# Euclid's Algorithm in Multiquadratic Fields

by

**A. F. Amy Feaver**

B.S., Rensselaer Polytechnic Institute, 2007

M.A., University of Colorado, 2011

A thesis submitted to the

Faculty of the Graduate School of the

University of Colorado in partial fulfillment

of the requirements for the degree of

Doctor of Philosophy

Department of Mathematics

2014

This thesis entitled:
Euclid's Algorithm in Multiquadratic Fields
written by A. F. Amy Feaver
has been approved for the Department of Mathematics

_____

Katherine Stange

_____

David Grant

Date _____

The final copy of this thesis has been examined by the signatories, and we find that both the content and the form meet acceptable presentation standards of scholarly work in the above mentioned discipline.

Amy Feaver, A. F. (Ph.D., Mathematics)

Euclid's Algorithm in Multiquadratic Fields

Thesis directed by Prof. Katherine Stange

In this thesis we find that all imaginary $n$-quadratic fields with $n \geq 4$ have class number larger than 1 and therefore cannot be Euclidean. We also examine imaginary triquadratic fields, presenting a complete list of 17 imaginary triquadratic fields with class number 1, and classifing many of them according to whether or not they are norm-Euclidean.

## Dedication

*The Lord gives, and the Lord takes away; blessed be the name of the Lord.*

Father, You have poured out Your blessings abundantly upon me. You have given me the ability to write this thesis and to spend a wonderful seven years in Boulder with great friends, surrounded by Your beautiful creation, and enjoying the life which You have given me. But even if you hadn't given me any of these gifts, even if all of this was taken away, I would still fall down and worship You because *You are worthy, O Lord, to receive glory and honor and power.*

This pile of paper which I have been able to produce by Your grace alone, I dedicate it to You. Take this Ph.D. and use it, and use me, to serve You and love You in any way that I can.

Take my intellect and use every power as Thou shalt choose.
Take my will and make it Thine; it shall be no longer mine.
Take my heart it is Thine own; it shall be Thy royal throne.
Take my love my Lord I pour at Thy feet its treasure store.
Take myself and I will be ever, only, all for Thee.

## Acknowledgements

I would like to thank:

my husband Nathan for his patience and delicious french onion soup;

my advisor Kate Stange who has offered so much insight, wisdom and support;

my 'little' brother Phil for answering my computer questions and telling me bad math jokes;

my great aunt Barbara for all of her advice and perspective on life and for encouraging me to never give up;

Nathan Wakefield, the best big (math) brother I could have ever asked for;

Divya, for being such a good listener and always giving excellent advice;

Ben Purkis, Justin Keller, Angela Nilles, Mike Martinez and Katherine Martinez for their friendship: for keeping me sane, helping me prepare for interviews and exams, and every hour we spent building snow forts, tubing on the creek, eating meals, celebrating holidays and hunting horcruxes.

# Contents

**Chapter**

# Chapter 1

# Introduction

## 1.1 Euclidean Rings

In 300 B.C., Euclid described an algorithm in books VII and X of his *Elements*; a highly effective algorithm to compute the greatest common divisor (GCD) of two rational integers. More than 2,000 years later, mathematicians began asking the question of whether or not a similar algorithm, called a Euclidean algorithm, exists in other rings. The study of this algorithm is no longer simply a means of finding GCDs, but is connected to several other interesting properties of rings; one of the most well-known connections being that the existence of a Euclidean algorithm in a ring implies unique factorization.

**Definition 1.1.1.** A ring $R$ is called *Euclidean* if there exists a function $f : R \setminus \{0\} \to \mathbb{N}$ such that for all $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ such that $a = qb + r$ and either $r = 0$ or $f(r) < f(b)$. A function which satisfies these properties is called a *Euclidean function* on $R$.

In addition to classifying a ring according to whether or not it is Euclidean we can ask much more specific questions about the size of the remainders $r$ which are obtained from division. For example, if we are told that $R$ is not Euclidean with respect to $f$, we still might wonder if $f(r)$ is at most only slightly larger than $f(b)$, or if $f(r)$ may be several times the value of $f(b)$. Also, if $R$ has two different Euclidean functions $f_1$ and $f_2$, it might turn out that these two functions exhibit different properties. It is possible that $f_1(r)/f_1(b)$ might get very close to 1 for some values of $b$, while $f_2(r)/f_2(b)$ might never exceed $1/4$. These questions lead us to the following definition:

**Definition 1.1.2.** Let $R$ be a ring and let $f$ be a function $f : R \to \mathbb{Z}$ such that $f(R \setminus \{0\}) \subseteq \mathbb{N}$ and $f(0) = 0$. Then the *Euclidean minimum* of $R$ with respect to $f$, denoted $M(R, f)$ is given by

$$M(R, f) = \inf\{\delta > 0 | \text{ for all } a, b \in R\backslash\{0\} \text{ there exist } q, r \in R \text{ such that } a = qb+r \text{ and } f(r)/f(b) < \delta\}.$$

If $M(R, f) < 1$ then clearly $R$ is Euclidean with respect to $f$. Similarly if $M(R, f) > 1$, $R$ is not Euclidean with respect to $f$. It is possible to have $M(R, f) = 1$, and this does not give us sufficient information to determine whether or not $R$ is Euclidean with respect to $f$.

## 1.2 Norm-Euclidean Integer Rings

The ring of integers $\mathcal{O}_K$ of an algebraic number field comes equipped with a function, the norm function $N$, which maps elements of $\mathcal{O}_K$ to $\mathbb{Z}$. The absolute value of this norm function is a Euclidean function on many number fields, so it is a natural function to look at when studying Euclideanity in the context of algebraic number theory.

In this section, we first must understand basic notions of number fields. An *(algebraic) number field* is a finite degree field extension of $\mathbb{Q}$. If $K$ is any number field, the *ring of integers of* $K$, denoted $\mathcal{O}_K$, is the ring consisting of all elements of $K$ which are zeros of some monic polynomial with coefficients in $\mathbb{Z}$. If $K$ is a degree $n$ extension of $\mathbb{Q}$ then there are $n$ embeddings $K \hookrightarrow \mathbb{C}$ which fix $\mathbb{Q}$, usually denoted $\sigma_1, ..., \sigma_n$. The *(absolute) norm* of an element $\alpha \in K$, denoted $N_{K/\mathbb{Q}}(\alpha)$ is given by

$$N_{K/\mathbb{Q}}(\alpha) = \sigma_1(\alpha) \cdots \sigma_n(\alpha).$$

When there is no ambiguity, the absolute norm of a number field will be denoted simply by $N$ instead of $N_{K/\mathbb{Q}}$.

We will also use a more general notion of the norm $N$, the *relative norm*. If $K$ and $L$ are two distinct number fields with $K \subset L$ then $L$ is a finite degree extension of $K$. Denote by $m$ the degree of this extension. Then there are $m$ embeddings $L \hookrightarrow \mathbb{C}$ which fix $K$, which we will call $\sigma_1, ..., \sigma_m$. The *relative norm* of an element $\alpha$ from $L$ to $K$, denoted $N_{L/K}(\alpha)$ is given by

$$N_{L/K}(\alpha) = \sigma_1(\alpha) \cdots \sigma_m(\alpha).$$

These functions have the property that for any $\alpha \in L$,

$$N_{L/\mathbb{Q}}(\alpha) = N_{K/\mathbb{Q}}(N_{L/K}(\alpha)).$$

**Definition 1.2.1.** Let $K$ be any number field. The ring of integers $\mathcal{O}_K$ is said to be *norm-Euclidean* if the function $f(\cdot) := |N(\cdot)|$ is a Euclidean function on $\mathcal{O}_K$. That is, for any $a, b \in \mathcal{O}_K \setminus \{0\}$ there exist $q, r \in \mathcal{O}_K$ such that $a = qb + r$ and $|N(r)| < |N(b)|$.

The phrase *norm-Euclidean number field* is often used in literature. This is used to mean *norm-Euclidean ring of integers associated with a number field*; because it does not make sense to study whether or not a field is norm-Euclidean, this phrase should not give rise to any ambiguity.

In the case of number fields, we will rely heavily on a different definition of norm-Euclidean, equivalent to the one presented above:

**Definition 1.2.2.** A number field $K$ is *norm-Euclidean* if and only if each $\gamma \in K$ can be written in the form $\gamma = x + \delta$ where $x \in \mathcal{O}_K$ and $|N(\delta)| < 1$.

It is fairly straightforward to see that these definitions are equivalent. Assume that a field $K$ is norm-Euclidean with respect to the first definition; that is, for any $a, b \in \mathcal{O}_K$ there exists $q, r \in \mathcal{O}_K$ such that $a = qb + r$ and $|N(r)| < |N(b)|$. Then if we divide $a = qb + r$ by $b$, we have $a/b = q + r/b$. Letting $\gamma = a/b \in K$, $x = q \in \mathcal{O}_K$ and $\delta = r/b$, we find that $|N(\delta)| = |N(r)|/|N(b)| < 1$. Thus the value $\gamma = a/b$ satisfies Definition 1.2.2. To see that the converse holds, choose any $\gamma \in K$. There exists $b \in \mathcal{O}_K$ such that $\gamma b \in \mathcal{O}_K$ (think about multiplication by $b$ as clearing the denominator of $\gamma$). Then setting $a = \gamma b$ we find that $a, b$ satisfy Definition 1.2.1.

As an example, consider the number field is $K = \mathbb{Q}[i]$, which has integer ring $\mathcal{O}_K = \mathbb{Z}[i]$, commonly referred to as the *Gaussian integers*. This can be shown to be Euclidean by applying Definition 1.2.2. Start with any $\gamma \in K$. Then $\gamma$ may be written $\frac{a_0}{d} + \frac{a_1}{d}i$ with $a_0, a_1, d \in \mathbb{Z}$; these fractions are not necessarily written in lowest terms because we want to ensure a common denominator $d$. For $i = 0, 1$ let $a_i'$ be the integer with smallest absolute value such that $a_i \equiv$

$a_i' \bmod d$. Then define $x \in \mathcal{O}_K$, $\delta \in K$ by

$$x = \frac{a_0 - a_0'}{d} + \frac{a_1 - a_1'}{d} i, \quad \delta = \frac{a_0'}{d} + \frac{a_1'}{d} i.$$

Clearly $\gamma = x + \delta$, and

$$|N(\delta)| = \left(\frac{a_0'}{d} + \frac{a_1'}{d} i\right)\left(\frac{a_0'}{d} - \frac{a_1'}{d} i\right) \leq \left(\frac{1}{2} + \frac{1}{2} i\right)\left(\frac{1}{2} - \frac{1}{2} i\right) = \frac{1}{4} + \frac{1}{4} = \frac{1}{2} < 1.$$

It is interesting in this case that $|N(\delta)|$ is not only less than 1, but it is actually less than or equal to $\frac{1}{2}$. For this number field, the Euclidean minimum is in fact equal to $\frac{1}{2}$.

Because the absolute value of the norm function on a number field is most commonly used to study the Euclideanity of these fields, we will assume for the remainder of this text that this is the function of study, unless otherwise stated. Thus we will define the *Euclidean minimum* of a number field to mean the Euclidean minimum with respect to $|N(\cdot)|$:

**Definition 1.2.3.** Let $K$ be a number field. Then the *Euclidean minimum* of $K$, $M(K)$, is:

$$M(K) = \inf \left\{ \delta > 0 \;\middle|\; \begin{array}{l} \text{for all } a, b \in \mathcal{O}_K \setminus \{0\} \text{ there exist } q, r \in \mathcal{O}_K \\ \text{such that } a = qb + r \text{ and } |N(r)/N(b)| < \delta \end{array} \right\}.$$

Notice that this construction of the Euclidean minimum uses the notation of Definition 1.2.1. There is a second way to define the Euclidean minimum, using the notation and ideas of the equivalent Definition 1.2.2:

**Definition 1.2.4.** Let $K$ be any number field. For any $\gamma \in K$, the *Euclidean minimum at* $\gamma$, denoted $M(K, \gamma)$, is given by

$$M(K, \gamma) = \inf_{x \in \mathcal{O}_K} \{|N(\gamma - x)|\}.$$

The *Euclidean minimum* of the field $K$, denoted $M(K)$, is

$$M(K) = \sup_{\gamma \in K} \{M(K, \gamma)\}.$$

## 1.3 Restricting to the Fundamental Domain

Looking at Definition 1.2.4 we see that $M(K,\gamma) = M(K,\gamma - x)$ for any $x \in \mathcal{O}_K$. We want to use this fact to our advantage when studying Euclidean minima. Notice that the relation given by $\gamma_1 \sim \gamma_2$ if and only if $\gamma_1 = \gamma_2 + x$ for some $x \in \mathcal{O}_K$ is an equivalence relation on $K$. Denote by $K/\mathcal{O}_K$ a set of representatives of the equivalence classes on $K$ given by this relation. Then the Euclidean minimum $M(K)$ is equal to

$$M(K) = \sup_{\gamma \in K/\mathcal{O}_K} \{M(K,\gamma)\}.$$

Any fundamental domain $\mathcal{F}$ of a number field $K$ is a set of representatives of these equivalence classes and is therefore sometimes denoted by $K/\mathcal{O}_K$. To define this more precisely we need to first fix an integral basis of $\mathcal{O}_K$. An *integral basis* of $\mathcal{O}_K$ is a set of integers $\{b_1, ..., b_n\}$ such $\mathcal{O}_K$ is equal to the set of all $\mathbb{Z}$-linear combinations of the $b_i$'s. Once we have a fixed integral basis for $K$ we can define a unique fundamental domain for $K$.

**Definition 1.3.1.** The *fundamental domain* $\mathcal{F}$ of a number field $K$ with respect to the integral basis $\{b_1, ..., b_n\}$ is given by

$$\mathcal{F} := \{r_1 b_1 + \cdots + r_n b_n | r_i \in [0,1) \cap \mathbb{Q},\ 1 \leq i \leq n\}.$$

**Definition 1.3.2.** Any point $\gamma$ in the fundamental domain of $K$ such that $M(K,\gamma) = M(K)$ is called a *critical point* of $K$.

Isolating critical points can be instrumental in studying fields which are Euclidean but not norm-Euclidean. For example, Clark showed in [5] that the field $\mathbb{Q}(\sqrt{69})$ has this property. Taking the integral basis to be $\{b_1, b_2\} = \{1, (1+\sqrt{69})/2\}$ he recognized

$$\gamma = \frac{16 + 4b_2}{10 + 3b_2}$$

as a critical point, and the Euclidean minimum at this point is greater than 1. In other words, when we divide $a = 16 + 4b_2$ by $b = 10 + 3b_2$ we cannot obtain a remainder $r$ such that $|N(r)| < |N(b)|$.

In fact, the smallest remainder which we can obtain in the division of $a$ by $b$ has $|N(r)| = 25$. Since $|N(b)| = 23$ the remainder will always be larger than $b$. Clark used this information to construct his own Euclidean function $f$ which is a slight modification of the absolute value of the norm function for $K$. He increased the value of $b$ under this function so that $f(r) < f(b)$. This function is $f : \mathcal{O}_K \to \mathbb{Z}$ given by

$$f(x) = \begin{cases} |N(x)| & : x \neq 10 + 3b_2 \\ 26 & : x = 10 + 3b_2 \end{cases}$$

Under this new function $f(\gamma) < 1$ and $K$ is Euclidean.

