A CLASSICAL APPROACH TO RELATIVE QUADRATIC EXTENSIONS

HATİCE BOYLAN AND NILS-PETER SKORUPPA

Abstract.

Needs still fine tuning

We show that we can develop a theory of relative quadratic extensions of a given number field K in the classical language which is as explicit and easy as for the well-known case that K is the field of rational numbers. As an application we prove a reciprocity law which expresses the number of solutions of a given quadratic equation modulo an integral ideal $\mathfrak{a}$ of K in terms of $\mathfrak{a}$ modulo the discriminant of the equation. .

Contents

1. Introduction

If L is a quadratic extension of $\mathbb{Q}$ we can pick any integral quadratic irrationality a in L, set $\Delta := \mathrm{tr}(a) - 4\,\mathrm{n}(a)$ and read off all important arithmetic properties

2010 *Mathematics Subject Classification.* 11R11 (primary) and 11R29, 11S99 (secondary) .

Key words and phrases. Algebraic Number Theory, Relative Quadratic Extensions, Quadratic Congruences in Number Fields, Discriminants of Relative Quadratic Extensions .

Edit

This work was supported by Scientific Research Projects Coordination Unit (BAP) of Istanbul University with project number IRP-39310. During the preparation of part of this article the first author was supported by the Max-Planck Institut für Mathematik, Bonn.

.

from the rational integer Δ: We have $L = \mathbb{Q}(\sqrt{\Delta})$, the integer Δ is a square modulo 4, and if we divide out the largest perfect square f^2 such that $\Delta_0 := \Delta/f^2$ is still a square modulo 4 then Δ_0 is the discriminant of L, which carries all information about the ramification of rational primes. The application which associates to a rational prime p the Legendre symbol $\left(\frac{\Delta}{p}\right)$ extends to a character modulo Δ. It factors through the primitive Dirichlet character $\left(\frac{\Delta_0}{*}\right)$. The Dedekind zeta functions $\zeta_L(s)$ and $\zeta_{\mathbb{Q}}(s) = \zeta(s)$ of L and $\mathbb{Q}$ are related by the identity $\zeta_L(s) = \zeta(s)L(\left(\frac{\Delta_0}{*}\right), s)$, where $L(\left(\frac{\Delta_0}{*}\right), s) = \sum_{n\geq 1}\left(\frac{\Delta_0}{n}\right)n^{-s}$, and this identity encodes the information of the splitting of the rational primes in L.

These facts are well-known since the beginning of algebraic number theory in the 19th century, and the explicit character of this theory is helpful in many applications. In contrast to this one does not find such an easy and smooth description of the arithmetic theory of relative quadratic extensions. On finds some hints towards such a theory in Hecke's "Vorlesungen Über die Theorie der Algebraischen Zahlen" [Hec23, §39] and, in particular its last section [Hec23, §63], which, however, is not as completely developed as in the case of extensions of $\mathbb{Q}$. In the modern treatment of algebraic number theory relative quadratic extensions are subsumed under the more abstract class field theory, which provides a conceptual background for the arithmetic of general abelian extensions but lacks often explicitness even in simpler subclasses of abelian extensions.

In this letter we show that in fact the described facts for quadratic extensions of $\mathbb{Q}$ remain true and are as easy and explicit for relative quadratic extensions if one extends correctly the notions of *discriminants* and *fundamental discriminants* to arbitrary number fields. In the second part of this note we apply our theory to derive a reciprocity law which expresses the number of solutions of a quadratic equation modulo a given integral ideal in terms of the "residue class" of the ideal modulo the discriminant of the equation (see Theorem 6).

2. Discriminants and relative quadratic extensions

2.1. **Discriminants in a number field.** For this section we fix a number field K with ring of integers $\mathfrak{o}$. Let L be a quadratic extension of K. We can obtain L by adjoining the square root $\Delta = \mathrm{tr}_{L/K}(a)^2 - 4\,\mathrm{n}_{L/K}(a)$ to K, where a is any integer in L not in K. Note that Δ is a square modulo 4 (not necessarily relatively prime to 2)[1]. For obtaining the quadratic extensions of K it suffices therefore to adjoin square roots of integers Δ in K which are squares modulo 4.

We shall call the nonzero integers Δ of K which are squares modulo 4 henceforth *discriminants in* K. For a discriminant Δ in K we let $\mathfrak{f}_\Delta$ be the largest integral ideal in K whose square divides Δ and such that

$$\Delta \equiv x^2 \bmod 4\mathfrak{f}_\Delta^2$$

for some integer x in K. We partition the discriminants of K into classes, where Δ_1 and Δ_2 belong to the same class if and only if $K\left(\sqrt{\Delta_1}\right) = K\left(\sqrt{\Delta_2}\right)$. If Δ is not a square in K then the class of Δ coincides with the set of all nonzero $\mathrm{tr}_{L/K}(a)^2 - 4\,\mathrm{n}_{L/K}(a)$, where a runs through the integers of $L = K\left(\sqrt{\Delta}\right)$. It is also clear that a class of discriminants coincides with the set of discriminants in a class of $K^\times/K^{\times 2}$.

2.2. **The discriminant of a relative quadratic extension.** For an extension L of K, we use $D_{L/K}$ for the discriminant of the relative extension L/K; recall that this is an integral ideal of K. It is a basic fact that $D_{L/K}$ divides the gcd of all

[1] primary

numbers $\mathrm{tr}_{L/K}(a)^2 - 4\,\mathrm{n}_{L/K}(a)$ $(a \in L)$, i.e. the gcd of all numbers in the class $\mathcal{D}$ of Δ.For relative quadratic extensions the discriminant can be easily described.

Theorem 1. *For any given integer Δ in $K^\times$ (not necessarily a square mod 4), let $\mathfrak{s}$ be the largest integral ideal whose square divides Δ, and let $\mathfrak{t}$ be the largest integral ideal dividing 2 such that Δ is a square mod $(\mathfrak{st})^2$. Then*

$$D_{K(\sqrt{\Delta})/K} = 4\Delta/(\mathfrak{st})^2. \tag{1}$$

In particular, if Δ is a discriminant in K, then one has

$$D_{K(\sqrt{\Delta})/K} = \Delta/\mathfrak{f}_\Delta^2. \tag{2}$$

Proof. If Δ is a square in K both sides of (1) are equal to the unit ideal. We can therefore assume that Δ is not a square, so that L is a quadratic extension of K with, say ring of integers $\mathfrak{O}$. Let $\mathfrak{p}$ be a prime ideal of K, and let $\mathfrak{o}_\mathfrak{p}$ be the localization of $\mathfrak{o}$ at $\mathfrak{p}$. Then

$$D_{L/K}\mathfrak{o}_\mathfrak{p} = \det\begin{pmatrix}1 & \omega\\ 1 & \omega'\end{pmatrix}^2 \mathfrak{o}_\mathfrak{p} = 4(\omega-\omega')^2\mathfrak{o}_\mathfrak{p},$$

where $1, \omega$ is an $\mathfrak{o}_\mathfrak{p}$-basis of $\mathfrak{O}\mathfrak{o}_\mathfrak{p}$, and where ω' is the Galois conjugate of ω in the extension L/K (see e.g. [Frö67, §3, Prop. 4]). The ring $\mathfrak{O}\mathfrak{o}_\mathfrak{p}$ is the algebraic closure of $\mathfrak{o}_\mathfrak{p}$ in L (see e.g. [Frö67, §4, Lemma 4]), i.e.

$$\mathfrak{O}\mathfrak{o}_\mathfrak{p} = \left\{a + b\sqrt{\Delta_1} : a \in \tfrac{1}{2}\mathfrak{o}_\mathfrak{p},\ b \in K,\ a^2 - b^2\Delta_1 \in \mathfrak{o}_\mathfrak{p}\right\}.$$

