R. Hill
Nagoya Math. J.
Vol. 137 (1995), 77–144

A GEOMETRIC PROOF OF A RECIPROCITY LAW

RICHARD HILL

1. Introduction

In this paper we prove the reciprocity law for a Kummer extension of an algebraic number field K. The proof is similar to the proof of the same theorem by Kubota [14, 15]. Such methods were applied by Gauss [6, 7] to the cases $K = \mathbf{Q}$, $\mathbf{Q}(\sqrt{-1})$ and by Habicht [8] to the case $K = \mathbf{Q}(\sqrt{-3})$. We now discuss informally the structure of the proof. All definitions and statements made at this stage are only approximations to the truth, and shouldn't be used as references for the later chapters.

In the following K will always be a fixed algebraic number field containing all the q^{th} roots of unity, where q is some fixed natural number. We shall write $\mathfrak{O}$ for the ring of algebraic integers in K. A Kummer extension of K is a field extension of the form $K(\sqrt[q]{\alpha}) \supset K$, where α is an element of K. The reciprocity law for such an extension is a description of how prime ideals $\mathfrak{b} \subset \mathfrak{O}$ split in the ring of algebraic integers of the extension field. This statement can be rephrased as a statement about the Legendre symbols $\left(\frac{\alpha}{\mathfrak{b}}\right)_q$. The proof given here is a calculation of the Legendre symbol by way of a generalization of the Gauss lemma, which expresses the Legendre symbol in terms of a finite sum. Following Gauss [7] we shall refer to the finite sums which arise in this way as *decidents*.

We shall investigate these sums in §2 using purely arithmetical methods. Actually we prove more there than we later need in proving the reciprocity law. In particular it is unnecessary to consider ideals $\mathfrak{b}$ since we will only use the results for elements (i.e. principal ideals).

A decident is a sum of the form

$$\text{Dec}\,\frac{\alpha}{\mathfrak{b}} = \sum_{\pi,j} j f(\zeta^j \pi) f(\alpha\pi), \tag{1}$$

where π runs through a set of $\mathfrak{b}$-division points of the lattice $\mathfrak{O}$ and j runs from 1

Received October 14, 1993.

to q. The number ζ is a fixed primitive q^{th} root of unity. The function $f : \mathfrak{O} \setminus K \to \mathbf{Z}/q\mathbf{Z}$ belongs to a class of functions which we shall call the *fundamental functions*. A fundamental function is like the characteristic function of a fundamental domain for a certain group. The value of the decident is independent of f.

Decidents look like Dedekind sums, and they are in the case $K = \mathbf{Q}$ virtually the same thing. This connection is described in [20] in the case $K = \mathbf{Q}$, and is investigated in [21, 22, 23, 11, 12, 13] in other cases. We shall say nothing more about this here.

The Gauss lemma says that the Legendre symbol $\left(\frac{\alpha}{\mathfrak{b}}\right)_q$ is equal to $\zeta^{\mathrm{Dec}\frac{\alpha}{\mathfrak{b}}}$, where ζ the primitive q^{th} root of unity. We are therefore only interested in the congruency class of the decident modulo q.

We shall also investigate modulo q sums of the form:

$$\langle f^1, f^2 \rangle = \sum_{\pi,j} j f^1(\zeta^j \pi) f^2(\pi), \tag{2}$$

where f^1 and f^2 are both fundamental functions. These sums can be thought of a skew products of f^1 and f^2. They are bilinear and skew-symmetric, and satisfy in addition the following cocycle relation:

$$\langle f^1, f^3 \rangle = \langle f^1, f^2 \rangle + \langle f^2, f^3 \rangle.$$

There is a strong connection between these skew products and decidents. In a certain sense one has $\mathrm{Dec}\frac{\alpha}{\mathfrak{b}} = \langle f, f \circ \alpha \rangle$. A very similar kind of sum has been related in [1, 17, 18] to the signs of cubic and biquadratic Gauss sums.

To find out more about decidents than we know from §2, it becomes necessary to construct explicit examples of fundamental functions. We do this in §3. Our construction is essentially a map from the set of paths from 0 to 1 (in $K \otimes_{\mathbf{Q}} \mathbf{R}$) to the set of fundamental functions. If one takes a straight path from 0 to 1, then the corresponding fundamental function will be the characteristic function of a finite union of parallelotopes. If on the other hand the path is not straight, then the corresponding function could look like the characteristic function of a twisted parallelotope. The fundamental function could however take on other values than just zero and one, if the corresponding path is too far from being straight.

Also in §3 we derive a formula for the skew products (2) in the case that f^1 and f^2 are constructed from paths. The formula is given in terms of a homotopy between the two paths, which can be chosen more or less arbitrarily. The sum (2) is expressed as a linear combination of numbers of lattice points inside certain

sets, the sets being constructed from the chosen homotopy.

In §4 we obtain analytic results which solve some difficulties arising from the constructions of §3. These difficulties occur when a lattice point lies on the boundary of a certain set. It is then not easy to decide whether the point should be counted or not. In general we shall show that we have enough freedom in choosing our paths and homotopies, that we can always move the boundaries away from the relevant points. The results of §4 enable us to apply those of §3.

In §5 use the results of §2 and §3 to prove the following theorem.

THEOREM 1. *Let K be an algebraic number field with ring of integers $\mathfrak{O}$. If K contains all q^{th} root of unity then there is an ideal $\mathfrak{f}$ of $\mathfrak{O}$ such that for all coprime elements $\alpha, \beta \in \mathfrak{O}$ with $\alpha \equiv \beta \equiv 1 \bmod \mathfrak{f}$ and α and β totally positive one has:*

$$\left(\frac{\alpha}{\beta}\right)_q = \left(\frac{\beta}{\alpha}\right)_q.$$

(*The left and right hand sides here are Legendre symbols.*)

The proof in §5 is similar to that given by Habicht [8] in the case $K = \mathbf{Q}(\sqrt{-3})$.

Using this we will prove in 1.4 the theorem proved by Kubota [14]:

THEOREM 2. *If K is an algebraic number field with ring of integers $\mathfrak{O}$ and if K contains all q^{th} root of unity, then there is an ideal $\mathfrak{f} \subset \mathfrak{O}$ such that for all $\alpha \in \mathfrak{O}$ and all totally positive $\beta \in \mathfrak{O}$ with $\beta \equiv 1 \bmod \alpha\mathfrak{f}$ one has:*

$$\left(\frac{\alpha}{\beta}\right)_q = 1.$$

Together Theorems 1 and 2 imply immediately:

THEOREM 3. *If K is an algebraic number field with ring of integers $\mathfrak{O}$ containing all q^{th} roots of unity, then there is an ideal $\mathfrak{f} \subset \mathfrak{O}$ such that for all totally positive $\alpha \in \mathfrak{O}$ with $\alpha \equiv \bmod \mathfrak{f}$ one has for all $\beta \in \mathfrak{O}$ coprime to $\alpha\mathfrak{f}$:*

$$\left(\frac{\alpha}{\beta}\right)_q = \left(\frac{\beta}{\alpha}\right)_q.$$

These theorems were first proved by Furtwängler [2, 3, 4, 5] using ideas from the work of Hilbert [9, 10].

1.1. Theorem 1 implies Theorem 2

We shall now assume Theorem 1, and use it to prove Theorem 2. We will do this in a sequence of lemmas. Suppose that Theorem 1 holds with the ideal $\mathfrak{f}_1$, which we may assume to be principal. We now fix an $\alpha \in \mathfrak{O}$. Depending on the real signs of α (for which there are only finitely many possibilities) we modify $\mathfrak{f}_1$ to make $\alpha\mathfrak{f}_1$ totally positive.

LEMMA. *For any $\varepsilon \in \mathfrak{O}$ and all $\beta \equiv 1 \bmod \mathfrak{f}_1$ with $(\beta, \alpha\varepsilon) = 1$ and β totally positive, one has*

$$\left(\frac{\alpha\mathfrak{f}_1}{\beta}\right)_q = \left(\frac{\alpha\mathfrak{f}_1}{\beta + \alpha\varepsilon^q\mathfrak{f}_1}\right)_q.$$

Proof. Let $\gamma = \beta + \alpha\varepsilon^q\mathfrak{f}_1$. Then $\gamma \equiv 1 \bmod \mathfrak{f}_1$ and is totally positive so by Theorem 1 we have $\left(\frac{\gamma}{\beta}\right)_q = \left(\frac{\beta}{\gamma}\right)_q$. Since $\gamma \equiv \alpha\varepsilon^q\mathfrak{f}_1 \bmod \beta$ and $\beta \equiv -\alpha\varepsilon^q\mathfrak{f}_1 \bmod \gamma$ we have $\left(\frac{\alpha\varepsilon^q\mathfrak{f}_1}{\beta}\right)_q = \left(\frac{-\alpha\varepsilon^q\mathfrak{f}_1}{\gamma}\right)_q$. Our conditions on β imply by Euler's criterion that $\left(\frac{-1}{\gamma}\right)_q = 1$. We therefore have as required $\left(\frac{\alpha\mathfrak{f}_1}{\beta}\right)_q = \left(\frac{\alpha\mathfrak{f}_1}{\gamma}\right)_q$.

LEMMA. *There is an ideal $\mathfrak{f}_2 \subset \mathfrak{O}$ such that every element γ of $\mathfrak{f}_2$ can be expressed as a finite sum*

$$\gamma = \sum a_i\varepsilon_i^q$$

where the $\varepsilon \in \mathfrak{O}$ are all congruent to 1 modulo $\mathfrak{f}_1$ and totally positive and the a_i are in $\mathbf{Z}$.

Proof. If this were not the case then all the ε^q for $\varepsilon \equiv 1 \bmod \mathfrak{f}_1$ and totally positive would lie in some proper subspace V of the real vector space $K \otimes_{\mathbf{Q}} \mathbf{R}$. This would imply that all $(\varepsilon/n)^q$ would also be in V for $n \in \mathbf{N}$. This cannot happen because these elements are dense in a neighbourhood of 1 in $K \otimes_{\mathbf{Q}} \mathbf{R}$.

LEMMA. *For all $\beta \equiv \beta' \bmod \alpha\mathfrak{f}_1\mathfrak{f}_2$ with $\beta = 1 \bmod \mathfrak{f}_1$, $(\alpha, \beta) = 1$ and both β and β' totally positive, one has*

$$\left(\frac{\alpha\mathfrak{f}_1}{\beta}\right)_q = \left(\frac{\alpha\mathfrak{f}_1}{\beta'}\right)_q.$$

Proof. By the previous lemma one can write $\beta - \beta'$ as a sum of elements $\pm \varepsilon^q \alpha \mathfrak{f}_1$. By induction one can assume that $\beta - \beta' = \varepsilon^q \alpha \mathfrak{f}_1$ with $\varepsilon \equiv 1 \bmod \mathfrak{f}_1$ and ε totally positive. If $(\beta, \varepsilon) = 1$ then the lemma then follows by the first lemma. If this is not the case then we may decompose ε as a product of ideals $\varepsilon = \varepsilon_\beta \cdot \varepsilon'$ with $(\varepsilon', \beta) = 1$ and ε_β divisible only by primes which divide β. We choose a $\phi \in \mathfrak{O}$ such that $\phi \equiv 1 \bmod \beta\beta'\varepsilon_\beta$ and $\phi \equiv 0 \bmod \varepsilon'$. This gives us $(\phi, \beta) = (\phi, \beta') = 1$ and also

$$(\beta + \alpha \mathfrak{f}_1 \phi^q, \varepsilon) = (\beta + \alpha \mathfrak{f}_1 \phi^q, \varepsilon_\beta) \cdot (\beta + \alpha \mathfrak{f}_1 \phi^q, \varepsilon') = 1.$$

Now applying the first lemma three times we get as before

$$\left(\frac{\alpha \mathfrak{f}_1}{\beta}\right)_q = \left(\frac{\alpha \mathfrak{f}_1}{\beta + \alpha \mathfrak{f}_1 \phi^q}\right)_q = \left(\frac{\alpha \mathfrak{f}_1}{\beta + \alpha \mathfrak{f}_1 \phi^q + \alpha \mathfrak{f}_1 \varepsilon^q}\right)_q = \left(\frac{\alpha \mathfrak{f}_1}{\beta' + \alpha \mathfrak{f}_1 \phi^q}\right)_q = \left(\frac{\alpha \mathfrak{f}_1}{\beta'}\right)_q.$$

This now gives us:

THEOREM. *Theorem 2 holds with* $\mathfrak{f} = \mathfrak{f}_1 \mathfrak{f}_2$.

2. Global notation, definitions and general lemmas

In this chapter we define in paragraphs §2.2 to §2.6 the terms *fundamental function* and *decident,* which we will investigate in the rest of the paper. In paragraph §2.7 we prove some unsurprising facts about division points of lattices, which we will use later. In paragraphs §2.8 to §2.10 we prove elementary, arithmetical facts about fundamental functions and decidents. Paragraph §2.11 is the Gauss-Schering lemma. In paragraph §2.12 we prove a lemma, which often occurs in proofs of the quadratic reciprocity law. The lemma was also used by Habicht [8] in the case $K = \mathbf{Q}(\sqrt{-3})$. It hasn't however appeared before in this generality. Finally we introduce in §2.13 the skew product of two fundamental functions. This will be useful in simplifying certain calculations in chaper §5.

2.1. Notation

From now on K will be an algebraic number field of degree n over $\mathbf{Q}$. The ring of the integers in K will be written $\mathfrak{O}$. $\mu_q \subset \mathfrak{O}$ will be the multiplicative group of q^{th} roots of unity, where q is a power of a prime p. We choose a primitive q^{th} root of unity $\zeta \in \mu_q$ and a primitive q^{th} root of unity $\rho \in \mu_q$. The notation K_∞ will mean the ring $K \otimes_{\mathbf{Q}} \mathbf{R}$. This is isomorphic to the direct sum of all infinite completions of K, and the diagonal embedding of K in K_∞ makes K a dense

subring of K_∞. This is summarized in the diagram:

$$\begin{array}{ccccccccc} \mu_p & \subset & \mu_q & \subset & \mathfrak{O} & \subset & K & \subset & K_\infty \\ \| & & \| & & \cup & & \cup & & \cup \quad (\text{degree } [K : \mathbf{Q}] = n) \\ \langle \rho \rangle & & \langle \zeta \rangle & & \mathbf{Z} & & \mathbf{Q} & & \mathbf{R} \end{array}$$

2.2. The cyclotomic crystallographic group

In this paragraph we define a group Γ of transformations of K (or of K_∞). We also describe the fixed points of Γ. Following Kubota [14] we call the group a *cyclotomic crystallographic group.*

The group Γ is important for us because our 'fundamental functions' will be fundamental with respect to this group, similarly to the way in which a fundamental domain is fundamental for a given group.

Let r and t be elements of K. We define affine functions

$$\begin{aligned} \sigma(r, t) &: K \to K \\ &\quad z \mapsto rz + t, \\ \sigma_1(r) &: K \to K \\ &\quad z \mapsto rz, \\ \sigma_2(t) &: K \to K \\ &\quad z \mapsto z + t. \end{aligned}$$

Thus σ is a map from $K^\times \times K$ to the set of affine bijections of K.

Now let L be a $\mathbf{Z}[\zeta]$-submodule of K, which is in addition a lattice in K_∞. For any such L we define a cyclotomic crystallographic group,

$$\Gamma(L, q) := \{\sigma(r, t) \mid r \in \mu_q \text{ and } t \in L\}.$$

Since L is μ_q-invariant, it follows that this is a group with composition of functions as the group law. It will sometimes be abbreviated $\Gamma(L)$ or simply Γ. We can think of L and μ_q as subgroups of $\Gamma(L, q)$ by identifying them with their images under σ_2 and σ_2. With this identification, Γ is a semi-direct product of L and μ_q, L being the normal subgroup and μ_q acting on L by the usual multiplication in K.

$$\Gamma(L, q) = L.\mu_q = \mu_q.L, \quad L \cap \mu_q = \{\mathrm{id}\}.$$

The action of Γ on K can be extended to an action on $K_\infty := K \otimes_{\mathbf{Q}} \mathbf{R}$. Since L is a lattice in K_∞, and L has finite index q in $\Gamma(L, q)$, we conclude that $\Gamma(L, q)$ is discrete and cocompact. The points of K_∞, which are fixed by non-trivial elements of $\Gamma(L)$ are exactly the points in $\dfrac{1}{1-\rho} L$.

This can be seen as follows: let $z \in K_\infty$ and $\sigma(r, t) \in L(L, q)$ such that $(\sigma(r, t))(z) := rz + t = z$. We then have $rz \equiv z \bmod L$. Since μ_p is a minimal subgroup of μ_q, we have $\rho z \equiv z \bmod L$; or in other words, there is an element t' in L such that $\rho z = z + t'$. From this we have $z = \frac{1}{1-\rho} t'$ and therefore $z \in \frac{1}{1-\rho} L$.

On the other hand if $z = \frac{1}{1-\rho} t$, where $t \in L$, then $z = \rho z + t = (\sigma(\rho, t))(z)$.

2.3. Quotient spaces and projections

We shall often be interested in the quotient spaces $L \backslash K_\infty$ and $\Gamma \backslash K_\infty$. The projection maps between these spaces will be written as follows:

$$\mathrm{pr}_L : K_\infty \to L \backslash K_\infty,$$
$$\mathrm{pr}_\Gamma : K_\infty \to \Gamma \backslash K_\infty,$$
$$\text{and } \mathrm{pr}_\Gamma^L : L \backslash K_\infty \to \Gamma \backslash K_\infty.$$

Now let ϕ be a function (to any set), defined on $L \backslash K_\infty$ (resp. $\Gamma \backslash K_\infty$). We then define as usual

$$\mathrm{pr}_L^*(\phi) := \phi \circ \mathrm{pr}_L$$
$$(\text{resp. } \mathrm{pr}_\Gamma^{L*}(\phi) := \phi \circ \mathrm{pr}_\Gamma^L$$
$$\text{and } \mathrm{pr}_\Gamma^*(\phi) := \phi \circ \mathrm{pr}_\Gamma).$$

If ϕ is a function with compact support into an additive, abelian group A, and defined for example on K_∞, then we define

$$\begin{aligned} \mathrm{pr}_{L*}(\phi) : L \backslash K_\infty &\to A \\ \pi &\mapsto \textstyle\sum_{\mathrm{pr}_L(z)=\pi} \phi(z) \\ \mathrm{pr}_{\Gamma*}(\phi) : \Gamma \backslash K_\infty &\to A \\ \varpi &\mapsto \textstyle\sum_{\mathrm{pr}_\Gamma(z)=\varpi} \phi(z). \end{aligned}$$

Since ϕ has compact support, these sums have only finitely many non-zeto terms.

In general we shall try to refer to elements of K or K_∞ as z; elements of $L \backslash K_\infty$ as π and elements of $\Gamma \backslash K_\infty$ as ϖ.

2.4. Fundamental functions

We now define the term *fundamental function*. The idea of generalizing the concept of a fundamental domain in this way, is due to Kubota.

A function $f : K_\infty \to \mathbf{Z}/q\mathbf{Z}$ with compact support will be called fundamental for Γ at a point $\varpi \in \Gamma\backslash K_\infty$, iff

$$\sum_{\mathrm{pr}_L(z)=\varpi} f(z) = (\mathrm{pr}_{\Gamma *} f)(\varpi) \equiv 1 \bmod q.$$

From this condition follows immediately

$$\sum_{\sigma\in\Gamma} f(\sigma z) = \#\,\mathrm{Stab}_\Gamma(z) \bmod q,$$

where $\mathrm{pr}_\Gamma(z) = \varpi$. Since f has compact support, all these sums have only finitely many non-zero terms. We shall say that f is fundamental for Γ, if it satisfies this condition for every $\varpi \in \Gamma\backslash K$. For example, the characteristic function of a system of representatives for Γ-orbits in K_∞ is always fundamental.

Now let $f : L\backslash K_\infty \to \mathbf{Z}/q\mathbf{Z}$ be a function defined on the quotient space. Analogously we call f fundamental for μ_q at ϖ, iff

$$\sum_{\mathrm{pr}^L_\Gamma(\pi)=\varpi} f(\pi) = (\mathrm{pr}^L_{\Gamma *} f)(\varpi) \equiv 1 \bmod q.$$

f is called fundamental for μ_q if it is fundamental for μ_q at every $\varpi \in \Gamma\backslash K_\infty$.

If $f : K_\infty \to \mathbf{Z}/q\mathbf{Z}$ is fundamental for $\Gamma(L, q)$, then obviously $(\mathrm{pr}_{L*} f) : L\backslash K_\infty \to \mathbf{Z}/q\mathbf{Z}$ will be fundamental for μ_q.

2.5. The periodic functions θ_f

Let f be fundamental for $\Gamma(L)$. To such an f we define a corresponding periodic function

$$\theta = \theta_f : K \to \mathbf{Z}/q\mathbf{Z}$$
$$z \mapsto \sum_{j=1}^{q-1} j \sum_{t\in L} f(\sigma(\zeta^{-j}, t)(z)).$$

Sometimes we will have to deal with many different fundamental function f, f', f'', etc. simultaneously. The corresponding periodic functions will be written with the same superscripts:

$$\theta' := \theta_{f'},$$
$$\theta'' := \theta_{f''}, \text{ etc.}$$

The function θ is periodic with lattice of periods L. By abuse of notation we shall often write

$$\begin{aligned} \theta: \ K/L &\to \mathbf{Z}/q\mathbf{Z} \\ z+L &\mapsto \theta(z) \end{aligned}$$

and also (by a less trivial abuse of notation)

$$\begin{aligned} f: \ K/L &\to \mathbf{Z}/q\mathbf{Z} \\ z+L &\mapsto \textstyle\sum_{t\in L} f(z+t) \end{aligned}$$

or in the language of §2.3, $f = \mathrm{pr}_{L*}(f)$. The following easily proved equation will be continually used without further clarification.

2.5.1 Lemma. *Let z be an element of K, and let $\pi = \mathbf{pr}_L(z)$, the projection of z in $L \setminus K$. Then*

$$\#\,\mathrm{Stab}_{\Gamma(L,q)}(z) = \#\,\mathrm{Stab}_{\mu_q}(\pi).$$

Proof. Let $\sigma(r, t) \in \Gamma(q, L)$ with $(\sigma(r, t))(z) = z$. We then have $rz + t = z$, thus $rz \equiv z$ modulo L or in other words $r\pi = \pi$. This means that $r \in \mathrm{Stab}_{\mu_q}(\pi)$.

Now let r be any element of $\mathrm{Stab}_{\mu_q}(\pi)$. We have $r\pi = \pi$. There is thus a $t \in L$ such that $rz + t = z$, or in other words $\sigma(r, t) \in \mathrm{Stab}_{\Gamma(q,L)}(z)$. Since the translation t is obviously unique, we know that $\#\,\mathrm{Stab}_\Gamma(z) = \#\,\mathrm{Stab}_{\mu_q}(\pi)$.

2.6. The decident

As above let L be a $\mathbf{Z}[\zeta]$-lattice. Let $\mathfrak{O}_L := \{z \in K \mid zL \subset L\}$ be the order associated to the lattice L. We now define the decident. This is a function of four variables: a lattice L; a function f, which is fundamental for $\Gamma(L, q)$; an element $\alpha \in \mathfrak{O}_L$ and an ideal $\mathfrak{b} \subset \mathfrak{O}_L$. Later we shall see that the value of the decident is to a certain extent independent of L and f.

Let $\alpha \in \mathfrak{O}_L$ and $\mathfrak{b}$ be an ideal of $\mathfrak{O}_L$. Let $\mathfrak{b}^{-1}$ be the fractional $\mathfrak{O}_L$-ideal $\{a \in K \mid a\mathfrak{b} \subset \mathfrak{O}_L\}$. We define the decident of α with respect to $\mathfrak{b}$ as follows:

$$\begin{aligned} \mathrm{Dec}_L \frac{\alpha}{\mathfrak{b}} &:= \sum_{z \in \mathfrak{b}^{-1}L \setminus L} f(z)\ \theta_f(\alpha z) \mod q \\ &= \sum_{\pi \in K/L \setminus L\{0\} \mid \mathfrak{b}\pi = 0} f(\pi)\ \theta_f(\alpha\pi) \mod q, \end{aligned}$$

where f is fundamental for $\Gamma(L)$. We shall see, that the decident is independent of

the choice of f, as long as αq and $\mathfrak{b}$ are coprime in $\mathfrak{O}_L$. Occasionally the notation $\mathrm{Dec}_L^{(f)} \frac{\alpha}{\mathfrak{b}}$, will be used to stress the choice of fundamental function f.

It is usually the case that arithmetical investigation of the decident can be carried out more easily in the quotient space $L \setminus K_\infty$. The reason for this is that the action of μ_q on $L \setminus K_\infty$ commutes with the action of α, whereas the action of Γ on K_∞ does not.

2.7. Division points of L

Arithmetical properties of rings such as $\mathfrak{O}_L$ are often disregarded in books on algebraic number theory. For this reason we collect here the results on this subject which we need, rather than citing results from literature. A fuller treatment of these rings can be found in Hilbert's Zahlbericht [9].

Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of $\mathfrak{O}_L$. We shall say that $\mathfrak{a}$ and $\mathfrak{b}$ are coprime in $\mathfrak{O}_L$ iff

$$\mathfrak{a} + \mathfrak{b} = \mathfrak{O}_L.$$

If α or β are elements rather than ideals, then they will be called coprime if the principle ideals which they generate are coprime. An element z of K is an $\mathfrak{a}$-division point of L, iff for every $\alpha \in \mathfrak{a}$ one has

$$az \in L.$$

We shall write $\bar{S}_\mathfrak{a}$ for the set of all $\mathfrak{a}$-division points of L. This is an additive group. Furthermore let $S_\mathfrak{a} = \bar{S}_\mathfrak{a} \setminus \{0\}$.

2.7.1 Lemma. *The ring $\mathbf{Z}[\zeta]$ is contained in the ring $\mathfrak{O}_L$, and there is a natural number $\mathfrak{d}$ with the property that $\mathfrak{d}\mathfrak{O} \subset \mathfrak{O}_L$.*

Proof. The first statement is obvious, since L is a $\mathbf{Z}[\zeta]$-module. For the second, we can suppose without loss of generality that $\mathfrak{O}$ is contained in the lattice L. We choose $\mathfrak{d} \in \mathbf{N}$ with the property that $\mathfrak{d}L \subset \mathfrak{O}$. Now let a be any element of $\mathfrak{O}$. We must show that $a\mathfrak{d} \in \mathfrak{O}_L$. This is however equivalent to saying that $a\mathfrak{d}L \subset L$, which follows from the following reasoning.

$$a\mathfrak{d}L \subset a\mathfrak{O} \subset \mathfrak{O} \subset L.$$

2.7.2 Lemma. *If $\mathfrak{a}$ and $\mathfrak{b}$ are coprime in $\mathfrak{O}_L$, and if z is both an $\mathfrak{a}$-division point and also a $\mathfrak{b}$-division point, then z is in L. If on the other hand $\mathfrak{a}$ and $\mathfrak{b}$ are*

arbitrary $\mathfrak{O}_L$-ideals with the property that every $\mathfrak{a}$- *and* $\mathfrak{b}$-*division point of* L *is an element of* L, *then* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are coprime in* $\mathfrak{O}_L$.

Proof. We only prove the first statement; the argument can be easily reversed. We have $\mathfrak{a}z \subset L$ and $\mathfrak{b}z \subset L$. Since L is additively closed, we also have $(\mathfrak{a}+\mathfrak{b})z \subset L$. However $\mathfrak{a}$ and $\mathfrak{b}$ are coprime, so $\mathfrak{O}_L z$ is contatined in L. The lemma follows because $\mathfrak{O}_L$ has a unit element.

2.7.3 Lemma. *Let* $\mathfrak{b}$ *be as in* §2.7.1 *and let* $\mathfrak{a}$ *and* $\mathfrak{b}$ *be ideals of* $\mathfrak{O}_L$. *If* $\mathfrak{a}\mathfrak{O}$, $\mathfrak{b}\mathfrak{O}$ *and* $\mathfrak{b}\mathfrak{O}$ *are pairwise coprime as* $\mathfrak{O}$-*ideals, then* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are coprime as* $\mathfrak{O}_L$-*ideals. If on the other hand* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are coprime* $\mathfrak{O}_L$-*ideals, then* $\mathfrak{a}\mathfrak{O}$ *and* $\mathfrak{b}\mathfrak{O}$ *are coprime in* $\mathfrak{O}$.

Proof. We prove the first statement first. Let $\mathfrak{a}\mathfrak{O}$, $\mathfrak{b}\mathfrak{O}$ and $\mathfrak{b}\mathfrak{O}$ be coprime in $\mathfrak{O}$. Again we suppose that $\mathfrak{b}L \subset \mathfrak{O} \subset L$. Let z be both an $\mathfrak{a}$-division point and a $\mathfrak{b}$-division point of L. Then $\mathfrak{b}z$ is also an $\mathfrak{a}$- and $\mathfrak{b}$-division point of $\mathfrak{O}$. We thus have $\mathfrak{b}z \in \mathfrak{O}$. Since $\mathfrak{O}$ is contained in L, we must have $\mathfrak{b}z \in L$. If $\mathfrak{a}$ and $\mathfrak{b}$ were coprime in $\mathfrak{O}_L$, then we could deduce from §2.7.2 that $z \in L$, and therefore that $\mathfrak{a}$ and $\mathfrak{b}$ are coprime in $\mathfrak{O}_L$. Thus it remains only to show that $\mathfrak{a}$ and $\mathfrak{b}$ are coprime in $\mathfrak{O}_L$. Since $\mathfrak{b} \in \mathbf{N}$, we know that $N(\mathfrak{a}\mathfrak{O})$ and $\mathfrak{b}$ are coprime in $\mathfrak{O}$. This implies that $N(\mathfrak{a}\mathfrak{O})$ and $\mathfrak{b}$ are coprime in $\mathbf{Z}$, so

$$\mathfrak{a}\mathfrak{O}_L + \mathfrak{b}\mathfrak{O}_L \supset N(\mathfrak{a})\mathbf{Z} + \mathfrak{b}\mathbf{Z} = \mathbf{Z} \ni 1.$$

We therefore have $\mathfrak{a}\mathfrak{O}_L + \mathfrak{b}\mathfrak{O}_L = \mathfrak{O}_L$.

Now let $\mathfrak{a}$ and $\mathfrak{b}$ be coprime in $\mathfrak{O}_L$. That means $\mathfrak{a}+\mathfrak{b} = \mathfrak{O}_L$ and therefore $1 \in \mathfrak{a}+\mathfrak{b}$. From this follows $1 \in \mathfrak{a}\mathfrak{O} + \mathfrak{b}\mathfrak{O}$, and therefore $\mathfrak{a}\mathfrak{O} + \mathfrak{b}\mathfrak{O} = \mathfrak{O}$.

2.7.4 Lemma. *Let* α *be an element of* $\mathfrak{O}_L$. *Then* $\bar{S}_\alpha$ *has exactly* $N(\alpha)$ *elements*[1] *If* a *and* q *are coprime then*

$$N(\alpha) \equiv 1 \bmod q.$$

Let $\mathfrak{b}$ *be an ideal of* $\mathfrak{O}_L$, *which is coprime in* $\mathfrak{O}_L$ *to* q. *Then*

$$\#\,\bar{S}_\mathfrak{b} \equiv 1 \bmod q.$$

Proof. The automorphism $K_\infty \to K_\infty$, $z \mapsto \alpha z$ has module $N(\alpha)$ (see eg. [24]). Since $L \setminus K_\infty$ is compact, the endomorphism

[1] here $N(\alpha)$ is the cardinality of the quotient $\mathfrak{O}/\alpha\mathfrak{O}$.

$$L \setminus K_\infty \to L \setminus K_\infty$$
$$\pi \mapsto \alpha\pi$$

must have degree $N(\alpha)$. Now let $\mathfrak{b}$ and q be coprime. Let π be a non-zero element of $\bar{S}_\mathfrak{b}$. Then by §2.7.2 π cannot be a q-division point. From this and §2.2 it follows that π has trivial stabilizer in μ_q. The μ_q-orbit of π thus has q element, all of which lie in $\bar{S}_\mathfrak{b}$. The lemma now follows from the observation that $\bar{S}_\mathfrak{b}$ is a disjoint union of μ_q-orbits.

2.7.5 Lemma. *Let α and β coprime elements of $\mathfrak{O}_L$. Then*

$$\bar{S}_{\alpha\beta} = \bar{S}_\alpha \oplus \bar{S}_\beta.$$

Proof. Let π_1 be an element of $\bar{S}_\alpha$ and π_2 an element of $\bar{S}_\beta$. Then $\alpha\beta(\pi_1 + \pi_2) = \alpha\beta\pi_1 + \alpha\beta\pi_2 = 0 + 0 = 0$. We therefore have $\pi_1 + \pi_2 \in \bar{S}_{\alpha\beta}$. There is thus a homomorphism

$$\Phi : \bar{S}_\alpha \oplus \bar{S}_\beta \to \bar{S}_{\alpha\beta}$$
$$(\pi_1, \pi_2) \mapsto \pi_1 + \pi_2.$$

Let $(\pi_1, -\pi_2)$ be in the kernel of the map Φ. That means $\pi_1 = \pi_2$. By §2.7.2, π_1 and π_2 must both be zero. Therefore Φ is injective. In addition we know from §2.7.4 that

$$\#\,\bar{S}_{\alpha\beta} = N(\alpha\beta) = N(\alpha)N(\beta) = \#\,(\bar{S}_\alpha \times \bar{S}_\beta),$$

so the map Φ is an isomorphism.

2.8. Some small lemmas

We now begin investigating the functions f, θ and Dec. Our methods in this chapter are arithmetical.

If one had a different group Γ acting on a different space X, then one could define corresponding fundamental functions and decidents for this action. One would then be able to prove similar statements to those in §2.8, 2.9, 2.10, 2.12. On the other hand there is no Gauss-Schering lemma to make such a generalization worthwhile.

Let L be a lattice and $L(L, q)$ the corresponding cyclotonic crystallographic group.

Let f, f', f'', f''' be fundamental for $\Gamma(L)$;

$\theta = \theta_f$,
$\theta' = \theta_f$, etc.
$S \subset K/L$ fonite μ_q-invariant subset.
Then the following identities hold in $\mathbf{Z}/q\mathbf{Z}$: -

1. *The function* $\theta : K_\infty \to \mathbf{Z}/q\mathbf{Z}$ *has the following transformation behaviour with respect to the group* $\Gamma(L, q)$:

$$\theta(\sigma(z)) \equiv \theta(z) + k \# \mathrm{Stab}_{\Gamma(L,q)}(z),$$

where $\sigma(z) = \zeta^k z + t$ *and* $t \in L$.
We have similarly for the functions $\theta : L \setminus K_\infty \to \mathbf{Z}/q\mathbf{Z}$:

$$\theta(\zeta^k \pi) \equiv \theta(\pi) + k \# \mathrm{Stab}_{\mu_q}(\pi).$$

2.
$$\sum_{\pi \in S} (f(\pi) - f'(\pi))(\theta''(\pi) - \theta'''(\pi)) \equiv 0.$$

3.
$$\sum_{\pi \in S} f(\pi)\, \theta'(\pi) \equiv - \sum_{\pi \in S} f'(\pi)\, \theta(\pi).$$

$$\sum_{\pi \in S} f(\pi)\, \theta(\pi) \equiv \begin{cases} 0 & \text{if } q \text{ is odd,} \\ \dfrac{q}{2} \# (S^{\mu_q}) & \text{if } q \text{ is even.} \end{cases}$$

Here S^{μ_q} *is the set if elements of* S *which are fixed by every element of* μ_q. *In applications of this formula this set will always be empty.*

4. *If* α *is an element of* $\mathfrak{O}_L$ *and* $\mathfrak{b}$ *an ideal of* $\mathfrak{O}_L$, *which is coprime to* αq *in* $\mathfrak{O}_L$, *then the decident* $\mathrm{Dec}_L \dfrac{\alpha}{\mathfrak{b}}$ *is independent of the choice of fundamental function* f.

5. *If* α *is an element of* $\mathfrak{O}_L$ *and* $\mathfrak{b}$ *an ideal of* $\mathfrak{O}_L$, *which is coprime to* αq *in* $\mathfrak{O}_L$, *then*

$$\mathrm{Dec}_L \frac{\alpha}{\mathfrak{b}} \equiv \sum_{\mathfrak{b}\pi = 0, \pi \neq 0} f(\pi)(\theta'(\alpha\pi) - \theta'(\pi)).$$

Here the sum is over those $\pi \in L \setminus K$ *which correspond to non-zero* $\mathfrak{b}$*-division points of* L.

Proofs.

1. By definition of θ we have

$$\theta(\zeta^k\pi) = \sum_{j=0}^{q-1} jf(\zeta^{-j}\zeta^k\pi) \equiv \sum_{j=0}^{q-1} (j+k)f(\zeta^{-j}\pi) \equiv \theta(\pi) + k\sum_{j=0}^{q-1} f(\zeta^{-j}\pi) \bmod q$$
$$\equiv \theta(\pi) + k\,\#\,\mathrm{Stab}_{\mu_q}(\pi) \bmod q, \text{ because } f \text{ is fundamental.}$$

2. From (1) we know that $\theta'' - \theta'''$ is constant modulo q on μ_q-orbits in K/L. Let $[\pi]$ be such an orbit. Then

$$\begin{aligned} \textstyle\sum_{\pi' \in [\pi]} f(\pi') &\equiv 1 \bmod q, && \text{because } f \text{ is fundamental} \\ &\equiv \textstyle\sum_{\pi' \in [\pi]} f'(\pi'), && \text{because } f' \text{ is fundamental} \end{aligned}$$

One therefore has

$$\sum_{\pi' \in [\pi]} (f(\pi') - f'(\pi'))(\theta''(\pi') - \theta'''(\pi')) \equiv (\sum_{\pi' \in [\pi]} f(\pi') - f'(\pi'))(\theta''(\pi) - \theta'''(\pi)) \equiv 0.$$

Since S is a disjoint union of μ_q-orbits, the result follows.

3. By definition of θ it follows that

$$\sum_{\pi \in S} f(\pi)\theta'(\pi) \equiv \sum_{\pi \in S, j=1 \ldots q-1} jf(\pi)f'(\zeta^{-j}\pi).$$

We now replace π by $\zeta^{-j}\pi$. Here we use the fact that S is invariant under the action of μ_q. The sum is then

$$\sum_{\pi \in S, j=1 \ldots q-1} jf(\zeta^j\pi)f'(\pi).$$

We now replace j by $q - j$. Since j still takes the same values, we have

$$\sum_{\pi \in S, j=1 \ldots q-1} (q-j)f(\zeta^{-j}\pi)f'(\pi).$$

We split the q and the $-j$ and obtain two sums

$$+ q \sum_{\pi \in S, j=1 \ldots q} f(\zeta^j\pi)f'(\pi) - \sum_{\pi \in S} \theta(\pi)f'(\pi).$$

The result follows from this.

4. We shall show, that $\mathrm{Dec}_L^{(f)} \frac{\alpha}{\mathfrak{b}} - \mathrm{Dec}_L^{(f')} \frac{\alpha}{\mathfrak{b}}$ is congruent to 0 modulo q.

This is equal to

$$\sum (f(\pi)\theta(\alpha\pi) - f'(\pi)\theta'(\alpha\pi)),$$

where π runs through the set $S_{\mathfrak{b}} = \{\pi \in L \setminus K \mid \mathfrak{b}\pi = 0 \text{ but } \pi \neq 0\}$. Multiplication by α induces a permutation of $S_{\mathfrak{b}}$ and this action commutes with the action of μ_q on $S_{\mathfrak{b}}$. The above sum is equal to

$$\sum (f(\pi)(\theta(\alpha\pi) - \theta'(\alpha\pi)) + (f(\pi) - f'(\pi))\theta'(\alpha\pi)).$$

In the second term we replace π by $\alpha\pi$. We then have

$$\sum (f(\pi)(\theta(\alpha\pi) - \theta'(\alpha\pi)) + (f(\alpha\pi) - f'(\alpha\pi))\theta'(\alpha^2\pi)).$$

By (3.) this is congruent to

$$\sum (f(\pi)(\theta(\alpha\pi) - \theta'(\alpha\pi)) - f'(\alpha^2\pi)(\theta(\alpha\pi) - \theta'(\alpha\pi))).$$

And this is equal to

$$\sum (f(\pi) - f'(\alpha^2\pi))(\theta(\alpha\pi) - \theta'(\alpha\pi)).$$

It now follows from (2.) that this is congruent to 0 modulo q.

5. We begin with the definition of the decident.

$$\mathrm{Dec}_L \frac{\alpha}{\mathfrak{b}} = \sum_{\pi} f'(\pi)\theta'(\alpha\pi),$$

where π runs through $S_{\mathfrak{b}} = \{\pi \in L \setminus K \mid \mathfrak{b}\pi = 0 \text{ but } \pi \neq 0\}$. From (4.) we easily have

$$\sum_{\pi} f'(\pi)\theta' = 0.$$

This gives us

$$\mathrm{Dec}_L \frac{\alpha}{\mathfrak{b}} = \sum_{\pi} f'(\pi)(\theta'(\alpha\pi) - \theta'(\pi)).$$

We now use the fact that $f \circ \alpha : L \setminus K_\infty \to \mathbf{Z}/q\mathbf{Z}$ is fundamental at $\mathfrak{b}$-division points. It then follows from (2.) that

$$\sum_{\pi} (f(\pi) - f'(\pi))(\theta'(\alpha\pi) - \theta'(\pi)) = 0.$$

We thus have

$$\mathrm{Dec}_L \frac{\alpha}{\mathfrak{b}} = \sum_{\mathfrak{b}\pi=0, \pi\neq 0} f(\pi)(\theta''(\alpha\pi') - \theta'''(\pi')).$$

2.9. Lemma (Independence of L)

In the previous paragraph we showed that if α and $\mathfrak{b}$ are coprime in $\mathfrak{O}_L$ and if $\mathfrak{b}$ is coprime to q, then $\mathrm{Dec}_L^{(f)} \frac{\alpha}{\mathfrak{b}}$ is independent of f. We now describe the behaviour of $\mathrm{Dec}_L \frac{\alpha}{\mathfrak{b}}$ as one changes the lattice L, under the condition that αq and $\mathfrak{b}$ remain coprime in $\mathfrak{O}_L$. We shall prove three statements; the most important of these for us is the second.

Let L and L' be two $\mathbf{Z}[\zeta]$-lattices in K.

1. *If there is an element $\gamma \in K$ with $\gamma L = L'$, then the rings $\mathfrak{O}_L$ and $\mathfrak{O}_{L'}$ are the same, and one has*

$$\mathrm{Dec}_L \frac{\alpha}{\mathfrak{b}} \equiv \mathrm{Dec}_{L'} \frac{\alpha}{\mathfrak{b}} \mod q$$

for all $\alpha \in \mathfrak{O}_L$ and all ideals $\mathfrak{b}$ of $\mathfrak{O}_L$, which are coprime to αq.

2. *To any two $\mathbf{Z}[\zeta]$-lattices $L, L' \subset K$, there is a "conductor" $\mathfrak{d}$, such that for all $\alpha, \beta \in \mathfrak{O}_L \cap \mathfrak{O}_{L'}$ with β and $\mathfrak{d}q\alpha$ coprime, one has*

$$\mathrm{Dec}_L \frac{\alpha}{\beta} \equiv \mathrm{Dec}_{L'} \frac{\alpha}{\beta} \mod q.$$

3. *If the lattice L is a fractional ideal of $\mathfrak{O}$, then the ring $\mathfrak{O}_L$ is the whole of $\mathfrak{O}$, and for all $\alpha \in \mathfrak{O}$ and all ideals $\mathfrak{b}$ of $\mathfrak{O}$ which are coprime to αq, one has*

$$\mathrm{Dec}_L \frac{\alpha}{\mathfrak{b}} \equiv \mathrm{Dec}_{\mathfrak{O}} \frac{\alpha}{\mathfrak{b}} \mod q.$$

Proofs.

1. It is clear that the rings $\mathfrak{O}_L$ and $\mathfrak{O}_L$ are the same. Let $f : K \to \mathbf{Z}/q\mathbf{Z}$ be fundamental for $\Gamma(L, q)$. Then $f'(z) := f(\gamma^{-1}z)$ is fundamental for $\Gamma(L', q)$, and one has

$$\begin{aligned}\mathrm{Dec}_L \frac{\alpha}{\mathfrak{b}} &= \sum_{z \in \mathfrak{b}^{-1}L \setminus L} f(z)\theta(\alpha z) = \sum_{z \in \gamma^{-1}\mathfrak{b}^{-1}L \setminus \gamma^{-1}L} f(\gamma z)\theta(\gamma \alpha z) \\ &= \sum_{z \in \mathfrak{b}^{-1}L' \setminus L'} f(z)\theta'(\alpha z) = \mathrm{Dec}_{L'} \frac{\alpha}{\mathfrak{b}}.\end{aligned}$$

Here $\mathfrak{b}^{-1}L \setminus L$ is the set $\{z \in K \mid \mathfrak{b}z \subset L \text{ but } z \notin L\}$.

2. We can assume that $L' \subset L$. If this were not the case then we could replace L' by its intersection with L; since L and L' are both contained in K, their intersection is also a lattice in K_∞. We choose $\mathfrak{d} \in \mathfrak{O}$ with $\mathfrak{d}L \subset L'$. Let β be coprime to $\mathfrak{d}$. Then multiplication by $\mathfrak{d}$ induces an isomorphism of $(\mathfrak{O}_L \cap \mathfrak{O}_{L'})$-modules

$$\{\pi \in L \setminus K \mid \beta\pi = 0\} \to \{\pi \in L' \setminus K \mid \beta\pi = 0\}.$$

If $(\beta, \alpha q) = 1$, then the decident is independent of the chosen fundamental function. It thus depends only on the actions of μ_q and α on this module. The lemma follows from the isomorphism.

3. If L is an ideal of $\mathfrak{O}$, then the $\mathfrak{O}$-modules $\mathfrak{b}^{-1}L/L$ and $\mathfrak{b}^{-1}\mathfrak{O}/\mathfrak{O}$ are isomorphic. We therefore have as in (2.), $\mathrm{Dec}_L \frac{\alpha}{\mathfrak{b}} \equiv \mathrm{Dec}_{\mathfrak{O}} \frac{\alpha}{\mathfrak{b}}$.

2.10. Lemma (Additivity with respect to α and $\mathfrak{b}$)

We now describe the behaviour of $\mathrm{Dec}_L \frac{\alpha}{\mathfrak{b}}$ on changing α and $\mathfrak{b}$, L remaining fixed. One could say that $\mathrm{Dec}_L \frac{\alpha}{\mathfrak{b}}$ is almost additive in α and $\mathfrak{b}$. The fourth statement is due to Schering [19], who stated it in the case $K = \mathbf{Q}$, $L = \mathbf{Z}$.

1. *If β and β' are elements of $\mathfrak{O}_L$, which are both coprime to αq in $\mathfrak{O}_L$, then*

$$\mathrm{Dec}_L \frac{\alpha}{\beta\beta'} \equiv \mathrm{Dec}_L \frac{\alpha}{\beta} + \mathrm{Dec}_L \frac{\alpha}{\beta'}.$$

2. *If $\mathfrak{b}$ and $\mathfrak{b}'$ are ideals of $\mathfrak{O}_L$, which are both coprime to αq in $\mathfrak{O}_L$, then*

$$\mathrm{Dec}_L \frac{\alpha}{\mathfrak{b}\mathfrak{b}'} \equiv \mathrm{Dec}_L \frac{\alpha}{\mathfrak{b}} + \mathrm{Dec}_{\mathfrak{b}^{-1}} \frac{\alpha}{\mathfrak{b}'}.$$

3. *If $\mathfrak{b}$ and $\mathfrak{b}'$ are ideals of $\mathfrak{O}_L$, which are both coprime to αq in $\mathfrak{O}_L$, and which are coprime to one another, then*

$$\mathrm{Dec}_L \frac{\alpha}{\mathfrak{b}\mathfrak{b}'} \equiv \mathrm{Dec}_L \frac{\alpha}{\mathfrak{b}} + \mathrm{Dec}_L \frac{\alpha}{\mathfrak{b}'}.$$

4. *If* $\mathfrak{b}$ *and* $\mathfrak{b}'$ *are ideals of* $\mathfrak{O}$, *which are both coprime to* αq *in* $\mathfrak{O}$, *then*

$$\mathrm{Dec}_{\mathfrak{O}} \frac{\alpha}{\mathfrak{b}\mathfrak{b}'} \equiv \mathrm{Dec}_{\mathfrak{O}} \frac{\alpha}{\mathfrak{b}} + \mathrm{Dec}_{\mathfrak{O}} \frac{\alpha}{\mathfrak{b}'}.$$

5. *If* α *and* α' *are elements of* $\mathfrak{O}_L$, *which are both coprime to* $\mathfrak{b}$ *in* $\mathfrak{O}_L$, *where* $\mathfrak{b}$ *is an ideal of* $\mathfrak{O}_L$ *coprime to* q, *then*

$$\mathrm{Dec}_L \frac{\alpha\alpha'}{\mathfrak{b}} \equiv \mathrm{Dec}_L \frac{\alpha}{\mathfrak{b}} + \mathrm{Dec}_L \frac{\alpha'}{\mathfrak{b}}.$$

Proofs.

Part 1 follows from part 2 and §2.9.1. Part 3 follows from part 2 and §2.9.2. Part 4 follows from part 2 and §2.9.3. It is therefore sufficient to prove part 2 and part 5.

