

CLASS GROUPS AND NORMS OF UNITS

A Dissertation

Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

in

The Department of Mathematics

by

Costel Ionita

B.S. in Math., Bucharest University, 1995

M.S., Louisiana State University, 2002

August 2004

Acknowledgments

This dissertation would not be possible without several contributions. It is a pleasure to thank Dr. Jurgen Hurrelbrink for his constant support and encouragement.

I want also to thank to my committee: Dr. Robert Perlis, Dr. Jerome Hoffman, Dr. Richard Litherland, Dr. Bogdan Oporowski and Dr. Louis Escobar.

This dissertation is dedicated to Adina and Razvan.

Table of Contents

Acknowledgments	ii
Abstract	iv
Introduction	1
1. Basic Tools	6
1.1 Basic Results	6
1.2 The Exact Hexagon	10
2. Relative Quadratic Extensions	13
2.1 Definitions and Notations	13
2.2 Quadratic Extensions	15
2.3 Construction of F/K with $h(F)$ Odd	35
2.4 The Hilbert Symbol	38
2.5 Elementary Abelian 2-groups	44
2.6 Star Extensions	46
2.7 Examples	53
3. Density Results	57
3.1 Background	57
3.2 The Extension	60
References	64
Appendix: List of Primes	68
Vita	71

Abstract

Our object of study is relative quadratic extensions of algebraic number fields $F/K = K(\sqrt{\sigma})/K$, with $\sigma \in K^* \setminus K^{*2}$. In [4], the authors P.E. Conner and J. Hurrelbrink study in detail the cases σ totally positive respectively totally negative. In this paper we generalize some of the results without any assumption on the sign of σ .

Introduction

In this paper we study relative quadratic extensions of algebraic number fields F/K . Using a unified approach, we shall deal with classical questions concerning the interplay between units, ideal class groups of F and K , and ramification in F/K . In their book [4], P.E. Conner and J. Hurrelbrink give a detailed treatment of $F = K(\sqrt{\sigma})/K$ when σ is totally positive or totally negative. We shall extend these results to any relative quadratic extension F/K .

Our main tool is the exact hexagon 1.18 which involves four cohomology groups $H^s(\text{Gal}(F/K); \mathcal{O}_F^*)$, $H^s(\text{Gal}(F/K); C(F))$ and two computable groups $R^s(F/K)$, $s = 0, 1$.

In order to do this, we introduce for any number field L and its ring of integers \mathcal{O}_L , the **ideal class group** of L , denoted $C(L)$.

Let J be the group of nonzero fractional \mathcal{O}_L -ideals and H the subgroup of nonzero principal fractional \mathcal{O}_L -ideals. Then $C(L)$ is the quotient group J/H . The group $C(L)$ is trivial if and only if \mathcal{O}_L is a principal ideal domain (PID) and thus we have unique prime element decomposition. For any number field L , $C(L)$ is a finite abelian group. The number of elements in $C(L)$ is the **class number** of L , denoted by $h(L)$. It is a classical problem to investigate the structure and order of the ideal class group.

Gauss knew for squarefree $d < 0$ that there are at least nine fields $\mathbb{Q}(\sqrt{d})$ with class number 1. Heilbronn and Linfoot [19] in 1934 showed that the class number is 1 for at most one more such d . It was finally proved that there are only nine such fields with class number 1, first by Heegner [18] in 1952, then independently

by Baker [1] and Stark [48] in 1966. All number fields with class number 2 were characterized by Carlitz [3].

To understand the structure of the ideal class group for a quadratic number field, it is important to determine the structure of its 2-Sylow subgroup. As the ideal class group $C(L)$ of L is a finite abelian group, it is a product of cyclic groups of prime power order. The **2-rank** of $C(L)$ is the number of cyclic factors of $C(L)$ of order divisible by 2. We note that this notion of 2-rank holds for any finite abelian group. Using quadratic forms, Gauss proved that the 2-rank of the (narrow) ideal class group of L is $t - 1$ where t is the number of distinct prime divisors of the discriminant of L . As a consequence, we have:

Proposition 0.1. *2-rk $(C(L)) = t - 2$ if L is real quadratic and -1 is not a norm from L , and $t - 1$ otherwise.*

In Chapter 2 we extend this result to a relative quadratic extension and prove the following, see Theorem 2.43

Theorem 0.2. *Let K be a totally real algebraic number field containing units with independent signs, and F/K a quadratic extension of K . If $h(K) \equiv 1 \pmod{2}$ and \mathcal{O}_F^* contains units with independent signs, then*

$$2\text{-rk}(C(F)) = \#\mathcal{R}(F/K) - 1$$

where $\#\mathcal{R}(F/K)$ represents the number of ramified prime ideals in F/K .

For a number field F and its ring of integers \mathcal{O}_F , the **units** of \mathcal{O}_F are the elements $u \in \mathcal{O}_F$ such that there exists $x \in \mathcal{O}_F$ with $ux = 1$. The units form a multiplicative group, denoted \mathcal{O}_F^* . Consider the quadratic number field $F = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$, squarefree, and its ring of integers \mathcal{O}_F . For an imaginary quadratic number field F , we have

Proposition 0.3. *If $d < 0$ and squarefree, then*

(i) *For $d = -1$, $\mathcal{O}_F^* = \{\pm 1, \pm i\}$*

(ii) *For $d = -3$, $\mathcal{O}_F^* = \{\pm 1, \pm \omega, \pm \omega^2\}$ where $\omega = \frac{-1+\sqrt{-3}}{2}$.*

(iii) *Otherwise, $\mathcal{O}_F^* = \{\pm 1\}$*

Determining \mathcal{O}_F^* in the case of a real quadratic field F relies on the fact that the Pell equation

$$x^2 - dy^2 = \pm 1$$

has a solution in nonzero integers x, y . Using this result, one obtains

Proposition 0.4. *If \mathcal{O}_F is the ring of integers in $F = \mathbb{Q}(\sqrt{d})$, $d > 0$ and square-free, then there exists a unit $\epsilon > 1$ such that every unit of \mathcal{O}_F is of the form $\pm \epsilon^m$, $m \in \mathbb{Z}$.*

The unique unit ϵ is called the **fundamental unit** of $\mathbb{Q}(\sqrt{d})$. For a real quadratic field F , Dirichlet related the class number $h(F)$ and the fundamental unit of F . Propositions 0.3 and 0.4 are very special cases of Dirichlet's Unit Theorem which gives the structure of the group of units in a number field.

A very important questions is when does a field F have units with independent signs. In [4] the authors prove the following

Proposition 0.5. *Let K be totally real and F/K a real quadratic extension. Then F has units with independent signs if and only if K has units with independent signs and $H^0(C_2; \mathcal{O}_F^*)$ is trivial.*

We shall generalize this and prove that, see Corollary 2.36

Proposition 0.6. *Let K be totally real, having units with independent signs and $F = K(\sqrt{\sigma})/K$. Denote by $n = [K : \mathbb{Q}]$ and by $0 \leq k \leq n$ the number of real*

embeddings of K with respect to which σ is positive. If $\sigma \notin \mathcal{O}_K^*/\mathcal{O}_K^{*2}$ then the following are equivalent:

1. F contains units with independent signs.
2. $2\text{-rk } H^0(C_2; \mathcal{O}_F^*) = n - k$.
3. Every unit of \mathcal{O}_K^* which is positive at every ordering of K with respect to which σ is negative, is the norm of a unit in \mathcal{O}_F^* .
4. $H^1(C_2; \mathcal{O}_F^*)$ is cyclic of order 2 (generated by $\text{cl}(-1)$).

Example 0.7. Let p be a prime. The structure of the 2-Sylow subgroup of the ideal class group of the real quadratic fields $\mathbb{Q}(\sqrt{2p})$ is given by:

$$\begin{aligned}
 p = 2 & : \{1\} \\
 p \equiv 3, 7 \pmod{8} & : \{1\} \\
 p \equiv 1 \pmod{8} & : C_2 \text{ if } p \neq x^2 + 32y^2 \text{ for all } x, y \in \mathbb{Z} \\
 & : C_{2^j} \text{ with } j \geq 2 \text{ if } p = x^2 + 32y^2 \text{ for some } x, y \in \mathbb{Z} \\
 p \equiv 5 \pmod{8} & : C_2.
 \end{aligned}$$

By Theorem 21.6 in [4], the sets $\{p \equiv 1 \pmod{8} : p \neq x^2 + 32y^2 \forall x, y \in \mathbb{Z}\}$ and $\{p \equiv 1 \pmod{8} : p = x^2 + 32y^2 \text{ for some } x, y \in \mathbb{Z}\}$ each have a density $\frac{1}{2}$ in the set of primes $p \equiv 1 \pmod{8}$.

In chapter 1, we introduce the notions and results which are necessary to prove our results. We also present the exact hexagon and the main results derived from its formalism.

In chapter 2, we prove the main results of our paper.

In chapter 3, we construct a finite extension of \mathbb{Q} which will enable us to prove a density result via Chebotarev's Density Theorem. In the end we present three

lists, obtained by using PariGP, that lead us to some conjectures about density results concerning the norm of fundamental units.

1. Basic Tools

1.1 Basic Results

In this section we will recall basic definitions and theorems that are going to be used in this paper. A *number field* is a subfield of \mathbb{C} which has finite degree over \mathbb{Q} . We will denote this degree by $[K : \mathbb{Q}]$. For a number field K we let \mathcal{O}_K denote the *ring of algebraic integers of K* , namely the set of all $x \in K$ which are roots of some monic polynomial with integer coefficients. Even though rings of integers are not unique factorization domains we can recover this feature by looking at the ideals of \mathcal{O}_K :

Theorem 1.8. *If K is a number field, then any nonzero ideal P of \mathcal{O}_K can be written uniquely, up to order, as a product of prime ideals.*

Thus, if $P = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdots \mathfrak{p}_r$ is the prime decomposition of P then \mathfrak{p}_i are exactly the prime ideals of \mathcal{O}_K containing P .

The *residue field* of the nonzero ideal P is the quotient ring \mathcal{O}_K/P . This ring is finite and we define the *norm* of P to be $N(P) = |\mathcal{O}_K/P|$. A very important thing to know is how primes are decomposing in finite extensions of number fields. Let K be a number field, and let F be a finite extension of K . If P is a prime ideal of K then $P\mathcal{O}_F$ is an ideal of F , and by Theorem 1.8 we have

$$P\mathcal{O}_F = Q_1^{e_1} \cdot Q_2^{e_2} \cdots Q_g^{e_g}$$

where the Q_i 's are distinct primes of F containing P . The integer e_i is called the *ramification index* of P in Q . We say that the prime ideal P of K is *ramified* in F if at least one e_i is greater than 1. If $P\mathcal{O}_F$ is prime in F then we say that P is *inert* in F . The *inertial degree* f_i of P in Q_i is $[\mathcal{O}_F/Q_i : \mathcal{O}_K/P]$. Then we have the following

Theorem 1.9. *Let $K \subset F$ be number fields, and let P be a prime of K . If e_i and f_i are the ramification and inertial degrees respectively for $i = 1, 2, \dots, g$, then*

$$\sum_{i=1}^g e_i f_i = [F : K].$$

Assume that $K \subset F$ is a Galois extension. Then

Theorem 1.10. *Let $K \subset F$ be a Galois extension, and let P be a prime ideal of K . Then the Galois group $\text{Gal}(F/K)$ acts transitively on the primes of F containing P . That is, if Q and Q' are primes of F containing P , then there is a $\phi \in \text{Gal}(F/K)$ such that $\phi(Q) = Q'$.*

If F is a Galois extension of K then Theorem 1.9 simplifies

Theorem 1.11. *Let $K \subset F$ be a Galois extension and let P be a prime of K . Then the primes Q_1, Q_2, \dots, Q_g of F containing P all have the same ramification index e , the same inertial degree f , and*

$$efg = [F : K].$$

For a Galois extension $K \subset F$, an ideal P of K is ramified in F if $e > 1$, and is *unramified* in F if $e = 1$. We say that P *splits completely* in F if $e = f = 1$. If P splits completely then it is also unramified and the number of primes in the decomposition of $P\mathcal{O}_F$ is $[F : K]$. Note that if P is inert in F then $g = e = 1$ and $f = [F : K]$. As an example let us consider quadratic number fields, i.e. fields of degree 2 over \mathbb{Q} . Let $K = \mathbb{Q}(\sqrt{d})$ with $d \neq 0, 1$ square free integer. The *discriminant* d_K is given by

$$d_K = \begin{cases} d & \text{if } d \equiv 1 \pmod{4} \\ 4d & \text{otherwise} \end{cases}$$

We also have that

$$\mathcal{O}_K = \begin{cases} \mathbb{Z} \left[\frac{1+\sqrt{d}}{2} \right] & \text{if } d \equiv 1 \pmod{4} \\ \mathbb{Z} \left[\sqrt{d} \right] & \text{otherwise} \end{cases}$$

Let us now define the *Legendre symbol* $\left(\frac{a}{p}\right)$. If a is an integer and p is an odd prime then

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p|a \\ 1 & \text{if } p \nmid a \text{ and } x^2 \equiv a \pmod{p} \text{ is solvable for some } x \in \mathbb{Z} \\ -1 & \text{if } p \nmid a \text{ and } x^2 \not\equiv a \pmod{p} \text{ for all } x \in \mathbb{Z} \end{cases}$$

Now we have the following

Proposition 1.12. *Let a and b be integers and p an odd prime. Then*

- (i) $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$
- (ii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$
- (iii) If $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Let us now state one of the most beautiful results in mathematics

Theorem 1.13. (*Law of Quadratic Reciprocity*) *Let p and q be odd primes. Then*

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

We can now describe the splitting behavior of primes of K .

Proposition 1.14. *Let p be an odd prime in \mathbb{Z} and K a quadratic number field of discriminant d_K . Then*

- (i) If $\left(\frac{d_K}{p}\right) = 0$, then $p\mathcal{O}_K = P^2$ for some ideal P of K (i.e. p ramifies in K).
- (ii) If $\left(\frac{d_K}{p}\right) = 1$, then $p\mathcal{O}_K = PP'$ for some prime ideals $P \neq P'$ of K (i.e. p splits completely in K).

(iii) If $\left(\frac{d_K}{p}\right) = -1$, then $p\mathcal{O}_K$ is prime in \mathcal{O}_K (i.e. p is inert in K).

Another important result is the Dirichlet's Unit Theorem:

Theorem 1.15. *Let K be a number field, \mathcal{O}_K^* its unit group and denote by $r_1(K)$ and $2r_2(K)$ the number of real and complex embeddings of K in \mathbb{C} . Then \mathcal{O}_K^* is the direct product $W \times V$ where W is a finite cyclic group consisting of the roots of unity in K , and V is a free abelian group of rank $r_1(K) + r_2(K) - 1$.*

In other words, V consists of products

$$u_1^{k_1} u_2^{k_2} \cdots u_{r_1(K)+r_2(K)-1}^{k_{r_1(K)+r_2(K)-1}}, \quad k_i \in \mathbb{Z}$$

for some set of $r_1(K) + r_2(K) - 1$ units. Note that if K is totally real, i.e. $r_2(K) = 0$, then V has rank $r_1(K) - 1$ and $W = \{\pm 1\}$.

We will introduce the notion of *units with independent signs* which is related to the narrow class group of a number field K .

Definition 1.16. *A number field K has units with independent signs if and only if for each embedding $\nu : K \rightarrow \mathbb{R}$ there is a unit in \mathcal{O}_K^* whose image under ν is negative but whose image under every other real embedding of K is positive.*

We note that if K has units with independent signs, then the sign homomorphism

$$\mathcal{O}_K^* \rightarrow (\mathbb{Z}^*)^{r_1(K)}$$

is an epimorphism. In [4] the authors prove the following result which we shall use later.

Lemma 1.17. *Let K be a totally real number field. Then K has units with independent signs if and only if every totally positive unit in \mathcal{O}_K^* is a square.*

1.2 The Exact Hexagon

We will follow [4] to define the exact hexagon. Let F/K be a quadratic extension whose Galois group is cyclic of order 2. We will denote by $\bar{}$ the non trivial automorphism. Let us define two homomorphisms

$$d^0 : H^0(C_2; C(F)) \rightarrow H^0(C_2; \mathcal{O}_F^*)$$

and

$$d_1 : H^1(C_2; C(F)) \rightarrow H^1(C_2; \mathcal{O}_F^*)$$

in the following way.

An element of $H^0(C_2; C(F))$ is represented by some \mathcal{O}_F -ideal A which satisfies $\bar{A} = xA$ for some $x \in F^*$. Then $A\bar{A} = \bar{x}xA\bar{A} = N(x)A\bar{A}$, hence $v = N(x) \in \mathcal{O}_K^*$.

Set

$$d_0(\text{cl}(A)) = \text{cl}(v) \in H^0(C_2; \mathcal{O}_F^*).$$

An element of $H^1(C_2; C(F))$ is represented by some \mathcal{O}_F -ideal A which satisfies $A\bar{A} = x\mathcal{O}_F$ for some $x \in F^*$. This time $x\mathcal{O}_F = A\bar{A} = \overline{A\bar{A}} = \bar{x}\mathcal{O}_F$, hence $u = \bar{x}x^{-1} \in \mathcal{O}_F^*$ and clearly $N(u) = 1$. Then set

$$d_1(\text{cl}(A)) = \text{cl}(u) \in H^1(C_2; \mathcal{O}_F^*).$$

Observe that to the extension F/K there is an associated abelian group consisting of all pairs (y, A) where $y \in K^*$ and A is an \mathcal{O}_F -fractional ideal such that $yA\bar{A} = \mathcal{O}_F$. Now the group $R^0(F/K)$ is the quotient of this group of pairs (y, A) by its subgroup consisting of pairs of the form $(N(z), z^{-1}\bar{B}B^{-1})$, where $z \in F^*$ and B is an \mathcal{O}_F -fractional ideal. We denote by $\langle y, A \rangle$ the class of (y, A) in the factor group $R^0(F/K)$.

Now we are going to relate $R^0(F/K)$ to the cohomology groups $H^0(C_2; \mathcal{O}_F^*)$ and $H^1(C_2; C(F))$. We define

$$i_0 : H^0(C_2; \mathcal{O}_F^*) \rightarrow R^0(F/K)$$

by

$$\text{cl}(v) \mapsto \langle v, \mathcal{O}_F \rangle \text{ for } v \in \mathcal{O}_F^*.$$

Also, let us define

$$j_1 : R^0(F/K) \rightarrow H^1(C_2; C(F))$$

by

$$\langle y, A \rangle \mapsto \text{cl}(A) \text{ for } y \in K^*, yA\bar{A} = \mathcal{O}_F.$$

To define the group $R^1(F/K)$ we begin with the set of all pairs (v, A) where $v \in \mathcal{O}_F^*$ is a unit with $N(v) = 1$ and A is an \mathcal{O}_F -fractional ideal such that $\bar{A} = A$. This set is an abelian group with respect to component wise multiplication. We call two pairs (v, A) and (v_1, A_1) equivalent if there exist $x \in F^*$ and B an \mathcal{O}_F -fractional ideal such that $xB\bar{B}A = A_1$ and $\bar{x}x^{-1}v = v_1$. It turns out that the above relation is an equivalence relation and we will denote the equivalence class of (v, A) by $|v, A|$. Then the group $R^1(F/K)$ is defined as the set of all such equivalence classes $|v, A|$ with $v \in \mathcal{O}_F^*$, $N(v) = 1$, A an \mathcal{O}_F -fractional ideal with $\bar{A} = A$.