It is likely that there are infinitely many number fields which are Euclidean but not norm-Euclidean. Weinberger showed in [26] that under the GRH a number field with infinitely many units has class number 1 if and only if it is Euclidean. In fact, there are only finitely many real quadratic fields which are norm-Euclidean, but it is conjectured that there are infinitely many which have class number 1, so there may be infinitely many Euclidean quadratic fields. It would be interesting to know whether or not it is possible to find Euclidean functions on more of these fields using Clark's technique.

Define the set $C$ to be the set of critical points of $K$,

$$C = \{\gamma \in K/\mathcal{O}_K | M(K, \gamma) = M(K)\}.$$

The size of $C$ may vary wildly, depending on the number field $K$. It is not known whether $C$ is always finite, though there are a lot of examples in which $C$ is very small. Pierre Lezowski provides a number of lists of critical points for small degree number fields on his website, which he has computed using his *euclid* program [18]. Even among real quadratic fields the list of critical points can be difficult to predict. For example, consider the fields $\mathbb{Q}(\sqrt{d})$ with $d = 111$ and $d = 115$. Since $111 \equiv 115 \equiv 3 \pmod 4$ we may take the integral basis to be $\{b_1, b_2\} = \{1, \sqrt{d}\}$. We find that when $d = 111$ there is exactly one critical point given by $\sqrt{111}/2$. However, when $d = 115$ there are four critical points, which are,

$$C = \left\{ \frac{1261\sqrt{115}}{4025}, \frac{2764\sqrt{115}}{4025}, \frac{3086\sqrt{115}}{4025}, \frac{939\sqrt{115}}{4025} \right\}.$$

It is worth noting that although these examples are all of the form $q\sqrt{d}$ for some rational number $q$, not all critical points of real quadratic fields take this form, thus adding to their unpredictability.

# Chapter 2

# The Structure of Multiquadratic Number Fields

## 2.1 Basic Notions

A number field of degree 2 over $\mathbb{Q}$ is a *quadratic number field* and can be written $\mathbb{Q}(\sqrt{a})$ for $a \neq 1$ a squarefree rational integer. If $a > 1$ the field $\mathbb{Q}(\sqrt{a})$ is a real quadratic number field, and if $a < 0$ it is an imaginary quadratic field.

**Definition 2.1.1.** An *$n$-quadratic number field*, $n \geq 0$, is any field $K$ of degree $2^n$ over $\mathbb{Q}$ which is formed by adjoining the square root of $m$ rational integers to $\mathbb{Q}$ for some $m \in \mathbb{Z}$. That is, $K = \mathbb{Q}(\sqrt{a_1}, ..., \sqrt{a_m})$ for $a_1, ..., a_m \in \mathbb{Z}$. A *real $n$-quadratic number field* is any $n$-quadratic number field which is totally real. Any $n$-quadratic number field which is not totally real is an *imaginary $n$-quadratic number field.*

**Remark 2.1.2.** Note that any field of the form $K = \mathbb{Q}(\sqrt{a_1}, ..., \sqrt{a_m})$ for $a_1, ..., a_m \in \mathbb{Z}$ is an $n$-quadratic field. That is, any field of this form always has degree $2^n$ for some $n \geq 0$. Also note that we always have $n \leq m$, since adjoining fewer than $n$ square roots to $\mathbb{Q}$ would necessarily produce a field of degree smaller than $2^n$.

**Definition 2.1.3.** Let $m, n \in \mathbb{Z}$ with $1 \leq n \leq m$. A list of squarefree rational integers $\{a_1, ..., a_m\}$ with $a_i \neq 1$, $1 \leq i \leq m$ is called a *radicand list* for the $n$-quadratic field $\mathbb{Q}(\sqrt{a_1}, ..., \sqrt{a_m})$. Further, the list $\{a_1, ..., a_m\}$ is called a *primitive radicand list* if $\mathbb{Q}(\sqrt{a_1}, ..., \sqrt{a_m})$ is $m$-quadratic.

**Lemma 2.1.4.** *The radicand list $\{a_1, ..., a_n\}$ for a multiquadratic number field is primitive if and*

*only if the following condition holds: for any proper subset* $I \subset \{1, ..., n\}$*, and any* $j \in \{1, ..., n\} \setminus I$*,* $a_j$ *is not equal to the squarefree part of the product* $\prod_{i \in I} a_i$*.*

*Proof.* First assume that there exists a proper subset $I \subset \{1, ..., n\}$ and $j \in \{1, ..., n\} \setminus I$ such that $a_j$ is equal to the squarefree part of the product $\prod_{i \in I} a_i$. Then $\sqrt{a_j} \in \mathbb{Q}(\sqrt{a_1}, ..., \sqrt{a_{j-1}}, \sqrt{a_{j+1}}, ..., \sqrt{a_n})$. If this is the case, we have $\mathbb{Q}(\sqrt{a_1}, ..., \sqrt{a_n}) \subseteq \mathbb{Q}(\sqrt{a_1}, ..., \sqrt{a_{j-1}}, \sqrt{a_{j+1}}, ..., \sqrt{a_n})$ so $\{a_1, ..., a_n\}$ generates a field of degree less than $2^n$, and thus is not a primitive set of generators. Therefore, if $\{a_1, ..., a_n\}$ is a primitive set of generators for an $n$-quadratic field, there does not exist any $I \subset \{1, ..., n\}$ and $j \in \{1, ..., n\} \setminus I$, such that $a_j$ is not equal to the squarefree part of the product $\prod_{i \in I} a_i$. Further, it is clear that if $\{a_1, ..., a_n\}$ is a primitive set of generators then no $a_j$ can equal 1 since $\sqrt{1} \in \mathbb{Q}$.

Now assume that the following condition holds for a list of squarefree integers $\{a_1, ..., a_n\}$: for any proper subset $I \subset \{1, ..., n\}$, and any $j \in \{1, ..., n\} \setminus I$, $a_j$ is not equal to the squarefree part of the product $\prod_{i \in I} a_i$. For $1 \leq j \leq n$ let $G_j := \{a_1, ..., a_j\}$ be the set of generators for $K_j := \mathbb{Q}(\sqrt{a_1}, ..., \sqrt{a_j})$. We will prove by induction that $G_j$ is a primitive set of generators for $K_j$ for $1 \leq j \leq n$. Since $a_1 \neq 1$ is squarefree we can clearly see that $K_1$ is a quadratic field with generator $\{a_1\} = G_1$. Now for $j > 1$, assume that $G_{j-1}$ is a primitive set of generators for $K_{j-1}$ and consider the polynomial $x^2 - a_j$. If this polynomial were reducible over the field $K_{j-1}$ we would have $r_1, r_2 \in K_{j-1}$ such that

$$x^2 - a_j = (x - r_1)(x - r_2) = x^2 - (r_1 + r_2)x + r_1 r_2.$$

This implies that $r_1 + r_2 = 0$ and $r_1 r_2 = a_j$, so $r_1, r_2 = \pm\sqrt{a_j}$ and thus $\sqrt{a_j} \in K_{j-1}$. However, since square roots of distinct squarefree integers are linearly independent over $\mathbb{Q}$ this implies that $a_j = 1$ or $a_j$ equals the squarefree part of the product $\prod_{i \in I} a_i$ for some subset $I \subset \{1, ..., a_{j-1}\}$. This is a contradiction, so $G_j$ must be a primitive set of generators for $K_j$ for all $j \in \{1, ..., n\}$. □

**Definition 2.1.5.** For any rational prime $p$, a primitive radicand list $\{a_1, ..., a_n\}$ of an $n$-quadratic field is said to be *$p$-headed* if $p \nmid a_i$ for any $i \in \{2, ..., n\}$.

**Lemma 2.1.6.** *For any $n$-quadratic field $K$ and any prime $p$ there exists a $p$-headed radicand list $\{a_1, ..., a_n\}$ for $K$.*

*Proof.* Choose any prime $p$ and assume that $\{a'_1, ..., a'_n\}$ is a primitive radicand list for $K$ which is not $p$-headed. Then there exists $i > 1$ such that $p|a'_i$; let $a_1 = a'_i$. For each $j \in \{2, ..., i-1, i+1, ..., n\}$ define

$$a_j := \begin{cases} a'_j & p \nmid a'_j \\ \frac{a'_i a'_j}{\gcd(a'_i, a'_j)^2} & p|a'_j \end{cases}$$

and similarly let

$$a_i := \begin{cases} a'_1 & p \nmid a'_1 \\ \frac{a'_i a'_1}{\gcd(a'_i, a'_1)^2} & p|a'_1 \end{cases}.$$

Thus we have a set $\{a_1, ..., a_n\}$ such that $p|a_1$. Also, each $a_k$ is squarefree because either $a_k$ is equal to an element of the set $\{a'_1, ..., a'_n\}$, which only contains squarefree integers, or it is equal to $\frac{a'_i a'_j}{\gcd(a'_i, a'_j)^2}$ for some $i \neq j$, and this is guaranteed to be squarefree since all squares in the product $a'_i a'_j$ are removed when dividing by $\gcd(a'_i, a'_j)^2$. Further, it is easy to see that $a_k \neq 1$ for any $1 \leq k \leq n$ since $\frac{a'_i a'_j}{\gcd(a'_i, a'_j)^2} = 1$ if and only if $a'_i = a'_j$, which clearly is impossible since $i \neq j$. Therefore, $\{a_1, ..., a_n\}$ satisfies the conditions of a primitive set of generators and is $p$-headed. □

**Definition 2.1.7.** A primitive radicand list $\{a_1, ..., a_n\}$ is said to be in *standard form* if

(1) it is 2-headed, and

(2) for any $i, j \in \{1, ..., n\}$ with $2 \nmid a_i a_j$, we have that $a_i \equiv a_j \bmod 4$.

Note that if $K$ is an $n$-quadratic field then there are usually multiple radicand lists for $K$ in standard form.

**Lemma 2.1.8.** *For any $n$-quadratic field $K$ there exists a primitive radicand list $\{a_1, ..., a_n\}$ for $K$ written in standard form.*

*Proof.* Let $\{a'_1, ..., a'_n\}$ be a primitive radicand list for $K$, and, by lemma 2.1.6 we may assume that this list is 2-headed. Assume that this set is not written in standard form; then there exists an

$i \in \{1, ..., n\}$ such that $a_i' \equiv 3 \bmod 4$. For each $j \in \{1, ..., i-1, i+1, ...n\}$ define

$$a_j := \begin{cases} a_j' & a_j' \equiv 2, 3 \pmod 4 \\ \frac{a_i' a_j'}{\gcd(a_i', a_j')^2} & a_j' \equiv 1 \bmod 4 \end{cases}.$$

Then $\{a_1, ..., a_n\}$ is a radicand list for $K$ in standard form. □

Some examples of the above definitions are provided in the following table:

| 4-quadratic number field $K$ | a primitive radicand list for $K$ | a 3-headed radicand list for $K$ | a radicand list for $K$ in standard form |
|---|---|---|---|
| $\mathbb{Q}\left(\sqrt{2}, \sqrt{6}, \sqrt{7}, \sqrt{3}, \sqrt{13}\right)$ | $\{2, 6, 7, 13\}$ | $\{6, 2, 7, 13\}$ | $\{2, 3, 7, 39\}$ |
| $\mathbb{Q}\left(\sqrt{-17}, \sqrt{20}, \sqrt{7}, \sqrt{-1}\right)$ | $\{-17, 5, 7, -1\}$ | $\{-17, 5, 7, -1\}$ | $\{-17, -5, 7, -1\}$ |
| $\mathbb{Q}\left(\sqrt{-3}, \sqrt{5}, \sqrt{-7}, \sqrt{17}\right)$ | $\{-3, 5, -7, 17\}$ | $\{-3, 5, -7, 17\}$ | $\{-3, 5, -7, 17\}$ |

**Lemma 2.1.9.** *Let $K$ be an imaginary $n$-quadratic field. Then there exist positive squarefree integers $a_1, ..., a_n$ such that $\{-a_1, ..., -a_n\}$ is a primitive radicand list for $K$.*

*Proof.* Let $\{a_1', ..., a_n'\}$ be a primitive radicand list for $K$. Since $K$ is not totally real, at least one element of this radicand list must be negative. Thus, without loss of generality assume this list is ordered so that for some $i$, $1 < i \leq n$ we have that $a_1', ..., a_i' < 0$ and $a_{i+1}', ..., a_n' > 0$. Let $a_j = |a_j'|$ for all $j \leq i$. Also, for $j$ satisfying $i < j \leq n$ set $a_j = |s.f.(a_1' a_j')|$. Then $\{-a_1, ..., -a_n\}$ is a primitive radicand list for $K$ satisfying the lemma. □

## 2.2 Subfields

The following lemma is a standard fact:

**Lemma 2.2.1.** *If $K$ is an $n$-quadratic field then the extension $K/\mathbb{Q}$ is Galois, with Galois group $G := \mathrm{Gal}(K/\mathbb{Q}) \cong \bigoplus_{i=1}^{n} (\mathbb{Z}/2\mathbb{Z})$.*

Because the Galois group of a multiquadratic field is a well-known abelian group, we immediately know a lot about the subfields of $K$. At times, we can glean information about a multiquadratic field simply from its quadratic subfields, so we will spend much of this section discussing these subfields.

**Lemma 2.2.2.** *If $K$ is an $n$-quadratic subfield, $n \geq 1$, there are $2^n - 1$ quadratic subfields of $K$.*

*Proof.* Since $G := \mathrm{Gal}(K/\mathbb{Q}) \cong \bigoplus_{i=1}^{n}(\mathbb{Z}/2\mathbb{Z})$ there are the same number of quadratic subfields of $K$ as there are subgroups of $G$ of order $2^{n-1}$; there are exactly $2^n - 1$ such subgroups of $G$. □

**Definition 2.2.3.** Let $m, n \in \mathbb{Z}$ with $1 \leq n \leq m$. A list of squarefree rational integers $\{a_1, ..., a_m\}$ is called a *complete radicand list* for an $n$-quadratic field if and only if the following conditions hold:

(1) $m = 2^n - 1$ and

(2) $a_i \neq a_j$ for all $i, j \in \{1, ..., m\}$ with $i \neq j$.