Here we set $\Delta_1 = \Delta/\pi^{2\lfloor l/2\rfloor}$, where $\mathfrak{p}^l$ is the exact power dividing Δ, and where π is an element of $\mathfrak{o}_\mathfrak{p}$ such that $\mathfrak{o}_\mathfrak{p}\mathfrak{p} = \pi\mathfrak{o}_\mathfrak{p}$. It is quickly verified that we can take $\omega = \sqrt{\Delta_1}$ if $\mathfrak{p}$ is odd, and also if $\mathfrak{p} \mid 2$ and Δ_1 is divisible by $\mathfrak{p}$. Otherwise one can take $\omega = (c + \sqrt{\Delta_1})/\pi^{s_\mathfrak{p}}$, where c is any solution of $\Delta_1 \equiv c^2 \bmod \mathfrak{p}^{2s_\mathfrak{p}}$. In other words,

$$4(\omega-\omega')^2 = \begin{cases} 4\Delta_1/\pi^{2s} & \text{if } \mathfrak{p} \mid 2 \text{ and } l \text{ is even,}\\ 4\Delta_1 & \text{otherwise.}\end{cases}$$

The formula (1) becomes now obvious.

Assume that Δ is a square mod 4. Then $\mathfrak{f} := \mathfrak{st}/2$ is integral. Indeed, let $\mathfrak{p}$ be a prime above 2. If $v_\mathfrak{p}(\Delta)$ is odd then $v_\mathfrak{p}(\Delta) > v_\mathfrak{p}(4)$, hence $v_\mathfrak{p}(\mathfrak{n}^2) \geq v_\mathfrak{p}(4)$ since Δ is a square mod 4. If $v_\mathfrak{p}(\Delta)$ is even, then $v_\mathfrak{p}\left((\mathfrak{st})^2\right) = v_\mathfrak{p}(\Delta\mathfrak{s}^2) \geq v_\mathfrak{p}(4)$ again since Δ is a square mod 4. Clearly $\mathfrak{f}^2$ divides Δ (since $(\mathfrak{st})^2$ divides 4Δ). Moreover, Δ is a square mod $4\mathfrak{f}^2 = (\mathfrak{st})^2$. From the definition of $\mathfrak{s}$ and $\mathfrak{t}$ it is also clear that there is no prime ideal $\mathfrak{p}$ such that the square of $\mathfrak{f}' := \mathfrak{fp}$ divides Δ and Δ is a square mod $4\mathfrak{f}'^2$. It follows $\mathfrak{f} = \mathfrak{f}_\Delta$. □

We note two corollaries.

Corollary 1. *The discriminant of a relative quadratic extension represents a square in the class group.*

Indeed, the square of the class of $D_{K(\sqrt{\Delta})/K}$ equals the square of the ideal class of $\mathfrak{f}_\Delta$. The corollary is due to Hecke [Hec23, §63, Satz 177], who proved it in fact for arbitrary (not necessarily quadratic) relative extensions.

For the $\mathfrak{f}_\Delta$ we find the following.

Corollary 2. *The $\mathfrak{f}_\Delta$, for Δ in a given class of $K^\times/{K^\times}^2$ belong all to one and the same ideal class of K.*

Proof. If Δ and Δ' are in the same class of $K^\times/{K^\times}^2$, then, using (2), we find $\mathfrak{f}_\Delta^2 = a^2\mathfrak{f}_{\Delta'}$ for some a in $K^\times$, which implies $\mathfrak{f}_\Delta = a\mathfrak{f}_{\Delta'}$. However, one can prove the corollary also more directly as follows. If a is a nonzero integer in K then $\mathfrak{f}_{a^2\Delta} = a\mathfrak{f}_\Delta$ (since $a\Delta$ is divisible by the square of $a\mathfrak{f}_\Delta$ a square modulo $4a^2\mathfrak{f}_\Delta^2$, and on the other hand $\mathfrak{f}_{a^2\Delta}$ can obviously not larger than $a\mathfrak{f}_\Delta$). Therefore, if Δ_i $(i = 1, 2)$ are in the same class, i.e. if $a_1^2\Delta_1 = a_2^2\Delta_2$ for integers a_i, we conclude that $a_1\mathfrak{f}_{\Delta_1} = a_2\mathfrak{f}_{\Delta_2}$. □

In fact, one can say more about the $\mathfrak{f}_\Delta$. The ring of integers $\mathfrak{O}$ of $K(\sqrt{\Delta})$, being in general not free as module over $\mathfrak{o}$, can be written as $\mathfrak{O} = \mathfrak{g}a \oplus \mathfrak{o}b$ with a suitable fractional ideal $\mathfrak{g}$ and a, b in $\mathfrak{O}$ if Δ is not a square(and otherwise as $\mathfrak{O} = \mathfrak{o} = \mathfrak{g}a$). The ideal $\mathfrak{g}$ is not unique, but its ideal class is, which is called the *Steinitz invariant of the $\mathfrak{o}$-module $\mathfrak{O}$* [?, Thm. 13].

Proposition 1. *The $\mathfrak{f}_\Delta^{-1}$, for Δ in a given class of $K^\times/{K^\times}^2$ belong to the Steinitz invariant of the ring of integers of $K(\sqrt{\Delta})$ as module over $\mathfrak{o}$.*

Proof. The case that Δ is a square being trivial we assume that $L = K(\sqrt{\Delta})$ has degree two over K. For a prime ideal $\mathfrak{p}$ of K we have $\mathfrak{O}\mathfrak{o}_\mathfrak{p} = \mathfrak{g}\mathfrak{o}_\mathfrak{p}a + \mathfrak{o}_\mathfrak{p}b$, and as in the proof of Theorem 1 we find therefore $D_{L/K}\mathfrak{o}\mathfrak{p} = \pi^{2g}(ab' - a'b)^2$, where $\pi\mathfrak{o}_\mathfrak{p} = \mathfrak{p}\mathfrak{o}_\mathfrak{p}$, and $\mathfrak{g}\mathfrak{o}_\mathfrak{p} = \pi^{2g}\mathfrak{o}_\mathfrak{p}$. It follows $D_{L/K} = \mathfrak{g}^2(ab' - a'b)^2$. On the other hand $D_{L/K} = \Delta/\mathfrak{f}_\Delta$, and hence $(\mathfrak{g}/\mathfrak{f}_\Delta)^2 = \Delta/(ab' - a'b)^2$. But $\Delta/(ab' - a'b)^2$ is a square in $K^\times$ (since $ab' - a'b$, being not invariant under the Galois group of L/K, is in L but not in K), and hence $\mathfrak{g}/\mathfrak{f}_\Delta$ is a principal ideal. This proves the proposition. □

2.3. **Fundamental discriminants.** There is still a dichotomy left since the notion "Fundamental discriminant" is missing for general relative quadratic extensions. More precisely, we would like to have, for a given class C in $K^\times/{K^\times}^2$, a discriminant Δ_0 such that $\Delta_0 f^2$ runs through all discriminants in the given class when f runs through all nonzero integers of K. Such a Δ_0 would be uniquely determined by this property modulo ${\mathfrak{o}^\times}^2$, and it would generate the discriminant ideal $D_{L/K}$ of the quadratic extension of K determined by C.

Such a Δ_0 will not in general exist. In fact, it is easy to see that it exists if and only if the ideal class of the $\mathfrak{f}_\Delta$ (Δ in C) is trivial (see Theorem 2). However, such a Δ_0 exists for any class C as an idèle of K, and it is useful to study this construction since it will give us, amongst others, further criteria for the existence of fundamental discriminant for classes in $K^\times/{K^\times}^2$.