We will connect $R^1(F/K)$ with the cohomology groups $H^1(C_2; \mathcal{O}_F^*)$ and $H^0(C_2; C(F))$ by defining two homomorphisms i_1 and j_0 . First define

$$i_1 : H^1(C_2; \mathcal{O}_F^*) \rightarrow R^1(F/K)$$

by

$$\text{cl}(v) \mapsto |v, \mathcal{O}_F|$$

for $v \in \mathcal{O}_F^*$ with $N(v) = 1$. Secondly define

$$j_0 : R^1(F/K) \rightarrow H^0(C_2; C(F))$$

by

$$|v, A| \mapsto \text{cl}(A)$$

for $v \in \mathcal{O}_F^*$ with $N(v) = 1$ and A is an \mathcal{O}_F^* -fractional ideal with $\bar{A} = A$.

Now Theorem 2.3 in [4] becomes

Theorem 1.18. *Let F/K be a quadratic extension. Then there is an exact hexagon*

$$\begin{array}{ccccc}
 & & \mathrm{H}^1(C_2; C(F)) & \xrightarrow{d_1} & \mathrm{H}^1(C_2; \mathcal{O}_F^*) & & \\
 & \nearrow^{j_1} & & & & \searrow^{i_1} & \\
 \mathrm{R}^0(F/K) & & & & & & \mathrm{R}^1(F/K) \\
 & \nwarrow_{i_0} & & & & \swarrow_{j_0} & \\
 & & \mathrm{H}^0(C_2; \mathcal{O}_F^*) & \xleftarrow{d_0} & \mathrm{H}^0(C_2; C(F)) & &
 \end{array}$$

2. Relative Quadratic Extensions

2.1 Definitions and Notations

We use as our base field a totally real number field K containing units with independent signs. We let $n = [K : \mathbb{Q}]$ denote the absolute degree of K . Thus n is the number of real infinite primes in Ω_K ; that is the number of distinct orderings of K .

Because K is totally real it follows, by Lemma 1.17 that K contains units with independent signs if and only if every totally positive unit in \mathcal{O}_K^* is a square (and hence the square of a unit).

Let $C(K)$ denote the ideal class group of K . Then for the narrow class group of K we have:

$$C^+(K) \cong C(K),$$

since K contains units with independent signs.

Frequently we shall make use of the multiplicative group of global square classes K^*/K^{*2} . This is an elementary abelian 2-group.

Let us take up a simple example employing K^*/K^{*2} . First we denote by $\mathcal{E} \subset K^*$ the subgroup of field elements $x \in K^*$ which satisfy the condition

$$\text{ord}_P x \equiv 0 \pmod{2}$$

at every prime ideal $P \subset \mathcal{O}_K$. Obviously $K^{*2} \subset \mathcal{E}$ and $\mathcal{O}_K^* \subset \mathcal{E}$. Then let us turn to the quotient group:

$$E = \mathcal{E}/K^{*2} \subset K^*/K^{*2}.$$

Since a unit in \mathcal{O}_K^* is a square in K^* if and only if it is a square in \mathcal{O}_K^* , then there is an inclusion

$$\mathcal{O}_K^*/\mathcal{O}_K^{*2} \subset E.$$

Next, if $C(K)_2 \subset C(K)$ is the subgroup of ideal classes with order less than or equal to 2, we shall define an epimorphism

$$\epsilon : \mathcal{E} \rightarrow C(K)_2.$$

Namely, if $x \in \mathcal{E}$, then there is a unique \mathcal{O}_K -ideal $A \subset K$ for which

$$x\mathcal{O}_K = A^2.$$

Set $\epsilon(x) = \text{cl}(A) \in C(K)_2$. This is an epimorphism for if A is an \mathcal{O}_K -ideal for which $\text{cl}(A)^2 = \text{cl}(A^2) = \mathbf{1} \in C(K)$, then by definition $x\mathcal{O}_K = A^2$ for some $x \in K^*$. Clearly $x \in \mathcal{E}$ with $\epsilon(x) = \text{cl}(A)$.

Now, $K^{*2} \subset \mathcal{E}$, but ϵ is trivial on K^{*2} . That is, if $z^2 = x \in \mathcal{E}$, then $x\mathcal{O}_K = z^2\mathcal{O}_K = (z\mathcal{O}_K)^2$ so that $\epsilon(x) = \text{cl}(z\mathcal{O}_K) = \mathbf{1} \in C(K)$. Then, there is an induced epimorphism, also denoted

$$\epsilon : E \rightarrow C(K)_2.$$

We shall now see that $\ker(\epsilon) \subset E$ is exactly $\mathcal{O}_K^*/\mathcal{O}_K^{*2} \subset E$.

Proposition 2.19. *We have: $\ker(\epsilon) = \mathcal{O}_K^*/\mathcal{O}_K^{*2}$.*

Proof. Suppose for $x \in \mathcal{E}$ that $x\mathcal{O}_K = a^2$ and A is principal, that is $x \in \ker(\epsilon)$. Thus, $z\mathcal{O}_K = A$, for some $z \in K^*$. Hence $x\mathcal{O}_K = z^2\mathcal{O}_K$, therefore $x = uz^2$ for some $u \in \mathcal{O}_K^*$. In $E = \mathcal{E}/K^{*2}$, we have $x = u$, hence $x \in \mathcal{O}_K^*/\mathcal{O}_K^{*2}$. It is trivial to see that $\mathcal{O}_K^*/\mathcal{O}_K^{*2} \subset \ker(\epsilon) \subset E$, for if $x = vw^2 \in \mathcal{O}_K^*/\mathcal{O}_K^{*2}$, then $\epsilon(x) = \epsilon(vw^2) = \mathbf{1} \in C(K)$. □

Lemma 2.20. *In K^*/K^{*2} the subgroup E is a finite elementary abelian 2-group of 2-rank:*

$$2\text{-rk } E = n + 2\text{-rk } C(K) = 2\text{-rk } \mathcal{O}_K^*/\mathcal{O}_K^{*2} + 2\text{-rk } C(K)_2.$$

Proof. Recall the short exact sequence:

$$\mathbf{1} \rightarrow \mathcal{O}_K^*/\mathcal{O}_K^{*2} \rightarrow E \rightarrow C(K)_2 \rightarrow \mathbf{1}.$$

Also, we have $2\text{-rk } \mathcal{O}_K^*/\mathcal{O}_K^{*2} = n$ since K is totally real. \square

We can use the assumption that K contains units with independent signs to canonically embed $C(K)_2$ back into E . Consider $c \in C(K)_2$ and represent c by an \mathcal{O}_K -ideal A . Then A^2 is principal so $x\mathcal{O}_K = A^2$ for some $x \in \mathcal{E}$. But \mathcal{O}_K^* contains units with independent signs, therefore for some $u \in \mathcal{O}_K^*$, $ux = y$ will be a totally positive generator for A^2 . If y_1 is a second such totally positive generator then $y_1y^{-1} = v \in \mathcal{O}_K^*$, with v totally positive. Thus, $y_1 = y$ in E since every totally positive unit in \mathcal{O}_K^* is a square. We can continue to see that there is a homomorphism

$$\eta : C(K)_2 \rightarrow E$$

with $\eta(c) = c$, $c \in C(K)_2$. By taking $E^+ \subset E$ to be the set of all totally positive square classes in E we find:

$$E^+ \cong C(K)_2 \tag{2.1}$$

2.2 Quadratic Extensions

For $1 \neq \sigma \in K^* \setminus K^{*2}$ we have the quadratic extension:

$$F/K = K(\sqrt{\sigma})/K.$$

Then, k , $0 \leq k \leq n$, will denote the number of orderings of K with respect to which σ is positive. Thus k is the number of real infinite primes in K each of which splits into a conjugate pair of orderings of F . Hence $n - k$ is the number of real infinite primes in K which ramify in F into complex infinite primes. Thus:

$$r_1(F) = 2k, \quad r_2(F) = n - k.$$

We denote by $S \subset \Omega_K$ the set of all infinite primes in K together with all the finite primes in K which ramify in F/K . Let us denote by $\mathcal{R}(F/K)$ the set of prime ideals $P \subset \mathcal{O}_K$ that ramify in F/K . Hence:

$$\#S = n + \#\mathcal{R}(F/K).$$

Let

$$\mathcal{E}_S = \{y \in K^* : \text{ord}_P y \equiv (0 \pmod{2}) \text{ for all } P \notin S\} \subset K^*.$$

Thus, $y \in \mathcal{E}_S$ has even order at all unramified prime ideals $P \subset \mathcal{O}_K$. Obviously $K^{*2} \subset \mathcal{E}_S$ and $U_S \subset \mathcal{E}_S$, where $U_S \subset K^*$ is the subgroup of S -units. Now, every element of K can be viewed as an element of F . In particular for $y \in \mathcal{E}_S$ we have:

1. If $P \subset \mathcal{O}_K$ and $P \in \Omega_K \setminus S$, then for a prime ideal $\mathcal{P} \subset \mathcal{O}_F$ extending P we have: $\text{ord}_{\mathcal{P}} y = \text{ord}_P y \equiv 0 \pmod{2}$.
2. If $P \subset \mathcal{O}_K$ and P is ramified, then $p\mathcal{O}_K = \mathcal{P}^2$ and: $\text{ord}_{\mathcal{P}} y = 2\text{ord}_P y \equiv (0 \pmod{2})$.

Thus, if $y \in \mathcal{E}_S$, then $y\mathcal{O}_F = A^2$ for a unique \mathcal{O}_F -ideal A . Note that $\text{cl}(A) \in C(F)_2$.

Then we have an homomorphism

$$H : \mathcal{E}_S \rightarrow C(F)_2.$$

If $y = z^2 \in \mathcal{E}_S$ we have $z^2\mathcal{O}_F = A^2$ or $(z\mathcal{O}_F)^2 = A^2$. Thus $A = z\mathcal{O}_F$ and $\text{cl}(A) = \mathbf{1} \in C(F)_2$. Hence H is trivial on $K^{*2} \subset \mathcal{E}_S$. Also, H is trivial on $\mathcal{O}_K^* \subset \mathcal{E}_S$. Finally, recall that $F/K = F(\sqrt{\sigma})/K$, hence $\sigma \in \mathcal{E}_S$ and since $\sigma\mathcal{O}_F = (\sqrt{\sigma}\mathcal{O}_F)^2$ we see that $H(\sigma) = \mathbf{1} \in C(F)_2$. We want to refine the group \mathcal{E}_S . First step is to note that H is well defined on

$$E_S = \mathcal{E}_S / K^{*2} \subset K^* / K^{*2}.$$

Let $C_S(K)$ denote the quotient of the ideal class group $C(K)$ by the subgroup which is generated by the ideal classes of the ramified prime ideals $P \subset \mathcal{O}_K$. We need:

Lemma 2.21. *There is a short exact sequence:*

$$\mathbf{1} \rightarrow U_S/U_S^2 \rightarrow E_S \rightarrow C_S(K)_2 \rightarrow \mathbf{1}.$$

Proof. Consider $y \in \mathcal{E}_S$. Then there is an \mathcal{O}_K -ideal $B \subset \mathcal{O}_K$ such that $\text{ord}_P y = \text{ord}_P B^2 = 2\text{ord}_P B$ at all $P \subset \mathcal{O}_K$, $P \notin S$. While B need not to be unique, it will define a unique $\text{cl}(B) \in C_S(K)_2$ with $\text{cl}(B^2) = \mathbf{1}$. If $y = x^2$, then B may be taken to be $x\mathcal{O}_K$. Thus $\text{cl}(B) = \mathbf{1} \in C_S(K)_2$. Hence we have an epimorphism

$$\epsilon : \mathcal{E}_S \rightarrow C_S(K)_2$$

which is trivial on $K^{*2} \subset \mathcal{E}_S$.

Now suppose $\epsilon(y) = \mathbf{1} \in C_S(K)_2$. Then, for $B \subset \mathcal{O}_K$ with $\text{ord}_P y = \text{ord}_P B^2$ at all $P \notin S$, there is an $x \in K^*$ for which $\text{ord}_P x = \text{ord}_P B$, at all $P \notin S$. Thus, $x^2 y^{-1} \in U_S$ or $y \in \text{im}(U_S/U_S^2 \rightarrow E_S)$. \square

Since $2\text{-rk } U_S/U_S^2 = \#S = \#\mathcal{R}(F/K) + n$ we conclude:

Corollary 2.22. *The 2-rank of E_S is $\#\mathcal{R}(F/K) + 2\text{-rk } C_S(K) + n$.*

In the previous section we have introduced the homomorphism :

$$H : \mathcal{E}_S \rightarrow C(F)_2.$$

We have the following:

Lemma 2.23. *If $y \in \mathcal{E}_S$, then $y \in \ker(H)$ if and only if there are $v \in \mathcal{O}_F^*$ and $x \in F^*$ for which $yv = x^2$.*

Proof. Assume $y \in \ker(H)$. Then for $y\mathcal{O}_F = A^2$ we can write $A = x\mathcal{O}_F$ for some $x \in F^*$. Thus $y\mathcal{O}_F = x^2\mathcal{O}_F$ and hence for some $v \in \mathcal{O}_F^*$ we have $yv = x^2$.

Conversely, if for some $v \in \mathcal{O}_F^*$, and $x \in F^*$ we have $yv = x^2$, then $yv\mathcal{O}_F = y\mathcal{O}_F = x^2\mathcal{O}_F$, hence $A = x\mathcal{O}_F$ and $H(y) = \mathbf{1} \in C(F)_2$. \square

Next we have:

Lemma 2.24. *If $v \in \mathcal{O}_F^*$, then there are elements $y \in \mathcal{E}_S$, $x \in F^*$ for which $yv = x^2$ if and only if $N(v) = v\bar{v} \in \mathcal{O}_K^{*2}$. That is, if and only if the norm of v is a square.*

Proof. First, if $yv = x^2$, then $N(yv) = y^2N(v) = (N(x))^2$ and hence $N(v)$ is a square. To see the converse, begin with the assumption $v\bar{v} = 1$. By Hilbert 90 we can write $v = x\bar{x}^{-1}$, for some $x \in F^*$. Then $\bar{x}x\bar{x}^{-1} = v$, that is $(x\bar{x})^{-1}v = (\bar{x}^{-1})^2$ and we can take $y = (x\bar{x})^{-1} \in K^*$. Let us show that if $yv = x^2$, then $y \in \mathcal{E}_S$. We have $y\mathcal{O}_F = yv\mathcal{O}_F = x^2\mathcal{O}_F = (x\mathcal{O}_F)^2$, whence $\text{ord}_P y = \text{ord}_P x^2 = 2\text{ord}_P x \equiv 0 \pmod{2}$ for all $P \notin S$. Thus $y \in \mathcal{E}_S$. If $N(v) = u^2$, $u \in \mathcal{O}_K^*$, then $N(u^{-1}v) = 1$. So there is $y \in \mathcal{E}_S$, $x \in K^*$ with $yu^{-1}v = x^2$. But $yu^{-1} \in \mathcal{E}_S$. \square

We have a uniqueness problem. Suppose $v \in \mathcal{O}_F^*$ with $N(v)$ a square. If $y, y_1 \in \mathcal{E}_S$, $x, x_1 \in F^*$ are such that $yv = x^2$ and $y_1v = x_1^2$, then $y_1y^{-1} = (x_1x^{-1})^2$. Then, either $y_1y^{-1} \in K^{*2}$ or y_1y^{-1} becomes a square in F^* . But that means $y_1y^{-1} = (a + b\sqrt{\sigma})^2 \in K^*$ with $a, b \in K$. Then $a^2 + b^2\sigma + 2ab\sqrt{\sigma} \in K^*$ so $ab = 0$, whence $a = 0$ or $b = 0$. Thus, either

$$y_1y^{-1} = a^2 \in K^{*2}, \text{ or}$$

$$y_1y^{-1} = b^2\sigma, \text{ hence } y_1y^{-1}\sigma = (b\sigma)^2 \in K^{*2}. \text{ Let us conclude:}$$

Lemma 2.25. *If $v\bar{v} \in \mathcal{O}_K^{*2}$ for $v \in \mathcal{O}_F^*$ and $yv = x^2$, $y_1v = x_1^2$, where $y, y_1 \in \mathcal{E}_S$, $x, x_1 \in F^*$, then either $y_1y^{-1} \in K^{*2}$ or $\sigma y_1y^{-1} \in K^{*2}$, but not both.*

Let us introduce the subgroup $\mathcal{E}_S^+ \subset \mathcal{E}_S$ consisting of those elements $y \in \mathcal{E}_S$ which are positive in each ordering of K with respect to which σ itself is positive. Let us note that if $y \in \mathcal{E}_S$, then there is a unit $u \in \mathcal{O}_K^*$ with $uy \in \mathcal{E}_S^+$ since K has units with independent signs. Since $H(u) = \mathbf{1} \in C(F)_2$ we can restrict our attention to \mathcal{E}_S^+ . Now, $K^{*2} \subset \mathcal{E}_S^+$ and, obviously, $\sigma \in \mathcal{E}_S^+$. Then, let us name:

$$\widetilde{\mathcal{O}}_K^* = \mathcal{O}_K^* \cap \mathcal{E}_S^+.$$

Still, $\mathcal{O}_K^{*2} \subset \widetilde{\mathcal{O}}_K^*$ and $2\text{-rk } \widetilde{\mathcal{O}}_K^*/\mathcal{O}_K^{*2} = n - k$. Let us now turn to:

$$E_S^+ = \mathcal{E}_S^+/K^{*2} \subset E_S.$$

We point out that $2\text{-rk } E_S = n + 2\text{-rk } C_S(K) + \#\mathcal{R}(F/K)$ and thus $2\text{-rk } E_S^+ = n - k + 2\text{-rk } C_S(K) + \#\mathcal{R}(F/K)$. We still have $\widetilde{\mathcal{O}}_K^*/\mathcal{O}_K^{*2} \subset E_S^+$ and the square class of $\sigma \in E_S^+$. Yet, the induced homomorphism $H : E_S^+ \rightarrow C(K)_2$ is trivial on the subgroup of E_S^+ generated by $\widetilde{\mathcal{O}}_K^*/\mathcal{O}_K^{*2}$ together with the square class of σ . Therefore we may as well factor out this subgroup resulting in a quotient group Π together with an induced homomorphism

$$\chi : \Pi \rightarrow C(K)_2.$$

Now there are two possibilities for the infinite elementary abelian 2-group Π :

Theorem 2.26. *If $\sigma \notin \mathcal{O}_K^*/\mathcal{O}_K^{*2}$, then*

$$2\text{-rk } \Pi = \#\mathcal{R}(F/K) + 2\text{-rk } C_S(K) - 1.$$

However, if $\sigma \in \mathcal{O}_K^/\mathcal{O}_K^{*2}$, then*

$$2\text{-rk } \Pi = \#\mathcal{R}(F/K) + 2\text{-rk } C_S(K).$$

Proof. By the definition of Π we have:

$$2\text{-rk } \Pi = 2\text{-rk } E_S^+ - 2\text{-rk } \left\langle \widetilde{\mathcal{O}}_K^*/\mathcal{O}_K^{*2}; \sigma \right\rangle.$$

Now, $2\text{-rk } E_S^+ = n - k + 2\text{-rk } C_S(K) + \#\mathcal{R}(F/K)$, while $2\text{-rk } \langle \widetilde{\mathcal{O}_K^*}/\mathcal{O}_K^{*2}; \sigma \rangle = n - k$ if $\sigma \in \mathcal{O}_K^*/\mathcal{O}_K^{*2}$, and $2\text{-rk } \langle \widetilde{\mathcal{O}_K^*}/\mathcal{O}_K^{*2}; \sigma \rangle = n - k + 1$ if $\sigma \notin \mathcal{O}_K^*/\mathcal{O}_K^{*2}$. Combining them, the lemma follows. \square

If $k = 0$, then σ is totally negative and $\mathcal{O}_F^+ = \mathcal{O}_F^*$. However if $k > 0$, then each ordering of K where σ is positive splits into a conjugate pair of orderings of F . Then F has $2k$ real orderings.