Note that in the above definition, the complete radicand list for a number field is usually much larger than the primitive radicand list. For example the field $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{-1}\right)$ has primitive radicand list $\{2, 3, 5, -1\}$, while its complete radicand list is

$$\{-1, 2, -2, 3, -3, 5, -5, 6, -6, 10, -10, 15, -15, 30, -30\}.$$

**Lemma 2.2.4.** *If $K$ is any $n$-quadratic field, then the set of squarefree integers, $\{a_1, ..., a_{2^n-1}\}$ is a complete radicand list for $K$ if and only if the fields given by $\mathbb{Q}(\sqrt{a_i})$, $1 \leq i \leq 2^n - 1$, are exactly the $2^n - 1$ distinct quadratic subfields of $K$.*

*Proof.* First assume that $\{a_1, ..., a_{2^n-1}\}$ is a complete radicand list for $K$. Since $a_i \neq 1$ for all $i \in \{1, ..., 2^n - 1\}$, $\mathbb{Q}(\sqrt{a_i})$ is a quadratic subfield of $K$. Further, since each $a_i$ is squarefree and $a_i \neq a_j$ whenever $i \neq j$, each of these quadratic fields is distinct. There are $2^n - 1$ quadratic subfields of $K$, so the set of quadratic subfields must be exactly $\left\{\mathbb{Q}(\sqrt{a_i})\right\}_{1 \leq i \leq 2^n-1}$.

Now assume that $\{a_1, ..., a_{2^n-1}\}$ is a list of squarefree integers such that the set $\left\{\mathbb{Q}(\sqrt{a_i})\right\}_{1 \leq i \leq 2^n-1}$ contains all quadratic subfields of $K$. Since the number of fields in this set is equal to the number of quadratic subfields of $K$, we must have that each element in this set is a quadratic field, and that they are all distinct. Therefore, we must have $a_i \neq 1$ for any $i \in \{1, ..., 2^n - 1\}$ and also that $a_i \neq a_j$ whenever $i \neq j$. Thus $\{a_1, ..., a_{2^n-1}\}$ is a complete radicand list for $K$. □

In general, a multiquadratic field will be described using a primitive radicand list for that field, and we will want to use this list to build a complete radicand list and thus understand the structure of the quadratic subfields. The following lemmas lay the foundation for this.

**Lemma 2.2.5.** *Given a primitive radicand list $\{a_1, ..., a_n\}$ for an $n$-quadratic field $K$, we may construct a complete radicand list for $K$, where the items in this list are exactly*

$$\left\{ s.f. \left( \prod_{i \in I} a_i \right) \mid \emptyset \subset I \subseteq \{1, ..., n\} \right\}.$$

*Proof.* Let

$$\mathcal{C} := \left\{ s.f. \left( \prod_{i \in I} a_i \right) \mid \emptyset \subset I \subseteq \{1, ..., n\} \right\}.$$

Clearly any element of $\mathcal{C}$ is squarefree. Further, by the definition of a primitive radicand list, each element in $\mathcal{C}$ must be distinct, and no element can equal 1. Also, we have that

$$\begin{aligned} \#\mathcal{C} &= \#\left\{ I \mid \emptyset \subset I \subseteq \{1, ..., n\} \right\} \\ &= \sum_{i=1}^{n} \binom{n}{i} \\ &= 2^n - 1. \end{aligned}$$

By the construction of $\mathcal{C}$, it is easy to see that for any $a \in \mathcal{C}$, $\sqrt{a} \in K$. Thus, the elements in $\mathcal{C}$ must make up a complete radicand list for $K$. □

**Lemma 2.2.6.** *Let $K$ be an imaginary $n$-quadratic number field with $n > 1$. Then there are $2^{n-1}$ imaginary quadratic subfields and $2^{n-1} - 1$ real quadratic subfields of $K$.*

*Proof.* Since $K$ is an imaginary $n$-quadratic field there exist positive integers $a_1, ..., a_n$ such that $\{-a_1, ..., -a_n\}$ is a primitive set of generators for $K$.

We begin by finding an upper bound on the number of imaginary quadratic subfields of $K$: $K$ contains the $n$ imaginary quadratic fields given by $\mathbb{Q}(\sqrt{-a_i})$, $1 \leq i \leq n$. Also, if $n \geq 3$, we see that $K$ will also contain the $\binom{n}{3}$ imaginary quadratic fields given by $\mathbb{Q}(\sqrt{-a_i a_j a_k})$, $1 \leq i, j, k \leq n$, and $i, j, k$ all distinct. Similarly, any product $-\pi$ of an odd number $\ell$ of distinct $-a_i$'s will give rise

to an imaginary quadratic subfield $\mathbb{Q}(\sqrt{-\pi})$. There will be $\binom{n}{\ell}$ such subfields, and other than these constructions of imaginary quadratic subfields of $K$, there are no other possibilities. Therefore, the number of imaginary quadratic subfields of $K$ is at most

$$I := \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots + \binom{n}{2\left\lfloor \frac{n-1}{2} \right\rfloor + 1}.$$

Simplifying this expression, we have

$$\begin{aligned} I &= \frac{1}{2}\left[\left(\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \binom{n}{4}\cdots\right) - \left(\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \binom{n}{4} - \cdots\right)\right] \\ &= \frac{1}{2}\left[(1+1)^n - (-1+1)^n\right] \\ &= 2^{n-1}. \end{aligned}$$

Now let's consider the number of real quadratic subfields of $K$. Using an argument similar to the one above, we construct all possible real quadratic fields by taking products of an even number of the $-a_i$'s, $1 \leq i \leq n$. This gives an upper bound on the number of real quadratic subfields of $K$:

$$R := \binom{n}{2} + \binom{n}{4} + \binom{n}{6} + \cdots + \binom{n}{2\left\lfloor \frac{n-1}{2} \right\rfloor}.$$

Computing $R$ in a similar manner to $I$, we find $R = 2^{n-1} - 1$.

Now $I$ and $R$ are upper bounds on the number of imaginary and real quadratic subfields of $K$, respectively. But $I + R = 2^{n-1} + 2^{n-1} - 1 = 2^n - 1$; the total number of quadratic subfields of $K$. Therefore these upper bounds are exactly equal to the number of these fields, so the lemma is established. □

**Lemma 2.2.7.** *Let $\{a_1, ..., a_n\}$ be a primitive radicand list for a field $K$ such that $a_i \equiv 1 \bmod 4$ for all $i \in \{1, ..., n\}$. Then if $\{m_1, ...., m_{2^n-1}\}$ is a complete radicand list for $K$, we have $m_i \equiv 1 \bmod 4$ for all $i \in \{1, ..., 2^n - 1\}$.*

The proof of this lemma is omitted, as it can be easily deduced from the construction of the complete radicand list as described in lemma 2.2.4.

## 2.3 Integers

The structure of the integers of quadratic fields is well-known; for a quadratic field $\mathbb{Q}(\sqrt{a})$, with $a$ squarefree, the integral basis is

$$\begin{cases} \{1, \sqrt{a}\} & a \equiv 2, 3 \bmod 4 \\ \{1, (1+\sqrt{a})/2\} & a \equiv 1 \bmod 4 \end{cases}$$

The structure of the integers of biquadratic fields was determined by Kenneth Williams [27]. Let $\{a_1, a_2\}$ be set of generators for a biquadratic field, written in standard form and let $a_i' = a_i / \gcd(a_1, a_2)$ for $i = 1, 2$. Then an integral basis for $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2})$ is given by

$$\begin{array}{ll} \left\{1, \frac{1+\sqrt{a_1}}{2}, \frac{1+\sqrt{a_2}}{2}, \frac{1+\sqrt{a_1}+\sqrt{a_2}+\sqrt{a_1'a_2'}}{4}\right\} & a_1 \equiv a_2 \equiv a_1' \equiv a_2' \equiv 1 \bmod 4 \\ \left\{1, \frac{1+\sqrt{a_1}}{2}, \frac{1+\sqrt{a_2}}{2}, \frac{1-\sqrt{a_1}+\sqrt{a_2}+\sqrt{a_1'a_2'}}{4}\right\} & a_1 \equiv a_2 \equiv 1 \bmod 4,\ a_1' \equiv a_2' \equiv 3 \bmod 4 \\ \left\{1, \sqrt{a_1}, \frac{1+\sqrt{a_2}}{2}, \frac{\sqrt{a_1}+\sqrt{a_1'a_2'}}{2}\right\} & a_1 \equiv 2 \bmod 4,\ a_2 \equiv 1 \bmod 4 \\ \left\{1, \sqrt{a_1}, \sqrt{a_2}, \frac{\sqrt{a_1}+\sqrt{a_1'a_2'}}{2}\right\} & a_1 \equiv 2 \bmod 4,\ a_2 \equiv 3 \bmod 4 \\ \left\{1, \sqrt{a_1}, \frac{\sqrt{a_1}+\sqrt{a_2}}{2}, \frac{1+\sqrt{a_1'a_2'}}{2}\right\} & a_1 \equiv a_2 \equiv 3 \bmod 4 \end{array}$$

If $K$ is an $n$-quadratic field with $n > 2$, it becomes increasingly difficult to determine an integral basis for $\mathcal{O}_K$.

In [22], Schmal discusses the integral bases of $n$-quadratic fields. In particular, given an $n$-quadratic field $K$ and an $m$-quadratic subfield $K_0$ of $K$, he discusses in detail when there exists a relative integral basis of $\mathcal{O}_K$ over $\mathcal{O}_{K_0}$. In the case when $m = n - 1$ (i.e. when $K$ is a quadratic extension of $K_0$) he gives a full description of this relative integral basis, when it exists. For example, in the case where $K_0 = \mathbb{Q}(\sqrt{14}, \sqrt{105})$ and $K = K_0(\sqrt{65})$, he proves that a relative integral basis for $K/K_0$ is

$$\left\{1, \frac{3}{4} + \frac{1}{4}\sqrt{105} + \sqrt{65} + \frac{1}{2}\sqrt{273}\right\}.$$

In addition to Schmal's results, we can determine some aspects of the structure of $\mathcal{O}_K$ in a more concrete fashion. We begin with a useful alternative definition of algebraic integer.

**Definition 2.3.1.** A number $\alpha$ is an *algebraic integer* if and only if $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module.

**Proposition 2.3.2.** *Let $L$ and $K$ be number fields such that $L$ is a degree 2 extension of $K$. For any $\alpha \in L$ the following are equivalent:*

*(1) $\alpha \in \mathcal{O}_L$,*

*(2) $N_{L/K}(\alpha)$ and $T_{L/K}(\alpha)$ are elements of $\mathcal{O}_K$.*

*Proof.* First, if $\alpha \in \mathcal{O}_L$, it is clear that $N_{L/K}(\alpha)$ and $T_{L/K}(\alpha)$ are also algebraic integers and thus elements of $\mathcal{O}_K$.

Now assume $N_{L/K}(\alpha), T_{L/K}(\alpha) \in \mathcal{O}_K$. Let $\sigma : L \hookrightarrow \mathbb{C}$ be the nontrivial embedding of $L$ into $\mathbb{C}$ which fixes $K$. Then the minimal polynomial of $\alpha$ over $K$ is

$$\begin{aligned}(x-\alpha)(x-\sigma(\alpha)) &= x^2 - (\alpha+\sigma(\alpha))x + \alpha\sigma(\alpha) \\ &= x^2 - T_{L/K}(\alpha)x + N_{L/K}(\alpha).\end{aligned}$$

Since the coefficients of this polynomial are elements of $\mathcal{O}_K$, we have that $\alpha^2$ can be written as an $\mathcal{O}_K$-linear combination of $1, \alpha$,

$$\mathbb{Z}[\alpha] = \mathcal{O}_K \oplus \alpha\mathcal{O}_K.$$

Let $\{b_1, ..., b_n\}$ be an integral baiss for $\mathcal{O}_K$. Then

$$\mathcal{O}_K = b_1\mathbb{Z} \oplus \cdots \oplus b_n\mathbb{Z},$$

so

$$\mathbb{Z}[\alpha] = b_1\mathbb{Z} \oplus \cdots \oplus b_n\mathbb{Z} \oplus (\alpha b_1)\mathbb{Z} \oplus \cdots \oplus (\alpha b_n)\mathbb{Z}$$

is a finitely generated $\mathbb{Z}$-module and therefore $\alpha \in \mathcal{O}_L$. □

**Proposition 2.3.3.** *Let $K$ be an $n$-quadratic field with $n > 2$ and radicand list $\{a_1, ..., a_n\}$ written in standard form. Let $\{m_1, ..., m_{2^n-1}\}$ be a complete radicand list for $K$. Then any nonzero element $z$ of $\mathcal{O}_K$ can be written*

$$z = \frac{x_0 + x_1\sqrt{m_1} + \cdots + x_{2^n-1}\sqrt{m_{2^n-1}}}{2^{k_z}}$$

*for some* $k_z \in \mathbb{Z}_{\geq 0}$ *and* $x_0, ..., x_{2^n-1} \in \mathbb{Z}$ *such that at least one* $x_i$ *is not divisible by 2. Then the maximum* $k = \max\{k_z : z \in \mathcal{O}_K \setminus \{0\}\}$ *exists and we have:*

*(1) If* $a_i \equiv 1 \bmod 4$ *for all* $i \in \{1, ..., n\}$ *then* $k = n$. *Further if for any* $z \in \mathcal{O}_K$ *we write*

$$z = \frac{x'_0 + x'_1\sqrt{m_1} + \cdots + x'_{2^n-1}\sqrt{m_{2^n-1}}}{2^k}$$

*for* $x'_0, ..., x'_{2^n-1} \in \mathbb{Z}$ *then* $x'_0 \equiv x'_1 \equiv \cdots \equiv x'_{2^n-1} \bmod 2$.

*(2) If* $a_1 \not\equiv 1 \bmod 4$ *then* $k = n - 1$.

**Remark 2.3.4.** Note that the above proposition includes all possible $n$-quadratic fields. Since the radicand list $\{a_1, ..., a_n\}$ is written in standard form, then either $a_i \equiv 1 \bmod 4$ for all $i$, or if any $a_i \not\equiv 1 \bmod 4$ then we always have that $a_1 \not\equiv 1 \bmod 4$.

**Remark 2.3.5.** The above proposition does not completely classify the integers of $n$-quadratic fields; it gives necessary, but not sufficient information to know the structure of the integers.

*Proof.* For any $\theta \in \mathcal{O}_K$ there exist rational numbers $r_0, r_1, ..., r_{2^n-1}$ such that

$$\theta := r_0 + r_1\sqrt{m_1} + \cdots + r_{2^n-1}\sqrt{m_{2^n-1}}.$$

Let $k_i := \mathbb{Q}(\sqrt{m_i})$, $1 \leq i \leq 2^n - 1$. Since $\theta$ is an algebraic integer, the relative trace of $\theta$ down to the field $k_i$ will also be equal to an algebraic integer. Thus for any $i$,

$$T_{K/k_i}(\theta) = 2^{n-1}r_0 + 2^{n-1}r_i\sqrt{m_i} \in \mathcal{O}_{k_i}.$$

Now if $m_i \equiv 2, 3 \bmod 4$, then $\mathcal{O}_{k_i}$ has integral basis $\{1, \sqrt{m_i}\}$ so $T_{K/k_i}(\theta) \in \mathcal{O}_{k_i}$ if and only if $2^{n-1}r_0$ and $2^{n-1}r_i$ are rational integers. Similarly, if $m_i \equiv 1 \bmod 4$, then $\mathcal{O}_{k_i}$ has integral basis $\{1, \frac{1}{2}\left(1 + \sqrt{m_i}\right)\}$ so this relative trace is an integer if and only if

$$\frac{1}{2}\left(2^n r_0 + 2^n r_i\sqrt{m_i}\right) \in \mathcal{O}_{k_i}.$$

This implies that $2^n r_0, 2^n r_i \in \mathbb{Z}$ and $2^n r_0 \equiv 2^n r_i \mod 2$.