For a valuation v of K let K_v denote the completion of K at v, and $\mathfrak{o}_v$ the ring of integers in K_v (with the convention $\mathfrak{o}_v = K_v$ if v is real or complex). We use I for the idèle group of K, and U for the direct product over all $\mathfrak{o}_v^\times$. Finally we identify K with its image in I under the diagonal embedding.

Let C be a class in $K^\times/{K^\times}^2$. Let $D_C U^2$ be the element of $K^\times I^2/U^2$ which at a finite place v is defined as

$$(D_C)_v = \Delta/\pi_v^{2v(\mathfrak{f}_\Delta)}, \tag{3}$$

and otherwise as $(D_C)_v = \Delta$. Here π_v is a prime element of K_v (and therefore unique up to multiplication by a unit in $\mathfrak{o}_v^\times$), and Δ is an element of C. Note that the coset $(D_C)_v{\mathfrak{o}_v^\times}^2$ does not depend on the choice of π.

Lemma 1. *The coset $D_C U^2$ does not depend on the choice of Δ in C.*

Proof. We have $D_C = \Delta/\varphi^2$, where φ is the ideal associated to $\mathfrak{f}_\Delta$, i.e. $\varphi_v = \pi_v^{v(\mathfrak{f}_\Delta)}$. If Δ' is another discriminant in C, then (2) implies $\Delta/\varphi^2 = \varepsilon\Delta'/\varphi'^2$, where φ' is the idèle associated to $\mathfrak{f}_{\Delta'}$ and ε is in U. Since Δ and Δ' differ by a square we conclude that ε is in fact in U^2, which proves the lemma. □

We call any representative D_C of $D_C U^2$ (by slight abuse of language) the *fundamental discriminant of* C. This is justified by the following proposition.

Proposition 2. *Let C be a class in $K^\times/{K^\times}^2$ and D_C its fundamental discriminant.*

(1) *Every discriminant Δ in C can be written uniquely mod U^2 as $\Delta = D_C\alpha^2$ with an ideal α whose valuation at a finite place is non-negative.*
(2) *D_C is mapped onto $D_{K(\sqrt{\Delta})/K}$ under the natural map which takes I/U^2 onto the group of fractional ideals[2] of K.*
(3) *$(D_C)_v$ is a square mod $4\mathfrak{o}_v$ at every finite place of K,*
(4) *For every real place the sign of $(D_C)_v$ equals the sign of $\sigma(\Delta)$, with the embedding σ of K corresponding to v.*

Proof. (1), (3) and (4) are immediate consequences of the definition (3) of D_C, and (2) follows from (3) and (2). □

Our D_C coincides with the enhanced notion of relative discriminant for arbitrary extensions as proposed in [Frö60], whose definition is, however, different from ours.

We call D_C *principal* if it is represented by a number in $K^\times$, i.e. if $D_C U^2 = \Delta_0 U^2$ for some number Δ_0. This number is then a discriminant in C (by (3) of the preceding proposition). Moreover, if D_C is principal, say represented by Δ_0, then $\Delta_0 a^2$ runs through all discriminants in C when a runs through the nonzero integers of K. (Namely, if Δ is a discriminant in C then $\Delta/\Delta_0 = \alpha^2$ for some α in I as in (1), and on the other hand Δ/Δ_0 is in ${K^\times}^2$, so that α is in fact in $\mathfrak{o}$.)

Theorem 2. *Let C be a class in $K^\times/{K^\times}^2$, let D_C denote its fundamental discriminant, and let Δ in C. Then the following statements are equivalent:*

(1) *D_C is principal.*
(2) *The ideal $\mathfrak{f}_\Delta$ is principal.*
(3) *The ring of integers of $K(\sqrt{\Delta})$ is a free module over $\mathfrak{o}$.*

Proof. (1) implies $\Delta = D_C a^2$ for some integer a in K. Since $D_C\mathfrak{o} = D_{K(\sqrt{\Delta})/K}$ (by Prop. 2 (2)) and $\Delta = D_{K(\sqrt{\Delta})/K}\mathfrak{f}_\Delta$ we conclude $\mathfrak{f}_\Delta = a\mathfrak{o}$. Vice versa, if $\mathfrak{f}_\Delta = a\mathfrak{o}$ for some integer a, then $\Delta/a^2{\mathfrak{o}_v^\times}^2 = D_C U^2$ for every v. (2) and (3) are equivalent since by Proposition 1 the ring of integers of $K(\sqrt{\Delta})$ is isomorphic as $\mathfrak{o}$-module to $\mathfrak{f}_\Delta^{-1} \oplus \mathfrak{o}$. □

As for the case that K is the field of rational numbers the fundamental discriminant D_C uniquely determines C and hence the extension $K(\sqrt{\Delta})$.

Theorem 3. *The map $C \to D_C U^2$ defines an injection $K^\times/{K^\times}^2 \to I^2K^\times/U^2$.*

Proof. This is trivial since the set of discriminants in C equals the set of principal idèles of the form $D_C\alpha^2$, where α runs through the idèles with non-negative valuation at every finite place. □

Idea: rewrite this subsection

We can avoid idèles (and hence fulfill better the promise "classical" in the title) by using

$$K^\times I^2/U^2 \cong K^\times/{K^\times}^2 \times I^2/U^2$$

and identifying I^2/U^2 with "something" derived from the group of fractional ideals of K. (Have still to think about ...)

[2] This is the map which takes an αU^2 to the product of all $\mathfrak{p}^{v(\alpha_v)}$, where $\mathfrak{p}$ runs through the prime ideals of K and v is the place corresponding to $\mathfrak{p}$.

2.4. **The Größencharakter of a relative quadratic extension.** We extend the Dirichlet characters $\left(\frac{\Delta}{*}\right)$ from the theory where K is the field of rational numbers to arbitrary number fields K as follows: Let Δ be a discriminant of K. For a prime ideal $\mathfrak{p} \nmid \Delta$, we set $\left(\frac{\Delta}{\mathfrak{p}}\right) = +1$ or $= -1$ accordingly as Δ is a square modulo $4\mathfrak{p}$ or not. Of course, for $\mathfrak{p} \nmid 2$ the number Δ is a square modulo $4\mathfrak{p}$ if and only if it is square modulo $\mathfrak{p}$ as follows from the Chinese remainder theorem. We continue $\left(\frac{\Delta}{*}\right)$ to a homomorphism of the group of fractional ideals relatively prime[3] to Δ onto the group $\{\pm 1\}$.

Theorem 4. *The homomorphism $\left(\frac{\Delta}{*}\right)$ defines a Größencharakter modulo Δ of infinity type $\alpha \mapsto \prod_{\sigma\in M} \operatorname{sign}\sigma(\alpha)$, where M is the set of real embeddings of K with $\sigma(\Delta) < 0$. Its conductor equals $\Delta/\mathfrak{f}_\Delta^2$.*

We postpone the proof to the end of this section.

According to the theorem the character $\left(\frac{\Delta}{*}\right)$ is the restriction of a primitive Größencharakter modulo $\Delta/\mathfrak{f}_\Delta^2$, which we denote in the sequel by $\left(\frac{\Delta}{*}\right)_0$. Note that $\left(\frac{\Delta}{*}\right)_0$ is uniquely determined by $\left(\frac{\Delta}{*}\right)$. Indeed, if the fractional ideal $\mathfrak{a}$ is relatively prime to $\mathfrak{D} := \Delta/\mathfrak{f}_\Delta^2$, then we can find an a in $K^\times$ relatively prime to $\mathfrak{D}$ and such that $\mathfrak{b} := \mathfrak{a}a$ is relatively prime to Δ. But then $\left(\frac{\Delta}{\mathfrak{a}}\right)_0 = \left(\frac{\Delta}{\mathfrak{b}}\right)\left(\frac{\Delta}{a\mathfrak{o}}\right)_0$, and $\left(\frac{\Delta}{a\mathfrak{o}}\right)_0 \prod_{\sigma\in M} \operatorname{sign}\sigma(a)$ depends only on a modulo $\mathfrak{D}\mathfrak{o}_\mathfrak{D}$ (where $\mathfrak{o}_\mathfrak{D}$ is the intersection of the localizations $\mathfrak{o}_\mathfrak{p}$ of $\mathfrak{o}$ at $\mathfrak{p}$ ($\mathfrak{p} \mid \mathfrak{D}$)), and hence can be evaluated by replacing a by any b in $a + \mathfrak{D}\mathfrak{o}_\mathfrak{D}$ which is relatively prime to Δ.

