

Louisiana State University

LSU Scholarly Repository

LSU Historical Dissertations and Theses

Graduate School

1988

Class Numbers and Units of Number Fields E With Elementary Abelian $K(2)O(E)$.

Ruth Ilse Berger

Louisiana State University and Agricultural & Mechanical College

Follow this and additional works at: https://repository.lsu.edu/gradschool_disstheses

Recommended Citation

Berger, Ruth Ilse, "Class Numbers and Units of Number Fields E With Elementary Abelian $K(2)O(E)$." (1988). *LSU Historical Dissertations and Theses*. 4483.
https://repository.lsu.edu/gradschool_disstheses/4483

This Dissertation is brought to you for free and open access by the Graduate School at LSU Scholarly Repository. It has been accepted for inclusion in LSU Historical Dissertations and Theses by an authorized administrator of LSU Scholarly Repository. For more information, please contact gradetd@lsu.edu.

INFORMATION TO USERS

The most advanced technology has been used to photograph and reproduce this manuscript from the microfilm master. UMI films the original text directly from the copy submitted. Thus, some dissertation copies are in typewriter face, while others may be from a computer printer.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyrighted material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each oversize page is available as one exposure on a standard 35 mm slide or as a 17" × 23" black and white photographic print for an additional charge.

Photographs included in the original manuscript have been reproduced xerographically in this copy. 35 mm slides or 6" × 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.



Accessing the World's Information since 1938

300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA

Order Number 8819923

**Class numbers and units of number fields E with elementary
abelian $K_2(O_E)$**

Berger, Ruth Ilse, Ph.D.

The Louisiana State University and Agricultural and Mechanical Col., 1988

U·M·I
300 N. Zeeb Rd.
Ann Arbor, MI 48106

Class numbers and units
of number fields E with elementary abelian $K_2(O_E)$

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

Ruth Ilse Berger

Vordiplom, Universität des Saarlandes, 1981

M.S., Louisiana State University, 1985

May 1988

Acknowledgments

I would like to thank my advisor Dr. J. Hurrelbrink for suggesting the problem and for supervising my progress on it. I would especially like to thank Dr. P.E. Conner who suggested many of the results and who helped me find access to their proofs. I am very grateful to Dr. J.W. Hoffman who was always available to discuss problems and who spent a lot of time on reading the first version and pointing out several mistakes.

Table of Contents

Abstract	iv
Introduction	v
 Chapter 1: Approaching the problem	1
1. Collection of facts about $K_2(O_F)$	2
2. Quadratic number fields	7
3. Biquadratic dicyclic number fields	9
4. Biquadratic cyclic number fields	11
 Chapter 2: Number fields with property (*)	18
5. Setting up the tools	19
6. The exact hexagon	26
7. Characterizing number fields with property (*)	29
8. The existence of number fields with property (*)	34
 Chapter 3: The complete picture	40
9. Detailed properties	40
10. Completions and generalized ideal class groups	44
11. Families of number fields with property (*)	53
12. The main theorem	60
 Chapter 4: Examples	69
13. Application to $F = \mathbb{Q}$	70
14. Biquadratic dicyclic number fields with property (*)	73
15. The fields $\mathbb{Q}(\sqrt{\varepsilon\sqrt{2q}})$ with $q \equiv 5 \pmod{8}$	74
16. Quadratic extensions of $\mathbb{Q}(\sqrt{10})$ with property (*)	78
 Bibliography	83

Class numbers and units of number fields E with elementary abelian $K_2(O_E)$.

by Ruth I. Berger

Abstract

This is a contribution to the research that is going on in Algebraic Number Theory, relating classical questions on class numbers and units of a number field F to the structure of $K_2(O_F)$, the Milnor K-group K_2 of the ring of integers.

We are interested in number fields F where the 2-primary subgroup of $K_2(O_F)$ is elementary abelian of rank $r_1(F)$, the number of real embeddings of F .

In [C- H_1] it is proven that the 2-primary subgroup of $K_2(O_F)$ is of the above type if and only if the number field has the following properties:

- a) the number field has exactly one dyadic prime,
- b) its S-class number is odd and
- c) it contains S-units with independent signs.

Here, the set S consists of all dyadic and all infinite primes of the number field.

The purpose of this paper is to examine the existence of number fields of the above type and to examine their properties with respect to the parity of their class number and the containment of units with independent signs. We will mostly restrict our attention to number fields that are totally real. For any given totally real number field F that satisfies the above properties we will prove that there exist infinitely many real quadratic extensions that also have the above properties. The main theorem will be a classification of these quadratic extensions of F into families that all share the same properties with respect to the parity of their class number and the containment of units with independent signs.

Introduction

Let us first review the objects that classical Number Theory deals with.

The field of rational numbers \mathbb{Q} contains the ring of integers \mathbb{Z} . The integers contain two kinds of elements that stand out: the units and the prime elements.

The units are defined as the integers u with the following property: there exists an integer x such that $ux = 1$. The elements of \mathbb{Z} that satisfy this property are 1 and -1 . The prime elements of \mathbb{Z} are defined as the integers p with the following property: if a, b are integers such that $ab = p$ then either a or b must equal p , up to unit factors ± 1 . The units and the prime elements are the “building blocks” for all integers. Up to factors of ± 1 , every integer can be expressed **uniquely** as a product of powers of prime numbers.

Instead of considering the field \mathbb{Q} , one can look more generally at a **number field**. These fields are defined as the finite algebraic extensions of \mathbb{Q} . This means that a finite number of roots of polynomials with coefficients in \mathbb{Q} are adjoined to \mathbb{Q} . A number field F shares many of the properties of \mathbb{Q} . F also contains what are called integers. They are defined as the integral closure of the rational integers, i.e., the roots of monic polynomials whose coefficients are in \mathbb{Z} . The integers of a number field F are denoted by O_F . Among the integers there are elements called units. As before, they are defined as the integers u with the property that there exists an integer x such that $ux = 1$. Note that x must then be a unit, too. The units form a multiplicative group. It is denoted by O_F^* .

In general, there are no integers that behave like the prime elements (numbers) of \mathbb{Z} ; there are no “smallest factors” of which all integers can be **uniquely** expressed as a product. Therefore the idea of integers and prime elements needs to be generalized to objects that reflect this property of being minimal factors. This is done by introducing the concept of ideals. They are subsets of the ring of integers that are obtained by taking a set of integers, called the generators of the ideal, and taking all possible finite sums of products of these elements with integers. If the generators are taken to be arbitrary field elements, the resulting ideal is called a fractional ideal. The set of all fractional ideals of a number field form a group. Those ideals that are generated by only one element are called principal ideals.

A prime ideal is defined to be an ideal with the following property: if the product of two integers is contained in the ideal, then at least one of the integers must be contained in the ideal. Note that this mimics the property of a prime element in \mathbb{Z} : if the product of two integers equals a prime element, then one of the integers must equal the prime element (up to units). The ring of integers of a number field is an example of a Dedekind ring. In such a ring every ideal can be factored uniquely as a product of prime ideals.

In \mathbb{Q} we also have ideals. Here, every ideal is generated by one integer. The prime ideals are exactly those that are generated by a prime element. This explains why prime ideals can be considered a generalization of prime elements.

If all ideals of the ring of integers of a number field happen to be principal, then we in fact have unique prime element decomposition.

One defines $C(F)$, the **ideal class group** of F as the quotient $I(F)/P(F)$ of the group of all fractional ideals of F by the subgroup of principal ideals of F . For any number field F the ideal class group is a finite group. The number of elements in $C(F)$ is the **class number** of F , denoted by $h(F)$. For number fields where every ideal is principal, like for \mathbb{Q} , the class number is 1. The number fields where this occurs, however, form a very small set among all number fields. In general it is very difficult to determine the class number of a given number field or even to determine whether the class number is 1 or not. In many cases one is therefore content with just determining whether the class number is even or odd.

The prime ideals of a number field are often called the **finite primes** of the number field. As this notation indicates, to a number field there are associated objects called infinite primes. They are defined as the embeddings of the number field into the complex numbers. \mathbb{Q} contains exactly one “infinite prime”, since there is exactly one way of embedding \mathbb{Q} into \mathbb{C} . In fact, \mathbb{Q} already embeds into the real numbers \mathbb{R} . In general, a number field F embeds into \mathbb{C} in different ways. Some embeddings can take F into \mathbb{R} , they are called real embeddings of F . A number field is called totally real if all of its embeddings are real embeddings. \mathbb{Q} is an example of a totally real number field.

Let $r_1(F)$ denote the number of real embeddings of a number field F . For every $x \in F$ there are $r_1(F)$ real numbers associated to x , namely the images of x under

the real embeddings of F . Some of these images are positive, others are negative. They are 0 iff $x = 0$. From the independence of valuations it follows that for any given $r_1(F)$ -tupel of ± 1 there is an integer $x \in F$ whose images under the $r_1(F)$ embeddings have exactly these signs. For some number fields it is even possible to find a set of **units** of F whose images under the $r_1(F)$ embeddings have any prescribed signs. Number fields with this property are said to contain **units with independent signs**.

The concept of units and the ideal class group of a number field F can be generalized in the following way:

Note that a principal ideal that is generated by a unit must be the whole ring, since it contains 1. A unit therefore has no prime divisors. If we let $\text{ord}_P(x)$ denote the order to which the finite prime P appears in the prime ideal decomposition of the principal ideal generated by x , then the units of F can be expressed as:

$$O_F^* = \{x \in F \mid \text{ord}_P(x) = 0 \text{ for all finite primes } P \text{ of } F\}$$

We obtain a bigger group by lifting some of the conditions:

Let S be a set consisting of a finite number of primes of F (S is usually required to contain all infinite primes of F), then the group of **S-units** of F is defined as:

$$U_F^S = \{x \in F \mid \text{ord}_P(x) = 0 \text{ for all finite primes } P, P \notin S\}$$

We say that F contains **S-units with independent signs** if there are S -units of F whose images under the $r_1(F)$ embeddings have any prescribed signs.

If we take $C(F)$, the ideal class group of F , and factor out the subgroup generated by finite primes that are contained in S we obtain $C^S(F)$, the **S-ideal class group** of F . The number of elements in $C^S(F)$ is the **S-class number** of F , $h^S(F)$. Note that $h^S(F)$ is a divisor of $h(F)$.

In the following, S will stand for a special collection of primes: S will denote the set containing all **dyadic** and all infinite primes of F .

Dyadic primes of F are defined to be the prime ideals of F that contain the rational prime number 2. Every other prime ideal of F contains exactly one odd prime number, they will be referred to as **odd primes** or **nondyadic primes**. Note that

a number field can contain several dyadic prime ideals, unlike \mathbb{Q} which has only one.

We can now give an overview over the content of this dissertation:

For the choice of S specified above we will examine number fields F with the following properties: F has exactly one dyadic prime, the S -class number of F is odd and F contains S -units with independent signs. These number fields are of interest because they are exactly the number fields whose 2-primary subgroup of the Milnor K -group of the ring of integers of F is elementary abelian of smallest possible rank.

Examples of number fields that have the above property are: \mathbb{Q} , $\mathbb{Q}(\sqrt{10})$ and $E = \mathbb{Q}(\sqrt{10+\sqrt{10}})$. An interesting property of E is that its class number is even, but its S -class number is odd and that it does not contain units with independent signs even though it contains S -units with independent signs. An example of such a number field had not been known before. The methods used in section 4 to prove that E has the claimed properties are rather elementary. From the general point of view they are unsatisfactory because they do not allow insight in **why** this example happens to have these properties. One is also left with the question: Are there other number fields that also satisfy all of the above properties?

In the second chapter we will therefore go about systematically examining number fields that have exactly one dyadic prime, odd S -class number and that contain S -units with independent signs. We will restrict our attention to totally real number fields. Number fields of this type will be said to have **property (*)**. We will see that for a number field F with property (*), there always exist infinitely many quadratic extensions E that also have property (*). These quadratic extensions $E|F$ all have the property that at most one odd prime of F ramifies in E . In fact, there is exactly one extension in which no odd prime of F ramifies, in all the others exactly one of the odd primes of F will ramify.

In the third chapter we give a complete classification of all quadratic extensions E with property (*) of a given number field F with property (*). This classification will be with respect to the parity of the class number of E , whether E contains units with independent signs and whether the dyadic prime of F ramifies in E . We will show that all information about what type of quadratic extension with property (*)

exists over a given F is already contained in the finite group of square classes of the completion of F at its dyadic prime.

From this general consideration we will see that there are infinitely many number fields that have the same properties as $\mathbb{Q}(\sqrt{10+\sqrt{10}})$, above.

Chapter 4 illustrates applications. Here we will also see how the special example from section 4 fits in the general picture.

CHAPTER 1

Approaching the problem

In the first chapter we will examine number fields of small degrees in search of examples of number fields with certain properties. The number fields we are interested in are those that contain exactly one dyadic prime, have odd S-class number and that contain S-units with independent signs. Here S is the set consisting of all infinite primes and all dyadic prime of the number field.

In section 1 we will see how the interest in these number fields arises from K-theory. An example of a number field that has all of the above properties is \mathbb{Q} .

One can impose further conditions on the number field by making requirements on the parity of its honest class number and the existence of honest units with independent signs in the number field.

Here the term "honest" is used to emphasize the distinction to "S-".

We ask: are there number fields E that have the above properties and furthermore:
A) we either have, that the class number of E is odd or that E contains units with independent signs, or both?

B) the class number of E is even and E does not contain units with independent signs?

The answer is yes in all cases.

In section 2 we will see that there are in fact infinitely many quadratic number fields that give rise to examples for each of the cases covered in A. Unfortunately, an example of a number field that satisfies the conditions in B does not exist among number fields of degree 2. We therefore need to consider higher degree extensions.

In section 3 we examine a certain type of number fields of degree 4: the biquadratic dicyclic number fields. Also among them, there is no example of type B.

In section 4 we therefore turn our attention to another type of number fields of degree 4: biquadratic cyclic number fields. Here we do find an example that satisfies the conditions of B: $\mathbb{Q}(\sqrt{10+\sqrt{10}})$.

We cannot deal with more general examples in this first chapter. Further examples will be given in chapter 4.

1. Collection of facts about $K_2(O_F)$

Let R be a ring, $E(R)$ the group generated by the elementary matrices with entries in R .

(1.1) Definition: $K_2(R)$ is the kernel of the universal central extension of $E(R)$.

For more details see for example [Mi, page 47]. We can think of $K_2(R)$ as the “nontrivial” relations among elementary matrices with entries in R .

We will now consider a special type of ring: the ring of integers of a number field F . It will be denoted by $R = O_F$. What does $K_2(O_F)$ look like? In [Ga] Garland shows that $K_2(O_F)$ is a finite abelian group for any number field F . Hence we have

$$(1.2) \quad K_2(O_F) = \prod_{i=1}^m \mathbb{Z}/2^{a_i} \times \prod_{\substack{i=1 \\ p \text{ odd primes}}}^{k_p} \mathbb{Z}/p^{b_i}$$

The order of the second product, the odd part of $K_2(O_F)$, is known for totally real abelian number fields. Mazur and Wiles, [M-W], have proven that for those number fields F the order of the odd part of $K_2(O_F)$ is exactly the odd part of the rational integer $|w_2(F) \cdot \zeta_F(-1)|$. This is a special case of the **Birch-Tate Conjecture** which suggests that for all totally real number fields

$$(1.3) \quad \#K_2(O_F) = |w_2(F) \cdot \zeta_F(-1)|$$

where ζ_F is the Dedekind zeta-function of F and $w_2(F)$ is the largest integer N such that the Galois group of $F(\mu_N)$ over F is an elementary abelian 2-group. Here μ_N denotes the group of N -th roots of unity. By the above remarks the odd part of this conjecture has been confirmed for all totally real abelian number fields. Less is known about the 2-primary subgroup of $K_2(O_F)$ which is therefore of particular interest. The 2-primary subgroup of $K_2(O_F)$ will be denoted by $2\text{-prim } K_2(O_F)$.

In [He] Hettling proved that the 2-part of the Birch-Tate Conjecture holds for totally real number fields F where 2-prim $K_2(O_F)$ is elementary abelian of rank $r_1(F)$. Here elementary abelian means elementary abelian 2-group, i.e. all factors are of the form $\mathbb{Z}/2$ and $r_1(F)$ denotes the number of real embeddings of F .

Kolster [Ko] has confirmed the 2-part of the Birch Tate Conjecture more generally for all number fields F where 2-prim $K_2(O_F)$ is elementary abelian. He also gives a criterion for when a number field has this property:

(1.4) Theorem: (Kolster)

Let F be a totally real number field . The following are equivalent:

- a) 2-prim $K_2(O_F)$ is elementary abelian
- b) No dyadic prime of F splits in $F(\sqrt{-1})$ and

$$2\text{-part } h^S(F(\sqrt{-1})) = 2\text{-part } h^S(F) \cdot 2^{2-\text{rk } C^S(F)}.$$

□

Notation: S is the set consisting of all dyadic and all infinite primes of F . The S -class group, $C^S(F)$, is defined as the quotient of the class group of F by the subgroup generated by the dyadic primes of F .

The S -class number of F , denoted by $h^S(F)$, is the order of the S -class group of F . The 2-rank of an abelian group G is denoted by $2\text{-rk } G$.

To determine the rank of 2-prim $K_2(O_F)$ we have Tate's 2-rank formula, see[Ta]:

(1.5) Theorem: (Tate)

Let $r_1(F)$ denote the number of real embeddings of F , $g_2(F)$ the number of dyadic prime ideals of F and $C^S(F)$ the S -class group of F . Then:

$$2\text{-rk } K_2(O_F) = r_1(F) + g_2(F) - 1 + 2\text{-rk } C^S(F)$$

□

Note that the smallest possible value for the 2-rank of $K_2(O_F)$ is $r_1(F)$. It occurs iff F has exactly one dyadic prime ($g_2(F) = 1$) and the S -class number of F , $h^S(F)$, is odd.

The smallest possible order for 2-prim $K_2(O_F)$ occurs if 2-prim $K_2(O_F)$ is elementary abelian and of smallest rank, which is $r_1(F)$. A criterion for when a number

field F has this property can be found in [C- H_1]:

(1.6) Theorem (Conner, Hurrelbrink)

Let F be a number field. The following are equivalent:

- a) 2-prim $K_2(O_F)$ is elementary abelian of rank $r_1(F)$
- b) F admits an extension $E|F$ with $\#K_2(O_E)$ odd
- c) F has exactly one dyadic prime, the S -class number of F is odd and F contains *S -units with independent signs*. (see definition below)

□

Remark: This has also been studied by Gras, see [Gr].

We now give the definition of S -units with independent signs for the special case where S is the set consisting of all dyadic and all infinite primes of F . To obtain the definition for the general case where S is any set of primes of F , we replace *dyadic* by *primes in S* in the following.

(1.7) Definition: The elements of $U_F^S := \{x \in F \mid \text{ord}_P(x) = 0 \text{ for all nondyadic finite primes of } F\}$ are the **S -units** of F .

F contains **S -units with independent signs** iff $\varphi : U_F^S / (U_F^S)^2 \rightarrow \{\mathbb{Z}/2\}^{r_1(F)}$ is surjective. This map is defined by mapping an S -unit (mod squares) to the signs of its images under the $r_1(F)$ real embeddings of F .

Remark: To understand the significance of the term “ S -units with independent signs”, note that it is a generalization of the term “units with independent signs”. The units of F are the elements of $O_F^* := \{x \in F \mid \text{ord}_P(x) = 0 \text{ for all finite primes } P \text{ of } F\}$.

(1.7') Definition: F contains **units with independent signs** iff

$\varphi : O_F^* / (O_F^*)^2 \rightarrow \{\mathbb{Z}/2\}^{r_1(F)}$ is surjective. This map is defined by mapping a unit (mod squares) to the signs of its images under the $r_1(F)$ real embeddings of F .

Remark: A real quadratic number field contains units with independent signs iff the norm of the fundamental unit is -1 . More generally, a totally real number field contains units with independent signs iff every totally positive unit is a square.

Note that for totally imaginary number fields F : $r_1(F) = 0$, hence φ is of course surjective. Therefore an imaginary number field always contains units with independent signs and also S -units with independent signs.

The following is an immediate consequence of (1.6.b):

(1.8) Corollary: If a number field satisfies one (and therefore all) of the properties in (1.6), then so does every subfield. \square

Recall the classical question: Which number fields F can be embedded in a number field E with odd class number $h(E)$? Since $K_0(O_F) = C(F) \times \mathbb{Z}$ this question can be reformulated as: Which number fields F can be embedded in a number field E where the torsion part of $K_0(O_E)$ is odd? Similarly one might ask: Which number fields F can be embedded in a number field E with $\#K_2(O_E)$ odd? Note that (1.6) answers this “embedding problem for K_2 ”.

Of course we must ask: Are there any number fields that satisfy the equivalent properties of (1.6)? An example of such a number field is \mathbb{Q} . For \mathbb{Q} we already have that the (honest) class number is odd and that \mathbb{Q} contains (honest) units with independent signs. Here the term *honest* is used as opposed to “ S -...” to emphasize the distinction.

Note that the S -class number is a factor of the honest class number. Hence, if a number field has odd honest class number then it also has odd S -class number. We also see that if a number field contains units with independent signs then it also contains S -units with independent signs since the honest units are contained in the set of S -units.

This gives rise to the following question: Is the “ S ” in (1.6.c) necessary? That is:

(1.9) Question: Are there number fields F that satisfy the properties of (1.6) and that furthermore satisfy:

- i) F has **odd** class number and **contains** units with independent signs?
- ii) F has **even** class number and does **not contain** units with independent signs?
- iii) F has **odd** class number and does **not contain** units with independent signs?
- iv) F has **even** class number and **contains** units with independent signs?

The answer will be yes in all cases. In section 2 we will see that there exist many number fields that satisfy the properties of (1.9) i,iii and iv. Examples of number fields that satisfy the properties in (1.9.ii) are more difficult to obtain. We will spend the remainder of this chapter searching for an example of this type. In section 4 we will obtain one example of such a number field. More examples will be given in the end.

Consider the following observation from [Hu]:

(1.10) Fact: (Conner):

Let F be a number field in which (2) is at most tamely ramified.

Then the following are equivalent:

- a) $2\text{-prim}K_2(O_F)$ is elementary abelian of rank $r_1(F)$
- b) $g_2(F) = 1$, $h(F)$ is odd and F contains units with indep. signs

This tells us that many number fields have the properties required in (1.9.i). It also tells us that in order to find number fields that are examples for the other cases we need to consider number fields where (2) is wildly ramified.

Note that wild ramification is necessary but **not** sufficient to obtain examples for (9.1) ii, iii and iv. Even in the case of wild ramification we can obtain a number field of the type (1.9.i), consider $F = \mathbb{Q}(\sqrt{2})$: Here we have: $2 \cdot O_F = (\sqrt{2})^2$, so F has exactly one dyadic prime. The elements ± 1 , $1 + \sqrt{2}$ and $-1 - \sqrt{2}$ are a set of units with independent signs and $h(F)=1$, which is odd.

We now wish to find number fields F for which $g_2(F) = 1$, $h^S(F)$ is odd, F contains S -units with independent signs **BUT** $h(F)$ is even and/or F does not contain units with independent signs. By (1.10) such examples can not be found among number fields of odd degree for the following reason:

If we want these fields to have only one dyadic prime, call it D , then $2 \cdot O_F = D^e$ for some positive integer e . Since e divides the degree of F , it is odd. By definition this means that (2) is at most tamely ramified.

We will therefore now examine number fields of even degree starting with quadratic number fields .

2. Quadratic number fields

Among quadratic number fields we will find many where $2\text{-prim}K_2(O_F)$ is elementary abelian of rank $r_1(F)$. We will not, however, find any that satisfy the condition that they have even class number **and** that they do not contain units with independent signs.

(2.1) Theorem: The quadratic number fields F where $2\text{-prim}K_2(O_F)$ is elementary abelian of rank $r_1(F)$ all have the property that $h(F)$, the class number of F , is odd **or** that F contains units with independent signs. For each of these cases there are in fact an infinite number of examples.

To prove (2.1) we will now collect some well known facts about quadratic number fields. From these a classification of all quadratic number fields F where $2\text{-prim}K_2(O_F)$ is elementary abelian of rank $r_1(F)$ will follow immediately. The classification will separate the fields according to the parity of $h(F)$ and whether or not F contains units with independent signs.

The proofs of the following facts can be found, for example, in [C- H_2]

(2.2) Fact: Let $F = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ squarefree, then the following are equivalent

- a) $2\text{-prim}K_2(O_F)$ is elementary abelian of rank $r_1(F)$
- b) $d = 2, p, 2p, -1, -2, -p, -2p$

where p is a prime with $p \equiv \pm 3 \pmod{8}$

□

(2.3) Fact: Let $F = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ squarefree, then the following are equivalent:

- a) The class number $h(F)$ is odd
- b) $d = -1, \pm 2, p$, where p is any odd prime and
 $d = -p, 2p, p_1 p_2$, for primes $p, p_1, p_2 \equiv 3 \pmod{4}$.

□

When determining whether a quadratic number field F has units with independent signs, recall that following the definition of units with independent signs in (1.7) we explained that an totally imaginary number field F always contains units with

independent signs. In particular: any imaginary quadratic number field contains units with independent signs. For real quadratic number fields we have the following criterion:

(2.4) Lemma: Let F be a real quadratic number field and let ε denote a fundamental unit of F , then:

$$F \text{ contains units with independent signs} \iff N_{F|Q}(\varepsilon) = -1$$

Proof: The set of units of F is $O_F^* = \{\pm \varepsilon^n | n \in \mathbb{Z}\}$. If $N(\varepsilon) = +1$, then $N(\pm \varepsilon^n) = N(\pm 1) \cdot N(\varepsilon)^n = +1$, i.e., the norm of every unit is $+1$. Since the norm is the product of the two conjugates, this shows that for every unit both it and its conjugate have the same sign. In this case F can not contain units with independent signs.

Conversely: if $N(\varepsilon) = -1$, then ± 1 and $\pm \varepsilon$ are a set of units with independent signs. □

The following can be found, for example, in [C- H_2]: 18.4, 19.9 and chapter 22.