Using these observations, we will look at the two cases stated in the proposition:

(1) First consider the case where $a_j \equiv 1 \bmod 4$ for all $j \in \{1, ..., n\}$. Then for any $J \subseteq \{1, ..., n\}$ the squarefree part of the product $\prod_{j \in J} a_j$ will also be congruent to 1 mod 4, so

$$m_1 \equiv \cdots \equiv m_{2^n-1} \equiv 1 \bmod 4.$$

This implies that for any $i \in \{1, ..., 2^n - 1\}$, $2^n r_0, 2^n r_i \in \mathbb{Z}$, so $r_i$ is of the form $x_i/2^n$ for some $x_i \in \mathbb{Z}$ and $r_0$ can be written $x_0/2^n$ for $x_0 \in \mathbb{Z}$. Further, $2^n r_0 \equiv 2^n r_i \mod 2$ for each $i$, or equivalently, $x_0 \equiv x_i \bmod 2$. Thus

$$x_0 \equiv \cdots \equiv x_{2^n-1} \bmod 2.$$

(2) Now consider the case where $a_1 \not\equiv 1 \bmod 4$. Then $I := \{1, ..., 2^n - 1\}$ is equal to the union of the two disjoint nonempty sets

$$I_1 := \{i \in I | m_i \equiv 1 \bmod 4\}$$

and

$$I_{2,3} = \{i \in I | m_i \equiv 2, 3 \bmod 4\}.$$

Then for any $i \in I_1 \cup \{0\}$, $r_i$ can be written $x_i'/2^n$ with $x_i' \in \mathbb{Z}$ and all $x_i'$ congruent mod 2. Also, for any $i \in I_{2,3} \cup \{0\}$, $r_i$ can be written $x_i/2^{n-1}$ with $x_i \in \mathbb{Z}$. Thus

$$r_0 = \frac{x_0}{2^{n-1}} = \frac{2x_0}{2^n} = \frac{x_0'}{2^n},$$

so $x_0'$ is even. Therefore, for each $i \in I_1$, $x_i'$ is even; let $x_i := x_i'/2 \in \mathbb{Z}$. Then we have shown we can write each $r_i$, $i \in I \cup \{0\}$ in the form $x_i/2^{n-1}$ for $x_i \in \mathbb{Z}$.

□

## 2.4 Ramification and splitting of primes

Let $K$ be any number field of degree $n$ with integral basis $\{b_1, ..., b_n\}$ and let $\sigma_1, ..., \sigma_n$ be the embeddings $K \hookrightarrow \mathbb{C}$ which fix $\mathbb{Q}$. The *discriminant* of $K$ is defined to be

$$\Delta_K = \Delta(b_1, , b_2, ..., b_n) = \begin{vmatrix} \sigma_1(b_1) & \sigma_1(b_2) & \dots & \sigma_1(b_n) \\ \sigma_2(b_1) & \sigma_2(b_2) & \dots & \sigma_2(b_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(b_1) & \sigma_n(b_2) & \dots & \sigma_n(b_n) \end{vmatrix}^2.$$

The discriminant of a number field is important when studying the ramification of primes since a prime $p \in \mathbb{Z}$ ramifies in $\mathcal{O}_K$ if and only if $p|\Delta_K$.

In the case of a quadratic field $\mathbb{Q}(\sqrt{a})$, with $a$ squarefree, we have

$$\Delta_{\mathbb{Q}(\sqrt{a})} = \begin{cases} a & : a \equiv 1 \bmod 4 \\ 4a & : a \equiv 2, 3 \bmod 4 \end{cases}$$

Thus we know precisely when a rational prime ramifies in a quadratic field. In particular, for any prime $p$, if $p|a$ then

$$p\mathcal{O}_{\mathbb{Q}(\sqrt{a})} = (p, \sqrt{a})^2.$$

Additionally, if $a \equiv 3 \bmod 4$

$$2\mathcal{O}_{\mathbb{Q}(\sqrt{a})} = (2, 1 + \sqrt{a})^2.$$

Further, we can completely describe the splitting of primes in quadratic fields; for the proof of this see chapter 3 of [19]. First, if $a \equiv 2, 3 \pmod 4$ we know that (2) ramifies, so (2) will only split when $a \equiv 1 \pmod 4$. In fact, we have that

$$2\mathcal{O}_{\mathbb{Q}(\sqrt{a})} = \begin{cases} \left(2, \frac{1+\sqrt{a}}{2}\right)\left(2, \frac{1-\sqrt{a}}{2}\right) & a \equiv 1 \bmod 8 \\ (2) & a \equiv 5 \bmod 8 \end{cases}$$

Also, if $p$ is any odd prime and $p \nmid a$ then

$$p\mathcal{O}_{\mathbb{Q}(\sqrt{a})} = \begin{cases} (p, n + \sqrt{a})\,(p, n - \sqrt{a}) & a \equiv n^2 \bmod p \text{ for some } n \in \mathbb{Z} \\ (p) & a \text{ is not a square mod } p \end{cases}.$$

To understand the ramification of primes in multiquadratic fields, we consider the following theorem due to Schmal [22].

**Theorem 2.4.1.** *Let $K$ be an $n$-quadratic field with radicand list $\{a_1, a_2, ..., a_n\}$ written in standard form. Let $\prod_{j=1}^{s} p_j^{m_j}$ be the prime factorization in $\mathbb{Z}$ of the product of the radicands, $\prod_{i=1}^{n} a_i$. Then*

$$\Delta_K = (2^e p_1 \cdots p_s)^{2^{n-1}},$$

*where*

$$e = \begin{cases} 0 & : a_1 \equiv 1 \bmod 4 \\ 2 & : (a_1, a_2) \equiv (2,1) \text{ or } (3,1) \bmod 4 \\ 3 & : (a_1, a_2) \equiv (2,3) \bmod 4 \end{cases}$$

Thus we can conclude

**Corollary 2.4.2.** *Let $K$ be an $n$-quadratic field with radicand list $\{a_1, a_2, ..., a_n\}$ written in standard form. For any prime $p \in \mathbb{Z}$ the following describes the inertia field of $K$ with respect to the prime $p$ and the ramification index of $p$ in $\mathcal{O}_K$:*

*First, when $p = 2$ we have:*

*(1) If $a_1 \equiv a_2 \equiv \cdots \equiv a_n \equiv 1 \pmod 4$ then $(2)$ is unramified in $\mathcal{O}_K$ and the inertia field is $K$.*

*(2) If $a_1 \not\equiv 1 \pmod 4$ and $a_i \equiv 1 \pmod 4$, $2 \leq i \leq n$, then $2\mathcal{O}_K$ has ramification index 2 and the inertia field is the $(n-1)$-quadratic field $\mathbb{Q}(\sqrt{a_2}, ..., \sqrt{a_n})$.*

*(3) If $a_1 \equiv 2 \pmod 4$ and $a_i \equiv 3 \pmod 4$, $2 \leq i \leq n$, then $2\mathcal{O}_K$ has ramification index 4. The inertia field is the $(n-2)$-quadratic field $\mathbb{Q}(\sqrt{a_2 a_3}, ..., \sqrt{a_2 a_n})$.*

*When $p$ is an odd prime we have:*

*(1) If $p \nmid a_i$ for all $i \in \{1, ..., n\}$ then $(p)$ is unramified in $\mathcal{O}_K$ and the inertia field is $K$.*

*(2) Otherwise $p\mathcal{O}_K$ has ramification index 2. Let $\{a_1', ..., a_n'\}$ be a $p$-headed radicand list for $K$, then the $(n-1)$-quadratic field $\mathbb{Q}(\sqrt{a_2'}, ..., \sqrt{a_n'})$ is the inertia field of $K$ for $p$.*

To better understand how primes behave in multiquadratic fields we can use the following theorem from [19], p. 107.

**Theorem 2.4.3.** *Let $K$ be a number field and let $L$ and $M$ be two extensions of $K$. Fix a prime $p$ of $K$. If $p$ is unramified in both $L$ and $M$ then $p$ is unramified in the composite field $LM$. If $p$ splits completely in both $L$ and $M$ then $p$ splits completely in $LM$.*

First we will discuss the splitting of the prime (2) in $K$. If $K$ is a multiquadratic number field and $K_E$ is the inertia field of the prime (2) then there are two cases which may occur. First, we may have $K_E = \mathbb{Q}$ which implies that (2) is completely ramified in $K$, and the decomposition field $K_D$ of (2) is also equal to $\mathbb{Q}$. If $K_E$ is not trivial then we may write $K_E = \mathbb{Q}(\sqrt{a_1}, ..., \sqrt{a_m})$ where $\{a_1, ..., a_m\}$ is a primitive radicand list for $K_E$, and $m$ satisfies $(n-2) \leq m \leq n$. Note from the above corollary that $a_i \equiv 1 \pmod 4$, $1 \leq i \leq m$.

**Proposition 2.4.4.** *Let $K$ be a multiquadratic field such that (2) is not completely ramified in $K$. Let $K_E$ be the inertia field of the prime (2); write $K_E = \mathbb{Q}(\sqrt{a_1}, ..., \sqrt{a_m})$ where $\{a_1, ..., a_m\}$ is a primitive radicand list for $K_E$. Then $a_i \equiv 1 \pmod 4$, $1 \leq i \leq m$, and the decomposition field $K_D$ of the prime (2) is given by:*

*(i) If $a_i \equiv 1 \pmod 8$ for all $i \in \{1, ..., m\}$ then (2) splits completely in $K_E$; i.e. $K_D = K_E$.*

*(ii) if $a_i \equiv 5 \pmod 8$ for any $i \in \{1, ..., m\}$ then (2) splits completely in an $(m-1)$-quadratic field, but not in $K_E$. We have $K_D = \mathbb{Q}\left(\sqrt{a'_1}, ...\sqrt{a'_{i-1}}, \sqrt{a'_{i+1}}, ..., \sqrt{a'_m}\right)$ where $a'_j$ for $j \in \{1, ..., i-1, i+1, ..., m\}$ is given by*

$$a'_j = \begin{cases} a_j & : a_j \equiv 1 \pmod 8 \\ s.f.(a_i a_j) & : a_j \equiv 5 \pmod 8 \end{cases}$$

*Proof.* Note that the decomposition fields defined in this proposition are multiquadratic fields such that each radicand is congruent to 1 mod 8. Since (2) splits completely in a quadratic field $\mathbb{Q}(\sqrt{a})$ with $a \equiv 1 \pmod 8$ and a multiquadratic field with all radicands congruent to 1 mod 8 is a

product of these quadratic fields, then Theorem 2.4.3 tells us that (2) willl split completely in a multiquadratic field of this form.

Thus we have proven part (i) of this proposition: (2) splits completely in $K_D = K_E$, and since the decomposition field must be a subfield of the inertia field, $K_D$ must be exactly this field $K_E$.

To prove part (ii) of this proposition, first note that from the above discussion (2) splits completely in the field $K_D$ given in the proposition. Also, (2) is inert in some quadratic subfield $\mathbb{Q}(\sqrt{a})$ of $K_E$ since $K_E$ has at least one radicand $a \equiv 5 \pmod 8$. Therefore (2) does not split completely in $K_E$ which implies that $K_D$ must be a proper subfield of $K_E$. Thus the field $K_D$ described in case (ii) is the largest subfield of $K$ such that (2) splits completely, so it is the decomposition field. □

Now let's investigate the decomposition field of $K$ for an odd prime $(p)$. As in the case of quadratic fields, the splitting of $(p)$ will be based entirely on whether or not the radicands are quadratic residues mod $p$. Recall that the inertia field in this case is an $m$-quadratic field $K_E = \mathbb{Q}(\sqrt{a_1}, ..., \sqrt{a_m})$ with $p \nmid a_i$, $1 \leq i \leq m$, and also that $m = n$ or $m = n - 1$.

**Proposition 2.4.5.** *Let $p \in \mathbb{Z}$ be an odd prime and $K$ be a multiquadratic field. Write the inertia field $K_E$ of $K$ for the prime $(p)$ as $K_E = \mathbb{Q}(\sqrt{a_1}, ..., \sqrt{a_m})$ with $\{a_1, ..., a_m\}$ a primitive radicand list. Then the decomposition field $K_D$ for the prime $(p)$ is given by:*

*(i) If $\left(\frac{a_i}{p}\right) = 1$ for all $i \in \{1, ..., m\}$ then $K_D = K_E$.*

*(ii) If there exists $i \in \{1, ..., m\}$ such that $\left(\frac{a_i}{p}\right) = -1$ then $(p)$ splits completely in an $(m-1)$-quadratic field, but not in $K_E$. We have $K_D = \mathbb{Q}\left(\sqrt{a'_1}, ...\sqrt{a'_{i-1}}, \sqrt{a'_{i+1}}, ..., \sqrt{a'_m}\right)$ where $a'_j$ for $j \in \{1, ..., i-1, i+1, ..., m\}$ is given by*

$$a'_j = \begin{cases} a_j & : \left(\frac{a_j}{p}\right) = 1 \\ s.f.(a_i a_j) & : \left(\frac{a_j}{p}\right) = -1 \end{cases}$$

*Proof.* We can see that (i) is true by observing that $(p)$ splits completely in all quadratic subfields of $K_D$ and applying Theorem 2.4.3. Since in this case $K_D = K_E$ then $K_D$ must be the maximal subfield of $K$ such that $(p)$ splits completely, and is thus the decomposition field.

For case (ii) first observe that all radicands $a$ of the field $K_D$ described satisfy $\left(\frac{a}{p}\right) = 1$ by the fact that the Legendre symbol is completely multiplicative. Thus applying Theorem 2.4.3 we have that $(p)$ splits completely in $K_D$. Also $(p)$ does not split completely in $K_E$ since $K_E$ has a radicand which is not a square mod $p$. This implies that $K_D$ must be a proper subfield of $K_E$. Thus the field $K_D$ described in case (ii) is the largest subfield of $K$ such that (2) splits completely, so it is the decomposition field. □

We also include two more lemmas. These will be cited in the following chapter to prove larger results:

**Lemma 2.4.6.** *Let $K$ be an $n$-quadratic field. Then:*

*(1) If $K$ is totally real, the number of primes ramified in $K$ is at least $n$.*

*(2) If $K$ is imaginary, the number of primes ramified in $K$ is at least $n-1$.*

*Proof.* First note that if we can prove (1) then (2) immediately follows. That is, if $K$ is an imaginary $n$-quadratic field, then $K$ has a real $(n-1)$-quadratic subfield. Assuming that (1) holds it follows that there are at least $n-1$ primes ramified in this subfield and thus in $K$.

Thus it only remains to prove this lemma for real $n$-quadratic fields. Let $K$ be a real $n$-quadratic field with primitive radicand list $\{a_1, ..., a_n\}$, $a_i > 1$ squarefree for $1 \leq i \leq n$. Then it follows, from Corollary 2.4.2, that every prime which divides the product $\pi_K = \prod_{i=1}^{n} a_i$ ramifies in $K$. Therefore, it is sufficient to prove that at least $n$ primes divide the product $\pi_K$.