Lemma 2.27. *If $v \in \mathcal{O}_F^+$, then $N(v)$ is a square. If $v \in \mathcal{O}_F^*$ with $N(v)$ a square, then $uv \in \mathcal{O}_F^+$ for some $u \in \mathcal{O}_K^*$.*

Proof. If $v \in \mathcal{O}_F^+$, then $v\bar{v}$ is positive at every ordering of K where σ is positive. Indeed, let $\eta : F \rightarrow \mathbb{R}$ be such that $\eta(\sigma) > 0$. Then $\eta_{1,2} : F \rightarrow \mathbb{R}$ extend η and moreover $\eta(v\bar{v}) = \eta_1(v)\eta_2(v) > 0$ since $v \in \mathcal{O}_F^+$. Now all norms from F^* are positive with respect to all orderings of K where σ is negative. For, $\eta(N(a+b\sqrt{\sigma})) = \eta(a^2 - b^2\sigma) = [\eta(a)]^2 - \eta(\sigma)[\eta(b)]^2 > 0$ since $\eta(\sigma) < 0$.

So, for $v \in \mathcal{O}_F^+$, $N(v) = v\bar{v}$ is totally positive in \mathcal{O}_K^* and therefore a square. This ends the first part of our lemma.

For the second part, let $v \in \mathcal{O}_F^*$ be such that $N(v) = x^2$ is a square. Then:

$$0 < [\eta(x)]^2 = \eta(x^2) = \eta(N(v)) = \eta_1(v)\eta_2(v).$$

Hence, in each of a conjugate pair of orderings of F , v must have the same sign. Since \mathcal{O}_K^* contains units with independent signs there is a unit $u \in \mathcal{O}_K^*$ such that

$$\eta(u) > 0 \text{ if } \eta_1(v), \eta_2(v) > 0 \text{ and}$$

$$\eta(u) < 0 \text{ if } \eta_1(v), \eta_2(v) < 0.$$

Then $\eta_i(uv) = \eta(u)\eta_i(v) > 0$, $i = 1, 2$. Therefore $uv \in \mathcal{O}_F^+$.

\square

Thus, we shall consider only $\mathcal{O}_F^+/\mathcal{O}_F^{*2}$. Now if $v \in \mathcal{O}_F^+$ we have a $y \in \mathcal{E}_S$ with $yv = x^2 \in F^*$. Since $v \in \mathcal{O}_F^+$ we may conclude $y \in \mathcal{E}_S^+$. Then y is unique up to multiplication by a z^2 or σz^2 . Recall that Π is the quotient of E^+ by the subgroup generated by K^{*2} , $\widetilde{\mathcal{O}_K^*}$, and σ . Hence we have a well defined homomorphism

$$h : \mathcal{O}_F^+ \rightarrow \Pi.$$

Lemma 2.28. *The image of h is the kernel of χ .*

Proof. Recall that:

$$\mathcal{O}_F^+ \xrightarrow{h} \Pi \xrightarrow{\chi} C(K)_2$$

$$v \xrightarrow{yv=x^2} \text{cl}(y) \xrightarrow{y\mathcal{O}_F=A^2} \text{cl}(A)$$

Let $\text{cl}(y) \in \ker(\chi)$. Then $y\mathcal{O}_F = A^2$ with A principal, so we can write $A = x\mathcal{O}_F$. Hence $y\mathcal{O}_F = x^2\mathcal{O}_F$ or $yv = x^2$ for some $v \in \mathcal{O}_F^*$. Thus $h(v) = \text{cl}(y)$ or $\text{cl}(y) \in \text{im}(h)$.

On the other hand, if $h(v) = \text{cl}(y) \in \text{im}(h)$, then $yv = x^2$. Thus $y\mathcal{O}_F = (x\mathcal{O}_F)^2$ and $\chi(\text{cl}(y)) = \text{cl}(x\mathcal{O}_F) = \mathbf{1} \in C(K)_2$. Therefore $\text{cl}(y) \in \ker(\chi)$. \square

But we really need more information about h . Surely $\mathcal{O}_F^{*2} \subset \mathcal{O}_F^+$ and h is trivial on \mathcal{O}_F^{*2} . Namely, if $v^2 \in \mathcal{O}_F^+$ we can choose y to be 1. Thus we induce:

$$h : \mathcal{O}_F^+/\mathcal{O}_F^{*2} \rightarrow \Pi.$$

Lemma 2.29. *There is a natural homomorphism*

$$\widetilde{\mathcal{O}_K^*}/\mathcal{O}_K^{*2} \rightarrow \mathcal{O}_F^+/\mathcal{O}_F^{*2}$$

which is a monomorphism if $\sigma \notin \mathcal{O}_K^/\mathcal{O}_K^{*2}$ and whose kernel is cyclic of order 2 generated by the square class of σ if $\sigma \in \mathcal{O}_K^*/\mathcal{O}_K^{*2}$.*

Proof. Note that if $u \in \widetilde{\mathcal{O}_K^*}$, then $u \in \mathcal{O}_F^+$ also, since only the real embeddings of K with respect to which σ is positive split into two real embeddings of F . Thus we send the square class of $\tau \in \widetilde{\mathcal{O}_K^*}/\mathcal{O}_K^{*2}$ to the square class of $\tau \in \mathcal{O}_F^+/\mathcal{O}_F^{*2}$.

Let $\tau \in \widetilde{\mathcal{O}_K^*}/\mathcal{O}_K^{*2}$ be such that τ is in the kernel of our homomorphism. Then $\tau \in \mathcal{O}_F^{*2}$ with $\tau = (a + b\sqrt{\sigma})^2 = a^2 + \sigma b^2 + 2ab\sqrt{\sigma} \in \mathcal{O}_K^*$, so $ab = 0$. Thus: $\tau = a^2$ or $\tau = b^2\sigma$.

If $\sigma \in \mathcal{O}_K^*/\mathcal{O}_K^{*2}$, then $\tau = a^2$ means τ is trivial in $\widetilde{\mathcal{O}_K^*}/\mathcal{O}_K^{*2}$, and $\tau = b^2\sigma$ means $\tau = \sigma$ in $\widetilde{\mathcal{O}_K^*}/\mathcal{O}_K^{*2}$. Hence, the kernel of our homomorphism is cyclic of order 2 generated by the square class of σ .

If $\sigma \notin \widetilde{\mathcal{O}_K^*}/\mathcal{O}_K^{*2}$, then $\tau = a^2$ means τ is trivial in $\widetilde{\mathcal{O}_K^*}/\mathcal{O}_K^{*2}$, and $\tau = b^2\sigma$ is impossible. Thus, in this case, our homomorphism is actually a monomorphism. \square

Lemma 2.30. (i) If $\sigma \notin \mathcal{O}_K^*/\mathcal{O}_K^{*2}$, then the sequence

$$\mathbf{1} \rightarrow \widetilde{\mathcal{O}_K^*}/\mathcal{O}_K^{*2} \rightarrow \mathcal{O}_F^+/\mathcal{O}_F^{*2} \xrightarrow{h} \ker(\chi) \rightarrow \mathbf{1}$$

is exact.

(i) If $\sigma \in \mathcal{O}_K^*/\mathcal{O}_K^{*2}$, then the sequence

$$\mathbf{1} \rightarrow C_2 \rightarrow \widetilde{\mathcal{O}_K^*}/\mathcal{O}_K^{*2} \rightarrow \mathcal{O}_F^+/\mathcal{O}_F^{*2} \xrightarrow{h} \ker(\chi) \rightarrow \mathbf{1}$$

is exact.

Proof. Take $v \in \mathcal{O}_F^+$ and write $yv = x^2$. Suppose we could write $y = uz^2\sigma$ or $y = uz^2$, i.e. $y \in \ker(h)$, for some $u \in \widetilde{\mathcal{O}_K^*}$, $z \in K^*$.

If $y = uz^2$, then $yv = uvz^2 = x^2$ and hence $uv = (x/z)^2 \in F^{*2}$. Thus $v \in \mathcal{O}_F^+$ lies in $\ker(h)$, and in $\mathcal{O}_F^+/\mathcal{O}_F^{*2}$, v lies in the image of the natural homomorphism 2.29.

If $y = uz^2\sigma$, then $yv = uz^2(\sqrt{\sigma})^2v = x^2$ and $uv = (xz^{-1}/\sqrt{\sigma})^2 \in F^{*2}$. Again v lies in the image of the natural homomorphism 2.29.

On the other hand, if v lies in this image, then $h(v) = \mathbf{1} \in \Pi$. □

Note that in our context, $\text{Gal}(F/K) = C_2$ acts as an automorphism of period 2 on \mathcal{O}_F^* , the group of units in F . We define, then, the Artin-Tate cohomology groups

$$H^0(C_2; \mathcal{O}_F^*) \text{ and } H^1(C_2; \mathcal{O}_F^*).$$

First, by definition:

$$H^0(C_2; \mathcal{O}_F^*) = \mathcal{O}_K^*/N(\mathcal{O}_F^*) = \text{coker}(N).$$

Thus each $u \in \mathcal{O}_K^*$ defines an element $\text{cl}(u) \in H^0(C_2; \mathcal{O}_F^*)$ which is trivial if and only if $u = N(v) = v\bar{v}$ for some $v \in \mathcal{O}_F^*$.

To define $H^1(C_2; \mathcal{O}_F^*)$ we turn to $\ker(N)$. Thus, $v \in \mathcal{O}_F^*$ defines a cohomology class $\text{cl}(v) \in H^1(C_2; \mathcal{O}_F^*)$ if and only if $N(v) = 1$. Then, $\text{cl}(v)$ is trivial if and only if $v = w\bar{w}^{-1}$ for some $w \in \mathcal{O}_F^*$. Both $H^0(C_2; \mathcal{O}_F^*)$ and $H^1(C_2; \mathcal{O}_F^*)$ are elementary abelian 2-groups.

Note that $-1 \in \mathcal{O}_F^*$ always defines a cohomology class $\text{cl}(-1) \in H^1(C_2; \mathcal{O}_F^*)$. This cohomology class is trivial if and only if there is a unit $w \in \mathcal{O}_F^*$ for which $w\bar{w}^{-1} = -1$, or $\bar{w} = -w$. When we might find such a skew unit? We can write $w = \alpha + \beta\sqrt{\sigma} \in \mathcal{O}_F^*$ for unique $\alpha, \beta \in K^*$. Since $\bar{w} = -w$ we have $\alpha = 0$. Thus, $\beta\sqrt{\sigma} \in \mathcal{O}_F^*$. Then $N(\beta\sqrt{\sigma}) = -\beta^2\sigma \in \mathcal{O}_K^*$. Hence a square class $\sigma \in \mathcal{O}_K^*/\mathcal{O}_K^{*2}$. We have proved:

Lemma 2.31. *In $H^1(C_2; \mathcal{O}_F^*)$ the $\text{cl}(-1)$ is trivial if and only if $\sigma \in \mathcal{O}_K^*/\mathcal{O}_K^{*2}$.*

In general we use $H^1(C_2; \mathcal{O}_F^*)/\text{cl}(-1)$ to denote the quotient of $H^1(C_2; \mathcal{O}_F^*)$ by the subgroup of at most order 2 which is generated by $\text{cl}(-1)$. Our task is to define a natural epimorphism

$$\rho : \mathcal{O}_F^+/\mathcal{O}_F^{*2} \rightarrow H^1(C_2; \mathcal{O}_F^*)/\text{cl}(-1) \rightarrow \mathbf{1}$$

whose kernel is the image of the natural homomorphism 2.29.

We begin with $v \in \mathcal{O}_F^+$. Then $N(v) = u^2$, $u \in \mathcal{O}_K^*$, and $N(u^{-1}v) = u^{-2}N(v) = 1$. Hence, $u^{-1}v$ defines $\text{cl}(u^{-1}v) \in H^1(C_2; \mathcal{O}_F^*)$. Carefully note that $(-u)^2 = N(v)$ also, and $\text{cl}(-u^{-1}v) = \text{cl}(-1)\text{cl}(u^{-1}v)$. Thus we obtain a well defined homomorphism:

$$\eta : \mathcal{O}_F^+ \rightarrow H^1(C_2; \mathcal{O}_F^*)/\text{cl}(-1).$$

This is an epimorphism. For, if $v_1 \in \mathcal{O}_F^*$ with $N(v_1) = 1$, then by Lemma 2.27 we can choose a unit $u \in \mathcal{O}_K^*$ so that $uv_1 \in \mathcal{O}_F^+$. Then $N(uv_1) = u^2$ and $u^{-1}uv_1 = v_1$ so $\eta(uv_1) = \text{cl}(v_1) \in H^1(C_2; \mathcal{O}_F^*)/\text{cl}(-1)$.

Let us check that η is trivial on $\mathcal{O}_F^{*2} \subset \mathcal{O}_F^+$. For $v^2 \in \mathcal{O}_F^{*2}$ we have $N(v^2) = [N(v)]^2$. Taking $u = N(v)$ we get $u^{-1}v^2 = v^{-1}\bar{v}^{-1}v^2 = v\bar{v}^{-1}$, hence $\eta(v^2)$ is trivial. Thus we arrive at the epimorphism: $\rho : \mathcal{O}_F^+/\mathcal{O}_F^{*2} \rightarrow H^1(C_2; \mathcal{O}_F^*)/\text{cl}(-1)$.

Let us next assume for $v \in \mathcal{O}_F^+$ that $\eta(v)$ is trivial in $H^1(C_2; \mathcal{O}_F^*)/\text{cl}(-1)$, i.e. $v \in \ker(\eta)$. Since $N(v) = u^2$, for some $u \in \mathcal{O}_K^*$ we get $\text{cl}(u^{-1}v) = \mathbf{1} \in H^1(C_2; \mathcal{O}_F^*)$. Thus $w\bar{w}^{-1} = u^{-1}v$ for some $w \in \mathcal{O}_F^+$. We write: $w\bar{w}\bar{w}^{-2} = u^{-1}v$ or $uw\bar{w} = vw^2$. Then, $uw\bar{w} \in \mathcal{O}_K^*$ but since $vw^2 \in \mathcal{O}_F^+$ it follows that $uw\bar{w} \in \widetilde{\mathcal{O}}_K^*$. Hence, the square class of $v \in \mathcal{O}_F^+/\mathcal{O}_F^{*2}$ lies in the image of the natural homomorphism 2.29.

Conversely, if $v \in \mathcal{O}_F^+$ assume $v = uw^2$ for some $u \in \widetilde{\mathcal{O}}_K^*$, $w \in \mathcal{O}_F^*$. Then, $N(v) = u^2 [N(w)]^2$. Thus we consider the class of

$$u^{-1}w^{-1}\bar{w}^{-1}v = u^{-1}w^{-1}\bar{w}^{-1}uw^2 = w\bar{w}^{-1}.$$

Hence, when $v \in \mathcal{O}_F^+/\mathcal{O}_F^{*2}$ lies in the image of the natural homomorphism 2.29 we find $\eta(v) = \mathbf{1} \in H^1(C_2; \mathcal{O}_F^*)$. Using, in addition, Lemma 2.31 and Lemma 2.30, we obtain the following:

Theorem 2.32. *We have:*

$$\ker(\chi) \cong H^1(C_2; \mathcal{O}_F^*)/\text{cl}(-1).$$

Thus, if $\sigma \notin \mathcal{O}_K^*/\mathcal{O}_K^{*2}$, then:

$$1 + 2\text{-rk ker}(\chi) = 2\text{-rk H}^1(C_2; \mathcal{O}_F^*),$$

while if $\sigma \in \mathcal{O}_K^*/\mathcal{O}_K^{*2}$, then:

$$2\text{-rk ker}(\chi) = 2\text{-rk H}^1(C_2; \mathcal{O}_F^*).$$

From [4], Proposition 5.2, we know:

$$1 + 2\text{-rk H}^0(C_2; \mathcal{O}_F^*) = n - k + 2\text{-rk H}^1(C_2; \mathcal{O}_F^*). \quad (2.2)$$

Let us combine this formula with Theorem 2.32 and obtain:

Corollary 2.33. (i) If $\sigma \notin \mathcal{O}_K^*/\mathcal{O}_K^{*2}$, then:

$$2\text{-rk H}^0(C_2; \mathcal{O}_F^*) = n - k + 2\text{-rk ker}(\chi).$$

(ii) If $\sigma \in \mathcal{O}_K^*/\mathcal{O}_K^{*2}$, then:

$$1 + 2\text{-rk H}^0(C_2; \mathcal{O}_F^*) = n - k + 2\text{-rk ker}(\chi).$$

Now we are able to prove the following:

Lemma 2.34. (i) If $\sigma \notin \mathcal{O}_K^*/\mathcal{O}_K^{*2}$, then:

$$0 \leq 2\text{-rk ker}(\chi) \leq k.$$

(ii) If $\sigma \in \mathcal{O}_K^*/\mathcal{O}_K^{*2}$, then:

$$1 \leq 2\text{-rk ker}(\chi) \leq k + 1.$$

Proof. Since $2\text{-rk } \mathcal{O}_K^+/\mathcal{O}_K^{*2} = n$, and $\mathcal{O}_K^{*2} \subset \text{im}(\text{N})$ it follows that $\text{H}^0(C_2; \mathcal{O}_F^*) = \text{coker}(\text{N})$ must have $2\text{-rk H}^0(C_2; \mathcal{O}_F^*) \leq n$. If $\sigma \notin \mathcal{O}_K^*/\mathcal{O}_K^{*2}$, then by Corollary 2.33(i) we have $2\text{-rk H}^0(C_2; \mathcal{O}_F^*) = n - k + 2\text{-rk ker}(\chi) \leq n$. Therefore $0 \leq 2\text{-rk ker}(\chi) \leq k$.

Next, recall formula 2.2. Then, $2\text{-rk } H^0(C_2; \mathcal{O}_F^*) \geq n - k$. Namely, if a unit $u \in \mathcal{O}_K^*$ is negative with respect to at least one ordering of K where σ is also negative, then u cannot be a norm from F/K and there are $n - k$ orderings of K at which σ is negative. It follows that $2\text{-rk } H^1(C_2; \mathcal{O}_F^*) \geq 1$ in all cases. But if $\sigma \in \mathcal{O}_K^*/\mathcal{O}_K^{*2}$ it must follow that, by Theorem 2.32, $2\text{-rk } \ker(\chi) \geq 1$. Then by Corollary 2.33(ii) we have $1 \leq 2\text{-rk } \ker(\chi) \leq k + 1$. \square

There is a natural homomorphism:

$$i_* : C(K) \rightarrow C(F).$$

This assigns to the ideal class of a fractional \mathcal{O}_K -ideal $A \subset \mathcal{O}_K$ the ideal class in $C(F)$ of the fractional \mathcal{O}_F -ideal $A\mathcal{O}_F \subset F$. We may restrict this to:

$$i_* : C(K)_2 \rightarrow C(F)_2,$$

We wish to relate the homomorphism i_* to the homomorphism $\chi : \Pi \rightarrow C(F)_2$.