Proposition 3. *The primitive Größencharakter $\left(\frac{\Delta}{*}\right)_0$ depends only on the class of Δ in $K^\times/{K^\times}^2$.*

Proof. Let Δ' be another discriminant in the same class as Δ. Then $\Delta a^2 = \Delta' a'^2$ with suitable nonzero integers a and a'. Let $\Delta'' = \Delta a'^2 = \Delta' a^2$. It suffices to show that $\left(\frac{\Delta''}{*}\right)_0 = \left(\frac{\Delta}{*}\right)_0$ and $\left(\frac{\Delta''}{*}\right)_0 = \left(\frac{\Delta'}{*}\right)_0$. But this is clear since $\left(\frac{\Delta''}{*}\right)$ is the restriction of $\left(\frac{\Delta}{*}\right)$ and of $\left(\frac{\Delta'}{*}\right)$ to the group of fractional ideals relatively prime to Δ''. □

2.5. **The decomposition of primes in relative quadratic extensions.** Let

$$L\left(\left(\frac{\Delta}{*}\right)_0, s\right) = \sum_{\mathfrak{a}} \left(\frac{\Delta}{\mathfrak{a}}\right)_0 \mathrm{n}(\mathfrak{a})^{-s},$$

where the sum runs over all integral ideals of K with the convention that $\left(\frac{\Delta}{\mathfrak{a}}\right)_0 = 0$ if $\mathfrak{a}$ is not relatively prime to conductor of $\left(\frac{\Delta}{*}\right)_0$.

Theorem 5. *If Δ is not a square in K, then*

$$\zeta_{K(\sqrt{\Delta})}(s) = \zeta_K(s) L\left(\left(\frac{\Delta}{*}\right)_0, s\right)$$

Proof. It is a basic fact [Hec23, Satz 117] that every prime ideal $\mathfrak{p}$ of K is inert (i.e. remains a prime in L), or splits (i.e. factors into a product of two different primes), or ramifies (i.e. is the square of a prime ideal in L). Moreover, which property holds true is given by the *character criterion*, namely, the first, second or third property holds true accordingly as $\left(\frac{\Delta}{\mathfrak{p}}\right)_0$ equals -1, $+1$ or 0. For $\mathfrak{p} \nmid \Delta$ the character criterion is [Hec23, Satz 118, 119] (for applying Satz 119 loc.cit. recall that $\left(\frac{\Delta}{\mathfrak{p}}\right)$ equals $+1$ or -1 according as Δ is a square mod $4\mathfrak{p}$, and that Δ is a square mod 4). But then the criterion is also true for any $\mathfrak{p} \nmid D_{L/K} = \Delta/\mathfrak{f}_\Delta^2$: If $\mathfrak{p} \mid \Delta$, but $\mathfrak{p} \nmid \Delta/\mathfrak{f}_\Delta^2$, we can find a discriminant Δ' in $\Delta {K^\times}^2$ with $\mathfrak{p} \nmid \Delta'$ and

[3] A fractional ideal is called *relatively prime* to Δ is it is of the form $\mathfrak{a}/\mathfrak{b}$ with integral ideals $\mathfrak{a}$ and $\mathfrak{b}$ both of which have no prime ideal common with Δ.

apply Satz 118, 119 loc.cit. to Δ'. Indeed, choose an integral ideal $\mathfrak{b}$ in the class of $\mathfrak{f}_\Delta$ relatively prime to $2\mathfrak{f}_\Delta$, let $a = \mathfrak{b}\mathfrak{f}_\Delta$, and set $\Delta' = \Delta a^2$.

If $\mathfrak{p} \mid \Delta/\mathfrak{f}_\Delta^2$, i.e. if $\left(\frac{\Delta}{\mathfrak{p}}\right)_0 = 0$, then $\mathfrak{p}$ is ramified according to Satz 118 loc.cit. if the exact $\mathfrak{p}$-power dividing $\Delta/\mathfrak{f}_\Delta^2$ is $\mathfrak{p}^f$ with odd f (which is always the case for $\mathfrak{p} \nmid 2$). If f is even and $\mathfrak{p} \mid 2$ the ideal $\mathfrak{p}$ ramifies in L by Satz 119 loc.cit. (for applying Satz 119 we write $L = K(\sqrt{d})$ with some integer d in $\Delta K^{\times 2}$ which is not divisible by $\mathfrak{p}$ and observe that d cannot be a square modulo 4 since otherwise $\Delta/\mathfrak{f}_\Delta^2 = d/\mathfrak{f}_d^2$, contradicting $\mathfrak{p} \nmid d$; one can choose $d = \Delta a^2$ with $a = \mathfrak{b}/\mathfrak{f}_\Delta \mathfrak{p}^{f/2}$ and $\mathfrak{b}$ relatively prime to $\mathfrak{p}$).

The claimed identity is now an easy consequence of the character criterion by comparing, for each prime ideal $\mathfrak{p}$ of K, the $\mathfrak{p}$th Euler factors on both sides of the claimed identity. □

If the conductor of $\left(\frac{\Delta}{*}\right)_0$ is 1 no prime ideal ramifies and vice versa. In other words, we have

Corollary 3. *The extension $K(\sqrt{\Delta})$ is unramified if and only if $\Delta = \mathfrak{f}_\Delta^2$.*

2.6. **Proof of Theorem 4.** It remains to prove Theorem 4. The educated reader might have noticed that $\left(\frac{\Delta}{*}\right)_0$ is essentially nothing else than the Artin reciprocity map associated to $K(\sqrt{\Delta})$.

Indeed, let Δ be a discriminant not a square, let $L = K(\sqrt{\Delta})$, let $\mathfrak{O}$ be the ring of integers of L and let σ be the nontrivial Galois substitution of L/K, which maps $\sqrt{\Delta}$ to $-\sqrt{\Delta}$. As we saw in the proof of Theorem 5, any prime ideal $\mathfrak{p}$ of K relatively prime to $D_{K(\sqrt{\Delta})/K}$ with $\left(\frac{\Delta}{\mathfrak{p}}\right) = 1$ factors in L in the form $\mathfrak{p}\mathfrak{O} = \mathfrak{P}\sigma(\mathfrak{P})$ with $\mathfrak{P} \neq \sigma(\mathfrak{P})$. The *Frobenius* $F_\mathfrak{p}$ (i.e. the generator of the subgroup of $\mathrm{Gal}(L/K)$ mapping each prime ideal of L over $\mathfrak{p}$ to itself) is therefore the identity. On the other hand, if $\left(\frac{\Delta}{\mathfrak{p}}\right) = -1$, then $\mathfrak{p}\mathfrak{O}$ is the only prime ideal in L over $\mathfrak{p}$, and hence $F_\mathfrak{p} = \sigma$. Therefore, if f denotes the isomorphism of $\{\pm 1\}$ with $\mathrm{Gal}(L/K)$, then $f \circ \left(\frac{\Delta}{*}\right)$ equals the Artin reciprocity map $\left(\frac{L/K}{\mathfrak{p}}\right)$ on the group of fractional ideals relatively prime to Δ, which maps a prime ideal $\mathfrak{p}$ to $F_\mathfrak{p}$. The fact that $\left(\frac{\Delta}{*}\right)$ is a Größencharakter follows then from well-known facts of Global Classfield theory, which include also that the discriminant $D_{L/K}$ is the conductor of $\left(\frac{\Delta}{*}\right)$ [**?**, Ch. VI §4.4].