We will prove this by induction on $n$. First if $\mathbb{Q}(\sqrt{a_1})$ is a real quadratic field then clearly at least one prime divides the product $\pi_{\mathbb{Q}(\sqrt{a_1})} = a_1$. Assume that for any real $(n-1)$-quadratic field $L$, there are at least $(n-1)$ primes dividing the product of the radicands $\pi_L$. Now consider the real $n$-quadratic field $K$. Then we can clearly see that at least one prime $p$ divides the product $\pi_K$.

Thus there exists a $p$-headed radicand list $\{a_1', a_2', ..., a_n'\}$ such that $p|a_1'$ but $p \nmid a_i'$ for $2 \leq i \leq n$. Then there is an $(n-1)$-quadratic subfield $K'$ of $K$ with radicand list $\{a_2', ..., a_n'\}$. Since there are at least $n-1$ primes dividing $\pi_{K'}$ and none of these primes are equal to $p$, then there must be at least $n$ primes dividing $\pi_K$. □

**Lemma 2.4.7.** *Let $K$ be an imaginary $n$-quadratic field with $n \geq 3$. There exists an odd prime $p$ and a real $(n-2)$-quadratic subfield $k$ of $K$ such that $p$ is unramified in $k$ but is ramified in $K$.*

*Proof.* By Lemma 2.4.6 there are at least $n-1$ primes which ramify in $K$. Since $n \geq 3$ we have that at least two primes ramify in $K$, and thus at least one of these primes must be odd. Choose any odd prime which ramifies in $K$ and denote it by $p$. By Corollary 2.4.2 there exists an $(n-1)$-quadratic subfield $K_E$ of $K$ which is the inertia field for $p$. If $K_E$ is totally real we may choose $k$ to be any $(n-2)$-quadratic subfield of $K_E$. If $K_E$ is imaginary write $K_E = \mathbb{Q}(\sqrt{-a_1}), ..., \sqrt{-a_{n-1}})$. Then we may choose $k = \mathbb{Q}\left(\sqrt{a_1 a_2}, ..., \sqrt{a_1 a_n}\right)$.

□

# Chapter 3

# Class Numbers of Multiquadratic Fields

## 3.1 Class Number

Let $K$ be a number field. There is an equivalence relation $\sim$ on the ideals of $\mathcal{O}_K$ which is defined in the following manner: If $I$ and $J$ are any two ideals of $\mathcal{O}_K$ then $I \sim J$ if and only if there exists $z_1, z_2 \in \mathcal{O}_K$ such that $z_1 I = z_2 J$.

The equivalence classes under $\sim$ are called the *ideal classes* of $K$. Denote by $h_K$ the number of ideal classes of $K$. This is called the *class number* of $K$. In the case of a quadratic field $\mathbb{Q}(\sqrt{a})$ with $a$ squarefree, we will denote the class number by $h(a)$ instead of $h_{\mathbb{Q}(\sqrt{a})}$.

All principal ideals of $\mathcal{O}_K$ are in the same ideal class; if $(z_1)$ and $(z_2)$ are any principal ideals of $\mathcal{O}_K$ then $(z_1) \sim (z_2)$ since $z_2(z_1) = z_1(z_2)$. On the other hand, no non-principal ideals are equivalent to a principal ideal under the relation $\sim$. Therefore we can also describe the ideal class group as the quotient

$$\frac{\{I : I \text{ is a fractional ideal of } \mathcal{O}_K\}}{\{I : I \text{ is a principal fractional ideal of } \mathcal{O}_K\}}.$$

One of the first known discussions of class numbers of number fields can be found in section V of Gauss's book *Disquisitiones Arithmeticae* [10] which was published in 1801. Using the language of quadratic forms, Gauss made several significant conjectures and proved some results about the class numbers of quadratic fields.

He proved that $h(a) = 1$ for $a \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$, and conjectured that there are no other imaginary quadratic fields with class number 1. This conjecture was proven

to be true by Stark in 1967 [23]. Gauss also conjectured that $h(a) \to \infty$ as $a \to -\infty$, and this was proven to be true by Heilbronn in 1934 [11]. This conjecture was proven in an unusual manner: by first showing it holds if the generalized Riemann hypothesis (GRH) is true, and then by showing it holds assuming the GRH is false.

Gauss also conjectured that there are infinitely many real quadratic fields of class number 1. This has not been proven to be true or false, though a lot of work has been done on this problem and these results support this conjecture. Some of the most famous work on this problem was done by Cohen and Lenstra in 1983. These results are a series of more specific conjectures on the class numbers of quadratic fields, called the Cohen-Lenstra Heuristics, and are well supported by numerical data. In particular, they conjecture that real quadratic fields with prime discriminant have class number 1 close to 75.446% of the time. For a more in-depth discussion see chapter 5, section 10 of Cohen's book [6].

One of the most famous results on class numbers is the analytic class number formula. This was proven by Dirichlet in 1839, though it was first conjectured by Jacobi. A complete discussion can be found on pages 43-53 of [7].

**Theorem 3.1.1** (Analytic Class Number Formula)**.** *Let $K$ be a number field and denote by $w_K$ is the number of roots of unity in $K$. Further, let $Reg_K$ be the regulator $K$. Then*

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} h_K Reg_K}{w_K\sqrt{|\Delta_K|}}.$$

Recall that $\zeta_K$ is the *Dedekind zeta function* of $K$, which is given by

$$\zeta_K(s) = \sum_{\substack{0\subset I\subseteq\mathcal{O}_K \\ I \text{ an ideal}}} \frac{1}{\left(N_{K/\mathbb{Q}}(I)\right)^s}$$

In the case of a quadratic number field $\mathbb{Q}(\sqrt{a})$ the analytic class number formula gives us:

$$h(a) = \begin{cases} \frac{\sqrt{|\Delta_K|}}{\pi} L(1,\chi) & a = -2 \text{ or } a < -4 \\ \frac{3\sqrt{3}}{\pi} L(1,\chi) & a = -3 \\ \frac{4}{\pi} L(1,\chi) & a = -1 \\ \frac{\sqrt{|\Delta_K|}}{\log\epsilon} L(1,\chi) & a > 1 \end{cases}$$

where

$$L(1,\chi) = \sum_{n=1}^{\infty} \left(\frac{\Delta_K}{n}\right) n^{-1}.$$

The series $L(1,\chi)$ can sometimes be evaluated directly, reduced to a finite sum or bounded from below.

## 3.2 Results for Multiquadratic Fields

In 1974, Brown and Parry determined a complete list of imaginary biquadratic number fields with class number 1 [3]. There are exactly 47 such fields and they are given by $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2})$ where the pairs $(a_1, a_2)$ appear in the following table:

| $(a_1, a_2)$ | $(a_1, a_2)$ | $(a_1, a_2)$ | $(a_1, a_2)$ | $(a_1, a_2)$ |
|---|---|---|---|---|
| (-1,2) | (2,-3) | (-3,5) | (-7,5) | (-11,17) |
| (-1,3) | (2,-11) | (-3,-7) | (-7,-11) | (-11,-19) |
| (-1,5) | (-2,-3) | (-3,-11) | (-7,13) | (-11,-67) |
| (-1,7) | (-2,5) | (-3,17) | (-7,-19) | (-11,-163) |
| (-1,11) | (-2,-7) | (-3,-19) | (-7,-43) | (-19,-67) |
| (-1,13) | (-2,-11) | (-3,41) | (-7,61) | (-19,-163) |
| (-1,19) | (-2,-19) | (-3,-43) | (-7,-163) | (-43,-67) |
| (-1,37) | (-2,29) | (-3,-67) | | (-43,-163) |
| (-1,43) | (-2,-43) | (-3,89) | | (-67,-163) |
| (-1,67) | (-2,-67) | (-3,-163) | | |
| (-1,163) | | | | |

Brown and Parry determined this list using techniques of Herglotz [12] who gives a formula that relates the class number of a biquadratic number field to that of its quadratic subfields, along with some other parameters. Below is a more general version of this formula as presented by Lemmermeyer [17], and it is used later in this chapter to determine a list of all other imaginary multiquadratic number fields of class number 1:

**Theorem 3.2.1.** *(Kuroda's Class Number Formula) For any number field $L$ define $E(L)$ to be the unit group of $\mathcal{O}_L$. Let $K/k$ be a $V_4$ extension of number fields and let $k_i$, $i \in \{1,2,3\}$, be the three number fields such that $k \subsetneq k_i \subsetneq K$. Let $h_i$ denote the class number of $k_i$, $i \in \{1,2,3\}$, and $h_k$ denote the class number of $k$. Then we have*

$$h(K) = 2^{d-\kappa-2-\nu} q(K/k) h_1 h_2 h_3 / h_k^2,$$

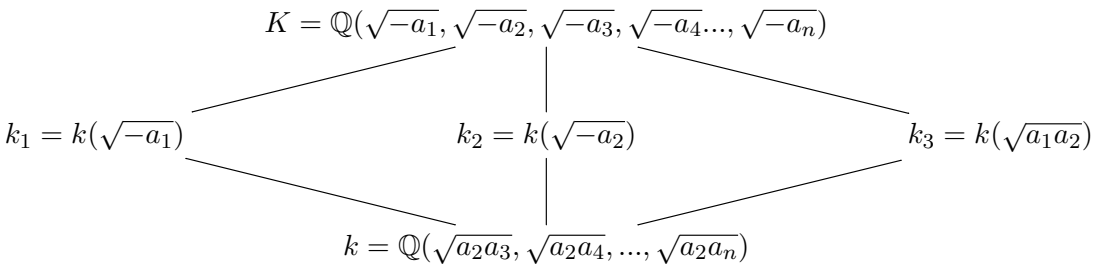
*where $q(K/k)$ is the (finite) unit index given by $q(K/k) := [E(K) : E(k_1)E(k_2)E(k_3)]$, $d$ denotes the number of infinite places ramified in $K/k$, $\kappa$ is the $\mathbb{Z}$-rank of $E(k)$ and*

$$\nu = \begin{cases} 1 & \text{if } K = k(\sqrt{\epsilon}, \sqrt{\eta}),\ \epsilon, \eta \in E(k) \\ 0 & \text{otherwise.} \end{cases}$$

*In particular,*

$$h(K) = \begin{cases} \frac{1}{4} q(K/\mathbb{Q}) h_1 h_2 h_3 & \text{if } k = \mathbb{Q} \text{ and } K \text{ is real,} \\ \frac{1}{2} q(K/\mathbb{Q}) h_1 h_2 h_3 & \text{if } k = \mathbb{Q} \text{ and } K \text{ is complex,} \\ \frac{1}{4} q(K/k) h_1 h_2 h_3 / h_k^2 & \text{if } k \text{ is a complex quadratic extension of } \mathbb{Q}. \end{cases}$$

**Remark 3.2.2.** In the next section, we will apply this theorem to imaginary $n$-quadratic fields $K$ viewed as a $V_4$ extension over a real $(n-2)$-quadratic field $k$:




In this case, it is easy to see that the unit index $q(K/k)$ is finite. By Dirichlet's unit theorem, the unit groups $E(K)$ and $E(k_3)$ have the same rank. Since these are finitely generated abelian groups with $E(k_3) \subseteq E(K)$ we clearly have that $[E(K) : E(k_1)E(k_2)E(k_3)] \in \mathbb{Z}_{>0}$.

Mouhib studied the 2-part of the ideal class group of real 4-quadratic fields with prime radicands. He proved the following theorem [20]:

**Theorem 3.2.3.** *Let $p_1, p_2, p_3, p_4 > 0$ be distinct primes and $K = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}, \sqrt{p_4})$. Then the 2-class group of $K$ is trivial if and only if, after a suitable permutation of the indices, the $p_i$ have one of the following properties:*

*(1)* $p_1 = 2$, $p_2 \equiv p_3 \equiv p_4 \equiv -1 \pmod 4$, $\left(\frac{2}{p_2}\right) = -\left(\frac{2}{p_3}\right) = -\left(\frac{2}{p_4}\right) = 1$ *and* $\left(\frac{p_2}{p_3}\right)\left(\frac{p_2}{p_4}\right) = -1$

*(2)* $p_1 = 2$, $p_2 \equiv p_3 \equiv p_4 \equiv -1 \pmod 4$, $\left(\frac{2}{p_2}\right) = -1$, *and*

*(i)* $\left(\frac{p_2}{p_3}\right) = \left(\frac{p_2}{p_4}\right) = -1$ *and* $\left(\frac{2}{p_3}\right)\left(\frac{2}{p_4}\right) = -1$, *or*

*(ii)* $\left(\frac{2}{p_3}\right) = \left(\frac{2}{p_4}\right) = -1$ *and* $\left(\frac{p_2}{p_3}\right)\left(\frac{p_2}{p_4}\right) = -1$, *or*

*(iii)* $\left(\frac{p_2}{p_3}\right)\left(\frac{p_2}{p_4}\right) = \left(\frac{2}{p_3}\right)\left(\frac{2}{p_4}\right) = -1$ *and* $\left(\frac{p_2}{p_3}\right) \neq \left(\frac{2}{p_3}\right)$.

## 3.3 A Special Case of Kuroda's Class Number Formula

Before reading the following lemma, it is helpful to be reminded of the statement of Lemma 2.4.7: If $K$ is an imaginary $n$-quadratic field with $n \geq 3$ then there exists a real $(n-2)$-quadratic subfield $k$ of $K$ and an odd prime $p$ such that $p$ ramifies in $K$ but not in $k$.

**Lemma 3.3.1.** *Let $K$ be an imaginary $n$-quadratic field with $n \geq 3$. Let $k$ be any real $(n-2)$-quadratic subfield of $K$ such that there exists an odd prime which ramifies in $K/k$. Then we have the following formula for the class number $h(K)$ of $K$:*

$$h(K) = \frac{1}{2} q(K/k) h_1 h_2 h_3 / h_k^2.$$

*Here $h_k$ is the class number of $k$, $h_1, h_2, h_3$ are the class numbers of the three $(n-1)$-quadratic fields $k_1, k_2, k_3$ between $k$ and $K$, and $q(K/k) = [E(K) : E(k_1)E(k_2)E(k_3)]$.*

*Proof.* Since $K/k$ is a $V_4$ extension of number fields we may apply Kuroda's class number formula:

$$h(K) = 2^{d-\kappa-2-\nu} q(K/k) h_1 h_2 h_3 / h_k^2,$$

where $\kappa$ is the $\mathbb{Z}$-rank of the unit group $E(k)$, $d$ is the number of infinite places ramified in $K/k$ and

$$\nu = \begin{cases} 1 & \text{if } K = k(\sqrt{\epsilon}, \sqrt{\eta}),\ \epsilon, \eta \in E(k) \\ 0 & \text{otherwise.} \end{cases}$$

Since $\kappa$ is the $\mathbb{Z}$-rank of the unit group $E(k)$, we may apply Dirichlet's unit theorem and find that $\kappa = 2^{n-2} - 1$. Next, recall that $d$ is the number of infinite places ramified in $K/k$. Now there are $2^{n-2}$ distinct infinite places in $k$ since it is a real $(n-2)$-quadratic field; call these embeddings $\sigma_1, ..., \sigma_n : k \hookrightarrow \mathbb{R}$. Each $\sigma_i$, $i = 1, ..., 2^{n-2}$ is going to extend to an embedding $\tau_i : K \hookrightarrow \mathbb{C}$. Now $\tau_i$ is complex embedding since $K$ is an imaginary $n$-quadratic field, so if $\tau_i$ lies over $\sigma_i$, then $\overline{\tau_i}$ also lies over $\sigma_i$. We know $\tau_i$ and $\overline{\tau_i}$ correspond to the same infinite place in $K$, so $\sigma_i$ must be ramified for all $i \in \{1, ..., 2^{n-2}\}$. Therefore, there are $2^{n-2}$ infinite places which ramify in $K$, forcing $d = 2^{n-2}$.