First we return to the subgroup of square classes $E^+ \subset K^*/K^{*2}$, defined by $z \in E^+$ if and only if z is totally positive and $\text{ord}_P z \equiv 0 \pmod{2}$ at every prime ideal $P \subset \mathcal{O}_K$. We already noted the natural isomorphism 2.1

$$C(K)_2 \cong E^+.$$

Recall that if the \mathcal{O}_K -ideal A represents $\text{cl}(A) \in C(K)_2$, then to $\text{cl}(A)$ we assign the square class $z \in E^+$ of the totally positive generator of A^2 .

Lemma 2.35. *If $\sigma \in K^*/K^{*2}$, then $K(\sqrt{\sigma})/K$ is unramified if and only if $\sigma \in E^+$.*

Proof. First, it is clear that if $K(\sqrt{\sigma})/K$ is unramified, then $\sigma \in E^+ \subset K^*/K^{*2}$. Second, from Class Field Theory we know that the maximum number of unramified independent quadratic extensions of K is equal to $2\text{-rk } C(K) = 2\text{-rk } C(K)_2 = 2\text{-rk } E^+$. \square

Now we examine $\ker(i_*) \subset C(K)_2$. First assume that $K(\sqrt{\sigma})/K$ has at least one ramified prime. Then by Lemma 2.35 $\sigma \notin E^+$. We know that $\mathcal{O}_K^*/\mathcal{O}_K^{*2} \cap E^+$ is trivial. Thus $E^+ \subset E_S$ and the quotient onto Π gives us a monomorphism $I_* : C(K)_2 \rightarrow \Pi$. Furthermore, the composition:

$$C(K)_2 \xrightarrow{I_*} \Pi \xrightarrow{\chi} C(F)_2$$

is exactly $i_* : C(K)_2 \rightarrow C(F)_2$. Thus $\ker(i_*) \subset \ker(\chi)$.

If $K(\sqrt{\sigma})/K$ is unramified the situation is quite different! In this case, $S \subset \Omega_K$ consists only of the real infinite primes. Thus $C_S(K) = C(K)$ and $E_S = E$. But we must be careful! Since now $\sigma \in E^+$, we see that I_* will have kernel cyclic of order 2, but it will be onto. Therefore in the ramified case we have:

$$\begin{array}{ccccccc} & & & C(F)_2 & & & \\ & & & \uparrow & \swarrow \chi & & \\ & & & i_* & & & \\ 1 & \longrightarrow & C_2 & \longrightarrow & C(K)_2 & \xrightarrow{I_*} & \Pi \longrightarrow 1 \end{array}$$

and:

$$2\text{-rk } \ker(i_*) = 1 + 2\text{-rk } \ker(\chi) \quad (2.3)$$

Although F may not be totally real, we may still ask if it contains units with independent signs. If $K(\sqrt{\sigma})/K$ is a CM-extension (i.e. σ is totally negative) then $\mathcal{O}_F^+ = \mathcal{O}_F^*$ by default.

Corollary 2.36. *If $\sigma \notin \mathcal{O}_K^*/\mathcal{O}_K^{*2}$ then the following are equivalent:*

1. \mathcal{O}_F^* contains units with independent signs.
2. $\ker(\chi)$ is trivial.
3. $2\text{-rk } H^0(C_2; \mathcal{O}_F^*) = n - k$.
4. Every unit of \mathcal{O}_K^* which is positive at every ordering of K with respect to which σ is negative, is the norm of a unit in \mathcal{O}_F^* .
5. $H^1(C_2; \mathcal{O}_F^*)$ is cyclic of order 2 (generated by $\text{cl}(-1)$).

Proof. Note that $2 \Leftrightarrow 3$ by 2.33 which says:

$$2\text{-rk } H^0(C_2; \mathcal{O}_F^*) = n - k + 2\text{-rk } \ker(\chi).$$

Also, $3 \Leftrightarrow 5$ by 2.32 which says:

$$1 + 2\text{-rk } H^0(C_2; \mathcal{O}_F^*) = n - k + 2\text{-rk } H^1(C_2; \mathcal{O}_F^*).$$

Let us prove that $4 \Rightarrow 1$. Let $\eta_1, \eta_2, \dots, \eta_k : K \rightarrow \mathbb{R}$ be the orderings of K with respect to which σ is positive. They extend (split) to $\eta_1^{1,2}, \dots, \eta_k^{1,2} : F \rightarrow \mathbb{R}$. Choose one of the real embeddings of F , say η_1^1 . Since K has units with independent signs we can find $v \in \mathcal{O}_K^*$ such that:

$$\begin{aligned} \eta_1(v) &< 0, \\ \eta_i(v) &> 0 \text{ if } i = 2, \dots, k, \\ \eta_j(v) &> 0 \text{ if } j = k + 1, \dots, n. \end{aligned}$$

So v is a unit which is positive whenever σ is negative. Hence there exists $V \in \mathcal{O}_F^*$ so that $v = V\bar{V}$. Then:

$$\begin{aligned} \eta_1(v) &= \eta_1^1(V)\eta_1^2(V) < 0, \\ \eta_i(v) &= \eta_i^1(V)\eta_i^2(V) > 0 \text{ if } i = 2, \dots, k. \end{aligned}$$

Suppose that $\eta_1^1(V) < 0$, otherwise we can replace V with $-V$. Now choose $u \in \mathcal{O}_K^*$ such that:

$$\begin{aligned} \eta_1(u) &> 0, \\ \text{if } \eta_i^1(V), \eta_i^2(V) &> 0, \text{ then } \eta_i(u) > 0, \\ \text{if } \eta_i^1(V), \eta_i^2(V) &< 0, \text{ then } \eta_i(u) < 0, \text{ where } i = 2, \dots, k. \end{aligned}$$

Then:

$$\begin{aligned} \eta_1^1(uV) &= \eta_1(u)\eta_1^1(V) < 0, \\ \eta_1^2(uV) &= \eta_1(u)\eta_1^2(V) > 0, \text{ and} \\ \eta_i^s(uV) &= \eta_i(u)\eta_i^s(V) > 0 \text{ for } i = 2, \dots, k, s = 1, 2. \end{aligned}$$

Therefore, F has units with independent signs.

Now we will show that $1 \Rightarrow 4$. Since F has units with independent signs, there is a unit $V \in \mathcal{O}_F^*$ so that: $\eta_1^1(V)\eta_1^2(V) < 0$ and $\eta_i^1(V)\eta_i^2(V) > 0$ for $i = 2, \dots, k$. Let $v = V\bar{V} \in \mathcal{O}_K^*$. Then:

$$\eta_1(v) = \eta_1^1(V)\eta_1^2(V) < 0,$$

$$\eta_i(v) = \eta_i^1(V)\eta_i^2(V) > 0 \text{ for } i = 2, \dots, k,$$

$$\eta_j(v) = \eta_j(V\bar{V}) = \eta_j(a^2 - \sigma b^2) = [\eta_j(a)]^2 - \eta_j(\sigma)[\eta_j(b)]^2 > 0 \text{ for } j = k+1, \dots, n.$$

Hence K has units with independent signs. Actually we have shown that \mathcal{O}_K^* contains units (which are positive whenever σ is negative) with independent signs that are norms from \mathcal{O}_F^* . Hence any unit (positive whenever σ is negative) in \mathcal{O}_K^* can be written as the product of a totally positive unit in \mathcal{O}_K^* with a unit (positive whenever σ is negative) that is a norm from \mathcal{O}_F^* . Since K is totally real, any totally positive unit is a square, hence a norm from \mathcal{O}_F^* .

Finally, $3 \Leftrightarrow 4$ is clear by the definition of $H^0(C_2; \mathcal{O}_F^*)$.

□

If $\sigma \in \mathcal{O}_K^*/\mathcal{O}_K^{*2}$, then we can prove similarly the following:

Corollary 2.37. *If $\sigma \in \mathcal{O}_K^*/\mathcal{O}_K^{*2}$ then the following are equivalent:*

1. \mathcal{O}_F^* contains units with independent signs.
2. $\ker(\chi)$ is cyclic of order 2.
3. $2\text{-rk } H^0(C_2; \mathcal{O}_F^*) = n - k$.
4. Every unit of \mathcal{O}_K^* which is positive at every ordering of K with respect to which σ is negative, is the norm of a unit in \mathcal{O}_F^* .
5. $H^1(C_2; \mathcal{O}_F^*)$ is cyclic of order 2.

If $\mathcal{A}(K)$, $\mathcal{A}(F)$ are the abelian groups of all fractional \mathcal{O}_K -, respectively \mathcal{O}_F -ideals, we can define a norm of ideals homomorphism

$$N : \mathcal{A}(F) \rightarrow \mathcal{A}(K).$$

It is enough to consider prime ideals. If $\mathcal{P} \subset \mathcal{O}_F$ is a prime ideal in \mathcal{O}_F , then $\mathcal{P}|P$ for a unique prime ideal $P \subset \mathcal{O}_K$. If P is either split or ramified, then $N(\mathcal{P}) = P$, while if P is inert, then $N(\mathcal{P}) = P^2$. We define N so that for $x \in F$ we have $N(x\mathcal{O}_F) = N(x)\mathcal{O}_K$. In any case there is an induced homomorphism of ideal class groups

$$\mathcal{N} : C(F) \rightarrow C(K).$$

Let us prove the following:

Proposition 2.38. *The image of χ lies in the kernel of \mathcal{N} .*

Proof. Let $y \in K^*$ be an element for which $\text{ord}_P y \equiv 0 \pmod{2}$ at all unramified prime ideals $P \subset \mathcal{O}_K$. Then we write $y\mathcal{O}_F = A^2$. We have the following cases:

(i) If P is inert, then:

$$\text{ord}_{\mathcal{P}} A = \frac{1}{2} \text{ord}_{\mathcal{P}} A^2 = \frac{1}{2} \text{ord}_{\mathcal{P}\mathcal{O}_F} y\mathcal{O}_F = \frac{1}{2} \text{ord}_{\mathcal{P}} y, \text{ hence } N(\mathcal{P})^{\text{ord}_{\mathcal{P}} A} = P^{\text{ord}_{\mathcal{P}} y}.$$

(ii) If P is ramified, then $\text{ord}_{\mathcal{P}} A = \text{ord}_{\mathcal{P}} y$, and hence $N(\mathcal{P})^{\text{ord}_{\mathcal{P}} A} = P^{\text{ord}_{\mathcal{P}} y}$.

(iii) If P splits, then $2\text{ord}_{\mathcal{P}} A = \text{ord}_{\mathcal{P}} y$.

Therefore:

$$N(A) = N\left(\prod_{\mathcal{P}|A} \mathcal{P}^{\text{ord}_{\mathcal{P}} A}\right) = \prod_{\mathcal{P}|A} N(\mathcal{P})^{\text{ord}_{\mathcal{P}} A} = \prod_{P|y\mathcal{O}_K} P^{\text{ord}_{\mathcal{P}} y} = y\mathcal{O}_K.$$

Since $\chi(y) = \text{cl}(A) \in C(F)_2$, we see that:

$$\mathcal{N}(\chi(y)) = \mathcal{N}(\text{cl}(A)) = \text{cl}(N(A)) = \text{cl}(y\mathcal{O}_K) = \mathbf{1} \in C(K), \text{ hence } \text{im}(\chi) \subseteq \ker(\mathcal{N}).$$

□

Referring to the exact hexagon 1.18, let us prove the following

Theorem 2.39. *If the class number $h(K)$ is odd, then*

$$2\text{-rk coker}(\chi) = 2\text{-rk ker}(i_0).$$

Proof. Since $h(K)$ is odd at least one finite prime ramifies and the natural homomorphism $i_* : C(K) \rightarrow C(F)$ has trivial kernel. Hence, by Proposition 7.1 [4], $j_1 : R^0(F/K) \rightarrow H^1(C_2; C(F))$ is an epimorphism. Furthermore, $H^1(C_2; C(F)) \cong C(F)/C(F)^2$ and thus $2\text{-rk } C(F)_2 = 2\text{-rk } C(F)/C(F)^2 = 2\text{-rk } H^1(C_2; C(F))$. We also now (see Proposition 4.2 [4]) that $2\text{-rk } R^0(F/K) = n - k + \#\mathcal{R}(F/K) - 1$. Thus from the exact hexagon we have:

$$\begin{aligned} 2\text{-rk } R^0(F/K) &= 2\text{-rk } \ker(j_1) + 2\text{-rk } \text{im}(j_1) \\ &= 2\text{-rk } \text{im}(i_0) + 2\text{-rk } H^1(C_2; C(F)) \\ &= 2\text{-rk } H^0(C_2; \mathcal{O}_F^*) - 2\text{-rk } \ker(i_0) + 2\text{-rk } H^1(C_2; C(F)) \end{aligned}$$

Therefore:

$$n - k + \#\mathcal{R}(F/K) - 1 - 2\text{-rk } H^0(C_2; \mathcal{O}_F^*) + 2\text{-rk } \ker(i_0) = 2\text{-rk } H^1(C_2; C(F)).$$

Now, if $\sigma \notin \mathcal{O}_K^*/\mathcal{O}_K^{*2}$ then we know by Corollary 2.33 that $2\text{-rk } H^0(C_2; \mathcal{O}_F^*) = n - k + 2\text{-rk } \ker(\chi)$. Therefore $2\text{-rk } H^1(C_2; C(F)) = \#\mathcal{R}(F/K) - 2\text{-rk } \ker(\chi) - 1 + 2\text{-rk } \ker(i_0)$. But we also know that in this case, see Lemma 2.26, that $2\text{-rk } \Pi = \#\mathcal{R}(F/K) - 1$. Hence we have $\#\mathcal{R}(F/K) - 2\text{-rk } \ker(\chi) - 1 = 2\text{-rk } \text{im}(\chi)$. Thus $2\text{-rk } \text{coker}(\chi) = 2\text{-rk } \ker(i_0)$.

Now we must consider the case $\sigma \in \mathcal{O}_K^*/\mathcal{O}_K^{*2}$. Again, by Corollary 2.33 we have $1 + 2\text{-rk } H^0(C_2; \mathcal{O}_F^*) = n - k + 2\text{-rk } \ker(\chi)$. Still $2\text{-rk } R^0(F/K) = n - k + \#\mathcal{R}(F/K) - 1$. Referring to the exact hexagon we obtain:

$$2\text{-rk } H^1(C_2; C(F)) = \#\mathcal{R}(F/K) - 2\text{-rk } \ker(\chi) + 2\text{-rk } \ker(i_0).$$

This time Lemma 2.26 gives us that $2\text{-rk } \Pi = \#\mathcal{R}(F/K)$. Thus $2\text{-rk } \text{im}(\chi) = \#\mathcal{R}(F/K) - 2\text{-rk } \ker(\chi)$ and again we obtain:

$$2\text{-rk } \text{coker}(\chi) = 2\text{-rk } \ker(i_0).$$

□

We have the following:

Corollary 2.40. *If $h(K)$ is odd, then the homomorphism χ is an epimorphism if and only if the homomorphism i_0 is a monomorphism.*

We can restate Corollary 2.40 as follows:

Remark 2.41. *If $h(K)$ is odd, then the homomorphism χ is an epimorphism if and only if each unit in \mathcal{O}_K^* which is a norm from F/K is also the norm of a unit in \mathcal{O}_F^* .*

We know that possibly $2\text{-rk } H^0(C_2; \mathcal{O}_F^*) = n - k$. But that means that a unit in \mathcal{O}_K^* fails to be the norm of a unit in \mathcal{O}_F^* if and only if it is negative with respect to at least one ordering of K with respect to which σ is also negative. However, such a unit in \mathcal{O}_K^* cannot even be a field norm from F/K . Therefore:

Proposition 2.42. *If $h(K)$ is odd and $2\text{-rk } H^0(C_2; \mathcal{O}_F^*) = n - k$, then i_0 is a monomorphism.*

Recall, see Corollary 2.36, that if $\sigma \notin \mathcal{O}_K^*/\mathcal{O}_K^{*2}$, then $\ker(\chi)$ is trivial if and only if $2\text{-rk } H^0(C_2; \mathcal{O}_F^*) = n - k$ if and only if \mathcal{O}_F^* contains units with independent signs. Also, if $\sigma \in \mathcal{O}_K^*/\mathcal{O}_K^{*2}$, then $2\text{-rk } H^0(C_2; \mathcal{O}_F^*) = n - k$ if and only if $2\text{-rk } \ker(\chi) = 1$ if and only if \mathcal{O}_F^* contains units with independent signs (by Corollary 2.37). Thus we obtain:

Corollary 2.43. *If $h(K) \equiv 1 \pmod{2}$ and \mathcal{O}_F^* contains units with independent signs, then:*

- (i) $2\text{-rk } C(F)_2 = \#\mathcal{R}(F/K) - 1$,
- (ii) If $\sigma \notin \mathcal{O}_K^*/\mathcal{O}_K^{*2}$, then $\Pi \cong C(F)_2$,
- (iii) If $\sigma \in \mathcal{O}_K^*/\mathcal{O}_K^{*2}$, then $\ker(\chi)$ is cyclic of order 2.

Since K has units with independent signs, we see that $h(K) = h^+(K) \equiv 1 \pmod{2}$. Hence $C(F)_2 = H^0(C_2; C(F))$. Thus, the homomorphism d_0 can be regarded as $d_0 : C(F)_2 \rightarrow H^0(C_2; \mathcal{O}_F^*)$. We showed, see Theorem 2.32, that $\ker(\chi) \cong H^1(C_2; \mathcal{O}_F^*)/\text{cl}(-1)$. Then we can see that there is an epimorphism

$$\rho : H^1(C_2; \mathcal{O}_F^*) \rightarrow \ker(\chi)$$

and $\ker(\rho)$ is the cyclic subgroup of $H^1(C_2; \mathcal{O}_F^*)$ generated by $\text{cl}(-1)$.