(2.5) Fact: For the real quadratic fields $F = \mathbb{Q}(\sqrt{d})$ from (2.2) we have:

$$\begin{array}{lll} \text{if } d=2 & \text{then} & N(\varepsilon) = N(1 + \sqrt{2}) = -1 \\ \text{if } d=p & \text{with } p \equiv +3 \pmod{8} & \text{then } N(\varepsilon) = +1 \\ \text{if } d=p & \text{with } p \equiv -3 \pmod{8} & \text{then } N(\varepsilon) = -1 \\ \text{if } d=2p & \text{with } p \equiv +3 \pmod{8} & \text{then } N(\varepsilon) = +1 \\ \text{if } d=2p & \text{with } p \equiv -3 \pmod{8} & \text{then } N(\varepsilon) = -1 \end{array}$$

□

This gives a complete classification of all quadratic number fields $F = \mathbb{Q}(\sqrt{d})$ with the property that $K_2(O_F)$ is elementary abelian of rank $r_1(F)$:

	$h(F)$ odd	$h(F)$ even
F contains units with indep. signs	$d=2, -1, -2$ $d=-p$ with $p \equiv +3 \pmod{8}$ $d=+p$ with $p \equiv -3 \pmod{8}$	$d=-p$ with $p \equiv -3 \pmod{8}$ $d=+2p$ with $p \equiv -3 \pmod{8}$ $d=-2p$ with $p \equiv \pm 3 \pmod{8}$
F does not contain u.w.i.s.	$d=+p$ with $p \equiv +3 \pmod{8}$ $d=+2p$ with $p \equiv +3 \pmod{8}$	NONE!

Remark: Other examples of number fields F where $K_2(O_F)$ is elementary abelian of rank $r_1(F)$ are:

$F = \mathbb{Q}(\sqrt[3]{6})$ and $\mathbb{Q}(\xi_{2^k})$ with $k \geq 2$.

They can be found in [Hu], 4.2 and 13.11. All of these number fields have odd class numbers and contain units with independent signs.

We have now seen an infinite number of examples of number fields for each of the types we asked for in (1.9i). Missing so far is an example of the type (1.9ii), i.e a number field F where $2\text{-prim}K_2(O_F)$ is elementary abelian of rank $r_1(F)$ with even classnumber that does not contain units with independent signs! They do not exist among quadratic number fields. In view of (1.10) the next step is to look for them among number fields of degree 4.

3. Biquadratic dicyclic number fields

In this section we will show that among biquadratic dicyclic number fields there does not exist an example of the type described in (1.9ii). First we recall a criterion on how to distinguish among the different types of number fields of degree 4. It can be found, for example, in [C- H_2].

(3.1) Fact: Let $F=\mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z}$ squarefree, be a quadratic number field and let $E=F(\sqrt{\sigma}) = \mathbb{Q}(\sqrt{d}, \sqrt{\sigma})$ where $\sigma \in F^*$ but $\sigma \notin (F^*)^2$. The normal closure

of E over \mathbb{Q} is given by $\mathbb{Q}(\sqrt{d}, \sqrt{\sigma}, \sqrt{N_{E|\mathbb{Q}}(\sigma)})$. We have:

- a) $E|\mathbb{Q}$ is biquadratic dicyclic $\iff N_{F|\mathbb{Q}}(\sigma) \in \mathbb{Q}^2$
- b) $E|\mathbb{Q}$ is biquadratic cyclic $\iff d \cdot N_{F|\mathbb{Q}}(\sigma) \in \mathbb{Q}^2$
- c) $E|\mathbb{Q}$ is non-abelian biquadratic $\iff N_{F|\mathbb{Q}}(\sigma) \notin \mathbb{Q}^2$ and $d \cdot N_{F|\mathbb{Q}}(\sigma) \notin \mathbb{Q}^2$

□

Remarks: In case c) “non-abelian biquadratic” means that E is a number field of degree 4, but the normal closure of E is of degree 8. The Galois group of this normal closure over \mathbb{Q} is non-abelian. It is the dihedral group of order 8.

In case a) E has exactly 3 quadratic subfields. This follows from the fact that the Galois group $\text{Gal}(E|\mathbb{Q})$ is $\mathbb{Z}/2 \times \mathbb{Z}/2$, which has exactly three nontrivial subgroups.

In case b) E has exactly one quadratic subfield. This follows from the fact that the Galois group $\text{Gal}(E|\mathbb{Q})$ is $\mathbb{Z}/4$, which has exactly one nontrivial subgroup.

(3.2) Theorem: All biquadratic dicyclic number fields that satisfy the conditions in (1.6) have odd class number.

Proof: By (3.1) all biquadratic dicyclic number fields can be expressed in the form $E = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ with $d_1 \neq d_2 \in \mathbb{Z}$ squarefree. Which of these are possible candidates for an example of the so far missing type (1.9ii)?

Note that biquadratic dicyclic number fields will always be either totally real or totally imaginary. Since totally imaginary number fields always contain units with independent signs, we only need to consider totally real number fields if we want 2-prim $K_2(O_E)$ to be elementary abelian of rank $r_1(E)$. By (1.6b) we know that this property is hereditary. Hence we can restrict our attention to those number fields whose quadratic subfields F all have the property that $K_2(O_F)$ is elementary abelian of rank $r_1(F) = 2$. These were listed in (2.2), but by the previous step we need only the real fields. Therefore we can restrict our attention to those fields E whose quadratic subfields F are all of the form $F = \mathbb{Q}(\sqrt{d})$, with $d = 2, p, 2p$ where p is a prime and $p \equiv \pm 3 \pmod{8}$.

Let $E = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$, the 3 quadratic subfields are:

$$\mathbb{Q}(\sqrt{d_1}) \quad \mathbb{Q}(\sqrt{d_2}) \quad \text{and} \quad \mathbb{Q}(\sqrt{d_1 d_2})$$

Hence we need not only d_1 and d_2 but also $d_1 d_2$, modulo squares, to be contained in $\{2, p, 2p \mid p \equiv \pm 3 \pmod{8}\}$. This shows that at least one of d_1, d_2 must equal 2, the other can be either p or $2p$ where $p \equiv \pm 3 \pmod{8}$. The resulting fields are $\mathbb{Q}(\sqrt{2}, \sqrt{p})$ and $\mathbb{Q}(\sqrt{2}, \sqrt{2p})$, which are identical.

How far are we in the proof of (3.2)? We have seen that the only biquadratic dicyclic number fields that **might** satisfy the conditions of (1.6) and that might not contain units with independent signs are those that are of the form $E = \mathbb{Q}(\sqrt{2}, \sqrt{p})$ with $p \equiv \pm 3 \pmod{8}$. Whether or not they actually do have all these properties is irrelevant at the moment since the next two propositions state that all of these fields have **odd** class number $h(E)$. They can therefore **not** provide an example of the type required in (1.9ii)! \square

(3.3) Proposition: Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{p})$ with $p \equiv -3 \pmod{8}$, then $h(E)$ is odd.

Proof: Since the Legendre symbol $\left(\frac{2}{p}\right) = -1$ for $p \equiv -3 \pmod{8}$ we can apply [C- H_2], theorem 21.1. It tells us that $h(E)$ is odd. \square

(3.4) Proposition: Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{p})$ with $p \equiv +3 \pmod{8}$, then $h(E)$ is odd.

Proof: apply [C- H_2], theorem 21.2. \square

These two propositions conclude the proof of theorem (3.2). It would, however, be nice to know if these possible candidates for fields that **might** satisfy the conditions in (1.6) actually do have these properties. It does not seem possible to check this with elementary methods. We will therefore not pursue this question at the moment. Instead we refer to section 14. There we will see that number fields of the type $E = \mathbb{Q}(\sqrt{2}, \sqrt{p})$ with $p \equiv \pm 3 \pmod{8}$ in fact do satisfy the conditions of (1.6).

4. Biquadratic cyclic number fields

In this section we will prove that among biquadratic cyclic number fields there is

at least one number field with the properties required in (1.9ii). The methods used here are elementary. When we need facts that cannot be seen very easily we will refer to Hasse [Ha], where he computes many examples. Later, in section 15, we will again prove that the example from this section satisfies all requirements of (1.9ii). There we will see that it is in fact a member of an infinite set of examples.

(4.1) Theorem: Let $E = \mathbb{Q}(\sqrt{10+\sqrt{10}})$, then
 E is biquadratic cyclic,
 E has exactly one dyadic prime,
the S -class number of E is odd,
 E contains S -units with independent signs
but furthermore the class number of E is **even**
and E does **not** contain units with independent signs

The proof of (4.1) will follow from (4.3), (4.10), (4.11), (4.9) and (4.8a) below.

To get a better idea about the structure of E , note that $E = \mathbb{Q}(\sqrt{10+\sqrt{10}})$ can also be written as $\mathbb{Q}(\sqrt{\epsilon\sqrt{10}})$ with $\epsilon = 1 + \sqrt{10}$.

(4.2) Proposition: $E = \mathbb{Q}(\sqrt{10+\sqrt{10}})$ is biquadratic cyclic.

Proof: E is a quadratic extension of the quadratic field $F = \mathbb{Q}(\sqrt{10})$. We check that E is cyclic by using the criterion from (3.1): $N_{F|\mathbb{Q}}(\epsilon\sqrt{10}) = N_{F|\mathbb{Q}}(\epsilon) \cdot (-10) = (-9) \cdot (-10) = 3^2 10 \notin \mathbb{Q}^2$ but $10 \cdot N_{F|\mathbb{Q}}(\epsilon\sqrt{10}) = 3^2 10^2 \in \mathbb{Q}^2$. \square

(4.3) Proposition: $E = \mathbb{Q}(\sqrt{10+\sqrt{10}})$ has exactly one dyadic prime.

Proof: $F = \mathbb{Q}(\sqrt{10})$ is the only nontrivial subfield of E and (2) is ramified in $F|\mathbb{Q}$. From this it follows that \mathbb{Q} is the maximal subfield of E in which (2) is unramified. This shows that (2) is totally ramified in $E|F$. \square

(4.4) Proposition: $\{1, \sqrt{10}, \sqrt{10+\sqrt{10}}, \sqrt{10-\sqrt{10}}\}$ is an integral basis of $E = \mathbb{Q}(\sqrt{10+\sqrt{10}})$, i.e. a \mathbb{Z} -basis of O_E .

Proof: In [Ha] Hasse computes this integral basis of E . □

For $E = \mathbb{Q}(\sqrt{10+\sqrt{10}})$ we will now compute the elements of $\text{Gal}(E|\mathbb{Q}) = \mathbb{Z}/4$:

$\sqrt{10+\sqrt{10}}$ satisfies $x^2 = 10+\sqrt{10}$ and therefore $(x^2-10)^2 = 10$ or $x^4 - 20x^2 + 90 = 0$.

This shows that the minimal polynomial of $\sqrt{10+\sqrt{10}}$ over \mathbb{Q} is: $x^4 - 20x^2 + 90$.

The roots of this polynomial are: $\pm\sqrt{10+\sqrt{10}}$ and $\pm\sqrt{10-\sqrt{10}}$. To get a better idea of the structure of this minimal polynomial, note that it can also be expressed as:

$$x^4 - T_{E|\mathbb{Q}}(\epsilon\sqrt{10})x^2 - N_{E|\mathbb{Q}}(\epsilon\sqrt{10}) \quad \text{with roots: } \pm\sqrt{\epsilon\sqrt{10}} \text{ and } \pm\sqrt{-\epsilon\sqrt{10}}$$

The four embeddings of $E = \mathbb{Q}(\sqrt{10+\sqrt{10}})$ into the real numbers are given by :

$$\sqrt{10+\sqrt{10}} \mapsto \pm\sqrt{10\pm\sqrt{10}}$$

The two embeddings that fix $F = \mathbb{Q}(\sqrt{10})$ are: $\sqrt{10+\sqrt{10}} \mapsto \pm\sqrt{10+\sqrt{10}}$ because $\sqrt{10} = (\sqrt{10+\sqrt{10}})^2 - 10$ clearly is invariant under these two homomorphisms.

The other two embeddings must then map $\sqrt{10} \mapsto -\sqrt{10}$ and either one of them generates $\text{Gal}(E|\mathbb{Q})$. Let ξ denote the map that takes $\sqrt{10+\sqrt{10}} \mapsto \sqrt{10-\sqrt{10}}$. Then ξ^2 is the nontrivial map that fixes F , but it does not fix $\sqrt{10-\sqrt{10}} \notin F$. Therefore ξ^2 maps $\sqrt{10-\sqrt{10}}$ to the only remaining possible root which is $-\sqrt{10-\sqrt{10}}$.

This determines $\text{Gal}(E|\mathbb{Q})$ completely, so we have proved:

(4.5) Lemma: Let $E = \mathbb{Q}(\sqrt{10+\sqrt{10}})$. The Galois group $\text{Gal}(E|\mathbb{Q}) \simeq \mathbb{Z}/4$ is generated by the automorphism $\xi : E \rightarrow E$ where ξ maps the generators of E over \mathbb{Q} as follows:

$$\begin{aligned} \xi(\sqrt{10+\sqrt{10}}) &= \sqrt{10-\sqrt{10}} \\ \xi(\sqrt{10-\sqrt{10}}) &= \xi^2(\sqrt{10+\sqrt{10}}) = -\sqrt{10+\sqrt{10}} \\ \xi(\sqrt{10}) &= -\sqrt{10} \\ \xi(1) &= 1 \end{aligned}$$

Next, we will compute a formula for the norm of E over \mathbb{Q} , denoted by $N_{E|\mathbb{Q}}$.

An arbitrary element of E can be written as $a + b\sqrt{10} + c\sqrt{10+\sqrt{10}} + d\sqrt{10-\sqrt{10}}$ with $a, b, c, d \in \mathbb{Q}$. All of its conjugates are:

$$\text{id}(a + b\sqrt{10} + c\sqrt{10+\sqrt{10}} + d\sqrt{10-\sqrt{10}}) = a + b\sqrt{10} + c\sqrt{10+\sqrt{10}} + d\sqrt{10-\sqrt{10}}$$

$$\begin{aligned}
\xi^2(a + b\sqrt{10} + c\sqrt{10+\sqrt{10}} + d\sqrt{10-\sqrt{10}}) &= a + b\sqrt{10} - c\sqrt{10+\sqrt{10}} - d\sqrt{10-\sqrt{10}} \\
\xi(a + b\sqrt{10} + c\sqrt{10+\sqrt{10}} + d\sqrt{10-\sqrt{10}}) &= a - b\sqrt{10} - d\sqrt{10+\sqrt{10}} + c\sqrt{10-\sqrt{10}} \\
\xi^3(a + b\sqrt{10} + c\sqrt{10+\sqrt{10}} + d\sqrt{10-\sqrt{10}}) &= a - b\sqrt{10} + d\sqrt{10+\sqrt{10}} - c\sqrt{10-\sqrt{10}}
\end{aligned}$$

The norm of an element in E is the product of all its conjugates:

$$\begin{aligned}
N_{E|Q}(a + b\sqrt{10} + c\sqrt{10+\sqrt{10}} + d\sqrt{10-\sqrt{10}}) \\
&= \left[(a + b\sqrt{10})^2 - (c\sqrt{10+\sqrt{10}} + d\sqrt{10-\sqrt{10}})^2 \right] \\
&\quad \cdot \left[(a - b\sqrt{10})^2 - (d\sqrt{10+\sqrt{10}} - c\sqrt{10-\sqrt{10}})^2 \right] \\
&= \left[a^2 + 10b^2 + 2ab\sqrt{10} - c^2(10 + \sqrt{10}) - d^2(10 - \sqrt{10}) - 2cd3\sqrt{10} \right] \\
&\quad \cdot \left[a^2 + 10b^2 - 2ab\sqrt{10} - d^2(10 + \sqrt{10}) - c^2(10 - \sqrt{10}) + 2cd3\sqrt{10} \right] \\
&= \left[a^2 + 10b^2 - 10(c^2 + d^2) + 2ab\sqrt{10} + (d^2 - c^2)\sqrt{10} - 2cd3\sqrt{10} \right] \\
&\quad \cdot \left[a^2 + 10b^2 - 10(c^2 + d^2) - 2ab\sqrt{10} - (d^2 - c^2)\sqrt{10} + 2cd3\sqrt{10} \right] \\
&= \left[a^2 + 10b^2 - 10(c^2 + d^2) \right]^2 - 10 \left[2ab + d^2 - c^2 - 6cd \right]^2
\end{aligned}$$

So we have shown:

(4.6) Proposition: Let $x = a + b\sqrt{10} + c\sqrt{10+\sqrt{10}} + d\sqrt{10-\sqrt{10}}$ with $a, b, c, d \in \mathbb{Q}$ be an arbitrary element of $E = \mathbb{Q}(\sqrt{10+\sqrt{10}})$, then

$$N_{E|Q}(x) = \left[a^2 + 10(b^2 - c^2 - d^2) \right]^2 - 10 \left[2ab + d^2 - c^2 - 6cd \right]^2$$

Now let $a + b\sqrt{10} + c\sqrt{10+\sqrt{10}} + d\sqrt{10-\sqrt{10}}$ be an integer in E , which by (4.3) is equivalent to assuming that $a, b, c, d \in \mathbb{Z}$. For an integer the above formula for the norm simplifies to:

$$(4.7) \quad N_{E|Q}(a + b\sqrt{10} + c\sqrt{10+\sqrt{10}} + d\sqrt{10-\sqrt{10}}) \equiv a^4 \pmod{5}$$

(4.8) Proposition: Let $E = \mathbb{Q}(\sqrt{10+\sqrt{10}})$ and let O_E denote the ring of integers of E . There is no element in O_E whose norm over \mathbb{Q} is -1 or ± 2 or 4 .

Proof: By (4.7) the norm over \mathbb{Q} of any integer in O_E is a 4-th power modulo 5. Hence the norm of an element is 0 or 1 modulo 5, depending on whether the first coefficient is divisible by 5 or not. It is therefore never $-1, \pm 2$ or 4. \square

This has the following consequences:

(4.8a) Corollary: E does not contain units with independent signs.

Proof: All units of E have norm $+1$. Hence every unit has an even number of negative and positive conjugates. From the definition of units with independent signs we see that E does not contain units with independent signs. \square

(4.8b) Corollary: The dyadic prime ideal of E is not principal.

Proof: If it were principal it would be generated by an integer whose norm equals the norm of the ideal (up to the sign). Since the dyadic prime is totally ramified in E , its norm over \mathbb{Q} is 2. There exists no integer of norm ± 2 , hence the dyadic prime can not be principal. \square

(4.9) Theorem: Let $E = \mathbb{Q}(\sqrt{10+\sqrt{10}})$ and let $h(E)$ denote the class number of E , then $h(E)=2$, in particular: it is even.

Proof: Hasse computes the class number in [Ha]. \square

(4.10) Corollary: Let E be as above and let $h^S(E)$ denote the S-class number of E , then $h^S(E) = 1$, in particular: $h^S(E)$ is odd.

Proof: By (4.9) we know that the ideal class group of E is isomorphic to $\mathbb{Z}/2$. Therefore it consists of the class of principal ideals and the class of not principal ideals. By (4.8b) the dyadic prime is not principal. To obtain the S-class group we factor the class group by the class of the dyadic prime, so $h^S(E) = 1$ \square

(4.11) Proposition: Let $E = \mathbb{Q}(\sqrt{10+\sqrt{10}})$, then E contains S-units with independent signs.

Proof: We can prove the existence of S-units with independent signs as follows: Take a generator of the square of the dyadic prime of E . It is an S-unit of norm

-4 , since $+4$ is excluded by (4.8). This generator and its conjugates form a set of S-units with independent signs. Practically, the proof ends here, but we will now give a set of S-units with independent signs explicitly:

Consider the integer $x := -2 - \sqrt{10} - \sqrt{10+\sqrt{10}} - \sqrt{10-\sqrt{10}}$

It is an integer of E and its norm is -2^2 , so x is a S-unit.

Computing the embeddings of x we obtain: $id(x) \approx -11.4 < 0$

$$\xi(x) \approx +2.18 > 0$$

$$\xi^2(x) \approx +1.08 > 0$$

$$\xi^3(x) \approx +0.15 > 0$$

The integers $\xi(x), \xi^2(x)$ and $\xi^3(x)$ all have the same norm as x . Therefore they are all S-units. The set $\{x, \xi(x), \xi^2(x), \xi^3(x)\}$ is in fact a set of S-units with independent signs since under $U_E^S \rightarrow \{\mathbb{Z}/2\}^4$ they map as follows:

$$x \mapsto \left(\text{sign } \xi^i(x) \right)_{i=0..3} = (-, +, +, +)$$

$$\xi(x) \mapsto \left(\text{sign } \xi^{i+1}(x) \right)_{i=0..3} = (+, -, +, +)$$

$$\xi^2(x) \mapsto \left(\text{sign } \xi^{i+2}(x) \right)_{i=0..3} = (+, +, -, +)$$

$$\xi^3(x) \mapsto \left(\text{sign } \xi^{i+3}(x) \right)_{i=0..3} = (+, +, +, -)$$

Here we used the fact that $\text{Gal}(E|\mathbb{Q})$ is cyclic, so the embeddings of the conjugates of x are obtained by cyclically permuting the embeddings of x .

Therefore x and its conjugates form a basis of S-units with independent signs.

This concludes the proof that $E = \mathbb{Q}(\sqrt{10+\sqrt{10}})$ has all the required properties. \square

As pointed out before, the infinite set of examples given in section 15 will include this example as special case. This infinite set of examples is obtained by considering $2q$ instead of 10, where q is a prime with $q \equiv 5 \pmod{8}$. Most of the properties claimed in (4.1) could be checked for this generalization by the same methods used in this section. The determination of the parity of the class number or the S-class number,

however, calls for more involved methods. We will therefore now establish general facts about number fields F where 2-prim $K_2(O_F)$ is elementary abelian of rank $r_1(F)$.

CHAPTER 2

Number Fields with property (*)

In chapter 1 we saw examples of number fields F for which 2-prim $K_2(O_F)$ is elementary abelian of smallest rank, namely: $r_1(F)$. These examples were \mathbb{Q} and degree 2 and degree 4 extensions of \mathbb{Q} . This leads to the question: Are there number fields of higher degree that also have this property? The answer is yes. In fact, we will see how to construct examples of such number field as consecutive quadratic extensions of \mathbb{Q} . By (1.6) we know that these number fields have the following properties: they have exactly one dyadic prime, odd S -class number and contain S -units with independent signs. From now on we will restrict our attention to number fields with these properties, with one additional condition: The number field is totally real. This is useful for later, when we will again wish to obtain examples of number fields where 2-prim $K_2(O_F)$ is elementary abelian of smallest rank and that do **not** contain units with independent signs. That the condition of the number field being totally real gives it a better chance of not containing units with independent signs becomes clear from the consideration of the following special case: if a quadratic number field it is not totally real then it has no real embeddings and therefore it contains units with independent signs by default. For higher degree extensions this argument does not hold, but at least one sees that it might be difficult to obtain examples of number fields that do not contain units with independent signs if the number of real embeddings is small.

For convenience of notation we define:

A number field F is said to have property (*) iff it satisfies all of the following:

- F is totally real
- F contains exactly one dyadic prime
- F has odd S -class number
- F contains S -units with independent signs

We will start this chapter by setting up the tools that we will need. In section 6 we introduce the exact hexagon that is given in [C- H_2]. We also collect some facts

that are related to it. Then we are ready to give a characterization of quadratic extensions of number fields with property (*). This will be done in section 7. In section 8 we are then able to prove the existence of infinitely many number fields with property (*) that can all be obtained by successive quadratic extensions of \mathbb{Q} or any other number field with property (*). A closer examination of which other properties these number field have will follow in chapter 3.

5. Setting up the tools

In all of the following we let F be a number field and S denotes the set consisting of the infinite and dyadic primes of F . As before, we will use O_F^* to denote the units of F and U_F^S to denote the S -units of F .

(5.1) Proposition: Let F be a number field. The group of square classes of units of F injects into the group of square classes of S -units of F . We can therefore consider $O_F^*/(O_F^*)^2$ to be contained in $U_F^S/(U_F^S)^2$.

Proof: Let $\alpha : O_F \longrightarrow U_F^S/(U_F^S)^2$ be the map induced by the inclusion of O_F into $U_F^S/(U_F^S)^2$. We have to show that an element of the kernel of α is contained in $(O_F^*)^2$. This can be seen as follows: Let u be a unit of F that is in the kernel of α . Then $u = v^2$ for some S -unit v . Since the square of v is a unit, it follows that v is a unit. Hence, $u \in (O_F^*)^2$. \square

(5.2) Dirichlet S -unit theorem (see for example [La]):

$$U_F^S \cong \mathbb{Z}^{r_1(F)+r_2(F)+d-1} \times (\text{roots of unity})$$

here $r_1(F)$ denotes the number of real embeddings of F , $r_2(F)$ denotes the number of pairs of complex embeddings and d is the number of finite primes in S . \square

What does this tell us about the group $U_F^S/(U_F^S)^2$? The roots of unity form a finite

cyclic group. They contain -1 , an element of even order, so they form a finite cyclic group of even order. Factoring out squares then leaves only a group isomorphic to $\mathbb{Z}/2$. We obtain:

$$U_F^S/(U_F^S)^2 \cong (\mathbb{Z}/2)^{r_1(F)+r_2(F)+d}$$

Applying this to the special type of number fields we are interested in, immediately yields:

(5.3) Corollary: Let F be a totally real number field that contains exactly one dyadic prime. Let $r_1(F)$ denote the number of real embeddings of F , which in this case equals the degree of F . Then:

$$\#U_F^S/(U_F^S)^2 = 2^{r_1(F)+1} \quad \text{and} \quad \#O_F^*/(O_F^*)^2 = 2^{r_1(F)}$$

□

Remark: By (5.1) we can consider $O_F^*/(O_F^*)^2$ as contained in $U_F^S/(U_F^S)^2$. In a number field that satisfies the conditions of (5.3) we can furthermore regard half of the square classes of $U_F^S/(U_F^S)^2$ as coming from square classes of $O_F^*/(O_F^*)^2$.

In particular, (5.3) applies to number fields with property (*). By definition such number fields contain S-units with independent signs. Recall that this means that the map $U_F^S/(U_F^S)^2 \rightarrow (\mathbb{Z}/2)^{r_1(F)}$ is surjective. The map is defined by mapping a class of $U_F^S/(U_F^S)^2$ to the signs of its representatives. For a totally real number field F with exactly one dyadic prime we just saw that $\#U_F^S/(U_F^S)^2 = 2^{r_1(F)+1}$. If furthermore F contains S-units with independent signs, then the kernel of the above map has $\frac{2^{r_1(F)+1}}{2^{r_1(F)}} = 2$ elements. One of them is the class represented by 1. The other we will denote by τ_F .

(5.4) Definition: Let F be a number field that has property (*). Let τ_F denote the nontrivial element in the kernel of $\varphi : U_F^S/(U_F^S)^2 \rightarrow (\mathbb{Z}/2)^{r_1(F)}$, i.e. the nontrivial square class of totally positive S-units of F .

Remarks: 1) For this definition to make sense, we only needed that F is totally real, has exactly one dyadic prime and contains S -units with independent signs. By stating it for number fields that have property $(*)$ we included the condition that F has odd S -class number. This is not necessary, but since we will be interested only in number fields with property $(*)$, it makes our statements easier to read.

