\omega, \omega^2\} = \{\omega, \omega\}\{\omega, \omega\},$$
but also
$$\{\omega, \omega^2\} = \{\omega, \omega^{-1}\} = \{\omega, \omega\}^{-1} = \{\omega, \omega\},$$
hence $\{\omega, \omega\} = 1$.

- Note that
$$1 = \{-\omega, 1 + \omega\} = \{-1, 1 + \omega\}\{\omega, 1 + \omega\}$$

by the Steinberg relation, hence

$$\{1+\omega, 1+\omega\} = \{-1, 1+\omega\} = \{1+\omega, \omega\}.$$

Using that $1+\omega = -\omega^2$, this yields

$$\{1+\omega, \omega\} = \{-1, \omega\}\{\omega^2, \omega\} = \{\omega, \omega\}\{\omega, \omega\}^2 = 1.$$

Hence we get

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

which concludes the proof. □

As in Section 3.1 we now order the noncomplex places of $\mathbf{Q}(\omega)$ by increasing norm,

$$\mathrm{Pl}^{\mathrm{nc}}_{\mathbf{Q}(\omega)} = \mathrm{Pl}_0 = \{v_1, v_2, \ldots \,|\, \mathrm{Nm}(\pi_{v_n}) \leq \mathrm{Nm}(\pi_{v_{n+1}}) \quad \forall n\},$$

and we let $K_2^{S_n}\mathbf{Q}(\omega)$ denote the subgroup of $K_2\mathbf{Q}(\omega)$ generated by elements $\{u, v\}$ for u, $v \in \mathbf{Z}[\omega]^{\times}_{S_n}$. Here S_n denotes as usual the set $S_n = \{v_1, \ldots, v_n\}$ of the first n places of $\mathbf{Q}(\omega)$ of smallest norm.

By Proposition 1.26, $\mathbf{Q}(\omega)/\mathbf{Q}$ is ramified only at 3, hence the smallest value for $\mathrm{Nm}\,\pi_v$ is 3. Thus v_1 is the place corresponding to the prime ideal $(2+\omega)$, and by Proposition 1.27 we have $k(v_1) \cong \mathbf{F}_3$.

Lemma 3.12. *We have* $K_2^{S_1}\mathbf{Q}(\omega) \cong k(v_1)^{\times} \cong \mathbf{F}_3^{\times}$.

Proof. We claim that the element $x := \{-1, 2+\omega\} = \{2+\omega, 2+\omega\}$ is the only nontrivial element in $K_2^{S_1}\mathbf{Q}(\omega)$. Note that

$$x^2 = \{-1, 2+\omega\}^2 = \{1, 2+\omega\} = 1,$$

so this element has order 2. Computing the regular symbol at v_1 yields

$$(-1, 2+\omega)^{\mathrm{reg}}_{v_1} \equiv -1 \pmod{\mathfrak{p}_{v_1}}$$

by Proposition 1.52. Since the regular symbol factors through $K_2\mathbf{Q}(\omega)$, it follows that x is nontrivial.

To conclude we must show that the rest of the symbols in $K_2^{S_1}\mathbf{Q}(\omega)$ are trivial. Using Lemma 3.11 along with bilinearity and antisymmetry, we see that it is enough to show that $\{2+\omega, \omega\} = 1$. To this end, note that since $2+\omega = 1-\omega^2$, the Steinberg relation yields

$$\{\omega^2, 2+\omega\} = 1.$$

Using that $\omega = \omega^{-2}$, we thus get

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

□

Theorem 3.13. *The global regular Hilbert symbol induces an isomorphism*

$$K_2(\mathbf{Q}(\omega)) \cong \bigoplus_{v \in \mathrm{Pl}^{\mathrm{nc}}_{\mathbf{Q}(\omega)}} k(v)^{\times} \cong \mathbf{F}_3^{\times} \oplus \bigoplus_{p \equiv 1 \pmod 3} (\mathbf{F}_p^{\times})^2 \oplus \bigoplus_{p \equiv 2 \pmod 3} \mathbf{F}_{p^2}^{\times}.$$

Proof. We proceed in the same manner as in Theorem 3.7, i.e., we use induction to prove that $K_2^{S_n}\mathbf{Q}(\omega) \cong \bigoplus_{j=1}^{n} k(v_j)^\times$. Lemma 3.12 furnishes the base case of the induction. For the induction step, we will again show that the map

$$\phi : k(v_{n+1})^\times \longrightarrow K_2^{S_{n+1}}\mathbf{Q}(\omega)/K_2^{S_n}\mathbf{Q}(\omega)$$

defined by

$$\phi(\overline{\alpha}) := \{\alpha, \pi\} \pmod{K_2^{S_n}\mathbf{Q}(\omega)}$$

is a well defined isomorphism, where $\pi := \pi_{v_{n+1}}$. Here α is to vary between all Eisenstein integers of norm bounded by $\mathrm{Nm}(\pi)/3$. This assumption can be made thanks to the Euclidean algorithm on $\mathbf{Z}[\omega]$ and Table 1.1, just as in Lemma 3.1.

To show ϕ is a well defined homomorphism, we proceed as before: If $\alpha\beta = \gamma + \pi\delta$ with $|\alpha|$, $|\beta|$, $|\gamma| \leq |\pi|/\sqrt{3}$, then

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

hence

$$|\delta| \leq \frac{|\pi|}{3} + \frac{1}{\sqrt{3}} < |\pi|.$$

An identical computation as the one done in the proof of Theorem 3.7 yields that ϕ is well defined and multiplicative. The proof of the bijectivity also follows from the same argument as we have seen. □

3.3 Tame and wild kernels, exotic symbols

In Section 2.2 we defined regular—or tame—kernels as well as the wild kernel (see Definition 2.22). The wild kernel $WK_2(F)$ was shown by Bass and Tate to always be finitely generated [Tat71]. Here F can be any field. A deep theorem of Garland established that in the case when F is a number field, $WK_2(F)$ is in fact finite [Gar71].

The tame and wild kernels encode deep arithmetic information about the number field F. For example, as conjectured by Birch-Tate and proved by Mazur-Wiles-Kolyvagin, if $F/\mathbf{Q}$ is a totally real abelian extension we have the expression [Gra03, II Remark 7.8.2]

$$\# R_2^{\mathrm{ord}}(F) = \frac{w_2}{2^{[K:\mathbf{Q}]}}|\zeta_F(-1)|.$$

Here ζ_F is the Dedekind zeta-function of F, and w_2 is the largest integer n such that $\mathrm{Gal}(F(\mu_n)/F)$ is killed by 2 [Wei13, p.516].

The computation in the previous sections is of course intimately linked with the study of the groups $R_2^{\mathrm{ord}}(F)$ and $WK_2(F)$. Indeed, the above computations show that the regular kernel $R_2^{\mathrm{ord}}(F)$ is trivial in the case when $F = \mathbf{Q}(\sqrt{-1})$ or $F = \mathbf{Q}(\sqrt{-3})$. In other words, $K_2(\mathbf{Z}[i]) = 1 = K_2(\mathbf{Z}[\omega])$ by Remark 2.23.

Example 3.14. In the case of a quadratic number field $\mathbf{Q}(\sqrt{d})$, it is quite easy to give examples for which there is a nontrivial regular kernel. For example, let F be the field $\mathbf{Q}(\sqrt{d})$ where $d < 0$ is a squarefree integer such that $d \equiv 1 \pmod 8$. By Proposition 1.10, 2 splits in the extension $F/\mathbf{Q}$. Now let v be a place of F above 2. The fact that $d \equiv 1 \pmod 8$ means that d has a square root in $\mathbf{Q}_2$ by Hensel's lemma, hence $F_v = \mathbf{Q}_2(\sqrt{d}) = \mathbf{Q}_2$. Thus

$$\left(\frac{-1,-1}{v}\right) = \left(\frac{-1,-1}{2}\right) = -1$$

by Example 1.54. This means that the element $\{-1,-1\}$ is nontrivial in $K_2(F)$. But the formula for tame symbols (Proposition 1.52) along with the fact that

$$\mu(F_v)^{\mathrm{reg}} = \mu(\mathbf{Q}_2)^{\mathrm{reg}} = 1$$

shows that $\{-1,-1\} \in R_2^{\mathrm{ord}}(F)$. On the other hand we clearly have $\{-1,-1\} \notin WK_2(F)$ since $h(\{-1,-1\})$ is nontrivial on the component $\mu(F_v) = \mu(\mathbf{Q}_2) = \mu_2$.

Among the imaginary quadratic fields, the first instance of a nontrivial regular kernel occurs for $\mathbf{Q}(\sqrt{-7})$.

Tate shows in [BT73, p.435] that the field $F := \mathbf{Q}(\sqrt{-35})$ has $R_2^{\mathrm{ord}}(F)$ nontrivial, yet there are no local Hilbert symbols showing this. This is an example of an imaginary quadratic field on which there is a symbol that cannot be expressed in terms of Hilbert symbols. Equivalently, such a symbol is nontrivial on the wild kernel. These symbols are called *exotic*. Thus the wild kernel is in some sense a measure of how many exotic symbols one can have on a number field.

Example 3.15. In [Keu97], Keune shows that if $d < 0$ is a squarefree integer with $d \equiv 2 \pmod{16}$, the element $\{-1, -1\} \in K_2(\mathbf{Q}(\sqrt{d}))$ lies in the wild kernel.

Example 3.16. Hutchinson shows in [Hut04] that the imaginary quadratic fields $\mathbf{Q}(\sqrt{d})$, where $d \equiv 2 \pmod{16}$ is negative and squarefree, possess exotic symbols. Specifically, he shows that there is a Steinberg symbol λ defined on $\mathbf{Q}(\sqrt{d})$ with values in μ_8 such that $\lambda(\{-1, -1\}) = -1$.

CHAPTER 4

Motivic Homotopy Theory

Motivic-, or $\mathbf{A}^1$-homotopy theory is a homotopy theory for smooth schemes, developed by Morel and Voevodsky [MV99]. Letting Sm_F denote the category of smooth schemes over a field F, the basic goal is to create suitably nice unstable and stable homotopy categories from Sm_F, in which the affine line $\mathbf{A}^1 := \mathbf{A}^1_F$ plays the role of the unit interval. Now the naive approach toward such a construction would be simply to directly lift the definition of a homotopy in topology by saying two morphisms

$$f, g : X \longrightarrow Y$$

in Sm_F are $\mathbf{A}^1$-*homotopic* if there is a morphism

$$H : X \times_F \mathbf{A}^1 \longrightarrow Y$$

such that $H|_{X\times\{0\}} = f$ and $H|_{X\times\{1\}} = g$. This approach is however unsatisfactory. Indeed, the resulting relation of "$\mathbf{A}^1$-homotopy" is not an equivalence relation, as it fails to be transitive. And even if we consider the equivalence relation generated by "$\mathbf{A}^1$-homotopy" there is no reasonable way in general to put a group structure on the resulting set of $\mathbf{A}^1$-homotopy classes of morphisms that we would like to call "$\mathbf{A}^1$-homotopy *groups*" [Mor04a, 2.2].

Instead of the above approach, one could try to invoke the machinery of model categories in order to create the desired homotopy category. But then the lack of certain categorical properties of Sm_F becomes apparent: For example, one of the first properties demanded of the category in order to put a model structure on it is bicompleteness, i.e., all small limits and colimits exist. This is not fulfilled by Sm_F since this category does not have all quotients. To fix this problem, one first enlarges the category Sm_F by considering instead the category

$$\mathrm{Pre}(\mathrm{Sm}_F) := [\mathrm{Sm}_F^{\mathrm{op}}, \mathrm{Set}]$$

of presheaves on Sm_F. Thus $\mathrm{Pre}(\mathrm{Sm}_F)$ is the category whose objects are functors $\mathrm{Sm}_F^{\mathrm{op}} \to \mathrm{Set}$, and whose morphisms are natural transformations. Via the Yoneda embedding

$$X \mapsto \mathrm{Hom}_{\mathrm{Sm}_F}(-, X) : \mathrm{Sm}_F \to \mathrm{Pre}(\mathrm{Sm}_F)$$

we identify Sm_F with the full subcategory of $\mathrm{Pre}(\mathrm{Sm}_F)$ consisting of representable functors. Moreover, the category $\mathrm{Pre}(\mathrm{Sm}_F)$ is bicomplete since Set is bicomplete. But in order to put a model structure on a functor category it is convenient to have a model structure on the target category. So we replace Set by the model category $\mathscr{S} := [\Delta^{\mathrm{op}}, \mathrm{Set}]$ of simplicial sets (see [Hov99, DLØ+07]). Thus we further embed $\mathrm{Pre}(\mathrm{Sm}_F)$ into the category

$$\Delta^{\mathrm{op}}\mathrm{Pre}(\mathrm{Sm}_F) := [\Delta^{\mathrm{op}}, \mathrm{Pre}(\mathrm{Sm}_F)] = [\mathrm{Sm}_F^{\mathrm{op}}, \mathscr{S}] = [\Delta^{\mathrm{op}} \times \mathrm{Sm}_F^{\mathrm{op}}, \mathrm{Set}]$$

of simplicial presheaves. The embedding $\mathrm{Pre}(\mathrm{Sm}_F) \hookrightarrow \Delta^{\mathrm{op}}\mathrm{Pre}(\mathrm{Sm}_F)$ is given by considering a presheaf X as a constant simplicial presheaf $[n] \mapsto X$. Note that the category of simplicial sets also embeds in $\Delta^{\mathrm{op}}\mathrm{Pre}(\mathrm{Sm}_F)$ by considering a simplicial set as constant on Sm_F, i.e., for $K \in \mathscr{S}$, define

$$K([n], X) := K_n \in \mathrm{Set}$$

for all $X \in \mathrm{Sm}_F$.

The category $\Delta^{\mathrm{op}}\mathrm{Pre}(\mathrm{Sm}_F)$ has all the desired properties one can ask for, and is therefore called the category of *motivic spaces*, denoted by $\mathcal{MS}(F)$. The category of motivic spaces is then provided with a model structure which generalizes the naive point of view, yielding the notion of $\mathbf{A}^1$-weak equivalences.

Notation 4.1. We will identify a scheme $X \in \mathrm{Sm}_F$ with its corresponding representable presheaf $\mathrm{Hom}_{\mathrm{Sm}_F}(-, X) \in \mathrm{Pre}(\mathrm{Sm}_F)$. For a smooth subscheme $Y \hookrightarrow X$ we write X/Y for the pointed sheaf associated to the presheaf $U \mapsto \mathrm{Hom}(U, Y)/\mathrm{Hom}(U, X)$.

We will denote by $\mathcal{MS}_\bullet(F)$ the category of *pointed* motivic spaces. The category $\mathcal{MS}(F)$ embeds in $\mathcal{MS}_\bullet(F)$ via $X \mapsto X_+ := X \amalg \mathrm{Spec}(F)$, where X_+ is pointed by $\mathrm{Spec}(F)$.

Below we will briefly discuss the model structure on $\mathcal{MS}_\bullet(F)$ and the construction of the motivic unstable and stable homotopy category $\mathcal{H}_\bullet(F)$ and $\mathcal{SH}(F)$. However, background material on, e.g., model categories is left out, as this is not the main objective of this thesis. The curious reader may consult [Hov99].

On the homological side we also mention below the theory of motives and motivic cohomology; in particular we will discuss Voevodsky's construction of the derived category of geometric motives.

4.1 The motivic unstable and stable homotopy category

The model structure on $\mathcal{MS}(F)$ is constructed to take into account the *Nisnevich topology* on Sm_F. This topology is finer than the Zariski topology, but coarser than the étale topology, and is precisely what is needed to prove, e.g., descent theorems for algebraic K-theory and the homotopy purity theorem.

Definition 4.2. A map $f : U \to X$ of schemes is *completely decomposed at* $x \in X$ if there is $u \in U$ such that $f(u) = x$ and the induced map on residue fields $k(x) \to k(u)$ is an isomorphism.

Definition 4.3. Let $X \in \mathrm{Sm}_F$. A covering $\{f_i : U_i \to X\}_{i \in I}$ is called a *Nisnevich covering* if I is finite, all the f_i's are étale and for all $x \in X$ there is an $i \in I$ such that f_i is completely decomposed at x.

The Nisnevich coverings provide a basis for a Grothendieck topology on Sm_F, called the Nisnevich topology. The resulting Nisnevich site is denoted $(\mathrm{Sm}_F)_{\mathrm{Nis}}$.

Definition 4.4. A cartesian square

$$\begin{array}{ccc} U \times_X V & \longrightarrow & V \\ \downarrow & & \downarrow{\scriptstyle p} \\ U & \xrightarrow{\ i\ } & X \end{array}$$

is called an *elementary distinguished square* in the Nisnevich topology if i is an open embedding, p is étale and $p^{-1}(X \setminus U) \xrightarrow{p} X \setminus U$ is an isomorphism of reduced schemes.