Theorem 2.44. *If K is a totally real number field with $h^+(K) \equiv 1 \pmod{2}$ then for $F/K = K(\sqrt{\sigma})/K$ there is an associated exact sequence:*

$$\begin{aligned} \mathbf{1} \rightarrow \text{cl}(-1) \rightarrow H^1(C_2; \mathcal{O}_F^*) \xrightarrow{\rho} \Pi \xrightarrow{\chi} C(F)_2 \xrightarrow{d_0} \\ \xrightarrow{d_0} H^0(C_2; \mathcal{O}_F^*) \xrightarrow{i_0} R^0(F/K) \rightarrow C(F)/C(F)_2 \rightarrow \mathbf{1}. \end{aligned}$$

Proof. From the exact hexagon we know $\text{im}(d_0) = \ker(i_0)$. Also Theorem 2.39 gives: $2\text{-rk im}(\chi) + 2\text{-rk ker}(i_0) = 2\text{-rk } C(F)_2 = 2\text{-rk im}(\chi) + 2\text{-rk im}(d_0)$ and also: $2\text{-rk } C(F)_2 = 2\text{-rk im}(d_0) + 2\text{-rk ker}(d_0)$, hence $2\text{-rk im}(\chi) = 2\text{-rk ker}(d_0)$, whence $\text{im}(\chi) \cong \ker(d_0)$, since both are elementary 2-abelian groups. Thus to show that $\text{im}(\chi) = \ker(d_0)$ we only need to verify that $\text{im}(\chi) \subseteq \ker(d_0)$. An element in $\text{im}(\chi)$ is represented by a fractional \mathcal{O}_F -ideal $A \subset F$ for which $A = \bar{A}$. Thus $\bar{A} = xA$, ($x = 1$), so $x\bar{x} = 1$ and thus: $d_0(\text{cl}(A)) = \text{cl}(x\bar{x}) = \text{cl}(1) \in H^0(C_2; \mathcal{O}_F^*)$. Therefore, $\text{im}(\chi) \subseteq \ker(d_0)$ and we are done. \square

The goal is to express the 2-rank of the class group $C(F)$ in terms of the homomorphism:

$$\chi : \Pi \rightarrow C(F)_2.$$

We recall that $\#\mathcal{R}(F/K) \geq 1$ and (see [4] 4.2)

$$2\text{-rk } R^0(F/K) = n - k + \#\mathcal{R}(F/K) - 1.$$

Also we have $H^1(C_2; C(F)) \cong C(F)/C(F)_2$, while $j_1 : R^0(F/K) \rightarrow H^1(C_2; C(F))$ is onto. Thus from the exact hexagon we write:

$$2\text{-rk im}(i_0) = 2\text{-rk } H^0(C_2; \mathcal{O}_F^*) - 2\text{-rk } \ker(i_0).$$

Hence:

$$\begin{aligned} 2\text{-rk } C(F)/C(F)_2 &= 2\text{-rk } H^1(C_2; C(F)) = 2\text{-rk im}(j_1) \\ &= 2\text{-rk } R^0(F/K) - 2\text{-rk } \ker(j_1) \\ &= 2\text{-rk } R^0(F/K) - 2\text{-rk im}(i_0) \\ &= n - k + \#\mathcal{R}(F/K) - 1 - 2\text{-rk } H^0(C_2; \mathcal{O}_F^*) + 2\text{-rk } \ker(i_0) \end{aligned}$$

We already showed (see 2.39) that:

$$2\text{-rk coker}(\chi) = 2\text{-rk } \ker(i_0),$$

while (see 2.33):

$$2\text{-rk } H^0(C_2; \mathcal{O}_F^*) = n - k + 2\text{-rk } \ker(\chi) \text{ if } \sigma \notin \mathcal{O}_K^*/\mathcal{O}_K^{*2}$$

and

$$1 + 2\text{-rk } H^0(C_2; \mathcal{O}_F^*) = n - k + 2\text{-rk } \ker(\chi) \text{ if } \sigma \in \mathcal{O}_K^*/\mathcal{O}_K^{*2}.$$

Hence:

$$2\text{-rk } C(F) = \#\mathcal{R}(F/K) - 1 - 2\text{-rk } \ker(\chi) + 2\text{-rk coker}(\chi), \text{ if } \sigma \notin \mathcal{O}_K^*/\mathcal{O}_K^{*2}$$

and

$$2\text{-rk } C(F) = \#\mathcal{R}(F/K) - 2\text{-rk } \ker(\chi) + 2\text{-rk coker}(\chi), \text{ if } \sigma \in \mathcal{O}_K^*/\mathcal{O}_K^{*2}.$$

Therefore we obtain the following:

Proposition 2.45. *If $\sigma \notin \mathcal{O}_K^*/\mathcal{O}_K^{*2}$, then $2\text{-rk ker}(\chi) \geq 2\text{-rk coker}(\chi)$, and*

$$2\text{-rk } C(F) = \#\mathcal{R}(F/K) - 1 - [2\text{-rk ker}(\chi) - 2\text{-rk coker}(\chi)].$$

If $\sigma \in \mathcal{O}_K^/\mathcal{O}_K^{*2}$, then $2\text{-rk ker}(\chi) \geq 1 + 2\text{-rk coker}(\chi)$ and*

$$2\text{-rk } C(F) = \#\mathcal{R}(F/K) - [2\text{-rk ker}(\chi) - 2\text{-rk coker}(\chi)].$$

2.3 Construction of F/K with $h(F)$ Odd

Let K be a totally real algebraic number field with absolute degree $[K : \mathbb{Q}] = n$ and $h^+(K) \equiv 1 \pmod{2}$. We also assume that K has exactly one dyadic prime ideal $D \subset \mathcal{O}_K$.

Let K_D be the localization of K at D . Then \mathcal{O}_D is the ring of local integers. We are concerned with the local units \mathcal{O}_D^* and their square classes $\mathcal{O}_D^*/\mathcal{O}_D^{*2}$. There is a unique local square class $\epsilon_D \neq 1 \in \mathcal{O}_D^*/\mathcal{O}_D^{*2}$ for which $K_D(\sqrt{\epsilon_D})/K_D$ is an unramified quadratic extension. Then ϵ_D generates a subgroup of order 2 in $\mathcal{O}_D^*/\mathcal{O}_D^{*2}$ and the quotient of $\mathcal{O}_D^*/\mathcal{O}_D^{*2}$ by this subgroup is denoted by Γ . There is also a localization homomorphism:

$$\nu_D : \mathcal{O}_K^*/\mathcal{O}_K^{*2} \rightarrow \Gamma.$$

Now, $2\text{-rk } \mathcal{O}_K^*/\mathcal{O}_K^{*2} = n = 2\text{-rk } \Gamma$. Thus

$$\mathcal{O}_K^*/\mathcal{O}_K^{*2} \xrightarrow{\nu_D} \Gamma,$$

since every quadratic extension of K has at least one ramified finite prime ideal. Hence for $1 \neq u \in \mathcal{O}_K^*/\mathcal{O}_K^{*2}$ the single dyadic prime must ramify in $K(\sqrt{u})/K$.

Since $h^+(K) \equiv 1 \pmod{2}$, there is for every prime ideal $P \subset \mathcal{O}_K$ a totally positive square $\pi_P \in K^*/K^{*2}$ for which $\text{ord}_P \pi_P \equiv 1 \pmod{2}$ and $\text{ord}_{P'} \pi_P \equiv 0 \pmod{2}$ if $P' \neq P$. Note that π_P is a unique square class.

For $1 \neq \sigma \in K^*/K^{*2}$ we showed for the resulting quadratic extension $F/K = K(\sqrt{\sigma})/K$ that if $\sigma \notin \mathcal{O}_K^*/\mathcal{O}_K^{*2}$, then (see 2.45)

$$2\text{-rk } C(F) + 2\text{-rk } \ker(\chi) - 2\text{-rk } \text{coker}(\chi) = \#\mathcal{R}(F/K) - 1.$$

Now this shows that $2\text{-rk } \ker(\chi) - 2\text{-rk } \text{coker}(\chi)$ has a *maximum value* when $h(F) \equiv 1 \pmod{2}$.

We begin with the simplest case, $\#\mathcal{R}(F/K) = 1$. First, with $0 \leq k \leq n$, choose k orderings of K . Then there is a unique square class $v \in \mathcal{O}_K^*/\mathcal{O}_K^{*2}$ which is positive in each of the chosen k orderings and negative in the remaining $n - k$. Note that $v = 1 \in \mathcal{O}_K^*/\mathcal{O}_K^{*2}$ if and only if $k = n$.

For the unique dyadic prime ideal there is the square class generator $\epsilon_D \in K^*/K^{*2}$. We see that $D \subset \mathcal{O}_K$ is the only finite prime ramified in $F/K = K(\sqrt{v\epsilon_D})/K$. Of course $n - k$ infinite primes also ramify. Thus $\#\mathcal{R}(F/K) = 1$, while $2\text{-rk } R^0(F/K) = n - k$ by [4] 4.2. Now we have the following

Proposition 2.46. *The homomorphism $i_0 : H^0(C_2; \mathcal{O}_F^*) \rightarrow R^0(F/K)$ is an epimorphism.*

Proof. Recall that $2\text{-rk } \text{im}(i_0) \geq n - k$. Thus, since $\text{im}(i_0) \subset R^0(F/K)$ we have:

$$n - k \leq 2\text{-rk } \text{im}(i_0) \leq 2\text{-rk } R^0(F/K) = n - k.$$

Hence $\text{im}(i_0) = R^0(F/K)$, and we are done. □

Now, by [4] 9.1, it follows that $h(F) \equiv 1 \pmod{2}$. Also we obtain that

$$2\text{-rk } H^0(C_2; \mathcal{O}_F^*) = n - k.$$

The maximum value of $2\text{-rk } \ker(\chi) - 2\text{-rk } \text{coker}(\chi)$ is 0 in this example. Actually i_0 is an isomorphism, hence χ is an epimorphism.

Let us now generalize the previous construction. Again with $0 \leq k \leq n$ choose k orderings of K . Then choose an integer s , $0 < s \leq k$. Next choose s non-negative integers m_1, m_2, \dots, m_s so that $m_1 + m_2 + \dots + m_s = k$. Now partition the chosen k orderings into pairwise disjoint subsets M_1, M_2, \dots, M_s with $\#M_i = m_i > 0$, $1 \leq i \leq s$.

Now we need some units $u_1, u_2, \dots, u_s \in \mathcal{O}_K^*/\mathcal{O}_K^{*2}$ such that each u_i is negative with respect to all orderings in M_i and positive at *all* other orderings of K (we can do this since K has units with independent signs). Then there is a $v \in \mathcal{O}_K^*/\mathcal{O}_K^{*2}$ which is negative at all the remaining $n - k$ orderings of K and positive for the first k orderings already chosen. For each $u_i \in \mathcal{O}_K^*/\mathcal{O}_K^{*2}$ we note u_i cannot be trivial since $M_i \neq \emptyset$. For each i , $1 \leq i \leq s$, choose a non-dyadic prime ideal $P_i \subset \mathcal{O}_K$ such that u_i is not a local square at P_i , but for $j \neq i$, u_j is a local square at P_i . To see that this is possible, consider the extension

$$K(\sqrt{u_1}, \sqrt{u_2}, \dots, \sqrt{u_s})/K$$

with Galois group elementary abelian of 2-rank s . Now for $1 \leq i \leq s$, there is a $\gamma_i \in \text{Gal}(K(\sqrt{u_1}, \sqrt{u_2}, \dots, \sqrt{u_s})/K)$ such that if $j \neq i$, then γ_i lies in the kernel of the epimorphism

$$\text{Gal}(K(\sqrt{u_1}, \sqrt{u_2}, \dots, \sqrt{u_s})/K) \rightarrow \text{Gal}(K(\sqrt{u_j})/K) \rightarrow \mathbf{1},$$

but for $j = i$, $\gamma_i \mapsto$ generator of $\text{Gal}(K(\sqrt{u_i})/K)$.

Proposition 2.47. *The set of primes $P \subset \mathcal{O}_K$ with $\omega(P) = \gamma_i$ have positive density.*

If P is a prime \mathcal{O}_K -ideal as in Proposition 2.47, then P is inert in $K(\sqrt{u_i})/K$, but P splits in $K(\sqrt{u_j})/K$ if $j \neq i$. Then having selected our primes P_1, P_2, \dots, P_s (non-dyadic) we have the totally positive square class generators $\pi_1, \pi_2, \dots, \pi_s$.

Now set

$$\sigma = v\pi_1\pi_2\cdots\pi_s \in K^*/K^{*2}.$$

This σ is positive in the originally chosen k orderings, but negative in the remaining $n - k$. Note,

$$\text{ord}_{P_i}\sigma \equiv 1 \pmod{2}, \quad 1 \leq i \leq s.$$

but

$$\text{ord}_P\sigma \equiv 0 \pmod{2}, \text{ if } P \neq P_1, P_2, \dots, P_s.$$

Hence P_1, P_2, \dots, P_s are the only non-dyadic primes ramified in $F/K = K(\sqrt{\sigma})/K$,
 $\sigma = v\pi_1\pi_2\cdots\pi_s$.

2.4 The Hilbert Symbol

We need Hilbert symbol computations. Let L be a number field and let L_p be the completion of L at p (p prime of L finite or infinite). For $a, b \in L_p^*$, the *Hilbert symbol*

$$(a, b)_p \in \{\pm 1\} = \mathbb{Z}^*$$

is defined as:

$$(a, b)_p = \begin{cases} +1 & \text{iff } a\alpha^2 + b\beta^2 = 1 \text{ has a solution } \alpha, \beta \in L_p \\ -1 & \text{otherwise} \end{cases}$$

In other words, $(a, b)_p = 1$ if and only if $a \in L_p^*$ is a norm from $L_p(\sqrt{b})$, if and only if $b \in L_p^*$ is a norm from $L_p(\sqrt{a})$.

At a complex infinite prime p of L , we have $L_p \cong \mathbb{C}$, so the Hilbert symbol is trivial. At a real infinite prime p of L we have $L_p \cong \mathbb{R}$, the isomorphism corresponding to an embedding $\nu : L \rightarrow \mathbb{R}$. Then $(a, b)_p = -1$ if and only if $\nu(a), \nu(b) < 0$. Let us list the properties of Hilbert symbol:

1. $(x, y)_p = (y, x)_p$
2. $(x, y)_p = 1$ if either x or y is a square in L_p^*
3. $(a, x)_p(b, x)_p = (ab, x)_p$ and $(x, u)_p(x, v)_p = (x, uv)_p$
4. $(x, -x)_p = 1$
5. $(x, x)_p = (x, -1)_p$
6. $(x, 1 - x)_p = 1, x \neq 0, 1$

Now, going back to our situation, there is no ordering of K at which u_i and σ are both negative, hence $(u_i, \sigma)_{P_\infty} = 1$, at every real infinite prime P_∞ of K . Now if $P \subset \mathcal{O}_K$ is a non-dyadic prime ideal $P \notin \{P_1, P_2, \dots, P_s\}$, then $\text{ord}_P u_i \equiv \text{ord}_P \sigma \equiv 0 \pmod{2}$ so $(u_i, \sigma)_P = 1$. However, $(u_i, \sigma)_{P_i} = (u_i, \pi_i)_{P_i} = -1$ and $(u_i, \sigma)_{P_j} = 1$, for $j \neq i$. To satisfy reciprocity we must have $(u_i, \sigma)_D = -1$ for the dyadic prime D . Hence D also ramifies in $F/K = K(\sqrt{\sigma})/K$. Thus $\#\mathcal{R}(F/K) = s + 1$.

In $\mathcal{O}_K^*/\mathcal{O}_K^{*2}$ the units u_1, u_2, \dots, u_s generate a subgroup of 2-rank s . Now, no non-trivial element of this subgroup can be a norm from F/K , since $(u_i, \pi_j)_{P_k} = -1$ if and only if $i = j = k$. Hence, $i_0 : H^0(C_2; \mathcal{O}_F^*) \rightarrow R^0(F/K)$ is an epimorphism. Thus

$$h(F) \equiv h(K) \equiv 1 \pmod{2}$$

and

$$2\text{-rk } H^0(C_2; \mathcal{O}_F^*) = n - k + s.$$

That is $\ker(\chi) = \Pi$, while $\text{coker}(\chi)$ is trivial.

We want to define a homomorphism

$$l : H^0(C_2; C(F)_2) \rightarrow H^0(C_2; \mathcal{O}_F^*).$$

If $\mathfrak{a} \in C(F)_2$ and $\bar{\mathfrak{a}} = \mathfrak{a}$, then represent \mathfrak{a} by an fractional \mathcal{O}_F -ideal $A \subset F$. Since $\bar{\mathfrak{a}} = \mathfrak{a}$, we may write $\bar{A} = xA$, for some $x \in F^*$. Then $A = \bar{x}\bar{A} = x\bar{x}A$, hence $x\bar{x} \in \mathcal{O}_K^*$. We then set

$$l(\text{cl}(\mathfrak{a})) = \text{cl}(x\bar{x}) \in H^0(C_2; \mathcal{O}_F^*).$$

Let us prove the following

Lemma 2.48. *If $\mathfrak{a} = \bar{\mathfrak{a}}$ in $C(F)_2$, then \mathfrak{a} can be represented by a fractional \mathcal{O}_F -ideal A for which $\bar{A} = A$ if and only if $l(\text{cl}(\mathfrak{a})) = \mathbf{1} \in H^0(C_2; \mathcal{O}_F^*)$.*

Proof. Necessity: If $\bar{A} = A$, then $xA = A$, so $x \in \mathcal{O}_F^*$. Then $x\bar{x} = N_{F/K}(x) \in \mathcal{O}_K^*$ and also $x\bar{x} \in N(\mathcal{O}_F^*)$, hence $\text{cl}(x\bar{x}) = \mathbf{1} \in H^0(C_2; \mathcal{O}_F^*) = \mathcal{O}_K^*/N(\mathcal{O}_F^*)$.

Sufficiency: Assume $\bar{A} = xA$ and for some $w \in \mathcal{O}_F^*$, $w\bar{w} = x\bar{x}$, i.e. $\text{cl}(x\bar{x}) = \mathbf{1} \in H^0(C_2; \mathcal{O}_F^*)$. We can then write $\bar{A} = xw^{-1}A$. But

$$xw^{-1}\overline{(xw^{-1})} = xw^{-1}\bar{x}\bar{w}^{-1} = \frac{x\bar{x}}{w\bar{w}} = 1,$$

hence, by Hilbert 90, we may write

$$z\bar{z}^{-1} = xw^{-1}, \quad \text{for some } z \in F^*.$$

Therefore $\bar{A} = z\bar{z}^{-1}A$ or $\bar{z}\bar{A} = zA$. Hence $\overline{zA} = zA$. Thus, zA represents $\mathfrak{a} \in C(F)_2$ and $\overline{zA} = zA$. □

The ideal norm induces a homomorphism

$$\mathcal{N} : C(F)_2 \rightarrow C(K)_2.$$

For $\mathfrak{b} \in C(F)_2$, $\mathcal{N}(\mathfrak{b}) = (\bar{\mathfrak{b}})$, thus $\mathcal{N}(\mathfrak{b}\bar{\mathfrak{b}}) = \mathcal{N}(\mathfrak{b}^2) = 1$. As a consequence we regard \mathcal{N} as a homomorphism

$$\mathcal{N} : H^0(C_2; C(F)_2) \rightarrow C(K)_2.$$

Let us introduce

$$\Gamma : H^0(C_2; C(F)_2) \rightarrow H^0(C_2; \mathcal{O}_F^*) \oplus C(K)_2,$$

by

$$\Gamma(\text{cl}(\mathfrak{a})) = (l(\mathfrak{a}), (\mathfrak{a})) = (l(\text{cl}(\mathfrak{a})), \mathcal{N}(\text{cl}(\mathfrak{a}))).$$

We then have

Theorem 2.49. *An ideal class $\mathfrak{a} \in C(F)_2$ lies in the image of $\chi : \Pi \rightarrow C(F)_2$ if and only if*

(i) $\mathfrak{a} = \bar{\mathfrak{a}}$ and

(ii) $\Gamma(\text{cl}(\mathfrak{a})) = (1, 1)$ in $H^0(C_2; \mathcal{O}_F^*) \oplus C(K)_2$.