2) In the following we will not always distinguish between the class τ_F and one of its representatives. Hence, from now on τ_F will either denote the above defined element of $U_F^S/(U_F^S)^2$ or, by abuse of notation, a totally positive S -unit of F that is not a square from U_F^S . The following is a useful criterion to check whether a number field F with property $(*)$ contains units with independent signs:

(5.5) Proposition: Let F be a number field with property $(*)$, then:

$$F \text{ contains units with independent signs} \iff \tau_F \notin O_F^*/(O_F^*)^2$$

Proof: In (5.1) we saw that $O_F^*/(O_F^*)^2$ can be considered as a subgroup of $U_F^S/(U_F^S)^2$. Let φ denote the surjective map from $U_F^S/(U_F^S)^2$ onto $(\mathbb{Z}/2)^{r_1(F)}$. By definition of τ_F we have: $\ker(\varphi) = \{1, \tau_F\}$. Consider the restriction map $\varphi|_O : O_F^*/(O_F^*)^2 \rightarrow (\mathbb{Z}/2)^{r_1(F)}$. Its kernel is contained in $\{1, \tau_F\}$. By definition we have: $\varphi|_O$ is surjective iff F contains units with independent signs. Since both $O_F^*/(O_F^*)^2$ and $(\mathbb{Z}/2)^{r_1(F)}$ are finite groups of the same order, namely $2^{r_1(F)}$, we have: $\varphi|_O$ is injective iff F contains units with independent signs. Now it is clear that F contains units with independent signs iff $\ker(\varphi|_O) = \{1\}$, which occurs if and only if $\tau_F \notin O_F^*/(O_F^*)^2$. \square

We are still setting up the tools we will need in the following sections. For this we now need to consider real quadratic extensions $E|F$ of a number field F . Here, “real quadratic” means that the square root of a totally positive element of F is adjoined to F , so no infinite prime of F will ramify in E . We will examine the relationship between E containing S -units with independent signs and F containing S -units with independent signs. Here S can stand for any set of primes of F that contains all infinite primes of F . In particular we will apply the result to the case where S consists of the infinite and dyadic primes of F and also to the case where S contains no finite

primes of F . In this second case we will get a relationship between E containing units with independent signs and F containing units with independent signs.

We will see that if E contains S -units with independent signs, then so does F ; but the converse does not hold in general. The relationship between S -units with independent signs of E and F will follow from examining the following diagram:

(5.6) Lemma: Let E be a real quadratic extension of a number field F .

Let $\{\sigma_1, \dots, \sigma_i, \dots, \sigma_{r_1(F)}\}$ denote the real embeddings of F and let

$\{\sigma_{11}, \sigma_{12}, \dots, \sigma_{i1}, \sigma_{i2}, \dots, \sigma_{r_1(F)1}, \sigma_{r_1(F)2}\}$ denote the real embeddings of E , where the notation is chosen such that $\sigma_{i1}|_F = \sigma_{i2}|_F = \sigma_i$ for $i = 1, \dots, r_1(F)$. The following diagram commutes:

$$\begin{array}{ccc} E^* & \xrightarrow{(\dots, \sigma_{i1}, \sigma_{i2}, \dots)} & \mathbf{R}^{2r_1(F)} \\ N_{E|F} \downarrow & & \downarrow m \\ F^* & \xrightarrow{(\dots, \sigma_i, \dots)} & \mathbf{R}^{r_1(F)} \end{array}$$

Here m is the map defined by multiplying two successive entries,

i.e. let $(a_{11}, a_{12}, \dots, a_{r_1(F)1}, a_{r_1(F)2}) \in \mathbf{R}^{2r_1(F)}$ then

$$m(a_{11}, a_{12}, \dots, a_{r_1(F)1}, a_{r_1(F)2}) := (a_{11} \cdot a_{12}, \dots, a_{r_1(F)1} \cdot a_{r_1(F)2})$$

Proof: Let T denote the generator of $Gal(E|F) \cong \mathbb{Z}/2$, then for any $a \in E$ we have: $N_{E|F}(a) = a \cdot T(a)$ and for $i = 1, \dots, r$ we have: $\sigma_{i2} = \sigma_{i1} \circ T$. In order to check the commutativity of the diagram we need to check:

$$m \circ (\sigma_{11} \cdot \sigma_{12}, \dots, \sigma_{r_1(F)1} \cdot \sigma_{r_1(F)2}) = (\sigma_1, \dots, \sigma_{r_1(F)}) \circ N_{E|F}$$

This is done as follows. Let $a \in E$, then:

$$\begin{aligned} [m \circ (\dots, \sigma_{i1}, \sigma_{i2}, \dots)](a) &= m(\dots, \sigma_{i1}(a), \sigma_{i2}(a), \dots) \\ &= (\dots, \sigma_{i1}(a) \cdot \sigma_{i2}(a), \dots) \\ &= (\dots, \sigma_{i1}(a) \cdot \sigma_{i1}(Ta), \dots) \\ &= (\dots, \sigma_{i1}(a \cdot Ta), \dots) \\ &= (\dots, \sigma_{i1}(N_{E|F}(a)), \dots) \\ &= (\dots, \sigma_i(N_{E|F}(a)), \dots) \end{aligned}$$

$$[(..., \sigma_i, ...) \circ N_{E|F}](a) = (..., \sigma_i, ...)(N_{E|F}(a))$$

In the second to last line we used the fact that $N_{E|F}(a) \in F$ and $\sigma_{i1}|_F = \sigma_i$. \square

Since we are interested in properties of E and F concerning units with independent signs and S -units with independent signs, we will now give a weaker version of (5.6). Instead of mapping an element of F^* or E^* into \mathbb{R} we only need the sign of its image in \mathbb{R} , so we will map an element to the signs of its embeddings. We also do not need all of E^* and F^* , but only the subgroups of S -units: U_E^S and U_F^S . Here, one set S is a collection of primes of F , the other S is the set of primes in E that lie over those from F . Which set S is meant, is clear from the context, we will not distinguish them in our notation.

Hence, (5.6) restricts to the following commutative diagram of groups:

$$\begin{array}{ccc} U_E^S & \xrightarrow{\pi} & (\mathbb{Z}/2)^{2r_1(F)} \\ n \downarrow & & \downarrow m \\ U_F^S & \xrightarrow{\varphi} & (\mathbb{Z}/2)^{r_1(F)} \end{array}$$

The maps m, φ, π and n are defined as follows:

The map m again denotes the map that multiplies two successive entries.

We let φ and π denote the maps that take an element to the signs of its embeddings:

$$\pi := (... , \text{sign} \sigma_{i1}, \text{sign} \sigma_{i2}, ...) : U_E^S \longrightarrow (\mathbb{Z}/2)^{2r_1(F)}$$

$$\varphi := (... , \text{sign} \sigma_i, ...) : U_F^S \longrightarrow (\mathbb{Z}/2)^{r_1(F)}$$

By n we denote the restriction of the norm map $N_{E|F}$ to U_E^S . Note that n in fact maps U_E^S into U_F^S . The image of n is $N_{E|F}(U_E^S)$. We can also consider this restricted norm map n as mapping $U_E^S/(U_E^S)^2$ into $U_F^S/(U_F^S)^2$. The image is $N_{E|F}(U_E^S)/(U_F^S)^2$ and the cokernel is isomorphic to $U_F^S/N_{E|F}(U_E^S)$.

Note that $(U_E^S)^2$ is contained in the kernel of π and $(U_F^S)^2$ is contained in the kernel of φ . We can therefore consider π and φ as mappings on square classes. This justifies the following:

(5.7) Corollary: With the notation as above, the following diagram of finite abelian groups commutes:

$$\begin{array}{ccc}
U_E^S / (U_E^S)^2 & \xrightarrow{\pi} & (\mathbb{Z}/2)^{2r_1(F)} \\
n \downarrow & & \downarrow m \\
U_F^S / (U_F^S)^2 & \xrightarrow{\varphi} & (\mathbb{Z}/2)^{r_1(F)}
\end{array}$$

The cokernel of n is isomorphic to $U_F^S / N_{E|F}(U_E^S)$. □

Remarks: If F has property (*), then the kernel of φ is $\{1, \tau_F\}$, where τ_F is as in (5.4).

Recall that, by definition, F contains S -units with independent signs iff φ is surjective. E contains S -units with independent signs iff π is surjective.

As explained above, the set S corresponding to E consists of all primes lying over those primes that are in the set S corresponding to F . The set S of primes of F can stand for any set of primes that contains all infinite primes of F . In particular, it applies to the case where S contains no finite primes. In this case we replace “ S -units with independent signs” by “units with independent signs” and U_F^S, U_E^S by O_F^*, O_E^* .

(5.8) Proposition: Let E be a real quadratic extension of a number field F . If E contains S -units with independent signs, then $\varphi \circ n : U_E^S / (U_E^S)^2 \longrightarrow (\mathbb{Z}/2)^{r_1(F)}$ is surjective; in particular: F contains S -units with independent signs.

Proof: The idea of the proof is that the norms of a set of S -units with independent signs of E form a set of S -units with independent signs in F . We are assuming that E contains S -units with independent signs, so π is surjective. Clearly the map m that multiplies two successive entries is also surjective. Hence, the composition $m \circ \pi : U_E^S / (U_E^S)^2 \longrightarrow (\mathbb{Z}/2)^{r_1(F)}$ is surjective. From the commutativity of the diagram in (5.7) we conclude that $\varphi \circ n$ is surjective. Therefore the restriction of φ to the image of n is surjective. In particular, this tells us that φ is surjective, so F contains units with independent signs. □

The converse of (5.8) holds, too. Note that to conclude that E contains S -units with independent signs it does not suffice that F contains S -units with independent signs. We need to assume the stronger condition that $\varphi \circ n$ is surjective.

(5.9) Proposition: Let E be a real quadratic extension of a number field F . If $\varphi \circ n : U_F^S / (U_F^S)^2 \longrightarrow (\mathbb{Z}/2)^{r_1(F)}$ is surjective [notation as in (5.7)], then E contains S -units with independent signs.

Proof: The idea of the proof is that S -units with independent signs of F can be “pulled up” to S -units with independent signs of E by the norm. We will use the same notation for the embeddings of E and F into \mathbb{R} as in (5.6), T will stand for the generator of $\text{Gal}(E|F)$. Let $\{a_1, \dots, a_{r_1(F)}\}$ be a set of representatives of square classes of S -units of E such that $\sigma_i(N_{E|F}a_i)$ is negative and $\sigma_j(N_{E|F}a_i)$ is positive for all $j \neq i$. It is possible to choose such a set since we are assuming that the restriction of φ to the image of the norm map n is surjective onto $(\mathbb{Z}/2)^{r_1(F)}$. To show that E contains S -units with independent signs, we need to show that π is surjective. For this it suffices to find a set $\{A_1, \dots, A_{r_1(F)}\}$ of S -units of E such that for every $i \in \{1, \dots, r_1(F)\}$ we have: $\sigma_{i1}(A_i)$ is negative and $\sigma_{j1}(A_i)$ is positive for all $j \neq i$ and $\sigma_{j2}(A_i)$ is positive for all $j \in \{1, \dots, r_1(F)\}$.

The existence of these elements suffices to conclude that π is surjective, because these A_i together with their conjugates $T(A_i)$ form a set of S -units of E that are negative in exactly one embedding of E into \mathbb{R} and positive in all the others. Under the map π products of these S -units will then map to any given element of $(\mathbb{Z}/2)^{2r_1(F)}$.

We now fix any $i \in \{1, \dots, r_1(F)\}$ and construct an element A_i with the desired properties. We start by considering the element a_i . We have $\sigma_i(N_{E|F}a_i) = \sigma_{i1}(a_i) \cdot \sigma_{i2}(a_i)$. Since $\sigma_i(N_{E|F}a_i)$ is negative we can conclude that exactly one of $\sigma_{i1}(a_i)$ or $\sigma_{i2}(a_i)$ is negative. By replacing a_i by its conjugate $T(a_i)$, if necessary, we can assume that $\sigma_{i1}(a_i)$ is negative. Unfortunately, when considering $\sigma_{j1}(a_i)$ and $\sigma_{j2}(a_i)$ for $j \neq i$ we can only conclude that they both have the same sign. This follows from the fact that their product is $\sigma_j(N_{E|F}a_i)$, which is positive. To obtain an element A_i as required, we need to alter a_i such that the signs under the embeddings σ_{i1} and σ_{i2} stay the same, i.e. negative and positive, respectively; but the signs of the element under all other embeddings are positive. Let I denote the set of indices where the embedding of a_i has negative signs: $I := \{k \mid \text{sign}[\sigma_{k1}a_i] < 0 \text{ and } \text{sign}[\sigma_{k2}a_i] < 0\}$. Since we already know that $\sigma_{j1}(a_k)$ and $\sigma_{j2}(a_k) = \sigma_{j1}(Ta_k)$ have the same sign for

all $j \neq i, k \in \{1, \dots, r_1(F)\}$, we can take:

$$A_i := a_i \cdot \prod_{k \neq i} a_k T(a_k)$$

This element will have the same signs as a_i at the embeddings σ_{i1} and σ_{i2} . Like a_i it will be positive under σ_{k1} and σ_{k2} for $k \notin I$, but whereas a_i was negative under σ_{k1} and σ_{k2} for $k \in I$, this element is positive. \square

In propositions (5.8) and (5.9) we have shown that E contains S -units with independent signs iff $\varphi \circ n$ is surjective. For the special case where S does not contain any finite primes this yields:

(5.10) Corollary: Let E be a real quadratic extension of F . Then E contains units with independent signs if and only if F contains units with independent signs and all units of F are norms of units of E .

Proof: If E contains units with independent signs then $\varphi \circ n : O_E^*/(O_E^*)^2 \rightarrow (\mathbb{Z}/2)^{r_1(F)}$ is surjective by (5.8). Hence φ is surjective, so F contains units with independent signs. Since φ maps $O_F^*/(O_F^*)^2$, which by (5.3) has order $2^{r_1(F)}$, into $(\mathbb{Z}/2)^{r_1(F)}$, we see that φ is an isomorphism. We conclude that $n : O_E^*/(O_E^*)^2 \rightarrow O_F^*/(O_F^*)^2$ is surjective, so every unit of F is the norm of a unit of E .

Conversely, assume that F contains units with independent signs, so φ is surjective, and that every unit of F is the norm of a unit from E , so n is surjective. It follows that $\varphi \circ n$ is surjective, so by (5.9) E contains units with independent signs. \square

6. The exact hexagon

We now need to introduce the exact hexagon that is defined in [C- H_2], applied to the case where $E|F$ is an extension of degree 2. S could be any finite set of primes of F containing all infinite primes of F . We will later apply this to two cases: the case where S is the set of all dyadic primes and all infinite primes of F and the case where S contains no finite primes of F .

Let T denote a generator of the galois group $\text{Gal}(E|F) = \mathbb{Z}/2 = C_2 = \langle T \rangle$. The set of S -integers of F and the set of S -units of F will be denoted by O_F^S and U_F^S , respectively. We will let O_E^S denote the integral closure of O_F^S in E , U_E^S the set of S -units of E and $C^S(E)$ the S -class group of E .

Note: In the case where S contains no finite primes of F we will just omit ' S ' in the notation. In accordance with this the set of integers of F will be denoted by O_F , but for the set of units of F we will use O_F^* .

We have the following cohomology groups:

$$H^1(C_2; C^S(E)) = \{cl(A) \in C^S(E) \mid \exists x \in E^* : A \cdot TA = xO_E^S\} / \{\frac{A}{TA}\}$$

here A is an ideal of E and $cl(A)$ its class in the S -ideal class group of E .

$$H^1(C_2; U_E^S) = \{v \in U_E^S \mid Nv = 1\} / \{\frac{v}{Tv}\}$$

$$H^0(C_2; U_E^S) = U_F^S / N_{E|F}(U_E^S)$$

$$H^0(C_2; C^S(E)) = \{cl(A) \in C^S(E) \mid \exists x \in E^* : TA = xA\} / N(C^S(E))$$

We will now give a collection of results from [C- H_2]:

(6.1) There exists an exact hexagon:

$$\begin{array}{ccccc}
 & & H^1(C_2; C^S(E)) & \xrightarrow{d_1^S} & H^1(C_2; U_E^S) & & \\
 & \nearrow j_1^S & & & & \searrow i_1^S & \\
 R_S^0(E|F) & & & & & & R_S^1(E|F) \\
 & \nwarrow i_0^S & & & & \swarrow j_0^S & \\
 & & H^0(C_2; U_E^S) & \xleftarrow{d_0^S} & H^0(C_2; C^S(E)) & &
 \end{array}$$

For the definitions of the six maps and the groups $R_S^0(E|F)$ and $R_S^1(E|F)$ we refer to [C- H_2]. It is known that all six groups in the above exact hexagon are **finite elementary abelian 2-groups**. Recall that this means that they are all of the form $(\mathbb{Z}/2)^k$ for some nonzero integer k . This k is called the 2-rank or just the rank of the group. In the next sections we will need the following facts:

(6.2) $H^0(C_2, C^S(E))$ and $H^1(C_2, C^S(E))$ have the same rank; they are noncanonically isomorphic.

(6.3) If E is a quadratic extension of F that is either ramified or in which at least one dyadic prime of F is inert, then

$$R_S^0(E|F) \cong (\mathbb{Z}/2)^{\text{number of ramified primes} + \text{number of inert primes in } S - 1},$$

$$R_S^1(E|F) \cong (\mathbb{Z}/2)^{\text{number of finite ramified primes outside of } S}$$

Note that in the case where S contains no finite primes of F we have:

$$R_S^0(E|F) \cong (\mathbb{Z}/2)^{\text{number of ramified primes} - 1},$$

$$R_S^1(E|F) \cong (\mathbb{Z}/2)^{\text{number of finite ramified primes}}$$

(6.4) There is an injection from $R_S^0(E|F)$ into the cohomology group $H^0(C_2, E^*) = F^*/N_{E|F}(E^*)$. We also have the canonical injection from $H^0(C_2, U_E^S)$ into $H^0(C_2, E^*)$. This canonical injection commutes with the composition of i_0^S and the inclusion of $R_S^0(E|F)$ into $H^0(C_2, E^*)$.

(6.5) If $h^S(F)$ is odd, then:

- a) $R_S^0(E|F) \xrightarrow{j_0^S} H^1(C_2, C^S(E))$ is surjective.
- b) $2\text{-rk} C^S(E) = 2\text{-rk} H^1(C_2, C^S(E))$
- c) $R_S^0(E|F) \cong (\mathbb{Z}/2)^{\text{number of ramified primes} + \text{number of inert primes in } S - 1},$

Remark: This can be found as 2.2 in [C- H_1].

(6.6) Let $E|F$ be a ramified quadratic extension. The following are equivalent:

- a) the relative class number $h(E|F)$ is odd
- b) $i_0 : H^0(C_2, O_E^*) \rightarrow R^0(E|F)$ is surjective and C_2 acts trivially on the 2-primary subgroup of $C(E)$.

Remark: This is a special case of 5.8 in [C- H_2].

For ramified extensions the relative class number $h(E|F)$ is defined as the quotient of the class numbers of E and F . This quotient is an integer.

(6.7) Let F be a number field and let S denote the set of infinite and dyadic primes of F . If $h^S(F)$, the S -class number of F , is odd then any quadratic extension of F in which no dyadic prime is inert must be a ramified extension.

Proof: Assume that F has an **unramified** quadratic extension E in which no dyadic prime of F is inert. It follows that E is a quadratic extension of F in which all dyadic primes split. E is therefore contained in the Hilbert S -Class Field of F .

The Galois group of the Hilbert S-Class Field of F over F therefore has a factor 2, i.e. it is even. By class field theory this Galois group is isomorphic to the S-ideal class group of F . Hence the order of the S-ideal class group, namely the S-class number $h^S(F)$, is even. This contradicts the assumption. \square

7. Characterizing quadratic extensions with property (*)

Before we can prove the existence of number fields with property (*) in the next section, we now give a very useful characterization of quadratic extensions with property (*).

(7.1) Theorem: Let F be a number field with property (*) and E a real quadratic extension of F . Let τ be any totally positive S-unit of F that is not a square. E has property (*) if and only if either

- 1) no odd prime of F ramifies in $E|F$ or
- 2) exactly one odd prime of F ramifies in $E|F$ and $\tau \notin N_{E|F}(E^*)$.

Proof: We will prove the claimed equivalence by proceeding in the following way: Let F have property (*) and let E be a real quadratic extension of F . We will check that:

- a) If no odd prime of F ramifies in $E|F$ then E has property (*).
- b) If more than one odd prime of F ramifies in $E|F$ then E does not have prop. (*).
- c) If exactly one odd prime of F ramifies in $E|F$ and if $\tau \in N_{E|F}(E^*)$ then E does not have property (*).
- d) If exactly one odd prime of F ramifies in $E|F$ and if $\tau \notin N_{E|F}(E^*)$ then E has property (*).

Before we start with the proof let us review what it means for F to have prop. (*): F is totally real, F contains exactly one dyadic prime, the S-class number of F , $h^S(F)$, is odd and F contains S-units with independent signs. Note that E is always

totally real, so to check whether E has property (*), we need to examine the number of dyadic primes of E , the S -class number, $h^S(E)$, and whether E contains S -units with independent signs.

This is done by computing some of the elementary abelian 2-groups in the exact hexagon (6.1). We then use the facts listed in section 6 to draw conclusions about other groups of the hexagon. In particular, we will determine the order of $H^0(C_2, U_E^S) = U_F^S / N_{E|F}(U_E^S)$ which is the cokernel of n in (5.7). This will allow us to determine whether $\varphi \circ n$ is surjective. By (5.8) and (5.9) we can then tell whether E contains S -units with independent signs. Note that by (5.4) we have $\ker \varphi = \{1, \tau\}$.

Case a): No odd prime of F ramifies in $E|F$

Since we are assuming that $h^S(F)$ is odd we can apply (6.5.c) to obtain:

$$2\text{-rk} R_S^0(E|F) = (\#\text{primes of } F \text{ that ramify in } E) + (\#\text{dyadic primes of } F \text{ that are inert in } E) - 1.$$

This number is not negative, hence F must either contain a prime that ramifies in $E|F$ or a dyadic prime (there is only one!) that is inert in $E|F$. Since no odd prime of F ramifies in $E|F$ we conclude that the dyadic prime of F is either ramified or inert in $E|F$. This shows that E contains exactly one dyadic prime.

We have $2\text{-rk} R_S^0(E|F) = 0$, so the elementary abelian 2-group $R_S^0(E|F)$ is trivial. Applying (6.5.a) yields that $H^1(C_2, C^S(E))$ is also trivial, since it is the image under a surjective map from a trivial set. By (6.5.b) we obtain that the 2-rank of $C^S(E)$ is the same as the 2-rank of $H^1(C_2, C^S(E))$, which by (6.2) is the same as the 2-rank of $H^0(C_2, C^S(E))$. This shows that $2\text{-rk} C^S(E)$ is trivial, i.e. $h^S(E)$ is odd. Plugging the information obtained so far into the exact hexagon from (6.1) gives an isomorphism:

$$H^0(C_2, U_E^S) \xrightarrow{i_0^S} R_S^0(E|F) = 1$$

Hence $H^0(C_2, U_E^S) = U_F^S / N_{E|F}(U_E^S)$ is trivial. The map $n : U_E^S / (U_E^S)^2 \rightarrow U_F^S / (U_F^S)^2$ in (5.7) therefore has a trivial cokernel, i.e., it is surjective. By assumption F contains S -units with independent signs, so φ of (5.7) is surjective. We conclude that the composition $\varphi \circ n$ is surjective. Applying (5.9) yields that E contains S -units with independent signs. This shows that E has property (*) in the case under consideration.

Case b): More than one odd prime of F ramifies in $E|F$.

We assume that at least two odd primes of F ramify in $E|F$ and that E has property (*). This will lead to a contradiction. We are assuming that F has property (*), so in particular $h^S(F)$ is odd. Under this condition we can apply (6.5.b): $2\text{-rk}C^S(E)=2\text{-rk}H^1(C_2, C^S(E))$. We are assuming that E has property (*), so $h^S(E)$ is odd. This means that $2\text{-rk}C^S(E)$ is trivial, hence $H^1(C_2, C^S(E))$ is trivial as well. The above equality then yields that also the elementary abelian 2-group $H^1(C_2, C^S(E))$ is trivial. By (6.2) we then also have $H^0(C_2, C^S(E))$ trivial. Plugging this into the exact hexagon results in an isomorphism:

$$H^0(C_2, U_E^S) \xrightarrow{i_0^S} R_S^0(E|F)$$

By (6.3) we have $2\text{-rk}R_S^0(E|F) \geq 2 + 1 - 1$, where 2 stands for the minimal number of odd primes of F that ramify in E and 1 stands for the dyadic prime of F which is either ramified or inert in E , since we are assuming E to have only one dyadic prime. Combining this with the above isomorphism yields: $H^0(C_2, U_E^S) = (\mathbb{Z}/2)^m$, with $m \geq 2$. Expressing $H^0(C_2, U_E^S)$ in a different way we have:

$$U_F^S / N_{E|F}(U_E^S) = (\mathbb{Z}/2)^m \text{ with } m \geq 2$$

For the map $n : U_E^S / (U_E^S)^2 \longrightarrow U_F^S / (U_F^S)^2$ in the diagram (5.7) this means that the cokernel of n has $(\mathbb{Z}/2)^m$ elements. From (5.3) we have $\#U_F^S / (U_F^S)^2 = 2^{r_1(F)+1}$. Hence, the image of n has $\frac{2^{r_1(F)+1}}{2^m} = 2^{r_1(F)+1-m} \leq 2^{r_1(F)-1}$ elements. The map $\varphi \circ n : U_F^S / (U_F^S)^2 \longrightarrow (\mathbb{Z}/2)^{r_1(F)}$ can therefore not be surjective. From (5.8) we conclude that E does not contain S -units with independent signs. This shows that in this case E does not have property (*).

Case c): Exactly one odd prime of F ramifies in $E|F$ and $\tau \in N_{E|F}(E^*)$

We want to show that E can not have property (*), but suppose E does have property (*):

Since $h^S(E)$ is odd by assumption, we have $2\text{-rk}C^S(E) = 0$. By (6.5.b) this equals the 2-rank of the elementary abelian 2-group $H^1(C_2, C^S(E))$, which in turn also equals the 2-rank of the elementary abelian 2-group $H^0(C_2, C^S(E))$. Hence both $H^0(C_2, C^S(E))$ and $H^1(C_2, C^S(E))$ are trivial. Plugging this into the exact hexagon yields an isomorphism:

$$H^0(C_2, U_E^S) \xrightarrow{i_0^S} R_S^0(E|F)$$

We now need to consider two possibilities: $\tau \notin N_{E|F}(U_E^S)$, but still in $N_{E|F}(E^*)$; or $\tau \in N_{E|F}(U_E^S)$:

If $\tau \notin N_{E|F}(U_E^S)$ then the classes of 1 and τ in $U_F^S/N_{E|F}(U_E^S)$ are distinct. By the above isomorphism the classes of 1 and τ are then also distinct in $R_S^0(E|F)$. By (6.4) $R_S^0(E|F)$ is a subset of $H^0(C_2, E^*) = F^*/N_{E|F}(E^*)$. But here the classes of τ and 1 are the same, since we are discussing a case where $\tau \in N_{E|F}(E^*)$. This is a contradiction, hence we must now assume that $\tau \in N_{E|F}(U_E^S)$.