Proposition 4.5 ([Sev06, Proposition 6.1.11])**.** *Given an elementary distinguished square (i, p) as in Definition 4.4 above, the set $\{U \xrightarrow{i} X, V \xrightarrow{p} X\}$ forms a Nisnevich covering of X.*

Moreover, a presheaf $\mathscr{F}$ on the Nisnevich site $(\mathrm{Sm}_F)_{\mathrm{Nis}}$ is a sheaf if and only if $\mathscr{F}(\varnothing) = *$ and for all elementary distinguished squares (i, p), the diagram

$$\begin{array}{ccc} \mathscr{F}(X) & \xrightarrow{\mathscr{F}(p)} & \mathscr{F}(V) \\ {\scriptstyle \mathscr{F}(i)}\downarrow & & \downarrow \\ \mathscr{F}(U) & \longrightarrow & \mathscr{F}(U \times_X V) \end{array}$$

is a pullback square in Set.

We let $\mathrm{Shv}_{\mathrm{Nis}}(\mathrm{Sm}_F)$ denote the category of sheaves on the Nisnevich site $(\mathrm{Sm}_F)_{\mathrm{Nis}}$.

Definition 4.6. The *projective objectwise model structure* on $\mathcal{MS}_\bullet(F)$ is defined as follows. Weak equivalences and cofibrations are defined objectwise—i.e., $\mathscr{X} \to \mathscr{Y}$ is a weak equivalence in $\mathcal{MS}_\bullet(F)$ if and only if $\mathscr{X}(X) \to \mathscr{Y}(X)$ is a weak equivalence in $\mathscr{S}$ for all $X \in \mathrm{Sm}_F$, and similarly for cofibrations. Fibrations are the maps having the right lifting property with respect to acyclic cofibrations.

Now let Q denote a Nisnevich elementary distinguished square as in Definition 4.4, and let Q^{hp} denote the homotopy pushout of $U \leftarrow U \times_X V \to V$. Form the class of morphisms

$$S_{\mathrm{Nis}}^{\mathrm{hp}} := \{Q^{\mathrm{hp}} \to X\}_Q \cup \{\varnothing \to h_\varnothing\},$$

where Q ranges over all Nisnevich elementary distinguished squares. Here $\varnothing$ means the empty simplicial set, while $h_\varnothing$ is the presheaf represented by the empty scheme. The set $\{\varnothing \to h_\varnothing\}$ is included only for technical reasons.

Definition 4.7. The *local projective* model structure on $\mathcal{MS}_\bullet(F)$ is the $S_{\mathrm{Nis}}^{\mathrm{hp}}$-localization of the projective model structure on $\mathcal{MS}_\bullet(F)$.

The local projective model structure makes $\mathcal{MS}_\bullet(F)$ into a proper model category [Sev06, Theorem 6.2.7]. This model structure takes into account certain relations that is needed to prove for example the purity theorem for Thom spaces. However, one can show that there is a full embedding of Sm_F into the homotopy category of $\mathcal{MS}_\bullet(F)$ with the local projetive model structure [Sev06, Proposition 6.2.4]. In other words, no schemes are identified in this homotopy category. Therefore we need to localize once more if we want the affine line to be contractible.

Definition 4.8. The *motivic projective* model structure on $\mathcal{MS}_\bullet(F)$ is the left Bousfield localization of the local projective model structure with respect to $S := \{X \times_F \mathbf{A}^1 \to X\}_{X \in \mathrm{Sm}_F}$. The resulting homotopy category is the *unstable motivic homotopy category* $\mathcal{H}_\bullet(F)$.

There are two kinds of circles in $\mathcal{H}_\bullet(F)$: Familiar from topology we have the simplicial circle $S^1 := \Delta^1/\partial\Delta^1$, which is pointed by Δ^0. On the geometric side we have the *Tate circle* $S^\alpha := \mathbf{A}^1 \setminus \{0\}$, pointed by 1. We will often identify S^α with the group scheme $\mathbf{G}_m$. There is a smash product on $\mathcal{H}_\bullet(F)$, defined pointwise, which allows us to talk about the mixed spheres

$$S^{m+n\alpha} := (S^1)^{\wedge m} \wedge (S^\alpha)^{\wedge n}.$$

Example 4.9. By taking complex realization we obtain $S^{m+n\alpha}(\mathbf{C}) = S^{m+n}$, where S^k is the usual topological sphere. If we consider the real realization we get $S^{m+n\alpha}(\mathbf{R}) = S^m$.

In Section 4.2 we will see that there is a canonical isomorphism $S^{1+\alpha} \cong \mathbf{P}^1$ in $\mathcal{H}_\bullet(F)$. We let $\Sigma_{\mathbf{P}^1}$ denote the $\mathbf{P}^1$-suspension functor $X \mapsto \mathbf{P}^1 \wedge X$. The process of stabilizing with respect to $\mathbf{P}^1$-suspension results in the *stable motivic homotopy category* $\mathcal{SH}(F)$, which we elaborate on next.

Definition 4.10. A $\mathbf{P}^1$*-spectrum* $X = (X_n)_{n\geq 0}$ is a sequence of pointed motivic spaces $X_n \in \mathcal{MS}_\bullet(F)$ together with structure maps $\sigma : \Sigma_{\mathbf{P}^1} X_n \to X_{n+1}$ for all n. A map $f : X \to Y$ of spectra is a sequence of maps $f_n : X_n \to Y_n$ compatible with the structure maps, i.e., the diagram

$$\begin{array}{ccc} \Sigma_{\mathbf{P}^1} X_n & \xrightarrow{\sigma_X} & X_{n+1} \\ {\scriptstyle \Sigma_{\mathbf{P}^1} f_n}\downarrow & & \downarrow{\scriptstyle f_{n+1}} \\ \Sigma_{\mathbf{P}^1} Y_n & \xrightarrow{\sigma_Y} & Y_{n+1} \end{array}$$

commutes for each $n \geq 0$. We let $\mathrm{Spt}(F)$ denote the category of $\mathbf{P}^1$-spectra. There is an embedding $\Sigma_{\mathbf{P}^1}^\infty : \mathcal{MS}_\bullet(F) \to \mathrm{Spt}(F)$, where $\Sigma_{\mathbf{P}^1}^\infty X$ is the spectrum with constituent spaces $(\Sigma_{\mathbf{P}^1}^\infty X)_n := \Sigma_{\mathbf{P}^1}^n X$ and identity structure maps.

Definition 4.11. The *sphere spectrum* is

$$\mathbf{1} := \Sigma_{\mathbf{P}^1}^\infty \operatorname{Spec}(F)_+ \in \mathrm{Spt}(F).$$

This spectrum is initial in the category of ring spectra.

We do not intend to go into details of the construction of the stable model structure on $\mathrm{Spt}(F)$; this can be found in, e.g., [Jar00]. The rough idea is however as follows. A map $f : X \to Y$ of spectra is called a *levelwise weak equivalence (resp. (co)fibration)* if the component maps $f_n : X_n \to Y_n$ are weak equivalences (resp. (co)fibrations) for all n. Thus the category $\mathrm{Spt}(F)$ inherits a model structure from $\mathcal{MS}_\bullet(F)$. The *projective model structure* on $\mathrm{Spt}(F)$ is defined by these levelwise fibrations and cofibrations. From this model structure one defines a certain localizing set S of morphisms in $\mathrm{Spt}(F)$, and weak equivalences are defined as the S-local weak equivalences. The resulting model structure is the *stable model structure*. The homotopy category of $\mathrm{Spt}(F)$ with the stable model structure is the motivic stable homotopy category $\mathcal{SH}(F)$.

Theorem 4.12 ([Voe98])**.** *We list a few properties of the category $\mathcal{SH}(F)$.*

- *$\mathcal{SH}(F)$ is a triangulated category, with simplicial suspension $\Sigma_s := - \wedge S^1$ as shift functor.*
- *There are realization functors*

$$\mathcal{SH}(F) \xrightarrow[F\subseteq\mathbf{C}]{\mathrm{Re}_{\mathbf{C}}} \mathcal{SH} \qquad \mathcal{SH}(F) \xrightarrow[F\subseteq\mathbf{R}]{\mathrm{Re}_{\mathbf{R}}} \mathcal{SH}^{\mathbf{Z}/2}$$

  Here $\mathcal{SH}$ denotes the topological stable homotopy category, and $\mathcal{SH}^{\mathbf{Z}/2}$ is the $\mathbf{Z}/2$-equivariant stable homotopy category. The realization of the motivic sphere spectrum is the topological sphere spectrum.
- *$\mathcal{SH}(F)$ satisfies Grothendieck's six functor formalism [CD12].*

In the category $\mathcal{SH}(F)$ we can define stable motivic homotopy groups:

Definition 4.13. Let $m, n \in \mathbf{Z}$ and $X \in \mathrm{Spt}(F)$. We write $\underline{\pi}_{m+n\alpha}(X)$ for the sheaf associated to the presheaf of stable homotopy groups

$$U \longmapsto \operatorname*{colim}_k \mathrm{Hom}_{\mathcal{SH}(F)}(S^{(m+k)+(n+k)\alpha} \wedge \Sigma^\infty_{\mathbf{P}^1} U_+, X)$$

where $U \in \mathrm{Sm}_F$. The bigraded *stable homotopy groups of* X is $\pi_{m+n\alpha}(X) := \underline{\pi}_{m+n\alpha}(X)(\operatorname{Spec} F)$.

There is a description of the stable weak equivalences in the stable model structure on $\mathrm{Spt}(F)$ that is more in line with classical topology:

Theorem 4.14 ([Jar00, Lemma 3.7])**.** *A map $f : X \to Y$ in $\mathrm{Spt}(F)$ is a stable weak equivalence if and only if f induces an isomorphism of presheaves $\underline{\pi}_{n+m\alpha}X \to \underline{\pi}_{n+m\alpha}Y$ for all $m, n \in \mathbf{Z}$.*

Notation 4.15. The notation $\pi_{p,q}$ and $S^{p,q}$ for the motivic homotopy groups and mixed spheres is also often used in the literature. To transition between the two, use $S^{p,q} = S^{(p-q)+q\alpha}$.

We will use a star $\star$ to denote bigrading, i.e., all indices $(m, n) \in \mathbf{Z}^2$, and an asterisk $*$ will denote monograding (e.g., compare $\pi_\star$ and $\pi_{*\alpha}$).

The most fundamental objects in stable motivic homotopy theory are perhaps the homotopy groups $\pi_{m+n\alpha}\mathbf{1}$ of the sphere spectrum. Very few of these groups are known; indeed, since the realization of $\mathbf{1}$ is the topological sphere spectrum, the groups $\pi_{m+n\alpha}\mathbf{1}$ are at least as hard to compute as the topological stable stems.

Morel's $\mathbf{A}^1$-connectivity theorem [Mor05] shows that $\pi_{m+n\alpha}\mathbf{1} = 0$ whenever $m < 0$, and in [Mor04a] the homotopy groups are computed for $m = 0$ (see Chapter 5, Theorem 5.1). Chapter 5 is essentially devoted to the study of these groups for $m = 0$, which Morel identifies as the *Milnor-Witt K-theory* of F (see Definition 5.6 in Chapter 5 for the definition). In Chapter 5 we will see a few computations of the Milnor-Witt K-theory of different fields—in other words, we compute $\pi_{n\alpha}\mathbf{1}$ for different base fields F.

The groups $\pi_{1+n\alpha}\mathbf{1}$ have recently been computed in [RSØ16], but the situation for higher values of m is in general unknown to this date.

4.2 Motivic spheres

In this section we list a few useful isomorphisms in $\mathcal{H}_\bullet(F)$ [Voe98, Lemma 4.1].

Proposition 4.16. *The Tate object $T := \mathbf{A}^1/(\mathbf{A}^1 \setminus \{0\})$ is weakly equivalent to the sphere $S^{1+\alpha}$.*

Proof. The homotopy colimit of the diagram $* \leftarrow \mathbf{A}^1 \setminus \{0\} \rightarrow *$ equals the simplicial suspension of $\mathbf{A}^1 \setminus \{0\}$ [Str11, p.153]; identifying $\mathbf{A}^1 \setminus \{0\}$ with $\mathbf{G}_m$, this yields

$$\operatorname{hocolim}(* \longleftarrow \mathbf{A}^1 \setminus \{0\} \longrightarrow *) = \Sigma_s(\mathbf{A}^1 \setminus \{0\}) = S^1 \wedge \mathbf{G}_m = S^{1+\alpha}.$$

On the other hand, the following diagram is a pushout by definition:

$$\begin{array}{ccc} \mathbf{A}^1 \setminus \{0\} & \rightarrowtail & \mathbf{A}^1 \\ \downarrow & \ulcorner & \downarrow \\ * & \longrightarrow & \mathbf{A}^1/(\mathbf{A}^1 \setminus \{0\}). \end{array}$$

Since the upper arrow in the diagram above is a cofibration and all $X \in \mathrm{Sm}_F$ are $\mathbf{A}^1$-local fibrant [Sev06, Lemma 6.2.16], the colimit of the above diagram coincides with the homotopy colimit [Lur09, Proposition A.2.4.4]. Since $\mathbf{A}^1 \simeq *$ this yields $\mathbf{A}^1/(\mathbf{A}^1 \setminus \{0\}) \simeq S^{1+\alpha}$. □

Proposition 4.17. *In the pointed motivic homotopy category $\mathcal{H}_\bullet(F)$ we have a canonical isomorphism*

$$\mathbf{A}^1/(\mathbf{A}^1 \setminus \{0\}) \cong \mathbf{P}^1,$$

and more generally,

$$\mathbf{A}^n/(\mathbf{A}^n \setminus \{0\}) \cong \mathbf{P}^n/\mathbf{P}^{n-1}$$

for any $n \geq 1$.

Proof. We prove the assertion for $n = 1$ by computing the homotopy pushout of

$$* \longleftarrow \mathbf{A}^1/(\mathbf{A}^1 \setminus \{0\}) \longrightarrow *$$

in a third way. Consider the diagram

$$\begin{array}{ccc} \mathbf{A}^1 \setminus \{0\} & \rightarrowtail & \mathbf{A}^1 \\ \downarrow & \ulcorner & \downarrow \\ \mathbf{A}^1 & \longrightarrow & \mathbf{P}^1 \end{array}$$

where the cofibrations are given by $x \mapsto x$ and $x \mapsto x^{-1}$. By gluing we obtain $\mathbf{P}^1$ as the pushout of this diagram, hence by the results above we obtain the following isomorphisms of homotopy pushouts:

$$\mathbf{P}^1 \cong \mathbf{A}^1/(\mathbf{A}^1 \setminus \{0\}) \cong S^{1+\alpha}.$$

□

Proposition 4.18 ([DI05, Example 2.11])**.** *In $\mathcal{H}_\bullet(F)$, we have a canonical isomorphism*

$$\mathbf{A}^n \setminus \{0\} \cong S^{(n-1)+n\alpha}$$

for any $n \geq 1$.