Proof. " \Leftarrow " If $\mathfrak{a} = \bar{\mathfrak{a}}$ and $l(\text{cl}(\mathfrak{a})) = \mathbf{1} \in H^0(C_2; \mathcal{O}_F^*)$ we can choose a representative \mathcal{O}_F -ideal A with $A = \bar{A}$ by Lemma 2.48. Since $\mathcal{N}(\text{cl}(\mathfrak{a})) = \mathbf{1} \in C(K)_2$, we can write $\mathcal{N}(A) = y\mathcal{O}_K$ for some $y \in K^*$. Without loss of generality we can take y to be totally positive since K contains units with independent signs. But now $y\mathcal{O}_F = \mathcal{A}\mathcal{O}_F = A\bar{A} = A^2$, which means that for $y \in \Pi$ we have $\chi(y) = \mathfrak{a} \in C(F)_2$.

" \Rightarrow " We already have showed that $\text{im}(\chi) \subset \ker(\mathcal{N})$ in Proposition 2.38. By the construction of χ we can see that $\chi(y)$ is always represented by an \mathcal{O}_F -ideal A with $A = \bar{A}$. □

Corollary 2.50. *For every $\mathfrak{b} \in C(F)_2$ the product $\mathfrak{b}\bar{\mathfrak{b}}$ lies in the image of χ .*

In fact the homomorphism l introduced earlier is a composition

$$H^0(C_2; C(F)_2) \rightarrow H^0(C_2; C(F)) \xrightarrow{d_0} H^0(C_2; \mathcal{O}_F^*).$$

We want to see what happens if we assume that the 2-primary subgroup of $C(K)$ is an elementary abelian 2-group. Actually to make the discussion simpler

we assume

$$C(K) = C(K)_2$$

and later we point how to generalize. First an elementary

Proposition 2.51. *If $\mathfrak{a} = \bar{\mathfrak{a}} \in C(F)_2$ is an element for which $\text{cl}(\mathfrak{a}) \in H^0(C_2; C(F))$ lies in the kernel of the natural homomorphism $H^0(C_2; C(F)_2) \rightarrow H^0(C_2; C(F))$, then $\mathfrak{a} \in \text{im}(\chi)$.*

Proof. We immediately see that $l(\text{cl}(\mathfrak{a})) = \mathbf{1} \in H^0(C_2; \mathcal{O}_F^*)$ by regarding l as the composition

$$H^0(C_2; C(F)_2) \rightarrow H^0(C_2; C(F)) \xrightarrow{d_0} H^0(C_2; \mathcal{O}_F^*).$$

Then we know that $\mathfrak{a} = \mathfrak{b}\bar{\mathfrak{b}}$ for some $\mathfrak{b} \in C(F)$. Thus

$$\mathcal{N}(\mathfrak{a}) = \mathcal{N}(\mathfrak{b}\bar{\mathfrak{b}}) = \mathcal{N}(\mathfrak{b})^2 \in C(K).$$

But $C(K) = C(K)_2$ and so $\mathcal{N}(\text{cl}(\mathfrak{a})) = \mathbf{1} \in C(K)_2 = C(K)$. Hence, by Theorem 2.49, $\mathfrak{a} \in \text{im}(\chi)$. \square

Associated to $F/K = K(\sqrt{\sigma})/K$ there is a specific *target subgroup* $T \subset C(K)_2 = C(K)$. This is the subgroup generated by the ideal classes of all finite prime ideals $P \subset \mathcal{O}_K$ that ramify in F/K .

Lemma 2.52. *If $\mathfrak{a} = \bar{\mathfrak{a}} \in C(F)_2$ is represented by a fractional \mathcal{O}_F -ideal $A \subset F$ with $A = \bar{A}$, then $\mathcal{N}(\text{cl}(\mathfrak{a})) \in T$.*

Proof. If $P \subset \mathcal{O}_K$ is unramified, then either $P\mathcal{O}_F = \mathcal{P}$ a prime ideal in \mathcal{O}_F , or $P\mathcal{O}_F = \mathcal{P}\bar{\mathcal{P}}$, a conjugate pair of prime ideals in \mathcal{O}_F .

If $P\mathcal{O}_F = \mathcal{P}$, then $\text{ord}_P \mathcal{N}(A) = \text{ord}_P A\bar{A} = \text{ord}_P A^2 = 2\text{ord}_P A$.

If $P\mathcal{O}_F = \mathcal{P}\bar{\mathcal{P}}$, then $\text{ord}_P\mathcal{N}(A) = \text{ord}_P A + \text{ord}_{\bar{P}} A = 2\text{ord}_P A$. Hence for all unramified finite prime ideals $P \subset \mathcal{O}_K$,

$$\text{ord}_P\mathcal{N}(A) \equiv 0 \pmod{2}.$$

Since $C(K)_2 = C(K)$, there is an $x \in K$ with

$$\text{ord}_P x = \text{ord}_P\mathcal{N}(A) \text{ at all unramified } P \subset \mathcal{O}_K.$$

Thus, $x^{-1}\mathcal{N}(A)$ is a fractional \mathcal{O}_K -ideal representing $\mathcal{N}(\text{cl}(A)) = \mathcal{N}(\text{cl}(\mathfrak{a})) \in T$. □

Next suppose B is a fractional ideal for which $\text{ord}_P B = 0$, for all unramified ideals $P \subset \mathcal{O}_K$. Then $B\mathcal{O}_F = A^2$, for a unique fractional \mathcal{O}_F -ideal A . Surely $\bar{A} = A$, but is $\text{cl}(A) = \mathfrak{a}$ actually in the subgroup $C(F)_2$? It is *if and only if* $B\mathcal{O}_F$ is a principal ideal. That is, if $\mathfrak{b} \in T \subset C(K)_2 = C(K)$, then \mathfrak{b} lies in the image of $\mathcal{N} : \ker(l) \rightarrow T$ if and only if $i_*(\mathfrak{b}) = \mathbf{1} \in C(F)_2 \subset C(F)$, where i_* is the natural homomorphism $C(K) = C(K)_2 \rightarrow C(F)_2 \subset C(F)$. Thus we let $\ker(l) \subset C(F)_2$ be all $\mathfrak{a} = \bar{\mathfrak{a}} \in C(F)_2$ for which $l(\text{cl}(\mathfrak{a})) = \mathbf{1} \in H^0(C_2; \mathcal{O}_F^*)$. Let us summarize:

Proposition 2.53. *If the 2-primary subgroup of $C(K)$ is elementary abelian, then the sequence*

$$\mathbf{1} \rightarrow \ker(\chi) \rightarrow \Pi \xrightarrow{\chi} \ker(l) \xrightarrow{\mathcal{N}} T \xrightarrow{i_*} C(F)_2$$

is exact.

Let us add that the target group T is trivial if the ideal class of every ramified prime ideal has odd order in $C(K)$. In particular, if F/K is unramified, then T is trivial. If we assume $H^0(C_2; \mathcal{O}_F^*) \rightarrow R^0(F/K)$ is a monomorphism it will follow that l is trivial, so $\ker(l) = \{\mathfrak{a} \mid \mathfrak{a} = \bar{\mathfrak{a}} \in C(F)_2\}$.

2.5 Elementary Abelian 2-groups

Let G denote an elementary abelian 2-group which will be multiplicatively written. The important point is that for every $g \in G$, we have $g^{-1} = g$. Next we assume that the cyclic group of order 2, C_2 , acts as a group of automorphisms on G . We denote this by $g \rightarrow \bar{g}$, for $g \in G$. Thus are defined the cohomology groups $H^0(C_2; G)$ and $H^1(C_2; G)$. Let us prove

Lemma 2.54. *For G an elementary abelian 2-group acted on only by C_2 we have $H^0(C_2; G) = H^1(C_2; G)$.*

Proof. We first observe for $g \in G$ that $\bar{g} = g$ if and only if $\bar{g} = g^{-1}$. Furthermore, for $h \in G$, $h\bar{h} = h\bar{h}^{-1}$. □

In our situation $C(F)_2$ is a finite elementary abelian 2-group acted on by the Galois group of the quadratic extension. Thus, by Lemma 2.54, $H^1(C_2; C(F)_2) = H^0(C_2; C(F)_2) = H^0(C_2; C(F))$. Referring to the exact hexagon 1.18, the natural homomorphism $H^1(C_2; C(F)_2) \rightarrow H^1(C_2; C(F))$ is composed with

$$d_1 : H^1(C_2; C(F)) \rightarrow H^1(C_2; \mathcal{O}_F^*)$$

to produce the homomorphism

$$\eta : H^1(C_2; C(F)_2) \rightarrow H^1(C_2; \mathcal{O}_F^*).$$

Recall also the homomorphism l on page 39. Thus we get the following diagram:

$$\begin{array}{ccc}
 H^1(C_2; C(F)) & \xrightarrow{d_1} & H^1(C_2; \mathcal{O}_F^*) \\
 \uparrow & \nearrow \eta & \\
 H^1(C_2; C(F)_2) & \xlongequal{\quad} & H^0(C_2; C(F)_2) \\
 & \nwarrow l & \downarrow \\
 H^0(C_2; \mathcal{O}_F^*) & \xleftarrow{d_0} & H^0(C_2; C(F))
 \end{array}$$

These two homomorphisms l and η may be directly described.

If $\mathfrak{a} \in C(F)_2$ and $\bar{\mathfrak{a}} = \mathfrak{a}$ then represent \mathfrak{a} by a fractional \mathcal{O}_F -ideal A . First we write $\bar{A} = xA$ for some $x \in F^*$. Then $A = \bar{\bar{A}} = \bar{x}\bar{A} = x\bar{x}A$, hence $x\bar{x}$ is a unit in \mathcal{O}_F^* . Thus $l(\mathfrak{a})$ is the cohomology class of $x\bar{x}$ in $H^0(C_2; \mathcal{O}_F^*)$. However, $A^{-1} \sim A$, $\bar{A}^{-1} \sim \bar{A}$. Thus, for $\mathfrak{a} = \bar{\mathfrak{a}}$ we also know that $A\bar{A}$ is a principal ideal. That is

$$A\bar{A} = z\mathcal{O}_F, \text{ for some } z \in F^*.$$

Thus $\bar{z}\mathcal{O}_F = \bar{A}A = A\bar{A} = z\mathcal{O}_F$. Hence $z\bar{z}^{-1} \in \mathcal{O}_F^*$ and this defines a class in $H^1(C_2; \mathcal{O}_F^*)$. So $\eta : H^0(C_2; C(F)_2) \rightarrow H^1(C_2; \mathcal{O}_F^*)$ is also described.

What does this mean? If $\mathfrak{a} = \bar{\mathfrak{a}}$ we have $\text{cl}(\mathfrak{a}) \in H^0(C_2; C(F)_2) = H^1(C_2; C(F)_2)$. There is a fractional \mathcal{O}_F -ideal A representing $\mathfrak{a} \in C(F)_2$ and for which $\bar{A} = A$ if and only if

$$l(\text{cl}(\mathfrak{a})) = \mathbf{1} \in H^0(C_2; \mathcal{O}_F^*).$$

Assume then $A = \bar{A}$. We have $A\bar{A} = A^2 = z\mathcal{O}_F$ and $\bar{A}^2 = A^2 = \bar{z}\mathcal{O}_F$. If $z\bar{z}^{-1} = \mathbf{1} \in H^1(C_2; \mathcal{O}_F^*)$, then $v\bar{v}^{-1} = z\bar{z}^{-1}$ for some $v \in \mathcal{O}_F^*$. Hence $\bar{z}v = z\bar{v}$, that is $\overline{(\bar{z}v)} = z\bar{v} = \bar{z}v$. Therefore $A^2 = y\mathcal{O}_F$ for some $y \in K^*$. We see that $\mathcal{N}(A)$ is principal in K with generator y . Thus we have

Proposition 2.55. *If $\bar{\mathfrak{a}} = \mathfrak{a} \in C(F)_2$, then \mathfrak{a} lies in the image of $\chi : \Pi \rightarrow C(F)_2$ (i.e. $\chi(y) = \mathfrak{a}$) if and only if $\text{cl}(\mathfrak{a}) \in H^0(C_2; C(F)_2)$ lies in the kernel of both l and η .*

Let us make some comments. If F/K is ramified, then for $i_* : C(K) \rightarrow C(F)$, $\ker(i_*)$ embeds in $H^1(C_2; \mathcal{O}_F^*)$. Furthermore $\text{im}(\eta) \subset \ker(i_*) \subset H^1(C_2; \mathcal{O}_F^*)$. As long as F/K is ramified we can also embed $C(K)_2$ into Π . That is we also have $\ker(i_*) \subset \ker(\chi)$, so

$$2\text{-rk im}(\eta) \leq 2\text{-rk ker}(i_*) \leq 2\text{-rk ker}(\chi) \leq k.$$

If $\ker(\chi)$ is trivial, then also $\ker(i_*)$ and $\text{im}(\eta)$ are trivial, and hence all $\mathfrak{a} = \bar{\mathfrak{a}} \in C(F)_2$ lie in the image of χ .

2.6 Star Extensions

We have noted (see 2.1) that there is a natural isomorphism $C(K)_2 \cong E^+$. Now if $F/K = K(\sqrt{\sigma})/K$ is a quadratic extension of K , then $S \subset \Omega_K$ consists of all infinite primes in K together with all finite primes in K that ramify in F/K . Recall (page 19) $E_S^+ \subset K^*/K^{*2}$, the subgroup of all totally positive square classes $y \in K^*/K^{*2}$ with $\text{ord}_P y \equiv 0 \pmod{2}$ at all $P \in \mathcal{O}_K$, $P \notin S$. Clearly $E^+ \subset E_S^+$. The subgroup Π can be regarded as a quotient group of E_S^+ .

If F/K is ramified then $C(K)_2$ embeds into Π , see 2.3, thus

$$C(K)_2 \subset \Pi.$$

Then, the restriction of $\chi : \Pi \rightarrow C(F)_2$ agrees with the restriction of the natural homomorphism $i_* : C(K) \rightarrow C(F)$ to the subgroup $C(K)_2$. We must note that $\ker(i_*)$ is entirely contained in $C(K)_2$. Hence we can say

$$\ker(i_*) \subset \ker(\chi)$$

if F/K is ramified.

Our only concern is when $2\text{-rk } C(K)_2 > 0$.

Definition 2.56. *A quadratic extension $F/K = K(\sqrt{\sigma})/K$ is a star extension (in short *-ext.) if and only if*

1. σ is totally positive;
2. no finite dyadic prime in Ω_K ramifies in F/K ;
3. at least one finite non-dyadic prime in Ω_K does ramify;

$$4. \ 2\text{-rk } C_S(K) < 2\text{-rk } C(K);$$

$$5. \ #\mathcal{R}(F/K) + 2\text{-rk } C_S(K) = 1 + 2\text{-rk } C(K).$$

Remember that $\#\mathcal{R}(F/K) > 0$. Thus a $*$ -ext. F/K is a ramified totally real quadratic extension of K . Furthermore, $\sigma \notin \mathcal{O}_K^*/\mathcal{O}_K^{*2}$ and $\sigma \notin E^+$ (see 2.35 on page 26). Hence $C(K)_2 \subset \Pi$. But now remember (see Lemma 2.26) that

$$2\text{-rk } \Pi = \#\mathcal{R}(F/K) + 2\text{-rk } C_S(K) - 1,$$

which together with our assumption

$$\#\mathcal{R}(F/K) + 2\text{-rk } C_S(K) = 1 + 2\text{-rk } C(K)$$

yields:

$$2\text{-rk } \Pi = 2\text{-rk } C(K).$$

As a result, for $*$ -ext. we have

$$\Pi = C(K)_2.$$

Immediately we see

Proposition 2.57. *If F/K is a quadratic $*$ -ext. then*

$$(i) \ \ker(i_*) = \ker(\chi)$$

$$(ii) \ 2\text{-rk } \ker(i_*) = 2\text{-rk } H^0(C_2; \mathcal{O}_F^*)$$

$$(iii) \ 1 + 2\text{-rk } \ker(i_*) = 2\text{-rk } H^1(C_2; \mathcal{O}_F^*)$$

Proof. Since σ is totally positive we have $n = k$. Using Theorem 2.32 and Corollary 2.33(i) the assertions follow. □

Since we are only concerned with the case $2\text{-rk } C(K) > 0$ and $\#\mathcal{R}(F/K) \geq 1$, we see that $\#\mathcal{R}(F/K) \geq 2$ for a $*$ -ext.. We shall refer to the exact hexagon 1.18 to regard $\ker(i_*) \subset H^1(C_2; \mathcal{O}_F^*)$ as the image of the homomorphism

$$d_1 : H^1(C_2; C(F)) \rightarrow H^1(C_2; \mathcal{O}_F^*),$$

thus $\text{im}(d_1) \subset H^1(C_2; \mathcal{O}_F^*)$ has index 2. Let us show

Proposition 2.58. *If F/K is a $*$ -ext. for which every unit in \mathcal{O}_K^* is a field norm from F/K , then*

$$2\text{-rk } H^1(C_2; \mathcal{O}_F^*) = \#\mathcal{R}(F/K) - 1 + 2\text{-rk } H^0(C_2; \mathcal{O}_F^*).$$

Proof. We refer to the exact hexagon 1.18. The homomorphism $i_0 : H^0(C_2; \mathcal{O}_F^*) \rightarrow R^0(F/K)$ is trivial since every unit in \mathcal{O}_K^* is a norm from F/K . Hence $j_1 : R^0(F/K) \rightarrow H^1(C_2; C(F))$ is a monomorphism. Since

$$2\text{-rk } R^0(F/K) = \#\mathcal{R}(F/K) - 1$$

and

$$2\text{-rk } \text{im}(d_1) = 2\text{-rk } H^0(C_2; \mathcal{O}_F^*)$$

the proposition follows. □

Note that the assumption that units in \mathcal{O}_K^* are all norms from F/K does not imply that $H^0(C_2; \mathcal{O}_F^*)$ is trivial. Let us now turn to another extreme:

Proposition 2.59. *If F/K is $*$ -ext. for which*

$$i_0 : H^0(C_2; \mathcal{O}_F^*) \rightarrow R^0(F/K)$$

is an epimorphism, then

$$2\text{-rk } H^1(C_2; C(F)) = 2\text{-rk } \ker(i_*) = 2\text{-rk } H^0(C_2; C(F)) \geq \#\mathcal{R}(F/K) - 1.$$

Proposition 2.60. *Let F/K be a $*$ -ext. for which $2\text{-rk } C(K) \leq n$. If $\#\mathcal{R}(F/K) = 1 + 2\text{-rk } C(K)$ and if i_0 is an epimorphism then*

$$2\text{-rk } H^1(C_2; C(F)) = 2\text{-rk } C(K) = 2\text{-rk } H^0(C_2; \mathcal{O}_F^*) = 2\text{-rk } \ker(i_*).$$

Proof. This follows from the previous proposition by noting that $2\text{-rk } \ker(i_*) \leq 2\text{-rk } C(K) = \#\mathcal{R}(F/K) - 1$. □

We must turn to the question of existence of $*$ -ext. All infinite primes of K are real. The number of finite dyadic primes of K is denoted by $g_2(K)$, $1 \leq g_2(K) \leq n = [K : \mathbb{Q}]$. The cycle c_D on K will consist of all real infinite primes of K , each, as usual, with multiplicity one. Each finite dyadic prime $D \subset \mathcal{O}_K$ will appear in c_D . If e_D is the ramification index of the dyadic prime, then the ramification index of the dyadic prime in c_D is $2e_D$.

Now, if $\sigma \in K^*$, and $\sigma \equiv 1 \pmod{*c_D}$ then σ is totally positive and at each dyadic ideal $D \subset \mathcal{O}_K$ this σ is a local unit modulo $\mathcal{P}_D^{2e_D}$ where $\mathcal{P} \subset \mathcal{O}_D$ is the maximal ideal in the local ring of integers at D .