By (6.3) the rank of the elementary abelian group $R_S^0(E|F)$ is $1 + 1 - 1 = 1$. Here, the first one is the number of odd ramified primes of F and the next one counts the dyadic prime of F which is either ramified or inert in E . Hence $R_S^0(E|F) \cong \mathbb{Z}/2$. From the isomorphism i_0^S we obtain: $U_F^S/N_{E|F}(U_E^S) = \mathbb{Z}/2$. In the commutative diagram (5.7) we now have that the cokernel of n has order 2. Since n maps into $U_F^S/(U_F^S)^2$, which by (5.3) has $2^{r_1(F)+1}$ elements, we see that the image of n has $2^{r_1(F)}$ elements. The restriction of φ to the image of n is therefore a map from a group of order $2^{r_1(F)}$ to $(\mathbb{Z}/2)^{r_1(F)}$, which has the same order. Hence $\varphi|_{\text{im } n}$ is surjective iff it is injective. In the present case it is not injective since we are assuming $\tau \in N_{E|F}(U_E^S)$, so $\ker \varphi|_{\text{im } n} = \{1, \tau\} \cap N_{E|F}(U_E^S) = \{1, \tau\}$. We conclude that $\varphi \circ n$ is not surjective, so by (5.8) E can not contain S -units with independent signs. In this case E does not have property (*).

Case d): Exactly one odd prime of F ramifies in $E|F$ and $\tau \notin N_{E|F}(E^*)$

We want to check that E has property (*). Since τ is not a norm from (E^*) it is certainly not the norm of an S -unit of E . Therefore the classes of 1 and τ in $H^0(C_2, U_E^S) = U_F^S/N_{E|F}(U_E^S)$ are distinct. In the exact hexagon (6.1) $H^0(C_2, U_E^S)$ maps into $R_S^0(E|F)$ by i_0^S . What can be said about the images of the classes of 1 and τ under i_0^S ? By (6.4) we can consider $R_S^0(E|F)$ to be contained in $H^0(E^*) = F^*/N_{E|F}(E^*)$. Here the images of the classes of 1 and τ are distinct, since $\tau \notin N_{E|F}(E^*)$. Hence the images of 1 and τ under i_0^S are distinct in $R_S^0(E|F)$, so $R_S^0(E|F)$ contains at least two elements. By (6.3) we know that the 2-rank of the elementary abelian 2-group $R_S^0(E|F)$ is:

$$1 + (\#\text{ramified dyadic primes of } F) + (\#\text{inert dyadic primes}) - 1.$$

Here, the first one is the one ramified odd prime of F . By our previous observations this number is to be at least 2. Since F contains exactly one dyadic prime we can

deduce that $R_S^0(E|F)$ has rank 1 and that the dyadic prime of F is either ramified or inert in E . This shows that E contains exactly one dyadic prime, the first step towards property (*). Another conclusion we can draw from the above is that i_0^S is surjective. This follows from the fact that $R_S^0(E|F)$ has only two elements and $i_0^S(1)$ is distinct from $i_0^S(\tau)$. Since $h^S(F)$ is odd we can apply (6.5.a) to obtain another surjective map: $R_S^0(E|F) \xrightarrow{j_1^S} H^1(C_2, C^S(E))$. From the exactness of the hexagon (6.1) we obtain that the kernel of j_1^S equals the image of i_0^S . This image is isomorphic to $R_S^0(E|F)$ since i_0^S is surjective. Hence j_1^S is the trivial map and since it is surjective we conclude that $H^1(C_2, C^S(E))$ is trivial. By (6.5b) this shows that $h^S(E)$ is odd. To complete the proof that E has property (*) we now need to show that E contains S -units with independent signs. We just saw that $H^1(C_2, C^S(E))$, and by (6.2) then also $H^0(C_2, C^S(E))$, is trivial. The exact hexagon therefore yields an isomorphism:

$$\mathbb{Z}/2 = R_S^0(E|F) \cong H^0(C_2, U_E^S) = U_F^S / N_{E|F}(U_E^S)$$

We now proceed as in case c). The map n in the diagram (5.7) has a cokernel of order $2^{r_1(F)}$. The kernel of $\varphi|_{im\ n}$ is $\{1, \tau\} \cap N_{E|F}(U_E^S)$ but this time we have $\tau \notin N_{E|F}(U_E^S)$. Hence, $\varphi|_{im\ n}$ is injective and then for reasons of order also surjective. This shows that $\varphi \circ n$ is surjective. By (5.9) we have that E contains S -units with independent signs. This concludes the proof that in this case E has property (*). \square

(7.2) Corollary: Let F be a number field with property (*) and let E be a quadratic extension of F that also has property (*).

- 1) If no odd prime of F ramifies in $E|F$ then all S -units of F are norms of S -units of E .
- 2) If exactly one odd prime of F ramifies in $E|F$ then $U_F^S / N_{E|F}(U_E^S) \cong \mathbb{Z}/2$. Hence, exactly half of all square classes of S -units of F are square classes of S -units of E . Furthermore, $N_{E|F}(U_E^S) / (U_F^S)^2$ is a subgroup of index 2 of $U_F^S / (U_F^S)^2$ that does not contain τ .

Proof: In part a) of the proof of (7.1) we showed that $U_F^S / N_{E|F}(U_E^S)$ is trivial. this proves claim 1). Claim 2) was shown in d) of the proof of (7.1). \square

(7.3) Remark: Let F be a number field and let E be a quadratic extension of F . Let S be a set of primes of F such that no finite prime of S splits in $E|F$. If a unit of F is the norm of an S -unit of E then it is the norm of a unit of E . \square

(7.4) Proposition: Let F be a number field with property (*). Let E be a quadratic extension of F with property (*) in which exactly one odd prime of F ramifies. Let u be a unit of F . If $u \in N_{E|F}(E^*)$ then $u \in N_{E|F}(O_E^*)$. Hence,

$$N_{E|F}(E^*) \cap O_F^* = N_{E|F}(O_E^*)$$

Proof: E is assumed to contain S -units with independent signs. By (5.8) we have that $\varphi \circ n : U_E^S / (U_E^S)^2 \rightarrow (\mathbb{Z}/2)^{r_1(F)}$ is surjective. Since the kernel of $\varphi : U_F^S / (U_F^S)^2 \rightarrow (\mathbb{Z}/2)^{r_1(F)}$ is $\{1, \tau\}$, we have that either u or τu is in the image of n . So either u or τu is a norm from an S -unit of E . By (7.2) we have $U_F^S / N_{E|F}(U_E^*) = \mathbb{Z}/2$. By (7.1) we know that the S -unit τ is not the norm of any element of E . Let $u \in N_{E|F}(E^*)$. Since $\tau \notin N_{E|F}(E^*)$ we must have $\tau u \notin N_{E|F}(E^*)$. In particular, $\tau u \notin N_{E|F}(U_E^S)$. We conclude that $u \in N_{E|F}(U_E^S)$. From (7.3) it follows that $u \in N_{E|F}(O_E^*)$. \square

8. The existence of number fields with property (*)

We start with a question: For any given number field F , do there exist extensions with property (*)? One part of the answer is clear from the hereditary nature of property (*), see (1.8):

(8.1) Proposition: If a number field F does not have property (*), then neither does any extension of F .

(8.2) Theorem: Let F be a number field with property (*).

There exists exactly one quadratic extension of F with property (*) in which no odd prime of F ramifies. It is given by $F(\sqrt{\tau})$, where τ denotes any totally positive S -unit of F that is not a square.

There exist infinitely many other quadratic extensions of F with property (*). In all of these exactly one odd prime of F ramifies.

When proving this we will actually show more than is claimed. This stronger version of (8.2) is given in (8.7). The proof will be given below, but first note that from (8.2) it follows immediately:

(8.3) Corollary: If a number field F has property (*), then there exist infinitely many extensions of F with property (*). There are number fields with property (*) of arbitrarily high degree; examples can be obtained by successive quadratic extensions of \mathbb{Q} . \square

Before we can give the proof of (8.2), here are two observations that we will need:

(8.4) Fact: Let F be a number field and P an odd prime of F , $\sigma \in F$.

$$P \text{ ramifies in } F(\sqrt{\sigma})|F \iff \text{ord}_P(\sigma) \equiv 1 \pmod{2}$$

This fact can be found, for example, in [Cohn] on page 215. He also gives a criterion for the ramification of dyadic primes of F , which is more involved.

(8.5) Proposition: Let F be a number field with odd S -class number $h^S(F)$. Let σ be an element of F and let the principal ideal generated by σ be denoted by $\sigma \cdot O_F$. Let P denote an odd prime of F . There exists an element $y \in F$ with the following properties:

- a) $F(\sqrt{y}) = F(\sqrt{\sigma})$.
- b) If the exact power of P dividing $\sigma \cdot O_F$ is odd then P divides $y \cdot O_F$ exactly to the odd power $h^S(F)$.
- c) If the exact power of P dividing $\sigma \cdot O_F$ is even then P does not divide $y \cdot O_F$.

Proof: Let P be an odd prime ideal of F and let P^k be the exact power of P dividing $\sigma \cdot O_F$. We will show that there exists an element $y \in F$ in whose prime ideal decomposition the prime P will appear iff k is odd. The odd prime factors of y different from P are the same as those of σ . The power with which they appear in y will be the power with which they appear in σ multiplied by an odd number, so the parity will be the same. Also, we will have $F(\sqrt{y}) = F(\sqrt{\sigma})$. The proposition follows from successive application of this.

Let n be such that $k = 2n$ or $k = 2n + 1$. We have $\sigma \cdot O_F = AP^{2n}$ for some ideal A . Consider $\sigma^{h^S(F)}$. Since $h^S(F)$ is odd we have $F(\sqrt{\sigma^{h^S(F)}}) = F(\sqrt{\sigma})$. Furthermore, we have $\sigma^{h^S(F)} \cdot O_F = A^{h^S(F)}(P^{h^S(F)})^{2n}$. The ideal $P^{h^S(F)}$ is principal up to dyadic factors. We obtain $\sigma^{h^S(F)} \cdot O_F = A^{h^S(F)}x^{2n}(D_F)^m$ for some $x \in F$ and some $m \in \mathbb{Z}$. We set $y := \frac{\sigma^{h^S(F)}}{x^{2n}}$. This y has the properties that we claimed. \square

Proof of (8.2): Let F have property (*) and let $E = F(\sqrt{\sigma})$ for some $\sigma \in F$. In the following let t denote the number of odd primes of F that ramify in E . In (7.1) we have shown that E has property (*) iff either $t=0$ or: $t=1$ and $\tau \notin N_{E|F}(E^*)$. We will use this to first derive a necessary condition on σ for $E(\sqrt{\sigma})$ to have property (*). Then we will show that this condition in fact suffices and it will also become clear that such σ exist.

Case 1: Suppose there exists $\sigma \in F$ such that $E = F(\sqrt{\sigma})$ has property (*) and $t=0$. What can be said about such σ ? Note that we are only interested in $\sigma \bmod F^2$, since we are concerned with the quadratic extension E . Since $t=0$, i.e. no odd prime of F ramifies in E , we know from (8.4) that the principal ideal $\sigma \cdot O_F$ can have odd prime factors only to an even degree. Applying (8.5) we can assume that $\sigma \cdot O_F$ contains no odd prime factors at all, i.e. $\sigma \cdot O_F$ is a pure power of the dyadic prime of F . Furthermore, since we are assuming that $E = F(\sqrt{\sigma})$ has property (*), we get that σ must be totally positive (so E is real) and not a square in F (for E to in fact be a proper extension of F). These conditions on σ tell us that σ is a totally positive S-unit that is not a square in F , so σ is a representative of the square class denoted by τ in (5.4). This shows that the only quadratic extension of F that could have property (*) and $t=0$ is $E = F(\sqrt{\tau})$. By (7.1.1) we know that $F(\sqrt{\sigma})$ in fact does have property (*).

This shows that there is a unique extension E of F with property (*) such that no odd prime of F ramifies in $E|F$. It is given by $E = F(\sqrt{\tau})$, where τ is a totally positive S -unit if F that is not a square.

Case 2: Suppose there exists $\sigma \in F$ such that $E = F(\sqrt{\sigma})$ has property (*) and $t=1$. What can be said about such σ ? Note that, as before, we are only interested in $\sigma \bmod F^2$. Since $t=1$ we know that exactly one odd prime of F ramifies in E . Let P be this prime. By (8.4) we have: $\text{ord}_P(\sigma) \equiv 1 \bmod 2$ and $\text{ord}_Q(\sigma) \equiv 0 \bmod 2$ for all other odd primes Q of F . Applying (8.5) we can assume that the principal ideal generated by σ does not contain any odd prime besides P and that the power to which P divides $\sigma \cdot O_F$ is odd. Applying (8.5b) we can assume that the power to which P divides $\sigma \cdot O_F$ is $h^S(F)$. Furthermore, σ must be totally positive since E is to be totally real. Hence, in order for a quadratic extension $E = F(\sqrt{\sigma})$ with property (*) and $t=1$ to exist it is necessary (not sufficient) that there exists an element $\sigma \in F$ with the following properties: σ is totally positive and the principal ideal generated by σ is of the form $D^m \cdot P^{h^S(F)}$ where D is the dyadic prime of F , $m \in \mathbb{Z}$ and P is an odd prime of F . There is another necessary condition that we have not taken into account so far: If E is to have property (*) and $t=1$, then $\tau \notin N_{E|F}(E^*)$. From the Hasse Norm Theorem it follows that there must exist a prime Λ of F (finite or infinite) such that $(\tau, \sigma)_\Lambda = -1$. Here $(\cdot, \cdot)_\Lambda$ denotes the Hilbert symbol. We will now show that if such a Λ exists it must equal P or D , where P is the odd prime dividing σ . We will also obtain a necessary condition on P for when we in fact do have $(\tau, \sigma)_P = -1$.

For an infinite prime Λ of F we have $(\tau, \sigma)_\Lambda = +1$ since τ is totally positive. For any finite prime $\Lambda \neq P, D$ we also have $(\tau, \sigma)_\Lambda = +1$. This can be seen as follows: consider F_Λ , the completion of F at Λ . Since Λ does not divide σ the extension $F_\Lambda(\sqrt{\sigma})|F_\Lambda$ is unramified, i.e. it has ramification index 1. By the Local Norm Index Theorem we have $\#O_{F_\Lambda}^*/N(O_{F_\Lambda(\sqrt{\sigma})}^*) = 1$. This shows that in this case every local unit is a local norm. The S -unit τ is a local unit in F_Λ since $\Lambda \neq D$. So τ is a local norm in F_Λ and it follows that $(\tau, \sigma)_\Lambda = +1$. The only two primes for which we have not yet checked the Hilbert symbol are P and D . By the Reciprocity Law we know that the product of the Hilbert symbols over all primes of F equals 1. Therefore $(\tau, \sigma)_P = (\tau, \sigma)_{D_F}$. This shows that for E to have property (*) and

$t=1$ it is necessary that E is of the form $F(\sqrt{\sigma})$ where $\sigma \cdot O_F = D^m \cdot P$ for some odd prime P such that $(\tau, \sigma)_P = -1$.

Since the S-unit τ is a local unit at P and σ has order 1 at P we have:

$$(\tau, \sigma)_P = -1 \iff \tau \text{ is not a square in the residue field } O_P/P$$

Hence, there are infinitely many primes P of F for which $(\tau, \sigma)_P = -1$.

Conversely, we ask: Given an odd prime P of F such that τ is not a square mod P do there exist $\sigma \in F$ such that $E := F(\sqrt{\sigma})$ has property (*) and $t=1$? Yes, we will now construct all such σ . Modulo squares of elements of F there will be exactly two such σ . It will turn out that for any given P there exist exactly two quadratic extensions of F with property (*) and $t=1$ where P is the odd prime that ramifies. Given an odd prime P of F such that τ is not a square mod P we want a totally positive element $\sigma \in F$ such that $\sigma \cdot O_F = D^m \cdot P$ for some $m \in \mathbb{Z}$. In the S-ideal class group $C^S(F)$ we have: $cl(P)^{h^S(F)} = 1$. So there exists some $x \in F^*$ such that $P^{h^S(F)} = x \cdot D^m$ for some $m \in \mathbb{Z}$. The principal ideal generated by x has the prime ideal decomposition: $P^{h^S(F)} \cdot D^{-m}$. Unfortunately x is not necessarily totally positive. Since F contains S-units with independent signs we can take an S-unit u whose embeddings into \mathbb{R} all have the same sign as the embeddings of x . We define $\sigma := x \cdot u$. This element is totally positive and since u contributed only powers of the dyadic prime D to the product, we get: $\sigma \cdot O_F = P^{h^S(F)} \cdot D^n$ for some integer n . Since $h^S(F)$ is odd and we are interested in σ only modulo squares, we can use (8.5) and assume that $\sigma \cdot O_F = P^{h^S(F)} \cdot D^n$. Note that by (8.5a) this new σ is still totally positive. If we now examine $E := F(\sqrt{\sigma})$ we see that E is totally real and P is the only odd prime ramifying. Furthermore, we have chosen P such that $(\tau, \sigma)_P = -1$, so $\tau \notin N_{E|F}(E^*)$. In (7.1) we have shown that such an extension has property (*). Are other choices for σ possible? Let $\sigma \cdot O_F$ be of the form $D^n \cdot P^{h^S(F)}$ for some $n \in \mathbb{Z}$ and assume that there is another totally positive element of F whose prime ideal decomposition is $D^m \cdot P^{h^S(F)}$ for some $m \in \mathbb{Z}$. The quotient of the two elements has only one prime divisor: the dyadic prime D . It is therefore an S-unit of F . Furthermore, it is totally positive. Modulo squares there is only one such S-unit, it has been denoted by τ . Hence there is exactly one other quadratic extension of F with property (*) and $t=1$ where the given prime P

ramifies. This extension is given by $F(\sqrt{\tau\sigma})$.

This completes the proof of (8.2). \square

For later use we note that in the proof of (8.2) we actually proved:

(8.7) Proposition: Let F be a number field with property (*). For every odd prime P of F such that τ is not a square in the residue field O_P/P there are exactly two quadratic extensions of F with property (*) in which exactly one odd prime of F ramifies. If one is given by $E_1 = F(\sqrt{\sigma})$ then the other is $E_2 = F(\sqrt{\tau\sigma})$. Besides these there is only one other quadratic extension of F with property (*). It is given by $F(\sqrt{\tau})$. Here the dyadic prime of F is the only ramifying prime.

Proof: That the dyadic prime ramifies in $F(\sqrt{\tau})$ was shown in the proof of (7.1).

The rest of (8.7) follows from the proof of (8.2). \square

(8.8) Remark: Let E be a quadratic extension of a number field F where both have property (*) and exactly one odd prime P of F ramifies in E . We know that $\tau \notin N_{E|F}(U_E^*)$, but in the proof of (8.2) we showed furthermore that τ is not a norm locally at P and D_F , i.e., if E is given by $F(\sqrt{\sigma})$ then $(\tau, \sigma)_P = (\tau, \sigma)_{D_F} = -1$. \square

CHAPTER 3

The complete picture

We now return to the question raised in chapter 1. Recall that we were looking for a number field F with elementary abelian 2-prim $K_2(O_F)$ of smallest rank with certain conditions on the parity of the honest class number and units with independent signs. In chapter 2 we examined number fields with property (*), which by definition are exactly the totally real number fields with elementary abelian 2-prim $K_2(O_F)$ of smallest rank. Using this, we now are able to list infinitely many number fields that share the properties of the example in section 4. In order to do this, we will first collect more properties of quadratic extensions where both number fields have property (*). This will be done in section 9. In section 10 we will recall generalized ideal class groups. They will be necessary in section 11. Here we will again show the existence of quadratic extensions with property (*), but this time we will be more specific and classify all quadratic extensions with property (*) according to their properties with respect to the honest class number and units with independent signs. In section 12 we finally put it all together in the main theorem. After this it will be easy to give many examples of number fields with property (*).

9. Detailed properties

Let F be a number field with property (*). We saw that in every quadratic extension $E|F$ with property (*) there is either none or exactly one odd prime of F that ramifies in E . This still leaves many questions:

What can be said about the dyadic prime of F ? We know that it does not split, but does it ramify or is it inert? How does this behavior of the dyadic prime affect the parity of the honest class number of E and whether E contains honest units with independent signs or not? We will now examine some of these relationships.

(9.1) Theorem: Let $E|F$ be a quadratic extension of number fields where both have property (*). Let t denote the number of odd primes of F that ramify in E and let D_F denote the dyadic prime of F .

1) if $t=1$ and if D_F is inert in E then: $h(E|F)$ is odd.

if D_F ramifies in E then:

$h(E|F)$ is even $\Leftrightarrow 2||h(E|F) \Leftrightarrow E$ contains units with independent signs.

2) If $t=0$ then:

F cont. units with indep. signs $\Leftrightarrow E$ cont. units with indep. signs.

furthermore, if D_F ramifies in E then: $h(E|F)$ is odd.

if D_F is inert in E then: $h(F)$ must be even and

$h(E)$ is odd $\Leftrightarrow 2||h(F)$

Remark: Note that this theorem covers all possible cases of quadratic extensions with property (*) since D_F can not split in E and by (7.1) we know that 0 and 1 are the only possible values of t .

Proof: First, we will check that if $t=0$, i.e., no odd prime of F ramifies in E , then: F contains units with independent signs $\Leftrightarrow E$ contains units with independent signs.

From (7.2.1) we know that every S -unit of F is the norm of an S -unit from E . In particular, every unit of F is the norm of an S -unit of E . By (7.3) we can conclude that every unit of F is the norm of a unit of S . By (5.10) we obtain the desired result.

Next, we will consider the case where $t=0$ and D_F is inert:

Since E is an unramified extension of F it is contained in the maximal unramified extension of F , the Hilbert class field of F . Since E is a quadratic extension of F it follows that the Hilbert class field of F over F is of even degree. By class field theory the Galois group of this extension is isomorphic to the ideal class group $C(F)$ of F . Hence, $C(F)$ is of even order, i.e. $h(F)$ is even. For the claim on the parity of $h(E)$ we refer to [C- H_2], theorem 8.2.

In all remaining cases we are dealing with a ramified extension $E|F$, so we can apply (6.6). We will now check that the condition: " C_2 acts trivially on the

2-primary subgroup of $C(E)''$ is always satisfied in the case where both E and F have property (*). Since $h^S(E)$ is odd we know that $2\text{-prim}C(E)$ is contained in the subgroup of $C(E)$ that consists of the class of the dyadic prime of E and all its powers. The dyadic prime of E is either equal to the dyadic prime of F (in the case where D_F is inert) or it is the square of the dyadic prime of F (ramified case). In either case we see that C_2 , the Galois group of E over F , acts trivially on the dyadic prime of E and therefore also on all its powers. Hence, C_2 acts trivially on $2\text{-prim}C(E)$. In the discussion of the following cases we can therefore use a simplified form of (6.6):

$$h(E|F) \text{ is odd} \iff i_0 : H^0(C_2, O_E^*) \rightarrow R^0(E|F) \text{ is surjective}$$

We can now easily prove the cases in which we claimed that $h(E|F)$ is odd:

Let $t=1$ and D_F inert in E or let $t=0$ and D_F ramified in E .

In either case we have that exactly one prime of F ramifies in $E|F$. The version of (6.3) where S is the set containing no finite primes of F is:

$2\text{-rk}R^0(E|F) = \text{number of ramified primes} - 1$. Since E is a real extension of F all infinite primes are not ramified. Hence, we see that $R^0(E|F)$ has rank 0, i.e. it is trivial. The map i_0 mapping into $R^0(E|F)$ is therefore trivially surjective. By (6.6) we conclude that the relative class number $h(E|F)$ is odd.

The only case that is left to check is: if $t=1$ and D_F ramifies in E , then

$h(E|F)$ is even $\Leftrightarrow 2 || h(E|F) \Leftrightarrow E$ contains units with independent signs.

One part of the statement is that if $h(E|F)$ is even then 2 is the exact 2-power dividing $h(E|F)$. This can be seen as follows: Let D_F denote the dyadic prime of F and D_E the dyadic prime of E . Let k be such that 2^k is the exact 2-power dividing $h(F)$. Since $h(E) = h(F) \cdot h(E|F)$, where $h(E|F)$ is even we know that 2^{k+1} divides $h(E)$. Why is 2^{k+1} in fact the exact 2-power dividing $h(E)$? Since $h^S(E)$ is odd we know that the class of D_E generates the 2-primary subgroup of the ideal class group $C(E)$. We need to check that 2^{k+1} is the exact 2-power dividing the order of D_E . We just showed that 2^{k+1} divides the order of D_E . For the converse, consider $D_E^{2^{k+1}}$:

$$D_E^{2^{k+1}} = (D_E^2)^{2^k} = (D_F^2)^{2^k}, \text{ if } D_F \text{ ramifies or } : (D_F^2)^{2^k}, \text{ if } D_F \text{ is inert}$$

In either case we are raising D_F , the generator of the 2-primary subgroup of $C(F)$,

to the order of this group, so we obtain 1. This shows that the order of D_E is a divisor of 2^{k+1} . So, we have checked that if $h(E|F)$ is even then 2 is the exact 2-power dividing it. The converse is, of course, also true.

The last step is to prove: E contains units with independent signs if and only if $h(E|F)$ is even.

Let E contains units with independent signs. From (5.10) we know that then every unit of F is the norm of a unit of E . Hence, $H^0(C_2, O_E^*) = O_F^*/N_{E|F}(O_E^*)$ is the trivial group. We compute the rank of $R^0(E|F)$ by (6.3) as: $2 - 1 = 1$. Here, the 2 counts the one odd prime of F ($t=1$) and the dyadic prime of F which is either ramified or inert in E . The map $i_0 : 1 \rightarrow R^0(E|F) \cong \mathbb{Z}/2$ can therefore not be surjective. By (6.6) we can conclude that $h(E|F)$ is even.

For the converse, we will show that if E does **not** contain units with independent signs then i_0 is surjective, so $h(E|F)$ is odd by (6.6).