However, we prefer to keep with the explicit character of this note and to give a more direct and elementary proof. We shall need the product formula for the quadratic Hilbert symbols though, which however can be proved without developing full Classfield Theory (see e.g. [O'M00, Ch. 7]).

Proof of Theorem 4. For a nonzero a in $K^\times$ relatively prime to Δ, set

$$\psi(a) := \left(\frac{\Delta}{a\mathfrak{o}}\right) \prod_{\sigma \in M} \operatorname{sign} \sigma(a).$$

Note that ψ defines a linear character of the multiplicative group $K_\Delta^\times$ of elements in $K^\times$ relatively prime to Δ. That $\left(\frac{\Delta}{*}\right)$ is a Größencharakter mod Δ means that ψ factors through a homomorphism of $(\mathfrak{o}/\Delta\mathfrak{o})^\times$, i.e. that ψ is trivial on the kernel of the natural map $K_\Delta^\times \to (\mathfrak{o}/\Delta\mathfrak{o})^\times$ (which sends a to $a' + \Delta\mathfrak{o}$, where a' is any element in $\mathfrak{o}$ such that $a' \equiv a \bmod \Delta K_\Delta$, and where K_Δ is the ring of elements in K relatively prime to Δ). For this it suffices to show that, for integral a, the value $\psi(a)$ depends only on the residue class of a modulo Δ (as one sees on writing any a in the kernel of the natural map in the form $a = \gamma/\delta$ with integers $\gamma \equiv \delta \bmod \Delta$ and $(\delta, \Delta) = 1$.)

So, let a be integral and relatively prime to Δ. For the proof that $\psi(a)$ depends only on a modulo Δ, we use the product formula (see e.g. [Neu99, Ch. VI, Thm. (8.1)] or [O'M00, 71:18 Thm.])

$$\prod_v (\Delta, a)_v = 1, \tag{4}$$

where v runs through all places of K (including the infinite ones) and $(\_,\_)_v$ denote the quadratic Hilbert symbol of the completion K_v of K. Thus, for a, b in K_v, we have $(a,b)_v = +1$ if $ax^2 + by^2 = 1$ has a solution x, y in K_v and $(a,b)_v = -1$, otherwise.

If v is infinite, corresponding to the embedding σ of K into $\mathbb{C}$, then obviously $(\Delta, a)_v = -1$ if and only if σ is real and $\sigma(\Delta)$ and $\sigma(a)$ are both negative. In other words, the contribution to the left hand side of (4) of the infinite places equals $\prod_{\sigma\in M} \operatorname{sign}\sigma(a)$. If v is a finite place corresponding to a prime ideal $\mathfrak{p}$ not dividing 2, then $(\Delta, a)_v = 1$, or $\left(\frac{\Delta}{\mathfrak{p}}\right)^{v(a)}$, or $\left(\frac{a}{\mathfrak{p}}\right)^{v(\Delta)}$ according as $\mathfrak{p} \nmid \Delta$, or $\mathfrak{p} \mid a$, or $\mathfrak{p} \mid \Delta$ (as follows e.g. from [Neu99, Ch. V, Prop. (3.4)] or [O'M00, p. 165, 63:11a]). Therefore the product formula (4) becomes

$$\left(\frac{\Delta}{\mathfrak{a}}\right)\left(\frac{a}{\mathfrak{D}}\right) \prod_{\sigma\in M} \operatorname{sign}\sigma(a) \prod_{v\mid 2} (\Delta, a)_v = 1,$$

where $\mathfrak{D}$ is the odd part of Δ (i.e. the product of all prime ideal powers dividing Δ and relatively prime to 2), and $\mathfrak{a}$ is the odd part of a. In other words

$$\psi(a) = \left(\frac{\Delta}{a/\mathfrak{a}}\right)\left(\frac{a}{\mathfrak{D}}\right) \prod_{v\mid 2} (\Delta, a)_v = \left(\frac{a}{\mathfrak{D}}\right) \prod_{v\mid 2} \left(\frac{\Delta}{\mathfrak{p}_v^{v(a)}}\right) (\Delta, a)_v \,,$$

where $\mathfrak{p}_v$ is the prime ideal corresponding to v. If $v(\Delta) = 0$ the vth factor on the right equals 1 (see [Ser79, Ch.XV,§3,Prop. 6]).

Finally, let $v \mid 2$ and $l := v(\Delta) \geq 1$ (and hence $v(a) = 0$). We need to prove that the quadratic character of $U := \mathfrak{o}_v^\times$ defined by

$$\kappa : a \mapsto (\Delta, a)_v$$

factors through a Dirichlet character modulo $\mathfrak{p}_v^l$. Since the natural map $\mathfrak{o}_v^\times \to \left(\mathfrak{o}/\mathfrak{p}_v^l\right)^\times$ is surjective and has kernel $U_l := 1 + \mathfrak{p}_v^l \mathfrak{o}_v$ the character κ factors through a Dirichlet character mod $\mathfrak{p}_v^l$ if and only if κ is trivial on U_l.

Since $U_{2e+1} \subseteq U^2$, where $e = v(2)$, i.e. by the Local Square Theorem (see Section 4), κ is in any case a Dirichlet character mod $\mathfrak{p}_v^{2e+1}$. Hence we can assume that $l \leq 2e$. But then l is even (since Δ is a square mod 4). Let π_v a uniformizer of K_v and write $\Delta = \pi_v^l b$. By assumption b is a square modulo $\mathfrak{p}_v^{2e-l}$, i.e. $b/c^2 \equiv 1 \bmod \mathfrak{p}_v^{2e-l}$. In other words, $\Delta = \pi_v^l c^2 d$, where d is in U_{2e-l}, with the convention $U_0 = U$ for the case $l = 2e$. It follows that $\kappa(a) = (d, a)_v$. It remains therefore to show that, for any even integers $i, j \geq 0$ with $i + j = 2e$, one has $(U_i, U_j)_v = 1$. Though this seems to be known we did not find any reference for this which does not use Local Class Field Theory (but see [Ser79, Ch.XV, §3, Ex. 3], which is the very last exercise loc.cit., or [**?**, ???]). For the convenience of the reader we give a self-contained and easy proof in Section 4, Theorem 7.

The conductor of $\left(\frac{\Delta}{*}\right)$ equals the conductor of the Dirichlet character ψ (see e.g. [Neu99, Ch. 7, (6.2) Prop.]). But this is the product all local conductors $\mathfrak{p}_v^{s_v}$ of the Dirichlet characters $a + \mathfrak{p}_v \mapsto (\Delta, a)_v$, taken over all finite v with $v(\Delta) \geq 1$. If $\mathfrak{p}_v \nmid 2$ then obviously $s_v = 0$ or $s_v = 1$ according as $v(\Delta)$ is even or odd, and therefore $s_v = v(\Delta/\mathfrak{f}_\Delta^2)$. If on the contrary $\mathfrak{p}_v \mid 2$ then $(\Delta, a)_v = \left(\Delta/\pi_v^{2k}, a\right)_v$ for any integer k, and as we saw $a \mapsto \left(\Delta/\pi_v^{2k}, a\right)_v$ factors through a Dirichlet character modulo Δ/π_v^{2k} if Δ/π_v^{2k} is integral and a square modulo 4. Therefore, s_v is $\leq$ the

largest power $\mathfrak{p}_v^{2k}$ dividing Δ and such that $\Delta' := \Delta/\mathfrak{p}_v^{2k}$ is a square modulo 4, i.e. $s_v \le v(\Delta')$. But s_v is even equal to $v(\Delta')$. For this let $l = v(\Delta')$. Clearly, $l \le 2e+1$ (with $e = v(2)$). If $l = 2e+1$, Theorem 7 below implies $(\Delta, a)_v = (\pi, a)_v$ for all units a, and another application of this theorem implies that there is a unit a in U_{4e} such that $(\pi, a)_v = -1$; we conclude $s_v = 2e+1$. If $l \le 2e$ (so that l is even), we proceed as in the last paragraph and write as before $\Delta' = \pi_v^l c^2 d$ with units c, d and d in U_{2e-l}. Again $(\Delta', a)_v = (d, a)_v$. Therefore $(d, U_{s_v})_v = 1$, and then Theorem 7 implies that d is in U_{2e-s_v}. But by the choice of k the unit d is not in any U_m for any $m \ge 2e-l+2$, and therefore $2e - s_v \le 2e - l + 1$, i.e. $s_v \ge l-1$. Since $U_{l-1}U_{(l-1)/2}^2 = U_{l-2}$ (see Lemma 2 below) we conclude $s_v \le l$, which was to be shown. This proves the theorem. □