2. We have a projection map

$$\mathrm{pr}^L_{\mathfrak{b}^{-1}L} : L \setminus K \to \mathfrak{b}^{-1}L \setminus K.$$

We define two sets

$$\bar{S}^L_{\mathfrak{b}\mathfrak{b}'} := \{\pi \in L \setminus K \mid \mathfrak{b}\mathfrak{b}'\pi = 0\}, \quad \bar{S}^{\mathfrak{b}^{-1}L}_{\mathfrak{b}'} := \{\pi \in (\mathfrak{b}^{-1}L \setminus K) \mid \mathfrak{b}'\pi = 0\}.$$

The projection map induces an $\mathfrak{O}_L$-module homomorphism from $\bar{S}^L_{\mathfrak{b}\mathfrak{b}'}$ to $\bar{S}^{\mathfrak{b}^{-1}L}_{\mathfrak{b}'}$. This homomorphism is surjective. Its kernel is the set

$$\bar{S}^L_{\mathfrak{b}} := \{\pi \in L \setminus K \mid \mathfrak{b}\pi = 0\}.$$

By §2.7.4 the cardinality of this set is congruent to 1 modulo q.

Let the function $f : (\mathfrak{b}^{-1}L \setminus K) \to \mathbf{Z}/z\mathbf{Z}$ be fundamental for $\Gamma(\mathfrak{b}^{-1}L, q)$ at all points apart from 0, and let $f(0) = 0$. We define

$$f^1 : L \setminus K \to \mathbf{Z}/q\mathbf{Z}$$
$$\pi \mapsto f(\mathrm{pr}^L_{\mathfrak{b}^{-1}L}(\pi)).$$

Then f^1 is fundamental for $\Gamma(L, q)$ away from the $\mathfrak{b}$-division points of L, where it is always zero. Let $f^2 : L \setminus K \to \mathbf{Z}/q\mathbf{Z}$ be fundamental for $\Gamma(L, q)$ at $\mathfrak{b}$-division points of L and zero everywhere else. Then the function $f^3 := f^1 + f^2$ is fundamental for $\Gamma(L, q)$ on the set $\bar{S}^L_{\mathfrak{b}\mathfrak{b}'}$.

One has

$$\mathrm{Dec}_L \frac{\alpha}{\mathfrak{b}\mathfrak{b}'} = \sum_{\pi \in \bar{S}^L_{\mathfrak{b}\mathfrak{b}'} \setminus 0} f^3(\pi)\theta^3(\alpha\pi).$$

Multiplication by α permutes by §2.7.2 the sets $\bar{S}^L_{\mathfrak{b}\mathfrak{b}'}$ and $\bar{S}^L_{\mathfrak{b}}$. Therefore α also permutes the set $\bar{S}^L_{\mathfrak{b}\mathfrak{b}'} \setminus \bar{S}^L_{\mathfrak{b}}$. We thus have

$$\mathrm{Dec}_L \frac{\alpha}{\mathfrak{b}\mathfrak{b}'} = \sum_{\pi \in \bar{S}^L_{\mathfrak{b}\mathfrak{b}'} \setminus \bar{S}^L_{\mathfrak{b}}} f^3(\pi)\theta^3(\alpha\pi) + \sum_{\pi \in \bar{S}^L_{\mathfrak{b}} \setminus 0} f^3(\pi)\theta^3(\alpha\pi),$$

and this is equal to

$$\sum_{\pi \in \bar{S}^L_{\mathfrak{b}\mathfrak{b}'} \setminus \bar{S}^L_{\mathfrak{b}}} f^1(\pi)\theta^1(\alpha\pi) + \sum_{\pi \in \bar{S}^L_{\mathfrak{b}} \setminus 0} f^2(\pi)\theta^2(\alpha\pi).$$

This is however the same as

$$\#(\bar{S}^L_{\mathfrak{b}}) \sum_{\pi \in \bar{S}^{\mathfrak{b}^{-1}L}_{\mathfrak{b}'} \setminus 0} f(\pi)\theta(\alpha\pi) + \sum_{\pi \in \bar{S}^L_{\mathfrak{b}} \setminus 0} f^2(\pi)\theta^2(\alpha\pi).$$

Modulo q this is congruent to

$$\mathrm{Dec}_{\mathfrak{b}^{-1}L} \frac{\alpha}{\mathfrak{b}'} + \mathrm{Dec}_L \frac{\alpha}{\mathfrak{b}}.$$

Part 2 is proved.

5. We now consider $\mathrm{Dec}_L \frac{\alpha\alpha'}{\mathfrak{b}}$. From §2.8.5 we know that

$$\mathrm{Dec}_L \frac{\alpha\alpha'}{\mathfrak{b}} = \sum_{\mathfrak{b}\pi = 0, \pi \neq 0} f(\pi)(\theta(\alpha\alpha'\pi) - \theta(\pi)).$$

We can write $\theta(\alpha\alpha'\pi) - \theta(\pi)$ as $\theta(\alpha\alpha'\pi) - \theta(\alpha\pi) + \theta(\alpha\pi) - \theta(\pi)$. The above sum then becomes

$$\sum_{\mathfrak{b}\pi = 0, \pi \neq 0} f(\pi)(\theta(\alpha\alpha'\pi) - \theta(\alpha\pi)) + \sum_{\mathfrak{b}\pi = 0, \pi \neq 0} f(\pi)(\theta(\alpha\pi) - \theta(\pi)).$$

The second sum here is $\mathrm{Dec}\frac{\alpha}{\mathfrak{b}}$. It only remains to show that the first sum is $\mathrm{Dec}\frac{\alpha'}{\mathfrak{b}}$. To see this, it is sufficient to observe that $f \circ \alpha$ is fundamental on $\mathfrak{b}$-division points and then to apply §2.8.5.

2.11. The Gauss-Schering Lemma

This lemma is the reason for studying decidents. *If αq and $\mathfrak{b}$ are coprime in $\mathfrak{O}$, then*

$$\left(\frac{\alpha}{\mathfrak{b}}\right)_q = \zeta^{\mathrm{Dec}_{\mathfrak{O}}\frac{\alpha}{\mathfrak{b}}}$$

where the left hand side is the q^{th} power Legendre symbol in the field K.

Proof. By §2.10.4 it is sufficient to prove this in the case that $\mathfrak{b}$ is a prime ideal. By §2.9.3 we have $\mathrm{Dec}_{\mathfrak{O}}\frac{\alpha}{\mathfrak{b}} = \mathrm{Dec}_{\mathfrak{b}}\frac{\alpha}{\mathfrak{b}}$. By §2.8.4 we may let f be the characteristic function of a fundamental domain D for μ_q in $K/\mathfrak{b}$. Let M be the intersection of D with the set

$$S_{\mathfrak{b}} = \{\pi \in K/\mathfrak{b} \mid \mathfrak{b}\pi = 0,\ \pi \neq 0\} = (\mathfrak{O}/\mathfrak{b})^{\times}.$$

We therefore have

$$\mathfrak{O}/\mathfrak{b} = \{0\} \dot{\cup} \bigcup_{\zeta \in \mu_q} \zeta M.$$

The union is disjoint because μ_q has no fixed points in $S_{\mathfrak{b}}$ (by §2.2, 2.7.2, 2.5.1). Since $\mathfrak{O}/\mathfrak{b}$ has cardinality $N(\mathfrak{b})$, M must have $\dfrac{N(\mathfrak{b}) - 1}{q}$ elements. Therefore we have from Euler's criterium:

$$\left(\frac{\alpha}{\mathfrak{b}}\right)_q \equiv \prod_{\pi \in M} \alpha \bmod \mathfrak{b}.$$

We now rearrange this as Gauss did:

$$\left(\frac{\alpha}{\mathfrak{b}}\right)_q \equiv \prod_{\pi \in M} \frac{\alpha\pi}{\pi} \equiv \prod_{\pi \in M} \frac{\zeta(\alpha\pi)\pi'(\alpha\pi)}{\pi} \equiv \prod_{\pi \in M} \zeta(\alpha\pi) \prod_{\pi \in M} \pi'(\alpha\pi) \prod_{\pi \in M} \pi^{-1} \bmod \mathfrak{b}$$

where $\zeta(\alpha\pi)$ is the unique element of μ_q with $\alpha\pi \in \zeta(\alpha\pi)M$ and $\pi'(\alpha\pi) = \zeta(\alpha\pi)\alpha\pi \in M$. Since α is coprime to $\mathfrak{b}$, multiplication with α permutes the set $S_{\mathfrak{b}}$. Since this permutation commutes with the action of μ_q on $S_{\mathfrak{b}}$, the map $\pi \mapsto \pi'(\alpha\pi)$ is a permutation of M. We therefore have

$$\left(\frac{\alpha}{\mathfrak{b}}\right)_q \equiv \prod_{\pi \in M} \zeta(\alpha\pi) \prod_{\pi \in M} \pi \prod_{\pi \in M} \pi^{-1} \equiv \prod_{\pi \in M} \zeta(\alpha\pi) \bmod \mathfrak{b}.$$

Now notice that if $\pi \in M$ then $\theta(\zeta^r\pi) = r$, so $\zeta^{\theta(\pi)} = \zeta(\pi)$ for all $\pi \in S_{\mathfrak{b}}$. We therefore have

$$\left(\frac{\alpha}{\mathfrak{b}}\right)_q \equiv \prod_{\pi \in M} \zeta^{\theta(\alpha\pi)} \equiv \zeta^{\sum_{\pi \in M}\theta(\alpha\pi)} \equiv \zeta^{\sum_{\pi \in S_{\mathfrak{b}}} f(\pi)\theta(\alpha\pi)} \equiv \zeta^{\mathrm{Dec}_{\mathfrak{b}}\frac{\alpha}{\mathfrak{b}}} \equiv \zeta^{\mathrm{Dec}_{\mathfrak{O}}\frac{\alpha}{\mathfrak{b}}}.$$

2.12. Lemma

Theorem 1, which we will prove in §5, is a statement about the quotient $\left(\frac{\alpha}{\beta}\right)_q\left(\frac{\beta}{\alpha}\right)_q^{-1}$. Using the Gauss-Schering lemma this can be rephrased as a statement about the difference $\mathrm{Dec}_{\mathfrak{D}}\frac{\alpha}{\beta} - \mathrm{Dec}_{\mathfrak{D}}\frac{\beta}{\alpha}$. This is however the difference of two sums over different sets, and is therefore difficult to handle. In this paragraph we show that the two sums can be taken over the same set. This lemma was proved by Habicht [8] in the case $K = \mathbf{Q}(\sqrt{-3})$, and by various authors in the case $K = \mathbf{Q}$. The idea probably appears first in Eisenstein's proofs of the reciprocity laws in $\mathbf{Q}(\sqrt{-1})$ and $\mathbf{Q}(\sqrt{-1})$ using elliptic functions. There is perhaps also a connection with Furtwängler's idea of studying the extensions $K(\sqrt[q]{\alpha}, \sqrt[b]{\beta}) \supset K(\sqrt[q]{\alpha\beta})$ rather than $K(\sqrt[q]{\alpha}) \supset K$. This is useful because the former extension is unramified.

If α, β and q are pairwise coprime elements in $\mathfrak{D}_L$, then

$$\mathrm{Dec}_L\frac{\alpha}{\beta} - \mathrm{Dec}_L\frac{\beta}{\alpha} \equiv \mathrm{Dec}_L^{(f)}\frac{\alpha}{\alpha\beta} - \mathrm{Dec}_L^{(f)}\frac{\beta}{\alpha\beta} + \frac{(N(\alpha)-)(N(\beta)-1)(q-1)}{2q} + \frac{q-1}{2}(N(a)-N(\beta)),$$

where both decidents in the right hand side are calculated with respect to the same fundamental function. Here $N(\alpha)$ is the cardinality of the quotient $\alpha^{-1}L/L$. In particular, if α and β are totally positive and $\alpha \equiv \beta \equiv 1 \bmod q^2$ then:

$$\mathrm{Dec}_L\frac{\alpha}{\beta} - \mathrm{Dec}_L\frac{\beta}{\alpha} \equiv \mathrm{Dec}_L^{(f)}\frac{\alpha}{\alpha\beta} - \mathrm{Dec}_L^{(f)}\frac{\beta}{\alpha\beta}.$$

Proof. We begin with the identity $\bar{S}_{\alpha\beta} = \bar{S}_\beta \oplus \bar{S}_\alpha$ given in Lemma 2.7.5. This implies the following expression for $S_{\alpha\beta}$ as a disjoint union:

$$S_{\alpha\beta} = S_\alpha \dot{\cup} S_\beta \dot{\cup} S'$$

where $S' = \{\pi \in L \setminus K \mid \alpha\beta\pi = 0 \text{ but } \alpha\pi \neq 0,\ \beta\pi \neq 0\}$. This leads to an identity of the sums over these sets:

$$\mathrm{Dec}_L^{(f)}\frac{\alpha}{\alpha\beta} - \mathrm{Dec}_L^{(f)}\frac{\beta}{\alpha\beta} = \sum_{\pi\in S_{\alpha\beta}} f(\pi)(\theta(\alpha\pi) - \theta(\beta\pi))$$

$$= \sum_{\pi\in S_\beta} f(\pi)(\theta(\alpha\pi) - \theta(\beta\pi)) + \sum_{\pi\in S_\alpha} f(\pi)(\theta(\alpha\pi) - \theta(\beta\pi))$$

$$+ \sum_{\pi \in S'} f(\pi)(\theta(\alpha\pi) - \theta(\beta\pi)).$$

Now using the simple fact that $\theta(0) = \dfrac{q(q-1)}{2}$, we have

$$\begin{aligned}\mathrm{Dec}_L^{(f)} \frac{\alpha}{\alpha\beta} - \mathrm{Dec}_L^{(f)} \frac{\beta}{\alpha\beta} &= \sum_{\pi \in S_\beta} f(\pi)\left(\theta(\alpha\pi) - \frac{q(q-1)}{2}\right) - \sum_{\pi \in S_\alpha} f(\pi)\left(\theta(\beta\pi) - \frac{q(q-1)}{2}\right) \\ &\quad + \sum_{\pi \in S'} f(\pi)(\theta(\alpha\pi) - \theta(\beta\pi)) \\ &= \mathrm{Dec}_L \frac{\alpha}{\beta} - \mathrm{Dec}_L \frac{\beta}{\alpha} + \frac{q-1}{2}(N(\alpha) - N(\beta)) \\ &\quad + \sum_{\pi \in S'} f(\pi)(\theta(\alpha\pi) - \theta(\beta\pi)).\end{aligned}$$

It remains to calculate the sum. By 2.8.2 together with the fact that $f \circ \alpha$ is fundamental on S', we have

$$\sum_{\pi \in S'} f(\pi)(\theta(\alpha\pi) - \theta(\beta\pi)) = \sum_{\pi \in S'} f(\alpha\pi)(\theta(\alpha\pi) - \theta(\beta\pi)).$$

By 2.8.3, we have $\sum_{\pi \in S'} f(\alpha\pi)\theta(\alpha\pi) = 0$, so

$$\begin{aligned}\sum_{\pi \in S'} f(\pi)(\theta(\alpha\pi) - \theta(\beta\pi)) &= - \sum_{\pi \in S'} f(\alpha\pi)\theta(\beta\pi) \\ &= - \sum_{\pi_1 \in S_\alpha} \sum_{\pi_2 \in S_\beta} f(\alpha(\pi_1 + \pi_2))\theta(\beta(\pi_1 + \pi_2)) \\ &= - \sum_{\pi_1 \in S_\alpha} \theta(\beta\pi_1) \times \sum_{\pi_2 \in S_\beta} f(\alpha\pi_2) \\ &= - \sum_{\pi_1 \in S_\alpha} \theta(\pi_1) \times \sum_{\pi_2 \in S_\beta} f(\pi_2) \\ &= - (1 + 2 + \cdots + (q-1)) \frac{N(\alpha) - 1}{q} \times \frac{N(\beta) - 1}{q}.\end{aligned}$$

The last line follows from the identity $\sum_\zeta f(\zeta\pi) = 1$ for $\pi \in S_\alpha$ or S_β, together with 2.7.4.

2.13. A skew product

In order to study decidents we introduce a skew product. Let L be a fixed lattice and let $\Gamma = \Gamma(L, q)$. We define $\chi : \Gamma \to \mathbf{Z}/q\mathbf{Z}$ by $\chi(\sigma(\zeta^a, b)) = a$. For two $\mathbf{Z}/q\mathbf{Z}$-linear combinations g^1 and g^2 of Γ-fundamental functions and an ideal $\mathfrak{b} \subset \mathfrak{O}_L$ we define

$$\langle g^1, g^2\rangle_{\mathfrak{b}} := \sum_{z\in S_{\mathfrak{b}},\sigma\in\Gamma} \chi(\sigma) g^1(\sigma z) g^2(z).$$

Here $S_{\mathfrak{b}}$ is the set $\{z \in K \mid \mathfrak{b}z \in L \text{ but } z \notin L\}$. If f^1 and f^2 are two fundamental functions, then

$$\begin{aligned}\langle f^1, f^2\rangle_{\mathfrak{b}} &= \sum_{z\in S_{\mathfrak{b}}} f^1(z)\theta^2(z)\\ &= \sum_{\mathfrak{b}\pi=0,\pi\neq 0} f^1(\pi)\theta^2(\pi).\end{aligned}$$

The skew product has for fundamental functions f^1, f^2 and f^3 the following three properties:

- $\langle f^1 + f^2, f^3\rangle_{\mathfrak{b}} \equiv \langle f^1, f^3\rangle_{\mathfrak{b}} + \langle f^2, f^3\rangle_{\mathfrak{b}}$,
- $\langle f^1, f^2\rangle_{\mathfrak{b}} \equiv -\langle f^2, +f^1\rangle_{\mathfrak{b}}$,
- $\langle f^1 - f^2, f^3\rangle_{\mathfrak{b}} \equiv \langle f^1, f^2\rangle_{\mathfrak{b}}$.

The first property needs no proof and the second is just a special case of §2.8.3. We now verify the third property. It follows from §2.8.2, that for every four fundamental functions f^1, f^2, f^3 and f^4, we have $\langle f^1 - f^2, f^3 - f^4\rangle_{\mathfrak{b}} \equiv 0$. Thus $\langle f^1 - f^2, f^3\rangle_{\mathfrak{b}}$ is independent of f^3, and we have in particular

$$\begin{aligned}\langle f^1 - f^2, f^3\rangle_{\mathfrak{b}} &= \langle f^1 - f^2, f^2\rangle_{\mathfrak{b}},\\ &= \langle f^1, f^2\rangle_{\mathfrak{b}} - \langle f^2, f^2\rangle_{\mathfrak{b}}\\ &= \langle f^1, f^2\rangle_{\mathfrak{b}}.\end{aligned}$$

3. Geometric constructions of some fundamental functions

We shall think of K_∞ as a real vector space of dimension $n := [K : \mathbf{Q}]$. Our next aim is to define the singular homology groups of a topological space. For our purposes, the definitions given in [16] are most convenient. Later in the chapter we shall construct using the homology groups a class of fundamental functions. At the end of the chapter we shall find a formula for the skew product $\langle f^1, f^2\rangle = \sum f^1(\pi)\theta^2(\pi)$, where f^1 and f^2 are from the class of fundamental functions which we shall construct.

The connection with the homology groups is the following we define $f^1(z)$ to be the degree of a map $\mathscr{P}^1 : I^n \to K_\infty$ at the point $z \in K_\infty$, where I^n is a hypercube.

3.1. Singular homology groups

1. Let I be the closed interval [0, 1] in $\mathbf{R}$. We shall write I^r for the carte-

sian product of r copies of I. I^0 will be a topological space with exactly one point.

2. Let X be a topological space. A continuous map

$$\mathcal{T} : I^r \to X$$

will be called a singular r-cube in X. We shall write $\mathcal{Q}_r(X)$ for the $\mathbf{Z}/q\mathbf{Z}$-module generated by the set of singular r-cube in X, and with relations

$$\mathcal{T} + \mathcal{T} \circ (ij) = 0 \quad 1 \leq i \leq j \leq r,$$

where

$$(ij)(x_1, \ldots, x_r) := (x_1, \ldots, x_{i-1}, x_j, x_{i+1}, \ldots, x_{j-1}, x_i, x_{j+1}, \ldots, x_r).$$

Therefore one always has in $\mathcal{Q}_r(X)$ the identity

$$\mathcal{T} \circ \Phi = \operatorname{sign}(\Phi), \mathcal{T},$$

where Φ is an element of the symmetry group S_r, acting on I^r by permutation of the coordinates.

3. A singular r-cube $\mathcal{T}$ is called *degenerate,* if the function $\mathcal{T}(x_1, \ldots, x_r)$ is independent of at least one of the coordinates x_i. We shall write $\mathcal{D}_r(X)$ for the submodule of $\mathcal{Q}_r(X)$ generated by the degenerate r-cubes. The quotient

$$\mathcal{C}_r(X) := \mathcal{Q}_r(X)/\mathcal{D}_r(X)$$

will be called the $\mathbf{Z}/q\mathbf{Z}$-*module of* r-*chains in* X.

4. Let $\mathcal{T}$ be a singular r-cube. We now define the i^{th} *front face of* $\mathcal{T}$,

$$\mathfrak{A}_i\mathcal{T} : I^{r-1} \to X$$
$$(x_1, \ldots, x_{r-1}) \mapsto \mathcal{T}(x_1, \ldots, x_{i-1}, 0, x_i, \ldots, x_{r-1})$$

and the i^{th} *back face of* $\mathcal{T}$,

$$\mathfrak{B}_i\mathcal{T} : I^{r-1} \to X$$
$$(x_1, \ldots, x_{r-1}) \mapsto \mathcal{T}(x_1, \ldots, x_{i-1}, 1, x_i, \ldots, x_{r-1}).$$

The faces of an r-cubes are $(r-1)$-cubes.

5. The *boundary* of an r-cube $\mathcal{T}$ is defined to be the element of $\mathcal{Q}_{r-1}(X)$ given by the following formula

$$\partial_r \mathcal{T} := \sum_{i=1}^{r} (-1)^i (\mathfrak{A}_i \mathcal{T} - \mathfrak{B}_i \mathcal{T}).$$

This definition can be extended by $\mathbf{Z}/q\mathbf{Z}$-linearity to $\mathcal{Q}_r(X)$.

$$\partial_r : \mathcal{Q}_r(X) \to \mathcal{Q}_{r-1}(X).$$

This induces a homomorphism of the chain modules

$$\partial_r : \mathcal{C}_r(X) \to \mathcal{C}_{r-1}(X).$$

We define the *r-cycles* to be the kernel of the boundary map

$$\mathcal{Z}_r(X) := \mathrm{Ker}\,(\partial_r) \subset \mathcal{C}_r(X),$$

and the *r-boundaries* to be its image

$$\mathcal{B}_r(X) := \mathrm{Im}\,(\partial_{r+1}) \subset \mathcal{C}_r(X).$$

One can check that every boundary is a cycle

$$\mathcal{B}_r(X) \subset \mathcal{Z}_r(X).$$

We can thus define the *r^{th} singular homology group of X* to be the quotient of the cycles by the boundaries:

$$\mathcal{H}_r(X) := \mathcal{Z}_r(X)/\mathcal{B}_r(X).$$

6. Now let Y be a subspace of X. Clearly there is an inclusion

$$\mathcal{Q}_r(Y) \subset \mathcal{Q}_r(X).$$

This induces an inclusion of chain modules

$$\mathcal{C}_r(Y) \subset \mathcal{C}_r(X),$$

and we define the relative chain modules of X w.r.t. Y to be the quotient:

$$\mathcal{C}_r(X, Y) := \mathcal{C}_r(X)/\mathcal{C}_r(Y).$$

The boundary map induces a homomorphism of relative chain modules

$$\partial_r : \mathcal{C}_r(X, Y) \to \mathcal{C}_{r-1}(X, Y),$$

and we define as before the relative cycles to be the kernel; the relative boundaries to be the image; and the relative homology groups to be the

quotient of the relative cycles by the relative boundaries.

$$\mathcal{Z}_r(X, Y) := \operatorname{Ker} \partial_r \subset \mathcal{C}_r(X, Y),$$
$$\mathcal{B}_r(X, Y) := \operatorname{Im} \partial_{r+1} \subset \mathcal{C}_r(X, Y),$$
$$\mathcal{H}_r(X, Y) := \mathcal{Z}_r(X, Y)/\mathcal{B}_r(X, Y).$$

7. The base set $|\mathcal{T}|$ of a singular r-cube $\mathcal{T}$ is defined to be the image of $\mathcal{T}$, if $\mathcal{T}$ is non-degenerate, and the empty set, if $\mathcal{T}$ is degenerate. The base set of an element of $\mathcal{C}_r(X)$ is defined to be the union of all base-sets of singular r-cubes in its support.