Plugging these quantities into the formula we have

$$h(K) = \frac{1}{2} 2^{-\nu} q(K/k) h_1 h_2 h_3 / h_k^2.$$

Thus we wish to show $\nu = 0$ to get the desired result. Denote by $p$ an odd prime which ramifies in $K$ but not in $k$. There exists a $p$-headed radicand list $\{a_1, a_2, ..., a_n\}$ for $K$. Further, we may assume this list is written so that $a_1 < 0$: since $K$ is imaginary then at least one $a_i < 0$, so if $a_1$ is positive, just replace it in the radicand list with $s.f.(a_1 a_i)$; the squarefree part of this product will still be divisible by $p$ since $p \nmid a_i$.

Recall that $\nu = 0$ if and only if $K$ cannot be written as $k(\sqrt{\eta}, \sqrt{\epsilon})$ for $\eta, \epsilon$ in $E(k)$, the unit group of $k$. I will show $\nu = 0$ by contradiction, so assume there exist units $\eta, \epsilon \in k$ such that $K = k(\sqrt{\eta}, \sqrt{\epsilon})$. Then the element $\sqrt{a_1} \in K$ can be written

$$\sqrt{a_1} = w + x\sqrt{\eta} + y\sqrt{\epsilon} + z\sqrt{\epsilon\eta}, \ \ w, x, y, z \in k.$$

However, since $\sqrt{a_1}$ is purely imaginary and does not have a real part, we must have $w = 0$. Also, without loss of generality, since at most 2 of $\sqrt{\epsilon}$, $\sqrt{\eta}$ and $\sqrt{\epsilon\eta}$ can be imaginary, assume $z\sqrt{\epsilon\eta}$ is real and thus $z = 0$ as well. Therefore

$$\sqrt{a_1} = x\sqrt{\eta} + y\sqrt{\epsilon}, \ \ x, y \in k.$$

There are two cases to consider: first, the case where both $x$ and $y$ are nonzero, and second, when exactly one of $x$ or $y$ is zero. If $x, y \neq 0$, then squaring both sides gives

$$a_1 = x^2\eta + y^2\epsilon + 2xy\sqrt{\eta\epsilon}.$$

Now since $a_1, x^2\eta, y^2\epsilon \in k$ and

$$a_1 - x^2\eta - y^2\epsilon = 2xy\sqrt{\eta\epsilon}$$

then we must have $\sqrt{\eta\epsilon} \in k$, so

$$K = k(\sqrt{\eta}, \sqrt{\epsilon}) = k(\sqrt{\eta}, \sqrt{\eta\epsilon}) = k(\sqrt{\eta}).$$

Thus $K$ is a degree 2 extension of $k$; which is a contradiction, because we know $K/k$ is a $V_4$ extension.

Thus assume that exactly one of $x, y$ is zero; without loss of generality assume $y = 0$. Then $\sqrt{a_1} = x\sqrt{\epsilon}$, so

$$a_1 = x^2\epsilon.$$

This implies that $a_1$ is equal to a square in $\mathcal{O}_k$ which is a contradiction since there is an odd prime $p|a_1$ which does not ramify in $k$. Thus $\nu = 0$.

□

**Theorem 3.3.2.** *Keeping the notation above, we have*

$$h(K) = \left(\frac{1}{2}\right)^{2^{n-1}-1} QPh_3,$$

*where $P$ is the product of the class numbers of all imaginary quadratic subfields of $K$ and $Q \in \mathbb{Z}_{>0}$ is a product of unit indices $q(L/\ell)$ where $L/\ell$ are $V_4$ extensions with $L \subseteq K$.*

*Proof.* Proof by induction. Base case: when $n = 2$ it is easy to check that this theorem holds. Now assume that the statement holds for imaginary $(n-1)$-quadratic fields. Consider, in particular, the $(n-1)$-quadratic fields $k_1$ and $k_2$. Let $k'$ be an $(n-3)$-quadratic field such that there exists a prime $p$ which ramifies in $k$ but not in $k'$. Then $k_1/k'$ and $k_2/k'$ are $V_4$ extensions which have $k$ as a totally real intermediate field.

Then

$$h(k_1) = \left(\frac{1}{2}\right)^{2^{(n-1)-1}-1} Q_1P_1h_k,$$

$$h(k_2) = \left(\frac{1}{2}\right)^{2^{(n-1)-1}-1} Q_2 P_2 h_k.$$

Here, $P_i$, $i = 1, 2$ is the product of the class numbers of all imaginary quadratic subfields of $k_i$. Also, $Q_i \in \mathbb{Z}_{>0}$, $i = 1, 2$ are products of unit indices $q(L/\ell)$ where $L/\ell$ are $V_4$ extensions with $L \subseteq k_i \subset k$.

Then, using the fact that

$$h(K) = \frac{1}{2} q(K/k) h_1 h_2 h_3 / h_k^2,$$

and plugging in for $h_1$ and $h_2$, we find that

$$\begin{aligned} h(K) &= \frac{1}{2} q(K/k) \left( \left(\frac{1}{2}\right)^{2^{n-2}-1} Q_1 P_1 h_k \right) \left( \left(\frac{1}{2}\right)^{2^{n-2}-1} Q_2 P_2 h_k \right) h_3 / h_k^2 \\ &= \left(\frac{1}{2}\right)^{1+2^{n-2}-1+2^{n-2}-1} q(K/k) Q_1 P_1 Q_2 P_2 h_3 \\ &= \left(\frac{1}{2}\right)^{2^{n-1}-1} (q(K/k) Q_1 Q_2)(P_1 P_2) h_3. \end{aligned}$$

Setting $Q = q(K/k) Q_1 Q_2$ we have that $Q \in \mathbb{Z}_{>0}$ and is a product of unit indices $q(L/\ell)$ where $L/\ell$ are $V_4$ extensions with $L \subseteq K$. Also, setting $P = P_1 P_2$ we have that $P$ is a product of imaginary quadratic subfields of $K$. From Lemma 2.2.6 we know that $k_1$ and $k_2$ each have $2^{n-2}$ imaginary quadratic subfields and $K$ has $2^{n-1}$ imaginary quadratic subfields. Further, we see that the set of imaginary quadratic subfields of $k_1$ and $k_2$ are disjoint. This is because both of these fields are imaginary quadratic extensions of the same totally real field $k$, and thus these imaginary quadratic extensions must be distinct and not produce any of the same imaginary quadratic subfields. Thus the product $P_1 P_2$ is the product of the class numbers of $2 \cdot 2^{n-2} = 2^{n-1}$ distinct imaginary quadratic subfields of $K$, which is all of the imaginary quadratic subfields of $K$. Therefore $P = P_1 P_2$ is the product of the class numbers of all imaginary quadratic subfields of $K$.

□

## 3.4 The Imaginary Triquadratic Fields of Class Number 1

In this section, we will apply the above formulas to determine a complete list of the imaginary triquadratic fields of class number 1. We will also use the following information about the class

number of imaginary quadratic fields:

Recall, from section 1 that the imaginary quadratic fiels of class number 1 are $\mathbb{Q}(\sqrt{-a})$ with $a \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$. Also:

**Lemma 3.4.1.** *The imaginary quadratic fields of class number 2 are given by* $\mathbb{Q}(\sqrt{-a})$ *with* $a \in \{5, 6, 10, 13, 15, 22, 35, 37, 51, 58, 91, 115, 123, 187, 235, 267, 403, 427\}$ *[21].*

**Lemma 3.4.2.** *The imaginary quadratic fields of class number 4 are given by* $\mathbb{Q}(\sqrt{-a})$ *with* $a \in \{14, 17, 21, 30, 33, 34, 39, 42, 46, 55, 57, 70, 73, 78, 82, 85, 93, 97, 102, 130, 133, 142, 155, 177, 190, 193, 195, 203, 219, 253, 259, 291, 323, 355, 435, 483, 555, 595, 627, 667, 715, 723, 763, 795, 955, 1003, 1027, 1227, 1243, 1387, 1411, 1435, 1507, 1555\}$ *[1].*

To begin, we will use the formula $h(K) = \left(\frac{1}{2}\right)^{2^{n-1}-1} QPh_3$ to find the class number of a particular imaginary triquadratic field:

**Lemma 3.4.3.** *The number field* $K = \mathbb{Q}(\sqrt{-1}, \sqrt{-2}, \sqrt{-3})$ *has class number 1.*

*Proof.* Let $k = \mathbb{Q}(\sqrt{2})$; this is a valid choice for $k$ to use with the formula given in Theorem 3.2.2

$$h(K) = \frac{1}{8} QPh_3$$

since we know there exists an odd prime $p = 3$ which ramifies in $K$ but not in $k$. Let $k_1 = \mathbb{Q}(\sqrt{-1}, \sqrt{2})$, $k_2 = \mathbb{Q}(\sqrt{-3}, \sqrt{2})$ and $k_3 = \mathbb{Q}(\sqrt{3}, \sqrt{2})$. Now $P$ is the product of the class numbers of all imaginary quadratic fields of $K$: $P = h(-1)h(-2)h(-3)h(-6) = 1 \cdot 1 \cdot 1 \cdot 2 = 2$, so

$$h(K) = \frac{1}{8} QPh_3 = \frac{1}{4} Qh_3.$$

To compute the values for $Q$ and $h_3$ we need to understand the unit indices $q(L)$, $L \in \{K, k_1, k_2, k_3\}$. We first find the units of the quadratic subfields. The unit groups $E(\mathbb{Q}(\sqrt{-2}))$ and

$E(\mathbb{Q}(\sqrt{-6}))$ are simply equal to $\{\pm 1\}$. The other unit groups are:

$$\begin{aligned} E(\mathbb{Q}(\sqrt{-1})) &= \left\{ \left(e^{\pi i/2}\right)^{\ell} : \ell \in \mathbb{Z} \right\} \\ E(\mathbb{Q}(\sqrt{-3})) &= \left\{ \left(e^{\pi i/3}\right)^{\ell} : \ell \in \mathbb{Z} \right\} \\ E(\mathbb{Q}(\sqrt{2})) &= \left\{ \pm \left(1+\sqrt{2}\right)^{\ell} : \ell \in \mathbb{Z} \right\} \\ E(\mathbb{Q}(\sqrt{3})) &= \left\{ \pm \left(2+\sqrt{3}\right)^{\ell} : \ell \in \mathbb{Z} \right\} \\ E(\mathbb{Q}(\sqrt{6})) &= \left\{ \pm \left(5+2\sqrt{6}\right)^{\ell} : \ell \in \mathbb{Z} \right\} \end{aligned}$$

Now, to find $Q = q(K/k)q(k_1/\mathbb{Q})q(k_2/\mathbb{Q})$ we first note that in [13] Kubota calculates $q(k_1/\mathbb{Q})$ and finds that it is equal to 2. To better understand this index, observe that an eighth root of unity, $e^{\pi i/4} = \frac{1}{2}(\sqrt{2}+\sqrt{-2})$ is in $k_1$ but is not in any of the quadratic subfields of $k_1$. This is what gives rise to the index $q(k_1/\mathbb{Q})$ being equal to 2, and in fact tells us that

$$E(k_1) = \left\{ \left(e^{\pi i/4}\right)^{\ell_1} \left(1+\sqrt{2}\right)^{\ell_2} : \ell_1, \ell_2 \in \mathbb{Z} \right\}.$$

Next we must compute $q(k_2/\mathbb{Q})$. A fundamental unit of $k_2$ is

$$\frac{\sqrt{2}}{2} - \frac{\sqrt{-6}}{2} + \frac{\sqrt{-3}}{2} - \frac{1}{2} = \left(\sqrt{2}-1\right)\left(\frac{1-\sqrt{-3}}{2}\right) \in E\left(\mathbb{Q}(\sqrt{2})\right) E\left(\mathbb{Q}(\sqrt{-3})\right).$$

Also, the roots of unity of $k_2$ are exactly the same as the roots of unity in $\mathbb{Q}(\sqrt{-3})$. Therefore,

$$E(k_2) = E\left(\mathbb{Q}(\sqrt{2})\right) E\left(\mathbb{Q}(\sqrt{-3})\right) E\left(\mathbb{Q}(\sqrt{-6})\right).$$

This gives us $q(k_2) = 1$.

At this point we have that $Q = q(K/k)q(k_1/\mathbb{Q})q(k_2/\mathbb{Q}) = 2q(K/k)$; it is useful to compute $h_3$ before finding $q(K/k)$.

To find $h_3$, recall that Kuroda's class number formula states

$$h_3 = \frac{1}{4}q(k_3/\mathbb{Q})h(2)h(3)h(6) = \frac{1}{4}q(k_3/\mathbb{Q}),$$

since the quadratic subfields all have class number 1. Since $k_3$ is a real biquadratic field, we can find the unit group $E(k_3)$, using results from Kubota [13]. To do this, we first take the norm of the

fundamental unit of each real quadratic subfield of $k_3$:

$$N_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(1+\sqrt{2}) = -1$$

$$N_{\mathbb{Q}(\sqrt{3})/\mathbb{Q}}(2+\sqrt{3}) = 1$$

$$N_{\mathbb{Q}(\sqrt{6})/\mathbb{Q}}(5+2\sqrt{6}) = 1$$

This tells us that a fundamental system of units for $\mathcal{O}_{k_3}$ is $\left\{1+\sqrt{2}, \sqrt{2+\sqrt{3}}, \sqrt{5+2\sqrt{6}}\right\}$. (Note that we are taking square roots of only those elements of norm 1; this rule does not apply in general, it only applies precisely because there are two fundamental units of norm 1 and one of norm -1). Further, since $k_3$ and all of its subfields are totally real, the only roots of unity contained in these fields are $\pm 1$. Putting this together we have that

$$E(k_3) = \left\{ \pm \left(1+\sqrt{2}\right)^{\ell_1} \left(\sqrt{2+\sqrt{3}}\right)^{\ell_2} \left(\sqrt{5+2\sqrt{6}}\right)^{\ell_3} : \ell_1, \ell_2\ell_3 \in \mathbb{Z} \right\}.$$

Therefore $q(k_3/\mathbb{Q}) = 4$, $h_3 = \frac{1}{4} \cdot 4 = 1$ and

$$h(K) = \frac{1}{4} \cdot 2q(K/k) \cdot 1 = \frac{1}{2} q(K/k).$$

Since $h(K) \in \mathbb{Z}$, $q(K/k)$ must be divisible by 2. Recall that

$$q(K/k) = \left[E(K) : E(k_1)E(k_2)E(k_3)\right].$$

First note that the roots of unity in $E(K)$ are equal to the roots of unity of $E(k_1)E(k_2)E(k_3)$: both of these groups contain a 24th root of unity.