Proof (following [DI05]). We use induction on n. For $n = 1$ this follows by definition: $\mathbf{A}^1 \setminus \{0\} = \mathbf{G}_m = S^\alpha$. For $n = 2$, we use the open covering $\mathbf{A}^2 \setminus \{0\} = U \cup V$, where

$$\begin{aligned} U &:= (\mathbf{A}^1 \setminus \{0\}) \times \mathbf{A}^1, \\ V &:= \mathbf{A}^1 \times (\mathbf{A}^1 \setminus \{0\}). \end{aligned}$$

Then $U \cap V = (\mathbf{A}^1 \setminus \{0\}) \times (\mathbf{A}^1 \setminus \{0\})$, and $\mathbf{A}^2 \setminus \{0\}$ is the homotopy pushout of $U \leftarrow U \cap V \rightarrow V$ in the category of presheaves. Using that the projections from $(\mathbf{A}^1 \setminus \{0\}) \times \mathbf{A}^1$ and $\mathbf{A}^1 \times (\mathbf{A}^1 \setminus \{0\})$ onto $\mathbf{A}^1 \setminus \{0\}$ are weak equivalences, we get the diagram

$$\begin{array}{ccccc} (\mathbf{A}^1 \setminus \{0\}) \times (\mathbf{A}^1 \setminus \{0\}) & \rightarrowtail & (\mathbf{A}^1 \setminus \{0\}) \times \mathbf{A}^1 & \xrightarrow{\sim} & \mathbf{A}^1 \setminus \{0\} \\ \downarrow & \ulcorner & \downarrow & & \downarrow \\ \mathbf{A}^1 \times (\mathbf{A}^1 \setminus \{0\}) & \rightarrowtail & \mathbf{A}^2 \setminus \{0\} & \xrightarrow{\sim} & P \\ \downarrow \sim & & & & \| \\ \mathbf{A}^1 \setminus \{0\} & & \longrightarrow & & P \end{array}$$

where P is the pushout of the outer diagram

$$\mathbf{A}^1 \setminus \{0\} \longleftarrow (\mathbf{A}^1 \setminus \{0\}) \times (\mathbf{A}^1 \setminus \{0\}) \longrightarrow \mathbf{A}^1 \setminus \{0\}.$$

Since the arrows in the upper left square are cofibrations and $\mathcal{MS}_\bullet(F)$ is a left proper model category we have $\mathbf{A}^2 \setminus \{0\} \simeq P$, so we proceed to compute the pushout P instead. Consider the diagram

$$\begin{array}{ccccc} * & \longleftarrow & * & \longrightarrow & * \\ \uparrow & & \uparrow & & \uparrow \\ \mathbf{A}^1 \setminus \{0\} & \longleftarrow & (\mathbf{A}^1 \setminus \{0\}) \vee (\mathbf{A}^1 \setminus \{0\}) & \longrightarrow & \mathbf{A}^1 \setminus \{0\} \\ \downarrow & & \downarrow & & \downarrow \\ \mathbf{A}^1 \setminus \{0\} & \longleftarrow & (\mathbf{A}^1 \setminus \{0\}) \times (\mathbf{A}^1 \setminus \{0\}) & \longrightarrow & \mathbf{A}^1 \setminus \{0\} \end{array}$$

where the middle and lower horizontal maps are the projections onto the factors. The homotopy colimits of the rows in this diagram are respectively $*$, $*$ and P, going from the top row to the bottom row. We thus obtain the diagram $* \leftarrow * \rightarrow P$, whose homotopy pushout is P. Here we have used that

$$\operatorname{hocolim}(X \xleftarrow{\mathrm{pr}_1} X \vee Y \xrightarrow{\mathrm{pr}_2} Y) = *.$$

On the other hand, if we identify $\mathbf{A}^1 \setminus \{0\} = \mathbf{G}_m$ and compute the homotopy pushouts of the columns, we obtain the diagram

$$* \longleftarrow \mathbf{G}_m \wedge \mathbf{G}_m \longrightarrow *$$

whose homotopy pushout is $\Sigma_s(\mathbf{G}_m \wedge \mathbf{G}_m) = S^{1+2\alpha}$. This yields $P = S^{1+2\alpha}$, as we must obtain the same homotopy type no matter which direction we start computing the homotopy pushouts.

For $n > 2$, one proceeds in the same manner as above: Cover $\mathbf{A}^n$ by open sets

$$\begin{aligned} U &= (\mathbf{A}^{n-1} \setminus \{0\}) \times \mathbf{A}^1 \\ V &= \mathbf{A}^1 \times (\mathbf{A}^{n-1} \setminus \{0\}) \end{aligned}$$

and perform a similar computation as above to obtain

$$\mathbf{A}^n \setminus \{0\} \simeq \Sigma_s((\mathbf{A}^{n-1} \setminus \{0\}) \wedge (\mathbf{A}^1 \setminus \{0\})),$$

from which the result follows by induction. □

4.3 The algebraic K-theory spectrum

We will concern ourselves with the motivic $\mathbf{P}^1$-spectrum KGL representing algebraic K-theory. Voevodsky defines this spectrum in [Voe98]; we start out by briefly recalling this construction.

For any $N \geq n$, consider the Grassmannian $\mathrm{Gr}_n(\mathbf{A}^N)$. There are canonical inclusions $\mathrm{Gr}_n(\mathbf{A}^N) \hookrightarrow \mathrm{Gr}_n(\mathbf{A}^{N+1})$; let BGL_n denote the union

$$\mathrm{BGL}_n := \operatorname*{colim}_m \mathrm{Gr}_n(\mathbf{A}^{n+m}).$$

Furthermore, there are canonical inclusions

$$\mathrm{Gr}_n(\mathbf{A}^N) \longhookrightarrow \mathrm{Gr}_{n+1}(\mathbf{A}^{N+1})$$

given by sending a linear subspace L of $\mathbf{A}^N$ to $L \oplus \{0\} \subseteq \mathbf{A}^{N+1}$. Hence we can define

$$\mathrm{BGL} := \operatorname*{colim}_n \mathrm{BGL}_n = \operatorname*{colim}_n \operatorname*{colim}_m \mathrm{Gr}_n(\mathbf{A}^{n+m}).$$

The constituent spaces of the spectrum KGL will be the spaces KGL, where KGL is the fibrant replacement of

$$\mathbf{Z} \times \mathrm{BGL} := \coprod_{\mathbf{Z}} \mathrm{BGL}\,.$$

The reason for taking a fibrant replacement lies in the definition of the structure maps $\mathbf{P}^1 \wedge \mathrm{KGL} \to \mathrm{KGL}$ of KGL, which again relies on the isomorphism

$$\mathrm{Hom}_{\mathcal{H}_\bullet(F)}(\mathbf{P}^1 \wedge (\mathbf{Z} \times \mathrm{BGL}), \mathbf{Z} \times \mathrm{BGL}) \cong \mathrm{Hom}_{\mathcal{H}_\bullet(F)}(\mathbf{Z} \times \mathrm{BGL}, \mathbf{Z} \times \mathrm{BGL})$$

of [Voe98, p.600]. Let

$$\overline{e} : \mathbf{P}^1 \wedge (\mathbf{Z} \times \mathrm{BGL}) \longrightarrow \mathbf{Z} \times \mathrm{BGL}$$

be the map corresponding to the identity morphism of $\mathbf{Z} \times \mathrm{BGL}$ under the above isomorphism. Since KGL is fibrant, $\overline{e}$ lifts to a map

$$e : \mathbf{P}^1 \wedge \mathrm{KGL} \longrightarrow \mathrm{KGL}$$

in $\mathrm{Spc}_\bullet(F)$.

Definition 4.19. The algebraic K-theory spectrum KGL has constituent spaces $\mathsf{KGL}_n = \mathrm{KGL}$ and structure maps given by $e : \mathbf{P}^1 \wedge \mathrm{KGL} \to \mathrm{KGL}$.

The spectrum KGL represents algebraic K-theory:

Theorem 4.20 ([Voe98, Theorem 6.9])**.** *For any $X \in \mathrm{Sm}_F$ there are canonical isomorphisms*

$$K_{m-n}(X) \cong \mathrm{Hom}_{\mathcal{SH}(F)}(S^{m+n\alpha} \wedge X_+, \mathsf{KGL}).$$

In particular, for $X = \operatorname{Spec} F$ we have $K_{m-n}(F) \cong \pi_{m+n\alpha}\mathsf{KGL}$.

In [PPR09], it is shown that this spectrum is essentially unique, and a product

$$\mu_{\mathsf{KGL}} : \mathsf{KGL} \wedge \mathsf{KGL} \longrightarrow \mathsf{KGL}$$

is constructed, providing KGL with the structure of a ring spectrum [PPR09, Theorem 2.2.1]. This product is the unique map in $\mathrm{Hom}_{\mathcal{SH}(F)}(\mathsf{KGL} \wedge \mathsf{KGL}, \mathsf{KGL})$ making the following diagram commutative:

$$\begin{array}{ccc}
K_0(X) \times K_0(X) & \xrightarrow{\quad\otimes\quad} & K_0(X) \\
\cong\downarrow & & \downarrow\cong \\
\pi_{m(1+\alpha)}\mathsf{KGL}(X) \times \pi_{n(1+\alpha)}\mathsf{KGL}(X) & \xrightarrow[\mu_{\mathsf{KGL}}]{} & \pi_{(m+n)(1+\alpha)}\mathsf{KGL}(X)
\end{array}$$

4.4 Motives

Voevodsky's construction of the derived category of motives—which predates the birth of motivic homotopy theory—allows for a definition of the long sought motivic cohomology theory. Originally it was Grothendieck and his collaborators who speculated upon the existence of such a universal cohomology theory. This section is therefore meant as a short "history lesson", although we conclude with a discussion on the connection between motivic cohomology-, and homotopy theory. In particular, we mention the "Hurewicz functor" $H : \mathcal{H}_\bullet(F) \to \mathrm{DM}^{\mathrm{eff}}_-(F)$, relating homotopy on one side with homology on the other. We will also see in Theorem 4.30 that familiar objects like Milnor K-theory are found among the motivic cohomology groups.

The notion of a *motive* was introduced by Grothendieck in 1964 [Mil14]. The basic idea was that motives should define a category through which all Weil cohomology theories should factor. Grothendieck called the objects of this hypothetical category *pure motives*. Until now, the so-called *mixed motives* have been defined. However, the existence of pure motives is equivalent to the standard conjecture on algebraic cycles—a problem which is still unsolved.

Below we briefly illustrate the construction of Voevodsky's derived categories of motives $\mathrm{DM}_{\mathrm{gm}}(F)$ and $\mathrm{DM}^{\mathrm{eff}}_-(F)$. Roughly speaking, we start out with Sm_F, i.e., smooth schemes over F, but we want this category to be Ab-enriched. So Sm_F is replaced with the category Cor_F of *finite correspondences*, the definition of which relies on Suslin-Voevodsky's theory of relative cycles. Through a process of localization and idempotent completion we arrive at the so-called category of *effective geometric motives* $\mathrm{DM}^{\mathrm{eff}}_{\mathrm{gm}}(F)$. Analogously to the situation in stable homotopy theory, the category $\mathrm{DM}_{\mathrm{gm}}(F)$ of geometric motives is then a stabilized version of $\mathrm{DM}^{\mathrm{eff}}_{\mathrm{gm}}(F)$ [CD12].

Definition 4.21. Let S be a regular scheme and let $X \in \mathrm{Sch}_S$ be an S-scheme. Let $Z(X)$ denote the free abelian group on the prime cycles of X (see [Ful98]). The group $C_{\mathrm{equi}}(X/S, 0)$ of *relative cycles of dimension* 0 is the subgroup of $Z(X)$ generated by the points $x \in X$ such that $\overline{\{x\}} \to S$ is finite and surjective (where $\overline{\{x\}}$ is given the reduced scheme structure).

The groups of relative cycles will form the Hom-sets in the category Cor_F:

Definition 4.22. Let $X, Y \in \mathrm{Sm}_F$. The *group of finite correspondences from X to Y* is

$$\mathrm{Cor}_F(X, Y) := C_{\mathrm{equi}}(X \times_F Y/X, 0).$$

A generator in $C_{\mathrm{equi}}(X \times Y/X, 0)$ is called an *elementary correspondence from X to Y*.

We can compose correspondences: The composition of two elementary correspondences $V \in \mathrm{Cor}_F(X, Y)$, $W \in \mathrm{Cor}_F(Y, Z)$ is defined as the pushforward along the projection

$$p : X \times Y \times Z \to X \times Z$$

of the intersection product $[T] := (V \times Z) \cdot (X \times W)$; see [MVW06, p.4].

Definition 4.23. Let Cor_F be the category whose objects are the objects of Sm_F, and whose morphisms are correspondences: $\mathrm{Hom}_{\mathrm{Cor}_F(X,Y)} := C_{\mathrm{equi}}(X \times Y/X, 0)$.

Definition 4.24. Let

$$\mathrm{PST}(F) := [\mathrm{Cor}_F^{\mathrm{op}}, \mathrm{Ab}]$$

denote category of *presheaves with transfers*. For X a smooth F-scheme we let $\mathbf{Z}_{\mathrm{tr}}(X)$ denote the representable presheaf with transfers $\mathbf{Z}_{\mathrm{tr}}(X) := \mathrm{Hom}_{\mathrm{Cor}_F}(-, X)$.

Defining $X \oplus Y := X \amalg Y$, it follows that Cor_F is an additive category with the empty scheme as zero-object. The category Cor_F is also symmetric monoidal—see [MVW06, p.6] for the definition of the tensor product $\otimes^{\mathrm{tr}}$ on Cor_F. The homotopy category $K^b(\mathrm{Cor}_F)$ of bounded chain complexes on Cor_F then becomes a tensor-triangulated category. We aim to localize the category $K^b(\mathrm{Cor}_F)$ with respect to a certain subcategory:

Definition 4.25. Let $\mathscr{B}$ be the localizing subcategory of $K^b(\mathrm{Cor}_F)$ generated by:

Homotopy invariance: For all $X \in \mathrm{Sm}_F$, $[X \times \mathbf{A}^1] \to [X]$ is in $\mathscr{B}$.

Mayer-Vietoris: For each Zariski open covering $X = U \cup V$ of X, the map

$$[U \cap V] \longrightarrow [U] \oplus [V] \longrightarrow [X]$$

is in $\mathscr{B}$.

We then define the category $\widehat{\mathrm{DM}}^{\mathrm{eff}}_{\mathrm{gm}}(F)$ as the localization of $K^b(\mathrm{Cor}_F)$ with respect to $\mathscr{B}$:

$$\widehat{\mathrm{DM}}^{\mathrm{eff}}_{\mathrm{gm}}(F) := K^b(\mathrm{Cor}_F)/\mathscr{B}.$$

Finally, the *category of effective geometric motives* $\mathrm{DM}^{\mathrm{eff}}_{\mathrm{gm}}(F)$ is the idempotent completion (see [Wei13, p.143]) of $\widehat{\mathrm{DM}}^{\mathrm{eff}}_{\mathrm{gm}}(F)$.

We have a functor $M_{\mathrm{gm}} : \mathrm{Sm}_F \to \mathrm{DM}^{\mathrm{eff}}_{\mathrm{gm}}(F)$ defined by the composition

$$\mathrm{Sm}_F \longrightarrow \mathrm{Cor}_F \longrightarrow K^b(\mathrm{Cor}_F) \longrightarrow \widehat{\mathrm{DM}}^{\mathrm{eff}}_{\mathrm{gm}}(F) \longrightarrow \mathrm{DM}^{\mathrm{eff}}_{\mathrm{gm}}(F).$$

Here $K^b(\mathrm{Cor}_F) \to \widehat{\mathrm{DM}}^{\mathrm{eff}}_{\mathrm{gm}}(F)$ is the localization functor, and $\widehat{\mathrm{DM}}^{\mathrm{eff}}_{\mathrm{gm}}(F) \to \mathrm{DM}^{\mathrm{eff}}_{\mathrm{gm}}(F)$ is the full embedding into the idempotent completion, defined by $X \mapsto (X, \mathrm{id}_X)$. For $X \in \mathrm{Sm}_F$, we call $M_{\mathrm{gm}}(X)$ the *effective geometric motive of* X. The functor M_{gm} is monoidal, satisfying $M_{\mathrm{gm}}(X \times Y) = M_{\mathrm{gm}}(X) \otimes M_{\mathrm{gm}}(Y)$. We write $\mathbf{Z} := M_{\mathrm{gm}}(\operatorname{Spec} F)$, as this object is the unit for the tensor product on $\mathrm{DM}^{\mathrm{eff}}_{\mathrm{gm}}(F)$.

The *reduced effective geometric motive* $\widetilde{M}_{\mathrm{gm}}(X)$ of $X \in \mathrm{Sm}_F$ is defined by the distinguished triangle

$$\widetilde{M}_{\mathrm{gm}}(X) \longrightarrow M_{\mathrm{gm}}(X) \longrightarrow \mathbf{Z} \longrightarrow \widetilde{M}_{\mathrm{gm}}(X)[1].$$

Definition 4.26. The *Lefschetz motive* is

$$\mathbf{Z}(1) := \widetilde{M}_{\mathrm{gm}}(\mathbf{P}^1)[-2].$$

More generally, $\mathbf{Z}(n) := \mathbf{Z}(1)^{\otimes n}$ for any $n \geq 0$. Moreover, for any effective geometric motive $\mathscr{M}$ in $\mathrm{DM}^{\mathrm{eff}}_{\mathrm{gm}}(F)$ we define its twist by n as $\mathscr{M}(n) := \mathscr{M} \otimes \mathbf{Z}(n)$.

To construct the category $\mathrm{DM}_{\mathrm{gm}}(F)$ of geometric motives we invert the Lefschetz motive:

Definition 4.27. The *category of geometric motives* $\mathrm{DM}_{\mathrm{gm}}(F)$ is defined as having as its objects pairs $(\mathscr{M}, m)$, where $\mathscr{M} \in \mathrm{DM}^{\mathrm{eff}}_{\mathrm{gm}}(F)$ is an effective geometric motive and $m \in \mathbf{Z}$ is an integer. The morphisms are defined as

$$\mathrm{DM}_{\mathrm{gm}}(F)((\mathscr{M}, m), (\mathscr{N}, n)) := \operatorname*{colim}_{k \geq -m, -n} \mathrm{DM}^{\mathrm{eff}}_{\mathrm{gm}}(F)(\mathscr{M}(k+m), \mathscr{N}(k+n)).$$

In the category $\mathrm{DM}_{\mathrm{gm}}(F)$, tensor product with the Lefschetz motive $\mathbf{Z}(1)$ is invertible. The process of inverting an object of $\mathrm{DM}^{\mathrm{eff}}_{\mathrm{gm}}(F)$ to obtain the category $\mathrm{DM}_{\mathrm{gm}}(F)$ is an analog of the Spanier-Whitehead construction in topology. In fact, one can carry out this process in any symmetric monoidal category [Voe98, p.588].