Assume that E does not contain units with independent signs. We are still in the case where $t=1$ and D_F is ramified in E , so $R^0(E|F) \cong \mathbb{Z}/2$.

$$\text{We have } H^0(C_2, O_E^*) = O_F^*/N_{E|F}(O_E^*) \xrightarrow{i_0} R^0(E|F) = \mathbb{Z}/2$$

In order to show that i_0 is surjective we need to find a class in $O_F^*/N_{E|F}(O_E^*)$ whose image in $R^0(E|F)$ is not trivial. By (6.4) we can consider $R^0(E|F)$ a subgroup of $H^0(C_2, E^*) = F^*/N_{E|F}(E^*)$. We are therefore looking for a class in $O_F^*/N_{E|F}(O_E^*)$ whose image in $F^*/N_{E|F}(E^*)$ is not trivial. This means that we need to find a unit of F that is not the norm of any element from E .

If F does not contain units with independent signs we take τ . Since E has property (*) and $t=1$ we know by (7.1) that $\tau \notin N_{E|F}(E^*)$. By (5.5) the class of τ is contained in $O_F^*/(O_F^*)^2$, so it is an element of the required kind.

If F contains units with independent signs τ will not be an element of the required kind since it is not a unit. Since E does not contain units with independent signs we know from (5.10) that not all units of F are norms of units from E . Let a be a unit of F that is not the norm of any unit of E . By (7.4) a can not be the norm of any element of E . Hence, a is a unit of F that is not a norm from E . This concludes the proof of (9.1). \square

(9.2) Lemma: Let $E|F$ be a quadratic extension where both number fields have property (*) and where exactly one odd prime of F ramifies in E .

If $h(F)$, the class number of F , is even then $h(E)$ is even.

If $h(F)$ is odd then $h(E)$ is odd, with the possible exception of the case where:

$h(F)$ is odd, the dyadic prime of F ramifies in E and F contains units with independent signs. In this case $h(E)$ is even iff E contains units with independent signs.

Proof: Since the extension $E|F$ is ramified we have $h(E) = h(F) \cdot h(E|F)$, where $h(E|F) \in \mathbb{Z}$ is the relative class number. From this it is clear that if $h(F)$ is even, then so is $h(E)$. Now let $h(F)$ be odd. From (9.1) we know that if D_F , the dyadic prime of F , is inert in E then $h(E)$ is odd. Also by (9.1) we know that if D_F ramifies then $h(E|F)$ is even iff E contains units with independent signs. \square

Remark: An example where $h(F)$ is odd and where there are quadratic extensions E of F that have $h(E)$ even and others with $h(E)$ odd is the following:

Let $F = \mathbb{Q}$, here $h(F) = 1$. The extensions $F(\sqrt{2p})$ where $p \equiv 5 \pmod{8}$ have even class number, the extensions $F(\sqrt{2})$; $F(\sqrt{2p})$ where $p \equiv 3 \pmod{8}$ and $F(\sqrt{p})$ where $p \equiv 3$ or $5 \pmod{8}$ all have odd class number.

10. Completions and generalized ideal class groups

We are trying to obtain a complete picture of what type of quadratic extensions with property (*) there can exist over a number field with property (*). We would like to get an idea of how many there are and what their properties are with respect to containing (honest) units with independent signs and the parity of their class numbers. We will see that the quadratic extensions with property (*) can be classified into families that all share certain properties. For this classification we need the completion of F at its dyadic prime, or rather the group of square classes of the

completion. We will also need generalized ideal class groups. They will be defined in (10.4).

Notation: Let F be a number field with property (*). In particular, F has only one dyadic prime. As before, it will be denoted by D_F or, if no confusion is possible, by D . The completion of F at its dyadic prime will be denoted by F_D . We will use O_D to denote the local ring of integers of F_D .

In the following we will restrict our attention to number fields with property (*). In particular, we will assume that F contains only one dyadic prime and that it has odd S -class number. All of the following holds true for a more general set S , but from now on we will formulate all statements for the case where S is the set consisting of D_F and the infinite primes of F .

Consider the group of S -integers of F , which is contained in the multiplicative group F^* . F^* , in turn is contained in its completion at the dyadic prime F_D^* . By taking square classes of U_F^S , F^* and F_D^* , we obtain the finite groups $U_F^S/(U_F^S)^2$ and $F_D^*/(F_D^*)^2$ and the infinite group $F^*/(F^*)^2$. Induced by the inclusion map we obtain an injective map from $U_F^S/(U_F^S)^2$ into $F^*/(F^*)^2$. The map from $F^*/(F^*)^2$ into $F_D^*/(F_D^*)^2$ cannot be injective. It is, however, surjective.

(10.1) Lemma: Let F be a number field with property (*) and let S be the set containing D_F and all infinite primes of F . Then the map $U_F^S/(U_F^S)^2 \longrightarrow F_D^*/(F_D^*)^2$ from the square classes of S -units of F to the square classes of the completion of F at D_F is injective.

Proof: Let $cl(v)$ be in the kernel, so v is an S -unit of F that is in F_D^2 under the inclusion of F into F_D . We need to show that v is already the square of an S -unit of F . It suffices to show that v is a square in F , since then it follows that it is a square in U_F^S .

Let us assume $v \notin (F^*)^2$. This leads to a contradiction:

$F(\sqrt{v})$ is an extension of degree 2 of F but $F_D(\sqrt{v}) = F_D$. Hence the degree of the extension $F_D(\sqrt{v})$ over F_D is 1, so both the ramification index e_D and the inertia degree f_D of $F_D(\sqrt{v})$ over F_D are 1. Since $F_D(\sqrt{v})$ is unramified over F_D we know that D_F does not ramify in $F(\sqrt{v})$. Can any other finite prime $P \neq D_F$ ramify in

$F(\sqrt{v})$? No. Note that v is an S-unit, so the prime ideal decomposition of $v \cdot \mathcal{O}_F$ contains no primes other than D . Comparing this to the criterion in (8.4) we see that no odd prime can ramify. Let $\sigma_1, \dots, \sigma_{r_1(F)}$ denote the infinite primes of F . Some of these could ramify in $F(\sqrt{v})$. Let $I := \{i \mid \sigma_i \text{ is ramified}\}$. We now need to use some facts from class field theory. The Artin reciprocity map gives a surjective map $\omega : C(F, c_f) \longrightarrow \text{Gal}(F(\sqrt{v})|F) = \mathbb{Z}/2$. Here $C(F, c_f)$ is the generalized ideal class group corresponding to the cycle $c_f = \prod_{i \in I} \sigma_i$. The definition of the generalized ideal class group is given in (10.4'). For the cycle c_f we have: $C(F, c_f) = I(F)/P(c_f)$ where $I(F)$ denotes the group of ideals of F and $P(F, c_f)$ denotes the group of principal ideals of F that have a generator z such that $\text{sign}[\sigma_i(z)] > 0$ for all $i \in I$. The class of the dyadic prime D maps to the identity under ω . This follows from the definition of ω and the fact that $f_D = 1$. Since $cl(D_F)$ is in the kernel of ω we see that ω factors through $C(F, c_f)/cl(D_F)$. This group is isomorphic to $C^S(F)$; the S-ideal class group of F . Recall the definition: $C^S(F) = I(F)/(P(F), D_F)$, where $P(F)$ is the set of principal ideals of F . The principal ideals do not necessarily have a generator that is positive under the embeddings σ_i with $i \in I$. Hence $P(F) \neq P(F, c_f)$. But if we consider ideals modulo the dyadic prime, then every principal ideal does have generators that are positive anywhere. This follows from the fact that F contains S-units with independent signs. For a given principal ideal, we multiply a generator by an S-unit with the appropriate signs of its embeddings. The resulting ideal differs from the given principal ideal by factors of D_F only. The order of $C(F, c_f)/cl(D_F)$ is therefore $h^S(F)$, which is odd. This odd ordered group is mapped into $\mathbb{Z}/2$ by the homomorphism ω , hence ω is the trivial map. This is a contradiction to the fact that ω is surjective onto $\mathbb{Z}/2$. \square

Remark: We can therefore consider $U_F^S/(U_F^S)^2$ as a subgroup of $F_D^*/(F_D^*)^2$ whenever this is convenient.

Note that $U_F^S/(U_F^S)^2$, $F^*/(F^*)^2$ and $F_D^*/(F_D^*)^2$ are $\mathbb{Z}/2$ -vector spaces. Here the nontrivial element of $\mathbb{Z}/2$ acts on the groups by squaring the classes. We have this vector space structure in mind when we now talk about "linearly independent" and "basis".

(10.2) Proposition: Let F be a number field with property (*) of degree $r_1(F)$

and denote the embeddings of F into \mathbf{R} by $\sigma_1, \dots, \sigma_{r_1(F)}$. Let $\{u_1, \dots, u_{r_1(F)}\}$ be a set of square classes of S -units of F such that $\text{sign}[\sigma_i(u_j)] = +1$ for $j \neq i$ and $\text{sign}[\sigma_i(u_i)] = -1$ for $i, j \in \{1, \dots, r_1(F)\}$. Let τ be the nontrivial totally positive square class [see (5.4)]. Then $\{u_1, \dots, u_{r_1(F)}, \tau\}$ are a basis of $U_F^S/(U_F^S)^2$. Furthermore: the Hilbert symbol $(\cdot, \tau)_{D_F}$ is trivial on $U_F^S/(U_F^S)^2$.

Proof: As before, we will simplify notation by denoting representatives of square classes by the same symbol as the class.

We will first check that the elements are linearly independent:

$$\text{Let } \tau^l \cdot \prod_{i=1}^{r_1(F)} u_i^{l_i} = 1 \quad \text{with } l, l_i \in \{0, 1\}$$

For any fixed $j \in \{1, \dots, r_1(F)\}$ we have:

$$1 = \text{sign}[\sigma_j(1)] = \text{sign}[\sigma_j(\tau^l \prod_i u_i^{l_i})] = \text{sign}[\sigma_j(u_j^{l_j})] = (-1)^{l_j}$$

Hence, $l_j = 0$ for all j . This leaves $\tau^l = 1$. By choice of τ as distinct from 1, we have $l = 0$. This shows that all exponents $l, l_1, \dots, l_{r_1(F)}$ are 0, so the elements are indeed independent. In (5.3) we showed $\#U_F^S/(U_F^S)^2 = 2^{r_1(F)+1}$. Hence the dimension of the $\mathbb{Z}/2$ -vector space $U_F^S/(U_F^S)^2$ is $r_1(F) + 1$. Therefore the $r_1(F) + 1$ linearly independent elements form a basis.

Every element of $U_F^S/(U_F^S)^2$ can be expressed as a product of elements of $\{u_1, \dots, u_{r_1(F)}, \tau\}$, as above. It therefore suffices to check that $(u, \tau)_{D_F} = +1$ for all $u \in \{u_1, \dots, u_{r_1(F)}, \tau\}$. We conclude this by reciprocity: The Hilbert symbol of u and τ is $+1$ at any infinite prime of F since τ is totally positive. The Hilbert symbol is $+1$ at any finite prime $P \neq D_F$ since both S -units u and τ are local units at P . \square

(10.3) Remark: If we consider $U_F^S/(U_F^S)^2$ as contained in $F_D^*/(F_D^*)^2$ the set $\{u_1, \dots, u_{r_1(F)}, \tau\}$ is also linearly independent in $F_D^*/(F_D^*)^2$. It does not form a basis, since $F_D^*/(F_D^*)^2$ has $2^{r_1(F)+2}$ elements. A basis of $F_D^*/(F_D^*)^2$ contains exactly one more element. Such an element $\beta \in F_D^*/(F_D^*)^2$ is characterized by: $(\beta, \tau)_{D_F} = -1$. In particular, we have: $U_F^S/(U_F^S)^2$ is the kernel of $(\cdot, \tau)_{D_F}$.

Proof: By (10.2) we have $(v, \tau)_{D_F} = +1$ for all $v \in U_F^S / (U_F^S)^2$. The Hilbert symbol $(\cdot, \cdot)_{D_F}$ is non degenerate. If $(\beta, \tau)_{D_F} = +1$ for $\beta \notin U_F^S / (U_F^S)^2$ then it would follow that $\tau = 1 \in F_D^* / (F_D^*)^2$. This contradicts the definition of τ as the nontrivial totally positive square class. Hence $(\beta, \tau)_{D_F} = -1$ for all $\beta \notin U_F^S / (U_F^S)^2$. \square

The definition of generalized ideal class groups can be found for example in [La]. We first state the general definition in (10.4') and then restate it in (10.4) for the special case that we need it in.

(10.4') Definition: Let F be a number field and let S be a set of primes of F . Let $c_S = \prod_{P \in S} P^{e_P}$ be a cycle, i.e. a formal product of the primes in S . For $z \in F^*$, we define: $z \equiv 1 \pmod{*c_S}$ iff z is positive at all real infinite primes in S and $z \equiv 1 \pmod{P^{e_P}}$ for all finite primes $P \in S$.

$I(c_S) := \{A \mid A \text{ is a fractional ideal of } F \text{ with } \text{ord}_P(A) = 0 \text{ for all } p \in S\}.$

$P(c_S) := \{A \mid A \text{ is a principal ideal that has a generator } z \equiv 1 \pmod{*c_S}\}$

The generalized ideal class group is defined as: $C(F, c_S) := I(c_S) / P(c_S).$

In the following we only need the generalized ideal class group in connection with number fields with property (*). In particular, F is a totally real number field that contains exactly one dyadic prime and by S we mean the set that consists of that dyadic prime and the infinite primes of F . We will therefore now give a definition that is restricted to apply to this special case.

(10.4) Definition: Let F be a totally real number field that contains exactly one dyadic prime D_F . Let $\sigma_1, \dots, \sigma_{r_1(F)}$ denote the real embeddings of F . Let c_S be the cycle: $(D_F)^{2e+1} \cdot \prod_{i=1}^{r_1(F)} \sigma_i$ where e is the ramification index of F_D over \mathbb{Q}_2 . (Here F_D is the completion of F at D_F and \mathbb{Q}_2 are the 2-adic numbers) For $z \in F^*$, we define:

$$z \equiv 1 \pmod{*c_S} \text{ iff } z \text{ is totally positive and } z \equiv 1 \pmod{(D_F)^{2e+1}}$$

Let $I(c_S)$ denote the group of fractional O_F ideals A such that $\text{ord}_{D_F} A = 0$ and let $P(c_S)$ denote the subgroup that consists of principal ideals for which there exist

generators that are congruent to 1 mod* c_S . The generalized ideal class group $C(F, c_S)$ is defined as the quotient $C(F, c_S) = I(c_S)/P(c_S)$.

(10.5) Lemma: If $z \equiv 1 \pmod{* c_S}$ then z is a local square, i.e., a square in the completion of F , at all primes that are contained in S .

Proof: Let $z \equiv 1 \pmod{* c_S}$. The completion of F at any infinite prime is \mathbf{R} . Since z is totally positive it certainly is a square in \mathbf{R} . We have to show that z is a square in F_D , the completion of F at the dyadic prime D_F . By assumption we have $z \equiv 1 \pmod{(D_F)^{2e+1}}$. We will apply Hensel's Lemma to show $z \in F_D^2$:

Consider the polynomial $f(x) = x^2 - z \in F_D[x]$. Modulo $(D_F)^{2e+1}$ there exists a solution to $f(x) = x^2 - z \equiv x^2 - 1$, namely: $f(1) \equiv 0 \pmod{(D_F)^{2e+1}}$. The derivative of $f(x)$ is $f'(x) = 2x$, so $f'(1) = 2$. Recall that e denotes the ramification index of F_D over \mathbb{Q}_2 . This tells us that the prime ideal decomposition of 2 in F is: $2 \cdot \mathcal{O}_F = (D_F)^e$. Hence, $\text{ord}_{D_F}(2) = e$. We have now checked the following inequality: $0 \leq 2 \cdot \text{ord}_{D_F}(f'(1)) < 2e + 1$. This is precisely the condition that needs to be satisfied in Hensel's Lemma. We can now conclude that $f(x) = x^2 - z$ has a solution in F_D , so z is a square in F_D . \square

The following theorem will be the key to our classification of quadratic extensions with property (*). We will formulate the theorem only for number fields with property (*) where S is the set consisting of D_F and the infinite primes of F . The theorem goes through in the same way for more general cases. It is, however, crucial that $h^S(F)$ be odd.

(10.6) Theorem: Let F be a number field with property (*). Let D_F denote the dyadic prime of F and let τ be the nontrivial totally positive square class, see (5.4). There exists a surjective group homomorphism Φ from $F_D^*/(F_D^*)^2$ onto $C(F, c_S)/C(F, c_S)^2$ whose kernel is $\{1, \tau\}$.

Remark: To simplify notation in all of the following we will not distinguish between an element in F or its image in the completion F_D , unless that distinction is essential

to the argument. Also, we will use the same notation for an element and its square class except for β and σ , which we need to distinguish.

Proof: Let $\sigma_1, \dots, \sigma_{r_1(F)}$ denote the embeddings of F into \mathbf{R} . Consider the inclusion of F^* into the product of completions of F : $F_D^* \times \mathbf{R}^{r_1(F)}$, defined by $z \mapsto (z, \sigma_1 z, \dots, \sigma_{r_1(F)} z)$. From the independence of valuations we know that this map is dense. The induced map into the finite group of square classes:

$$F^* \longrightarrow F_D^*/(F_D^*)^2 \times (\mathbb{Z}/2)^{r_1(F)} \quad z \mapsto (z, \text{sign}[\sigma_1 z], \dots, \text{sign}[\sigma_{r_1(F)} z])$$

is therefore surjective.

We can now define the map $\Phi : F_D^*/(F_D^*)^2 \longrightarrow C(F, c_S)/C(F, c_S)^2$

Let $\beta \in F_D^*/(F_D^*)^2$. By the above, we can choose a totally positive element $\sigma \in F$ such that $\sigma = \beta \in F_D^*/(F_D^*)^2$. Note that this choice of σ is not unique! Let $m \in \mathbb{Z}$ be the exact power to which D_F appears in the prime ideal decomposition of the principal ideal generated by σ in F . We have:

$$\sigma \cdot O_F = D_F^m A \quad \text{for some fractional ideal } A \in I(c_S)$$

We take the odd part of this, i.e. A . We define the class of A in $C(F, c_S)/C(F, c_S)^2$ to be the image of β .

After defining this map

$$\Phi : F_D^*/(F_D^*)^2 \longrightarrow C(F, c_S)/C(F, c_S)^2 \quad \text{with } \beta \mapsto cl(A)$$

we must check that it is well defined and that it is a surjective group homomorphism with kernel $\{1, \tau\}$.

Φ is well defined:

For a given β the choice of σ was certainly not unique. We therefore need to check if different choices of σ result in the same class in $C(F, c_S)/C(F, c_S)^2$. Let $\sigma, s \in F^*$ be two totally positive elements such that $\sigma = s \in F_D^*/(F_D^*)^2$. (Again, we are simplifying the notation by not distinguishing between $\sigma, s \in F$ and their images in $F_D^*/(F_D^*)^2$!) Consider $\frac{s}{\sigma} \in F$. This is a totally positive element since both σ and s are totally positive. We claim that there exists an element $a \in F$ such that

$\frac{s}{\sigma} \cdot a^{-2} \equiv 1 \pmod{*c_S}$. For any $a \in F$ we certainly have that $\frac{s}{\sigma} \cdot a^{-2}$ is a totally positive element of F . To prove the claim we must show that there exists a such that $\frac{s}{\sigma} \cdot a^{-2} \equiv 1 \pmod{(D_F)^{2e+1}}$. By assumption we have that $\sigma = s \in F_D^*/(F_D^*)^2$, so $\frac{s}{\sigma}$ is a square in F_D . therefore the element $\frac{s}{\sigma} \in F$ is a square modulo any power of D_F . In particular, there exists $a \in F$ such that $\frac{s}{\sigma} \equiv a^2 \pmod{(D_F)^{2e+1}}$. This completes the proof that there exists $a \in F$ such that $\frac{s}{\sigma} \cdot a^{-2} \equiv 1 \pmod{*c_S}$.

Let $\sigma \cdot O_F = D_F^m A$ with $A \in I(c_S)$. Since $s = \frac{s}{\sigma} \cdot \sigma = (\frac{s}{\sigma} \cdot a^{-2}) \cdot a^2 \cdot \sigma$ we can write the principal ideal generated by s as:

$$s \cdot O_F = \left(\frac{s}{\sigma} \cdot a^{-2}\right) a^2 D_F^m A$$

We have $a \cdot O_F = D_F^b B$ for some $b \in \mathbb{Z}$ and $B \in I(c_S)$. Plugging this into the above equation yields:

$$s \cdot O_F = \left(\frac{s}{\sigma} \cdot a^{-2}\right) D_F^{2b+m} B^2 A$$

By definition of Φ , we now take the class of the odd part of $s \cdot O_F$:

$$cl\left(\left[\frac{s}{\sigma} \cdot a^{-2}\right] B^2 A\right) = cl\left(\left[\frac{s}{\sigma} \cdot a^{-2}\right] \cdot O_F\right) \cdot cl(B)^2 \cdot cl(A) \in C(F, c_S)/C(F, c_S)^2$$

The class of $\left[\frac{s}{\sigma} \cdot a^{-2}\right] \cdot O_F$ is trivial already in $C(F, c_S)$ since $\frac{s}{\sigma} \cdot a^{-2} \equiv 1 \pmod{*c_S}$. In $C(F, c_S)/C(F, c_S)^2$ we therefore obtain:

$$cl\left(\left[\frac{s}{\sigma} \cdot a^{-2}\right] B^2 A\right) \equiv cl(A)$$

This shows that different choices of s and σ still give the same class in $C(F, c_S)/C(F, c_S)^2$, hence the map Φ is well defined.

We check that Φ is a homomorphism of multiplicative groups:

Recall how the map was defined: For $\beta \in F_D^*/(F_D^*)^2$ we chose a totally positive inverse image $\sigma \in F^*$. This map from the group of totally positive elements in F^* to $F_D^*/(F_D^*)^2$ is a group homomorphism. We then take the odd part of $\sigma \cdot O_F$. This map from F^* into $I(c_S)$ is again a group homomorphism. Factoring out $P(c_S)$ and taking square classes also preserves the group structure, i.e. it is a group homomorphism. The map is surjective:

Given $cl(A) \in C(F, c_S)/C(F, c_S)^2$ for any $A \in I(c_S)$ we will construct an inverse image. A is a fractional ideal of F and by assumption the S-class number $h^S(F)$

is odd. Therefore there exist $m \in \mathbb{Z}$ and $\sigma \in F$ such that $A^{h^S(F)} = \sigma \cdot D_F^m$. Claim: the class of σ in $F_D^*/(F_D^*)^2$ is an inverse image of $cl(A)$. To check where $\sigma \in F_D^*/(F_D^*)^2$ maps to we need a totally positive inverse image in F . The condition "totally positive" prevents us from taking $\sigma \in F$. Since F is assumed to contain S -units with independent signs we can take an S -unit $u \in F$ that has the same sign as σ in all embeddings of F . The product $\sigma u \in F$ is totally positive and we know that the ideal $\sigma u \cdot O_F$ differs from $\sigma \cdot O_F$ only by powers of the dyadic prime. Since $\sigma \cdot O_F$ was equal to $A^{h^S(F)} D_F^{-m}$, we have $\sigma u \cdot O_F = A^{h^S(F)} D_F^{-m+n}$ for some $n \in \mathbb{Z}$. The odd part of this is $A^{h^S(F)}$. Its class in $C(F, c_S)$ is $cl(A)^{h^S(F)}$. Modulo squares this is equivalent to $cl(A)$, since $h^S(F)$ is odd. This shows that $\sigma \in F_D^*/(F_D^*)^2$ is an inverse image of $cl(A) \in C(F, c_S)/C(F, c_S)^2$.

We compute the kernel of Φ :

Let $\beta \in F_D^*/(F_D^*)^2$ be in the kernel of the map. First, we show that there must exist a totally positive S -unit of F whose image in $F_D^*/(F_D^*)^2$ equals β : We know that there exists a totally positive element $\sigma \in F$ whose image in $F_D^*/(F_D^*)^2$ equals β . The ideal generated by σ in F is of the form $\sigma \cdot O_F = A \cdot (D_F)^n$ for some $n \in \mathbb{Z}$ and some $A \in I(c_S)$. By definition of the image of β under Φ we take the class in $C(F, c_S)/C(F, c_S)^2$ of the odd part of $\sigma \cdot O_F$. Hence this image is $cl(A)$. We are assuming that β is in the kernel, so $cl(A) = 1 \in C(F, c_S)/C(F, c_S)^2$. This means that $A = z \cdot B^2$ for some $z \in F$ with $z \equiv 1 \pmod{c_S}$ and some $B \in I(c_S)$. In F we have: $\sigma \cdot O_F = z \cdot B^2 (D_F)^n$. We now raise this to the power $h^S(F)$. Since $h^S(F)$ is the S -class group of F we have: $B^{h^S(F)} = b \cdot (D_F)^m$ for some $b \in F$ and $m \in \mathbb{Z}$. We obtain:

$$\sigma^{h^S(F)} \cdot O_F = z^{h^S(F)} (B^{h^S(F)})^2 (D_F)^{h^S(F)n} = z^{h^S(F)} b^2 (D_F)^{2m+h^S(F)n}$$

We consider the element: $\frac{\sigma^{h^S(F)}}{z^{h^S(F)} b^2} \in F$. It has the following properties:

- a) it is a totally positive S -unit,
- b) its image in $F_D^*/(F_D^*)^2$ is β .

To check this we first note that $z \equiv 1 \pmod{c_S}$, hence by (10.5) z is totally positive and its image in F_D is a square. We have σ , z and of course b^2 are totally positive, therefore $\frac{\sigma^{h^S(F)}}{z^{h^S(F)} b^2}$ is totally positive. It is an S -unit because it generates the ideal $(D_F)^{2m+h^S(F)n}$, which contains no odd primes. This proves a).

The element σ was chosen such that its image in $F_D^*/(F_D^*)^2$ is β . Since $h^S(F)$ is odd we see that $\sigma^{h^S(F)}$ also has image β . The elements z and b^2 both have trivial images in $F_D^*/(F_D^*)^2$ since they are contained in F_D^2 . This proves b).

Recall that by (10.1) we can consider $U_F^S/(U_F^S)^2$ a subgroup of $F_D^*/(F_D^*)^2$. We have just shown that if an element of $F_D^*/(F_D^*)^2$ is in the kernel, then it is represented by a totally positive S-unit. Modulo squares there are exactly two such S-units: 1 and τ . Both of these are in fact in the kernel. This concludes the proof of (10.6). \square

11. Families of number fields with property (*)

Recall that for a given F with property (*) there is exactly one quadratic extension with property (*) in which no odd prime of F ramifies. It is given by $F(\sqrt{\tau})$. In all other quadratic extensions with property (*) there is exactly one odd prime of F that ramifies. It is these other extensions that we will now be concerned with. In the previous section we defined a surjective group homomorphism Φ from $F_D^*/(F_D^*)^2$ onto $C(F, c_S)/C(F, c_S)^2$ whose kernel has two elements, namely 1 and τ . We will now use the 2 to 1 correspondence that Φ gives to classify the infinitely many quadratic extensions E with property (*) of F in which one odd prime ramifies.