8. Let X be an abelian topological group (whose group law we shall write additively) and let $\mathcal{T}$ be a singular r-cube and $\mathcal{U}$ a singular s-cube in X. We can define a product $(r+s)$-cube:

$$\mathcal{T} \times \mathcal{U} : I^{r+s} \to X$$
$$(x_1, \ldots, x_r, y_1, \ldots, y_s) \mapsto \mathcal{T}(x_1, \ldots, x_r) + \mathcal{U}(y_1, \ldots, y_s).$$

This product operation can be extended by bilinearity

$$\mathcal{Q}_r(X) \times \mathcal{Q}_s(X) \to \mathcal{Q}_{r+s}(X),$$

and this induces a product operation on the chain modules:

$$\mathcal{C}_r(X) \times \mathcal{C}_s(X) \to \mathcal{C}_{r+s}(X).$$

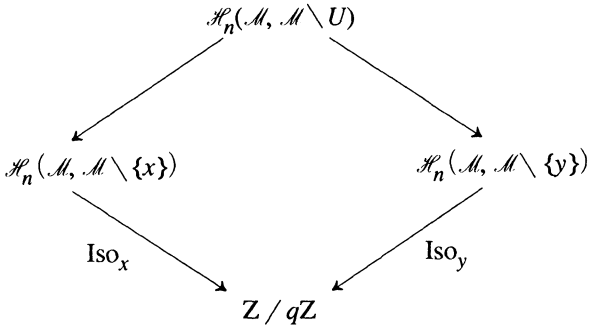
9. Let $\mathcal{M}$ be a manifold. If $x \in \mathcal{M}$ then

$$\mathcal{H}_n(\mathcal{M}, \mathcal{M} \setminus \{x\}) \cong \mathbf{Z}/q\mathbf{Z}.$$

(This is a non-canonical isomorphism of $\mathbf{Z}/q\mathbf{Z}$-modules.) The manifold $\mathcal{M}$ is called orientable w.r.t. $\mathbf{Z}/q\mathbf{Z}$, if one can associate to each point $x \in \mathbf{Z}/q\mathbf{Z}$ an isomorphism

$$\operatorname{Iso}_x : \mathcal{H}_n(\mathcal{M}, \mathcal{M} \setminus \{x\}) \to \mathbf{Z}/q\mathbf{Z}$$

with the property that for every $x \in \mathcal{M}$ there is a neighbourhood U of x, such that for every $y \in U$ the diagram commutes



Such a set of isomorphisms is called an orientation. Every manifold is orientable over $\mathbf{Z}/2\mathbf{Z}$, and if a manifold is orientable over $\mathbf{Z}$ then it is orientable over $\mathbf{Z}/q\mathbf{Z}$ for every natural number q. An n-dimensional, differentiable manifold, which posesses a global, non-vanishing differential n-form, is orientable over $\mathbf{Z}$.

Assume that $\mathscr{M}$ is orientable over $\mathbf{Z}/q\mathbf{Z}$, and fix an orientation Iso. Let $\mathscr{T} \in \mathscr{C}_n(\mathscr{M})$. Then $\partial\mathscr{T}$ is a singular $n-1$ chain. Suppose that $x \in \mathscr{M}$ does not lie in the base set $|\partial\mathscr{T}|$ of $\partial\mathscr{T}$. Then $\mathscr{T}$ represents a homology class in $\mathscr{H}_n(\mathscr{M}, \mathscr{M} \setminus \{x\})$. We define the degree of $\mathscr{T}$ at the point x to be

$$\mathbf{I}_{\mathscr{T}}(x) := \mathrm{Iso}_x(\mathscr{T}).$$

From our condition on Iso, we have a locally constant function

$$\mathbf{I}_{\mathscr{T}} : \mathscr{M} \setminus |\partial\mathscr{T}| \to \mathbf{Z} \setminus q\mathbf{Z}.$$

10. The spaces K_∞ and $L \setminus K_\infty$ are orientable over $\mathbf{Z}/q\mathbf{Z}$ (the first is a vector space and the second is a torus). If q is odd, then the q^{th} roots of unity have positive norms. In that case $\Gamma \setminus K_\infty$ is orientable over $\mathbf{Z}$. Suppose that q and $n := [K : \mathbf{Q}]$ are both even. Then again the q^{th} roots of unity have positive norm. If on other hand n is odd, then K has no subfield whose degree over $\mathbf{Q}$ is even. In particular, K doesn't contain $\mathbf{Q}(\sqrt{-1})$. From this it follows that $q = 2$, and thus $\Gamma \setminus K_\infty$ is orientable over $\mathbf{Z}/q\mathbf{Z}$.[2]

11. The group Γ acts on $\mathscr{C}_r(K_\infty)$ by composition of functions. The projection

[2] If $q = 2$, then $\Gamma \setminus K_\infty$ is unfortunately not a manifold. It is however apart from at the 2-division points a manifold.

maps pr_Γ, pr_L and pr_Γ^L induce maps between the chain complexes

$$\mathrm{pr}_{L*} : \mathscr{C}_r(K_\infty) \to \mathscr{C}_r(L \setminus K_\infty),$$
$$\mathrm{pr}_{L*} : \mathscr{C}_r(K_\infty) \to \mathscr{C}_r(\Gamma \setminus K_\infty),$$
$$\mathrm{pr}_{\Gamma*}^L : \mathscr{C}_r(L \setminus K_\infty) \to \mathscr{C}_r(\Gamma \setminus K_\infty).$$

and we have canonical isomorphisms

$$\mathscr{C}_r(L \setminus K_\infty) \to L \setminus \mathscr{C}_r(K_\infty),$$
$$\mathscr{C}_r(\Gamma \setminus K_\infty) \to \Gamma \setminus \mathscr{C}_r(K_\infty),$$
$$\mathscr{C}_r(\Gamma \setminus K_\infty) \to \mu_q \setminus \mathscr{C}_r(\Gamma \setminus K_\infty).$$

We can choose orientations on K_∞, $L \setminus K_\infty$ and $\Gamma \setminus K_\infty$, which are compatible with the projection maps. We then have in the notation of §2.3

$$\mathbf{I}_{\mathrm{pr}_{\Gamma*}(K)}(\varpi) = (\mathrm{pr}_{\Gamma*}(\mathbf{I}_K))(\varpi),$$
$$\mathbf{I}_{\mathrm{pr}_{\Gamma*}(K)}(\pi) = (\mathrm{pr}_{\Gamma*}(\mathbf{I}_K))(\pi),$$
$$\mathbf{I}^L_{\mathrm{pr}_{\Gamma*}(K)}(\varpi) = (\mathrm{pr}^L_{\Gamma*}(\mathbf{I}_K))(\varpi).$$

12. If S is a discrete subset of an n-dimensional orientable manifold $\mathscr{M}$, and if $\mathscr{T}$ is an n-chain in $\mathscr{M}$ with $S \cap |\partial\mathscr{T}| = \emptyset$, then we define

$$\{\{S \mid \mathscr{T}\}\} := \sum_{x \in S} \mathbf{I}_{\mathscr{T}}(x).$$

Since $|\mathscr{T}|$ is compact, the sum has finite support. If $\sigma : \mathscr{M} \to \mathscr{M}$ is an orientation preserving transformation, then

$$\{\{\sigma S \mid \sigma\mathscr{T}\}\} = \{\{S \mid \mathscr{T}\}\}.$$

The transformations $\sigma(r, t)$ of K_∞, with r in the multiplicative group $K_\infty^\times$ and $t \in K_\infty$ are all orientation preserving with respect to $\mathbf{Z}/q\mathbf{Z}$.

13. The singular 0-cubes in a topological space X correspond to the points x of X. We shall write $[x]$ for the singular 0-cube corresponding to x. The singular 1-cubes in X are paths between points x and y in X. If X is a real vector space then we shall write the straight path from x to y as

$$[x, y]$$

and a general path from x to y in X as

$$[x, y]'.$$

Let X be an Abelian topological group and let $\mathcal{T}$ be a singular r-cube in X. Then

$$[x] \times \mathcal{T}$$

is a translation of $\mathcal{T}$ by x, and one has (because 0 is an even number)

$$[x] \times \mathcal{T} = \mathcal{T} \times [x].$$

This equality is at the level of singular r-cubes.

3.2. Remarks

1. The boundary of a product of paths is given by

$$\partial\Big(\prod_{i=1}^{n} [0, a_i]^i\Big) = \sum_{j=1}^{n} (-1)^{j-1}([a_i] - [0]) \prod_{i=1, \neq j}^{n} [0, a_i]^i,$$

where $[0, a_i]^i$ is any path from 0 to a_i in K_∞, and the products are taken in ascending order.

2. $\forall\, \sigma \in \Gamma(L)$, $\partial(\sigma(\mathcal{S})) = \sigma(\partial(\mathcal{S}))$
   $\forall$ translations $\sigma_2 \in L$, $\sigma_2(\mathcal{S}) \times \mathcal{T} = \sigma_2(\mathcal{S} \times \mathcal{T})$
   $\forall$ rotations $\sigma_1 \in \mu_q$, $\sigma_1(\mathcal{S}) \times \sigma_1(\mathcal{T}) = \sigma_1(\mathcal{S} \times \mathcal{T})$

3. Let $\mathcal{T} : I^n \to X$ be a singular n-cube in the topological space X, and let Y be a subspace of the space X with

$$|\partial\mathcal{T}| \subset Y.$$

Then $\mathcal{T}$ represents a homology class in $\mathcal{H}_n(X, Y)$. We cut $\mathcal{T}$ into two pieces:

$$\mathcal{T}_1 : I^n \to X$$
$$(x_1, \ldots, x_n) \mapsto \mathcal{T}\Big(\frac{x_1}{2}, x_2, \ldots, x_n\Big)$$

and

$$\mathcal{T}_2 : I^n \to X$$
$$(x_1, \ldots, x_n) \mapsto \mathcal{T}\Big(\frac{x_1 + 1}{2}, x_2, \ldots, x_n\Big).$$

If in addition

$$|\partial\mathcal{T}_1| \subset Y$$
$$\text{and } |\partial\mathcal{T}_2| \subset Y,$$

then we have in $\mathcal{H}_n(X, Y)$ the equation

$$\mathcal{T}_1 + \mathcal{T}_2 = \mathcal{T}.$$

4. Let $\mathcal{M}$ be a manifold with an orientation Iso. and let $\mathcal{T}$ be a singular n-cube in $\mathcal{M}$. Then we may define as in §3.1.9 a function $\mathbf{I}_{\mathcal{T}}$. Let $z \in \mathcal{M}$ lie outside the base set of $\mathcal{T}$. Then we always have

$$\mathbf{I}_{\mathcal{T}}(z) = 0.$$

We shall now use the homology groups to construct fundamemtal functions. We shall define the function $f : K_\infty \to \mathbf{Z}/q\mathbf{Z}$ to be $\mathbf{I}_{\mathcal{P}}$, where $\mathcal{P}$ is a sum of singular n-cubes. The construction works for every action of a group Γ on a real vector space V, if the pair (Γ, V) has the Kubota property. We define this property in the next paragraph. The content of the next 5 paragraphs can be found in Kubota [14].

3.3. The Kubota property

For the moment we shall forget fundamental functions. Instead we shall use the simpler idea of a fundamental domain. For our purposes, the following definition is most convenient:

Let Γ be a group acting on a finite dimensional, real vector space V. A fundamental domain for Γ in V is a subset $U \subset V$, satisfying the following three conditions:

(i) every Γ-orbit has at least one point in U

(ii) U is closed in V

(iii) if z is in the interior of U, then no other point of the Γ-orbit of z lies in U.

By the word *parallelotope* we shall mean an expression of the form

$$\prod_{i=1}^{r} [a_i, b_i] \in C^r(V),$$

where the vectors $a_i - b_i$ are linearly independent. The point

$$\sum_{i=1}^{r} a_i \in V$$

will be called the *origin* of the parallelotope. We shall say that two parallelotopes are *properly touching,* if their intersection is either empty or a mutual face of both parallelotopes, having the same origin as a face of each parallelotope.

Now assume Γ has discrete orbits and a compact fundamental domain. We shall say that the pair (Γ, V) has the *Kubota property,* if V can be tiled by properly touching parallelotopes, which are permuted by the action of Γ, without a parallelotope being mapped to itself by a non-trivial group element. The Kubota property is equivalent to saying that Γ has a fundamental domain consisting of finitely many parallelotopes, whose images under Γ are properly touching. We shall show that (Γ, K_∞) has the Kubota property. This statement is not trivial; for example if q is not a power of a prime, then $(\Gamma(\mathfrak{D}, q), K_\infty)$ does not always have the Kubota property. The following observations will be useful:

(i) If (Γ, V) has the Kubota property, and Γ' is a subgroup of Γ with finite index, then (Γ', V) also has the Kubota property.

(ii) If (Γ, V) has the Kubota property, then (Γ^r, V^r) also has the Kubota property, the action of Γ^r on V^r being defined componentwise.

3.4. The Kubota property in $Q(\rho)$

We first consider the case that K is the cyclotomic field $\mathbf{Q}(\rho)$, where ρ is a primitive p^{th} root of unity for any prime p (even 2).

Define

$$\mathcal{S} := \prod_{i=1}^{p-1} \left[0, \frac{\rho^i}{1-\rho}\right].$$

This is a singular $p-1$-cube in K_∞, and represents a $p-1$-chain. By choosing an orientation on K_∞ we may define the function $\mathbf{I}_{\mathcal{S}}$ as in §3.1.9. We shall choose the orientation so that $\mathbf{I}_{\mathcal{S}}$ takes only the values 0 and 1. This is possible since $\mathcal{S}$ is a linear map. We then have:

3.5. Lemma (Kubota)

The base set $|\mathcal{S}|$ *of* $\mathcal{S}$ *is a fundamental domain for* $\Gamma(\mathbf{Z}[\rho], p)$ *in* $\mathbf{Q}(\rho)_\infty$, *and it touches its images under elements of* $\Gamma(\mathbf{Z}[\rho], p)$ *properly. If* $p \neq 2$ *then the* $(p-1)$*-cube* $\mathrm{pr}_{\Gamma *}\mathcal{S}$ *has zero boundary in* $\mathcal{C}_{p-2}(\Gamma\backslash \mathbf{Q}(\rho)_\infty)$ *and represents a generator of* $\mathcal{H}_{p-1}(\Gamma\backslash \mathbf{Q}(\rho)_\infty)$. *If* $\varpi \in \Gamma\backslash \mathbf{Q}(\rho)_\infty$ *satisfies the condition* $\varpi \notin \mathrm{pr}_\Gamma |\partial\mathcal{S}|$, *then* $\mathbf{I}_{\mathcal{S}}$

is fundamental for Γ at ϖ, and one has in $\mathbf{Z}/q\mathbf{Z}$:

$$(\mathrm{pr}_{\Gamma *}\mathbf{I}_{\mathcal{S}})(\varpi) = \mathbf{I}_{\mathrm{pr}_{\Gamma *}\mathcal{S}}(\varpi) = 1.$$

Proof. (i) *The structure of the proof*

If $p = 2$ then this is all trivial. From now on, assume p to be an odd prime. We first show that $\partial(\mathrm{pr}_{\Gamma *}(\mathcal{S}))$ is zero in $\mathscr{C}_{n-1}(\Gamma\backslash K_\infty)$. Since $\mathbf{I}_{\mathrm{pr}_{\Gamma *}(\mathcal{S})}$ is locally constant on the complement of $|\,\partial(\mathrm{pr}_{\Gamma *}(\mathcal{S}))\,|$, we can deduce that $\mathbf{I}_{\mathrm{pr}_{\Gamma *}(\mathcal{S})}$ is locally constant on $\Gamma\backslash K_\infty$. The space $\Gamma\backslash K_\infty$ is however a quotient of the connected space K_∞, and is itself therefore connected. Thus, we know that $\mathbf{I}_{\mathrm{pr}_{\Gamma *}(\mathcal{S})}$ is a constant function. We check that this constant is 1 by integrating the function and comparing the answer with the volume of $\Gamma\backslash K_\infty$. The lemma follows from this, since for every $\varpi \in \Gamma\backslash K_\infty$ not lying in $\mathrm{pr}_\Gamma|\,\partial\mathcal{S}\,|$, the following holds:

$$\mathbf{I}_{\mathrm{pr}_{\Gamma *}(\mathcal{S})}(\varpi) = (\mathrm{pr}_{\Gamma *}\mathbf{I}_{\mathcal{S}})(\varpi).$$

(ii) *Calculation of* $\partial(\mathrm{pr}_{\Gamma *}(\mathcal{S}))$

First we apply the statement §3.2.1 to the definition of $\mathcal{S}$. This gives us:

$$\partial\mathcal{S} = \sum_{j=1}^{p-1} (-1)^{j-1}\,\partial\Big[0, \frac{\rho^j}{1-\rho}\Big] \prod_{\substack{i=1,\dots,p-1,\\ i\neq j}} \Big[0, \frac{\rho^i}{1-\rho}\Big].$$

From our assumption that p is an odd prime, it follows that $\dfrac{p-1}{2}$ is a whole number. We can therefore split the sum in two halves as follows:

$$\partial\mathcal{S} = \sum_{j=1}^{\frac{p-1}{2}} \Big((-1)^{j-1}\,\partial\Big[0, \frac{\rho^j}{1-\rho}\Big] \prod_{\substack{i=1,\dots,p-1,\\ i\neq j}} \Big[0, \frac{\rho^i}{1-\rho}\Big] + (-1)^{(p-j)-1}\,\partial\Big[0, \frac{\rho^{p-j}}{1-\rho}\Big] \prod_{\substack{i=1,\dots,p-1,\\ i\neq p-j}} \Big[0, \frac{\rho^i}{1-\rho}\Big]\Big).$$

Again since p is odd, we have $(-1)^{(p-j)-1} = -(-1)^{j-1}$, which gives us

$$\partial\mathcal{S} = \sum_{j=1}^{\frac{p-1}{2}} (-1)^{j-1}\Big(\partial\Big[0, \frac{\rho^j}{1-\rho}\Big] \prod_{\substack{i=1\dots p-1,\\ i\neq j}} \Big[0, \frac{\rho^i}{1-\rho}\Big] - \partial\Big[0, \frac{\rho^{p-j}}{1-\rho}\Big] \prod_{\substack{i=1\dots p-1,\\ i\neq p-j}} \Big[0, \frac{\rho^i}{1-\rho}\Big]\Big).$$

We now apply the elementary fact that $\rho^j - 1$ is divisible by $1-\rho$ in $\mathbf{Z}[\rho]$ for every j. We therefore have $\mathrm{pr}_{\mathfrak{D}}\Big(\dfrac{\rho^i}{1-\rho}\Big) = \mathrm{pr}_{\mathfrak{D}}\Big(\dfrac{1}{1-\rho}\Big)$. Replacing $\partial\Big[0, \dfrac{\rho^j}{1-\rho}\Big]$ by $\Big[\dfrac{\rho^j}{1-\rho}\Big] - [0]$, we obtain

$$\mathrm{pr}_{\mathfrak{D}*}\Big(\partial\Big[0, \frac{\rho^j}{1-\rho}\Big]\Big) = \mathrm{pr}_{\mathfrak{D}*}\Big(\partial\Big[0, \frac{1}{1-\rho}\Big]\Big).$$

We substitute this into the above formula.

$$\mathrm{pr}_{\mathfrak{D}*}(\partial\mathscr{Z}) = \mathrm{pr}_{\mathfrak{D}*}\Big(\sum_{j=1}^{\frac{p-1}{2}} (-1)^{j-1}\partial\Big[0, \frac{1}{1-\rho}\Big]\Big(\prod_{\substack{i=1,\dots,p-1,\\ i\neq j}}\Big[0, \frac{\rho^i}{1-\rho}\Big] - \prod_{\substack{i=1,\dots,p-1,\\ i\neq p-j}}\Big[0, \frac{\rho^i}{1-\rho}\Big]\Big)\Big).$$

We shall now reorder the second product in the inner bracket. Since p is odd, this product has an odd number of terms. Therefore every cyclic reordering is an even permutation, requiring no change of sign. We thus have

$$\prod_{\substack{i=1,\dots,p-1,\\ i\neq p-j}}\Big[0, \frac{\rho^t}{1-\rho}\Big] = \prod_{i=p-j+1}^{p-1}\Big[0, \frac{\rho^i}{1-\rho}\Big]\prod_{i=1}^{p-j-1}\Big[0, \frac{\rho^i}{1-\rho}\Big].$$

By renumbering things we obtain

$$\begin{aligned}\prod_{\substack{i=1,\dots,p-1,\\ i\neq p-j}}\Big[0, \frac{\rho^i}{1-\rho}\Big] &= \prod_{i=1}^{p-1-(p-j)}\Big[0, \frac{\rho^{i+(p-j)}}{1-\rho}\Big]\prod_{i=1+j}^{p-j-1+j}\Big[0, \frac{\rho^{i-j}}{1-\rho}\Big]\\ &= \prod_{i=1}^{j-1}\Big[0, \frac{\rho^{i-j}}{1-\rho}\Big]\prod_{i=j+1}^{p-1}\Big[0, \frac{\rho^{i-j}}{1-\rho}\Big]\\ &= \prod_{\substack{i=1,\dots,p-1,\\ i\neq j}}\Big[0, \frac{\rho^{i-j}}{1-\rho}\Big]\\ &= \sigma_1(\rho^{-j})\prod_{\substack{i=1,\dots,p-1,\\ i\neq j}}\Big[0, \frac{\rho^i}{1-\rho}\Big].\end{aligned}$$

We therefore have in $\mathscr{C}_{p-2}(\Gamma\backslash K_\infty)$

$$\mathrm{pr}_{\Gamma*}\Big(\prod_{\substack{i=1,\dots,p-1,\\ i\neq j}}\Big[0, \frac{\rho^i}{1-\rho}\Big] - \prod_{\substack{i=1,\dots,p-1,\\ i\neq p-j}}\Big[0, \frac{\rho^i}{1-\rho}\Big]\Big) = 0.$$

Thus

$$\mathrm{pr}_{\Gamma*}(\partial\mathscr{Z}) = 0.$$

(ii) *Computation of the constant*

From this we deduce as described above that $\mathbf{I}_{\mathrm{pr}_{\Gamma*}(\mathscr{Z})}$ is a constant function. Its value is given by

$$\frac{1}{\mathrm{vol}(\Gamma\backslash K_\infty)}\int_{\Gamma\backslash K_\infty}\mathbf{I}_{\mathrm{pr}_{\Gamma*}(\mathscr{Z})}.$$

From §3.1.11 this is equal to

$$\frac{1}{\mathrm{vol}(\Gamma\backslash K_\infty)}\int_{K_\infty}\mathbf{I}_{\mathcal{S}},$$

which is just $\dfrac{\mathrm{vol}(|\mathcal{S}|)}{\mathrm{vol}(\Gamma\backslash K_\infty)}$. Since p is the index of $\mathbf{Z}[\rho]$ in $\Gamma(\mathbf{Z}[\rho], p)$, we know that

$$\mathrm{vol}(\Gamma\backslash K_\infty) = p^{-1}\mathrm{vol}(\mathbf{Z}[\rho]\backslash\mathbf{Q}(\rho)_\infty).$$

On the other hand, the set $|\sigma_1(1-\rho)\mathcal{S}|$ is a well known fundamental domain for $\mathbf{Z}[\rho]$ in $\mathbf{Q}(\rho)_\infty$. We thus have

$$\mathrm{vol}(\sigma_1(1-\rho)\mathcal{S}) = \mathrm{vol}(\mathbf{Z}[\rho]\backslash\mathbf{Q}(\rho)_\infty).$$

When $\mathcal{S}$ is magnified by multiplication with $1-\rho$, its volume is multiplied by $N(1-\rho) = p$. From this we deduce that

$$\mathrm{pr}_{\Gamma *}(\mathbf{I}_{\mathcal{S}}) = 1.$$

3.6. The Kubota property in $Q(\zeta)$

The previous lemma shows that $\mathcal{S}$ is a fundamental domain for $\Gamma(\mathbf{Z}[\rho], p)$ in $\mathbf{Q}(\rho)_\infty$. This implies that $\mathbf{Q}(\rho)_\infty$ is tiled by the images of $\mathcal{S}$ under elements of $\Gamma(\mathbf{Z}[\rho], p)$. We now apply §3.3 (ii). The field $\mathbf{Q}(\zeta)$ is a vector space over $\mathbf{Q}(\rho)$ with basis $\left\{\zeta^i \mid i = 1, \ldots, \dfrac{q}{p}\right\}$. Thus $\mathbf{Q}(\zeta)_\infty$ is tiled by the images of

$$\mathcal{T} := \prod_{i=1}^{q/p}\sigma_1(\zeta^1)\mathcal{S}$$

under elements of the direct sum of $\dfrac{q}{p}$ copies of $\Gamma(\mathbf{Z}[\rho], p)$ (acting componentwise with respect to this basis). Since the basis is contained in $\mathbf{Z}[\zeta]$, we know that the action of $\mathbf{Z}[\zeta]$ permutes these images of $\mathcal{T}$. Clearly the action of μ_q also permutes the images of $\mathcal{T}$. We thus know that $\Gamma(\mathbf{Z}[\zeta], q)$ permutes the images of $\mathcal{T}$. To verify the Kubota property for $(\Gamma(\mathbf{Z}[\zeta], q), \mathbf{Q}(\zeta)_\infty)$, we need only show that none of the images of $\mathcal{T}$ is mapped to itself by a non-trivial element of $\Gamma(\mathbf{Z}[\zeta], q)$.