3. A reciprocity law

Using the Größencharakter $\left(\frac{\Delta}{*}\right)$ we define a function χ_Δ on the semigroup of all integral ideals $\mathfrak{a}$ by setting

$$\chi_\Delta(\mathfrak{a}) := \begin{cases} \mathrm{N}(\mathfrak{g}) \left(\frac{\Delta}{\mathfrak{a}/\mathfrak{g}^2}\right)_0 & \text{if } (\mathfrak{a}, \Delta) = \mathfrak{g}^2 \text{ and } \Delta \text{ is a square mod } 4\mathfrak{g}^2, \\ 0 & \text{otherwise.} \end{cases}$$

Note that, for an integral square $\mathfrak{g}^2 \mid \Delta$, the condition that Δ is a square mod $4\mathfrak{g}^2$ is equivalent to $\mathfrak{g} \mid \mathfrak{f}_\Delta$. Of course, χ_Δ is no longer a homomorphism, but it remains multiplicative in the sense that $\chi_\Delta(\mathfrak{ab}) = \chi_\Delta(\mathfrak{a})\chi_\Delta(\mathfrak{b})$ whenever $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime.

Theorem 6. *For any integral ideal $\mathfrak{a}$, one has*

$$\operatorname{card}\left(\{x \in \mathfrak{o}/2\mathfrak{a} : x^2 \equiv \Delta \bmod 4\mathfrak{a}\}\right) = \sum_{\substack{\mathfrak{b} \mid \mathfrak{a} \\ \mathfrak{a}/\mathfrak{b} \text{ squarefree}}} \chi_\Delta(\mathfrak{b}). \tag{5}$$

(The sum is over all integral ideals diving $\mathfrak{a}$ and such that $\mathfrak{a}/\mathfrak{b}$ is squarefree.)

Should this be here or in the Eisenstein paper?

Remark. In terms of Dirichlet series the formula of the theorem can be rewritten as

$$\sum_{\mathfrak{a}} \frac{\operatorname{card}\left(\{x \in \mathfrak{o}/2\mathfrak{a} : x^2 \equiv \Delta \bmod 4\mathfrak{a}\}\right)}{\mathrm{N}(\mathfrak{a})^s} = \frac{\zeta_K(s)}{\zeta_K(2s)} L(\chi_\Delta, s).$$

The L-series is essentially the L-series associated to the Größencharakter $\left(\frac{\Delta}{*}\right)_0$, i.e.

$$L\left(\left(\frac{\Delta}{*}\right)_0, s\right) = \sum_{(\mathfrak{a}, \Delta/\mathfrak{f}_\Delta^2)=1} \left(\frac{\Delta}{\mathfrak{a}}\right)_0 \mathrm{N}(\mathfrak{a})^{-s}$$

(the sum being over all integral ideals relatively prime to $\Delta/\mathfrak{f}_\Delta^2$). More precisely, one has

$$L(\chi_\Delta, s) = L\left(\left(\frac{\Delta}{*}\right)_0, s\right) \sum_{\mathfrak{t} \mid \mathfrak{f}_\Delta} \frac{\mu(\mathfrak{t})\left(\frac{\Delta}{\mathfrak{t}}\right)_0}{\mathrm{N}(\mathfrak{t})^s} \sigma_{1-2s}(\mathfrak{f}_\Delta/\mathfrak{t}),$$

where $\left(\frac{\Delta}{\mathfrak{t}}\right)_0 = 0$ if $\mathfrak{t}$ is not relatively prime to $\Delta/\mathfrak{f}_\Delta$. Here $\mu(\mathfrak{a})$ is the Möbius μ-function of K. See Lemma **??** in the next section.

TODO

This is ??? classical and cite Don ??? [Zag77, p. 130] ???

Proof of Theorem 6. Denote the left hand side of the claimed identity by $S_\Delta(\mathfrak{a})$. Note that $S_\Delta(\mathfrak{a})$ is multiplicative in $\mathfrak{a}$. Indeed, the $\Delta \equiv s^2 \bmod 4$ has a unique solution $s \bmod 2$. Hence $S_\Delta(\mathfrak{a})$ equals the number of solutions mod $\mathfrak{a}2_\mathfrak{a}$ of $x^2 \equiv \Delta \bmod \mathfrak{a}2_\mathfrak{a}^2$, where $2_\mathfrak{a}$ is the product of all prime powers $\mathfrak{p}^e$ exactly dividing 2 where $\mathfrak{p} \mid a$. Using this description of $S_\Delta(\mathfrak{a})$ the claimed multiplicativity follows now from the Chinese remainder theorem.

It suffices therefore to prove (5) for prime ideal powers $\mathfrak{p}^k$ ($k \geq 1$), i.e. it suffices to prove, for $k \geq 1$,

$$S_\Delta(\mathfrak{p}^k) = \chi_\Delta(\mathfrak{p}^k) + \chi_\Delta(\mathfrak{p}^{k-1}). \tag{6}$$

Moreover, we can replace $\mathfrak{o}$ and $\mathfrak{p}$ in the definition of $S_\Delta(\mathfrak{p}^k)$ by the localization $\mathfrak{o}_\mathfrak{p}$ and the principal ideal $\widehat{\mathfrak{p}} = \pi\mathfrak{o}_\mathfrak{p}$, where π is a uniformizing parameter for the maximal ideal of $\mathfrak{o}_\mathfrak{p}$.

Assume first of all $\mathfrak{p} \nmid \Delta$. The right hand side of (6) equals then $1+\chi_\Delta(\mathfrak{p})$, which is 2 or 0 according as Δ is a square mod $4\mathfrak{p}$ or not. This proves (6) for $k = 1$. But then (6) is also true for all $k \geq 1$ since $S_\Delta(\mathfrak{p}^k) = S_\Delta(\mathfrak{p})$. For this it suffices to show that, for $k \geq 1$, the canonical reduction map $\rho : S_\Delta(\mathfrak{p}^{k+1}) \to S_\Delta(\mathfrak{p}^k)$ is a bijection. Indeed, let x be in $S_\Delta(\mathfrak{p}^k)$, and let y in $x + 2\widehat{\mathfrak{p}}^k$, say $y = x + 2\pi^k t$ for some t in $\mathfrak{o}_\mathfrak{p}$. The congruence

$$\left(x + 2\pi^k t\right)^2 \equiv \Delta \bmod 4\pi^{k+1}$$

is equivalent to $xt \equiv \frac{\Delta - x^2}{4\pi^k} \bmod \pi$, which has exactly one solution mod π (since $\pi \nmid x$).

Next, suppose that $\mathfrak{p}^l$ for some $l \geq 1$ is the exact power of $\mathfrak{p}$ dividing Δ, and let $\mathfrak{p}^e$ be the exact $\mathfrak{p}$-power dividing 2.