Thus, if $\sigma \equiv 1 \pmod{*c_D}$, then $F = K(\sqrt{\sigma})/K$ is a totally real quadratic extension of K in which no dyadic prime of K ramifies. A finite non-dyadic prime ideal $P \subset \mathcal{O}_K$ ramifies if and only if $\text{ord}_P \sigma \equiv 1 \pmod{2}$. Let $C(K, c_D)$ be the generalized ideal class group associated to c_D . This is a finite abelian group with a natural epimorphism

$$C(K, c_D) \rightarrow C(K) \rightarrow 1.$$

Clearly, F/K is a $*$ -ext. if and only if $\sigma \equiv 1 \pmod{*c_D}$ and $\text{ord}_P \sigma \equiv 1 \pmod{2}$ for at least one finite non-dyadic prime $P \subset \mathcal{O}_K$.

Let us choose a minimal generating set u_1, u_2, \dots, u_n for $\mathcal{O}_K^*/\mathcal{O}_K^{*2}$. Let us consider the extension field L/K which is the compositum of the quadratic extensions

$$K(\sqrt{u_j})/K, \quad 1 \leq j \leq n.$$

This extension contains the square root of every unit in \mathcal{O}_K^* . The Galois group $\text{Gal}(L/K)$ is an elementary abelian 2-group with $2\text{-rk Gal}(L/K) = n$. Then we can give a minimal generating set b_1, b_2, \dots, b_n as follows. For each j , $1 \leq j \leq n$, let $b_j \in \text{Gal}(L/K)$ be the unique element for which the image for which the image of b_j under

$$\text{Gal}(L/K) \rightarrow \text{Gal}(K(\sqrt{u_j})/K) \rightarrow 1$$

is the generator of $\text{Gal}(K(\sqrt{u_j})/K)$, but for $i \neq j$, $1 \leq i \leq n$, the image of b_i under

$$\text{Gal}(L/K) \rightarrow \text{Gal}(K(\sqrt{u_i})/K) \rightarrow 1$$

is trivial in $\text{Gal}(K(\sqrt{u_i})/K)$.

No finite non-dyadic prime ideal of K ramifies. Thus, if $P \subset \mathcal{O}_K$ is a finite non-dyadic prime ideal of K then it has an Artin symbol

$$A(P, L/K) \in \text{Gal}(L/K).$$

If the Artin symbol is trivial, then every unit in $\mathcal{O}_K^*/\mathcal{O}_K^{*2}$ is a local square at P , but if $A(P, L/K) = b_j$, then u_j is not a local square at P , while for $i \neq j$, u_i is a local square at P .

To simplify our treatment we assume $C(K)$ is a 2-group (not necessarily elementary abelian). Let H/K be the Hilbert class field of K . No prime ideal of K ramifies in H/K . The Artin symbol induces the isomorphism

$$A : C(K) \rightarrow \text{Gal}(H/K).$$

Now we can express the finite abelian 2-group as a direct product of cyclic factors. Then the number of such cyclic factors is $2\text{-rk } C(K) = r > 0$. For each of our chosen cyclic factors we pick a generator $\beta_1, \beta_2, \dots, \beta_r \in C(K)$. Then

$$A(\beta_j, L/K) = b_j \in \text{Gal}(H/K)$$

will be generators of the corresponding cyclic factors in the associated direct product splitting of $\text{Gal}(H/K)$. There is, of course, the extension field HL/K . As H/K is unramified and every subfield of L/K is ramified, the composition HL/K has

$$\text{Gal}(HL/K) \cong \text{Gal}(H/K) \times \text{Gal}(L/K).$$

For each $g \in \text{Gal}(HL/K)$ the density of the finite non-dyadic primes P with $A(P, HL/K) = g$ is

$$\frac{1}{[H : K] \cdot [L : K]} = \frac{1}{\#C(K) \cdot 2^n}.$$

At this point let us construct $*$ -ext. for which every unit in \mathcal{O}_K^* is a field norm from F/K .

Choose l , $1 \leq l \leq r = 2\text{-rk } C(K)$. Now select finite non-dyadic prime ideals in \mathcal{O}_K , P_1, P_2, \dots, P_l so that

$$A(P_j, HL/K) = (\beta_j, \text{id}), \quad \text{for } 1 \leq j \leq l.$$

Thus $A(P_j, L/K) = \text{id} \in \text{Gal}(L/K)$ and hence every unit is a local square at each P_j . Next we choose one more finite non-dyadic prime ideal $Q \subset \mathcal{O}_K$ so that the product $P_1 \cdot P_2 \cdots P_l \cdot Q$ has trivial generalized class in $C(K, c_D)$. Thus there is a $\sigma \in K^*$, $\sigma \equiv 1 \pmod{*c_D}$, generating the product $P_1 \cdot P_2 \cdots P_l \cdot Q$.

If we form $F/K = K(\sqrt{\sigma})/K$, then $\#\mathcal{R}(F/K) = l + 1$, that is P_1, P_2, \dots, P_l, Q ramify. Moreover $l + 2\text{-rk } C_S(K) = 2\text{-rk } C(K)$ in this construction and hence we have a $*$ -ext.. Every unit $u \in \mathcal{O}_K^*/\mathcal{O}_K^{*2}$ is a norm from F/K . First σ is totally positive. At each dyadic prime ideal D , σ is a local unit which is either a local square or the local unit for which $K_D(\sqrt{\sigma})/K_D$ is the unit non-trivial local unramified extension.

For each P_j , $1 \leq j \leq l$, all units are local squares. Thus $(u, \sigma)_P = 1$ at every prime ideal of K , except possibly for Q , where $u \in \mathcal{O}_K^*$. By Hilbert symbol reciprocity, $(u, \sigma)_Q = 1$ also. Hence, u is a field norm from F/K for every $u \in \mathcal{O}_K^*$.

Next, let us assume $1 \leq l \leq \min(n; 2\text{-rk } C(K))$. We may consider the pairs $(B_j, b_j) \in \text{Gal}(HL/K)$, $1 \leq j \leq l$. So there are finite non-dyadic prime ideals P_1, P_2, \dots, P_l with

$$A(P_j, HL/K) = (B_j, b_j) \in \text{Gal}(HL/K).$$

Then $A(P_j, H/K) = B_j$ corresponding to a generator of a cyclic factor of $C(K)$, while $A(P_j, L/K) = b_j \in \text{Gal}(L/K)$ which means u_j is not a local square at P_j , but is a local square at each P_i , $i \neq j$, $1 \leq i \leq l$.

Choose another non-dyadic prime ideal Q with $P_1 \cdot P_2 \cdots P_l \cdot Q$ principal in $C(K, c_D)$. Thus σ generates this product with $\sigma \equiv 1 \pmod{*c_D}$.

Let us turn to $F/K = K(\sqrt{\sigma})/K$. This is a $*$ -ext.. Let us check Hilbert symbols. Take a unit $u_j \in \mathcal{O}_K^*$. Then $\text{ord}_{P_j} \sigma \equiv 1 \pmod{2}$ and u_j is not a local square at P_j . Thus

$$(u_j, \sigma)_{P_j} = -1.$$

However u_j is a local square at P_i , $i \neq j$. Thus

$$(u_j, \sigma)_{P_i} = 1, \text{ for } i \neq j.$$

The only other prime ideal at which the Hilbert symbol of u_j and σ is -1 is

$$(u_j, \sigma)_Q = -1.$$

Thus u_1, u_2, \dots, u_l generate a subgroup of $\mathcal{O}_K^*/\mathcal{O}_K^{*2}$ with 2-rank equal to l . But no other element of this subgroup besides the identity can be a norm from F/K . Thus $\mathcal{O}_K^*/\mathcal{O}_K^{*2}$ contains a subgroup of rank l , generated by u_1, u_2, \dots, u_l , which maps isomorphically into $\text{R}^0(F/K)$ by i_0 . Hence, since $2\text{-rk } \text{R}^0(F/K) = l = \#\mathcal{R}(F/K) - 1$ we see that $i_0 : \text{H}^0(C_2; \mathcal{O}_F^*) \rightarrow \text{R}^0(F/K) \rightarrow 1$ is an epimorphism. Hence

$$2\text{-rk } \text{H}^1(C_2; C(F)) = 2\text{-rk } \ker(i_*) = 2\text{-rk } \text{H}^0(C_2; \mathcal{O}_F^*) \geq l = \#\mathcal{R}(F/K) - 1.$$

Now obviously

$$2\text{-rk } H^0(C_2; \mathcal{O}_F^*) = 2\text{-rk } \ker(i_*) \leq n$$

while

$$2\text{-rk } \ker(i_*) \leq 2\text{-rk } C(K).$$

Thus, if $2\text{-rk } C(K) \leq n$, we may take $l = 2\text{-rk } C(K)$ in the preceding construction to produce a $*$ -ext. F/K with $2\text{-rk } C(K) \leq 2\text{-rk } \ker(i_*) \leq 2\text{-rk } C(K)$. Thus $2\text{-rk } \ker(i_*) = 2\text{-rk } C(K) = 2\text{-rk } H^0(C_2; \mathcal{O}_F^*) = 2\text{-rk } H^1(C_2; C(F))$. Finally, if $n \leq 2\text{-rk } C(F)$ we can always use $l = n$. We then have

$$2\text{-rk } \ker(i_*) = n = 2\text{-rk } H^0(C_2; C(F)) = 2\text{-rk } H^1(C_2; C(F)).$$

Let us make some comments. For $*$ -ext. we can identify $C(K)_2$ with Π and hence $\ker(\chi)$ with $\ker(i_*)$. Combining what we know of $\ker(\chi)$ with the small amount of information we had about $\ker(i_*) \subset H^1(C_2; \mathcal{O}_F^*)$ as the image of d_1 we can use the exact hexagon to produce a great deal of information about $\ker(i_*)$ as well as $H^1(C_2; C(F))$. Thus, $*$ -ext. seems to be very worthwhile commenting on.

2.7 Examples

Assume K is totally real containing units with independent signs and $[K : \mathbb{Q}] = n \geq 2$. Since K has units with independent signs, for every ordering of K there will be a unit positive in only that ordering and negative in the remaining $n - 1$ orderings of K . Denote by $v \in \mathcal{O}_K^*/\mathcal{O}_K^{*2}$ the square class of such a unit. There is a natural one-to-one correspondence between these square classes and the orderings of K .

For a choice of $v \in \mathcal{O}_K^*/\mathcal{O}_K^{*2}$ form the quadratic extension

$$F/K = K(\sqrt{v})/K.$$

Then $n - 1$ infinite primes ramify in F/K and one ordering of K splits into a conjugate pair of orderings in F . Thus $r_1(F) = 2$, and $r_2(F) = n - 1$.

Since $C^+(K) \cong C(K)$ there must be at least one finite prime in \mathcal{O}_K that ramifies in F/K . Since v is a unit, all finite ramified primes must be dyadic.

By Theorem 2.26 we have that

$$2\text{-rk } \Pi = \#\mathcal{R}(F/K) + 2\text{-rk } C_S(K).$$

Now Corollary 2.33 says

$$1 + 2\text{-rk } H^0(C_2; \mathcal{O}_F^*) = n - 1 + 2\text{-rk } \ker(\chi),$$

while Theorem 2.32 gives

$$2\text{-rk } H^1(C_2; \mathcal{O}_F^*) = 2\text{-rk } \ker(\chi).$$

Up to square classes, the only non-trivial element of $\mathcal{O}_K^*/\mathcal{O}_K^{*2}$ that can be a field norm from F/K is $-v$ which is the norm of the unit $\sqrt{v} \in \mathcal{O}_F^*$. Thus

$$2\text{-rk } H^0(C_2; \mathcal{O}_F^*) = n - 1,$$

and so

$$2\text{-rk } \ker(\chi) = 1 = 2\text{-rk } H^1(C_2; \mathcal{O}_F^*).$$

Now Corollary 2.37 implies that \mathcal{O}_F^* has also units with independent signs.

If $h(K)$ is odd, then Proposition 2.42 implies that $\chi : \Pi \rightarrow C(F)_2$ is onto, hence

$$2\text{-rk } C(F) = \#\mathcal{R}(F/K) - 1,$$

by Proposition 2.45.

On the other hand, if $h(K)$ is even we see that $2\text{-rk } \ker(i_*) \leq 1$ by Lemma 2.35.

Now we still have, by Theorem 4.2 [4], that

$$2\text{-rk } R^0(F/K) = \#\mathcal{R}(F/K) + n - 2.$$

Looking at the exact hexagon, we see that $i_0 : H^0(C_2; \mathcal{O}_F^*) \rightarrow R^0(F/K)$ is a monomorphism. Now Theorem 5.1 [4] says that

$$2\text{-rk } R^1(F/K) = \#\mathcal{R}(F/K).$$

Thus,

$$j_0 : R^1(F/K) \rightarrow H^0(C_2; C(F))$$

is onto. Let us summarize:

Theorem 2.61. *Let K be a totally real number field having units with independent signs. Let $v \in \mathcal{O}_K^*$ be a unit which is positive with respect to exactly one ordering of K and negative with respect to the remaining $n - 1$ orderings of K , where $n = [K : \mathbb{Q}] \geq 2$. Put $F = K(\sqrt{v})$.*

If $\ker(i_)$ is trivial, then*

$$2\text{-rk } H^0(C_2; C(F)) = \#\mathcal{R}(F/K) - 1.$$

If $\ker(i_)$ is cyclic of order 2, then*

$$2\text{-rk } H^0(C_2; C(F)) = \#\mathcal{R}(F/K).$$

Let us be more specific. Let $N > 1$ be a square free rational integer so that $N \equiv 1 \pmod{8}$. Then $K = \mathbb{Q}(\sqrt{N})$ has a conjugate pair of dyadic primes D, D^* in \mathcal{O}_K . Each completion, K_D and K_{D^*} , can be identified with the 2-adic rationals \mathbb{Q}_2 as follows.

Since $N \equiv 1 \pmod{8}$, N has two distinct square roots, v and $-v$, in the units of the 2-adic integers \mathbb{Z}_2^* . Then, embed $K = \mathbb{Q}(\sqrt{N})$ into \mathbb{Q}_2 in two ways:

$$r + s\sqrt{N} \mapsto r + sv \in \mathbb{Q}_2,$$

$$r + s\sqrt{N} \mapsto r - sv \in \mathbb{Q}_2.$$

Thus, the localizations K_D and K_{D^*} are identified with \mathbb{Q}_2 .

We now assume that the norm of the fundamental unit $\epsilon \in \mathcal{O}_K^*$ is -1 . Then, let

$$F/K = K(\sqrt{\epsilon})/K.$$

We can show:

Proposition 2.62. *Only one dyadic prime of K ramifies in F/K .*

Proof. Note that $\epsilon \cdot \epsilon^* = -1$. That is, in \mathbb{Z}_2^* , ϵ and ϵ^* are a pair of units with $\epsilon \cdot \epsilon^* = -1$. Also note that

$$\mathbb{Z}_2/8\mathbb{Z}_2 \cong \mathbb{Z}/8\mathbb{Z}.$$

If $\alpha, \beta \in \mathbb{Z}/8\mathbb{Z}$ with $\alpha \cdot \beta = -1$, then $\alpha, \beta \in (\mathbb{Z}/8\mathbb{Z})^*$ and so (α, β) is one of $(1, 7)$; $(7, 1)$; $(3, 5)$; $(5, 3)$. Observe that

$$\mathbb{Q}_2(\sqrt{7})/\mathbb{Q}_2, \text{ and } \mathbb{Q}_2(\sqrt{3})/\mathbb{Q}_2$$

are locally ramified. However, $\mathbb{Q}_2(\sqrt{5})/\mathbb{Q}_2$ is the unique unramified local quadratic extension, while $\mathbb{Q}_2(\sqrt{1})/\mathbb{Q}_2$ is trivial, and so unramified. Thus we can see that only one dyadic prime ideal of K ramifies in F/K .

□

3. Density Results

Using Chebotarev's Theorem we will prove that the four sets of primes:

$$X_1 = \{p \text{ prime} : p \equiv 1 \pmod{16}, p \in A^+(2)\}$$

$$X_2 = \{p \text{ prime} : p \equiv 1 \pmod{16}, p \in A^-(2)\}$$

$$X_3 = \{p \text{ prime} : p \equiv 9 \pmod{16}, p \in A^+(2)\}$$

$$X_4 = \{p \text{ prime} : p \equiv 9 \pmod{16}, p \in A^-(2)\}$$

have equal natural densities in the set of all primes.

3.1 Background

We will define the notions of Dirichlet Density, natural density and we will see how the Artin symbol is related to the splitting behavior of primes. Also we will state the Chebotarev's Theorem which we will use in the next section.

Definition 3.63. *A set \mathcal{P} of prime numbers has Dirichlet Density $d(\mathcal{P})$, if*

$$\lim_{s \rightarrow 1^+} \frac{\sum_{p \in \mathcal{P}} p^{-s}}{\sum_{p \text{ prime}} p^{-s}}$$

exists and equals $d(\mathcal{P})$.

Another notion of density, which we find it to be more natural is:

Definition 3.64. *A set \mathcal{P} of prime numbers has natural density $\Delta(\mathcal{P})$ if*

$$\lim_{n \rightarrow \infty} \frac{|\{p \leq n : p \in \mathcal{P}\}|}{|\{p \leq n : p \text{ prime}\}|}$$

exists and equals $\Delta(\mathcal{P})$.

If a set of primes has natural density, then it has Dirichlet density and the two densities are equal, see [24], page 252.

In 1837, Dirichlet proved the famous theorem:

Theorem 3.65. *Let n be a positive integer. Then for each a such that $(a, n) = 1$, the set of prime numbers p such that $p \equiv a \pmod{n}$ has natural density $1/\phi(n)$.*

Here, $\phi(n)$ denotes the Euler function, namely:

$$\phi(n) = |\{d : (d, n) = 1\}|$$

The most important consequence of this theorem is that in any arithmetic progression $a, a + n, a + 2n, \dots$ where $(a, n) = 1$, there are infinitely many prime numbers.

Now we will introduce the Artin symbol. First we have the following lemma:

Lemma 3.66. *Let $K \subset L$ be a Galois extension, and let \mathfrak{p} be a prime of \mathcal{O}_K which is unramified in L . If \mathfrak{q} is a prime of \mathcal{O}_L containing \mathfrak{p} , then there is a unique element $\sigma \in \text{Gal}(L/K)$ such that*

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{q}}, \text{ for all } \alpha \in \mathcal{O}_L,$$

where $N(\mathfrak{p}) = |\mathcal{O}_L/\mathfrak{p}|$ is the norm of \mathfrak{p} .

The proof of this lemma can be found in [6], for example.

Definition 3.67. *The unique element σ in Lemma 3.66, is called the Artin Symbol. We will denote this symbol by $\left(\frac{L/K}{\mathfrak{q}}\right)$ as it depends on K, L and \mathfrak{q} .*

Now we list the properties of the Artin symbol which are going to be used in the next section.