Suppose $\sigma(r, t)$ maps one of the images $\mathcal{T}'$ of $\mathcal{T}$ under $\Gamma(\mathbf{Z}[\rho], p)^{\frac{q}{p}}$ to itself. Then $\sigma(r, t)$ cannot be simply a translation, so $r \neq 1$. Therefore, the projection of $\mathcal{T}'$ in $\mathbf{Z}[\zeta]\backslash\mathbf{Q}(\zeta)_\infty$ is fixed be a non-trivial subgroup of μ_q. Every such subgroup contains μ_p, so $\mathrm{pr}_L(\mathcal{T}')$ is mapped to itself by ρ. It follows that $\rho\mathcal{T}'$ is a transla-

tion of $\mathcal{T}'$ by an element of $\mathbf{Z}[\zeta]$. In other words, $\mathcal{T}'$ is fixed by $\sigma(\rho, t)$ for a suitable $t \in \mathbf{Z}[\zeta]$. This leads to a contradiction with §3.5, by projecting $\mathcal{T}'$ and t onto one of the $\mathbf{Q}(\rho)_\infty$ components. We have shown that $(\Gamma, \mathbf{Q}(\zeta))$ has the Kubota property with the tiling described above.

3.7. The Kubota property in any number field

We now drop all conditions on K. As before, let ζ be a primitive q^{th} root of unity in K. We fix a basis $b_1, b_2, \ldots, b_N$ for K as a vector space over $\mathbf{Q}(\zeta)$. We then have

$$K_\infty = \bigoplus_{i=1}^{N} \sigma_1(b_i)\, \mathbf{Q}(\zeta)_\infty.$$

Let L be the free lattice over $\mathbf{Z}[\zeta]$, generated by $b_1, b_2, \ldots, b_N$. As before, we have a componentwise action on K_∞ by the direct sum of N copies of $\Gamma(\mathbf{Z}(\zeta], q)$. By §3.3 (ii), $(K_\infty, \Gamma(\mathbf{Z}[\zeta], q)^N)$ has the Kubota property. It follows however from the construction of L, that $\Gamma(L, q)$ is a subgroup of $\Gamma(\mathbf{Z}[\zeta], q)^N$, so from §3.3 (i) we know that $(K_\infty, \Gamma(L, q))$ has the Kubota property. Although it is not necessary, we could choose our basis so that the lattice L contains the ring $\mathfrak{O}$. This implies that $\Gamma(\mathfrak{O}, q)$ is a subgroup of $\Gamma(L, q)$, and we deduce by §3.3 (i), that $\Gamma(\mathfrak{O}, q)$ also has the Kubota property.

3.8. Modified parallelotopes

In the previous three lemmas we have shown, that $(\Gamma(L, q), K_\infty)$ has the Kubota property, where L is free over $\mathbf{Z}[\zeta]$. We now exploit this fact to construct fundamental functions.

Notation. Let $\mathcal{P} = \sum \mathcal{P}_i \in \mathcal{C}_n(K_\infty)$ be a fundamental domain for $\Gamma(L, q)$ in K_∞, where every $\mathcal{P}_i$ is a parallelotope:-

$$\mathcal{P}_i = \prod_{j=1}^{n} [0, a_{i,j}].$$

(It is clear from our construction, that every $\mathcal{P}_i$ can be chosen to have origin 0.) We fix an orientation on K_∞. Then each parallelotope $\mathcal{P}_i$ gives rise to a function $\mathbf{I}_{\mathcal{P}_i}$ as discribed in §3.1.9. By reordering the $a_{i,j}$ if necessary, we ensure that the function $\mathbf{I}_{\mathcal{P}_i}$ takes only the values 0 and 1. Since the intersection of any two parallelotopes is contained in their boundaries, it follows that $\mathbf{I}_{\mathcal{P}}$ takes only the values

0 and 1. The boundary of each paralellotope can be expressed in $\mathcal{C}_{n-1}(K_\infty)$ as a sum of faces:-

$$\partial \mathcal{P}_i = \sum_{\mathcal{F}} wt(\mathcal{F}, i)\mathcal{F}, \quad wt(\mathcal{F}, i) = \pm 1.$$

Each face $\mathcal{F}$ has an expression as an $(n-1)$-cube:-

$$\mathcal{F} = \prod_{j=1}^{n-1} [0, a_{\mathcal{F},j}].$$

We shall write $\mathcal{F} < \mathcal{P}_i$ to mean that $\mathcal{F}$ is a face of $\mathcal{P}_i$. The function $\mathbf{I}_{\mathcal{P}}$ is fundamental at all points $z \in K_\infty$, whose Γ-orbit does not intersect the boundary of $\mathcal{P}$.

Now let $[0, 1]'$ be any path from 0 to 1 in K_∞, that is a continuous function $[0, 1]'$: $I \to K_\infty$ with $[0, 1]'(0) = 0$ and $[0, 1]'(1) = 1$. We shall use the following notation:

$$[a, b]' := \sigma(b-a, a)\,[0,1]',$$
$$\mathcal{P}'_i := \prod_{j=1}^{n} [0, a_{i,j}]', \quad \mathcal{F}'_i := \prod_{j=1}^{n-1} [0, a_{\mathcal{F},j}]'$$

and

$$\mathcal{P}' := \sum \mathcal{P}'_i, \quad f' := \mathbf{I}_{\mathcal{P}'}.$$

Thus $\mathcal{P}'_i$ is an element of $\mathcal{C}_n(K_\infty)$. We shall call $\mathcal{P}'_i$ a *modified parallelotope.* The following lemma was known to Kubota. It says that if we modify all our parallelotopes with the same path, then their sum is still fundamental.

3.9. Lemma (Kubota)

Let $z \in K_\infty$ be chosen such that its orbit Γ_z has empty intersection with the base set $|\partial \mathcal{P}'|$. Then $f' := \mathbf{I}_{\mathcal{P}'}$ is fundamental for Γ at z. In other words $\sum_{z' \in \Gamma z} f'(z') = 1$.

Proof. Since $\mathcal{P}$ is fundamental for Γ and the images of $\mathcal{P}$ are properly touching, we have in $\mathcal{C}_{n-1}(\Gamma \backslash K_\infty)$ [3]

$$\mathrm{pr}_{\Gamma *}(\partial \mathcal{P}) = 0.$$

---

[3] If $K = \mathbf{Q}$ then this only holds in $\mathcal{C}_{n-1}\left(\Gamma \backslash \left(\mathbf{R} - \frac{1}{2}\mathbf{Z}\right)\right)$. In that case the lemma is however trivial, since $f' = f$.

One has

$$\partial \mathscr{P} = \sum_{\mathscr{F} < \mathscr{P}} wt(\mathscr{F})\mathscr{F},$$

where $wt(\mathscr{P}) := \sum wt(\mathscr{P}, i)$. If $[\mathscr{F}]$ is the Γ-orbit of the face $\mathscr{F}$, then we have from the first formula

$$\sum_{\mathscr{G} \in [\mathscr{F}]} wt(\mathscr{G}) = 0.$$

If however $\mathscr{G} = \sigma\mathscr{F}$, then we also have $\mathscr{G}' = \sigma\mathscr{F}'$, and thus

$$\mathrm{pr}_{\Gamma *}(\partial \mathscr{P}') = 0.$$

From this it follows as in the proof of §3.5 that $\mathbf{I}_{\mathrm{pr}_{\Gamma *}(\mathscr{P}')}$ is constant. We must now show that

$$\mathbf{I}_{\mathrm{pr}_{\Gamma *}(\mathscr{P}')} = \mathbf{I}_{\mathrm{pr}_{\Gamma *}(\mathscr{P})}.$$

It suffices to show that $\mathrm{pr}_{\Gamma *}\mathscr{P}$ and $\mathrm{pr}_{\Gamma *}\mathscr{P}'$ are homotopic. We shall construct in §3.10 a homotopy between $\mathrm{pr}_{\Gamma *}\mathscr{P}$ and $\mathrm{pr}_{\Gamma *}\mathscr{P}'$.

3.10. The difference of two modified parallelotopes

We now depart from Kubota's proof. What follows is based on a technique used in Habicht's paper [8]. We investigate the difference $f' - f''$ of two of the functions, which we constructed in §3.8. The basic idea is to express $\mathscr{P}' - \mathscr{P}''$ as a sum of pieces, each piece being associated to a face $\mathscr{F}$ of a parallelotope of $\mathscr{P}$. Actually these pieces will be homotopies from $\mathscr{F}'$ to $\mathscr{F}''$. This method will lead to a formula for the skew product

$$\langle f', f'' \rangle := \sum f'(\pi)\theta''(\pi) = \sum (f'(\pi) - f''(\pi))\theta(\pi),$$

Notation. Let h be a homotopy from $[0,1]'$ to $[0,1]''$ in K_∞. This means $h : I^2 \to K_\infty$ with $h|_{\{0\}\times I} = 0$, $h|_{\{1\}\times I} = 1$ and $\partial h \equiv [0,1]' - [0,1]''$ modulo $\mathscr{D}_1(K_\infty)$. Then for any parallelotope $\mathscr{P}_t = \Pi_{j=1}^n [0, a_{i,j}]$ we define

$$\tilde{h}_i(x_1, \ldots, x_n, h) := \sum_{j=1}^{n} a_{i,j} h(x_j, t).$$

Similarly for any face $\mathscr{F} = \sigma_2(v_{\mathscr{F}}) \Pi_{j=1}^{n-1} [0, a_{\mathscr{F},j}]$ we define

$$\tilde{h}_{\mathscr{F}}(x_1, \ldots, x_{n-1}, t) := v_{\mathscr{F}} + \sum_{j=1}^{n-1} a_{\mathscr{F},j} h(x_j, t).$$

Then $\tilde{h}_i$ is a homotopy from $\mathscr{P}'_i$ to $\mathscr{P}''_i$ and $\tilde{h}_{\mathscr{F}}$ is a homotopy from $\mathscr{F}'$ to $\mathscr{F}''$, and one has in $\mathscr{C}_n(K_\infty)$:-

$$\begin{aligned}\partial\tilde{h}_i &= \sum_{j=1}^{n+1}(-1)^j(\mathfrak{U}_j(\tilde{h}_i) - \mathfrak{B}_j(\tilde{h}_i)) \\ &= (-1)^{n+1}(\mathscr{P}'_i - \mathscr{P}''_i) + \sum_{\mathscr{F}<\mathscr{P}_i} wt(i, \mathscr{F})\,\tilde{h}_{\mathscr{F}}.\end{aligned}$$

Letting $\tilde{h} = \sum \tilde{h}_i$ in $C_{n+1}(K_\infty)$ one then has

$$\mathscr{P}' - \mathscr{P}'' = (-1)^n \sum_{\mathscr{F}<\mathscr{P}} wt(\mathscr{F})\,\tilde{h}_{\mathscr{F}} + (-1)^n\partial\tilde{h}.$$

If z is a point of K_∞ which is not contained in $|\,\partial\tilde{h}_{\mathscr{F}}\,|$ for any $\mathscr{F}$ then one has in $\mathscr{H}_n(K_\infty, K_\infty \setminus z)$

$$\mathscr{P}' - \mathscr{P}'' = (-1)^n \sum_{\mathscr{F}<\mathscr{P}} wt(\mathscr{F})\,\tilde{h}_{\mathscr{F}},$$

and therefore (in the notation of §3.8)

$$f'(z) - f''(z) = (-1)^n \sum_{\mathscr{F}<\mathscr{P}} wt(\mathscr{F})\mathbf{I}_{\tilde{h}\mathscr{F}}(z).$$

We now consider the equivalence classes of faces of $\mathscr{P}$ under the action of Γ. We shall refer to the class of $\mathscr{F}$ as $[\mathscr{F}]$. We split the above sum over $\mathscr{F} < \mathscr{P}$ into sums over the classes:-

$$f(z) - f''(z) = (-1)^n \sum_{[\mathscr{F}]} \sum_{\mathscr{G}\in[\mathscr{F}]} wt(\mathscr{F})\mathbf{I}_{\tilde{h}\mathscr{G}}(z).$$

Note that since $\mathrm{pr}_{\Gamma *}\,\partial\mathscr{P} = 0$ in $\mathscr{C}_{n-1}(\Gamma\setminus K_\infty)$ we have

$$\sum_{\mathscr{G}\in[\mathscr{F}]} wt(\mathscr{F}) = 0.$$

The set $S_{\alpha\beta} = \{z \in K \mid \alpha\beta z \in L,\ z \notin L\}$ is $\Gamma(L)$-stable, so for $\sigma \in \Gamma(L)$ and $\mathscr{T} \in \mathscr{H}_n(K_\infty, K_\infty \setminus S_{\alpha\beta})$, one has

$$\sum_{z\in S_{\alpha\beta}} \mathbf{I}_{\mathscr{T}}(z) = \sum_{z\in S_{\alpha\beta}} \mathbf{I}_{\sigma\mathscr{T}}(z).$$

We have analogously by §2.8.1, if $\sigma = \sigma(\zeta', t)$,

$$\sum_{z\in S_{\alpha\beta}} \mathbf{I}_{\mathscr{T}}(z)\,\theta(z) = \sum_{z\in S_{\alpha\beta}} \mathbf{I}_{\sigma\mathscr{T}}(z)\ (\theta(z) - j).$$

Therefore

$$(-1)^n \sum_{\mathscr{G}\in[\mathscr{F}]} \sum_{z\in S_{\alpha\beta}} wt(\mathscr{G})\,\mathbf{I}_{\tilde{h}_{\mathscr{G}}}(z)\ \theta(z) = \sum_{z\in S_{\alpha\beta}} w[\mathscr{F}]\,\mathbf{I}_{\tilde{h}_{\mathscr{T}}}(z),$$

where

$$w[\mathcal{F}] = (-1)^n wt(\mathcal{F}) \sum_{\mathcal{G}\in[\mathcal{F}]} wt(\mathcal{G})\, j(\mathcal{F}, \mathcal{G})$$

and

$$\mathcal{G} = \sigma(\zeta^{j(\mathcal{F},\mathcal{G})}, t)\mathcal{F}.$$

We can rewrite this as follows:

$$(-1)^n \sum_{\mathcal{G}\in[\mathcal{F}]} \sum_{z\in S_{\alpha\beta}} wt(\mathcal{G})\, \mathbf{I}_{\tilde{h}_{\mathcal{G}}}(z)\, \theta(z) = w[\mathcal{F}]\, \{\{S_{\alpha\beta} \mid \tilde{h}_{\mathcal{F}}\}\}.$$

After summing this over the set of classes $[\mathcal{F}]$ of faces, we obtain:

3.11. Theorem (Formula for the skew product)

Let $[0,1]'$ *and* $[0,1]''$ *be two paths from* 0 *to* 1 *in* K_∞, *and let* $h : I^2 \to K_\infty$ *be a homotopy from* $[0,1]'$ *to* $[0,1]''$. *For a face* $\mathcal{F} = \sigma_2(v_{\mathcal{F}})\, \Pi_{j=1}^{n-1} [0, a_{\mathcal{F},j}]$ *we define an* n*-cube*

$$\tilde{h}_{\mathcal{F}}(x_1, \ldots, x_{n-1}, t) = v_{\mathcal{F}} + \sum_{j=1}^{n-1} a_{\mathcal{F},j} h(x_j, t), \quad x_j, t \in I.$$

If for every face $\mathcal{F} < \mathcal{P}$

$$S_{\alpha\beta} \cap |\, \partial \tilde{h}_{\mathcal{F}}\, | = \emptyset,$$

then we have

$$\langle f', f'' \rangle_{\alpha\beta} = \sum_{z\in S_{\alpha\beta}} (f'(z) - f''(z))\, \theta(z) = \sum_{[\mathcal{F}]} w[\mathcal{F}]\, \{\{S_{\alpha\beta} \mid \tilde{h}_{\mathcal{F}}\}\}.$$

Here the constants $w[\mathcal{F}] \in \mathbf{Z}/q\mathbf{Z}$ *depend only on* $\mathcal{P}$.

3.12. Summary of notation and results

For reference purposes we fix our notation for the remaining chapters and state the main results in this notation. This will hopefully avoid confusion.

We fix a basis

$$\{b_1, \ldots, b_N\}$$

for K as a vector space over $\mathbf{Q}(\zeta)$. We write L for the free lattice generated by $\{b_1, \ldots, b_N\}$ over $\mathbf{Z}[\zeta]$. We then have an n-chain $\mathcal{P} \in \mathcal{C}_n(K_\infty)$ with the following

properties:

1.
$$\mathrm{pr}_{\Gamma}(\partial\mathscr{P}) = 0 \text{ in } \mathscr{C}_{n-1}(\Gamma(L)\setminus K_{\infty}) ;$$

2. For every point $\varpi \in \Gamma\setminus K_{\infty}$ we have
$$\mathbf{I}_{\mathrm{pr}_{\Gamma}(\partial\mathscr{P})}(\varpi) = 1 \quad \text{in } \mathbf{Z}/q\mathbf{Z};$$

3. There is a (finite) decomposition
$$\mathscr{P} = \sum_{i} \mathscr{P}_{i}, \quad \text{in } \mathscr{C}_{n}(K_{\infty}),$$
where each $\mathscr{P}_{i}$ is a parallelotope. More precisely
$$\mathscr{P}_{i} = \prod_{j=1}^{n} [0, a_{i,j}],$$
where each $a_{i,j}$ is of the form
$$\frac{1}{1-\rho}\zeta^{k}b_{l};$$

4. We have a decomposition of $\partial\mathscr{P}$ as a sum of faces,
$$\partial\mathscr{P} = \Sigma_{\mathscr{F}<\mathscr{P}}\, wt(\mathscr{F})\mathscr{F}$$
where $\mathscr{F} < \mathscr{P}$ means that $\mathscr{F}$ is a face of at least one of the parallelotopes $\mathscr{P}_{i}$. We write the Γ-equivalence class of $\mathscr{F}$ as $[\mathscr{F}]$. Then for every class $[\mathscr{F}]$,
$$\sum_{\mathscr{G}\in[\mathscr{F}]} wt(\mathscr{G}) = 0 \quad \text{in } \mathbf{Z}/q\mathbf{Z}.$$
For every face $\mathscr{F} < \mathscr{P}$ there is an expression
$$\mathscr{F} = \sigma_{2}(v_{\mathscr{F}}) \prod_{j=1}^{n-1} [0, a_{\mathscr{F},j}],$$
where the $a_{\mathscr{F},j}$ and $v_{\mathscr{F}}$ are $(1-\rho)$-division points of L.

4. Admissible paths and admissible homotopies

Let $\mathscr{P}: I^n \to K_\infty$ be a singular n-cube. If $z \in |\partial\mathscr{P}|$ then $\mathbf{I}_\mathscr{P}(z)$ is not defined. Thus if we write formulae involving $\mathbf{I}_\mathscr{P}(z)$, we must be certain that $z \notin |\partial\mathscr{P}|$. This is the purpose of this chapter. The proofs here are quite technical. For those just interested in the applications, it is only necessary to understand §4.2, §4.4 and the statement of §4.3. We first prove a technical lemma, which we shall need for the other proofs in the chapter.

4.1. A technical lemma

2 *Let Φ be a Hausdorff, real, topological vector space and V an n-dimensional, real vector space. Let X be a compact polyhedron of dimension less than n. Let $B: \Phi \times X \to V$ be a map with following properties:*

- *B is continuous and piecewise differentiable.*
- *$\forall x \in X$, $B(-, x): \Phi \to V$ is an affine map.*
- *$\forall x \in X$ where $B(-, x): \Phi \to V$ is not surjective, one has $0 \notin B(\Phi, x)$.*

We define a subset

$$\Psi := \{\phi \in \Phi \mid \forall x \in X \text{ one has } B(\phi, x) \neq 0\}.$$

Then Ψ is a dense, open subset of Φ.

Proof. (i) Let $\phi_0 \in \Phi$. We shall show that Ψ is dense in a neighbourhood of ϕ_0 and that Ψ is open in Φ. We call a point $x \in X$ *degenerate* if $B(-, x)$ is not surjective. The degenerate points form a closed and therefore compact set. For every degenerate point x we choose neighbourhoods $D(x)$ of x in X and $U(x)$ of ϕ_0 in Φ, small enough that for all $\phi \in U(x)$ and $y \in D(x)$ one has $B(y, \phi) \neq 0$. There are finitely many points $x_1, \ldots, x_s$ such that every degenerate point lies in the union $D(x_1) \cup \ldots \cup D(x_s)$. We set $D = D(x_1) \cup \ldots \cup D(x_s)$ and $U = U(x_1) \cap \ldots \cap U(x_s)$. Thus U is a neighbourhood of ϕ_0 in Φ and D a neighbourhood of the set of degenerate points. For every $x \in D$ and $\phi \in U$, we have by construction $B(\phi, x) \neq 0$. We shall show that $\Psi \cap U$ is dense in U.

(ii) Let $Y := X \setminus D$. This is closed in X and is therefore compact. To every $y \in Y$ we define

$$E(y) := \{\phi \in \Phi \mid B(\phi, y) = 0\}.$$

Since y is not degenerate, $E(y)$ has codimension n in Φ. Let W be an n-dimensional subspace of Φ. We define a subset of Y:

$$Y(W) := \{y \in Y \mid \#(W \cap E(y)) = 1\}.$$

If $\phi_1, \ldots, \phi_n$ is a basis of W, then

$$Y(W) = \{y \in Y \mid B(\phi_1, y), \ldots, B(\phi_n, y) \text{ are linearly independent}\}.$$

One sees from this that the subsets $Y(W)$ are open in Y. Now let y be any element of Y. Since y is non-degenerate, the map $B(-, y)$ is surjective. There are thus vectors $\phi_1, \ldots, \phi_n \in \Phi$ such that $B(\phi_1, y), \ldots, B(\phi_n, y)$ form a basis of V. That implies $y \in Y(\mathbf{R}\phi_1 \oplus \ldots \oplus \mathbf{R}\phi_n)$. Therefore the subsets $Y(W)$ form an open cover of Y. Since Y is compact, there is a finite subcover:

$$Y = Y(W_1) \cup \ldots \cup Y(W_r).$$

For each $i = 1, \ldots, r$ we choose a compact subset $Z(i) \subset Y(W_i)$ large enough so that

$$Y = Z(1) \cup \ldots \cup Z(r).$$

(iii) For every $i = 1, \ldots, r$, define

$$\Psi(i) := \{\phi \in \Phi \mid \forall x \in Z(i),\ B(\phi, x) \neq 0\}.$$

We then have

$$\Psi \cap U = (\Psi(1) \cap \ldots \cap \Psi(r)) \cap U = (\Psi(1) \cap U) \cap \ldots \cap (\Psi(r) \cap U).$$

We want to show that $\Psi \cap U$ is a dense subset of U, and that Ψ is an open subset of Φ. For this we shall need the following lemma:

LEMMA. *If R_1 is a topological space and if R_2 and R_3 are dense, open subsets of R_1, then their intersection $R_2 \cap R_3$ is also dense and open in R_1.*

Proof. Since R_2 and R_3 are open, $R_2 \cap R_3$ is also open. Let R_4 be a non-empty, open subset of R_1. Then $R_4 \cap R_2$ is non-empty, because R_2 is dense. The set $R_4 \cap R_2$ is also open, because R_2 and R_4 are both open. Therefore $R_4 \cap R_2 \cap R_3$ is non-empty, because R_3 is dense. This implies that $R_2 \cap R_3$ is also dense in R_1.

It thus suffices to show, that for any i the subset $\Psi(i) \cap U$ is dense in U, and Ψ is open in Φ.

(iv) We first show that Ψ is open in Φ. Let $\phi \in \Psi$. We shall construct a neighbourhood of ϕ in Ψ. Since $\phi \in \Psi$, we have for every $x \in X$, $B(\phi, x) \neq 0$. We choose for every $x \in X$ neighbourhoods $U_2(x)$ of x in X and $U_3(x)$ of ϕ in

Φ small enough that for $y \in U_2(x)$ and $\phi' \in U_3(x)$ we have $B(\phi', y) \neq 0$. Since X is compact, there are $x_1, \ldots, x_t \in X$ such that $X = U_2(x_1) \cup \ldots \cup U_2(x_2)$. Let $U_3 = U_3(x_1) \cap \ldots \cap U_3(x_t)$. This is a neighbourhood of ϕ in Φ. It suffices to show that $U_3 \subset \Psi$. Let $\phi' \in U_3$. For every $x \in X$ we have $x \in U_2(x_i)$ for at least one i, but also $\phi' \in U_3(x_i)$. By our choice of $U_2(x_i)$, $U_3(x_i)$ we have $B(\phi', x) \neq 0$. Therefore $\phi' \in \Psi$. We have shown that Ψ is open in Φ.

(v) We now show that $\Psi(1) \cap U$ lies dense in U. We actually prove that $\Psi(1)$ is dense in Φ (this is stronger). Suppose $\phi \notin \Psi(1)$. Then by definition, $B(\phi, y) = 0$ for at least one $y \in Z(1)$. This means $\phi \in E(y)$. Since $y \in Z(1)$, the intersection $(\phi + W_1) \cap E(y)$ has exactly one point. There is thus a surjective map

$$Z(1) \to (\phi + W_1) \setminus \Psi(1)$$
$$y \mapsto (\phi + W_1) \cap E(y).$$

Since B is piecewise differentiable, this map is also piecewise differentiable . Since Φ is Hausdorff, $W_1 + \phi$ has the usual topology as an n-dimensional real topological vector space. Since $Z(1)$ has dimension less than n, $(\phi, W_1) \setminus \Psi(1)$ contains no open subset of $\phi + W_1$. There is thus in every neighbourhood of ϕ in $\phi + W_1$, and therefore in every neighbourhood of ϕ in Φ, a $\phi' \in \Psi$. This finishes the proof.