The Hom-groups in $\mathrm{DM}^{\mathrm{eff}}_{\mathrm{gm}}(F)$ are of great interest. In fact, they are one possible definition of motivic cohomology:

Definition 4.28. For $X \in \mathrm{Sm}_F$, let

$$H^{p,q}(X, \mathbf{Z}) := \mathrm{DM}^{\mathrm{eff}}_{\mathrm{gm}}(F)(M_{\mathrm{gm}}(X), \mathbf{Z}(q)[p])$$

be the *motivic cohomology* of X with coefficients in $\mathbf{Z}$. The index p is called the *cohomological degree*, and q is called the *weight*.

Example 4.29. Suppose $X \in \mathrm{Sm}_F$ is a connected scheme. By [MVW06, Lecture 4] there is a quasi-isomorphism of motivic complexes $\mathbf{Z}(1) \xrightarrow{\sim} \mathcal{O}_X^\times[-1]$, where $\mathcal{O}_X^\times$ is the sheaf of units in the structure sheaf on X. This theorem can be used to describe some motivic cohomology groups in weight one. The result is:

$$H^{p,q}(X, \mathbf{Z}) = \begin{cases} 0, & q \leq 1, (p,q) \neq (0,0), (1,1), (2,1) \\ \mathbf{Z}, & (p,q) = (0,0) \\ \mathcal{O}_X^\times(X), & (p,q) = (1,1) \\ \mathrm{Pic}(X), & (p,q) = (2,1). \end{cases}$$

Milnor K-theory is also found along the diagonal motivic cohomology groups:

Theorem 4.30 ([MVW06, Theorem 5.1])**.** *For any integer $n \geq 0$ there is a natural isomorphism $H^{n,n}(\mathrm{Spec}\, F, \mathbf{Z}) \cong K_n^M(F)$.*

The effective geometric motives can be realized as a thick subcategory of the category of *effective motives*:

Definition 4.31 ([MVW06, p.109])**.** Let $\mathrm{DM}_-^{\mathrm{eff}}(F)$ denote the localization

$$\mathrm{DM}_-^{\mathrm{eff}}(F) := D^-(\mathrm{Shv}_{\mathrm{Nis}}(\mathrm{Cor}_F))/\mathscr{A},$$

where $\mathscr{A}$ is the localizing subcategory generated by complexes

$$\mathbf{Z}_{\mathrm{tr}}(X \times \mathbf{A}^1) \xrightarrow{\mathbf{Z}_{\mathrm{tr}}(p)} \mathbf{Z}_{\mathrm{tr}}(X)$$

for any $X \in \mathrm{Sm}_F$ with $p : X \times \mathbf{A}^1 \to X$ being the canonical projection.

Theorem 4.32 (The embedding theorem [MVW06, p.110])**.** *The category $\mathrm{DM}_{\mathrm{gm}}^{\mathrm{eff}}(F)$ embeds as a full subcategory of $\mathrm{DM}_-^{\mathrm{eff}}(F)$.*

Theorem 4.33 ([MVW06, pp.110-111])**.** *We list a few properties of the category $\mathrm{DM}_-^{\mathrm{eff}}(F)$.*

- *(Mayer-Vietoris) Given a Zariski open covering $X = U \cup V$ of $X \in \mathrm{Sm}_F$, there is a Mayer-Vietoris distinguished triangle*

$$M_{\mathrm{gm}}(U \cap V) \longrightarrow M_{\mathrm{gm}}(U) \oplus M_{\mathrm{gm}}(V) \longrightarrow M_{\mathrm{gm}}(X) \longrightarrow M_{\mathrm{gm}}(U \cap V)[1]$$

  in $\mathrm{DM}_-^{\mathrm{eff}}(F)$.

- *If $\mathscr{E} \to X$ is a vector bundle, then the induced map $M_{\mathrm{gm}}(\mathscr{E}) \to M_{\mathrm{gm}}(X)$ is an isomorphism.*

- *(Projective bundle formula) Let $\mathscr{E} \to X$ be a vector bundle of rank $d+1$, giving rise to the projective bundle $p : \mathbf{P}(\mathscr{E}) \to X$. The map p induces an isomorphism*

$$\bigoplus_{n=0}^{d} M_{\mathrm{gm}}(X)(n)[2n] \xrightarrow{\cong} M_{\mathrm{gm}}(\mathbf{P}(\mathscr{E})).$$

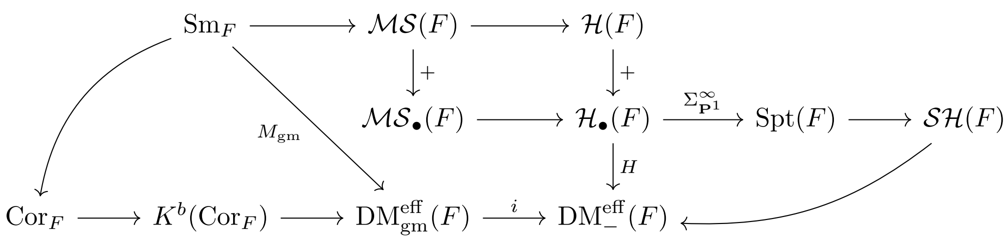
- *(Blowup triangle) If Z is a smooth closed subscheme of $X \in \mathrm{Sm}_F$, let $p : \mathrm{Bl}_Z(X) \to X$ denote the blowup morphism. Then there is a distinguished triangle*

$$M_{\mathrm{gm}}(p^{-1}(Z)) \longrightarrow M_{\mathrm{gm}}(Z) \oplus M_{\mathrm{gm}}(\mathrm{Bl}_Z(X)) \longrightarrow M_{\mathrm{gm}}(X) \longrightarrow M_{\mathrm{gm}}(p^{-1}(Z))[1]$$

  in $\mathrm{DM}_-^{\mathrm{eff}}(F)$.

4.5 Overview

The following diagram is meant as a short overview of all the categories constructed above and how they relate.



Here $i : \mathrm{DM}^{\mathrm{eff}}_{\mathrm{gm}}(F) \to \mathrm{DM}^{\mathrm{eff}}_{-}(F)$ is the full embedding from Theorem 4.32, and the "Hurewicz functor" $H : \mathcal{H}_\bullet(F) \to \mathrm{DM}^{\mathrm{eff}}_{-}(F)$ is defined as follows. By Nisnevich sheafification we obtain a functor $\mathcal{MS}_\bullet(F) \to D^-(\mathrm{Shv}_{\mathrm{Nis}}(\mathrm{Cor}_F))$. This functor sends $X \times \mathbf{A}^1 \to X$ to $\mathbf{Z}_{\mathrm{tr}}(X \times \mathbf{A}^1) \to \mathbf{Z}_{\mathrm{tr}}(X)$, hence $\mathbf{A}^1$-weak equivalences of spaces are mapped to $\mathbf{A}^1$-weak equivalences of complexes. It follows that this functor preserves localization, i.e., it induces the functor H. By [Wei04, Lemma 2], H extends to a functor $\mathcal{SH}(F) \to \mathrm{DM}^{\mathrm{eff}}_{-}(F)$. We refer the reader to [Wei04] for further details.

CHAPTER 5

Symbols in Motivic Homotopy Theory

In Chapter 1 and Chapter 3 we have seen the importance of Steinberg symbols in number theory. The aim of this chapter is to illustrate how elements in certain motivic homotopy groups give rise to Steinberg symbols as well as Witt classes. These homotopy groups may perhaps be thought of as more fundamental, since the relations of both Milnor K-theory and Witt theory can be described by operations in stable motivic homotopy theory.

5.1 The Steinberg relation

Let a denote a rational point $a : \mathrm{Spec}(F) \to \mathbf{G}_m$ of $\mathbf{G}_m$. Then a induces a map of sheaves

$$[a] : S^0 \longrightarrow \mathbf{G}_m$$

by sending the nonbase point to $a \in \mathbf{G}_m(F)$ and preserving the base point, and hence defines an element $[a] \in \pi_{-\alpha}\mathbf{1}$. If b is another rational point of $\mathbf{G}_m$, then the smash product yields a map

$$[a] \cdot [b] \in \mathrm{Hom}_{\mathcal{SH}(F)}(S^0, \mathbf{G}_m \wedge \mathbf{G}_m),$$

that is, $[a] \cdot [b] \in \pi_{-2\alpha}\mathbf{1}$. In [HK01], Hu and Kriz show that these elements satisfy the Steinberg relation, i.e.,

$$[a] \cdot [1-a] = 0 \in \pi_{-2\alpha}\mathbf{1}.$$

Based on this result, Morel gives in [Mor04a, Ch.6] a full description of the homotopy groups $\pi_{*\alpha}\mathbf{1}$ in terms of the graded Milnor-Witt ring $K_*^{MW}(F)$ (defined in Section 5.3):

Theorem 5.1 ([Mor04a, p.40]). *If F is a perfect field of characteristic not 2, then for each $n \in \mathbf{Z}$ there is an isomorphism*

$$\pi_{n\alpha}\mathbf{1} \xrightarrow{\cong} K_{-n}^{MW}(F).$$

Observe that this isomorphism switches degrees.

In addition to the elements $[u] \in \pi_\star\mathbf{1}$, the following maps are of great interest in stable motivic homotopy theory:

- By performing the Hopf construction [DI13] on the multiplication map $\mathbf{G}_m \times \mathbf{G}_m \to \mathbf{G}_m$ one obtains a morphism

  $$\eta : \mathbf{A}^2 \setminus \{0\} = S^{1+2\alpha} \longrightarrow S^{1+\alpha} = \mathbf{P}^1$$

  given by $\mathbf{A}^2 \setminus \{0\} \ni (x, y) \mapsto (x : y) \in \mathbf{P}^1$. This map represents an element $\eta \in \pi_\alpha\mathbf{1}$; it is the motivic analog of the Hopf fibration $\eta_{\mathrm{top}} : S^3 \to S^2$ in topology. Indeed, we obtain η_{top} from η by taking complex realization:

  $$\eta_{\mathrm{top}} : S^{1+2\alpha}(\mathbf{C}) = S^3 \to S^{1+\alpha}(\mathbf{C}) = S^2.$$

  In Section 5.3 we will mention that multiplication with the image of η in Milnor-Witt K-theory is an isomorphism. It follows that η is not nilpotent. This is a major difference from the situation in topology, where $\eta_{\mathrm{top}}^4 = 0$.

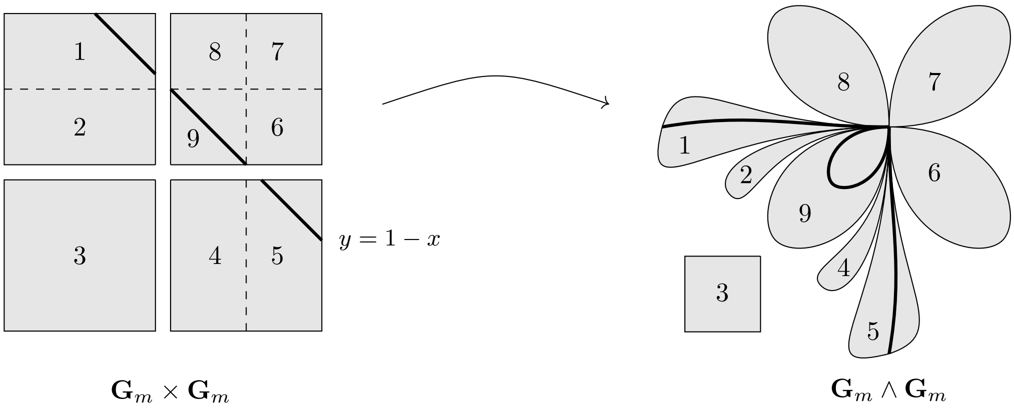


Figure 5.1: Suggested picture of the real points of $\mathbf{G}_m \times \mathbf{G}_m$—where $\mathbf{G}_m$ is pointed by 1—and of $\mathbf{G}_m \wedge \mathbf{G}_m = (\mathbf{G}_m \times \mathbf{G}_m)/(\mathbf{G}_m \vee \mathbf{G}_m)$. The thick line is the graph of the Steinberg morphism $\mathbf{A}^1 \setminus \{0,1\} \to \mathbf{G}_m \times \mathbf{G}_m$, $a \mapsto (a, 1-a)$. To the right we see that the image of this graph becomes connected in $\mathbf{G}_m \wedge \mathbf{G}_m$, suggesting that the Steinberg morphism should extend to $\mathbf{A}^1$.

- The twist morphism

$$\epsilon : \mathbf{G}_m \wedge \mathbf{G}_m \longrightarrow \mathbf{G}_m \wedge \mathbf{G}_m$$

defines a degree-zero element $\epsilon \in \pi_0 \mathbf{1}$. Morel has shown that the elements η and ϵ satisfy the relation

$$\epsilon\eta = \eta,$$

and that the graded ring $\pi_{*\alpha}\mathbf{1}$ is graded ϵ-commutative [Mor04a].

- For $u \in F^\times$ we let $\langle u \rangle$ denote the degree-zero element

$$\langle u \rangle := 1 + \eta[u] \in \pi_0 \mathbf{1}.$$

Then ϵ is given by multiplication by $-\langle -1 \rangle$ [Mor04a].

We will revisit all the elements considered above when we discuss Milnor-Witt K-theory in Section 5.3, although in a purely algebraic setting. But first we start out by explaining Hu and Kriz' proof [HK01] of the Steinberg relation in motivic homotopy theory.

The idea is to show that, after a single simplicial suspension (i.e., smashing with the simplicial circle S^1), the "Steinberg morphism"

$$a \longmapsto (a, 1-a) : \mathbf{A}^1 \setminus \{0,1\} \longrightarrow \mathbf{G}_m \times \mathbf{G}_m \tag{5.1}$$

becomes nullhomotopic when $\mathbf{G}_m \times \mathbf{G}_m$ is replaced by $\mathbf{G}_m \wedge \mathbf{G}_m$. In other words, we want to show that the composition

$$\mathbf{A}^1 \setminus \{0,1\} \longrightarrow \mathbf{G}_m \times \mathbf{G}_m \longrightarrow \mathbf{G}_m \wedge \mathbf{G}_m$$

extends to $\mathbf{A}^1$ after simplicial suspension (see Figure 5.1).

To begin with, we need a lemma on Zariski excision. Let $X \in \mathrm{Sm}_F$ be a scheme and $X = U \cup V$ a Zariski open covering of X. Thus, in the category of motivic spaces there is a pushout square

$$\begin{array}{ccc} U \cap V & \longrightarrow & U \\ \downarrow & & \downarrow \\ V & \longrightarrow & X \end{array}$$

Given such a covering of X, we have an analog in the motivic setting to excision in topology:

Lemma 5.2 (Zariski excision [MP02]). *Let $X = U \cup V$ be a Zariski open covering of $X \in \mathrm{Sm}_F$. Then we have the following isomorphisms in the category $\mathcal{H}_\bullet(F)$:*

1. $U/(U \cap V) \cong X/V$;
2. $(X/U) \vee (X/V) \cong X/(U \cap V)$.

Proof. In the category of motivic spaces we have the diagram

$$\begin{array}{ccc} U \cap V & \longrightarrow & U \\ \downarrow & \ulcorner & \downarrow \\ V & \longrightarrow & X \\ \downarrow & \ulcorner & \downarrow \\ * & \longrightarrow & X/V \end{array}$$

in which the two small squares are pushouts, hence X/V is the pushout of the large rectangle. But the pushout of the rectangle is $U/(U \cap V)$ by definition, hence $X/V \simeq U/(U \cap V)$.