By Dirichlet's unit theorem, $E(K)$ has three fundamental units. Computing a fundamental system of units in Sage we find

$$\begin{aligned}
\epsilon_1 &:= \tfrac{1}{2}\sqrt{3} - \tfrac{1}{2}\sqrt{-1} - \tfrac{1}{2}\sqrt{-3} + \tfrac{1}{2} \\
\epsilon_2 &:= -\tfrac{1}{4}\sqrt{-6} - \tfrac{1}{4}\sqrt{2} + \sqrt{-1} + \tfrac{1}{4}\sqrt{6} - \tfrac{1}{4}\sqrt{-2} \\
\epsilon_3 &:= \tfrac{1}{4}\sqrt{6} - \tfrac{1}{4}\sqrt{2} - \sqrt{-1} + \tfrac{1}{4}\sqrt{6} - \tfrac{3}{4}\sqrt{-2} + \tfrac{1}{2}\sqrt{-3} - \tfrac{1}{2}
\end{aligned}$$

We can factor the first unit

$$\epsilon_1 = \frac{1-i}{\sqrt{2}} \cdot \frac{1+\sqrt{3}}{\sqrt{2}} = e^{\pi i/4} \cdot \frac{\sqrt{2}+\sqrt{6}}{2} = e^{\pi i/4} \cdot \sqrt{2+\sqrt{3}}.$$

Finding a factorization for $\epsilon_2$ and $\epsilon_3$ cannot be achieved in Sage. However, dividing one by the other yields:

$$\begin{aligned}\frac{\epsilon_2}{\epsilon_3} &= \frac{1}{2}\sqrt{-6} - \frac{1}{2}\sqrt{2} - \frac{1}{2}\sqrt{-3} + \frac{1}{2} \\ &= \frac{-1+\sqrt{-3}}{2} \cdot (\sqrt{2}-1) \\ &= e^{2\pi i/3} \cdot (\sqrt{2}-1).\end{aligned}$$

Thus $\left\{1+\sqrt{2}, \sqrt{2+\sqrt{3}}, \epsilon_3\right\}$ is a fundamental system of units for $K$. As noted previously, $q(K/k)$ is divisible by 2, so the fact that $1+\sqrt{2}, \sqrt{2+\sqrt{3}}$ are units of the subfield $k_3$ of $K$ implies that we must have $\epsilon_3 \notin E(k_1)E(k_2)E(k_3)$. Let $E'(K)$ denote the group of units generated by the set

$$\left\{e^{2\pi i/12}, 1+\sqrt{2}, \sqrt{2+\sqrt{3}}, \epsilon_3^2\right\}.$$

Then

$$q(K/k) = 2 \cdot \left[E'(K) : E(k_1)E(k_2)E(k_3)\right].$$

Squaring $\epsilon_3$ yields

$$\begin{aligned}\epsilon_3^2 &= \frac{-1+i}{\sqrt{2}} \cdot \frac{5+4\sqrt{2}-3\sqrt{3}-2\sqrt{6}}{\sqrt{2}} \\ &= e^{3\pi i/4} \cdot \frac{1}{2}\left(8+5\sqrt{2}-4\sqrt{3}-3\sqrt{6}\right).\end{aligned}$$

The latter factor is in $E(k_3)$, so the index $[E'(K) : E(k_1)E(k_2)E(k_3)]$ must equal 1. Thus $q(K/k) = 2$ and the class number of $K$ is

$$h(K) = \frac{1}{2}q(K/k) = 1.$$

□

The formula given in Theorem 3.2.2 can be used to find a complete list of imaginary triquadratic fields of class number 1, though to find such a list we will not repeat these calculations in the amount of detail used to prove Lemma 3.4.3.

**Theorem 3.4.4.** *There are 17 imaginary triquadratic fields with class number 1. They are given by* $\mathbb{Q}(\sqrt{-a_1}, \sqrt{-a_2}, \sqrt{-a_3})$ *where all possiblities for* $(a_1, a_2, a_3)$ *are those found in this table:*

| $(a_1, a_2, a_3)$ | $(a_1, a_2, a_3)$ | $(a_1, a_2, a_3)$ | $(a_1, a_2, a_3)$ | $(a_1, a_2, a_3)$ |
|---|---|---|---|---|
| $(1, 2, 3)$ | $(1, 3, 5)$ | $(1, 7, 5)$ | $(2, 3, 7)$ | $(3, 7, 15)$ |
| $(1, 2, 5)$ | $(1, 3, 7)$ | $(1, 7, 13)$ | $(2, 3, 10)$ | $(3, 11, 6)$ |
| $(1, 2, 11)$ | $(1, 3, 11)$ | $(1, 7, 19)$ | $(2, 7, 10)$ | $(3, 11, 19)$ |
| | $(1, 3, 19)$ | | | $(3, 11, 51)$ |

*Proof.* If $K$ has class number 1, then

$$1 = h(K) = \frac{1}{8}QPh_3 = \frac{1}{8}Q \cdot (h(-a_1)h(-a_2)h(-a_3)h(-a_1a_2a_3)) \cdot h_3,$$

for an appropriate choice of subfields $k, k_1, k_2, k_3$. Now $Q$ and $h_3$ are positive intgers, so the product $h(-a_1)h(-a_2)h(-a_3)h(-a_1a_2a_3)$ must be a power of 2 not exceeding $2^3 = 8$. Also, without loss of generality since $a_1, a_2, a_3$ and the square-free part of $a_1a_2a_3$ are interchangeable, there are six possibilities to consider:

(i) $h(-a_1) = h(-a_2) = h(-a_3) = h(-a_1a_2a_3) = 1$

(ii) $h(-a_1) = h(-a_2) = h(-a_3) = 1$ and $h(-a_1a_2a_3) = 2$ or 4,

(iii) $h(-a_1) = h(-a_2) = 1$, $h(-a_3) = h(-a_1a_2a_3) = 2$,

(iv) $h(-a_1) = h(-a_2) = 1$, $h(-a_3) = 2$ and $h(-a_1a_2a_3) = 4$,

(v) $h(-a_1) = 1$ and $h(-a_2) = h(-a_3) = h(-a_1a_2a_3) = 2$,

(vi) $h(-a_1) = h(-a_2) = h(-a_3) = 1$ and $h(-a_1a_2a_3) = 8$.

Case (i) cannot occur: all $\mathbb{Q}(\sqrt{-a})$ with class number 1 and $a > 0$ square-free have $a$ either equal to 1 or a prime integer. If $a_1 \neq a_2 \neq a_3$ are all 1 or prime, then the square-free part of the product $a_1a_2a_3$ will be composite, so $h(-a_1a_2a_3)$ will not equal 1.

Before moving on to cases (ii)-(v) it is worth noting that each of these has $h(-a_1) = 1$ and at least one imaginary quadratic subfield of class number 2 or 4. Then any prime that the radicand $a_1$ takes on must divide at least one of $a_2, a_3$ or $s.f.(a_1a_2a_3)$. Some of the radicands appearing in the list for imaginary quadratic fields of class number 1 do not divide any of the radicands of imaginary quadratic fields of class number 2 or 4. These are 43, 67 and 163. Thus, in these cases, any imaginary quadratic subfields of class number 1 must be chosen from the set $\{1, 2, 3, 7, 11, 19\}$.

It is also worth noting that 19 does not divide the radicand of any imaginary quadratic field of class number 2.

Now consider case (ii): Examining the lists of imaginary quadratic fields with class number 1, 2 and 4, we see that there are only two imaginary triquadratic fields with $h(-a_i) = 1$, $1 \leq i \leq 3$ and $h(-a_1a_2a_3) = 2$: $\mathbb{Q}(\sqrt{-1}, \sqrt{-2}, \sqrt{-3})$ and $\mathbb{Q}(\sqrt{-1}, \sqrt{-2}, \sqrt{-11})$. Both of these fields have class number 1. The proof of this fact for $\mathbb{Q}(\sqrt{-1}, \sqrt{-2}, \sqrt{-3})$ is in the previous lemma, and the class number for $\mathbb{Q}(\sqrt{-1}, \sqrt{-2}, \sqrt{-11})$ using the same methods. Also, there are 7 imaginary triquadratic fields with $h(-a_i) = 1$, $1 \leq i \leq 3$ and $h(-a_1a_2a_3) = 4$. They have radicand lists $\{-a_1, -a_2, -a_3\}$ given by:

$$\{-1,-2,-7\} \quad \{-1,-3,-7\} \quad \{-1,-3,-11\} \quad \{-2,-3,-7\}$$
$$\{-1,-3,-19\} \quad \{-1,-7,-19\} \quad \{-3,-11,-19\}$$

For each of these fields we may choose $k = \mathbb{Q}(a_1a_2)$, $k_1 = k(\sqrt{-a_1}), k_2 = k(\sqrt{-a_3})$ and $k_3 = k(\sqrt{a_1a_3})$. We are guaranteed $P = 4$ for each of these triquadratic fields $K$, and can check, using the methods used in the proof of the lemma that $h_3 = 1$ for each of these fields. Thus we have

$$h(K) = \frac{1}{2}Q = \frac{1}{2}q(K/k)q(k_1/\mathbb{Q})q(k_2/\mathbb{Q}),$$

so in order for $h(K)$ to equal 1 the product $q(K/k)q(k_1/\mathbb{Q})q(k_2/\mathbb{Q})$ must equal 2.

When $K = \mathbb{Q}(\sqrt{-1}, \sqrt{-2}, \sqrt{-7})$ we already know from the proof of the previous lemma that $q(k_1/\mathbb{Q}) = 2$. Also, $q(k_2/\mathbb{Q}) = 1$ but $q(K/k) = 2$ so this number field has class number $h(K) = 2$.

Aside from this choice for $K$, all other fields with radicand lists given above have class number 1. Thus we have completed the examination of case (ii).

Cases (iii)-(iv) can be worked with simultaneously since they both have $h(-a_1) = h(-a_2) = 1$ and $h(-a_3) = 2$. Taking $a_1, a_2$ to be in the list $\{1, 2, 3, 7, 11, 19\}$ and $-a_3$ to be a radicand of an imaginary quadratic field of class number we have a finite list of imaginary triquadratic fields to consider. Using Sage to compute these possibilities, along with the class number of each associated imaginary triquadratic field, we find the remainder of the class number 1 fields listed in the statement of the theorem.

Cases (v) and (vi) each have $P = 8$, so for an appropriate choice of a real quadratic subfield $k$ of $K$, and three intermediate fields $k_1, k_2, k_3$ with $k_3$ a real biquadratic field, we have

$$h(K) = q(K/k)q(k_1/\mathbb{Q})q(k_2/\mathbb{Q})h_3.$$

In case (v), $h(-a_1) = 1$ and all other imaginary quadratic subfields have class number 2. Thus $a_1 \in \{1, 2, 3, 7, 11\}$ by the discussion at the beginning of this proof. Using a similar argument, we see that the imaginary quadratic subfields of $K$ with class number 2 must be $\mathbb{Q}(\sqrt{-a_2}), \mathbb{Q}(\sqrt{-a_3}), \mathbb{Q}(\sqrt{-a_1a_2a_3})$ with

$$a_2, a_3, s.f.(a_1a_2a_3) \in \{5, 6, 10, 13, 15, 22, 35, 51, 91, 187\}.$$

We find that there are only four possibilities satisfying the conditions on the imaginary quadratic fields; these are the imaginary triquadratic fields with radicand lists given by:

$$\{-1, -6, -10, -15\}, \{-2, -5, -6, -15\}, \{-3, -5, -6, -10\}, \{-11, -5, -10, -22\}.$$

For each of these fields we can verify that our subfields can be chosen so that at least one of the factors $q(K/k), q(k_1/\mathbb{Q}), q(k_2/\mathbb{Q}), h_3$ is greater than 1, forcing $h(K) = q(K/k)q(k_1/\mathbb{Q})q(k_2/\mathbb{Q})h_3 > 1$.

Last, consider case (vi): $h(-a_1) = h(-a_2) = h(-a_3) = 1$ and $h(-a_1a_2a_3) = 8$. Using Sage to find all values for $a_1a_2a_3$ with $h(-a_1a_2a_3) = 8$ we find

$$a_1a_2a_3 \in \{66, 77, 114, 154, 418, 258, 301, 2451\};$$

assuming, without loss of generality, that $a_1 < a_2 < a_3$ we can uniquely determine $a_1, a_2, a_3$ from these products. Choosing appropriate subfields $k, k_1, k_2, k_3$ and using the fact that

$$h(K) = q(K/k)q(k_1/\mathbb{Q})q(k_2/\mathbb{Q})h_3$$

we find that none of the triquadratic fields corresponding to these values have class number 1. □

## 3.5 Class Numbers of $n$-quadratic Fields, $n \geq 4$

The primary goal of this section is to prove the following theorem:

**Theorem 3.5.1.** *If $K$ is an imaginary $n$-quadratic field with $n \geq 4$ then $K$ has class number greater than 1.*

The proof of this theorem follows from Corollary 3.5.4 and Lemmas 3.5.5, 3.5.6 in the remainder of this section.

We begin with the following theorem of Frölich [9]:

**Theorem 3.5.2.** *If $K$ is any number field, and the number of primes which ramify in $K$ is $\geq 5$ then the class number of $K$ is even.*

In light of this theorem, along with Lemma 2.4.6 we can deduce the following corollary:

**Corollary 3.5.3.** *Let $h(K)$ denote the class number of an $n$-quadratic field $K$. Then*

*(1) if $K$ is totally real and $n \geq 5$ then $2|h(K)$ and*

*(2) if $K$ is imaginary and $n \geq 6$ then $2|h(K)$*

**Lemma 3.5.4.** *If $K$ is an imaginary 5-quadratic field then $K$ does not have class number 1.*

*Proof.* Let $K$ be an imaginary 5-quadratic field. From Theorem 3.5.1 we know that if the class number $h(K)$ of $K$ is equal to 1 then there must be fewer than 5 primes ramified in $K$. Thus there must exist a primitive radicand list for $K$ of the form $\{-1, -p_1, -p_2, -p_3, -p_4\}$ for rational primes $p_1, ..., p_4$.