4.2. Admissible paths

As before, L is a $\mathbf{Z}[\zeta]$-lattice in K and $\mathfrak{O}_L$ is its ring of multipliers, i.e. $\mathfrak{O}_L = \{\alpha \in K \mid \alpha L \subset L\}$. From now on we require α, β and q to be pairwise coprime elements of $\mathfrak{O}_L$ such that $\alpha \equiv \beta \equiv 1 \bmod (1 - \rho)q^2$.

We are interested in the values of our various fundamental functions on the subset

$$\frac{1}{\alpha\beta} L \setminus L = \{z \in K_\infty \mid \alpha\beta z \in L \text{ but } z \notin L\}$$

of K_∞, or the subset

$$\{\pi \in L \setminus K_\infty \mid \alpha\beta\pi = 0 \text{ but } \pi \neq 0\}$$

of the quotient space $L \setminus K_\infty$. These two sets will be referred to as the *critical sets* in $L \setminus K_\infty$ and K_∞. We shall write them as

$$S_{\alpha\beta} \subset K_\infty \text{ and } \mathrm{pr}_L(S_{\alpha\beta}) \subset L \setminus K_\infty.$$

Since α, β and q are pairwise coprime, it follows from §2.7.2 and §2.2, that the

points of the critical sets have trivial stabilizers. It is important that our functions are fundamental on these sets. The functions which we constructed in §3 are fundamental outside the boundaries of the modified parallelotopes used in their construction. We shall therefore try to modify our parallelotopes in such a way that their boundaries avoid the critical sets.

We call a path $[0.1]'$ from 0 to 1 in K_∞ *admissible,* iff

$$|\partial \mathscr{P}'| \cap S_{\alpha\beta} = \emptyset .$$

This means that the function f' is fundamental on the critical set $S_{\alpha\beta}$.

4.3. Lemma (Existence of admissible paths)

For every neighbourhood U of zero in K_∞ there is a differentiable, admissible path $[0.1]^1$ from 0 to 1 in K_∞ with

$$\frac{d}{dx}\left([0,1]^1(x) - [0,1](x)\right) \in U$$
$$\text{and } [0.1]^1(x) - [0,1](x) \in U.$$

And if we define

$$[0,1]^\alpha(x) := \begin{cases} \left[0, \frac{1}{\alpha}\right]^1(2x) & x \le \frac{1}{2} \\ \left[\frac{1}{\alpha}, 1\right]^1(2x-1) & x \ge \frac{1}{2} \end{cases}$$

$$[0,1]^\beta(x) := \begin{cases} \left[0, \frac{1}{\beta}\right]^1(2x) & x \le \frac{1}{2} \\ \left[\frac{1}{\beta}, 1\right]^1(2x-1) & x \ge \frac{1}{2}, \end{cases}$$

$$[0,1]^{\alpha,\beta}(x) := \begin{cases} \left[0, \frac{1}{\alpha\beta}\right]^1(4x) & x \le \frac{1}{4} \\ \left[\frac{1}{\alpha\beta}, \frac{1}{\alpha}\right]^1(4x-1) & \frac{1}{4} \le x \le \frac{1}{2} \\ \left[\frac{1}{\alpha}, 1\right]^1(2x-1) & x \ge \frac{1}{2}, \end{cases}$$

$$[0,1]^{\beta,\alpha}(x) := \begin{cases} \left[0, \frac{1}{\alpha\beta}\right]^1(4x) & x \le \frac{1}{4} \\ \left[\frac{1}{\alpha\beta}, \frac{1}{\beta}\right]^1(4x-1) & \frac{1}{4} \le x \le \frac{1}{2} \\ \left[\frac{1}{\beta}, 1\right]^1(2x-1) & x \ge \frac{1}{2}, \end{cases}$$

$$[0,1]^{\$}(x) := \begin{cases} \left[0, \frac{1}{\alpha\beta}\right]^{1}(2x) & x \leq \frac{1}{2} \\ \left[\frac{1}{\alpha\beta}, 1\right]^{1}(2x-1) & x \geq \frac{1}{2}, \end{cases}$$

then the paths $[0,1]^{\alpha}$, $[0,1]^{\beta}$, $[0,1]^{\alpha,\beta}$, $[0,1]^{\beta,\alpha}$, $[0,1]^{\$}$ *are also all admissible.*

Proof. (i) Let Φ be the real vector space of functions $\phi : I \to K_{\infty}$ satisfying the conditions

$$\phi(0) = \frac{d\phi}{dx}(0) = 0,$$

$$\forall\, 0 \leq x \leq \frac{q^2-1}{q^2} \text{ one has } \phi\left(x + \frac{1}{q^2}\right) = \phi(x).$$

Φ becomes a topological vector space with the following norm:

$$\| \phi \| := \inf_{x \in I} \left\{ \left| \phi(x) \right|, \left| \frac{d\phi}{dx}(x) \right| \right\}.$$

With this topology Φ is Hausdorff.

To each face $\mathcal{F} < \mathcal{P}$ we define $X_{\mathcal{F}}$ to be the disjoint union of six copies of I^{n-1}. We call these copies $X^{1}_{\mathcal{F}}$, $X^{\alpha}_{\mathcal{F}}$, $X^{\beta}_{\mathcal{F}}$, $X^{\alpha,\beta}_{\mathcal{F}}$, $X^{\beta,\alpha}_{\mathcal{F}}$ and $X^{\$}_{\mathcal{F}}$. Let X be the disjoint union over all $\mathcal{F} < \mathcal{P}$ of the sets $X_{\mathcal{F}}$. Then X is a compact, $(n-1)$-dimensional polyhedron.

To each $z \in S_{\alpha\beta}$ we shall define a map $B_z : X \times \Phi \to K_{\infty}$ to which we shall apply the technical lemma §4.1.

(ii) Let $\phi \in \Phi$. We define paths.

$$[0,1]^{1,\phi}(x) := [0,1](x) + \phi(x),$$

$$[0,1]^{\alpha,\phi}(x) := \begin{cases} \left[0, \frac{1}{\alpha}\right]^{1,\phi}(2x) & x \leq \frac{1}{2} \\ \left[\frac{1}{\alpha}, 1\right]^{1,\phi}(2x-1) & x \geq \frac{1}{2} \end{cases}$$

$$[0,1]^{\beta,\phi}(x) := \begin{cases} \left[0, \frac{1}{\beta}\right]^{1,\phi}(2x) & x \leq \frac{1}{2} \\ \left[\frac{1}{\beta}, 1\right]^{1,\phi}(2x-1) & x \geq \frac{1}{2}, \end{cases}$$

$$[0,1]^{\alpha,\beta,\phi}(x) := \begin{cases} \left[0, \frac{1}{\alpha\beta}\right]^{1,\phi}(4x) & x \le \frac{1}{4} \\ \left[\frac{1}{\alpha\beta}, \frac{1}{\alpha}\right]^{1,\phi}(4x-1) & \frac{1}{4} \le x \le \frac{1}{2} \\ \left[\frac{1}{\alpha}, 1\right]^{1,\phi}(2x-1) & x \ge \frac{1}{2}, \end{cases}$$

$$[0,1]^{\beta,\alpha,\phi}(x) := \begin{cases} \left[0, \frac{1}{\alpha\beta}\right]^{1,\phi}(4x) & x \le \frac{1}{4} \\ \left[\frac{1}{\alpha\beta}, \frac{1}{\beta}\right]^{1,\phi}(4x-1) & \frac{1}{4} \le x \le \frac{1}{2} \\ \left[\frac{1}{\beta}, 1\right]^{1,\phi}(2x-1) & x \ge \frac{1}{2}, \end{cases}$$

$$[0,1]^{\$,\phi}(x) := \begin{cases} \left[0, \frac{1}{\alpha\beta}\right]^{1,\phi}(2x) & x \le \frac{1}{2} \\ \left[\frac{1}{\alpha\beta}, 1\right]^{1,\phi}(2x-1) & x \ge \frac{1}{2}. \end{cases}$$

(iii) Let $\underline{x} = (x_1, \ldots, x_{n-1}) \in X^1_{\mathscr{F}}$, where $\mathscr{F} = \sigma_2(v_{\mathscr{F}}) \prod_{j=1}^{n-1}[0, a_{\mathscr{F},j}]$. We define for $x \in S_{\alpha\beta}$,

$$B_z(\underline{x}, \phi) := \mathscr{F}^{1,\phi}(\underline{x}) - z = v_{\mathscr{F}} + \sum_{j=1}^{n-1} [0, a_{\mathscr{F},j}]^{1,\phi}(x_j) - z.$$

The point $\underline{x}$ is degenerate (in the sense of §4.1) precisely when for all $j = 1, \ldots, n-1$, $x_j \in \left\{0, \frac{1}{q^2}, \ldots, 1\right\}$. If that is the case, then $v_{\mathscr{F}} + \sum_{j=1}^{n-1} [0, a_{\mathscr{F},j}]^{1,\phi}(x_j)$ is a $(1-\rho)q^2$-division point, and is therefore not in $S_{\alpha\beta}$. Therefore, if $\underline{x} \in X^1_{\mathscr{F}}$ is degenerate, then $B_z(\underline{x}, \phi) \neq 0$.

(iv) Let $\underline{x} = (x_1, \ldots, x_{n-1}) \in X^{\alpha}_{\mathscr{F}}$. We define

$$B_z(\underline{x}, \phi) := \mathscr{F}^{\alpha,\phi}(\underline{x}) - z = v_{\mathscr{F}} + \sum_{j=1}^{n-1} [0, a_{\mathscr{F},j}]^{\alpha,\phi}(x_j) - z.$$

The point $\underline{x}$ is degenerate precisely when for all $j = 1, \ldots, n-1$, $x_j \in \left\{0, \frac{1}{2q^2}, \ldots, 1\right\}$. We want to show that in that case, $B_z(\underline{x}, \phi) \neq 0$. Let $\underline{x}$ be degenerate. We shall compute $\alpha(v_{\mathscr{F}} + \sum_{j=1}^{n-1} [0, a_{\mathscr{F},j}]^{\alpha,\phi}(x_j))$ modulo L. We shall often use the fact that $\alpha \equiv 1 \bmod (1-\rho)q^2$. One has

$$\alpha\left(v_{\mathscr{F}} + \sum_{j=1}^{n-1} [0, a_{\mathscr{F},j}]^{\alpha,\phi}(x_j)\right) \equiv v_{\mathscr{F}} + \sum_{j=1}^{n-1} [0, \alpha a_{\mathscr{F},j}]^{\alpha,\phi}(x_j) \mod L.$$

Suppose $x_j > \frac{1}{2}$. Then

$$\begin{aligned}[0, \alpha a_{\mathscr{F},j}]^{\alpha,\phi}(x_j) &= [a_{\mathscr{F},j}, \alpha a_{\mathscr{F},j}](2x_j - 1) \\ &= a_{\mathscr{F},j} + (\alpha - 1)a_{\mathscr{F},j}(2x_j - 1) \\ &\equiv a_{\mathscr{F},j} \mod L \\ &\equiv [0, \alpha a_{\mathscr{F}',j}]^{\alpha,\phi}\left(\frac{1}{2}\right).\end{aligned}$$

We can thus assume $x_j \leq \frac{1}{2}$. We then have

$$\alpha\left(v_{\mathscr{F}} + \sum_{j=1}^{n-1} [0, a_{\mathscr{F},j}]^{\alpha,\phi}(x_j)\right) \equiv v_{\mathscr{F}} + \sum_{j=1}^{n-1} 2x_j a_{\mathscr{F},j} \mod L.$$

This is a $(1 - \rho)q^2$-division point and can only be in L if for all j, $x_j = 0$. Thus $v_{\mathscr{F}} + \sum_{j=1}^{n-1}[0, a_{\mathscr{F},j}]^{\alpha,\phi}(x_j)$ can only be an $\alpha\beta$-division point, if for all $j\, x_j = 0$. If that is the case, then $v_{\mathscr{F}} + \sum_{j=1}^{n-1}[0, a_{\mathscr{F},j}]^{\alpha,\phi}(x_j) = v_{\mathscr{F}} \notin S_{\alpha\beta}$. It follows that for degenerate $\underline{x} \in X_{\mathscr{F}}^{\alpha}$, $B_z(\underline{x}, \phi) \neq 0$.

(v) We define further for $\underline{x} \in X_{\mathscr{F}}^{\beta}$, $z \in S_{\alpha\beta}$:

$$B_z(\underline{x}, \phi) := \mathscr{F}^{\beta,\phi}(\underline{x}) - z,$$

and so on. As in (iv), we show that if $\underline{x}$ is degenerate, then for all $\phi \in \Phi$, $B_z(\underline{x}, \phi) \neq 0$. We can now apply §4.1.

(vi) We define for $z \in S_{\alpha\beta}$,

$$\Psi_z := \{\phi \in \Phi \mid \forall x \in X \text{ one has } B_z(x, \phi) \neq 0\}.$$

From §4.1, Ψ_z is a dense, open subset of Φ. If $\phi \in \Psi_z$, then by definition of B_z,

$$z \notin |\partial\mathscr{P}^{1,\phi}| \cup |\partial\mathscr{P}^{\alpha,\phi}| \cup \ldots \cup |\partial\mathscr{P}^{\$,\phi}|.$$

(vii) Let $S_{\alpha\beta}^{\text{finite}}$ be the set of all elements of $S_{\alpha\beta}$, in a large compact subset of K_∞. This is a finite set, but if $z \in S_{\alpha\beta} \setminus S_{\alpha\beta}^{\text{finite}}$, then Ψ_z contains a neighbourhood U' of 0 in Φ, which is independent of z. Let $\Psi := \cap_{z \in S_{\alpha\beta}} \Psi_z$. Then $\Psi \cap U' := \cap_{Z \in S_{\alpha\beta}^{\text{finite}}} \Psi_z$. This is also dense and open in U'. We can therefore choose a $\phi \in \Psi$ arbitrarily close to 0. Let $[0,1]^1(x) := [0,1](x) + \phi(x)$. Then $[0,1]^1$ satisfies the conditions of the lemma.

4.4. Admissible homotopies

In Theorem §3.11 we obtained a formula for the skew product $\langle f', f'' \rangle_{\alpha\beta} =$

$\sum_{z \in S_{\alpha\beta}} f'(z)\theta''(z)$, where $[0,1]'$ and $[0,1]''$ are two admissible paths. Our formula depends on the choice of a homotopy $h : I^2 \to K_\infty$ from $[0,1]'$ to $[0,1]''$, where h satisfies the following condition:

$$S_{\alpha\beta} \cap (\cup_{\mathscr{F}<\mathscr{P}} | \partial \tilde{h}_{\mathscr{F}} |) = \emptyset ,$$

with $\tilde{h}_{\mathscr{F}}$ as is §3.10. We shall call a homotopy which satisfies this condition *admissible*. To be able to apply Theorem §3.11 we must show that admissible homotopies exist. The following statements are easily proved (so we won't prove them).

- If $[0,1]'$, $[0,1]''$ and $[0,1]'''$ are three admissible paths, and h' and h'' are admissible homotopies from $[0,1]'$ to $[0,1]''$ and from $[0,1]''$ to $[0,1]'''$, then the composition (in the category of paths).

$$(h' \circ h'')(x, t) := \begin{cases} h'(x, 2t) & t \leq \frac{1}{2} \\ h''(x, 2t-1) & t \geq \frac{1}{2} \end{cases}$$

  is an admissible homotopy from $[0,1]'$ to $[0,1]'''$.
- If h is an admissible homotopy from $[0,1]'$ to $[0,1]''$ and of h' is pointwise close to h and also a homotopy from $[0,1]'$ to $[0,1]''$, then h' is also admissible.

We now show that close to any homotopy, there is always an admissible homotopy.

4.5. Lemma (Existence of admissible homotopies)

Let $[0,1]'$ and $[0,1]''$ be two admissible paths from 0 to 1 in K_∞, and let h_0 be any homotopy from $[0,1]'$ to $[0,1]''$. Then for any neighbourhood of zero $0 \in U \subset K_\infty$ there is an admissible homotopy $h : I^2 \to K_\infty$ from $[0,1]'$ to $[0,1]''$, with the property that for all $(x, t) \in I^2$,

$$h(x, t) - h_0(x, t) \in U .$$

If the functions $[0,1]'$, $[0,1]''$ and h_0 are differentiable, then we may also require that h is differentiable, and in addition that

$$\frac{\partial}{\partial x}(h(x, t) - h_0(x, t)) \in U$$

$$\text{and } \frac{\partial}{\partial t}(h(x, t) - h_0(x, t)) \in U .$$

Proof. (i) We first prove the lemma in the case that $[0,1]'$, $[0,1]''$ and h_0 are differentiable.

For each $\mathscr{F} < \mathscr{P}$ let $X_{\mathscr{F}}$ be the set ∂I^n, and let X be the disjoint union of all $X_{\mathscr{F}}$. Then X is a compact, $(n-1)$-dimensional polyhedron. We shall write points of $X_{\mathscr{F}}$ as $(\underline{x}, t)$, where $\underline{x} = (x_1, \ldots, x_{n-1}) \in I^{n-1}$ and $t \in I$.

(ii) Let Φ be the real vector space of differentiable functions

$$\phi : I^2 \to K_\infty$$
$$\partial I^2 \to 0,$$

whose restrictions to ∂I^2 are zero. We give Φ the topology, induced by the following norm:

$$\| \phi \| := \sup_{(x,t)\in I^2} \left\{ \left| \phi(x, t) \right|, \left| \frac{\partial \phi}{\partial x}(x, t) \right|, \left| \frac{\partial \phi}{\partial t}(x, t) \right| \right\}.$$

For every $z \in S_{\alpha\beta}$ we define a function $B_z : X \times \Phi \to K_\infty$. If $(\underline{x}, t) \in X_{\mathscr{F}}$ then we define

$$B_z((\underline{x}, t), \phi) := v_{\mathscr{F}} + \sum_{j=1}^{n-1} a_{\mathscr{F},j}(h_0(x_j, t) + \phi(x_j, t)) - z.$$

Since h_0 and ϕ are differentiable, B_z is also differentiable.

(iii) A point $(\underline{x}, t) \in X_{\mathscr{F}}$ is degenerate precisely when either $t \in \{0,1\}$, or $\underline{x}$ is a vertex of I^{n-1}.

- If $t = 0$ then $B_z((\underline{x}, t), \phi) = \mathscr{F}'(\underline{x}) - z$. Since $[0, 1]'$ is admissible, $B_x((\underline{x}, t), \phi) \neq 0$.
- If $t = 1$ then since $[0,1]''$ is admissible, $B_z((\underline{x}, t), \phi) \neq 0$.
- If $\underline{x}$ is a vertex of I^{n-1}, then $B_z((\underline{x}, t), \phi) + z$ is a vertex of a parallelotope $\mathscr{P}_t$. Therefore $B_z((x, t), \phi) \neq 0$.

The function B_z thus satisfies the conditions of §4.1.

(iv) Let $\Psi_z := \{\phi \in \Phi \mid \forall\, x \in X$ one has $B_z(x, \phi) \neq 0\}$. By §4.1, Ψ_z is dense and open in Φ. Let $\Psi := \cap_{z\in S_{\alpha\beta}} \Psi_z$. As in the proof of §4.3, Ψ is also a dense, open subset of Φ. We choose $\phi \in \Psi$ close to 0. Since $\phi \in \Psi$, one has for all $z \in S_\alpha$ and all $\mathscr{F} < \mathscr{P}$,

$$z \notin | \partial \tilde{h}^{\phi}_{\mathscr{F}} |,$$

where $h^\phi(x, t) := h_0(x, t) + \phi(x, h)$. The homotopy h^ϕ is therefore admmissible. Since ϕ close to 0, h^ϕ is close to h_0. The proof in the differentiable case is finished.

The non-differentiable case

Now consider continuous functions

$$[0,1]' : I \to K_\infty$$
$$[0,1]'' : I \to K_\infty$$
$$h_0 : I^2 \to K_\infty$$

with the conditions

$$[0,1]'(0) = [0,1]''(0) = h_0(0, t) = 0,$$
$$[0,1]'(1) = [0,1]''(1) = h_0(1, t) = 1,$$
$$h_0(x, 0) = [0,1]'(x),$$
$$h_0(x, 1) = [0,1]''(x),$$

and with $[0,1]'$ and $[0,1]''$ admissible. There are differentiable functions

$$[0,1]^{d'} : I \to K_\infty,$$
$$[0,1]^{d''} : I \to K_\infty,$$
$$h_0^d : I^2 \to K_\infty,$$

which are pointwise close to $[0,1]'$, $[0,1]''$ and h_0 and which satisfy the same conditions. Since $[0,1]'$ and $[0,1]''$ are admissible, and $[0,1]^{d'}$ and $[0,1]^{d''}$ are close to them, $[0,1]^{d'}$ and $[0,1]^{d''}$ are also admissible. From what we have already proved, there is an admissible homotopy h^d close to h_0^d. We define

$$h'(x, t) = (1 - t)[0,1]'(x) + t[0, 1]^{d'}$$
$$\text{and } h''(x, t) = (1 - t)[0,1]''(x) + t[0, 1]^{d''}.$$

The two homotopies h' and h'' are admissible. Now let

$$h(x, t) = \begin{cases} h'\left(x, \dfrac{t}{\varepsilon}\right) & t \leq \varepsilon \\ h_0^d\left(x, \dfrac{1}{1 - 2\varepsilon}(t - \varepsilon)\right) & \varepsilon \leq t \leq 1 - \varepsilon \\ h''\left(x, \dfrac{1 - t}{\varepsilon}\right) & t \geq 1 - \varepsilon. \end{cases}$$

The function h is an admissible homotopy from $[0,1]'$ to $[0,1]''$, and for small ε, h is close to h_0.

5. Proof of Theorem 1

As before let K be an algebraic number field with integers $\mathfrak{O}$. The field K contains a primitive q^{th} root of unity ζ, where q is a power of a prime p. We set $\rho = \zeta^{q/p}$, so ρ a primitive q^{th} root of unity. We fix a basis $\{b_1, \ldots, b_N\}$ of K as a vector space over $\mathbf{Q}(\zeta)$ such that the lattice L, generated by $\{b_1, \ldots, b_N\}$ over $\mathbf{Z}[\zeta]$ contains the ring $\mathfrak{O}$. We choose a $\mathfrak{d} \in \mathbf{N}$ such that $\mathfrak{d}L \subset \mathfrak{O} \subset L$. Let $\mathfrak{O}_L$ be the ring of the maltipliers of L.

In this chapter we prove the following

Let $\alpha, \beta \in \mathfrak{O}_L$ with the following conditions:

- *α, β and q are pairwise coprime in $\mathfrak{O}_L$:*
- *$\alpha, \beta \equiv \bmod (1-\rho)q^2$;*
- *α and β are totally positive. This means, that for every real place $v : K \to \mathbf{R}$ of K we have $v(\alpha), v(\beta) > 0$.*

Then

$$\mathrm{Dec}_L \frac{\alpha}{\beta} = \mathrm{Dec}_L \frac{\beta}{\alpha}.$$

With the help of the Gauss-Schering Lemma (§2.11) and Lemma §2.9.2 this implies the first theorem of the introduction:

THEOREM 1. *Let $\alpha, \beta \in \mathfrak{O}$ with the following conditions:*

- *$\alpha, \beta, \mathfrak{d}$ and q are pairwise coprime in $\mathfrak{O}$;*
- *$\alpha, \beta \equiv 1 \bmod \mathfrak{d}(1-\rho)q^2$;*
- *α and β are totally positive.*

Then

$$\left(\frac{\alpha}{\beta}\right)_q = \left(\frac{\beta}{\alpha}\right)_q.$$

We now give a summary of the proof. We begin with the statement of §2.12. With our conditions on α and β, this says:

$$\mathrm{Dec}_L \frac{\alpha}{\beta} - \mathrm{Dec}_L \frac{\beta}{\alpha} = \mathrm{Dec}_L \frac{\alpha}{\alpha\beta} - \mathrm{Dec}_L \frac{\beta}{\alpha\beta}.$$

The proof then consists of four lemmas. In §5.3 we show that

$$\sum_{z \in S_{\alpha\beta}} f^{\alpha}(z)\theta^1(\alpha z) = 0,$$

where $[0,1]^1$ and $[0,1]^{\alpha}$ are the admissible paths constructed in §4 and f^1 and f^{α}

are the corresponding fundamental functions. For the same reasons, we also have

$$\sum_{z \in S_{\alpha\beta}} f^{\beta}(z)\,\theta^{1}(\beta z) = 0.$$

We use these two statements in §5.4 together with the arithmetic results of §2, to express the difference $\mathrm{Dec}_L \frac{\alpha}{\alpha\beta} - \mathrm{Dec}_L \frac{\beta}{\alpha\beta}$ as a sum of four skew products. In §3.11 we proved a formula for these products. We apply this an §5.5 to reduce the four products down to one product. We finally show in §5.6, again using §3.11, that this last product is zero. This gives us $\mathrm{Dec}_L \frac{\alpha}{\beta} = \mathrm{Dec}_L \frac{\beta}{\alpha}$. Since we shall use the decidents $\mathrm{Dec}_L \frac{\alpha}{\alpha\beta}$ and $\mathrm{Dec}_L \frac{\beta}{\alpha\beta}$, it is important that our fundamental functions f^1, f^{α}, etc. are also fundamental in points of L. We thus define $f^1(0) = f^{\alpha}(0) = \ldots = 1$ and $f^1(z) = f^{\alpha}(z) = \ldots = 0$ for $z \in L \setminus 0$. At other $\alpha\beta$-division points, the functions are already defined and fundamental.