For $2e + k \leq l$, the congruence $x^2 \equiv \Delta \bmod 4\mathfrak{p}^k$ is equivalent to $\mathfrak{p}^{e+\lceil k/2 \rceil} \mid x$, $x \equiv s \bmod 2$ (where $s^2 \equiv \Delta \bmod 4$), and hence has $\mathrm{N}(\mathfrak{p})^{\lfloor k/2 \rfloor}$ solutions mod $2\mathfrak{p}^k$. But $\mathrm{N}(\mathfrak{p})^{\lfloor k/2 \rfloor}$ equals also the right hand side of (5) since one of the terms is zero and the other one equals $\mathrm{N}(\mathfrak{p})^{\lfloor k/2 \rfloor}$. (For the verification note that $2e \leq l - k$, so that $\Delta/\mathfrak{p}^{2\lfloor k/2 \rfloor}$ is divisible by $\mathfrak{p}^{2e}$, and hence still a square modulo 4.

For $2e + k > l$ and odd l, the congruence $x^2 \equiv \Delta \bmod 4\mathfrak{p}^k$ has no solution (since a square x^2 cannot have the odd $\mathfrak{p}$-power $\mathfrak{p}^l$ as exact divisor). But the right hand side of (6) is also zero since, for any k' with $2e + k' \geq l$, either the gcd of Δ and $\mathfrak{p}^{k'}$ equals $\mathfrak{p}^l$ (which is not a square), or else it equals $\mathfrak{p}^{k'}$, where $\pi^{k'}$ is not a square, or where $2e > l - k'$ and hence $\Delta/\pi^{k'}$ is not a square mod 4).

Finally, let $2e + k > l$ and l be even. Then the congruence $x^2 \equiv \Delta \bmod 4\mathfrak{p}^k$ is equivalent to $x \equiv \pi^{l/2} y \bmod 2\pi^k$ and $y^2 \equiv \Delta/\pi^l \bmod 4\pi^{k-l}$. In other words,

$$S_\Delta(\mathfrak{p}^k) = \mathrm{card}\left(\left\{y \in \mathfrak{o}_\mathfrak{p}/2\pi^{k-l/2} : y^2 \equiv \Delta' \bmod 4\pi^{k-l}\right\}\right),$$

where $\Delta' = \Delta/\pi^l$.

Suppose Δ' is a square mod 4. Then, for $k > l$, we have

$$S_\Delta(\mathfrak{p}^k) = \mathrm{N}(\mathfrak{p})^{l/2} S_{\Delta'}(\mathfrak{p}^{k-l}) = \mathrm{N}(\mathfrak{p})^{l/2}\left(\chi_{\Delta'}(\mathfrak{p}^{k-l}) + \chi_{\Delta'}(\mathfrak{p}^{k-l-1})\right),$$

where the second identity follows from the already proven validity of (6) for squares Δ mod 4 not divisible by $\mathfrak{p}$. But the right hand side of the last identity equals the right hand side of (6). If $k \leq l$ then $y^2 \equiv \Delta' \bmod 4\pi^{k-l}$ is equivalent to $y \equiv s \bmod 2\pi^{\lceil \frac{k-l}{2} \rceil}$. Hence $S_\Delta(\pi^k) = \mathrm{N}(\mathfrak{p})^{\lfloor k/2 \rfloor}$, which again proves (6).

Suppose now that Δ' is not a square mod 4. Then, for $k \geq l$ both sides of (6) equal 0. If $l > k$ (and $k > l - 2e$, so that in particular, $e \geq 1$) then $y^2 \equiv \Delta' \bmod 4\pi^{k-l}$ might have a solution or not. Let $\delta = \delta(\Delta')$ be the largest integer $1 \leq \delta \leq 2e - 1$ such that Δ' is a square mod π^δ. Note that δ must be odd (see Lemma 2 below). Note also that Δ' is a square mod $\mathfrak{p}$ (since squaring is the Frobenius isomorphism in a field of characteristic 2). Note also that the congruence

$\Delta' \equiv x^2 \bmod \pi^t$ with $t < 2e$ determines x uniquely mod $\pi^{\lceil t/2 \rceil}$. We therefore find $S_\Delta(\mathfrak{p}^k) = \mathrm{N}(\mathfrak{p})^{\lfloor k/2 \rfloor}$ for $1 \le 2e + k - l \le \delta$, and $S_\Delta(\mathfrak{p}^k) = 0$ for $\delta + l - 2e < k < l$. Again this equals the right hand side of (6) since, for $k' = k$ or $k' = k-1$, we have $(\Delta, \mathfrak{p}^{k'}) = \mathfrak{p}^{k'}$ and exactly one of these k' is even, and for this k' we have $\chi_\Delta(\mathfrak{p}^{k'}) = \mathrm{N}(\mathfrak{p})^{\lfloor k/2 \rfloor}$ or $\chi_\Delta(\mathfrak{p}^{k'}) = 0$ according as $\Delta/\pi^{k'}$ is a square mod 4, or not. But $\Delta/\mathfrak{p}^{k'}$ being a square mod 4 is equivalent to Δ' being a square mod $2e + k' - l$, i.e. $2e + k' - l \le \delta$. Since δ is odd, the latter is equivalent to $2e + k - l \le \delta$. This completes the proof of Theorem 6. □

4. The Hilbert symbol and the higher unit groups

In this section K denotes a finite extension of $\mathbb{Q}_2$ with ring of integers $\mathfrak{o}$ and prime element π. We let e be the ramification index of K, i.e. the largest integer such that $\pi^e \mid 2$. We use $(\_,\_)_K$ for the quadratic Hilbert symbol of K. Recall that this is the map $K^\times \times K^\times \to \{\pm 1\}$ such that $(a,b)_K = 1$ if and only if $ax^2 + by^2 = 1$ has solutions x, y in K. The Hilbert symbol is bilinear (see e.g. [O'M00, Prop. 57:10 and p. 166]), it obviously factors through a bilinear form on $K^\times/{K^\times}^2$, and this form is non-degenerate, i.e. $(a,b)_K = 1$ for all b is only possible if a is a square in K (see e.g. [O'M00, 63:13] for a short proof).

We set $U_0 := \mathfrak{o}^\times$, and, for $n \ge 1$, let $U_n = 1 + \pi^n \mathfrak{o}$ be the nth higher unit group of K. Clearly $U_n \supseteq U_{n+1}$ and $U_k^2 \subseteq U_{2k}^2$. The Local Square Theorem states that $U_{2e+1} = U_{e+1}^2$. (Recall a simple proof: $1 + 4\pi X = \left(\sum_{n \ge 0} \binom{1/2}{n} (4\pi X)^n\right)^2$ in the ring of formal power series $\mathfrak{o}[\![X]\!]$, and the series converges with respect to the valuation v of K towards an element of U_{e+1}^2 since $v(\binom{1/2}{n}(4\pi X)^n) = n(e+1) - (2^k - k - 2)e$, where $k = \lfloor \log_2 n \rfloor$.)