For the second claim, we make use of the first result along with the following pushout diagram:

$$\begin{array}{ccc} * & \longrightarrow & U/(U \cap V) \\ \downarrow & & \downarrow \\ V/(U \cap V) & \longrightarrow & X/(U \cap V) \end{array}$$

This yields an isomorphism

$$\frac{U}{U \cap V} \vee \frac{V}{U \cap V} \xrightarrow{\sim} \frac{X}{U \cap V}.$$

By 1 we have $U/(U \cap V) \simeq X/V$ and $V/(U \cap V) \simeq X/U$, hence the result follows. ☐

Now consider the space

$$X_1 := (\mathbf{G}_m \times \mathbf{G}_m) \coprod_{\mathbf{G}_m \times \{1\}} (\mathbf{A}^1 \times \{1\}).$$

That is, X_1 is the pushout of $\mathbf{G}_m \times \mathbf{G}_m$ and $\mathbf{A}^1 \times \{1\}$ along $\mathbf{G}_m \times \{1\}$, with attaching maps the inclusions. For simplicity, we will in the following write $V := [y - 1 = xz, y \neq 0]$ for the affine scheme

$$V := \mathrm{Spec}\big(F[x, y, y^{-1}, z]/(y - 1 - xz)\big).$$

Let ϕ be the natural map

$$\begin{aligned} \phi : X_1 &\longrightarrow V, \\ (a, b) &\longmapsto \left(a, b, \frac{b-1}{a}\right). \end{aligned}$$

Lemma 5.3 ([HK01, Lemma 2]). *The simplicial suspension $\Sigma_s \phi$ is a weak equivalence in $\mathcal{MS}_\bullet(F)$.*

Proof. We consider the diagram

$$\begin{array}{ccc} (\mathbf{G}_m \times \mathbf{G}_m) \coprod_{\mathbf{G}_m \times \{1\}} (\mathbf{A}^1 \times \{1\}) & \xrightarrow{\phi} & [y - 1 = xz, y \neq 0] \\ \downarrow & & \downarrow \\ (\mathbf{G}_m \times \mathbf{A}^1) \coprod_{\mathbf{G}_m \times \{1\}} (\mathbf{A}^1 \times \{1\}) & \longrightarrow & [y - 1 = xz] \\ \downarrow & & \downarrow \\ C & \xrightarrow{\psi} & D \end{array}$$

i.e., diagram (5) in the article [HK01]. Here the two vertical columns are cofiber sequences, where

$$C \;:=\; \frac{(\mathbf{G}_m \times \mathbf{A}^1) \coprod_{\mathbf{G}_m \times \{1\}} (\mathbf{A}^1 \times \{1\})}{(\mathbf{G}_m \times \mathbf{G}_m) \coprod_{\mathbf{G}_m \times \{1\}} (\mathbf{A}^1 \times \{1\})};$$

$$D \;:=\; \frac{[y-1=xz]}{[y-1=xz, y \neq 0]}.$$

Here the middle horizontal map is defined similarly as ϕ, and ψ is the induced map on cofibers.

Now we claim that both ψ and the middle horizontal map are equivalences. If so, the statement follows, because we then have a diagram of the form

$$\begin{array}{ccccccccccc} X_1 & \longrightarrow & X_1' & \longrightarrow & C & \longrightarrow & \Sigma_s X_1 & \longrightarrow & \Sigma_s X_1' & \longrightarrow & \Sigma_s C \\ \phi\downarrow & & \downarrow\sim & & \psi\downarrow\sim & & \Sigma_s\phi\downarrow & & \downarrow\sim & & \downarrow\sim \\ V & \longrightarrow & V' & \longrightarrow & D & \longrightarrow & \Sigma_s V & \longrightarrow & \Sigma_s V' & \longrightarrow & \Sigma_s D \end{array}$$

hence the 5-lemma for triangulated categories [Wei94, Exercise 10.2.2] implies that $\Sigma_s\phi$ is an equivalence.

To prove the claim, we start out by showing that both sides of the middle horizontal map are $\mathbf{A}^1$-contractible. For the space to the right, note that the assignment

$$\begin{aligned} F[x,y,z] &\longrightarrow F[s,t], \\ x &\longmapsto s; \\ y &\longmapsto 1+st; \\ z &\longmapsto t \end{aligned}$$

identifies

$$F[x,y,z]/(y-1-xz) \cong F[s,t],$$

hence

$$[y-1=xz] = \operatorname{Spec}(F[x,y,z]/(y-1-xz)) \cong \mathbf{A}^2,$$

which is contractible in the motivic homotopy category. Turning the the space on the left, we use again that $\mathbf{A}^1$ is contractible to obtain:

$$\operatorname{hocolim}(\mathbf{G}_m \times \mathbf{A}^1 \longleftarrow \mathbf{G}_m \times \{1\} \longrightarrow \mathbf{A}^1 \times \{1\}) = \operatorname{hocolim}(\mathbf{G}_m \longleftarrow \mathbf{G}_m \longrightarrow *) = *.$$

Thus $(\mathbf{G}_m \times \mathbf{A}^1) \amalg_{\mathbf{G}_m \times \{1\}} (\mathbf{A}^1 \times \{1\}) \simeq *$, and hence the middle horizontal map is an equivalence.

The next step is to show that ψ is an equivalence. In fact, we show that ψ is an isomorphism of sheaves. Note that, by Zariski excision (Lemma 5.2) we have

$$D \cong \frac{[y-1=xz, y \neq 1]}{[y-1=xz, y \neq 0, y \neq 1]}$$

We claim that the right hand side is isomorphic to

$$C' := \frac{\mathbf{G}_m \times (\mathbf{A}^1 \setminus \{1\})}{\mathbf{G}_m \times (\mathbf{A}^1 \setminus \{0,1\})}.$$

Indeed,

$$\begin{aligned} \mathbf{G}_m \times (\mathbf{A}^1 \setminus \{1\}) &\cong \operatorname{Spec}(F[t,t^{-1}] \otimes_F F[s,(s-1)^{-1}]) \\ &\cong \operatorname{Spec}(F[t,t^{-1},s,(s-1)^{-1}]) \\ &\cong \operatorname{Spec}(F[u,u^{-1},v,v^{-1}]), \end{aligned}$$

where the last isomorphism is induced by the map $F[u,v] \to F[s,t]$ sending u to s and v to $s-1$. Furthermore, we have

$$\begin{aligned}
[y-1=xz, y\neq 1] &= \operatorname{Spec}(F[x,y,z,(y-1)^{-1}]/(y-1-xz)) \\
&\cong \operatorname{Spec}(F[x,y,(xy)^{-1}]) \\
&= \operatorname{Spec}(F[x,y,x^{-1},y^{-1}]),
\end{aligned}$$

so that $\mathbf{G}_m \times (\mathbf{A}^1 \setminus \{1\}) \cong [y-1=xz, y\neq 1]$, hence $D \cong C'$.

Now consider the diagram

$$\begin{array}{ccccccc}
 & & \mathbf{G}_m \times \{1\} & \rightarrowtail & \mathbf{A}^1 \times \{1\} & & \\
 & & \downarrow & (2) & \downarrow & & \\
\mathbf{G}_m \times (\mathbf{A}^1 \setminus \{0,1\}) & \rightarrowtail & \mathbf{G}_m \times (\mathbf{A}^1 \setminus \{0\}) & \longrightarrow & (\mathbf{G}_m \times (\mathbf{A}^1 \setminus \{0\})) \coprod_{\mathbf{G}_m \times \{1\}} (\mathbf{A}^1 \times \{1\}) & \longrightarrow & * \\
\downarrow & (1) & \downarrow & (3) & \downarrow & (4) & \downarrow \\
\mathbf{G}_m \times (\mathbf{A}^1 \setminus \{1\}) & \rightarrowtail & \mathbf{G}_m \times \mathbf{A}^1 & \longrightarrow & (\mathbf{G}_m \times \mathbf{A}^1) \coprod_{\mathbf{G}_m \times \{1\}} (\mathbf{A}^1 \times \{1\}) & \longrightarrow & C
\end{array}$$

The square (1) is a pushout because the spaces $\mathbf{G}_m \times (\mathbf{A}^1 \setminus \{0\})$ and $\mathbf{G}_m \times (\mathbf{A}^1 \setminus \{1\})$ form an open cover of $\mathbf{G}_m \times \mathbf{A}^1$, with intersection $\mathbf{G}_m \times (\mathbf{A}^1 \setminus \{0,1\})$. The square (2) is a pushout by definition, and the space in the lower right corner of (3) is the pushout of the large rectangle made by (2) and (3), which must coincide with the pushout of (3). Finally, note that C' is the pushout of the large rectangle consisting of (1), (3) and (4). Since this pushout must coincide with the pushout of (4), we have $C \cong C'$, thus $C \cong D$. □

Consider the composition

$$\mathbf{A}^1 \setminus \{0,1\} \longrightarrow \mathbf{G}_m \times \mathbf{G}_m \longrightarrow X_1 \xrightarrow{\phi} V,$$

where the first map is the Steinberg morphism 5.1 and the second map is the induced map on the pushout. This composition maps $a \in \mathbf{A}^1 \setminus \{0,1\}$ to $(a, 1-a, -1) \in V$, and extends to a map

$$\mathbf{A}^1 \setminus \{1\} \longrightarrow V$$

by letting $a \mapsto (a, 1-a, -1)$.

Symmetrically, define

$$\begin{aligned}
X_2 &:= (\mathbf{G}_m \times \mathbf{G}_m) \coprod_{\{1\}\times \mathbf{G}_m} (\{1\} \times \mathbf{A}^1), \\
W &:= [x-1 = yz, x \neq 0]
\end{aligned}$$

and a map

$$\begin{aligned}
\phi' : X_2 &\longrightarrow W, \\
(a,b) &\longmapsto \left(a, b, \frac{a-1}{b}\right).
\end{aligned}$$

Similarly as above, 5.1 extends to a map

$$\begin{aligned}
\mathbf{A}^1 \setminus \{0\} &\longrightarrow W \\
a &\longmapsto (a, 1-a, -1).
\end{aligned}$$

Hence 5.1 also extends to a map

$$\mathbf{A}^1 \longrightarrow V \coprod_{\mathbf{G}_m \times \mathbf{G}_m} W,$$

where $V \amalg_{\mathbf{G}_m \times \mathbf{G}_m} W$ means the pushout of $V \xleftarrow{\phi} \mathbf{G}_m \times \mathbf{G}_m \xrightarrow{\phi'} W$.

By a similar argument as the one given in Lemma 5.3, $\Sigma_s \phi'$ is an equivalence.

Theorem 5.4. *The maps ϕ and ϕ' induce an equivalence*

$$\Sigma_s(\mathbf{G}_m \wedge \mathbf{G}_m) \simeq \Sigma_s\left(V \coprod_{\mathbf{G}_m \times \mathbf{G}_m} W\right).$$

Hence, after simplicial suspension, the Steinberg morphism 5.1 extends to

$$\Sigma_s \mathbf{A}^1 \longrightarrow \Sigma_s(\mathbf{G}_m \wedge \mathbf{G}_m).$$

Proof. First note that the colimit of the diagram

$$\begin{array}{ccc}
 & & \mathbf{G}_m \times \{1\} \longrightarrow * \\
 & & \downarrow \\
\{1\} \times \mathbf{G}_m & \rightarrowtail & \mathbf{G}_m \times \mathbf{G}_m \\
\downarrow & & \\
* & &
\end{array}$$

is $(\mathbf{G}_m \times \mathbf{G}_m)/(\mathbf{G}_m \vee \mathbf{G}_m) = \mathbf{G}_m \wedge \mathbf{G}_m$. Now consider the diagram

$$\begin{array}{ccccc}
 & & \mathbf{G}_m \times \{1\} & \longrightarrow & \mathbf{A}^1 \times \{1\} \\
 & & \downarrow & & \downarrow \\
\{1\} \times \mathbf{G}_m & \rightarrowtail & \mathbf{G}_m \times \mathbf{G}_m & \longrightarrow & X_1 \\
\downarrow & & \downarrow & & \downarrow \\
\{1\} \times \mathbf{A}^1 & \longrightarrow & X_2 & \longrightarrow & P
\end{array}$$

where P is the pushout of the lower right square. This diagram is an extended version of (11) in [HK01]. Since the arrows in the upper left half-square are cofibrations, P coincides with the homotopy colimit of the diagram

$$\begin{array}{ccccc}
 & & \mathbf{G}_m \times \{1\} & \rightarrowtail & \mathbf{A}^1 \times \{1\} \\
 & & \downarrow & & \\
\{1\} \times \mathbf{G}_m & \rightarrowtail & \mathbf{G}_m \times \mathbf{G}_m & & \\
\downarrow & & & & \\
\{1\} \times \mathbf{A}^1 & & & &
\end{array}$$

which is $\mathbf{G}_m \wedge \mathbf{G}_m$ by the discussion above since $\mathbf{A}^1 \simeq *$.

Finally, note that ϕ and ϕ' induce maps from $P = \mathbf{G}_m \wedge \mathbf{G}_m$ to $V \amalg_{\mathbf{G}_m \times \mathbf{G}_m} W$. Since $\Sigma_s \phi$ and $\Sigma_s \phi'$ are equivalences, the induced map on pushouts yields an equivalence

$$\Sigma_s(\mathbf{G}_m \wedge \mathbf{G}_m) \simeq \Sigma_s\left(V \coprod_{\mathbf{G}_m \times \mathbf{G}_m} W\right),$$

as desired. □

5.2 On the ring spectrum map $1 \to \mathsf{KGL}$

Since the sphere spectrum $\mathbf{1}$ is initial in the category of ring spectra, there is a unique map from $\mathbf{1}$ to the algebraic K-theory spectrum KGL. This morphism induces a ring map

$$u : \pi_\star \mathbf{1} \longrightarrow \pi_\star \mathsf{KGL}.$$

The unit map $\mathbf{1} \to \mathsf{KGL}$ corresponds to a choice of generator for $K_0(F) \cong \mathbf{Z}$; indeed, we have

$$\begin{aligned} \mathrm{Hom}_{\mathcal{SH}(F)}(\mathbf{1}, \mathsf{KGL}) &= \pi_0 \mathsf{KGL}(F) \\ &\cong K_0(F) \\ &\cong \mathbf{Z}\{[F]\} \end{aligned}$$

by Chapter 2, Example 2.2. By composing with the unit map $\mathbf{1} \to \mathsf{KGL}$ we obtain morphisms

$$\pi_{*\alpha}\mathbf{1} \longrightarrow \pi_{*\alpha}\mathsf{KGL}.$$

Below we will consider the map

$$\pi_{-\alpha}\mathbf{1} = \mathrm{Hom}_{\mathcal{SH}(F)}(\Sigma_t^{-1}\mathbf{1}, \mathbf{1}) \longrightarrow \mathrm{Hom}_{\mathcal{SH}(F)}(\Sigma_t^{-1}\mathbf{1}, \mathsf{KGL}) = \pi_{-\alpha}\mathsf{KGL},$$

where $\Sigma_t = - \wedge \mathbf{G}_m$ denotes $\mathbf{G}_m$-suspension.

Proposition 5.5. *The map*

$$u : \pi_{-2\alpha}\mathbf{1} \longrightarrow \pi_{-2\alpha}\mathsf{KGL}$$

sends the element $[a] \cdot [b] \in \pi_{-2\alpha}\mathbf{1}$ *to* $\{a, b\} \in K_2(F) = \pi_{-2\alpha}\mathsf{KGL}$.

Sketch of proof. By the identification $\pi_{-\alpha}\mathsf{KGL} \cong K_1(F)$, it follows that the map u sends $[a] \in \pi_{-\alpha}\mathbf{1}$ to $\{a\} \in K_1(F)$. Since u is a ring map we obtain a commutative diagram

$$\begin{array}{ccc} \pi_{-\alpha}\mathbf{1} \times \pi_{-\alpha}\mathbf{1} & \longrightarrow & \pi_{-2\alpha}\mathbf{1} \\ \downarrow & & \downarrow \\ \pi_{-\alpha}\mathsf{KGL} \times \pi_{-\alpha}\mathsf{KGL} & \longrightarrow & \pi_{-2\alpha}\mathsf{KGL} \\ \wr\Vert & & \wr\Vert \\ K_1(F) \times K_1(F) & \longrightarrow & K_2(F) \end{array}$$

The bottom horizontal map is the product on $K_1(F)$, which sends $(\{a\}, \{b\}) \in K_1(F) \times K_1(F)$ to $\{a, b\} \in K_2(F)$ (cf. Theorem 2.15). The top horizontal morphism is the product in $\pi_{-*\alpha}\mathbf{1}$, mapping $([a], [b])$ to $[a][b] \in \pi_{-2\alpha}\mathbf{1}$. Thus $u([a][b]) = \{a, b\} \in K_2(F)$. □

Proposition 5.5 tells us that many of the relations in K-theory comes from relations in motivic homotopy groups of spheres. We move on to study these fundamental objects next—albeit in the form of Milnor-Witt K-theory.

5.3 The Milnor-Witt ring

As mentioned at the beginning of this chapter, the so-called Milnor-Witt K-theory gives an exact description of certain operations in stable motivic homotopy theory. In this section, we proceed to study the Milnor-Witt K-groups in their own right.