5.1. Proportional equivalence classes

We can embed the multiplicative group $\mathbf{R}^{>0}$ in $K_\infty^\times$ by the map $r \mapsto r.1$. We write the quotient group $K_\infty^\times/\mathbf{R}^{>0}$ as $K_\infty^\times{:}$. We call the cosets of $\mathbf{R}^{>0}$ (the elements of $K_\infty^\times{:}$) *proportional equivalence classes.* We write $z{:}$ for the proportional equivalence class of z. If $z_1{:} = z_2{:}$ then we say, that z_1 and z_2 are *proportionally equivalent.*

If $q \neq 2$ then K_∞ is a direct sum of $\frac{n}{2}$ copies of $\mathbf{C}$. Therefore $K_\infty^\times$ is a direct sum of $\frac{n}{2}$ copies of $\mathbf{C}^\times$, and is thus connected. Being a quotient of $K_\infty^\times$, the group $K_\infty^\times{:}$ is also connected. We shall assume that $\alpha{:}$ and $\beta{:}$ are both in a small neighbourhood of 1: in $K_\infty^\times{:}$. This implies in particular that α and β are totally positive[4]. It also implies that the paths $[0,1]^{\alpha}$, $[0,1]^{\beta}$, $[0,1]^{\alpha,\beta}$ and $[0,1]^{\beta,\alpha}$ are nearly straight, and that die maps $\mathcal{P}_i^{\alpha}$, $\mathcal{P}_i^{\beta}$, $\mathcal{P}_i^{\alpha,\beta}$ and $\mathcal{P}_i^{\beta,\alpha} : I^n \to K_\infty$ are injective.

5.2. Remark

If $[a, b]^1 \times \mathcal{T}$ is an element of $z_n\left(K_\infty, K_\infty \setminus \frac{1}{\alpha\beta} L\right)$ such that $b - a \in \frac{q}{\alpha\beta} L$, then one has in $\mathbf{Z}/q\mathbf{Z}{:}$

[4] totally positive means that for every embedding $v : K \to \mathbf{R}$ of the field K in the real numbers, $v(\alpha) > 0$ and $v(\beta) > 0$.

$$\left\{\left\{\frac{1}{\alpha\beta}L \,\middle|\, [a, b]^1 \times \mathcal{T}\right\}\right\} = 0.$$

We will often use this fact.

The next lemmas are similar to lemmas due to Habicht in the case $K = \mathbf{Q}(\sqrt{-3})$.

5.3. Lemma.

If $\alpha, \beta \in \mathfrak{O}_L$ *with* $\alpha \equiv 1 \bmod (1-\rho)q$ *and* α: *is close to* 1:, *then*

$$\sum_{\alpha\beta\pi=0, \pi\neq 0} f^{\alpha}(\pi)\theta^1(\alpha\pi) \equiv 1 \mod q.$$

(This however is not the reciprocity law.)

Proof. We have $\mathcal{P}^{\alpha} = \sum_i \mathcal{P}_i^{\alpha}$ for some set of parallelotopes $\mathcal{P}_i$. Correspondingly we have $f^{\alpha} = \sum_i \mathbf{I}_{\mathcal{P}_i^{\alpha}}$. We first consider sums of the form

$$\sum_{\alpha\beta\pi=0, \pi\neq 0} \mathbf{I}_{\mathcal{P}^{\alpha}}(\pi)\theta^1(\alpha\pi).$$

For each parallelotope there is an expression

$$\mathcal{P}_i^{\alpha} = \prod_{j=1}^{n} [0, a_{i,j}]^{\alpha},$$

where $a_{i,j} \in \frac{1}{1-\rho}L$. By definition (§4.3) of $[0, a_{i,j}]^{\alpha}$, this is the equivalent to

$$\prod_{j=1}^{n} \left(\left[0, \frac{a_{i,j}}{\alpha}\right]^1 + \left[\frac{a_{i,j}}{\alpha}, a_{i,j}\right]^1\right).$$

Expanding the brackets we obtain:

$$\prod_{j=1}^{n} \left[0, \frac{a_{i,j}}{\alpha}\right]^1 + \text{parallelotopes, at least one of whose edges is a vector in } \frac{q}{\alpha}L.$$

The first term is equal to

$$\sigma_1(\alpha^{-1})\mathcal{P}_i^1.$$

On summing again over the parallelotopes we obtain

$$\mathcal{P}^{\alpha} = \sigma_1(\alpha^{-1})\mathcal{P}^1 + \text{parallelotopes, at least one of whose edges is a vector in } \frac{q}{\alpha}L.$$

The function $\theta^1(z)$ is periodic with respect to L. Thus $\theta^1(a\pi)$ is periodic with period lattice $\frac{1}{\alpha}L$. The set $\frac{1}{\alpha\beta}L$ is also invariant under translations by elements of $\frac{1}{\alpha}L$. Therefore the sum of $\theta^1(\alpha\pi)$ over a parallelotope with at least one edge in $\frac{q}{\alpha}L$ vanishes modulo q. Since α: is close to 1:, the base set of one of these parallelotopes cannot contain 0. We therefore have:

$$\sum_{\alpha\beta\pi=0\ \pi\neq 0} \mathbf{I}_{\mathscr{P}^\alpha}(\pi)\,\theta^1(\alpha\pi) = \sum_{z\in(\alpha\beta)^{-1}L\ z\neq 0} \mathbf{I}_{\sigma_1(\alpha^{-1})\mathscr{P}^1}(z)\,\theta^1(\alpha z).$$

Either α has positive norm or $q = 2$. Thus in $\mathbf{Z}/q\mathbf{Z}$ one has

$$\mathbf{I}_{\sigma_1(\alpha^{-1})\mathscr{P}^1}(z) = \mathbf{I}_{\mathscr{P}^1}(\alpha z).$$

Our sum is therefore

$$\sum_{z\in(\alpha\beta)^{-1}L\ z\neq 0} \mathbf{I}_{\mathscr{P}^1}(\alpha z)\,\theta^T(\alpha z),$$

or more simply

$$\sum_{z\in\beta^{-1}L\ z\neq 0} \mathbf{I}_{\mathscr{P}^1}(z)\,\theta^T(z).$$

Since this expression is identical to $\mathrm{Dec}_{L\frac{1}{\beta}}$, we know (for example by the additivity properties §2.10), that it vanishes in $\mathbf{Z}/q\mathbf{Z}$.

5.4. Arithmetical calculations

In this paragraph let α and β be totally positive elements of $\mathfrak{O}_L$ with $\alpha \equiv \beta \equiv 1 \bmod (1-\rho)q$ and α: and β: in a small neighbourhood of 1: - small enough, that is, for the previous lemma (§5.3) to apply.

We use Lemma §5.3 together with some results from Chapter §2. It is first clear that

$$\mathrm{Dec}_L^{(f^1)}\frac{\alpha}{\alpha\beta} = \sum_{\alpha\beta\pi=0,\pi\neq 0} (f^1(\pi) - f^\alpha(\pi))\ \theta^1(\alpha\pi).$$

The variable π here is in $L\setminus K_\infty$. The function $f^1(\alpha\pi): L\setminus K \to \mathbf{Z}/q\mathbf{Z}$ is 1 at $\pi = 0$ and zero at all other α-division points. At points other than α-division point, the function is fundamental. The sum is thus by §2.8.2

$$\sum_{\alpha\beta\pi=0,\alpha\pi\neq 0} (f^1(\pi) - f^\alpha(\pi))\,\theta^1(\pi).$$

We rewrite this as follows:

$$\sum_{\alpha\beta\pi=0,\pi\neq 0} (f^1(\pi) - f^\alpha(\pi))\,\theta^1(\pi) - \sum_{\alpha\pi=0,\pi\neq 0} (f^1(\pi) - f^\alpha(\pi))\,\theta^1(\pi).$$

Since $\mathrm{Dec}_L \frac{1}{\alpha\beta}$ and $\mathrm{Dec}_L \frac{1}{\alpha}$ are both zero (this holds for example by §2.10), this is equal to

$$-\sum_{\alpha\beta\pi=0,\pi\neq 0} f^\alpha(\pi)\,\theta^1(\pi) + \sum_{\alpha\pi=0,\pi\neq 0} f^\alpha(\pi)\,\theta^1(\pi).$$

This is a sum of skew products:

$$-\langle f^\alpha, f^1\rangle_{\alpha\beta} + \langle f^\alpha, f^1\rangle_\alpha.$$

Thus from Lemma §2.12 we know that $\mathrm{Dec}_L \frac{\alpha}{\beta} - \mathrm{Dec}_L \frac{\beta}{\alpha}$ is equal to

$$-\langle f^\alpha, f^1\rangle_{\alpha\beta} + \langle f^\alpha, f^1\rangle_\alpha + \langle f^\beta, f^1\rangle_{\alpha\beta} - \langle f^\beta, f^1\rangle_\beta.$$

5.5. Lemma

If $\alpha, \beta \equiv 1 \bmod (1-\rho)q^2$ *in* $\mathfrak{O}_L$ *and* α, β *and* q *are pairwise coprime in* $\mathfrak{O}_L$, *and if* α: *and* β: *are close to* 1: *in* K_∞:, *then*

$$\mathrm{Dec}_L \frac{\alpha}{\beta} - \mathrm{Dec}_L \frac{\beta}{\alpha} = \langle f^{\beta,\alpha}, f^{\alpha,\beta}\rangle_{\alpha\beta}.$$

Proof. (i) The proof is quite long but the idea is simple. In the one dimensional case ($K = \mathbf{Q}$) this is all trivial because the fundamental functions are independent of the paths. The lemma can be easily understood for fields of degree 2. In higher dimensions some new phenomena arise and the two-dimensional picture becomes inaccurate. A full impression of the proof can be gained by considering three-dimensional cases, in which everything goes wrong that can go wrong.

Our calculations will be mainly in the homology group $\mathcal{H}_n(K_\infty, K_\infty \setminus S_{\alpha\beta})$. We shall first show that

$$\langle f^\alpha, f^1\rangle_\alpha = \langle f^{\beta,\alpha}, f^\beta\rangle_{\alpha\beta}. \tag{1}$$

This follows because the difference between $[0,1]^{\beta,\alpha}$ and $[0,1]^\beta$ is essentially $\frac{1}{\beta}$ times the difference between $[0,1]^\alpha$ and $[0,1]^1$ (this can be seen by drawing a pic-

ture). On the other hand the sum on the right is over $\alpha\beta$-division points, whereas that on the left is only over α-division points. Our proof of (1) will use the skew product formula §3.11. After proving this, the lemma follows from §5.4 using only the elementary properties of the skew-product.

(ii) To apply §3.11, we need admissible homotopies from $[0,1]^{\alpha}$ to $[0,1]^{1}$ and from $[0,1]^{\beta,\alpha}$ to $[0,1]^{\beta}$. We now construct these homotopies. Let U be a neighbourhood of 0 in K_{∞}. We define

$$h_0(x, t) := t[0,1]^{1}(x) + (1 - t)[0,1]^{\alpha}(x).$$

The function h_0 is a homotopy from $[0,1]^{1}$ to $[0,1]^{\alpha}$. We choose using §4.5 an admissible homotopy h^{1} from $[0,1]^{1}$ to $[0,1]^{\alpha}$, which is uniformly close to h_0 (it is not so important which admissible homotopy we choose). We therefore have a continuous function $h^{1}: I^{2} \to K_{\infty}$ satisfying the following:

$$h^{1}(x, 0) = [0,1]^{1}(x), \quad h^{1}(x, 1) = [0,1]^{\alpha}(x),$$
$$h^{1}(0, t) = 0, \quad h^{1}(1, t) = 1,$$
$$\forall\, (x, t) \in I^{2} \text{ one has } h^{1}(x, t) - h_0(x, t) \in U, \quad h^{1} \text{ is admissible.}$$

We compress this by β^{-1}, and obtain a homotopy from $[0, \beta^{-1}]^{1}$ to $[0, \beta^{-1}]^{\alpha}$, which we shall denote h^{2}:

$$h^{2}(x, t) := \frac{1}{\beta} h^{1}(x, t).$$

Finally we extend h^{2} by a constant homotopy from $\left[\frac{1}{\beta}, 1\right]^{1}$ to itself, thus obtaining a homotopy h^{3} from $[0,1]^{\beta}$ to $[0,1]^{\beta,\alpha}$.

$$h^{3}(x, t) := \begin{cases} h^{2}(2x, t) & \text{if } x \leq \frac{1}{2}, \\ \left[\frac{1}{\beta}, 1\right]^{1}(2x - 1) & \text{if } x \geq \frac{1}{2}. \end{cases}$$

The admissibility of h^{3} follows from that of h^{1}. We construct as described in §3.10 the homotopies $\widetilde{h^{1}}$, $\widetilde{h^{2}}$ and $\widetilde{h^{3}}$.

(iii) From Theorem §3.11 we have

$$\langle f^{\alpha}, f^{1} \rangle_{\alpha} = \sum_{[\mathcal{F}]} w[\mathcal{F}]\{\{S_{\alpha} \mid \widetilde{h^{1}}_{\mathcal{F}}\}\},$$
$$\langle f^{\beta\alpha}, f^{\beta} \rangle_{\alpha\beta} = \sum_{[\mathcal{F}]} w[\mathcal{F}]\{\{S_{\alpha\beta} \mid \widetilde{h^{3}}_{\mathcal{F}}\}\}.$$

To show that $\langle f^{\alpha}, f^{1} \rangle_{\alpha} = \langle f^{\beta\alpha}, f^{\beta} \rangle_{\alpha\beta}$, it is clearly sufficient to prove for each

face $\mathscr{F} < \mathscr{P}$ that

$$\{\{S_\alpha \mid \tilde{h}^1{}_{\mathscr{F}}\}\} = \{\{S_{\alpha\beta} \mid \tilde{h}^3{}_{\mathscr{F}}\}\}.$$

We shall prove this.

(iv) Let $\mathscr{F}$ be a general face of a parallelotope of $\mathscr{P}$. Then there is an expression of the form

$$\mathscr{F} = \sigma_2(v_{\mathscr{F}}) \prod_{i=1}^{n-1} [0, a_{\mathscr{F},i}],$$

where $v_{\mathscr{F}}, a_{\mathscr{F},i} \in \frac{1}{1-\rho} L$. We cut the n-cube $\tilde{h}^3_{\mathscr{F}}$ into 2^{n-1} pieces. This cutting process corresponds to cutting $\mathscr{F}$ into 2^{n-1} pieces, each half as big as $\mathscr{F}$. We thus have in $\mathscr{H}_n(K_\infty, K_\infty \setminus S_{\alpha\beta})$:

$$\tilde{h}^3_{\mathscr{F}} \doteq \sum_{T \subset \{1,2,\ldots,n-1\}} \tilde{h}^{3T}_{\mathscr{F}},$$

where

$$\tilde{h}^{3T}_{\mathscr{F}}(x_1, x_2, \ldots, x_{n-1}, t) = v_{\mathscr{F}} + \sum_{j \in \{1,2,\ldots,n-1\} \setminus T} a_{\mathscr{F},j} h^3\left(\frac{x_j}{2}, t\right) + \sum_{j \in T} a_{\mathscr{F},j} h^3\left(\frac{x_j + 1}{2}, t\right).$$

We first see that the boundary of $\tilde{h}^{3T}_{\mathscr{F}}$ has no intersection with $S_{\alpha\beta}$. This follows because the boundary can be covered by translations of the boundary of $\tilde{h}^3{}_{\mathscr{F}}$ by $\alpha\beta$-division points, and h^3 is admissible. We therefore have

$$\{\{S_{\alpha\beta} \mid \tilde{h}^3{}_{\mathscr{F}}\}\} = \sum_{T \subset \{1,2,\ldots,n-1\}} \{\{S_{\alpha\beta} \mid \tilde{h}^{3T}_{\mathscr{F}}\}\}.$$

We now compute the terms in this sum.

(v) First suppose T is empty. We then have

$$\begin{aligned}
\tilde{h}^{3T}_{\mathscr{F}}(x_1, x_2, \ldots, x_{n-1}, t) &= v_{\mathscr{F}} + \sum_{j=1}^{n-1} a_{\mathscr{F},j} h^3\left(\frac{x_j}{2}, t\right) \\
&= v_{\mathscr{F}} + \sum_{j=1}^{n-1} a_{\mathscr{F},j} h^2(x_j, t) \\
&= v_{\mathscr{F}} + \frac{1}{\beta} \sum_{j=1}^{n-1} a_{\mathscr{F},j} h^1(x_j, t) \\
&= \frac{1}{\beta}\left(v_{\mathscr{F}} + \sum_{j=1}^{n-1} a_{\mathscr{F},j} h^1(x_j, t)\right) + \frac{\beta - 1}{\beta} v_{\mathscr{F}}.
\end{aligned}$$

Thus

$$\tilde{h}^{3T}_{\mathscr{F}} = \sigma\left(\frac{1}{\beta}, \frac{\beta - 1}{\beta} v_{\mathscr{F}}\right) \tilde{h}^1_{\mathscr{F}},$$

and therefore

$$\begin{aligned}\{\{S_{\alpha\beta} \mid \tilde{h}^{3T}_{\mathscr{F}}\}\} &= \left\{\left\{S_{\alpha\beta} \,\middle|\, \sigma\left(\frac{1}{\beta}, \frac{\beta-1}{\beta} v_{\mathscr{F}}\right)\tilde{h}^{1}{}_{\mathscr{F}}\right\}\right\} \\ &= \left\{\left\{\frac{1}{\alpha\beta} L \setminus \{0\} \,\middle|\, \sigma\left(\frac{1}{\beta}, \frac{\beta-1}{\beta} v_{\mathscr{F}}\right)\tilde{h}^{1}{}_{\mathscr{F}}\right\}\right\} \\ &= \left\{\left\{\frac{1}{\alpha} L \setminus \{0\} \,\middle|\, \sigma_2((\beta-1)v_{\mathscr{F}})\tilde{h}^{1}{}_{\mathscr{F}}\right\}\right\}.\end{aligned}$$

We now distinguish two cases. First suppose $v_{\mathscr{F}} = 0$. We then have immediately

$$\{\{S_{\alpha\beta} \mid \tilde{h}^{3T}_{\mathscr{F}}\}\} = \left\{\left\{\frac{1}{\alpha} L \setminus \{0\} \,\middle|\, \tilde{h}^{1}{}_{\mathscr{F}}\right\}\right\}.$$

In the other case $v_{\mathscr{F}} \neq 0$. Then there is a neighbourhood of $|\mathscr{F}|$, which is disjoint from L. We therefore have for α: and β: sufficiently close to 1: and $[0,1]^1$ sufficiently close to $[0,1]$, $L \cap |\tilde{h}^{1}{}_{\mathscr{F}}| = \emptyset$. Therefore (since $(\beta-1)v_{\mathscr{F}} \in L$) $|\sigma_2((\beta-1)v_{\mathscr{F}})\tilde{h}^{1}{}_{\mathscr{F}}| \cap L = \emptyset$. We thus have as in the first case

$$\{\{S_{\alpha\beta} \mid \tilde{h}^{3T}_{\mathscr{F}}\}\} = \left\{\left\{\frac{1}{\alpha} L \setminus \{0\} \,\middle|\, \tilde{h}^{1}{}_{\mathscr{F}}\right\}\right\}.$$

(vi) Now suppose T is non-empty. Without loss of generality, assume $1 \in T$. Then

$$\tilde{h}^{3T}_{\mathscr{F}}(x_1, x_2, \ldots, x_{n-1}, t) = a_{\mathscr{F},1} h^3\left(\frac{x_1+1}{2}, t\right) + g(x_2, \ldots, x_{n-1}, t)$$

with a suitable function g. However $h^3\left(\frac{x_1+1}{2}, t\right) = \left[\frac{1}{\beta}, 1\right]^1(x_1)$. We therefore have

$$\tilde{h}^{3T}_{\mathscr{F}} = \left[\frac{a_{\mathscr{F},1}}{\beta}, a_{\mathscr{F},1}\right]^1 \times g.$$

Since T is non-empty, $|\tilde{h}^{3T}_{\mathscr{F}}|$ contains no point of L. Therefore by Remark §5.2,

$$\{\{S_{\alpha\beta} \mid \tilde{h}^{3T}_{\mathscr{F}}\}\} = 0.$$

(vii) We have shown in (iv), (v) and (vi) that for every face $\mathscr{F} < \mathscr{P}$,

$$\{\{S_{\alpha\beta} \mid \tilde{h}^{3}{}_{\mathscr{F}}\}\} = \{\{S_{\alpha} \mid\mid \tilde{h}^{1}{}_{\mathscr{F}}\}\}.$$

Therefore by Theorem §3.11,

$$\langle f^{\alpha}, f^{1}\rangle_{\alpha} = \langle f^{\beta,\alpha}, f^{\beta}\rangle_{\alpha\beta}.$$

Of course we have for the same reasons:

$$\langle f^{\beta}, f^{1}\rangle_{\beta} = \langle f^{\alpha,\beta}, f^{\alpha}\rangle_{\alpha\beta}.$$

Substituting this into the formula at the end of §5.4 we obtain:

$$\mathrm{Dec}_L \frac{\alpha}{\beta} - \mathrm{Dec}_L \frac{\beta}{\alpha} = + \langle f^{\beta}, f^{1}\rangle_{\alpha\beta} + \langle f^{\beta,\alpha}, f^{\beta}\rangle_{\alpha\beta} - \langle f^{\alpha}, f^{1}\rangle_{\alpha\beta} - \langle f^{\alpha,\beta}, f^{\alpha}\rangle_{\alpha\beta}.$$

From the skew-symmetry of the product we have:

$$\mathrm{Dec}_L \frac{\alpha}{\beta} - \mathrm{Dec}_L \frac{\beta}{\alpha} = + \langle f^{\beta}, f^{1}\rangle_{\alpha\beta} - \langle f^{\beta}, f^{\beta,\alpha}\rangle_{\alpha\beta} - \langle f^{\alpha}, f^{1}\rangle_{\alpha\beta} + \langle f^{\alpha}, f^{\alpha,\beta}\rangle_{\alpha\beta}.$$

From the bilinearity we have:

$$\mathrm{Dec}_L \frac{\alpha}{\beta} - \mathrm{Dec}_L \frac{\beta}{\alpha} = + \langle f^{\beta}, f^{1} - f^{\beta,\alpha}\rangle_{\alpha\beta} - \langle f^{\alpha}, f^{1} - f^{\alpha,\beta}\rangle_{\alpha\beta}.$$

The third property of the product gives us

$$\mathrm{Dec}_L \frac{\alpha}{\beta} - \mathrm{Dec}_L \frac{\beta}{\alpha} = + \langle f^{\beta,\alpha}, f^{1}\rangle_{\alpha\beta} - \langle f^{\alpha,\beta}, f^{1}\rangle_{\alpha\beta}.$$

Again by bilinearity it follows that

$$\mathrm{Dec}_L \frac{\alpha}{\beta} - \mathrm{Dec}_L \frac{\beta}{\alpha} = + \langle f^{\beta,\alpha} - f^{\alpha,\beta}, f^{1}\rangle_{\alpha\beta},$$

and by the third property:

$$\mathrm{Dec}_L \frac{\alpha}{\beta} - \mathrm{Dec}_L \frac{\beta}{\alpha} = + \langle f^{\beta,\alpha}, f^{\alpha,\beta}\rangle_{\alpha\beta}.$$

5.6. The reciprocity law (first form)

We now prove the following:

If

$$\alpha, \beta \equiv 1 \bmod \begin{cases} (1-\rho)q^2 & \text{for odd } q \\ 4q^2 & \text{for even } q \end{cases} \text{ in } \mathfrak{O}_L,$$

and if α, β and q are pairwise coprime in $\mathfrak{O}_L$ and if α: and β: are sufficiently

close to 1: *in* K_∞:, *then*

$$\mathrm{Dec}_L \frac{\alpha}{\beta} = \mathrm{Dec}_L \frac{\beta}{\alpha}.$$

Using the Gauss-Schering Lemma (§2.11) and Lemma §2.9.2 this gives us the following:

If

$$\alpha, \beta \equiv 1 \bmod \begin{cases} (1-\rho)q^2\mathfrak{d} & \text{for odd } q \\ 4q^2\mathfrak{d} & \text{for even } q \end{cases} \text{ in } \mathfrak{O},$$

and if α, β,$\mathfrak{d}$ *and* q *are coprime in* $\mathfrak{O}$, *and if* α: *and* β: *are sufficiently close to* 1: *in* K_∞:, *then*

$$\left(\frac{\alpha}{\beta}\right)_q = \left(\frac{\beta}{\alpha}\right)_q.$$

(*Here* $\mathfrak{d}$ *is chosen so that* $\mathfrak{d}L \subset \mathfrak{O} \subset L$.)