Lemma 2. *For $0 \le k \le e-1$, one has*

$$U_{2k} = U_{2k+1} U_k^2.$$

Proof. Let a in U_{2k}. The congruence $a \equiv \left(1 + \pi^k t\right)^2 \bmod \pi^{2k+1}$ is equivalent to $t^2 \equiv (a-1)/\pi^{2k} \bmod \pi$ (since the assumption $k < e$ implies $\pi^{2k+1} \mid 2\pi^k$), and this has a solution t (as the map $t \mapsto t^2$ defines an automorphism of $\mathfrak{o}/\pi$). With such a solution t, we have $a/\left(1 + \pi^k t\right)^2 \equiv 1 \bmod \pi^{2k+1}$, i.e. $a \in U_{2k+1}\left(1 + \pi^k t\right)^2$. For proving the inverse inclusion it suffices to note that $U_k^2 \subseteq U_{2k}$. Indeed, for any $(1 + \pi^k t) \in U_k$, we have $(1 + \pi^k t)^2 \equiv 1 \bmod \pi^{2k}$, since $\pi^k \mid 2$. □

Lemma 3. *One has $U_{2e}/U_e^2 \cong \mathbb{F}_2$.*

Proof. The application $1 + 4x \mapsto \mathrm{tr}_{\mathfrak{o}/\pi/\mathbb{F}_2} \overline{x}$ (where $\overline{x}$ is the residue class of x mod π) defines an epimorphism of U_{2e} onto $\mathbb{F}_2$. We claim that its kernel equals U_e^2. It contains U_e^2 since Since $(1+ey)^2 = 1 + 4(y + y^2)$ and $\mathrm{tr}_{\mathfrak{o}/\pi/\mathbb{F}_2}(\overline{y} + \overline{y}^2) = 0$. Vice versa, if $1 + 4x$ has $\mathrm{tr}_{\mathfrak{o}/\pi/\mathbb{F}_2} \overline{x} = 0$ then $1 + 4x \equiv (1 + 2y)^2 \bmod 4\pi$, i.e. $x \equiv y + y^2 \bmod \pi$, or equivalently $(1 + 4x)/(1 + 2y)^2 \in U_{2e+1} = U_{e+1}^2$, has a solution y. Namely, $\overline{y} \mapsto \overline{y} + \overline{y}^2$ defines an $\mathbb{F}_2$-linear endomorphism of $\mathfrak{o}/\pi$ with kernel $\mathbb{F}_2$ and image equal to the the kernel of $\mathrm{tr}_{\mathfrak{o}/\pi/\mathbb{F}_2}$. □

We use $\overline{U}_n$ for the image of U_n under the canonical map $K^\times \to K^\times/{K^\times}^2$.

Proposition 4. *One has*

$$\begin{aligned} 1 = \overline{U}_{2e+1} &\subseteq_2 \overline{U}_{2e} \\ &\subseteq_{2^f} \overline{U}_{2e-1} = \overline{U}_{2e-2} \cdots \subseteq_{2^f} \overline{U}_{2k+1} = \overline{U}_{2k} \cdots \subseteq_{2^f} \overline{U}_1 = \overline{U}_0 \\ &\subseteq_2 K^\times/{K^\times}^2, \end{aligned}$$

where "$\subseteq_n$" means "is subgroup of index n". In particular, for $0 \leq k \leq e$,

$$\operatorname{card}\left(\overline{U}_{2k}\right) = 2 \cdot 2^{f(e-k)}. \tag{7}$$

Proof. The first equality in the filtration chain, i.e. that the elements of U_{2e+1} are squares, is the Local Square Theorem.

For proving the equalities note that $\overline{U}_n = U_n {K^\times}^2 / {K^\times}^2$. But Lemma 2 implies $U_{2k}{K^\times}^2 = U_{2k+1}{K^\times}^2$.

For the first "$\subseteq_2$" we note that $U_{2e} \cap {K^\times}^2 = U_e^2$, whence

$$U_{2e}/U_e^2 \cong U_{2e}{K^\times}^2/{K^\times}^2,$$

and apply Lemma 3.

For the last "$\subseteq_2$" note that $K^\times = \langle\pi\rangle \times U_0$, from which we deduce $K^\times/{K^\times}^2 = \langle\overline{\pi}\rangle \times \overline{U}_0$, where $\overline{(\ )}$ is the canonical projection.

For the "$\subseteq_{2^f}$" we calculate

$$\overline{U}_{2k-1}/\overline{U}_{2k} \cong U_{2k-1}{K^\times}^2/U_{2k}{K^\times}^2 \cong U_{2k-1}/U_{2k} \cong \mathfrak{o}/\pi\mathfrak{o}$$

The last two isomorphisms are from right to left: $a + \pi\mathfrak{o} \mapsto (1 + a\pi^{2k-1})U_{2k}$ and $uU_{2k} \mapsto uU_{2k}{K^\times}^2$. Note that the second application defines indeed an isomorphism: It is obviously surjective. For proving that it is injective suppose, uU_{2k}, for a given u in U_{2k-1}, is mapped to $U_{2k}{K^\times}^2$, i.e. $u = va^2$ for some v in U_{2k} and a in $K^\times$. But then a must be unit, and since $a^2 \equiv 1 \bmod \pi^{2k-1}$ and $k \leq e$, we conclude that, in fact, $a \equiv 1 \bmod \pi^k$, which in turn implies that a^2 is in U_{2k} (again since $k \leq e$); hence $u = va^2$ is in U_{2k}. □

Theorem 7. *For $0 \leq k \leq e$ let $V_k = \overline{U}_{2k}$, and set $V_{-1} = K^\times/{K^\times}^2$, and $V_{e+1} = 1$. Then one has*

$$V_k^{\#} = V_{e-k},$$

for any $-1 \leq k \leq e+1$, where $V_k^{\#}$ denotes the subgroup of all $a{K^\times}^2$ in V_{-1} such that $(a,b)_K = 1$ for all $b{K^\times}^2$ in V_k.

Proof. The Hilbert symbol defines a non-degenerate bilinear form on the $\mathbb{F}_2$-vector space V_{-1}. From (7) we know

$$\dim_{\mathbb{F}_2} V_k + \dim_{\mathbb{F}_2} V_{e-k} = \dim V_{-1},$$

and hence $\dim_{\mathbb{F}_2} V_k^{\#} = \dim_{\mathbb{F}_2} V_{e-k}$. It suffices therefore to prove $V_k^{\#} \supseteq V_{e-k}$. For $k = -1$ or $k = e+1$ this is trivial. For $0 \leq k \leq e$ the inclusion is equivalent to $(U_{2k}, U_{2e-2k})_K = 1$.

But this is [Ser79, Ch.XV, §3, Ex. 3].

We should replace the ref to Serre by an easy proof

Elementary proof for $k = 0$

Given b in U_{4e} and a unit a, choose t such that $t^2 \equiv \frac{1-b}{4a} \bmod \pi$, so that then $a(2t)^2 + b(1 + 4\pi z) = 1$ for some integral z, and observe that$1 + 4\pi z$ is a square by the Local Square Theorem.

Proof for arbitrary k

There should be a similarly easy proof.

□

References

[Frö60] Albrecht Frölich. Discriminants of algebraic number fields. *Math. Z*, 74:18–28, 1960. 5

[Frö67] A. Fröhlich. Local fields. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*,, pages 1–41. Thompson, Washington, D.C., 1967. 3

[Hec23] Erich Hecke. *Vorlesungen über die Theorie der algebraischen Zahlen. 2te Aufl.* Akademische Verlagsgesellschaft, M.B.H., Leipzig, 1923. 2, 3, 6

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. 8

[O'M00] O. Timothy O'Meara. *Introduction to quadratic forms*. Classics in Mathematics. Springer-Verlag, Berlin, 2000. Reprint of the 1973 edition. 7, 8, 11

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg. 8, 12

[Zag77] D. Zagier. Modular forms whose Fourier coefficients involve zeta-functions of quadratic fields. In *Modular functions of one variable, VI (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, pages 105–169. Lecture Notes in Math., Vol. 627. Springer, Berlin, 1977. 9

İstanbul Üniversitesi, Fen Fakültesi, Matematik Bölümü, 34134 Vezneciler, İstanbul, Turkey

Current address: Max-Planck Institute für Mathematik, Vivatsgasse 7, 53111, Bonn, Germany

E-mail address: hatice.boylan@gmail.com

Universität Siegen, Department Mathematik, 57068 Siegen, Germany

E-mail address: nils.skoruppa@gmail.com