A quadratic extension E of F is of the form $E = F(\sqrt{\sigma})$ for some $\sigma \in F$, where σ is determined uniquely up to squares in F . The extension therefore determines a unique element of $F_D^*/(F_D^*)^2$, by taking the image of σ . In the following this image of σ in $F_D^*/(F_D^*)^2$ will be denoted by β . If E has property (*) and if one odd prime of F ramifies in E , then the extension determines a unique odd prime, namely the one that ramifies. This prime can be considered an element of $I(c_S)$. The extension therefore determines a unique element in the factor group $C(F, c_S)$.

(11.1) Proposition: Let F be a number field with property (*) and let $E = F(\sqrt{\sigma})$ be a quadratic extension with property (*) in which one odd prime of F

ramifies. Let β denote the class of σ in $F_D^*/(F_D^*)^2$ and let P be the odd prime of F that ramifies in E . Then the image of β under the map Φ , defined in (10.6), is the class of P in $C(F, c_S)/C(F, c_S)^2$.

Proof: Recall how the image of β under Φ was defined:

We take a totally positive element of F whose image in $F_D^*/(F_D^*)^2$ is β . Such an element is given by σ . Note, that it is indeed totally positive since E is totally real. We then need the odd part of the principal ideal $\sigma \cdot O_F$. We are assuming that P is the only odd prime that ramifies in $E = F(\sqrt{\sigma})$. Applying (8.4) we obtain that the prime ideal decomposition of $\sigma \cdot O_F$ contains P to an odd power and every other odd prime to an even power. We take the class in $C(F, c_S)/C(F, c_S)^2$ of this odd part of $\sigma \cdot O_F$. This leaves $cl(P)$, since all squares are factored out. So, $cl(P)$ is indeed the image of β under Φ . \square

In the following proposition we consider $U_F^S/(U_F^S)^2$ as a subgroup of $F_D^*/(F_D^*)^2$, which can be done by (10.1). The complement of $U_F^S/(U_F^S)^2$ in $F_D^*/(F_D^*)^2$ will be denoted by $F_D^*/(F_D^*)^2 - U_F^S/(U_F^S)^2$.

(11.2) Proposition: Let F be a number field with property (*) and let $E = F(\sqrt{\sigma})$ be a quadratic extension of F with property (*) in which exactly one odd prime of F ramifies. Then the class of σ in $F_D^*/(F_D^*)^2$ is contained in $F_D^*/(F_D^*)^2 - U_F^S/(U_F^S)^2$.

Proof: Let σ denote the element of F or $F^*/(F^*)^2$ and β its image in F_D or $F_D^*/(F_D^*)^2$. As before, our notation does not distinguish between elements and their square classes. By (10.2) we have $(\tau, v)_{D_F} = +1$ for all S -units v . On the other hand, since E has property (*) and one odd prime of F ramifies in E , we know from (8.8) that τ is not a local norm at the dyadic prime D_F : $(\tau, \beta)_{D_F} = -1$. This shows that $\beta \in F_D^*/(F_D^*)^2$, the image of σ , can not be contained in the subgroup $U_F^S/(U_F^S)^2$. \square

The converse of (11.2) also holds, namely: for every $\beta \in F_D^*/(F_D^*)^2 - U_F^S/(U_F^S)^2$ there exist extensions of F with property (*). Note that (8.2) already gave the existence

of infinitely many quadratic extensions of F with property (*) in which exactly one odd prime ramifies. Proposition (11.3) will be an improvement on this because it shows the existence of infinitely many such $E = F(\sqrt{\sigma})$ for any given image β of σ .

By (8.7) we must show that for a given $\beta \in F_D^*/(F_D^*)^2 - U_F^S/(U_F^S)^2$ there exists $\sigma \in F$ (modulo squares) that has the following properties:

σ is totally positive and its prime ideal decomposition is of the form $\sigma \cdot O_F = (D_F)^m P^{h^S(F)}$ for some odd prime P for which τ is not a square in the residue field O_P/P .

Any $\beta \in F_D^*/(F_D^*)^2$ certainly has many totally positive inverse images in $F^*/(F^*)^2$, but why should there be those among them that contain exactly one odd prime? This is where we will use the map Φ that was constructed in (10.6). It takes β to a class in the generalized ideal class group modulo squares. The class of $\Phi(\beta)$ contains infinitely many primes P . We will see that for each such P we can construct an element σ whose image in $F_D^*/(F_D^*)^2$ is β and where P is the only odd prime that ramifies in $F(\sqrt{\sigma})$. Furthermore, we will see that if β was chosen in $F_D^*/(F_D^*)^2 - U_F^S/(U_F^S)^2$ then each $F(\sqrt{\sigma})$ will have property (*), i.e., each P will have the property that τ is not a square in the residue field O_P/P .

(11.3) Proposition: Let F be a number field with property (*).

For each $\beta \in F_D^*/(F_D^*)^2 - U_F^S/(U_F^S)^2$ there exist infinitely many quadratic extensions $E = F(\sqrt{\sigma})$ of F such that E has property (*), exactly one odd prime of F ramifies in E and β is the image of σ in $F_D^*/(F_D^*)^2$.

Proof: Given $\beta \in F_D^*/(F_D^*)^2$, consider its image in $C(F, c_S)/C(F, c_S)^2$ under Φ . Every class in $C(F, c_S)/C(F, c_S)^2$ contains infinitely many prime ideals of F . They are all odd primes, by the definition of $C(F, c_S)$. As in the proof of (8.2) we have that every odd prime P gives rise to exactly two real quadratic extensions of F in which P is the only odd prime that ramifies. Recall that these extensions are obtained by raising P to the power $h^S(F)$. This ideal is of the form: $P^{h^S(F)} = \sigma D_F^m$, where we can assume $\sigma \in F$ to be totally positive since F contains S -units with independent signs. The real quadratic extensions of F that are uniquely determined by the fact

that P is the only odd prime that ramifies are: $E_1 = F(\sqrt{\sigma})$ and $E_2 = F(\sqrt{\tau\sigma})$. What are the images of σ and $\tau\sigma$ in $F_D^*/(F_D^*)^2$? By definition of Φ both images map to $cl(P) \in C(F, c_S)/C(F, c_S)^2$. By the choice of P we also know that β is an inverse of $cl(P)$. Since Φ is a two to one map we have: β is the image of either σ or $\tau\sigma$ in $F_D^*/(F_D^*)^2$. Since we are dealing with square classes we can multiply by τ , if necessary, and assume that β is the image of σ .

The above works for any $\beta \in F_D^*/(F_D^*)^2$. If we take $\beta \in F_D^*/(F_D^*)^2 - U_F^S/(U_F^S)^2$, then we claim that both $E_1 = F(\sqrt{\sigma})$ and $E_2 = F(\sqrt{\tau\sigma})$ have property (*):

By the criterion in (7.1) we need to check that τ is not a norm from E_1 over F and also not from E_2 over F . It suffices to show that τ is not a norm locally for some prime of F . We consider the dyadic prime D_F : we have chosen $\beta \notin U_F^S/(U_F^S)^2$ by (10.3) we have $(\tau, \beta)_{D_F} = -1$. This shows that τ is not a norm from $E_1 = F(\sqrt{\sigma})$ over F . We have $(\tau, \tau)_{D_F} = +1$ since the Hilbert symbol of τ and τ is clearly $+1$ at all other primes. Hence, we have:

$$(\tau, \tau\sigma)_{D_F} = (\tau, \sigma)_{D_F}(\tau, \tau)_{D_F} = (\tau, \sigma)_{D_F} = -1$$

Therefore, τ is also not a norm from $E_2 = F(\sqrt{\tau\sigma})$ over F .

We have shown: For any given $\beta \in F_D^*/(F_D^*)^2 - U_F^S/(U_F^S)^2$ there are infinitely many P that each give rise to exactly one quadratic extension $E = F(\sqrt{\sigma})$ such that this extension has property (*), exactly one odd prime, namely P , ramifies in E and β is the image of σ in $F_D^*/(F_D^*)^2$.

Note that the other extensions $E = F(\sqrt{\tau\sigma})$ do not satisfy all of the required properties since the image of $\tau\sigma$ in $F_D^*/(F_D^*)^2$ is $\tau\beta \neq \beta$. \square

(11.4) Definition: Let F be a number field with property (*). Let $E = F(\sqrt{\sigma})$ and $E' = F(\sqrt{s})$ be quadratic extensions with property (*) in which exactly one odd prime of F ramifies. We say that E and E' are members of the same *family* iff σ and s determine the same element in $F_D^*/(F_D^*)^2$.

(11.5) Remarks:

a) By (11.2) each family is determined by an element in $F_D^*/(F_D^*)^2 - U_F^S/(U_F^S)^2$. There are $2^{r_1(F)+1}$ such elements.

- b) For each element of $F_D^*/(F_D^*)^2 - U_F^S/(U_F^S)^2$ we obtain a family that contains infinitely many members. This follows immediately from (11.3). We will often refer to families as *infinite families*.
- c) For a number field F with property (*) there is a one to one correspondence between the elements of $F_D^*/(F_D^*)^2 - U_F^S/(U_F^S)^2$ and the families of quadratic extensions with property (*) in which exactly one odd prime ramifies.

We will now justify this classification of extensions with property (*) into families by showing that members of the same family have the same behavior with respect to many of the properties that we are interested in.

(11.6) Proposition: Let F be a number field with property (*). Let \mathbf{E} be a family of quadratic extensions of F with property (*) in which exactly one odd prime of F ramifies.

- a) The dyadic prime D_F of F either ramifies in all members of \mathbf{E} or in none.
- b) The members of \mathbf{E} either all contain units with independent signs or they all do not contain units with independent signs.
- c) All members E of \mathbf{E} have the same exact 2-power dividing their class numbers $h(E)$, in particular, they are either all even or all odd.

Proof: Let β denote the element of $F_D^*/(F_D^*)^2 - U_F^S/(U_F^S)^2$ that corresponds to the family \mathbf{E} . Let $E = F(\sqrt{\sigma})$ be a member of \mathbf{E} . This means that β is the image of σ in $F_D^*/(F_D^*)^2$.

- a) We have: D_F ramifies in E over $F \Leftrightarrow F_D(\sqrt{\beta})$ is a ramified extension of F_D . This proves that the behavior of the dyadic prime in $E|F$ is determined by the family that E belongs to.

c) follows immediately from a), b) and (9.1)

- b) If F does not contain units with independent signs, then no extension E with property (*) contains units with independent signs.

If F contains units with independent signs we have from (5.10): E contains units with independent signs iff all units of F are norms of units of E . Let a be a unit of F . We will now check that whether or not a is a norm from E depends only on

β . To check if a is a norm we check if it is a norm locally at all primes of F . To do this we consider the Hilbert symbol of a and σ . At an infinite prime of F it is $+1$ since σ is totally positive. At a finite prime that is distinct from D_F and the one prime that ramifies in E , the Hilbert symbol is again $+1$ since both a and σ are local units. By reciprocity the value of the Hilbert symbol is the same at the two primes that are left. Hence, a is a norm locally everywhere iff $(a, \beta)_{D_F} = +1$. By the Hasse Norm Theorem we then have: a is a norm from E iff $(a, \beta)_{D_F} = +1$. By (7.4) we know that a unit of F is a norm from E iff it is the norm of a unit of E . This shows that whether all units of F are norms of units of E depends only on β . \square

(11.7) Remark: Let $E|F$ be a quadratic extension of number fields that both have property (*) and where exactly one odd prime of F ramifies in E . From (7.2) we know that $N_{E|F}(U_E^S)/(U_F^S)^2$ is a subgroup of index 2 of $U_F^S/(U_F^S)^2$ that does not contain τ . Since both E and F contain S -units with independent signs we have by (5.8) that $N_{E|F}(U_E^S)/(U_F^S)^2$, which is the image of n , maps surjectively onto $(\mathbb{Z}/2)^{r_1(F)}$ under φ . Hence the subgroup contains a set $\{u_1, \dots, u_{r_1(F)}\}$ of square classes of S -units of F of the following type: $\text{sign}[\sigma_i(u_j)] = +1$ for $j \neq i$ and $\text{sign}[\sigma_i(u_i)] = -1$ for all $i, j \in \{1, \dots, r_1(F)\}$. Here $\{\sigma_1, \dots, \sigma_{r_1(F)}\}$ denote the embeddings of F into \mathbb{R} . By (10.2) such a set $\{u_1, \dots, u_{r_1(F)}\}$ together with τ form a basis of the $\mathbb{Z}/2$ -vector space $U_F^S/(U_F^S)^2$. Hence a set of the above type already generates a subgroup of index 2 in $U_F^S/(U_F^S)^2$. \square

Let E be a quadratic extension of F that has property (*) and in which exactly one odd prime of F ramifies. We just stated that, by taking norms of S -units of E , E uniquely determines a subgroup of index 2 in $U_F^S/(U_F^S)^2$ that does not contain τ . The converse also holds:

(11.8) Proposition: Let F be a number field with property (*).

For any subgroup of index 2 of $U_F^S/(U_F^S)^2$ that does not contain τ there exist two infinite families of quadratic extensions of F with property (*) such that for any member E of the families we have: all classes in the given subgroup consist of norms from S -units of E .

Before we prove (11.8), note that this has the following consequences:

(11.9) Corollary: Let F be a number field with property (*) that contains units with independent signs. Among the $2^{r_1(F)+1}$ infinite families of quadratic extensions with property (*) there are exactly two that also contain units with independent signs. They correspond to the choice of $O_F^*/(O_F^*)^2$ as the subgroup of $U_F^S/(U_F^S)^2$ in (11.8). All other families do not contain units with independent signs.

Proof of (11.9): We use the fact that $O_F^*/(O_F^*)^2$ is a subgroup of $U_F^S/(U_F^S)^2$ of index 2. Since F contains units with independent signs we have from (5.5) that τ is not a square class of honest units of F , so $O_F^*/(O_F^*)^2$ does not contain τ . By (11.8) there are two infinite families such that for every member E we have: all classes in $O_F^*/(O_F^*)^2$ consist of norms from S -units of E . By (7.3) we know that a unit of F that is the norm of an S -unit of E is already the norm of a unit of E . Hence, all members E of the two infinite families have the property that all classes in $O_F^*/(O_F^*)^2$ consist of norms from (honest) units of E . By (5.10) we conclude that all these E contain units with independent signs. We also see that no member of any other family can contain units with independent signs. \square

Proof of (11.8): Every subgroup of index 2 of $U_F^S/(U_F^S)^2$ that does not contain τ must map surjectively to $(\mathbb{Z}/2)^2$ under φ , as defined in (5.7). Hence the subgroup contains, and is also generated by, a set $\{u_1, \dots, u_{r_1(F)}\}$ of square classes of S -units of F of the following type: $\text{sign}[\sigma_i(u_j)] = +1$ for $j \neq i$ and $\text{sign}[\sigma_i(u_i)] = -1$ for all $i, j \in \{1, \dots, r_1(F)\}$. We identify u_i with their images in $F_D^*/(F_D^*)^2$. From (10.2) we know that $\{u_1, \dots, u_{r_1(F)}, \tau\}$ form a basis of the $\mathbb{Z}/2$ -vector space $U_F^S/(U_F^S)^2$, so they are linearly independent in $F_D^*/(F_D^*)^2$. Consider the vector space isomorphism: $F_D^*/(F_D^*)^2 \cong \text{Hom}_{\mathbb{Z}/2}(F_D^*/(F_D^*)^2, \mathbb{Z}/2)$ that is given by mapping $\beta \in F_D^*/(F_D^*)^2$ to its the Hilbert symbol at the dyadic prime $(\cdot, \beta)_{D_F}$. This tells us that any given $\mathbb{Z}/2$ homomorphism f from $F_D^*/(F_D^*)^2$ to $\mathbb{Z}/2$ there exists exactly one $\beta \in F_D^*/(F_D^*)^2$ such that $\beta \equiv f$. If we prescribe values on the set $\{u_1, \dots, u_{r_1(F)}, \tau\}$, which is one element short of being a basis of $F_D^*/(F_D^*)^2$, then there are exactly two elements of $F_D^*/(F_D^*)^2$ that correspond to it. Let $f \in \text{Hom}_{\mathbb{Z}/2}(F_D^*/(F_D^*)^2, \mathbb{Z}/2)$ such that

$f(\tau) = -1$ and $f(u_i) = +1$ for all i . Let β be an element of $F_D^*/(F_D^*)^2$ such that $(\cdot, \beta)_{D_F} = f$. The other element of $F_D^*/(F_D^*)^2$ that corresponds to f is then $\tau\beta$. This follows from the bimultiplicativity of the Hilbert symbol and from the fact that $(v, \tau)_{D_F} = +1$ for all $v \in U_F^S/(U_F^S)^2$ which we saw in (10.2). Note that both β and $\tau\beta$ are in $F_D^*/(F_D^*)^2 - U_F^S/(U_F^S)^2$ since $(\tau, \beta)_{D_F} = (\tau, \tau\beta)_{D_F} = -1$, see (10.3). We take the two infinite families that correspond to β and $\tau\beta$. Let E be a member of one of these infinite families. We will now show that the square classes $\{u_1, \dots, u_{r_1(F)}\}$ consist of norms from E . E is of the form $F(\sqrt{\sigma})$ or $F(\sqrt{\tau\sigma})$ for some totally positive $\sigma \in F$ whose image in $F_D^*/(F_D^*)^2$ is β . Let us assume that $E = F(\sqrt{\sigma})$. The other case is completely analogous. Let u be a representative of any of the classes $\{u_1, \dots, u_{r_1(F)}\}$. As was explained in the proof of (11.6b), to check if u is a norm globally from $F(\sqrt{\sigma})$ over F is equivalent to checking if it is a norm locally from $F_D(\sqrt{\beta})$ over F_D . By the choice of β we have: $(u, \beta)_{D_F} = +1$ for all u . This shows that u is a norm from E . Hence, the square classes $\{u_1, \dots, u_{r_1(F)}\}$ consist of norms from E for every member of the families corresponding to β and $\tau\beta$. The above square classes generate the given subgroup of index 2, hence all classes in the given subgroup consist of norms from S -units of E for every member of the families corresponding to β and $\tau\beta$. \square

12. The main theorem

We now put together all the information we obtained in the previous sections to obtain a complete picture of the type of quadratic extensions with property (*) that exist for a given number field. The properties that such an extension can have, of course, depend on properties of F . We will therefore need many separate case discussions. Recall that property (*) is hereditary, so the given number field F must have property (*), or there are no such extensions.

(12.1) Theorem: Let F be a number field with property (*) of degree $r_1(F)$ and let τ be as defined in (5.4). The following is a complete list of all quadratic extensions of F that have property (*): There is exactly one extension in which no odd prime of F ramifies. It is given by $F(\sqrt{\tau})$. There are $2^{r_1(F)+1}$ infinite families of extensions [in the sense of (11.4)]. In all members of these families exactly one odd prime of F ramifies. Furthermore, the extensions have the following properties concerning the ramification of the dyadic prime D_F , the parity of the class number and the containment of units with independent signs:

A) If $h(F)$ is odd and if F contains units with independent signs:

The extension $F(\sqrt{\tau})$ has odd class number, it contains units with independent signs and D_F ramifies. There is one infinite family whose members have odd class number, contain units with independent signs and in which D_F is inert. There is one infinite family whose members have even class number [in fact $2 \parallel h(E)$], contain units with independent signs and in which D_F ramifies. The members of all other infinite families have odd class number, do not contain units with independent signs and D_F ramifies in these extensions.

B) If $h(F)$ is odd and if F does not contain units with independent signs:

All quadratic extensions with property (*) have odd class number, do not contain units with independent signs and D_F ramifies in these extensions.

C) If $h(F)$ is even and if F contains units with independent signs:

The extension $E = F(\sqrt{\tau})$ contains units with independent signs and D_F is inert. It is an unramified extension, so $h(E)$ is odd iff $2 \parallel h(F)$. There are two infinite families whose members contain units with independent signs. They have even class number, in fact $2 \parallel h(E|F)$, and D_F ramifies. The members of all other infinite families do not contain units with independent signs. They also have even class number, but here the relative class number is odd, and D_F ramifies.

D) If $h(F)$ is even and if F does not contain units with independent signs:

The extension $E = F(\sqrt{\tau})$ does not contain units with independent signs and D_F is inert. It is an unramified extension, so $h(E)$ is odd iff $2 \parallel h(F)$. The members of all $2^{r_1(F)+1}$ infinite families have even class number [in fact the relative class number is odd], they do not contain units with independent signs and D_F ramifies.

(12.2) Remark: In the first chapter we were looking for a number field with property (*) that has even class number and does not contain units with independent signs. Such a number field does not exist among quadratic extensions of a number field of type A) [using the notation of the main theorem]. Since \mathbb{Q} is of type A), we see again, that it does not have a quadratic extension of the required kind. If we are looking for an example among quadratic extensions of a quadratic number field we see that the quadratic number field must be of type C). This is indeed the case in our example from section 4. The main theorem tells us that for **every** number field of type C) there exist quadratic extensions with property (*), even class number and units with independent signs. Examples will be given in section 15.

We now list some corollaries that illustrate the implications of the main theorem.

(12.3) Corollary: For any natural number n there exists a number field F of degree 2^n with property (*) and $2^n \parallel h(F)$.

Proof: With the notation of the main theorem \mathbb{Q} is of type A). For the case $n = 1$ we take any member of the one infinite family that contains units with independent signs and where 2 is the exact 2-power dividing the class number. Such a number field is of type C). For $n \geq 2$ we take successive quadratic extensions of the above number field. These extensions are always chosen from the two families that contain units with independent signs. Each time we take such an extension the exact 2-power dividing the number field rises by 1. \square

(12.4) Corollary: If F is a number field with property (*) that is built from successive quadratic extensions of $\mathbb{Q}(\sqrt{p})$ or $\mathbb{Q}(\sqrt{2p})$ then the class number of F is odd.

Proof: Note that $\mathbb{Q}(\sqrt{p})$ or $\mathbb{Q}(\sqrt{2p})$ are of type B) in the main theorem, see (2.5) or (13.1). \square

Before we can completely prove the main theorem (12.1), here is one more important observation: In (11.6.a) we saw that the dyadic prime D_F will either ramify in all members of an infinite family or in none. We will now see how this behavior of D_F is determined by the $\beta \in F_D^*/(F_D^*)^2$ that is related to the family. For all families

the related β is contained in $F_D^*/(F_D^*)^2 - U_F^S/(U_F^S)^2$, but the following proposition also applies to the case $F(\sqrt{\tau})$. We therefore do not restrict β in the following proposition, so it includes the case $\beta = \tau$.

(12.5) Proposition: Let F be a number field with exactly one dyadic prime D_F . Let F_D denote the completion of F at D_F . Let σ be an element of F such that $L := F_D(\sqrt{\beta})$ is a proper extension of F_D ; where we denote the image of σ in $F_D^*/(F_D^*)^2$ by β .

a) The classes in $F_D^*/(F_D^*)^2$ that contain units of F_D form a subgroup of index 2.

b) (Local norm index theorem)

The classes in $F_D^*/(F_D^*)^2$ that consist of norms from L form a subgroup of index 2.

c) Let $E := F(\sqrt{\sigma})$, then D_F does **not** ramify in $E|F$ iff in $F_D^*/(F_D^*)^2$ we have: the subgroup of norms coincides with the subgroup of classes containing local units.

Proof: Let O_D denote the ring of integers of F_D . In O_D the ideal D_F is principal, a generator is called a uniformizer. The classes of $F_D^*/(F_D^*)^2$ are all generated by elements of the form u and $u\pi$, where u denotes a unit of F_D and π denotes a uniformizer. The class of u is distinct from $u\pi$, so exactly half of the classes contain local units. This proves a).

b) We are assuming that L is a proper quadratic extension of F_D , i.e., the degree of the extension $L|F_D$ is 2. From local class field theory, see for example [La], we have $\#F_D^*/N_{L|F_D}(L^*) = \text{degree of the extension} = 2$. Hence, half of all elements of F_D^* are norms from L . Note that squares of F_D are always norms from L over F_D , so taking square classes we see that exactly half of all classes consist of norms.

c) To check if D_F ramifies in $E|F$ we only need to consider this locally. What is the ramification index of L over F_D ? By the local norm index theorem, see for example [La], we have that the ramification index is given by the number of elements in $O_D^*/N_{L|F_D}(O_L^*)$. For local extensions we have: if a unit of F_D is a norm from L , then it is the norm of a unit of L . Hence, $N_{L|F_D}(O_L^*) = N_{L|F_D}(L^*) \cap O_D^*$. This shows that the ramification index of L over F_D is 1 if all local units of F_D are norms from L and it is 2 otherwise. Hence, the ramification index is 1 iff the classes of norms coincide with those that contain local units. That the ramification index locally is

1 means exactly that D_F is not ramified in $E|F$. □

Remark: In the proof of (12.1) we will apply (12.5) to the cases where $\beta = \tau$ or $\beta \in F_D^*/(F_D^*)^2 - U_F^S/(U_F^S)^2$. In either case the condition that $L := F_D(\sqrt{\beta})$ is a proper extension is satisfied.

Proof of (12.1):

That $F(\sqrt{\tau})$ and the members of the $2^{r_1(F)+1}$ infinite families corresponding to the elements of $F_D^*/(F_D^*)^2 - U_F^S/(U_F^S)^2$ are in fact the only extensions of F with property (*) was explained in (8.2) and (11.5).

We will first examine the extension $E = F(\sqrt{\tau})$:

By (9.1.2) we have: E contains units with independent signs iff F contains units with independent signs. We have to show that if $h(F)$ is odd then D_F ramifies in $E|F$ and if $h(F)$ is even then D_F does not ramify, so it is inert. The claim on the parity of $h(E)$ will then follow by (9.1.2).

For $E = F(\sqrt{\tau})$ all S -units of F are norms from E by (7.2.1). Considering $U_F^S/(U_F^S)^2$ as a subset of $F_D^*/(F_D^*)^2$ we can say that the square classes of $U_F^S/(U_F^S)^2$ are exactly those that consist of norms. We want to apply the criterion from (12.5c). We know that the subgroup of norms (global and therefore also local) is $U_F^S/(U_F^S)^2$. We will now examine whether this subgroup coincides with the subgroup of square classes that contain local units.

If $h(F)$ is even we claim that the two groups coincide. For this we must show that the image of an S -unit of F in $F_D^*/(F_D^*)^2$ is the class of a local unit. This can be seen as follows: $h(F)$ is even but $h^S(F)$ is odd, so the dyadic prime D_F has even order in the ideal class group of F . Let u be any S -unit of F . Then $u \cdot \mathcal{O}_F = D_F^m$ for some even $m \in \mathbb{Z}$. Let π be the uniformizer of D_F in F_D . In F_D we have $u = \pi^m v$ for some local unit v . The square class of u therefore contains the local unit v . This shows that in F_D the subgroup of norms is contained in the subgroup containing local units. Both groups have index 2, so they are equal. Hence, if $h(F)$ is even then the classes of norms coincide with the classes that contain units. We conclude by (12.5c) that D_F does not ramify.