Lemma 3.68. *Let $K \subset L$ be a Galois extension, and let \mathfrak{p} be a prime of \mathcal{O}_K which is unramified in \mathcal{O}_L . Given \mathfrak{q} a prime of \mathcal{O}_L containing \mathfrak{p} , we have:*

(i) \mathfrak{p} splits completely in \mathcal{O}_L if and only if $\left(\frac{L/K}{\mathfrak{q}}\right) = \text{id}$

(ii) If $K = \mathbb{Q}$, then $\left(\frac{L/K}{\mathfrak{p}}\right) = \{g\} \subset Z(\text{Gal}(L/\mathbb{Q}))$ if and only if \mathfrak{p} splits completely in $Z(G)'$.

In the above $\{g\}$ denotes the conjugacy class of g (and contains only one element since $g \in Z(\text{Gal}(L/\mathbb{Q}))$), $Z(G)$ is the center of the group G , and $Z(G)'$ is the fixed field of $Z(G)$.

The main theorem which we need is Chebotarev's Density Theorem, 1922:

Theorem 3.69. *Let N be a normal extension of \mathbb{Q} , $G = \text{Gal}(N/\mathbb{Q})$, q a rational prime unramified in N/\mathbb{Q} , and C_g the conjugacy class of $g \in G$. Then the set of rational primes q for which $\left(\frac{N/\mathbb{Q}}{q}\right) = C_g$ has natural density $|C_g|/|G|$.*

The proof of this theorem can be found in [29] or [27].

Corollary 3.70. *The set of rational primes p that split completely in N has natural density $1/|G|$.*

Proof. Let p be a rational prime that is unramified in N . Since p splits completely in N , by Lemma 2.5 (i) we obtain:

$$\left(\frac{N/\mathbb{Q}}{p}\right) = \{\text{id}_{\text{Gal}(N/\mathbb{Q})}\}$$

Applying Theorem 2.6 we get that the set of primes p for which

$$\left(\frac{N/\mathbb{Q}}{p}\right) = \{\text{id}_{\text{Gal}(N/\mathbb{Q})}\}$$

has natural density $|\text{id}_G|/|G|$. Therefore, the set of rational primes p that split completely in N has natural density $1/|G|$. \square

Another result that we need is (see [31]):

Theorem 3.71. *Let K be a number field, and let L and M be two extensions of K . Then for a prime \mathfrak{p} of K we have:*

(i) *If \mathfrak{p} splits completely in both L and M , then \mathfrak{p} splits completely in LM ,*

(ii) *If \mathfrak{p} is unramified in both L and M , then \mathfrak{p} is unramified in LM .*

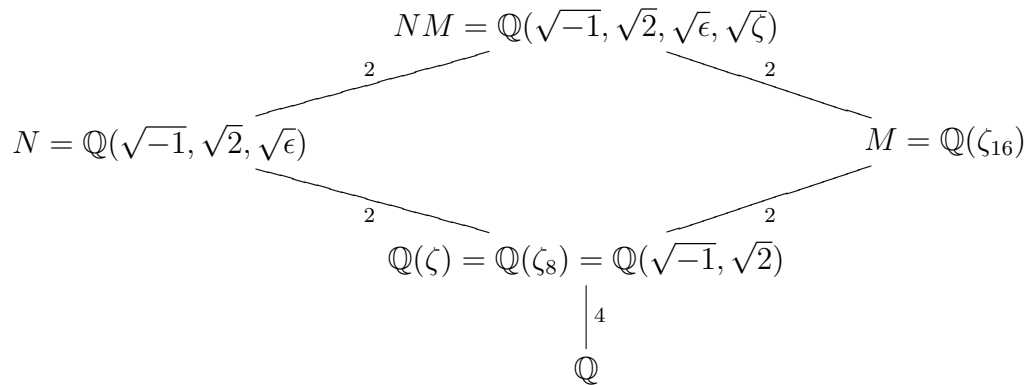
An immediate consequence of the above theorem is:

Corollary 3.72. *Let K and L be number fields, $K \subset L$ and let \mathfrak{p} be a prime of K . Then:*

- (i) *If \mathfrak{p} splits completely in L , then \mathfrak{p} splits completely in the normal closure M of L over K ,*
- (ii) *If \mathfrak{p} is unramified in L , then \mathfrak{p} is unramified in the normal closure M of L over K .*

3.2 The Extension

Consider the following extension:



Here, $\epsilon = 1 + \sqrt{2}$ is the fundamental unit of $\mathbb{Q}(\sqrt{2})$ which has norm -1 . The Galois group $G = \text{Gal}(NM/\mathbb{Q})$ is given by the following table:

	$\sqrt{-1}$	$\sqrt{2}$	$\sqrt{\zeta}$	$\sqrt{\epsilon}$	Order
σ_1	+	+	+	+	1
σ_2	+	+	+	-	2
σ_3	+	+	-	+	2
σ_4	+	+	-	-	2
σ_5	+	-	+	$\sqrt{\bar{\epsilon}}$	2
σ_6	+	-	+	$-\sqrt{\bar{\epsilon}}$	2
σ_7	+	-	-	$\sqrt{\bar{\epsilon}}$	2
σ_8	+	-	-	$-\sqrt{\bar{\epsilon}}$	2
σ_9	-	+	$\sqrt{\bar{\zeta}}$	-	2
σ_{10}	-	+	$\sqrt{\bar{\zeta}}$	+	2
σ_{11}	-	+	$-\sqrt{\bar{\zeta}}$	-	2
σ_{12}	-	+	$-\sqrt{\bar{\zeta}}$	+	2
σ_{13}	-	-	$\sqrt{\bar{\zeta}}$	$\sqrt{\bar{\epsilon}}$	4
σ_{14}	-	-	$\sqrt{\bar{\zeta}}$	$-\sqrt{\bar{\epsilon}}$	4
σ_{15}	-	-	$-\sqrt{\bar{\zeta}}$	$\sqrt{\bar{\epsilon}}$	4
σ_{16}	-	-	$-\sqrt{\bar{\zeta}}$	$-\sqrt{\bar{\epsilon}}$	4

The center of this group is

$$Z(G) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\} \cong C_2 \times C_2$$

since all the elements of $Z(G)$ have order two.

In [4], Addendum (3.7), the authors proved the following:

Proposition 3.73. *The prime p splits completely in N over \mathbb{Q} if and only if $p \in A^+(2)$.*

Also, we recall the classic result, see [24]:

Proposition 3.74. *The rational prime p splits completely in $\mathbb{Q}(\zeta_m)$ if and only if $p \equiv 1 \pmod{m}$.*

Let $\Omega = \{p \text{ prime} : p \equiv 1 \pmod{8}\}$. We have the following properties of $p \in \Omega$. By [35], Proposition 3.65, we have:

Proposition 3.75. *If $p \in \Omega$ then p is unramified in N .*

Also, from [31], page 27, we obtain $\text{disc}(\mathbb{Q}(\zeta_{16})) \mid 16^{\phi(16)}$, whence

$$\text{disc}(\mathbb{Q}(\zeta_{16})) \mid (2^4)^8 = 2^{32}.$$

Recall that an odd prime p is unramified in a number field F if and only if $p \nmid \text{disc}(F)$. Thus every odd rational prime p is unramified in $\mathbb{Q}(\zeta_{16})$. Let us state this:

Proposition 3.76. *Every $p \in \Omega$ is unramified in $M = \mathbb{Q}(\zeta_{16})$.*

Using Propositions 3.75, 3.76 and Theorem 3.71 (ii) we obtain:

Theorem 3.77. *If $p \in \Omega$ then p is unramified in NM .*

Also, from Propositions 3.73, 3.74 and Theorem 3.71 (i) we get:

Theorem 3.78. *If $p \in \Omega$ then p splits completely in NM .*

Therefore we have the following splitting behavior:

Theorem 3.79. *(i) p splits completely in N and M iff $p \equiv 1 \pmod{16}$ and*

$$p \in A^+(2) \text{ iff } \left(\frac{MN/\mathbb{Q}}{p}\right) = \{\sigma_1\},$$

(ii) p splits completely in N , yet not in M iff $p \equiv 9 \pmod{16}$ and $p \in A^+(2)$ iff

$$\left(\frac{MN/\mathbb{Q}}{p}\right) = \{\sigma_3\},$$

(iii) p splits completely in M , yet not in N iff $p \equiv 1 \pmod{16}$ and $p \in A^-(2)$ iff

$$\left(\frac{MN/\mathbb{Q}}{p}\right) = \{\sigma_2\},$$

(iv) p splits completely neither in N nor in M iff $p \equiv 9 \pmod{16}$ and $p \in A^-(2)$
iff $\left(\frac{MN/\mathbb{Q}}{p}\right) = \{\sigma_4\}$.

Proof. The proof follows easily from 3.68, 3.71, 3.73, 3.74, 3.77, 3.78 since $Z(G)' = \mathbb{Q}(\zeta)$. □

Let us apply Chebotarev's Density Theorem 3.69 to our extension NM/\mathbb{Q} . Thus we obtain:

Theorem 3.80. *The four sets of primes X_1, X_2, X_3, X_4 have the same natural density in Ω , namely $1/4$.*

References

- [1] A. Baker, *Linear Forms in the logarithms of algebraic number I*, *Mathematika* **13** (1966), 204–216.
- [2] Z. I. Borevich and I. R. Shatarevich, *Number Theory*, Academic Press, New York, 1966.
- [3] L. Carlitz, *A characterization of algebraic number fields with class number two*, *Proc. Am. Math. Soc.* **11** (1960), 391–392.
- [4] P. Conner, J. Hurrelbrink *Class Number Parity*, Series in Pure Mathematics, **8**, World Scientific, 1988.
- [5] P. E. Conner and J. Hurrelbrink, *On elementary abelian 2-Sylow K_2 of rings of integers of certain quadratic number fields*, *Acta Arith.* **73** (1995), 59–65.
- [6] D. Cox, *Primes of the Form $X^2 + nY^2$: Fermat, Class Field Theory, and Complex Multiplication*, Wiley, New York, 1989.
- [7] C. de la Vallée-Poussin, *Recherches analytiques sur la théorie des nombres premiers. Deuxième partie: Les fonctions de Dirichlet et les nombres premiers de la forme linéaire $Mx + N$* , *Ann. Soc. Sci. Bruxelles* **20** (1896), 281–362.
- [8] P. G. L. Dirichlet, *Vorlesungen über Zahlentheorie*, Chelsea, New York, 1968.
- [9] J. Esmonde and M. Ram Murty, *Problems in Algebraic Number Theory*, Graduate Texts in Math. Vol. **190**, Springer-Verlag, New York, 1999.
- [10] J. Gallian, *Contemporary Abstract Algebra*, Third Ed. Heath, Lexington, MA, 1994.
- [11] H. Garland, *A finiteness theorem for K_2 of a number field*, *Ann. of Math.* **94** (1971), 534–548.
- [12] C. F. Gauss, *Disquisitiones Arithmeticae*, Göttingen, 1801.
- [13] F. Gerth, *The 4-class ranks of quadratic extensions of certain imaginary quadratic fields*, *Ill. J. of Math.* **33** (1989), 132–142.
- [14] F. Gerth, *The 4-class ranks of quadratic extensions of certain real quadratic fields*, *J. Number Theory* **33** (1989), 18–31.
- [15] F. Gerth, *The 4-class ranks of quadratic fields*, *Inventiones mathematicae* **77** (1984), 489–515.
- [16] L. J. Goldstein, *Analytic Number Theory*, Prentice Hall, N.J. 1971.

- [17] E. Hecke, *Über die L-Funktionen und den Dirichletschen Primzahlsatz für einen beliebigen Zahlkörper*, Nachr. Akad. Wiss. Göttingen Math. - Phys. Kl. (1917), 299–318.
- [18] K. Heegner, *Diophantische Analysis und Modulfunktionen*, Math. Zeit. **56** (1952), 227–253.
- [19] H. Heilbronn and E. H. Linfoot, *On the imaginary quadratic corpora of class number one*, Quart. J. Math. Oxford Ser. **5** (1934), 293–301.
- [20] D. Hilbert, *Über die Zerlegung der Ideale eines Zahlkörpers in Primideale*, Math. Annalen **44** (1894), 1–8.
- [21] T. Hungerford, *Algebra*, Graduate Texts in Math. Vol. **73**, Springer-Verlag, New York, 1974.
- [22] J. Hurrelbrink and M. Kolster, *Tame kernels under relative quadratic extensions and Hilbert symbols*, J. reine angew. Math. **499** (1998), 145–188.
- [23] J. Hurrelbrink, *Circulant Graphs and 4-Ranks of Ideal Class Groups*, Can. J. Math. **46** (1994), 169–183.
- [24] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Second Ed. Graduate Texts in Math. Vol. **84**, Springer-Verlag, New York, 1990.
- [25] G. Janusz, *Algebraic Number Fields*, Academic Press, New York, 1973.
- [26] C. U. Jensen and N. Yui, *Quaternion Extensions*, Algebraic Geometry and Commutative Algebra in Honor of Masayoshi Nagata, 1987, 155–182.
- [27] J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarëv density theorem*, Algebraic Number Fields, L-functions and Galois properties, Proc. of the 1975 Durham Symposium, Academic Press, London 1977, 409–464.
- [28] J. C. Lagarias, *On Determining the 4-Rank of the Ideal Class Group of a Quadratic Field*, J. Number Theory **12** (1980), 191–196.
- [29] S. Lang, *Algebraic Number Theory*, Addison-Wesley, Reading, MA, 1970.
- [30] H. W. Lenstra, Jr. and P. Stevenhagen, *Chebotarëv and his Density Theorem*, The Mathematical Intelligencer Vol. **18**, No. 2, Springer-Verlag, New York, 1996.
- [31] D. Marcus, *Number Fields*, Springer-Verlag, New York, 1977.
- [32] H. Matsumoto, *Sur les sous-groupes arithmétiques des groupes semi-simples déployés*, Ann. Sci. Éc. Norm. Sup. 4^e serie, **2** (1969), 1-62.

- [33] J. Milnor, *An Introduction to Algebraic K-Theory*, Ann. Math. Studies. Vol. **72**, Princeton Univ. Press, Princeton, 1971.
- [34] P. Morton, *Density results for the 2-classgroups and fundamental units of real quadratic fields*, Studia Scientiarum Math. Hungarica **17** (1982), 21–43.
- [35] R. Osburn, *Densities of 4-ranks of K_2 of rings of integers*, Ph.D. Thesis, Baton Rouge, 2001.
- [36] H. Qin, *The 2-Sylow subgroups of the tame kernel of imaginary quadratic fields*, Acta Arith. **69** (1995), 153–169.
- [37] H. Qin, *The 4-ranks of $K_2(\mathcal{O}_F)$ for real quadratic fields*, Acta Arith. **72** (1995), 323–333.
- [38] D. Quillen, *Higher algebraic K-theory*, Algebraic K-Theory I, Lecture Notes in Mathematics, Vol. **341**, Springer-Verlag, New York, 1973, 85–147.
- [39] L. Rédei and H. Reichardt, *Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, J. reine angew. Math. **170** (1933), 69–74.
- [40] L. Rédei, *Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper*, J. reine angew. Math. **171** (1934), 55–60.
- [41] L. Rédei, *Eine obere Schranke der Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper*, J. reine angew. Math. **171** (1934), 61–64.
- [42] L. Rédei, *Über die Klassenzahl des imaginären quadratischen Zahlkörpers*, J. reine angew. Math. **159** (1928), 210–219.
- [43] L. Rédei, *Über die Grundeinheit und die durch 8 teilbaren Invarianten der absoluten Klassengruppe in quadratischen Zahlkörpern*, J. reine angew. Math. **171** (1934), 131–148.
- [44] H. Reichardt, *Zur Struktur der absoluten Idealklassengruppe im quadratischen Zahlkörper*, J. reine angew. Math. **170** (1934), 75–82.
- [45] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, 1979.
- [46] J. P. Serre, *A Course in Arithmetic*, Graduate Texts in Math. Vol. **7**, Springer-Verlag, 1973.
- [47] J. R. Silvester, *Introduction to Algebraic K-Theory*, Chapman and Hall, London, 1981.

- [48] H. M. Stark, *A complete determination of the complex quadratic fields of class number one*, Michigan Math. J. **14** (1967), 1–27.
- [49] P. Stevenhagen, *On the Solvability of the Negative Pell Equation*, preprint.
- [50] J. Tate, *Relations between K_2 and Galois cohomology*, Invent. Math. **36** (1976), 257–274.
- [51] J. Tate, *Symbols in arithmetic*, Actes du Congrès International des Mathématiciens, Tome **1**, Nice, 1970, 201–211.
- [52] A. Vazzana, *Elementary abelian 2-primary parts of $K_2(\mathcal{O})$ and related graphs in certain quadratic number fields*, Acta Arith. **81** (1997), 253–264.
- [53] A. Vazzana, *On the 2-primary part of K_2 of rings of integers in certain quadratic number fields*, Acta Arith. **80** (1997), 225–235.
- [54] M. Watkins, *Atlas Mathematical Conference Abstract Service*, available at <http://at.yorku.ca/cgi-bin/amcal>.
- [55] H. Weyl, *Algebraic Theory of Numbers*, Princeton University Press, Princeton, 1940.
- [56] A. Wiles, *The Iwasawa conjecture for totally real fields*, Ann. Math. **131** (1990), 493–540.

Appendix: List of Primes

List 1

Let p be a prime number and consider the field $K = \mathbb{Q}(\sqrt{2p})$. Denote by ϵ the fundamental unit of the field K .

The last column represents the number of primes with $N(\epsilon) = -1$ over the total number of primes.

Primes \leq	$N(\epsilon) = +1$	$N(\epsilon) = -1$	
10000	815	413	0.3363192182410423452768729641
20000	1513	748	0.3308270676691729323308270676
30000	2163	1081	0.3332305795314426633785450061
40000	2803	1399	0.3329366968110423607805806758
50000	3428	1704	0.3320342946219797349961028838
60000	4035	2021	0.3337186261558784676354029062
70000	4635	2299	0.3315546582059417363715027401
80000	5224	2612	0.333333333333333333333333333333
90000	5797	2915	0.334595959595959595959595959595
100000	6393	3198	0.3334375977478886456052549264
110000	6971	3481	0.3330463069269039418293149636
120000	7536	3764	0.3330973451327433628318584070
130000	8103	4055	0.3335252508636288863299884849
140000	8678	4331	0.3329233607502498270428165116
150000	9227	4620	0.3336462771719506030187044125
160000	9794	4888	0.3329246696635335785315352131
170000	10334	5162	0.3331182240578213732576148683
180000	10886	5455	0.3338228994553576892479040450
190000	11452	5717	0.3329838662706039955734172054
200000	11980	6003	0.3338152699772006895401212255
210000	12518	6288	0.3343613740295650324364564500

List 3

Let p be prime number, $p \equiv 1 \pmod{16}$, $p \in A^+$ and consider the field $K = \mathbb{Q}(\sqrt{2p})$. Denote by ϵ the fundamental unit of the field K .

The last column represents the number of primes with $N(\epsilon) = -1$ over the total number of primes.

Primes \leq	$N(\epsilon) = +1$	$N(\epsilon) = -1$	
160000	592	303	0.3385474860335195530726256983
320000	1111	587	0.3457008244994110718492343933
480000	1632	824	0.3355048859934853420195439739

Vita

Costel Ionita was born on January 16, 1972, in Focsani, Romania. He finished his undergraduate studies at University of Bucharest in May 1995. In August 2000 he came to Louisiana State University to pursue graduate studies in mathematics. He earned a master of science degree in mathematics from Louisiana State University in May 2002. He is currently a candidate for the degree of Doctor of Philosophy in mathematics, which will be awarded in August 2004.