Proof. (i) We first consider the case that q is odd. The minor changes required for the case that q is even will be described at the end of the proof. The conditions of the previous lemma are satisfied. We therefore have

$$\mathrm{Dec}_L \frac{\alpha}{\beta} - \mathrm{Dec}_L \frac{\beta}{\alpha} = \langle f^{\beta,\alpha}, f^{\alpha,\beta} \rangle_{\alpha\beta}.$$

From the properties of the skew product (§2.13) we obtain,

$$\begin{aligned} \mathrm{Dec}_L \frac{\alpha}{\beta} - \mathrm{Dec}_L \frac{\beta}{\alpha} &= \langle f^{\beta,\alpha} - f^{\alpha,\beta}, f^{\$} \rangle_{\alpha\beta} \\ &= \langle f^{\beta,\alpha}, f^{\$} \rangle_{\alpha\beta} - \langle f^{\alpha,\beta}, f^{\$} \rangle_{\alpha\beta}. \end{aligned}$$

We shall show that $\langle f^{\alpha,\beta}, f^{\$} \rangle_{\alpha\beta} \equiv 0$. Since our conditions on α and β are symmetric, we obtain in the same way $\langle f^{\beta,\alpha} f^{\$} \rangle_{\alpha\beta} \equiv 0$ and therefore as required $\mathrm{Dec}_L \frac{\alpha}{\beta} = \mathrm{Dec}_L \frac{\beta}{\alpha}$. If α and β are coprime to $\mathfrak{d}$, then by §2.9.2 $\mathrm{Dec}_L \frac{\alpha}{\beta} = \mathrm{Dec}_{\mathfrak{O}} \frac{\alpha}{\beta}$ and $\mathrm{Dec}_L \frac{\beta}{\alpha} = \mathrm{Dec}_{\mathfrak{O}} \frac{\beta}{\alpha}$. We thus have in this case $\mathrm{Dec}_{\mathfrak{O}} \frac{\alpha}{\beta} = \mathrm{Dec}_{\mathfrak{O}} \frac{\beta}{\alpha}$ and by the Gauss-Schering Lemma (§2.11).

$$\left(\frac{\alpha}{\beta}\right)_q = \left(\frac{\beta}{\alpha}\right)_q.$$

It is therefore sufficient to prove that $\langle f^{\alpha,\beta}, f^{\$}\rangle_{\alpha\beta} \equiv 0$.

(ii) We recall that the functions $f^{\$}$ and $f^{\alpha,\beta}$ are defined using the paths $[0,1]^{\$}$ and $[0,1]^{\alpha,\beta}$, where

$$[0,1]^{\$}(x) = \begin{cases} \left[0, \frac{1}{\alpha\beta}\right]^1(2x) & x \le \frac{1}{2}, \\ \left[\frac{1}{\alpha\beta}, 1\right]^1(2x-1) & x \ge \frac{1}{2}, \end{cases}$$

$$[0,1]^{\alpha,\beta}(x) = \begin{cases} \left[0, \frac{1}{\alpha\beta}\right]^1(2x) & x \le \frac{1}{2}, \\ \left[\frac{1}{\alpha\beta}, \frac{1}{\alpha}\right]^1(4x-2) & \frac{1}{2} \le x \le \frac{3}{4}, \\ \left[\frac{1}{\alpha}, 1\right]^1(4x-3) & x \ge \frac{3}{4}. \end{cases}$$

From this we see that the difference between $[0,1]^{\$}$ and $[0,1]^{\alpha,\beta}$ is essentially a triangle whose vertices $\left(\frac{1}{\alpha\beta}, \frac{1}{\alpha}\right.$ and $\left.1\right)$ are congruent modulo $\frac{(1-\rho)q^2}{\alpha\beta}L$. We shall exploit this congruence to show that $\langle f^{\alpha,\beta}, f^{\$}\rangle_{\alpha\beta} \equiv 0$.

(iii) We shall construct a special admissible homotopy h from $[0,1]^{\$}$ to $[0,1]^{\alpha,\beta}$. Then by the skew product formula (§3.11),

$$= \langle f^{\alpha,\beta}, f^{\$}\rangle_{\alpha\beta} \equiv \sum_{[\mathcal{F}]} w[\mathcal{F}]\{\{S_{\alpha\beta} \mid \tilde{h}_{\mathcal{F}}\}\}.$$

For every face $\mathcal{F} < \mathcal{P}$ we shall show that

$$\{\{S_{\alpha\beta} \mid \tilde{h}_{\mathcal{F}}\}\} \equiv 0.$$

From this it follows that $\langle f^{\alpha,\beta}, f^{\$}\rangle_{\alpha\beta} \equiv 0$. The difficult thing is to find the right homotopy h.

(iv) We now begin to construct the homotopy h. The two paths $[0,1]^{\$}$ and $[0,1]^{\beta,\alpha}$ are the same from 0 to $\frac{1}{\alpha\beta}$. We call this part of the paths the singular part. In the singular part, whose preimage in I is $\left[0, \frac{1}{2}\right]$, we define $h(x, t)$ to be independent of t. Thus for $x \le \frac{1}{2}$ we have

$$h(x, t) = \left[0, \frac{1}{\alpha\beta}\right]^1(2x).$$

The rest of h depends on t, since $[0,1]^{\$}$ and $[0,1]^{\beta,\alpha}$ are not the same between $\frac{1}{\alpha\beta}$

and 1. We call this part of h the non-singular part. If the face $\mathcal{F}$ is given by the product

$$\sigma_2(v_{\mathcal{F}}) \prod_{i=1}^{n-1} [0, a_{\mathcal{F},j}],$$

then we have

$$\tilde{h}_{\mathcal{F}}(x_1, \ldots, x_{n-1}, t) = v_{\mathcal{F}} + \sum_{x_i \in [0,\frac{1}{2}]} \left[0, \frac{a_{\mathcal{F},j}}{\alpha\beta}\right]^1 (2x_i) + \sum_{x_i \notin [0,\frac{1}{2}]} a_{\mathcal{F},j}\, h(x_i, t).$$

To make this more readable, we define for every subset $T \subset \{1,2,\ldots,n-1\}$ a function

$$g_T(x_1, \ldots, x_{n-1}, t) = v_{\mathcal{F}} + \sum_{j \in T} \left[0, \frac{a_{\mathcal{F},j}}{\alpha\beta}\right]^1 (x_j) + \sum_{j \notin T} a_{\mathcal{F},j}\, h\left(\frac{x_i + 1}{2}, t\right).$$

The function g_T is a singular n-cube in K_∞. We have an equivalence in $\mathcal{H}_n(K_\infty, K_\infty \setminus S_{\alpha\beta})$:

$$\tilde{h}_{\mathcal{F}} \simeq \sum_{T \subset \{1,2,\ldots,n-1\}} g_T.$$

We shall construct the non-singular part of h such that for every T one has

$$\{\{S_{\alpha\beta} \mid g_T\}\} = 0.$$

If T is empty then g_T is degenerate and the equation follows immediately. Thus the totally singular part of $\tilde{h}_{\mathcal{F}}$ vanishes. Now suppose T is non-empty. Since α: and β: are close to 1:, we can (and shall) choose h is such a way that for non-empty T the sets $|\, g_T\,|$ and L are disjoint. It is then sufficient to show that

$$\left\{\left\{\frac{1}{\alpha\beta} L \,\middle|\, g_T\right\}\right\} \equiv 0.$$

(v) We would now like to construct the non-singular part of h. For this purpose we define

$$h^{ns} : I^2 \to K_\infty$$
$$(x, t) \mapsto h\left(\frac{x+1}{2}, t\right).$$

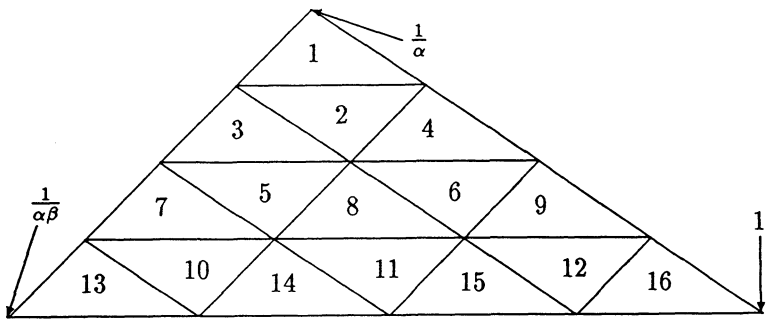
This function is a homotopy between the non-singular parts of $[0,1]^{\alpha,\beta}$ and $[0,1]^{\$}$. We can now express g_T more easily:

$$g_T(x_1, \ldots, x_{n-1}, t) = v_{\mathfrak{F}} + \sum_{j \in T} \left[0, \frac{a_{\mathfrak{F},j}}{\alpha\beta}\right]^1 (x_j) + \sum_{j \notin T} a_{\mathfrak{F},j}\, h^{ns}(x_j, t).$$

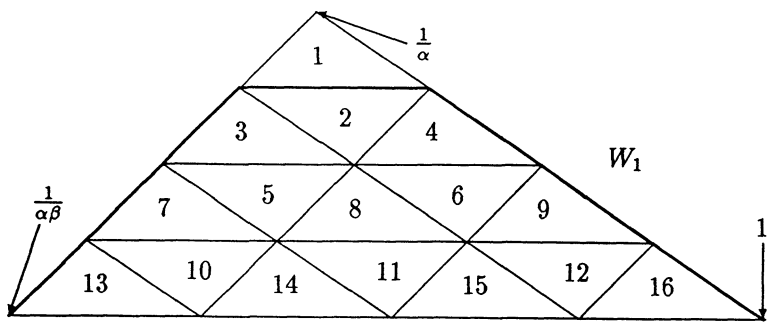
(vi) We first construct a sequence of paths between $\frac{1}{\alpha\beta}$ and 1:

$$W_0, W_1, W_2, \ldots, W_{q^2}$$

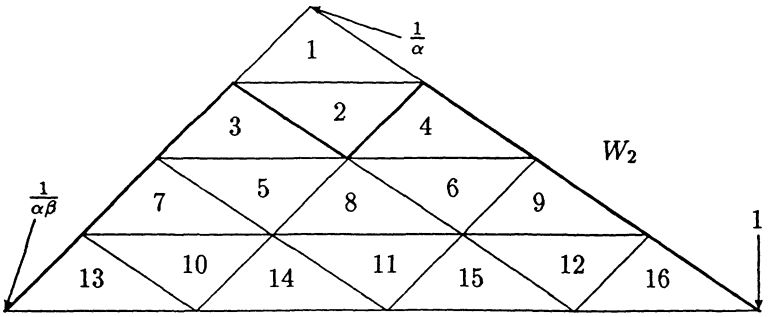
where W_0 is the non-singular part of $[0,1]^{\alpha,\beta}$ and W_{q^2} is $\left[\frac{1}{\alpha\beta}, 1\right]^1$. Between W_0 and W_{q^2} there is a modified triangle, whose vertices are $\frac{1}{\alpha\beta}$, $\frac{1}{\alpha}$ and 1. The vertices are congruent modulo $\frac{(1-\rho)q^2}{\alpha\beta}\mathfrak{O}_L$. We cut this triangle into q^2 smaller, similar triangles, whose vertices are congruent modulo $\frac{(1-\rho)q}{\alpha\beta}\mathfrak{O}_L$.



We number the triangles as shown in the diagram. Thus the path W_0 runs above all triangles in the Diagram. We now construct the path W_1 to run below of the first triangle but above every other triangle



Correspondingly W_2 runs below the first two triangles, and so on.



We choose the paths W_{i-1} and W_i so that they are equal outside the subinterval $[c_i, d_i]$ of I, which is mapped to the boundary of the i^{th} triangle. Thus $W_{i-1}(x) = W_i(x)$ for $x \notin (c_i, d_i)$. We shall choose homotopies $h_i^{ns}(x, t)$ from W_{i-1} to W_i in such a way that they are independent of t for $x \notin (c_i, d_i)$. Thus for $x \notin (c_i, d_i)$.

$$h_i^{ns}(x, t) = W_i(x) = W_{i-1}(x).$$

We now choose by §4.5 h_1^{ns} and h_2^{ns} for x in (c_1, d_1) and (c_2, d_2) such that h_1 and h_2 are admissible. If $i > 2$ then the i^{th} triangle is a translation either of the first or of the second triangle by an element v_i of $\frac{(1-\rho)q}{\alpha\beta}\mathfrak{D}_L$. We can now construct $h_i^{ns}(x, t)$ for $x \in (c_i, d_i)$ as follows:

$$h_i(c_i + (d_i - c_i)x, t) = v_i + \begin{cases} h_1(c_1 + (d_1 - c_1)x, t) \\ h_2(c_2 + (d_2 - c_2)x, t) \end{cases}.$$

We define the non-singular part, h^{ns} of h:

$$h^{ns}(x, t) := h_i^{ns}(x, q^2t - i + 1), \quad \text{for } \frac{i-1}{q^2} \leq t \leq \frac{i}{q^2}.$$

We also define

$$g_T^i(x_1, \ldots, x_{n-1}, t) := v_{\mathcal{F}} + \sum_{j \in T} \left[0, \frac{a_{\mathcal{F},j}}{\alpha\beta}\right]^1(x_j) + \sum_{j \notin T} a_{\mathcal{F},j}\, h_i^{ns}(x_j, t).$$

There is an equivalence in $\mathcal{H}_n(K_\infty, K_\infty \setminus S_{\alpha\beta})$:

$$g_T \simeq \sum_{i=1}^{q^2} g_T^i.$$

(vii) We now consider the functions h_i^{ns} and g_T^i in more detail. We have

$$g_T^i(x_1, \ldots, x_{n-1}, t) = v_{\mathfrak{F}} + \sum_{j \in T} \left[0, \frac{a_{\mathfrak{F},j}}{\alpha\beta}\right]^1 (x_j) + \sum_{j \notin T, x_j \notin (c_i, d_i)} a_{\mathfrak{F},j} W_i(x_j) + \sum_{j \notin T, x_j \in (c_i, d_i)} a_{\mathfrak{F},j} h_i(x_j, t).$$

If T^1 and T^2 are two subsets of $\{1,2,\ldots,n-1\}$, such that T, T^1 and T^2 are pairwise disjoint, then we define

$$l_{T^1,T^2}^i(x_1, \ldots, x_{n-1}, t) = v_{\mathfrak{F}} + \sum_{j \in T} \left[0, \frac{a_{\mathfrak{F},j}}{\alpha\beta}\right]^1 (x_j) + \sum_{j \in T^1} a_{\mathfrak{F},j} W_i(c_i x_j) + \sum_{j \in T^2} a_{\mathfrak{F},j} W_i((1 - d_i)x_j + d_i) + \sum_{j \notin T \cup T^1 \cup T^2} a_{\mathfrak{F},j} h_i(c_i + (d_i - c_i)x_j, t).$$

We then have an equivalence in $\mathcal{H}_n(K_\infty, K_\infty \setminus S_{\alpha\beta})$:

$$g_T^i \simeq \sum_{T^1, T^2 \subset \{1,2,\ldots,n-1\} \setminus T, T^1 \cap T^2 = \emptyset} l_{T^1,T^2}^i.$$

We shall compute the terms of this sum.

(viii) If T^1 is non-empty, then l_{T^1,T^2}^i is a product of $\sigma_1(a_{\mathfrak{F},j}) W_i|_{[0,c_i]}$ with other things. We know however that $\sigma_1(a_{\mathfrak{F},j}) W_i|_{[0,c_i]}$ is a sum of modified line segments, whose lengths are in $\frac{q}{\alpha\beta} L$. Therefore by Remark §5.2,

$$\left\{\left\{\frac{1}{\alpha\beta} L \,\middle|\, \text{These terms}\right\}\right\} \equiv 0 \text{ modulo } q.$$

The terms in which T^2 is non-empty vanish in the same way. We are therefore only interested in the term, for which T^1 and T^2 are empty. First suppose the i^{th} triangle is a translation by v_i of the first triangle. We then have

$$\begin{aligned} l_{\emptyset,\emptyset}^i(x_1, \ldots, x_{n-1}, t) &= v_{\mathfrak{F}} + \sum_{j \in T} \left[0, \frac{a_{\mathfrak{F},j}}{\alpha\beta}\right] (x_j) + \sum_{j \notin T} a_{\mathfrak{F},j} h_i^{ns}(c_i + (d_i - c_i)x_j, t) \\ &= v_{\mathfrak{F}} + \sum_{j \in T} \left[0, \frac{a_{\mathfrak{F},j}}{\alpha\beta}\right] (x_j) + \sum_{j \notin T} a_{\mathfrak{F},j} (v_i + h_1^{ns}(c_1 + (d_1 - c_1)x_j, t)) \\ &= \sum_{j \notin T} a_{\mathfrak{F},j} v_i + l_{\emptyset,\emptyset}^1(x_1, \ldots, x_{n-1}, t). \end{aligned}$$

The $a_{\mathfrak{F},j}$ are in $\frac{1}{1-\rho} L$. Since $v_i \in \frac{(1-\rho)q}{\alpha\beta} \mathfrak{O}_L$, we must have $\sum_{j \notin T} a_{\mathfrak{F},j} v_i \in \frac{q}{\alpha\beta} L$. In particular this translation is in $\frac{1}{\alpha\beta} L$. Therefore

$$\left\{\left\{\frac{1}{\alpha\beta}L \,\middle|\, l^{i}_{\emptyset,\emptyset}\right\}\right\} = \left\{\left\{\frac{1}{\alpha\beta}L \,\middle|\, l^{1}_{\emptyset,\emptyset}\right\}\right\}.$$

Analogously, if the i^{th} triangle is a translation of the second triangle,

$$\left\{\left\{\frac{1}{\alpha\beta}L \,\middle|\, l^{i}_{\emptyset,\emptyset}\right\}\right\} = \left\{\left\{\frac{1}{\alpha\beta}L \,\middle|\, l^{2}_{\emptyset,\emptyset}\right\}\right\}.$$

The number of the triangles which are translation of the first triangle is $\frac{q(q+1)}{2}$

The number of the triangles which are translations of the second triangle is $\frac{q(q-1)}{2}$. We therefore have

$$\left\{\left\{\frac{1}{\alpha\beta}L \,\middle|\, g_T\right\}\right\} \equiv \frac{q(q+1)}{2}\left\{\left\{\frac{1}{\alpha\beta}L \,\middle|\, l^{1}_{\emptyset}\right\}\right\} + \frac{q(q-1)}{2}\left\{\left\{\frac{1}{\alpha\beta}L \,\middle|\, l^{2}_{\emptyset}\right\}\right\}.$$

Since both these numbers are divisible by q, the theorem is proved in the case that q is odd.

(ix) We now consider the case that q is even. The whole proof would be the same, but at the end one doesn't have the result, that $\frac{q(q+1)}{2}$ and $\frac{q(q-1)}{2}$ are divisible by q. Instead we require at the beginning that $\alpha, \beta \equiv 1 \bmod 2(1-\rho)q^2 = 4q^2$. We cut the large triangle into $4q^2$ instead of q^2 pieces. At the end we have for the two numbers $\frac{2q(2q+1)}{2}$ and $\frac{2q(2q-1)}{2}$, which are obviously divisible by q.

5.7. Corollary (Theorem 1)

We now prove the result stated at the beginning of the chapter:

Let $\alpha, \beta \in \mathfrak{O}_L$ with the following conditions:

- *α, β and q are pairwise coprime in $\mathfrak{O}_L$;*
- *$\alpha, \beta \equiv 1 \bmod (1-\rho)q^2$;*
- *α and β are totally positive.*

Then

$$\mathrm{Dec}_L \frac{\alpha}{\beta} = \mathrm{Dec}_L \frac{\beta}{\alpha}.$$

With the help of the Gauss-Schering Lemma (§2.11) and of Lemma §2.9.2 this implies the following:

Let $\alpha, \beta \in \mathfrak{O}$ *with the following conditions*:

- $\alpha, \beta, \mathfrak{b}$ *and* q *are pairwise coprime in* $\mathfrak{O}$;
- $\alpha, \beta \equiv 1 \bmod \mathfrak{b}(1-\rho)q^2$;
- α *and* β *are totally positive.*

Then

$$\left(\frac{\alpha}{\beta}\right)_q = \left(\frac{\beta}{\alpha}\right)_q.$$

Proof. First let α: be close to 1: in $K_\infty^\times$:, and let $\alpha, \beta \equiv 1 \bmod (1-\rho)q^2$ and α and β totally positive. The set $\{b^{-1}\beta' \mid b \in \mathbf{N}$ and $\beta' \in \mathfrak{O}_L, \beta' \equiv 1 \bmod (1-\rho)q^2\}$ is dense in $K_\infty^\times$. Since β is totally positive, it is in the connected component of 1 in $K_\infty^\times$. We can therefore find a β' such that $(\beta'^q\beta)$: is close to 1: and $\beta' \equiv 1 \bmod (1-\rho)q^2$. We have from the previous paragraph

$$\mathrm{Dec}_L \frac{\alpha}{\beta'^q\beta} = \mathrm{Dec}_L \frac{\beta'^q\beta}{\alpha}.$$

By §2.10.1 we have $\mathrm{Dec}_L \dfrac{\alpha}{\beta'^q\beta} = \mathrm{Dec}_L \dfrac{\alpha}{\beta}$, and by §2.10.5, $\mathrm{Dec}_L \dfrac{\beta'^q\beta}{\alpha} = \mathrm{Dec}_L \dfrac{\beta}{\alpha}$. Therefore

$$\mathrm{Dec}_L \frac{\alpha}{\beta} = \mathrm{Dec}_L \frac{\beta}{\alpha}.$$

With the same trick we can remove the condition that α: is close to 1:.

REFERENCES

[1] J. W. S. Cassels, On Kummer Sums, Proc. London Math. Soc, (3), **21** (1970), 19–27.

[2] Ph. Furtwängler, Über die Reziprozitätsgesetz zwischen l ten Potenzreste in algebraischen Zahlkörpern, wenn l eine ungerade Primzahl bedeutet, Math. Annalen, **58**.

[3] ——, Die Reziprozitätsgesetze für Potenzreste mit Primzahlexponenten in algebraischen Zahlkörpern, I, Math. Annalen, **67** (1909), 1–31.

[4] ——, Die Reziprozitätsgesetze für Potenzreste mit Primzahlexponenten in algebraischen Zahlkörpern, II, Math. Annalen, **72** (1912), 346–386.

[5] ——, Die Reziprozitätsgesetze für Potenzreste mit Primzahlexponenten in algebraischen Zahlkörpern, III, Math. Annalen, **74** (1913), 413–429.

[6] C. F. Gauß, Zur Theorie der biquadratischen Reste, Werke, Band **2**, 313–385.

[7] ——, Disquisitiones Arithmeticae, Art. 133, Werke Band **I**, S. 101.

[8] Habicht, Ein elementarer Beweis des kubischen Reziprozitätsgesetzes, Math. Annalen, **139** (1959–60), 343–365.

[9] D. Hilbert, Die Theorie der algebraischen Zahlkörper, Jahresbericht der Deutschen Mathematiker-Vereinigung, Band **4**, (1894–95).

[10] Über die Theorie des relativquadratischen Zahlkörpers, Math. Annalen Bd. **51** (1898), 1–127.
[11] Hiroshi Ito, On a property of elliptic Dedekind sums, J. Number Theory, **27** (1987) 17–21.
[12] ——, Dedekind sums and quadratic residue symbols, Nagoya Math. J., **118** (1990) 35–43.
[13] ——, A note on Dedekind sums, in Number Theory, Proc. 1st Conf. Canadian Number Theory Association, Banff/Alberta (Canada) 1988, (1990), 239–248.
[14] T. Kubota, Geometry of Numbers and Class Field Theory, Japan. J. Math., **13**, No. 2 (1987), 235–275.
[15] ——, Geometric Foundation of Class Field Theory, (in Japanese) Sugaka **44**, 1 (1992), 1–12.
[16] Massey, Singular Homology Theory, Graduate Texts in Mathematics, Springer-Verlag.
[17] C. R. Matthews, Gauss Sums and Elliptic Functions I, The Kummer Sum, Invent. Math., **52** (1979), 163–185.
[18] ——, Gauss Sums and Elliptic Functions II. The Quartic Sum, Invent. Math., **54** (1979), 23–52.
[19] Schering, Verallgemeinerung des Gaußischen Criterium für den quadratischen Rest-charakter einer Zahl in Bezug auf eine andere, Werke Band I, 285–286.
[20] Rademacher und Grosswald, Dedekind sums, Carus Mathematical Monographs, No 16, Mathematical Assoc. America, Washington D. C., (1972).
[21] Szech, Dedekindsummen mit elliptischen Funktionen, Invent. Math., **76** (1984), 523–551.
[22] ——, Dedekind sums and power residue symbols, Compositio. Math., **59** (1986), 89–112.
[23] ——, Theta functions on the hyperbolic three space, Kokyuroku RIMS, Kyoto Univ., No. **603** (1987), 9–20.
[24] A. Weil, Basic Number Theory, Grundlehren der Math. Wissenschaften in Einzeldarstellung Band **144**, Springer-Verlag (1967).

Mathematisches Institut der Georg August Universität,
Göttingen

Current address
Max-Planck-Institut für Mathematik
Gottfried-Claren-Straße 26
53225 Bonn
Germany