If $h(F)$ is odd, then D_F has odd order n . We have $D_F^n = u \cdot \mathcal{O}_F$ for some S -unit u

of F . Locally, in F_D , we obtain $u = \pi^n v$ for some local unit v . Modulo squares this leaves: $u = \pi v$. Hence, the square class of u does not contain a local unit. It does, however, consist of norms, since we pointed out above that all classes of S-units consist of norms. Hence, if $h(F)$ is odd, the subgroup of norms does not coincide with the subgroup of square classes that contain units. By (12.5c) we conclude that D_F ramifies in $E|F$. This completes the discussion of the case $E = F(\sqrt{\tau})$.

We now turn to those extensions of F where exactly one odd prime of F ramifies. Recall that here we have $\tau \notin N_{E|F}(E^*)$. Furthermore, we showed in the proof of (8.2) that τ is not a local norm from $L = F_D(\sqrt{\beta})$ over F_D . As before, we will consider $O_F^*/(O_F^*)^2$ as a subset of $U_F^S/(U_F^S)^2$. By (5.5) we know that if F does not contain units with independent signs then $\tau \in O_F^*/(O_F^*)^2$.

For each type of F we now examine the $2^{r_1(F)+1}$ families.

Cases B) and D): If F does not contain units with independent signs, then E does not contain units with independent signs for any member E of any of the $2^{r_1(F)+1}$ families. This is clear, because otherwise the norms of S-units of E would give S-units with independent signs in F , see (5.8). F does not contain units with independent signs, so $\tau \in O_F^*/(O_F^*)^2$. Since every global unit is also a local unit we see that in $F_D^*/(F_D^*)^2$ the class of τ is a class containing a local unit. But τ is not a local norm, by (8.8), so this square class does not contain any norms. Therefore, the classes of norms do not coincide with those containing local units. By (12.5c) we conclude that D_F ramifies in $E|F$. From (9.1.1) we obtain that $h(E|F)$ is odd for these cases, so the parity of $h(E)$ is the same as the parity of $h(F)$.

Cases A) and C): If F contains units with independent signs, then from (11.9) we know that there exist exactly two infinite families whose members all contain units with independent signs. The members of all the other infinite families do not contain units with independent signs. We now need to separate the cases where $h(F)$ is even/odd:

C) If $h(F)$ is even and if F contains units with independent signs:

We show that in this case the subgroup of norms in $F_D^*/(F_D^*)^2$ does not coincide with the subgroup of square classes containing local units. An example of a square class that does not consist of norms but that does contain a local unit is: τ . For the S-unit τ we have $\tau \cdot O_F = D_F^m$ for some $m \in \mathbb{Z}$ where the order of D_F divides m .

This order is even because $h(F)$ is even but $h(S(F))$ is odd. Hence, $\tau \cdot O_F$ is an even power of D_F . Let π be a uniformizer in F_D , then $\tau = \pi^m v$ for some local unit $v \in F_D$. Modulo squares we obtain that the class of τ equals the class of the local unit v . By (8.8) τ is not a local norm, so in $F_D^*/(F_D^*)^2$ the classes of norms do not coincide with those containing units. By (12.5c) we obtain that D_F ramifies in $E|F$ for any member E of any of the $2^{r_1(F)+1}$ infinite families. Since all members of the infinite families are ramified extensions of F we know that $h(F)$ divides $h(E)$, so $h(E)$ is even. By (9.1.1) we see furthermore that $2||h(E|F)$ if E contains units with independent signs, which is the case for two infinite families, and $h(E|F)$ is odd if E does not contain units with independent signs.

A) If $h(F)$ is odd and if F contains units with independent signs:

Case A_1 : Let E be a member of any of the families whose members do not contain units with independent signs. Since F contains units with independent signs but E does not, we have by (5.10) that not all units of F are norms of units of E . Let u be a unit of F that is not a norm from a unit of E . By the same argument as in the proof of (11.6b) we see that u can not be the norm of any element of E . Since u is not a norm globally it must be a “not norm” also locally for some prime of F . We let $E = F(\sqrt{\sigma})$ and check the Hilbert symbol of σ and u at all primes. For infinite primes it is $+1$ since σ is totally positive. For any prime distinct from D_F and the one odd prime that ramifies in E the Hilbert symbol is also $+1$ since both σ and u are local units. Hence, u is a norm locally for all of the above primes. So the only primes where u can be a “not norm” are D_F and the odd ramified prime. By reciprocity u is a norm locally either in none or in both. We conclude: the image of u in F_D is not a norm from $F_D(\sqrt{\sigma})$ over F_D . But the global unit u is a local unit in F_D . We obtain that the classes of norms in $F_D^*/(F_D^*)^2$ do not coincide with the classes containing local units. By (12.5c) we see that D_F ramifies in $E|F$. From (9.1.1) we then have that $h(E|F)$ is odd, so $h(E)$ is odd.

Case A_2 : We now consider the two infinite families whose members contain units with independent signs. By (11.9) they both belong to the choice of square classes of honest units as classes that are norms from E over F . In the proof of (11.8) we saw that if one of the families corresponds to $\beta \in F_D^*/(F_D^*)^2$, in the sense of (11.4), then the other corresponds to $\tau\beta \in F_D^*/(F_D^*)^2$.

We claim that either the class of β or the class of $\tau\beta$ in $F_D^*/(F_D^*)^2$ is the class of a local unit. This can be seen as follows: From (5.5) we have $\tau \notin O_F^*/(O_F^*)^2$ because F contains units with independent signs. Let $\tau \cdot O_F = D_F^m$ for some $m \in \mathbb{Z}$. The order of D_F is odd in the class group of F and it divides m . This m can not be even because if $m = 2n$ for some $n \in \mathbb{Z}$ then the order of D_F divides n and we have: $\tau \cdot O_F = (D_F)^{2n} = (D_F^n)^2$. The ideal D_F^n is principal, call its generator x . Then $\tau = x^2 u$ for some $u \in O_F$. Hence, the class of τ in $U_F^S/(U_F^S)^2$ is contained in the subgroup $O_F^*/(O_F^*)^2$. This is a contradiction. We conclude that $\tau \cdot O_F = D_F^m$ for some **odd** integer m . If we let π denote a uniformizer of D_F in F_D , then $\tau = \pi^m v$ for some local unit v . Hence, the power to which the uniformizer appears in β and $\tau\beta$ is distinct modulo 2. This shows that either the class of β or the class of $\tau\beta$ in $F_D^*/(F_D^*)^2$ is the class of a local unit.

Note that for square classes we have: $\beta = \tau^2\beta = \tau(\tau\beta)$. Therefore we can assume without loss of generality that the class of β is the class of a local unit. This is done by replacing β by $\tau\beta$ if necessary.

Let $E_1 = F(\sqrt{\sigma})$ and $E_2 = F(\sqrt{\tau\sigma})$ be representatives of the two families that we are examining. Note that σ is a totally positive element of F whose image in F_D is β . Let $L_1 = F_D(\sqrt{\beta})$ and $L_2 = F_D(\sqrt{\tau\beta})$.

We claim that β is a norm from L_1 over F_D but not from L_2 over F_D .

To check that β is not a norm from $L_1 = F_D(\sqrt{\beta})$ we need to show: $(\beta, \beta)_{D_F} = +1$. We first note that by (5.10) all units of F are norms from E_1 , hence also $-1 \in N_{E_1|F}(E_1)$. In particular, -1 is a norm locally at all primes of F . So, -1 is a norm from L_1 over F_D . Note that $-\beta$ is the norm of $\sqrt{\beta}$, so it is a norm from L_1 over F_D . In terms of Hilbert symbols this means: $(\beta, -1)_{D_F} = +1$ and $(\beta, -\beta)_{D_F} = +1$. The product of these gives: $(\beta, \beta)_{D_F} = +1$. This shows that β is a norm from L_1 over F_D . Furthermore, we have $(\beta, \tau) = -1$. This is true because $\beta \in F_D^*/(F_D^*)^2 = U_F^S/(U_F^S)^2$, as we saw in the proof of (.). This gives $(\beta, \tau\beta)_{D_F} = -1$, so β is not a norm from L_2 over F_D .

We have now shown that β is a class containing a local unit in $F_D^*/(F_D^*)^2$, but it does not consist of norms from L_2 . By (12.5c) we conclude that D_F ramifies in $E_2|F$. For any member of the infinite family that is represented by E_2 we now know that D_F ramifies and by (9.1.1) we have that 2 is the exact 2-power dividing the relative

class number.

To examine the behavior of D_F in E_1 we proceed as follows:

Consider the classes of $F_D^*/(F_D^*)^2$. Which of these are classes of local units? We saw above that the class of β is the class of a local unit. Also, the classes of global units $u \in O_F$ are classes of local units. The subgroup $O_F^*/(O_F^*)^2$ has index 4 in $F_D^*/(F_D^*)^2$ and $\beta \notin O_F^*/(O_F^*)^2$. This shows that the subgroup of $F_D^*/(F_D^*)^2$ generated by $O_F^*/(O_F^*)^2$ and β has index 2, so it is the complete subgroup of square classes that contains local norms. We claim that these classes are classes of norms from L_1 over F_D . This holds because we just checked that β is a norm from L_1 over F_D . We also know that all units of F are norms from E_1 over F , so their images in F_D are all norms from L_1 . Since both subgroups have the same order, this shows that in $F_D^*/(F_D^*)^2$ the classes of norms coincide with the classes that contain local units. By (12.5c) we conclude that D_F is not ramified in $E_1|F$. It must therefore be inert. For any member of the infinite family that is represented by E_1 we now know that D_F is inert and by (9.1.1) we have that the relative class number is odd.

This concludes the proof of (12.1)

□

CHAPTER 4

Examples

Let F be a number field, let $r_1(F)$ denote the number of real embeddings of F and let S be the set consisting of all infinite and all dyadic primes of F . Recall that for a number field F to have property (*), means that F is totally real, it has exactly one dyadic prime, it contains S -units with independent signs and its S -class number is odd. An equivalent formulation of property (*) is: F is totally real and $2\text{-prim}K_2(F)$ is elementary abelian of rank $r_1(F)$.

We have shown that for a given number field F with property (*) there exist exactly $2^{r_1(F)+1}$ infinite families of quadratic extensions with property (*). Each member E of such a family has the property that exactly one odd prime of F ramifies in $E|F$. Besides these, there exists one more quadratic extension of F with property (*). It is given by $F(\sqrt{\tau})$, where τ denotes the nontrivial square class of totally positive S -units of F , see (5.4).

We will now illustrate how to apply our results to actually determine quadratic extensions with property (*) of a given number field F . The easiest case is $F = \mathbb{Q}$. In section 13 we will show how our methods can be used to determine all quadratic extensions of \mathbb{Q} with property (*). Note that in section 2 we already listed all quadratic number fields where $2\text{-prim}K_2(O_F)$ is of rank $r_1(F) = 1$. By applying our results about quadratic extensions with property (*), we again obtain the real number fields among these.

In section 14 we consider the biquadratic dicyclic number fields from section 3. We will see that the number fields $\mathbb{Q}(\sqrt{2}, \sqrt{p})$ with $p \equiv \pm 3 \pmod{8}$ have property (*).

In section 4 we saw that $\mathbb{Q}(\sqrt{10+\sqrt{10}})$ is a number field with property (*), that has even class number and that does not contain units with independent signs. From our main theorem we know that there exist many number fields that all share the same properties. Section 15 will explicitly list an infinite number of these. The example from section 4 will be a special case.

In section 16 we give one explicit example for each of the 8 infinite families of quadratic extensions with property (*) of $\mathbb{Q}(\sqrt{10})$.

13. Application to $F = \mathbb{Q}$

The number field $F = \mathbb{Q}$ has property (*) since it is totally real, it has exactly one dyadic prime: $D_F = (2)$, it has odd class number: $h(\mathbb{Q}) = 1$, and it contains units with independent signs: ± 1 . Furthermore, we have $r_1(F) = 1$ and $\tau = 2$.

We will now recall our general results and apply them to $F = \mathbb{Q}$.

Recall: For a number field F with property (*) we have the inclusions:

$$O_F^*/(O_F^*)^2 \longrightarrow U_F^S/(U_F^S)^2 \longrightarrow F_D^*/(F_D^*)^2$$

If $r_1(F)$ denotes the degree of F , then the above groups have order $2^{r_1(F)}$, $2^{r_1(F)+1}$ and $2^{r_1(F)+2}$, respectively. See: (5.1)(10.1)(5.3). To determine $F_D^*/(F_D^*)^2$ we recall that $F_D^*/(F_D^*)^2$ is a $\mathbb{Z}/2$ -vector space of one more dimension than $U_F^S/(U_F^S)^2$. By (10.3) we know that to obtain an element β which together with $U_F^S/(U_F^S)^2$ generates $F_D^*/(F_D^*)^2$ we need β such that $(\tau, \beta)_{D_F} = -1$.

Claim: For $F = \mathbb{Q}$ an element β , as above, is given by $\beta = 5$.

Proof: Since $(\tau, 5)_{D_F}$, we must check: $(2, 5)_2 = -1$.

We have $(2, 5)_p = +1$ for the infinite prime of \mathbb{Q} since 2 and 5 are positive. Furthermore, $(2, 5)_p = +1$ for all finite primes $p \neq 2, 5$ since both 2 and 5 are local units at p . By reciprocity we have $(2, 5)_2 = (2, 5)_5$. This equals the Legendre symbol $\left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1$. \square

For $F = \mathbb{Q}$ we have $O_F^*/(O_F^*)^2 = \{1, -1\}$ and $U_F^S/(U_F^S)^2 = \{1, -1, 2, -2\}$, hence

$$F_D^*/(F_D^*)^2 = \{1, -1, 2, -2, 5, -5, 2 \cdot 5, -2 \cdot 5\}$$

Note that $3 \equiv -5 \pmod{8}$ and -5 is invertible mod 8, so $\frac{3}{-5} \equiv 1 \pmod{8}$. By Hensel's lemma we know that such an element is a square in \mathbb{Q}_2 , so $3 = -5$ in $F_D^*/(F_D^*)^2$.

We therefore have:

$$F_D^*/(F_D^*)^2 = \{1, -1, 2, -2, 5, 3, 2 \cdot 5, 2 \cdot 3\}$$

Recall: For a number field F with property (*) we proved in (11.2) and (11.3) that there is a one-to-one correspondence between the $2^{r_1(F)+1}$ elements $\beta \in F_D^*/(F_D^*)^2 - U_F^S/(U_F^S)^2$ and the infinite families of quadratic extensions E of F with property (*). The correspondence is given by: the members of the family corresponding to β are of the form $E = F(\sqrt{\sigma})$ where $\sigma \in F^*/(F^*)^2$ is an element that maps to $\beta \in F_D^*/(F_D^*)^2$, it is totally positive and it has only one odd prime in its prime ideal decomposition.

For $F = \mathbb{Q}$ there are $2^{r_1(F)+1} = 4$ infinite families of quadratic extensions of F with property (*). They correspond to the elements $\{5, 3, 10, 6\} \in F_D^*/(F_D^*)^2 - U_F^S/(U_F^S)^2$.

We now explicitly determine the members of the families:

We need totally positive elements $\sigma \in F^*/(F^*)^2$ that contain exactly one odd prime to an odd power and that map to $5, 3, 10, 6 \in F_D^*/(F_D^*)^2$, respectively. Since we need σ only modulo squares this means that either $\sigma = p$ or $\sigma = 2p$ for some prime p . Since all elements of \mathbb{Q} that are congruent to 1 mod 8 are in \mathbb{Q}_2^2 we have:

The members of the infinite families corresponding to 5 and $2 \cdot 5 \in F_D^*/(F_D^*)^2$ are $E = F(\sqrt{p})$ and $E = F(\sqrt{2p})$ for $p \equiv 5 \pmod{8}$.

The members of the infinite families corresponding to 3 and $2 \cdot 3 \in F_D^*/(F_D^*)^2$ are $E = F(\sqrt{p})$ and $E = F(\sqrt{2p})$ for $p \equiv 3 \pmod{8}$.

Recall: For a number field F with property (*), let $\sigma_1, \dots, \sigma_{r_1(F)}$ denote the (real) embeddings of F . We have shown in (11.7) and (11.8) that there is a one-to-one correspondence between pairs $\beta, \tau\beta \in F_D^*/(F_D^*)^2 - U_F^S/(U_F^S)^2$ and subgroups of index 2 of $U_F^S/(U_F^S)^2$ that do not contain τ . This correspondence is given by $(\beta, u)_{D_F} = (\tau\beta, u)_{D_F} = +1$ for all u in the subgroup. The subgroup is also uniquely determined as those square classes of S -units of F that are norms from E over F for all E in the families associated to β and $\tau\beta$.

For $F = \mathbb{Q}$ the subgroups of index 2 of $U_F^S/(U_F^S)^2$ that do not contain 2 are: $\{1, -1\}$ and $\{1, -2\}$. Note that 1 is always a norm. We have to check which one of -1

or -2 is a norm from members of each of the 4 families. For $\beta = 5$ we have: $(-1, \beta)_{D_F} = (-1, 5)_2 = +1$. This holds because $1x^2 + 5y^2 = 1$ has a solution: $x = 2, y = 1$.

Hence, for any member E of the family corresponding to $5 \in F_D^*/(F_D^*)^2$ we know that -1 is a norm from E over F . Since there is also a one-to-one correspondence between pairs of families and sets of S -units that are norms, we conclude that -1 is a norm for any member E of the families corresponding to 5 and $2 \cdot 5$. These E contain units with independent signs. For the members E of the families corresponding to 3 and $2 \cdot 3$, we must then have that -2 is a norm from E over F . These E do not contain units with independent signs.

Recall: The main theorem (12.1) classifies the quadratic extensions with property (*) of a given number field F with respect to their properties concerning the class number, units with independent signs and whether the dyadic prime of F ramifies.

We know that $\mathbb{Q}_2(\sqrt{5})$ is the unramified extension of \mathbb{Q}_2 , so in any member of the family corresponding to $\beta = 5$ the dyadic prime will be inert.

With the notation as in our main theorem we have: $F = \mathbb{Q}$ is of type A), i.e., $h(F)$ is odd and F contains units with independent signs. We conclude:

(13.1) Proposition: The $2^{r_1(F)+1} = 2^2$ infinite families of quadratic extensions with property (*) of $F = \mathbb{Q}$ classify by:

A) There is exactly one family whose members have odd class number, contain units with independent signs and in which D_F is inert. This family is the one corresponding to $\beta = 5$, namely: $\mathbb{Q}(\sqrt{p})$ with $p \equiv 5 \pmod{8}$.

B) There are $2^2 - 2 = 2$ families whose members have odd class number, do not contain units with independent signs and in which D_F ramifies. They are the ones corresponding to $\beta = 3$ and 6 , namely: $\mathbb{Q}(\sqrt{p})$ and $\mathbb{Q}(\sqrt{2p})$ with $p \equiv 3 \pmod{8}$.

C) There is exactly one family whose members have even class number, in fact $2 \mid h(E)$, contain units with independent signs and in which D_F ramifies. This family is the one corresponding to $\beta = 10$, namely $\mathbb{Q}(\sqrt{2p})$ with $p \equiv 5 \pmod{8}$.

Furthermore, the one quadratic extension with property (*) of \mathbb{Q} in which no odd prime ramifies is given by $\mathbb{Q}(\sqrt{\tau}) = \mathbb{Q}(\sqrt{2})$. It contains units with independent signs and has odd class number. \square

All of these results agree with the facts stated in section 2.

14. Biquadratic dicyclic number fields with property (*)

Recall that in section 3 we saw that the number fields $E = \mathbb{Q}(\sqrt{2}, \sqrt{p})$ with $p \equiv \pm 3 \pmod{8}$ were the only candidates among biquadratic dicyclic number fields that could have elementary abelian 2-prim $K_2(O_F)$ of rank $r_1(F)$. At that time we were not interested in whether or not they actually do have this property, because we were looking for an example with even class number. Note, that these number fields are totally real, so to ask whether they have elementary abelian 2-prim $K_2(O_F)$ of rank $r_1(F) = 4$ is equivalent to asking whether they have property (*).

(14.1) Theorem: The biquadratic dicyclic number fields that have property (*) are given by $\mathbb{Q}(\sqrt{2}, \sqrt{p})$ where p is a prime with $p \equiv \pm 3 \pmod{8}$.

Furthermore, the number fields $\mathbb{Q}(\sqrt{2}, \sqrt{p})$ with $p \equiv +3 \pmod{8}$ have odd class number and do not contain units with independent signs.

The number fields $\mathbb{Q}(\sqrt{2}, \sqrt{p})$ with $p \equiv 5 \pmod{8}$ also have odd class number but they contain units with independent signs.

Proof: We examine the quadratic fields $F = \mathbb{Q}(\sqrt{p})$ where p is a prime with $p \equiv \pm 3 \pmod{5}$. In the previous section we showed that these number fields have property (*). We have $\mathbb{Q}(\sqrt{2}, \sqrt{p}) = F(\sqrt{2})$. We claim $F(\sqrt{\tau}) = F(\sqrt{2})$, the one quadratic extension of F with property (*) in which no odd prime ramifies. By definition, τ is any representative of the non trivial square class of totally positive S -units of F . To show that 2 is a representative of the class of τ , we must show that 2 is a totally

positive S-unit of F that is not a square.

This can be seen as follows: $2 \in \mathbb{Q}(\sqrt{p})$ is certainly a totally positive S-unit. Assume that 2 is a square, i.e., there exist $a, b \in \mathbb{Q}$ such that $2 = (a + b\sqrt{p})^2$. We have $2 = a^2 + b^2p + 2ab\sqrt{p}$, so $2 = a^2 + b^2p$ and $2ab = 0$. Hence, either $a = 0$ or $b = 0$, so either $2 = b^2p$ or $2 = a^2$. Both of these are impossible for an odd prime p and $a, b \in \mathbb{Q}$. Therefore 2 is not a square, hence $F(\sqrt{\tau}) = F(\sqrt{2})$.

We conclude that $\mathbb{Q}(\sqrt{2}, \sqrt{p})$ has property (*) for any prime $p \equiv \pm 3 \pmod{8}$. From the main theorem we also know that $h(E)$ is odd and E contains units with independent signs iff F contains units with independent signs. \square

15. The fields $\mathbb{Q}(\sqrt{\varepsilon\sqrt{2q}})$ with $q \equiv 5 \pmod{8}$

(15.1) Theorem: For any prime q with $q \equiv 5 \pmod{8}$, let ε denote a positive fundamental unit of $\mathbb{Q}(\sqrt{2q})$. The number fields $\mathbb{Q}(\sqrt{\varepsilon\sqrt{2q}})$ and $\mathbb{Q}(\sqrt{2\varepsilon\sqrt{2q}})$ have property (*). Furthermore, they are biquadratic cyclic, they have even class number, in fact 2 is the exact 2-power dividing the class number, and they do not contain units with independent signs.

(15.2) Remark: This gives infinitely many examples for the type of number field that we were looking for in chapter 1. The example from section 4 is included in the above, by taking $q = 5$ in $\mathbb{Q}(\sqrt{2\varepsilon\sqrt{2q}})$.

Proof: For $\mathbb{Q}(\sqrt{10})$ we have $\varepsilon = 3 + \sqrt{10}$.

$$2\varepsilon\sqrt{10} = 2(3 + \sqrt{10})\sqrt{10} = 2(10 + 3\sqrt{10}) = \left[\frac{2+\sqrt{10}}{3}\right]^2(10 + \sqrt{10})$$

This shows that $2\varepsilon\sqrt{10}$ and $10 + \sqrt{10}$ are in the same square class of F , hence adjoining their square root results in the same field. \square

Proof of (15.1): Let $F = \mathbb{Q}(\sqrt{2q})$ where q is a prime with $q \equiv 5 \pmod{8}$.

In (13.1.C) we showed that these number fields have property (*). Furthermore, we showed that $2||h(F)$ and F contains units with independent signs.

By a positive fundamental unit ε we mean a fundamental unit of F whose image in \mathbb{R} is positive under the embedding of F that takes $\sqrt{2q}$ to $\sqrt{2q}$. Since F contains units with independent signs, we have that $N_{F|\mathbb{Q}}(\varepsilon) = -1$, so the image of ε in \mathbb{R} is negative under the embedding that takes $\sqrt{2q}$ to $-\sqrt{2q}$.

We have $r_1(F) = 2$ and the ring of integers is $O_F = \mathbb{Z}[\sqrt{2q}]$.

The rational primes that ramify in F are 2 and q . We have $2 \cdot O_F = (\sqrt{2q}, 2)^2$ and $q \cdot O_F = (\sqrt{2q}, q)^2$. The dyadic prime of F is $D_F = (\sqrt{2q}, 2)$ and let $Q = (\sqrt{2q}, q)$. Note that $\sqrt{2q} \cdot O_F = Q \cdot D_F$. We know that 2 is a totally positive S-unit of F that is not a square since $2 = (a + b\sqrt{q})^2$ has no solution $a, b \in \mathbb{Q}$. Therefore we can take $\tau = 2$.

We have $O_F^*/(O_F^*)^2 = \{\pm 1, \pm \varepsilon\}$ and $U_F^S/(U_F^S)^2 = \{\pm 1, \pm \varepsilon, \pm 2, \pm 2\varepsilon\}$.

Consider the element $\varepsilon\sqrt{2q} \in F$. It is totally positive (by choice of ε) and the prime ideal decomposition of the principal ideal it generates is $\varepsilon\sqrt{2q} \cdot O_F = Q \cdot D_F$. It contains exactly one odd prime, namely Q , to an odd power. We would like to conclude that $F(\sqrt{\varepsilon\sqrt{2q}})$ has property (*). By the criterion in (8.7) we need to check that $\tau = 2$ is not a square in the residue field O_Q/Q .

The ramification index of F_Q over \mathbb{Q}_q is 2, so the inertia degree is $f = 1$. We have $\#O_Q/Q = q^f = q$, hence $O_Q/Q \cong \mathbb{Z}/q$. To check that 2 is not a square in \mathbb{Z}/q we use the Legendre symbol:

$$\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}} = -1 \quad \text{since } q \equiv 5 \pmod{8}$$

From (8.7) we obtain that both $F(\sqrt{\varepsilon\sqrt{2q}})$ and $F(\sqrt{2\varepsilon\sqrt{2q}})$ have property (*).

So far we have shown:

For any prime q with $q \equiv 5 \pmod{8}$, the number fields $\mathbb{Q}(\sqrt{\varepsilon\sqrt{2q}})$ and $\mathbb{Q}(\sqrt{2\varepsilon\sqrt{2q}})$ have property (*).