Definition 5.6 (Hopkins-Morel [Mor04a, p.40])**.** The *Milnor-Witt K-theory* $K_*^{MW}(F)$ of F is the $\mathbf{Z}$-graded associative ring freely generated by symbols $[x]$ ($x \in F^\times$) in degree $+1$, and one symbol η of degree -1, subject to the following relations:

1. $[x][1-x] = 0$ for all $x \in F^\times \setminus \{1\}$,
2. $[xy] = [x] + [y] + \eta[x][y]$,
3. $\eta[x] = [x]\eta$,
4. $\eta h = 0$, where $h := 2 + \eta[-1] \in K_0^{MW}(F)$

for $x, y \in F^\times$.

There is a natural map

$$K_*^{MW}(F) \longrightarrow K_*^M(F)$$

sending $[x]$ to $\{x\}$ and η to 0, which yields a canonical isomorphism

$$K_*^{MW}(F)/\eta \cong K_*^M(F).$$

Indeed, the term $\eta[x][y]$ in the second relation of Milnor-Witt K-theory is the obstruction for additivity in $K_*^{MW}(F)$.

Definition 5.7. For $u \in F^\times$, let $\langle u \rangle$ denote the degree-zero element

$$\langle u \rangle := 1 + \eta[u] \in K_0^{MW}(F).$$

In particular, let $\epsilon := -\langle -1 \rangle$.

Note the relation

$$\epsilon\eta = \eta.$$

Moreover, we have that

$$\eta(1 + \langle -1 \rangle) = 0,$$

which is reminiscent of the defining relation of the Witt ring. In fact, the map $F^\times \to K_0^{MW}(F)$ defined by $u \mapsto \langle u \rangle$ induces an isomorphism $GW(F) \xrightarrow{\cong} K_0^{MW}(F)$ [Mor12a, p.65], and for $n > 0$, multiplication with η^n induces an isomorphism $W(F) \xrightarrow{\cong} K_{-n}^{MW}(F)$ [Mor12a, Lemma 2.10, p.65].

In addition to the maps $K_n^{MW}(F) \to K_n^M(F)$ there are, for $n \geq 1$, canonical homomorphisms

$$K_n^{MW}(F) \longrightarrow I^n(F),$$

which maps an element $[a_1] \cdots [a_n]$ of $K_n^{MW}(F)$ to the class of the Pfister form $\langle\langle a_1 \ldots, a_n \rangle\rangle \in I^n(F)$ (defined in Chapter 2, Definition 2.30). A theorem of Morel shows how these maps relate:

Theorem 5.8 ([Mor04b]). *The diagram*

$$\begin{array}{ccc} K_n^{MW}(F) & \longrightarrow & K_n^M(F) \\ \downarrow & & \downarrow \\ I^n(F) & \longrightarrow & I^n(F)/I^{n+1}(F) \end{array}$$

is a pullback square.

Example 5.9. Since $I^2(\mathbf{F}_q) = 0$ (cf. Table 2.1 in Chapter 2) for any finite field $\mathbf{F}_q$, Theorem 5.8 implies that $K_n^{MW}(\mathbf{F}_q) \cong K_n^M(\mathbf{F}_q)$ for all $n \geq 1$.

Lemma 5.10 ([Mor12a, Lemma 2.5, p.62 and Lemma 2.7, p.63]). *For any x, $y \in F^\times$, the following relations hold in $K_*^{MW}(F)$:*

1. $[1] = 0$.
2. $[x][-x] = 0$.
3. $[x][x] = [x][-1] = [-1][x]$.
4. $[x][y] = \epsilon[y][x]$.
5. $\langle x^2 \rangle = 1$.

Lemma 5.11. *The element $\langle x \rangle = 1 + \eta[x]$ is a unit in $K_0^{MW}(F)$, whose inverse is $\langle x^{-1} \rangle$. Moreover, for any x, $y \in F^\times$, the following relations hold in $K_*^{MW}(F)$:*

1. $\left[\frac{x}{y}\right] = [x] - \left\langle \frac{x}{y} \right\rangle [y]$, *hence* $[x^{-1}] = -\langle x^{-1} \rangle [x]$.

2. $\langle xy \rangle = \langle x \rangle \langle y \rangle$.
3. $[x][y] = [y^{-1}][x]$.
4. $[xy] = [x] + \langle x \rangle [y]$.
5. $[x^2][y] = [x][y] - [y][x]$.

Proof. We only prove the last relation. Proof of the first assertion along with Item 1 and Item 2 is found in [Mor12a, Lemma 2.5, p.62]. Moreover, Item 3 is proved in [HT08, Lemma 2.7], and Item 4 follows from the definitions.

By definition of Milnor-Witt K-theory we have

$$[x^2] = 2[x] + \eta[x]^2.$$

Multiplying from the right by $[y]$ then yields

$$[x^2][y] = 2[x][y] + \eta[x]^2[y].$$

On the other hand, using the ϵ-commutativity $[x][y] = \epsilon[y][x]$ we have

$$\begin{aligned}
[x][y] - [y][x] &= [x][y] - \epsilon[x][y] \\
&= [x][y] + \langle -1 \rangle [x][y] \\
&= [x][y] + (1 + \eta[-1])[x][y] \\
&= 2[x][y] + \eta[-1][x][y] \\
&= 2[x][y] + \eta[x]^2[y] = [x^2][y],
\end{aligned}$$

where we have used that $[-1][x] = [x]^2$. □

Proposition 5.12 ([Mor12a, Proposition 2.13, p.67]). *If any unit in F is a square, then for each $n \geq 0$ the canonical surjection*

$$K_n^{MW}(F) \longrightarrow K_n^M(F)$$

is an isomorphism.

Proof. By the second and fourth relation of Milnor-Witt K-theory along with the relation $[x][x] = [x][-1]$ we have

$$\eta[x^2] = \eta(2[x] + \eta[x][-1]) = \eta[x](2 + \eta[-1]) = 0.$$

Since any unit in F is a square, this says that $\eta[z] = 0$ for all $z \in F^\times$. This implies additivity in $K_n^{MW}(F)$, i.e.,

$$[xy] = [x] + [y] + \eta[x][y] = [x] + [y].$$

Therefore the map $K_n^M(F) \to K_n^{MW}(F)$ which sends $\{x_1, \ldots, x_n\}$ to $[x_1] \cdots [x_n]$ is well defined. Composing with the canonical map $K_n^{MW}(F) \to K_n^M(F)$, which sends η to 0, yields the respective identities, so this map is an isomorphism. □

Lemma 5.13 ([Mor12a, Lemma 2.6, p.63]). *For all $n \geq 1$, the group $K_n^{MW}(F)$ is generated by the products of the form $[u_1][u_2] \cdots [u_n]$, with $[u_j] \in F^\times$.*

Proof. Clearly any generator of $K_n^{MW}(F)$ is of the form $\eta^m[u_1] \cdots [u_\ell]$ where $m, \ell \geq 0$ and $\ell - m = n$. The result follows from the relation $\eta[x][y] = [xy] - [x] - [y]$. □

Lemma 5.14. *Suppose v is a discrete valuation on F. If π and π' are two uniformizers, then*

$$[\pi][\pi'] = [\pi][u]$$

for a unit $u \in \mathcal{O}_v^\times$.

Proof. We may write $\pi' = -u\pi$ for u a unit of $\mathcal{O}_v$. Then

$$\begin{aligned}[\pi][u(-\pi)] &= [\pi]([u] + [-\pi] + \eta[u][-\pi]) \\ &= [\pi][u] + [\pi][-\pi] + \eta\epsilon[u][\pi][-\pi] \\ &= [\pi][u]\end{aligned}$$

since $[\pi][-\pi] = 0$. □

Lemma 5.15 ([Mor12a, Lemma 2.14, p.67]). *For any $x \in F^\times$ and any $n \in \mathbf{Z}$, we have the following expression for $[x^n] \in K_1^{MW}(F)$:*

$$[x^n] = n_\epsilon[x],$$

where $n_\epsilon \in K_0^{MW}(F)$ is defined as follows. If $n \geq 0$, we set

$$n_\epsilon := \sum_{j=1}^{n} \langle (-1)^{j-1} \rangle,$$

and for $n < 0$, $n_\epsilon := -\langle -1 \rangle (-n)_\epsilon = \epsilon(-n)_\epsilon$.

Lemma 5.16 ([Mor12a, Corollary 2.8, p.63]). *Given $\alpha \in K_n^{MW}(F)$ and $\beta \in K_m^{MW}(F)$, we have*

$$\alpha\beta = \epsilon^{nm}\beta\alpha.$$

Thus the graded $K_0^{MW}(F)$-algebra $K_*^{MW}(F)$ is graded ϵ-commutative.

In [Mor12a], Morel establishes the existence of an analog in Milnor-Witt K-theory to the well known regular symbols in Milnor K-theory:

Theorem 5.17 ([Mor12a, Section 2.2]). *For each discrete valuation v on F and each choice of uniformizer π, there exists a unique homomorphism*

$$\partial_v^\pi : K_*^{MW}(F) \longrightarrow K_*^{MW}(k(v))$$

commuting with product by η and satisfying

$$\partial_v^\pi([\pi][u_2]\cdots[u_n]) = [\overline{u}_2]\cdots[\overline{u}_n]$$

and

$$\partial_v^\pi([u_1][u_2]\cdots[u_n]) = 0$$

for all units $u_1, \ldots, u_n \in \mathcal{O}_v^\times$.

Remark 5.18. In Milnor-Witt K-theory, the maps ∂_v^π depends on the choice of uniformizer. For if $\pi' = u\pi$, where $u \in \mathcal{O}_v^\times$, then $[\pi'] = [u] + [\pi] + \eta[u][\pi]$. This differs from the situation in Milnor K-theory, where $\{\pi'\} = \{u\} + \{\pi\}$, hence $\partial_v(\pi') = \partial_v(\pi)$ in this case.

Using the technique of Tate, Morel establishes in [Mor12a, Theorem 2.24, p.73] a split exact sequence

$$0 \longrightarrow K_n^{MW}(F) \longrightarrow K_n^{MW}(F(t)) \xrightarrow{\bigoplus_{\mathfrak{p}} \partial_{\mathfrak{p}}^\pi} \bigoplus_{\mathfrak{p} \in \mathrm{Spec}(F[t]) \setminus \{0\}} K_{n-1}^{MW}(F[t]/\mathfrak{p}) \longrightarrow 0,$$

similarly to the sequence in Milnor K-theory.

Theorem 5.17 also allows us to define sheaves of unramified Milnor-Witt K-groups [CF14, p.5]. Let $X \in \mathrm{Sm}_F$ be an integral scheme, and let $X^{(n)}$ denote the set of points $x \in X$ of codimension n. We let $k(X)$ denote the field of rational functions on X.

Definition 5.19. For any $X \in \mathrm{Sm}_F$, choose for each $x \in X^{(1)}$ a corresponding uniformizer π_x. Then, for each $n \in \mathbf{Z}$ we define

$$K_n^{MW}(X) := \ker\left(K_n^{MW}(k(X)) \longrightarrow \bigoplus_{x \in X^{(1)}} K_{n-1}^{MW}(k(x)) \right),$$

where the map is induced by the morphisms $\partial_{v_x}^{\pi_x}$.

Any morphism $f : X \to Y$ in Sm_F induces a homomorphism $h^* : K_n^{MW}(Y) \to K_n^{MW}(X)$ [CF14, p.6], so that $X \mapsto K_n^{MW}(X)$ is a presheaf on Sm_F. This presheaf is in fact a Nisnevich sheaf [Mor12a], which is denoted by $\mathbf{K}_n^{MW}$.

5.4 Milnor-Witt K-theory of $\mathbf{Q}$

In this section we aim to compute the groups $K_n^{MW}(\mathbf{Q})$ for all $n \geq 2$.

Definition 5.20. Let $\Lambda_\infty \subseteq K_*^{MW}\mathbf{Q}$ be the graded subring of $K_*^{MW}\mathbf{Q}$ generated by the elements $[-1]^n \in K_n^{MW}\mathbf{Q}$ for $n \geq 0$, and let Λ_∞^n denote the n-th graded piece of Λ_∞. Thus Λ_∞^n is the subgroup of $K_n^{MW}\mathbf{Q}$ additively generated by $[-1]^n$.

Moreover, let Λ_0 be the graded subring of $K_*^{MW}\mathbf{Q}$ generated by η and the elements $[a]$ with a a positive rational number:

$$\Lambda_0 := \langle \eta, [a] : a \in \mathbf{Q}_{>0} \rangle.$$

For any $n \in \mathbf{Z}$ we let Λ_0^n denote the n-th graded piece of Λ_0.

Lemma 5.21. *For any $n \geq 2$ we have $K_n^{MW}\mathbf{Q} = \Lambda_\infty^n \oplus \Lambda_0^n$.*

Proof. The relation $[-1][a] = [a][a]$ implies that

$$([-1] + x)([-1] + y) = [-1]^2 + [-1]x + [-1]y + xy \in \Lambda_\infty \oplus \Lambda_0$$

for any $x, y \in \Lambda_0$.

Now, fix an $n \geq 2$ and recall from Lemma 5.13 that $K_n^{MW}\mathbf{Q}$ is generated by the symbols $[a_1] \cdots [a_n]$ for which $a_i \in \mathbf{Q}^\times$. If $a_1, \ldots, a_n \in \mathbf{Q}_{>0}$, then the observation above along with the relation $[-a] = [-1] + [a] + \eta[a]^2$ implies that any generator $[\pm a_1] \cdots [\pm a_n]$ of $K_n^{MW}(\mathbf{Q})$ lies in $\Lambda_\infty^n \oplus \Lambda_0^n$.

To conclude we must show that $\Lambda_\infty^n \cap \Lambda_0^n = 0$. Recall again that Λ_0^n is generated by elements of the form $[a_1] \cdots [a_n]$ for $a_i \in \mathbf{Q}_{>0}$. So suppose that $k[-1]^n \in \Lambda_0^n$ for some $k \neq 0$, say

$$k[-1]^n = \sum_i k_i [a_{1i}] \cdots [a_{ni}],$$

with all the a_{ji}'s positive rationals and $k_i \in \mathbf{Z}$. Recall that the canonical map

$$K_n^{MW}(\mathbf{Q}) \longrightarrow I^n(\mathbf{Q})$$

maps a generator $[a_1] \cdots [a_n] \in K_n^{MW}\mathbf{Q}$ to the Pfister form

$$\langle\langle a_1, \ldots, a_n \rangle\rangle = (\langle 1 \rangle - \langle a_1 \rangle) \cdots (\langle 1 \rangle - \langle a_n \rangle) \in I^n(\mathbf{Q}).$$

Hence, passing to the Witt ring $W(\mathbf{Q})$ we obtain the relation of Pfister forms

$$k\langle\langle -1, \ldots, -1 \rangle\rangle = \sum_i k_i \langle\langle a_{1i}, \ldots, a_{ni} \rangle\rangle \in I^n(\mathbf{Q}). \tag{5.2}$$

We claim that such a relation is impossible. Indeed, consider the natural map $W(\mathbf{Q}) \to W(\mathbf{R})$ induced by the inclusion $\mathbf{Q} \hookrightarrow \mathbf{R}$, giving rise to the same relation (5.2) in $W(\mathbf{R})$. Let P denote the standard ordering on $\mathbf{R}$. Note that, since the a_{ji}'s are positive we have $\sigma_P(\langle a_{ji} \rangle) = +1$ for all i, j by Example 2.34. Hence

$$\sigma_P(\langle\langle a_{1i}, \ldots, a_{ni} \rangle\rangle) = \sigma_P((\langle 1 \rangle - \langle a_{1i} \rangle) \cdots (\langle 1 \rangle - \langle a_{ni} \rangle)) = \prod_j (\sigma_P \langle 1 \rangle - \sigma_P \langle a_{ji} \rangle) = 0.$$

On the other hand, a similar computation shows that $\sigma_P(\langle\langle -1, \ldots, -1 \rangle\rangle) = 2^n$, hence the relation (5.2) is impossible whenever $k \neq 0$. ☐

Lemma 5.22. *For any $n \geq 1$, the group Λ^n_∞ is the free additive group generated by $[-1]^n$.*

Proof. Note that, since $\langle -a\rangle = -\langle a\rangle$ in the Witt ring, it follows that the canonical morphism $K^{MW}_n \mathbf{Q} \to I^n(\mathbf{Q})$ maps $k[-1]^n$ to

$$k\langle\langle -1, \dots, -1\rangle\rangle = k(\langle 1\rangle - \langle -1\rangle)^n = k(2\langle 1\rangle)^n = k \cdot 2^n\langle 1\rangle.$$

By [MH73, Theorem 4.5, p.75], $m\langle 1\rangle \neq 0 \in W(\mathbf{Q})$ for any nonzero integer m. Hence $k[-1]^n \neq \ell[-1]^n$ whenever $k \neq \ell$. □

Now we proceed in the same manner as for Milnor K-theory to show that

$$\Lambda^n_0 \cong \bigoplus_{p \geq 2} K^{MW}_{n-1}(\mathbf{F}_p)$$

for any $n \geq 2$. For each prime p and each $n \geq 2$, Theorem 5.17 establishes a map

$$\partial := \bigoplus_{p \geq 2 \text{ prime}} \partial_p : K^{MW}_n(\mathbf{Q}) \longrightarrow \bigoplus_{p \geq 2 \text{ prime}} K^{MW}_{n-1}(\mathbf{F}_p),$$

where we write $\partial_p := \partial^p_{(p)}$; p being the canonical choice of uniformizer for the place (p). Note that $\Lambda^n_\infty \subseteq \ker \partial$ by Theorem 5.17.