That they are biquadratic cyclic is checked by using the criterion from (3.1):

$$2q \cdot N(\varepsilon\sqrt{2q}) = 2q(-1)(-2q) = (2q)^2.$$

Let $F = \mathbb{Q}(\sqrt{2q})$ for any prime $q \equiv 5 \pmod{8}$. The two quadratic extensions $F(\sqrt{\varepsilon\sqrt{2q}})$ and $F(\sqrt{2\varepsilon\sqrt{2q}})$ are members of the two infinite families with property (*) that correspond to $\beta = \varepsilon\sqrt{2q}$ and $\tau\beta = 2\varepsilon\sqrt{2q}$. Since F is of type C) in our

main theorem, we know that both quadratic extensions have even class number. We do not know if they belong to the two families whose members contain units with independent signs. By (11.9) we must check if the subgroup $O_F^*/(O_F^*)^2$ of $U_F^S/(U_F^S)^2$ consists of norms from S-units of the extensions $F(\sqrt{\varepsilon\sqrt{2q}})$ or $F(\sqrt{2\varepsilon\sqrt{2q}})$.

Note: we do know that the set of square classes of S-units of F that are norms from either extension is the same.

By computing Hilbert symbols we will now check that $\pm\varepsilon$ are not norms locally at D_F . It follows that they cannot be global norms.

In (15.3) below, we will show:

$$(\varepsilon, -\varepsilon)_{D_F} = +1, \quad (\varepsilon, \varepsilon)_{D_F} = -1, \quad (\sqrt{2q}, -1)_{D_F} = -1 \quad \text{and} \quad (\sqrt{2q}, \varepsilon)_{D_F} = +1.$$

Using this we can now check that $\pm\varepsilon$ are not local norms at D_F :

$$(\varepsilon\sqrt{2q}, \varepsilon)_{D_F} = (\varepsilon, \varepsilon)_{D_F}(\sqrt{2q}, \varepsilon)_{D_F} = (+1)(-1) = -1$$

$$(\varepsilon\sqrt{2q}, -\varepsilon)_{D_F} = (\varepsilon, -\varepsilon)_{D_F}(\sqrt{2q}, -1)_{D_F}(\sqrt{2q}, \varepsilon)_{D_F} = (+1)(-1)(+1) = -1$$

We conclude that $F(\sqrt{\varepsilon\sqrt{2q}})$ and $F(\sqrt{2\varepsilon\sqrt{2q}})$ do not contain units with independent signs. This concludes the proof of (15.1) \square

(15.3) Proposition: $(\varepsilon, -\varepsilon)_{D_F} = +1, \quad (\varepsilon, \varepsilon)_{D_F} = -1, \quad (\sqrt{2q}, -1)_{D_F} = -1$
and $(\sqrt{2q}, \varepsilon)_{D_F} = +1.$

Proof: $(\varepsilon, -\varepsilon)_{D_F} = +1$, by properties of the Hilbert symbol.

$(\varepsilon, \varepsilon)_{D_F} = -1$, since the Hilbert symbol is $+1$ at all other primes except for one infinite prime.

$(\sqrt{2q}, -1)_{D_F} = -1$ can be seen as follows: We have $q \equiv 5 \pmod{8}$, so $(\frac{-1}{q}) = +1$, i.e. -1 is a square in $O_Q/Q = \mathbb{Z}/q$. From this it follows that $(\sqrt{2q}, -1)_Q = +1$. The Hilbert symbol of $\sqrt{2q}$ and -1 has the following values: It is $+1$ at all finite primes distinct from Q and D_F since both elements are local units there. The Hilbert symbol is negative at the infinite prime under which $\sqrt{2q}$ is negative and positive at the other. By reciprocity we conclude that it is -1 at D_F .

To show that $(\sqrt{2q}, \varepsilon)_{D_F} = +1$ we again consider the Hilbert symbol at all other primes. It is positive in one and negative in the other infinite prime. At all finite

primes distinct from Q and D_F it is $+1$, since $\sqrt{2q}$ and ε are local units. We will now prove that $(\sqrt{2q}, \varepsilon)_Q = -1$. Using this we can conclude by reciprocity that $(\sqrt{2q}, \varepsilon)_{D_F} = +1$.

We claim that $(\sqrt{2q}, \varepsilon)_Q = -1$, i.e., we claim that the equation $\sqrt{2q}x^2 + \varepsilon y^2 = 1$ has no solution in F_Q , the completion of F at Q . This is equivalent to: $\sqrt{2q}x^2 + \varepsilon y^2 = z^2$ has no solution in O_Q , the ring of integers of F_Q .

Suppose that there exists a solution $x, y, z \in O_Q$. We can assume that x, y, z are relatively prime. Since O_Q has only one prime, namely a generator of Q , we can assume that at least one of x, y, z is a local unit.

Case 1: z is not a local unit:

We check that it is impossible for $\sqrt{2q}x^2 + \varepsilon y^2 = z^2$ to have a solution where x or y is a unit. We have $\text{ord}_Q(\sqrt{2q}) = 1$ and $\text{ord}_Q(\varepsilon) = 0$. In the present case we also have $\text{ord}_Q(z) \geq 1$, so $\text{ord}_Q(z^2) \geq 2$. If we assume that y is a local unit, then $\text{ord}_Q(\varepsilon y^2) = 0$. But $\text{ord}_Q(\sqrt{2q}x^2) \geq 1$, so $\text{ord}_Q(\sqrt{2q}x^2 + \varepsilon y^2) = 0 < 2 \leq \text{ord}_Q(z^2)$. Hence, y can not be a unit, so x must be a unit. We have $\text{ord}_Q(\sqrt{2q}x^2) = 1$ and $\text{ord}_Q(\varepsilon y^2) \geq 2$. This gives $\text{ord}_Q(\sqrt{2q}x^2 + \varepsilon y^2) = 1 < 2 \leq \text{ord}_Q(z^2)$, which again shows that $\sqrt{2q}x^2 + \varepsilon y^2$ can not equal z^2 .

Case 2: z is a local unit:

Dividing the equation by z yields: $\sqrt{2q}x^2 + \varepsilon y^2 = 1$ for some $x, y \in O_Q$. This will also lead to a contradiction. Let $\varepsilon = \alpha + \beta\sqrt{2q}$ for some $\alpha, \beta \in \mathbb{Z}$. Note that since $N(\varepsilon) = \alpha^2 - 2q\beta^2 = -1$, we have $\alpha^2 \equiv -1 \pmod{q}$. We are assuming that the equation $\sqrt{2q}x^2 + (\alpha + \beta\sqrt{2q})y^2 = 1$ has a solution in O_Q . It therefore also has a solution modulo $Q = (\sqrt{2q}, q)$. Since $\sqrt{2q} \in Q$ the equation reduces to $\alpha y^2 \equiv 1 \pmod{Q}$. If we let $y = c + d\sqrt{2q}$ for some $c, d \in \mathbb{Z}$, then $y^2 = c^2 + 2qd^2 + 2cd\sqrt{2q} \equiv c^2 \pmod{Q}$. This equation reduces to $\alpha c^2 \equiv 1 \pmod{q}$. Multiplying by $\alpha^{-1} \equiv -\alpha \pmod{q}$ yields: $c^2 \equiv -\alpha \pmod{q}$. This is impossible since $-\alpha$ is not a square modulo q . This can be seen by checking the Legendre symbol:

$$\left(\frac{-\alpha}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{\alpha}{q}\right) = (-1)(+1)$$

Here we used the fact that $q \equiv 5 \pmod{8}$, so $\left(\frac{-1}{q}\right) = +1$. Also, we have that $\alpha^2 \equiv -1 \pmod{q}$. The subgroup of 4-th powers of $(\mathbb{Z}/q)^*$ has $\frac{q-1}{4}$ elements, so its order is odd. This shows that -1 is not a fourth power modulo q , and therefore α is not a

square modulo q , i.e., $(\frac{\alpha}{q}) = -1$.

This concludes the proof that $\sqrt{2q}x^2 + \varepsilon y^2 = z^2$ does not have a solution in F_Q , hence $(\sqrt{2q}, \varepsilon)_Q = -1$. \square

16. Quadratic extensions of $\mathbb{Q}(\sqrt{10})$ with property (*)

In the previous section we were examining number fields of the type $F = \mathbb{Q}(\sqrt{2q})$ for a prime $q \equiv 5 \pmod{8}$. We saw that:

$$O_F^*/(O_F^*)^2 = \{\pm 1, \pm \varepsilon\} \quad U_F^S/(U_F^S)^2 = \{\pm 1, \pm \varepsilon, \pm 2, \pm 2\varepsilon\}$$

Furthermore, we proved that $\sqrt{2q} \in F_D^*/(F_D^*)^2 - U_F^S/(U_F^S)^2$, so

$$F_D^*/(F_D^*)^2 = \{\pm 1, \pm \varepsilon, \pm 2, \pm 2\varepsilon, \pm \sqrt{2q}, \pm \varepsilon\sqrt{2q}, \pm 2\sqrt{2q}, \pm 2\varepsilon\sqrt{2q}\}$$

We now apply this to the case $q = 5$. For $F = \mathbb{Q}(\sqrt{10})$ a positive fundamental unit is given by $\varepsilon = 3 + \sqrt{10}$. From the above we have:

$$O_F^*/(O_F^*)^2 = \{\pm 1, \pm \varepsilon\} \quad U_F^S/(U_F^S)^2 = \{\pm 1, \pm \varepsilon, \pm 2, \pm 2\varepsilon\}$$

$$F_D^*/(F_D^*)^2 = \{\pm 1, \pm \varepsilon, \pm 2, \pm 2\varepsilon, \pm \sqrt{10}, \pm \varepsilon\sqrt{10}, \pm 2\sqrt{10}, \pm 2\varepsilon\sqrt{10}\}$$

The $2^{r_1(F)+1} = 8$ infinite families of quadratic extensions with property (*) of $F = \mathbb{Q}(\sqrt{10})$ correspond to the 8 elements $\beta \in \{\pm \sqrt{10}, \pm \varepsilon\sqrt{10}, \pm 2\sqrt{10}, \pm 2\varepsilon\sqrt{10}\}$. Each pair $\beta, 2\beta$ corresponds to a subgroup of index 2 of $U_F^S/(U_F^S)^2$ that does not contain $\tau = 2$. This subgroup consists of those square classes that are norms from the members of the corresponding families. There are four such subgroups:

$$\langle \varepsilon, -\varepsilon \rangle = \{1, \varepsilon, -\varepsilon, -1\} \quad \langle \varepsilon, -2\varepsilon \rangle = \{1, \varepsilon, 2\varepsilon, -2\varepsilon\}$$

$$\langle 2\varepsilon, -\varepsilon \rangle = \{1, 2\varepsilon, -\varepsilon, -2\varepsilon\} \quad \langle 2\varepsilon, -2\varepsilon \rangle = \{1, 2\varepsilon, -2\varepsilon, -1\}$$

We will now determine which β they correspond to. We will also explicitly determine one member for each of the corresponding infinite families.

(16.1) Theorem: Let $F = \mathbb{Q}(\sqrt{10})$. A positive fundamental unit of F is given by $\varepsilon = 3 + \sqrt{10}$. This number field contains units with independent signs and $2||h(F)$. There exists exactly one quadratic extension with property (*) in which no odd prime of F ramifies. It is given by $F(\sqrt{2})$. This is an unramified extension of F . Its class number is odd.

There are 8 infinite families of quadratic extensions of F with property (*). The following table lists one member E of each family together with the $\beta \in F_D^*/(F_D^*)^2 - U_F^S/(U_F^S)^2$ that is associated to the family, the subgroup of $U_F^S/(U_F^S)^2$ that consists of square classes of norms from E over F , the exact 2-power dividing the class number of E and whether E contains units with independent signs [uwis] or not.

E	β	norms $E F$	
$F(\sqrt{10+3\sqrt{10}})$	$\varepsilon\sqrt{10}$	$\{1, 2\varepsilon, -2\varepsilon, -1\}$	$2 h(E)$ no uwis
$F(\sqrt{2(10+3\sqrt{10})})$	$2\varepsilon\sqrt{10}$	$\{1, 2\varepsilon, -2\varepsilon, -1\}$	$2 h(E)$ no uwis
$F(\sqrt{20-5\sqrt{10}})$	$\sqrt{10}$	$\{1, \varepsilon, -2\varepsilon, -2\}$	$2 h(E)$ no uwis
$F(\sqrt{2(20-5\sqrt{10})})$	$2\sqrt{10}$	$\{1, \varepsilon, -2\varepsilon, -2\}$	$2 h(E)$ no uwis
$F(\sqrt{20+5\sqrt{10}})$	$-\sqrt{10}$	$\{1, 2\varepsilon, -\varepsilon, -2\}$	$2 h(E)$ no uwis
$F(\sqrt{2(20+5\sqrt{10})})$	$-2\sqrt{10}$	$\{1, 2\varepsilon, -\varepsilon, -2\}$	$2 h(E)$ no uwis
$F(\sqrt{38+11\sqrt{10}})$	$-\varepsilon\sqrt{10}$	$\{1, \varepsilon, -\varepsilon, -1\}$	$4 h(E)$ uwis
$F(\sqrt{2(38+11\sqrt{10})})$	$-2\varepsilon\sqrt{10}$	$\{1, \varepsilon, -\varepsilon, -1\}$	$4 h(E)$ uwis

Remark: In (15.2) we saw $F(\sqrt{2(10+3\sqrt{10})}) = F(\sqrt{10+\sqrt{10}})$, so the example from section 4 is among the above.

Remark: In (3.1) we recalled a criterion on how to distinguish among the different types of number fields of degree 4. From the norms that are computed in 16.2 we obtain: The first two fields listed in the above table are **biquadratic cyclic** (see 15.1), whereas all others are **non-abelian biquadratic**.

Proof of (16.1):

By (13.1.C) we know that F contains units with independent signs and that $2||h(F)$. With the notation as in our main theorem $F = \mathbb{Q}(\sqrt{10})$ is of type C). The claims on $F(\sqrt{2})$ all follow from this. The main theorem also tells us the properties of all

infinite families.

To determine which $\beta \in \{\sqrt{10}, -\sqrt{10}, \varepsilon\sqrt{10}, -\varepsilon\sqrt{10}\}$ each of the 4 subgroups of norms correspond to, we determine Hilbert symbols at D_F :

$$\begin{aligned} \text{From (15.3) we have: } (\sqrt{10}, -1)_{D_F} &= -1 & (\sqrt{10}, \varepsilon)_{D_F} &= +1 & (\varepsilon, -\varepsilon)_{D_F} &= +1 \\ (\varepsilon, \varepsilon)_{D_F} &= -1 & (1, \varepsilon)_{D_F} &= -1 & (-1, -1)_{D_F} &= +1 \end{aligned}$$

Using these we obtain:

$$(\sqrt{10}, \varepsilon)_{D_F} = +1$$

$$(\sqrt{10}, -\varepsilon)_{D_F} = (\sqrt{10}, -1)_{D_F}(\sqrt{10}, \varepsilon)_{D_F} = (-1)(+1) = -1$$

Hence $\sqrt{10}$ corresponds to $\langle \varepsilon, -2\varepsilon \rangle$

$$(-\sqrt{10}, \varepsilon)_{D_F} = (-1, \varepsilon)_{D_F}(\sqrt{10}, \varepsilon)_{D_F} = (-1)(+1) = -1$$

$$(-\sqrt{10}, -\varepsilon)_{D_F} = (-1, -\varepsilon)_{D_F}(\sqrt{10}, -1)_{D_F}(\sqrt{10}, \varepsilon)_{D_F} = (-1)(-1)(+1) = +1$$

Hence $-\sqrt{10}$ corresponds to $\langle 2\varepsilon, -\varepsilon \rangle$

$$(\varepsilon\sqrt{10}, \varepsilon)_{D_F} = (\varepsilon, \varepsilon)_{D_F}(\sqrt{10}, \varepsilon)_{D_F} = (-1)(+1) = -1$$

$$(\varepsilon\sqrt{10}, -\varepsilon)_{D_F} = (\varepsilon, -\varepsilon)_{D_F}(\sqrt{10}, -\varepsilon)_{D_F} = (+1)(-1) = -1$$

Hence $\varepsilon\sqrt{10}$ corresponds to $\langle 2\varepsilon, -2\varepsilon \rangle$

$$(-\varepsilon\sqrt{10}, \varepsilon)_{D_F} = (-\varepsilon, \varepsilon)_{D_F}(\sqrt{10}, \varepsilon)_{D_F} = (+1)(+1) = +1$$

$$(-\varepsilon\sqrt{10}, -\varepsilon)_{D_F} = (-1, -1)_{D_F}(-1, \varepsilon)_{D_F}(\varepsilon\sqrt{10}, -\varepsilon)_{D_F} = (+1)(-1)(-1) = +1$$

Hence $-\varepsilon\sqrt{10}$ corresponds to $\langle \varepsilon, -\varepsilon \rangle$

Note that by (11.9) the members of the families corresponding to $\beta = -\varepsilon\sqrt{10}$ and $\tau\beta = -2\varepsilon\sqrt{10}$ will be the ones that contain units with independent signs, since they have $O_F^*/(O_F^*)^2$ as the subset of $U_F^S/(U_F^S)^2$ that are norms. This determines all properties of the members of each family: The members E of the two families corresponding to $-\varepsilon\sqrt{10}$ and $-2\varepsilon\sqrt{10}$ contain units with independent signs and have $4||h(E)$ (since $2||h(F)$). All others do not contain units with independent signs and $2||h(E)$.

We still have to show that the number fields E listed in the table of (16.1) are in fact members of the infinite families of their corresponding β . For this we need to prove that $10 + 3\sqrt{10}$, $20 - 5\sqrt{10}$, $20 + 5\sqrt{10}$ and $38 + 11\sqrt{10}$ are totally positive elements of F whose image in $F_D^*/(F_D^*)^2$ is $\varepsilon\sqrt{10}, \sqrt{10}, -\sqrt{10}, -\varepsilon\sqrt{10}$, respectively,

and whose prime ideal decomposition contains exactly one odd prime to an odd power.

For $\beta = \varepsilon\sqrt{10}$ we already saw in the general case (15.1) that $\varepsilon\sqrt{10} = 10 + 3\sqrt{10}$ satisfies all required properties.

The other 3 elements will be examined in (16.2). \square

(16.2) Proposition: The elements $20 - 5\sqrt{10}$, $20 + 5\sqrt{10}$ and $38 + 11\sqrt{10}$ in $F = \mathbb{Q}(\sqrt{10})$ have the following properties:

- a) they are totally positive,
- b) their prime ideal decomposition contains exactly one odd prime of F to an odd power,
- c) in $F_D^*/(F_D^*)^2$ they map to $\sqrt{10}, -\sqrt{10}, -\varepsilon\sqrt{10}$, respectively.

Proof: a) All three elements are in fact totally positive.

b) We compute their norms over \mathbb{Q} :

$$N(20 \pm 5\sqrt{10}) = 20^2 - 250 = 150 = 2 \cdot 3 \cdot 5^2$$

$$N(38 + 11\sqrt{10}) = 38^2 - 1210 = 234 = 2 \cdot 3^2 \cdot 13$$

The rational primes 3 and 13 split in F over \mathbb{Q} . The primes 2 and 5 are exactly the ramified primes. Let D_F denote the prime over 2, Q the prime over 5, P a prime over 3 and P' a prime over 13. Note that 3 appears to a second power in the norm of $38 + 11\sqrt{10}$. The prime ideal decomposition of $(38 + 11\sqrt{10}) \cdot O_F$ therefore contains either P^2 or both primes that lie over 3, each to the first power. The second case is not possible since 3 does not divide 38 and 11. We therefore have:

$$(20 \pm 5\sqrt{10}) \cdot O_F = (D_F)^2 \cdot P \cdot Q^2$$

$$(38 + 11\sqrt{10}) \cdot O_F = (D_F)^2 \cdot P^2 \cdot P'$$

In either case, we see that the prime ideal decomposition contains exactly one odd prime.

c) To prove that in $F_D^*/(F_D^*)^2$ we have:

$$\sqrt{10} = 20 - 5\sqrt{10}, \quad -\sqrt{10} = 20 + 5\sqrt{10} \quad \text{and} \quad -\varepsilon\sqrt{10} = 38 + 11\sqrt{10}$$

we observe that the following equalities hold in F :

$$20 - 5\sqrt{10} = \sqrt{10}(-5 + 2\sqrt{10}) = \sqrt{10} \cdot [(1 + \sqrt{10})^2 - 2^4]$$

$$20 + 5\sqrt{10} = -\sqrt{10}(-5 - 2\sqrt{10}) = -\sqrt{10} \cdot [(1 - \sqrt{10})^2 - 2^4]$$

$$38 + 11\sqrt{10} = -\varepsilon\sqrt{10} \cdot \frac{-50+4\sqrt{10}}{10} = -\varepsilon\sqrt{10} \cdot \frac{1}{10} \cdot [(2 + \sqrt{10})^2 - 2^6]$$

Note that $\frac{1}{10} = (\frac{1}{\sqrt{10}})^2 \in (F^*)^2$, so this element is trivial in $F_D^*/(F_D^*)^2$.

We will now check that the elements in [...] are also trivial in $F_D^*/(F_D^*)^2$, i.e., that they are in $(F_D)^2$. This is done by applying Hensel's lemma:

The elements are all of the type $[A^2 - 2^n]$ with $n \geq 4$ and $A \in O_F$ with

$\text{ord}_{D_F}(A) = 0$, for $A = 1 \pm \sqrt{10}$, and $\text{ord}_{D_F}(A) = 1$, for $A = 2 + \sqrt{10}$.

The polynomial $F(x) = x^2 - (A^2 - 2^n)$ has a solution modulo $(D_F)^{2^n}$.

Such a solution is given by A , since $\text{ord}_{D_F}(2) = 2$, so $2^n \equiv 0 \pmod{(D_F)^{2^n}}$. We have:

$$\text{ord}_{D_F}(F'(A)) = \text{ord}_{D_F}(2A) = \text{ord}_{D_F}(2) + \text{ord}_{D_F}(A) \leq 3$$

Since $2 \cdot 3 + 1 \leq 2n$ for $n \geq 4$, the hypothesis of Hensel's lemma is satisfied and we obtain that $F(x)$ has a solution in F_D . Hence, all elements in [...], above, are squares in F_D . \square

BIBLIOGRAPHY

- [Cohn] H. COHN: A classical invitation to algebraic numbers and class fields, Springer-Verlag, New York, 1978
- [C- H_1] P.E. CONNER, J. HURRELBRINK: A comparison theorem for the 2-rank of $K_2(O)$, AMS Contemporary Math.55, part 2, 411-420, 1986
- [C- H_2] P.E. CONNER, J. HURRELBRINK: Class number parity, set of notes, 240 p., LSU, to appear
- [Ga] H. GARLAND: A finiteness theorem for K_2 of a number field , Ann. of Math. 94, 534-548, 1971
- [Gr] G. GRAS: Remarks on K_2 of number fields, J. Number Th., Vol. 23, no. 3, 322-335, 1986
- [Ha] H. HASSE: Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern, Abh. Dt. Akad. Wiss. Berlin, Math. Naturwiss. Kl.2, 1-95, 1950
- [He] K.F. HETTLING: On K_2 of rings of integers of totally real number fields, Doctoral dissertation, LSU, 1985; J. Algebra 107, 292-296, 1987
- [Hu] J. HURRELBRINK: Class numbers, units and K_2 , to appear in the Proceedings of the 1987 Algebraic K-Theory Conference at Lake Louise, Canada, in the NATO ASI series.
- [I-R] K. IRELAND, M. ROSEN: A classical introduction to modern number theory, Grad. Texts in math. 84, Springer Verlag, New York-Heidelberg-Berlin, 1982

- [Ko] M. KOLSTER: The structure of the 2-Sylow subgroup of $K_2(O)$, I,
Comment. Math. Helvetici 61, 376-388, 1986
- [La] S. LANG: Algebraic number theory,
Grad. Texts in math. 110, Springer Verlag, New York, 1986
- [Mi] J. MILNOR: Introduction to algebraic K-theory,
Ann. Math. Stud. 72, Princeton Univ. Press, 1971
- [M-W] B. MAZUR and A. WILES: Class fields of abelian extensions of \mathbb{Q} ,
Invent. math. 76, 179-330, 1984
- [O'M] O.T. O'MEARA: Introduction to quadratic forms,
Springer Verlag, Berlin, New York, 1971
- [Ta] J. TATE: Relations between K_2 and Galois cohomology,
Invent. math. 36, 257-274, 1976

Vita

Name: Ruth I. Berger

Social sec.: 434-51-3458

Date of birth: 12/31/59

Place of birth: Friedberg, W-Germany

Citizenship: German

Education:

Highschool attended: Albertus Magnus Gymnasium, St. Ingbert, W-Germany

Vordiplom, July 81, Universität des Saarlandes, W-Germany

M.S., December 85, Louisiana State University

PhD in Mathematics, May 88, Louisiana State University

Major field in Mathematics: Algebra and algebraic number theory

Research interests: Relations between classical number theory and K-groups

Thesis advisor: Dr. J. Hurrelbrink, Louisiana State University

Thesis title: "Class numbers and units of number fields E
with elementary abelian $K_2(O_E)$ "

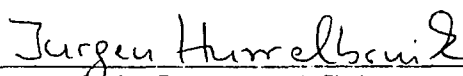
DOCTORAL EXAMINATION AND DISSERTATION REPORT

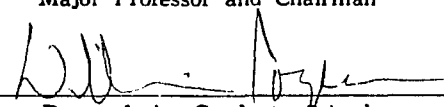
Candidate: Ruth Ilse Berger

Major Field: Mathematics

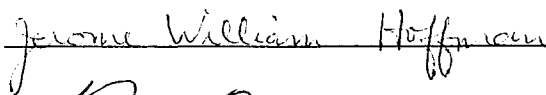
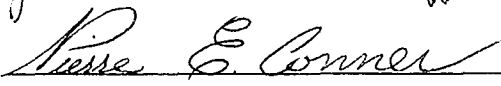
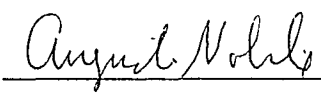
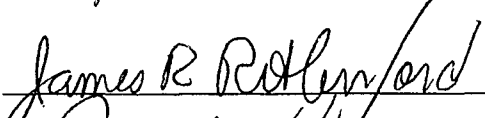
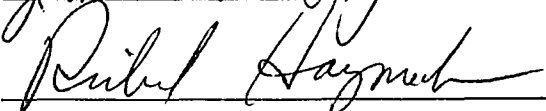
Title of Dissertation: Class Numbers and Units of Number Fields E with Elementary Abelian $K_2(O_E)$

Approved:


Major Professor and Chairman


Dean of the Graduate School

EXAMINING COMMITTEE:

Date of Examination:

February 23, 1988