Definition 5.23. Define a filtration

$$L_2 \subseteq L_3 \subseteq \cdots \subseteq L_p \subseteq \cdots \subseteq \Lambda_0$$

of $\Lambda_0 \subseteq K^{MW}_* \mathbf{Q}$ by letting L_p be the subring

$$L_p := \langle \eta, [a] : a \in \mathbf{Z}, 1 \leq a \leq p\rangle.$$

For each $n \in \mathbf{Z}$, we let L^n_p denote the n-th graded piece of L_p.

By Lemma 5.11, if $[a]$ and $[b]$ are elements of L_p then so are $[ab]$ and $[a/b]$. Thus, by Lemma 5.13 this filtration is exhaustive, i.e., $\varinjlim_p L_p = \Lambda_0$.

Lemma 5.24. *For each $n \geq 2$, the group L^n_2 is trivial.*

Proof. We have $[2][2] = [2][-1] = 0$ by the Steinberg relation. Thus any generator $[a_1] \cdots [a_n]$ with $a_i \in \{1, 2\}$ is trivial. □

Lemma 5.25. *Let $n \geq 1$. For any prime $p > 2$, let q be the largest prime $< p$. Then L^n_p is generated by L^n_q along with elements of the form*

$$\eta^m[p][a_2][a_3] \cdots [a_{n+m}],$$

where the $a_j \in \mathbf{Z}$ are units modulo p for all $j \geq 2$.

Proof. Let $x = \eta^m[a_1] \cdots [a_{m+n}]$ be a generator of L^n_p, with $1 \leq a_i \leq p$. Using ϵ-commutativity we may assume x is of the form $x = \eta^m[p]^k[a_{k+1}] \cdots [a_{n+m}]$ for some $k \leq n+m$ and a_i units modulo p. But then the result follows from the relation $[p][p] = [-1][p] = [p][-1]$. □

Lemma 5.26. *Let p be an odd prime and let q be the biggest prime $< p$. Suppose $i \geq 2$ and $a_j \in \mathbf{Z}$ such that $a_1 \cdots a_i \equiv c \pmod p$, say $\prod_j a_j = c + pd$, where $|c| < p$ and $|a_j| < p$ for all j. Then*

$$[p][a_1 \cdots a_i] \equiv [p][c] \pmod{L_q}.$$

Proof (following [Mor12a, Lemma 2.25, p.74]). We proceed by induction. For the case $i = 2$, assume $ab = c + pd$, with $|a|, |b|, |c| < p$. Note that

$$|pd| \leq |ab| + |c| \leq (p-1)^2 + p - 1,$$

hence $|d| < p$. Since

$$\frac{pd}{ab} + \frac{c}{ab} = 1$$

we have

$$\left[\frac{pd}{ab}\right]\left[\frac{c}{ab}\right] = 0.$$

Moreover,

$$\left[\frac{pd}{ab}\right] = \left[\frac{d}{ab}\right] + \left\langle\frac{d}{ab}\right\rangle[p]$$

by Item 4 of Lemma 5.11. Thus

$$\begin{aligned} 0 &= \left[\frac{pd}{ab}\right]\left[\frac{c}{ab}\right] \\ &= \left(\left[\frac{d}{ab}\right] + \left\langle\frac{d}{ab}\right\rangle[p]\right)\left[\frac{c}{ab}\right], \end{aligned}$$

i.e.,

$$\left\langle\frac{d}{ab}\right\rangle[p]\left[\frac{c}{ab}\right] = -\left[\frac{d}{ab}\right]\left[\frac{c}{ab}\right].$$

Multiplying from the left by $\langle d/(ab)\rangle^{-1} = \langle ab/d\rangle$ we obtain

$$[p]\left[\frac{c}{ab}\right] = -\left\langle\frac{ab}{d}\right\rangle\left[\frac{d}{ab}\right]\left[\frac{c}{ab}\right] \in L_q.$$

Note that

$$\begin{aligned} \left[\frac{x}{y}\right] &= [x] - \left\langle\frac{x}{y}\right\rangle[y] \\ &= [x] - [y] - \eta\left[\frac{x}{y}\right][y] \end{aligned}$$

by Lemma 5.11. Using this relation on $[c/(ab)]$ and multiplying from the left by $[p]$ get that

$$\begin{aligned} [p]\left[\frac{c}{ab}\right] &= [p][c] - [p][ab] - \eta[p][ab]\left[\frac{c}{ab}\right] \\ &= [p][c] - [p][ab] - \eta\epsilon[ab][p]\left[\frac{c}{ab}\right]. \end{aligned}$$

Since

$$\begin{aligned} -\eta\epsilon[ab][p]\left[\frac{c}{ab}\right] &= \eta\langle -1\rangle[ab][p]\left[\frac{c}{ab}\right] \\ &= \eta(1 + \eta[-1])[ab][p]\left[\frac{c}{ab}\right] \\ &= \eta[ab][p]\left[\frac{c}{ab}\right] + \eta^2[ab]^2[p]\left[\frac{c}{ab}\right] \in L_q \end{aligned}$$

we thus have

$$[p][c] \equiv [p][ab] \pmod{L_q}.$$

For the general case $i > 2$, write $a_2 \cdots a_i \equiv c' \pmod p$. Then $c \equiv a_1 \cdots a_i \equiv a_1 c' \pmod p$. By the second relation of Milnor-Witt K-theory and the induction hypothesis we have

$$\begin{aligned}[p][a_1 \cdots a_i] &= [p][a_1] + [p][a_2 \cdots a_i] + \eta[p][a_1][a_2 \cdots a_i] \\ &\equiv [p][a_1] + [p][c'] + \eta[p][a_1][c'] \pmod{L_q}.\end{aligned}$$

Now $[p][a_1] + [p][c'] + \eta[p][a_1][c'] = [p][a_1 c']$, which we know from the case $i = 2$ equals $[p][c]$ modulo L_q. Hence $[p][a_1 \cdots a_i] \equiv [p][c] \pmod{L_q}$. □

Theorem 5.27. *For each $n \geq 2$, the map $\partial = \bigoplus_p \partial_p$ induces an isomorphism*

$$K_n^{MW}(\mathbf{Q}) \cong \mathbf{Z} \oplus \bigoplus_{p \geq 2} K_{n-1}^{MW}(\mathbf{F}_p) \cong \mathbf{Z} \oplus \bigoplus_{p \geq 2} K_{n-1}^{M}(\mathbf{F}_p).$$

Proof. The proof is similar to [Mor12a, p.76]. We fix an $n \geq 2$. By Lemma 5.21 and Lemma 5.22 it remains to show that

$$\Lambda_0^n \cong \bigoplus_{p \geq 2} K_{n-1}^{MW}(\mathbf{F}_p).$$

As before, we use induction to prove that for each prime p, $L_p^n \cong \bigoplus_{\ell=2}^{p} K_{n-1}^{MW}(\mathbf{F}_\ell)$; the statement then follows.

To start the induction, note that $K_m^{MW}(\mathbf{F}_2) \cong K_m^M(\mathbf{F}_2)$ for each $m \geq 0$ by Proposition 5.12. But $K_m^M(\mathbf{F}_2) = 0$ for $m \geq 1$, hence Lemma 5.24 furnishes the base case of the induction.

Now let p be an odd prime. As in Chapter 3, it suffices to show that there is an isomorphism

$$\phi : K_{n-1}^{MW}(\mathbf{F}_p) \xrightarrow{\cong} L_p^n / L_q^n,$$

where q is the greatest prime less than p.

We first establish the map ϕ. Let $\mu(x)$ denote the endomorphism of the quotient of graded $\mathbf{Z}$-modules L_p/L_q defined by multiplication from the left by an element $x \in L_p$. Thus, if for example $x = \epsilon[u]$, then $\mu(\epsilon[u])$ is the degree-1 homomorphism

$$\begin{aligned}\mu(\epsilon[u]) : L_p/L_q &\longrightarrow L_p/L_q \\ \eta^m[p][u_1] \cdots [u_{n+m}] &\longmapsto \epsilon[u]\eta^m[p][u_1] \cdots [u_{n+m}] = \eta^m[p][u][u_1] \cdots [u_{n+m}]\end{aligned}$$

Let

$$\mathscr{E}_p := \operatorname{Hom}(L_p/L_q, L_p/L_q)$$

denote the graded associative ring of graded endomorphisms of L_p/L_q. We shall prove that the maps

$$\overline{u} \mapsto \mu(\epsilon[u]) : \mathbf{F}_p^\times \longrightarrow (\mathscr{E}_p)_1$$

(where $|u| < p$) along with $\mu(\eta) \in (\mathscr{E}_p)_{-1}$ satisfy the relations of Milnor-Witt K-theory.

1. For the Steinberg relation, take $u \not\equiv 1 \pmod p$. Then

$$\mu(\epsilon[u]) \circ \mu(\epsilon[1-u]) = \mu(\epsilon^2[u][1-u]) = 0.$$

2. Suppose u and v are units modulo p, with $uv \equiv w \pmod p$. By Lemma 5.26 we then have

$$\begin{aligned}\mu(\epsilon[w])(\eta^m[p][u_1] \cdots [u_{n+m}]) &= \eta^m[p][w][u_1] \cdots [u_{n+m}] \\ &= \eta^m[p][uv][u_1] \cdots [u_{n+m}]\end{aligned}$$

in L_p/L_q. Writing out $[uv] = [u] + [v] + \eta[u][v]$ yields

$$\mu(\epsilon[uv]) = \mu(\epsilon[u]) + \mu(\epsilon[v]) + \mu(\eta) \circ \mu(\epsilon[u]) \circ \mu(\epsilon[v]).$$

The last two relations $\mu(\eta)\circ\mu([u]) = \mu([u])\circ\mu(\eta)$ and $\mu(\eta)\circ\mu(1+\langle -1\rangle) = 0$ follows similarly from the relations in L_p/L_q.

Thus we obtain a graded homomorphism $f : K_*^{MW}(\mathbf{F}_p) \to \mathscr{E}_p$, with $[\overline{u}] \mapsto \mu(\epsilon[u])$. Under the adjunction

$$\mathrm{Hom}(K_*^{MW}(\mathbf{F}_p), \mathscr{E}_p) \cong \mathrm{Hom}(K_*^{MW}(\mathbf{F}_p)\otimes L_p/L_q, L_p/L_q),$$

the morphism $f \in \mathrm{Hom}(K_*^{MW}(\mathbf{F}_p), \mathscr{E}_p)$ corresponds to the map

$$\begin{aligned} \widetilde{f} : K_*^{MW}(\mathbf{F}_p)\otimes L_p/L_q &\longrightarrow L_p/L_q \\ [\overline{u}]\otimes y &\longmapsto f([\overline{u}])(y) = \mu(\epsilon[u])(y) = \epsilon[u]y. \end{aligned}$$

By restricting $\widetilde{f}$ to $K_*^{MW}(\mathbf{F}_p)\otimes[p]$ we establish the desired map

$$\begin{aligned} \phi : K_{n-1}^{MW}(\mathbf{F}_p) &\longrightarrow L_p^n/L_q^n \\ \eta^m[\overline{u}_1]\cdots[\overline{u}_{n+m-1}] &\longmapsto \eta^m[p][u_1]\cdots[u_{n+m-1}]. \end{aligned}$$

By Lemma 5.25, ϕ is surjective. By Theorem 5.17, ∂_p vanishes on L_q^n and thus induces a map $\partial_p : L_p^n/L_q^n \to K_{n-1}^{MW}(\mathbf{F}_p)$. Furthermore, the compostition

$$K_{n-1}^{MW}(\mathbf{F}_p) \xrightarrow{\ \phi\ } L_p^n/L_q^n \xrightarrow{\ \partial_p\ } K_{n-1}^{MW}(\mathbf{F}_p)$$

is the identity; indeed,

$$\partial_p(\phi([\overline{u}_1]\cdots[\overline{u}_{n-1}])) = \partial_p([p][u_1]\cdots[u_{n-1}]) = [\overline{u}_1]\cdots[\overline{u}_{n-1}]$$

by Theorem 5.17. By Lemma 5.13, $K_{n-1}^{MW}(\mathbf{F}_p)$ is generated by the elements $[\overline{u}_1]\cdots[\overline{u}_{n-1}]$. Thus ϕ is an isomorphism. □

Example 5.28. In the case $n=2$, note that $2k[-1]^2 \in \Lambda_\infty^2$ is mapped to

$$2k\{-1,-1\} = k\{(-1)^2,-1\} = 0 \in K_2^M(\mathbf{Q})$$

under the canonical map $K_2^{MW}(\mathbf{Q}) \to K_2^M(\mathbf{Q})$. On the other hand, if k is odd, then

$$k[-1]^2 \mapsto \{(-1)^k,-1\} = \{-1,-1\} \neq 0 \in K_2^M(\mathbf{Q}).$$

Hence the kernel of the restriction of the canonical map $K_2^{MW}(\mathbf{Q}) \to K_2^M(\mathbf{Q})$ to Λ_∞^2 is $2\Lambda_\infty^2$.

By [MH73, Corollary 2.5, p.90], $I^3(\mathbf{Q})$ is the free additive group generated by $8\langle 1\rangle$. Since

$$K_2^{MW}(\mathbf{Q}) \ni 2k[-1]^2 \longmapsto k\cdot 8\langle 1\rangle \in I^3(\mathbf{Q}),$$

the canonical map $K_2^{MW}(\mathbf{Q}) \to I^2(\mathbf{Q})$ sends $2\Lambda_\infty^2$ onto $I^3(\mathbf{Q}) = \mathbf{Z}\cdot 8\langle 1\rangle$. Moreover, for each $n \geq 0$ there is an inclusion

$$I^{n+1}(F) \longrightarrow K_n^{MW}(F)$$

given by

$$\langle\langle x_1,\dots,x_{n+1}\rangle\rangle \longmapsto \eta[x_1]\cdots[x_{n+1}].$$

The element

$$k\cdot 8\langle 1\rangle = k\langle\langle -1,-1,-1\rangle\rangle \in I^3(\mathbf{Q})$$

will thus be mapped to

$$k\eta[-1]^3 = -2k[-1]^2 \in 2\Lambda_\infty^2.$$

We may thus identify $I^3(\mathbf{Q})$ with the kernel of the map $K_2^{MW}(\mathbf{Q}) \to K_2^M(\mathbf{Q})$. This illustrates the exact sequence

$$0 \longrightarrow I^3(\mathbf{Q}) \longrightarrow K_2^{MW}(\mathbf{Q}) \longrightarrow K_2^M(\mathbf{Q}) \longrightarrow 0$$

that Theorem 5.8 predicts.

Example 5.29. Theorem 5.27 yields $K_n^{MW}(\mathbf{Q}) \cong \mathbf{Z}$ for any $n \geq 3$. On the other hand, for any $n \geq 3$ we have $K_n^M(\mathbf{Q}) \cong \mathbf{Z}/2$ by [Mil70, Example 1.8], and $I^n(\mathbf{Q}) \cong \mathbf{Z}$ by [MH73, Theorem 4.5, p.75]. The exact sequence

$$0 \longrightarrow I^{n+1}(\mathbf{Q}) \longrightarrow K_n^{MW}(\mathbf{Q}) \longrightarrow K_n^{MW}(\mathbf{Q}) \longrightarrow 0$$

takes the form $0 \to \mathbf{Z} \xrightarrow{\cdot 2} \mathbf{Z} \to \mathbf{Z}/2 \to 0$ whenever $n \geq 3$.

Example 5.30. In light of Definition 5.19, we can define $K_n^{MW}(\mathbf{Z}) := K_n^{MW}(\operatorname{Spec} \mathbf{Z})$. Theorem 5.27 then shows that $K_n^{MW}(\mathbf{Z}) = \mathbf{Z}$ for $n \geq 2$, and also that the sequence

$$0 \longrightarrow K_n^{MW}(\mathbf{Z}) \longrightarrow K_n^{MW}(\mathbf{Q}) \xrightarrow{\partial} \bigoplus_{p \geq 2} K_{n-1}^{MW}(\mathbf{F}_p) \longrightarrow 0$$

is split exact. We do not expect this split exactness to hold for general number fields; indeed, it is not true in general for the corresponding sequence in neither Milnor K-theory nor Witt theory.

5.5 Milnor-Witt K-theory of $\mathrm{Q}(\sqrt{-1})$

Let us consider briefly the case of the Gaussian numbers. By [MH73, p.81], $I^3(F) = 0$ for any totally imaginary number field F. This simplifies matters greatly, because then Theorem 5.8 implies that the map $K_n^{MW}(F) \to K_n^M(F)$ is an isomorphism in degrees $n \geq 2$. However, it is possible to obtain the isomorphism directly by the same method as we have seen. Let us illustrate the case $n = 2$:

Definition 5.31. Define a filtration

$$L_1 \subseteq \cdots \subseteq L_n \subseteq \cdots \subseteq K_2^{MW}(\mathbf{Q}(i))$$

of $K_2^{MW}\mathbf{Q}(i)$ by letting

$$L_n := \langle \eta, [\alpha] : \alpha \in \mathbf{Z}[i]_{S_n}^\times \rangle \cap K_2^{MW}(\mathbf{Q}(i)),$$

where the S_n are defined as in Definition 3.6 of Chapter 3.

As before, we have $\varinjlim_n L_n = K_2^{MW}\mathbf{Q}(i)$.

Lemma 5.32. *The group L_1 is trivial.*

Proof. By Lemma 5.25, it is enough to show that the elements $[u][u']$, for $u, u' \in \mathbf{Z}[i]_{S_1}^\times$, are trivial. Note that $[i][-i] = 0$ by Lemma 5.10.

- By Item 5 of Lemma 5.11, we have:

$$[i][i] = [-1][i] = [i^2][i] = [i][i] - [i][i] = 0.$$

  Moreover,

$$[-1][-1] = [i^2][-1] = [i][-1] - [-1][i] = [i][i] - [i][i] = 0.$$

- Note that $[1+i][-i] = 0 = [1-i][i]$ by the Steinberg relation. Using this we have:

$$[1-i] = [(1+i)(-i)] = [1+i] + [-i] + \eta[1+i][-i] = [1+i] + [-i].$$

  Multiplying by $[i]$ from the right we obtain

$$0 = [1-i][i] = [1+i][i] + [-i][i].$$

  Since $[-i][i] = 0$, this yields $[1+i][i] = 0$.

- The second relation of Milnor-Witt K-theory now gives $[\pm 1 \pm i][u] = 0$ for any $u \in \mu_4$; indeed, if $u' \in \mu_4$ we have

$$[u'(1+i)][u] = [u'][u] + [1+i][u] + \eta[u'][1+i][u] = 0.$$

- By Item 3 of Lemma 5.11, $[u][(1+i)^{-1}] = [1+i][u] = 0$ for any $u \in \{\pm 1, \pm i, 1+i\}$.

By the cases considered above, Lemma 5.14 assures that $[1+i][\pm 1 \pm i] = 0$. Using the ϵ-commutativity of Milnor-Witt K-groups we establish also the symmetric counterparts of all cases above. Finally, we consider the general case $[u(1+i)^n][u'(1+i)^m]$ for $n, m \in \mathbf{Z}$, $u, u' \in \mu_4$. By the second relation of Milnor-Witt K-theory along with Lemma 5.15 and Lemma 5.16 we have

$$\begin{aligned}
[u(1+i)^n][u'(1+i)^m] &= ([u] + n_\epsilon[1+i] + \eta[u]n_\epsilon[1+i])([u'] + m_\epsilon[1+i] + \eta[u']m_\epsilon[1+i]) \\
&= [u][u'] + m_\epsilon[u][1+i] + \eta n_\epsilon[u][u'][1+i] \\
&\quad + n_\epsilon[1+i][u'] + n_\epsilon m_\epsilon[1+i][1+i] + \eta n_\epsilon m_\epsilon[1+i][u'][1+i] \\
&\quad + \eta n_\epsilon[u][1+i][u'] + \eta m_\epsilon[u][1+i] + \eta^2 n_\epsilon m_\epsilon[u][1+i][u'][1+i].
\end{aligned}$$

In the last expression, all terms vanish by the cases considered above, so this concludes the proof. □

From here on we proceed identically as in Theorem 5.27 to obtain the isomorphism:

Theorem 5.33. *For each finite place v of $\mathbf{Q}(i)$, choose a uniformizer π_v. Then the map $\partial := \bigoplus_v \partial_v^{\pi_v}$ induces an isomorphism*

$$K_2^{MW}(\mathbf{Q}(i)) \cong \bigoplus_{v \in \mathrm{Pl}^{\mathrm{nc}}_{\mathbf{Q}(i)}} K_1^{MW}(k(v)) \cong \bigoplus_{v \in \mathrm{Pl}^{\mathrm{nc}}_{\mathbf{Q}(i)}} K_1^{M}(k(v)).$$

Final Remarks

The theory of motivic homotopy is quite new, and the discovery of Milnor-Witt K-theory is even newer. Thus there are yet many unanswered questions. One possibility for further studies is to try to see if there exist analogs of Hilbert symbols in Milnor-Witt K-theory—at least for K_2^{MW}. Recall that in algebraic K-theory we have Moore's theorem, stating that there is an exact sequence

$$K_2(F) \xrightarrow{h} \bigoplus_{v \in \mathrm{Pl}^{\mathrm{nc}}} \mu(F_v) \xrightarrow{\pi} \mu(F) \longrightarrow 1.$$

Here the map h is induced by the Hilbert symbols defined on the number field F. As we have seen in Chapter 2, the above exact sequence should be considered as a uniqueness theorem for Hilbert reciprocity.

On the other hand, in [Lam05, p.159], Lam defines Hilbert symbols in Witt theory and uses these to show that there is an exact sequence

$$0 \longrightarrow I^2(\mathbf{Q})/I^3(\mathbf{Q}) \longrightarrow \bigoplus_{v \in \mathrm{Pl}_{\mathbf{Q}}} I^2(\mathbf{Q}_v)/I^3(\mathbf{Q}_v) \longrightarrow \mathbf{Z}/2 \longrightarrow 0,$$

which is interpreted as a uniqueness theorem for Hilbert reciprocity in Witt theory. This result was originally proved for any global field F by Bass and Tate in the equivalent form [Mil70, Lemma A.1]

$$0 \longrightarrow k_2^M(F) \longrightarrow \bigoplus_{v \in \mathrm{Pl}_F^{\mathrm{nc}}} k_2^M(F_v) \longrightarrow \mathbf{Z}/2 \longrightarrow 0$$

(remember that $I^2(F)/I^3(F) \cong K_2^M(F)/2K_2^M(F) = k_2^M(F)$). As there is a uniqueness of reciprocity laws-theorem in both Milnor K-theory and Witt theory, this suggests that there should also be a corresponding result in Milnor-Witt K-theory that specializes to the two mentioned sequences. The first step toward such a result would be to define Hilbert symbols on Milnor-Witt K-theory.

Bibliography

[BMS67] H. Bass, J. Milnor, and J.-P. Serre. Solution of the congruence subgroup problem for SL_n $(n \geq 3)$ and Sp_{2n} $(n \geq 2)$. *Inst. Hautes Études Sci. Publ. Math.*, (33):59–137, 1967.

[BT73] H. Bass and J. Tate. The Milnor ring of a global field. In *Algebraic K-theory, II: "Classical" algebraic K-theory and connections with arithmetic (Proc. Conf., Seattle, Wash., Battelle Memorial Inst., 1972)*, pages 349–446. Lecture Notes in Math., Vol. 342. Springer, Berlin, 1973.

[CD12] Denis-Charles Cisinski and Frédéric Déglise. Triangulated categories of mixed motives, 2012. http://arxiv.org/abs/0912.2110.

[CF14] Baptiste Calmès and Jean Fasel. Finite Chow-Witt correspondences, 2014. http://arxiv.org/abs/1412.2989v1.

[Dal06] Chandan Singh Dalawat. Some aspects of the functor K_2 of fields. *J. Ramanujan Math. Soc.*, 21(2):129–151, 2006.

[DI05] Daniel Dugger and Daniel C. Isaksen. Motivic cell structures. *Algebr. Geom. Topol.*, 5:615–652, 2005.

[DI13] Daniel Dugger and Daniel C. Isaksen. Motivic Hopf elements and relations, 2013. http://arxiv.org/abs/1307.6596.

[DLØ+07] B. I. Dundas, M. Levine, P. A. Østvær, O. Röndigs, and V. Voevodsky. *Motivic homotopy theory*. Universitext. Springer-Verlag, Berlin, 2007. Lectures from the Summer School held in Nordfjordeid, August 2002.

[Dug04] Daniel Dugger. Notes on the Milnor conjectures, 2004. http://arxiv.org/abs/math/0408436.

[Ful98] William Fulton. *Intersection theory*, volume 2 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, second edition, 1998.

[Gar71] Howard Garland. A finiteness theorem for K_2 of a number field. *Ann. of Math. (2)*, 94:534–548, 1971.

[Gra03] Georges Gras. *Class field theory*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2003. From theory to practice, Translated from the French manuscript by Henri Cohen.

[Har77] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[HK01] Po Hu and Igor Kriz. The Steinberg relation in $\mathbb{A}^1$-stable homotopy. *Internat. Math. Res. Notices*, (17):907–912, 2001.

[Hov99] Mark Hovey. *Model categories*, volume 63 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1999.

[HT08] Kevin Hutchinson and Liqun Tao. A note on Milnor-Witt K-theory and a theorem of Suslin. *Comm. Algebra*, 36(7):2710–2718, 2008.

[HT10] Kevin Hutchinson and Liqun Tao. Homology stability for the special linear group of a field and Milnor-Witt K-theory. *Doc. Math.*, (Extra volume: Andrei A. Suslin sixtieth birthday):267–315, 2010.

[Hut04] Kevin Hutchinson. On tame and wild kernels of special number fields. *J. Number Theory*, 107(2):368–391, 2004.

[IR90] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[Jan96] Gerald J. Janusz. *Algebraic number fields*, volume 7 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, second edition, 1996.

[Jar00] J. F. Jardine. Motivic symmetric spectra. *Doc. Math.*, 5:445–553 (electronic), 2000.

[Keu97] Frans Keune. Quadratic number fields having $\{-1, -1\}$ as a non-trivial element of their wild kernel. *J. Number Theory*, 63(1):30–33, 1997.

[Lam05] T. Y. Lam. *Introduction to quadratic forms over fields*, volume 67 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2005.

[Lan70] Serge Lang. *Algebraic number theory*. Addison-Wesley Publishing Co., Inc., Reading, Mass.-London-Don Mills, Ont., 1970.

[Lem95] Franz Lemmermeyer. The Euclidean algorithm in algebraic number fields. *Exposition. Math.*, 13(5):385–416, 1995.

[Lem00] Franz Lemmermeyer. *Reciprocity laws*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2000. From Euler to Eisenstein.

[Lur09] Jacob Lurie. *Higher topos theory*, volume 170 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2009.

[MH73] John Milnor and Dale Husemoller. *Symmetric bilinear forms*. Springer-Verlag, New York-Heidelberg, 1973. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 73.

[Mil70] John Milnor. Algebraic K-theory and quadratic forms. *Invent. Math.*, 9:318–344, 1969/1970.

[Mil71] John Milnor. *Introduction to algebraic K-theory*. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1971. Annals of Mathematics Studies, No. 72.

[Mil13a] James S. Milne. Algebraic number theory (v3.05), 2013. Available at `www.jmilne.org/math/`.

[Mil13b] James S. Milne. Class field theory (v4.02), 2013. Available at `www.jmilne.org/math/`.

[Mil14] James S. Milne. Motives—Grothendieck's Dream (v2.04), 2014. Available at `www.jmilne.org/math/`.

[ML98] Saunders Mac Lane. *Categories for the working mathematician*, volume 5 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1998.

[Mor04a] Fabien Morel. *On the motivic π_0 of the sphere spectrum*, volume 131 of *NATO Sci. Ser. II Math. Phys. Chem.* Kluwer Acad. Publ., Dordrecht, 2004.

[Mor04b] Fabien Morel. Sur les puissances de l'idéal fondamental de l'anneau de Witt. *Comment. Math. Helv.*, 79(4):689–703, 2004.

[Mor05] Fabien Morel. The stable $\mathbb{A}^1$-connectivity theorems. *K-Theory*, 35(1-2):1–68, 2005.

[Mor12a] Fabien Morel. $\mathbf{A}^1$-algebraic topology over a field, 2012. Available at http://www.mathematik.uni-muenchen.de/~morel/Prepublications/A1TopologyLNM.pdf (visited 2016-04-08).

[Mor12b] Masanori Morishita. *Knots and primes.* Universitext. Springer, London, 2012. An introduction to arithmetic topology.

[MP02] Geoffrey M.L. Powell. Zariski excision and the Steinberg relation. 2002. Available at http://math.univ-angers.fr/~powell/documents/2002/steinberg.pdf (visited 2015-12-17).

[MV99] Fabien Morel and Vladimir Voevodsky. $\mathbf{A}^1$-homotopy theory of schemes. *Inst. Hautes Études Sci. Publ. Math.*, (90):45–143 (2001), 1999.

[MVW06] Carlo Mazza, Vladimir Voevodsky, and Charles Weibel. *Lecture notes on motivic cohomology*, volume 2 of *Clay Mathematics Monographs.* American Mathematical Society, Providence, RI; Clay Mathematics Institute, Cambridge, MA, 2006.

[OVV07] D. Orlov, A. Vishik, and V. Voevodsky. An exact sequence for $K^M_*/2$ with applications to quadratic forms. *Ann. of Math. (2)*, 165(1):1–13, 2007.

[PPR09] Ivan Panin, Konstantin Pimenov, and Oliver Röndigs. On Voevodsky's algebraic K-theory spectrum. In *Algebraic topology*, volume 4 of *Abel Symp.*, pages 279–330. Springer, Berlin, 2009.

[Qui73] Daniel Quillen. Higher algebraic K-theory. I. In *Algebraic K-theory, I: Higher K-theories (Proc. Conf., Battelle Memorial Inst., Seattle, Wash., 1972)*, pages 85–147. Lecture Notes in Math., Vol. 341. Springer, Berlin, 1973.

[Ros94] Jonathan Rosenberg. *Algebraic K-theory and its applications*, volume 147 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1994.

[RSØ16] Oliver Röndigs, Markus Spitzweck, and Paul Arne Østvær. The first stable homotopy groups of motivic spheres, 2016. http://arxiv.org/abs/1604.00365.

[Sch85] Winfried Scharlau. *Quadratic and Hermitian forms*, volume 270 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences].* Springer-Verlag, Berlin, 1985.

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics.* Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg.

[Sev06] Markus Severitt. Motivic homotopy types of projective curves, 2006. Available at https://www.math.uni-bielefeld.de/~rost/data/severitt.pdf (visited 2016-04-06).

[Str11] Jeffrey Strom. *Modern classical homotopy theory*, volume 127 of *Graduate Studies in Mathematics.* American Mathematical Society, Providence, RI, 2011.

[Tat71] John Tate. Symbols in arithmetic. In *Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 1*, pages 201–211. Gauthier-Villars, Paris, 1971.

[Tat76a] J. Tate. Problem 9: The general reciprocity law. In *Mathematical developments arising from Hilbert problems (Proc. Sympos. Pure Math., Northern Illinois Univ., De Kalb, Ill., 1974)*, pages 311–322. Proc. Sympos. Pure Math., Vol. XXVIII. Amer. Math. Soc., Providence, R. I., 1976.

[Tat76b] John Tate. Relations between K_2 and Galois cohomology. *Invent. Math.*, 36:257–274, 1976.

[Voe98] Vladimir Voevodsky. $\mathbf{A}^1$-homotopy theory. In *Proceedings of the International Congress of Mathematicians, Vol. I (Berlin, 1998)*, number Extra Vol. I, pages 579–604 (electronic), 1998.

[Was82] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1982.

[Wei94] Charles A. Weibel. *An introduction to homological algebra*, volume 38 of *Cambridge Studies in Advanced Mathematics.* Cambridge University Press, Cambridge, 1994.

[Wei04] Charles A. Weibel. A road map of motivic homotopy and homology theory, 2004. Available at `http://www.math.uiuc.edu/K-theory/630/roadmap.pdf` (visited 2016-03-17).

[Wei13] Charles A. Weibel. *The K-book*, volume 145 of *Graduate Studies in Mathematics.* American Mathematical Society, Providence, RI, 2013. An introduction to algebraic K-theory.

[Wym72] B. F. Wyman. What is a reciprocity law? *Amer. Math. Monthly*, 79:571–586; correction, ibid. 80 (1973), 281, 1972.