From Theorem 3.3.2 we have the following formula for the class number of $K$:

$$h(K) = \left(\frac{1}{2}\right)^{2^{5-1}-1} QPh_3 = \left(\frac{1}{2}\right)^{15} QPh_3$$

where $P$ is the product of the class numbers of all of the imaginary quadratic subfields of $K$. If $h(K) = 1$ then this implies all imaginary quadratic subfields of $K$ must have class number which is a power of 2, and this product cannot exceed $2^{15}$. Recall that the imaginary quadratic fields of class number 1 are $\mathbb{Q}(\sqrt{-a})$ with $a \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$. Also recall that when $a \in \{43, 67, 163\}$ then $a$ does not divide the radicand of any imaginary quadratic field of class number 2 or 4. Thus if

$p_i \in \{43, 67, 163\}$ for some $i \in \{1, 2, 3, 4\}$ then there will be at least 7 imaginary quadratic subfields of $K$ with class number not equal to 1, 2 or 4. This will cause the product $P$ to either be $\geq 2^{15}$ or to have an odd prime factor. In either case we will have $QPh_3 \neq 2^{15}$ so $h(K)$ will not equal 1. Similarly, $h(K)$ cannot equal 1 if any $p_i$ is equal to 19, since of the imaginary quadratic fields of class number 2 and 4, only one field has radicand which is divisible by 19.

It is worth noting that the fact that we must have $\mathbb{Q}(\sqrt{-1})$ as a subfield of $K$ allows these arguments to hold. This is because, for example, the prime $p_1$ divides the radicands of the imaginary quadratic fields $\mathbb{Q}(\sqrt{-a})$ with

$$a \in \{p_1, p_1p_2, p_1p_3, p_1p_4, p_1p_2p_3, p_1p_2p_4, p_1p_3p_4, p_1p_2p_3p_4\}.$$

If $-1$ were not a radicand for $K$ then $\mathbb{Q}\left(\sqrt{-p_1p_2}\right) = \mathbb{Q}\left(\sqrt{(-1)(-p_1)(-p_2)}\right)$ would not be a subfield of $K$.

Considering the divisibility of the radicands of the imaginary quadratic fields of class number 2 and 4 we find that there are no imaginary 5-quadratic fields with radicand lists $\{-1, -p_1, -p_2, -p_3, -p_4\}$ which have class number 1. □

**Lemma 3.5.5.** *If $n = 4$, $K$ does not have class number 1.*

*Proof.* This proof does not arise from a straightforward counting argument like the others in this section, but we do use this to narrow down the number of possibilities before finally computing the class numbers of a small list of candidates. Theorem 3.3.2 implies that if $h(K) = 1$ we have

$$1 = h(K) \geq \left(\frac{1}{2}\right)^7 P.$$

We know that $K$ has $2^{4-1} = 8$ imaginary quadratic subfields. If more than 2 of these subfields had class number larger than 4, we would have

$$1 = h(K) \geq \frac{8^3}{2^7} > 1,$$

which would give a contradiction. Therefore, at least 6 of the 8 imaginary quadratic subfields of $K$ must have class number 1, 2 or 4; call these fields $\mathbb{Q}(\sqrt{-a_i})$, $1 \leq i \leq 6$; and write $\mathbb{Q}(\sqrt{-a_7}), \mathbb{Q}(\sqrt{-a_8})$

for the remaining two imaginary quadratic subfields.

Then clearly $\mathbb{Q}(\sqrt{-a_1a_2a_3}), \mathbb{Q}(\sqrt{-a_1a_2a_4}), \mathbb{Q}(\sqrt{-a_1a_2a_5}) \subset K$. Since the $a_i$ are distinct, at most 2 of these fields may be equal to $\mathbb{Q}(\sqrt{-a_7})$ or $\mathbb{Q}(\sqrt{-a_8})$. Thus, without loss of generality, assume $\mathbb{Q}(\sqrt{-a_1a_2a_3}) \neq \mathbb{Q}(\sqrt{-a_7})$ or $\mathbb{Q}(\sqrt{-a_8})$. Then we may define

$$k_1 = \mathbb{Q}(\sqrt{-a_1}, \sqrt{-a_2}, \sqrt{-a_3});$$

so $k_1$ is an imaginary triquadratic field with all imginary quadratic subfields having class number 1, 2 or 4. Further, at most one of $\sqrt{-a_4}$, $\sqrt{-a_5}$ may be contained in $k_1$; assume without loss of generality that $\sqrt{-a_4} \notin k_1$. Then $K = k_1(\sqrt{-a_4})$.

Therefore, a list of candidates for imaginary 4-quadratic fields $K$ with class number 1 may be constructed as follows:

- Make a list $S$ of all imaginary triquadratic fields $k_1$ such that all imaginary quadratic subfields have class number 1, 2 or 4.
- Make a second list, $T$, as follows: for each $k_1 \in S$ and each $a$ such that $\sqrt{-a} \notin k_1$ and $\mathbb{Q}(\sqrt{-a})$ has class number 1, 2 or 4, add $k(\sqrt{-a})$ to $T$. Remove all repeat entries from this list.
- For each $K \in T$, we want the product $P$ of the class numbers of the imaginary quadratic subfields to not exceed $2^7$. Find a lower bound for $P$ as follows: start with $P = 1$ and iterate through all imaginary quadratic subfields; if we know the class number of that subfield, multiply $P$ by that number, otherwise, multiply $P$ by 8. If the lower bound for $P$ is greater than $2^7$, discard that field from the possibility list.

Following these steps yields only four candidates for imaginary 4-quadratic fields with class number 1: $\mathbb{Q}(\sqrt{-1}, \sqrt{-2}, \sqrt{-3}, \sqrt{-7})$ (has class number 4), $\mathbb{Q}(\sqrt{-1}, \sqrt{-2}, \sqrt{-3}, \sqrt{-11})$ (has class number 4), $\mathbb{Q}(\sqrt{-1}, \sqrt{-2}, \sqrt{-3}, \sqrt{-5})$ (has class number 2), and $\mathbb{Q}(\sqrt{-1}, \sqrt{-2}, \sqrt{-5}, \sqrt{-7})$ (has class number 4).

□

# Chapter 4

# Euclid's Algorithm in Multiquadratic Fields

## 4.1 Background

It is well-known that the norm-Euclidean quadratic fields have already been fully classified; they are the fields $\mathbb{Q}(\sqrt{a})$ such that

$$a \in \{-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 41, 57, 73\}.$$

The complete determination of this list took place through a series of papers published over the course of more than 100 years (from 1848–1952). In chapter 4 of [15], Lemmermeyer gives an excellent summary of this development.

Further by [8] we can explicitly state the Euclidean minimum for any imaginary quadratic field $\mathbb{Q}(\sqrt{-a})$ with $a$ squarefree:

$$M(\mathbb{Q}(\sqrt{a})) = \begin{cases} \frac{a+1}{4} & \text{if } -a \equiv 2, 3 \pmod 4 \\ \frac{(a+1)^2}{16a} & \text{if } -a \equiv 1 \pmod 4. \end{cases}$$

More recently, a complete list of all norm-Euclidean imaginary biquadratic fields was determined [16]. These are the thirteen fields given by $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2})$ with the possibilities for $a_1$ and $a_2$

as follows:

$$a_1 = -1,\ a_2 = 2, 3, 5, 7;$$

$$a_1 = -2,\ a_2 = -3, 5;$$

$$a_1 = -3,\ a_2 = 2, 5, -7, -11, 17, -19;$$

$$a_1 = -7,\ a_2 = 5.$$

To consider the question of whether or not other imaginary multiquadratic fields are Euclidean first note that, for a ring of integers $\mathcal{O}_K$, we have

$$\left\{\begin{array}{c}\text{norm-Euclidean}\\ \text{domains}\end{array}\right\} \subset \left\{\begin{array}{c}\text{Euclidean}\\ \text{domains}\end{array}\right\} \subseteq \left\{\begin{array}{c}\text{principal ideal}\\ \text{domains}\end{array}\right\} = \left\{\begin{array}{c}\text{unique factorization}\\ \text{domains}\end{array}\right\}.$$

Assuming the generalized Riemann hypothesis (GRH), then whenever $K$ not an imaginary quadratic field, equality holds between the set of Euclidean domains and the set of principal ideal domains [26].

Therefore, to consider the question of Euclideanity of imaginary multiquadratic fields, we may apply the results from chapter 3, and only consider those fields with class number 1. Recall that we proved that all imaginary $n$-quadratic fields with $n \geq 4$ have class number strictly greater than 1, and that there are exactly 17 imaginary triquadratic fields of class number 1. Thus to complete the classification of all norm-Euclidean multiquadratic fields, we only need to complete the triquadratic case.

## 4.2 Imaginary Triquadratic Fields

The goal of this section is to prove the following Theorem:

**Theorem 4.2.1.** *Of the 17 imaginary triquadratic fields of class number 1, at least three are norm-Euclidean, and at least five are not norm-Euclidean. These fields are*

| *norm-Euclidean fields:* | *non norm-Euclidean fields:* | |
|---|---|---|
| $\mathbb{Q}\left(\sqrt{-1},\sqrt{-2},\sqrt{-3}\right)$ | $\mathbb{Q}\left(\sqrt{-1},\sqrt{-2},\sqrt{-11}\right)$ | $\mathbb{Q}\left(\sqrt{-1},\sqrt{-7},\sqrt{-19}\right)$ |
| $\mathbb{Q}\left(\sqrt{-1},\sqrt{-2},\sqrt{-5}\right)$ | $\mathbb{Q}\left(\sqrt{-1},\sqrt{-3},\sqrt{-11}\right)$ | $\mathbb{Q}(\sqrt{-1},\sqrt{-7},\sqrt{-91})$ |
| $\mathbb{Q}\left(\sqrt{-1},\sqrt{-3},\sqrt{-5}\right)$ | $\mathbb{Q}\left(\sqrt{-1},\sqrt{-3},\sqrt{-19}\right)$ | |

*Proof.* Combining the results of Corollary 4.2.4 and Lemmas 4.2.9 and 4.2.10, which are proven later in this section, we obtain this list of imaginary triquadratic fields which are not norm-Euclidean. The fields which are norm-Euclidean were determined computationally, using Pierre Lezowski's *euclid* program [18], on the University of Colorado's JANUS supercomputer. □

We start with the following proposition of Lemmermeyer [16]:

**Proposition 4.2.2.** *Let $K/k$ be a finite extension of number fields of relative degree $n$, and suppose that the non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_k$ is completely ramified in $K/k$, i.e. there exists a prime ideal $\mathfrak{B} \subset \mathcal{O}_K$ such that $\mathfrak{p}\mathcal{O}_K = \mathfrak{B}^n$. If $K$ is norm-Euclidean, then for any $\alpha, \beta \in \mathcal{O}_k \setminus \mathfrak{p}$ with $\beta \equiv \alpha^n \bmod \mathfrak{p}$, there exists $b \in \mathcal{O}_k$ such that*

*(1) $b = N_{K/k}\delta$ for some $\delta \in \mathcal{O}_K$,*

*(2) $b \equiv \beta \bmod \mathfrak{p}$ and*

*(3) $|N_{k/\mathbb{Q}}b| < |N_{k/\mathbb{Q}}\mathfrak{p}|$.*

**Remark 4.2.3.** Though we will not prove this proposition here, it is very useful to give some intuition as to why this proposition works.

Assume $K/k$ is a degree $n$ extension of number fields, $\mathfrak{p} \in \mathcal{O}_k$ a prime with $\mathfrak{p}\mathcal{O}_K = \mathfrak{B}^n$ and $K$ norm-Euclidean. Then $\mathcal{O}_K$ has class number 1 so there exists a prime $p \in \mathcal{O}_K$ such that $\mathfrak{B} = (p)$. Now any $\alpha \in \mathcal{O}_k$ is also an element of $\mathcal{O}_K$. The above proposition arises from using the division algorithm on $\alpha$ and $p$ in $\mathcal{O}_K$. That is, since $K$ is norm-Euclidean, there exists $q, r \in \mathcal{O}_K$ such that $\alpha = qp + r$ and $|N_{K/\mathbb{Q}}(r)| < |N_{K/\mathbb{Q}}(\alpha)|$.

Now we take the relative norm of each side of the equation $\alpha = qp + r$ down to $k$. Since $\alpha \in \mathcal{O}_k$ we have that $N_{K/k}(\alpha) = \alpha^n$. Let $\sigma_1, ..., \sigma_n$ be the $n$ embeddings of $K$ into $\mathbb{C}$ which fix $k$.

Then we have

$$\begin{aligned}\alpha^n &= N_{K/k}(qp+r)\\ &= \sigma_1(qp+r)\cdots\sigma_n(qp+r)\\ &= (\sigma_1(q)\sigma_1(p)+\sigma_1(r))\cdots(\sigma_n(q)\sigma_n(p)+\sigma_n(r))\end{aligned}$$

If we were to multiply out the product given in the last line, we would find that all terms but one would have at least one factor of the form $\sigma_i(p)$ for some $i \in \{1, ..., n\}$. The only term without any factors of this form is the relative norm of the remainder $r$:

$$\sigma_1(r)\cdots\sigma_n(r) = N_{K/k}(r).$$

Now since $\mathfrak{B} \cap \mathcal{O}_k = \mathfrak{p}$ we have that any term of the product with a factor of the form $\sigma_i(p)$ will be contained in the ideal $\mathfrak{p}$. Thus we have that $\alpha^n \equiv N_{K/k}(r) \bmod \mathfrak{p}$. Also, since $|N_{K/\mathbb{Q}}(r)| < |N_{K/\mathbb{Q}}(\alpha)|$ we have $|N_{k/\mathbb{Q}}\left(N_{K/k}(r)\right)| < |N_{k/\mathbb{Q}}(\alpha^n)|$.

In the above proposition, the value $\delta$ is equal to the remainder $r \in \mathcal{O}_K$ and $b$ is just equal to $N_{K/k}(r)$. In other words, the existence statement defining norm-Euclideanity in $K$ translates to an existence statement in the subfield $k$.

**Corollary 4.2.4.** *The imaginary triquadratic field $K = \mathbb{Q}(\sqrt{-1}, \sqrt{-2}, \sqrt{-11})$ is not norm-Euclidean.*

*Proof.* Let $k = \mathbb{Q}(\sqrt{-11})$. Since $-11 \equiv 5 \bmod 8$ the ideal $(2)$ is prime in $\mathcal{O}_k$. Further, $(2)$ ramifies completely in $K/k$ so we can apply Proposition 4.2.2 with $\mathfrak{p} = (2)$. Let $\alpha = \frac{1+\sqrt{-11}}{2}$. Then

$$b \equiv \alpha^4 = \frac{7-5\sqrt{-11}}{2} \equiv \frac{-1-\sqrt{-11}}{2} \bmod 2.$$

If $K$ is norm-Euclidean we must have $b$ satisfying condition 3 of the proposition. We have $|N_{k/\mathbb{Q}}\mathfrak{p}| = 4$ so the only choice for $b$ with $|N_{k/\mathbb{Q}}b| < |N_{k/\mathbb{Q}}\mathfrak{p}|$ is $b = \frac{-1-\sqrt{-11}}{2}$; which gives $N_{k/\mathbb{Q}}b = 3$. However, if we make this choice for $b$, condition 2 of the proposition will not be satisfied since there is no element in $\mathcal{O}_K$ with an absolute norm of 3; since 3 is prime in the subfield $\mathbb{Q}(\sqrt{2}) \subset K$ we know that any prime lying above 3 in $\mathcal{O}_K$ will have norm at least 9. Therefore, $K$ cannot be norm-Euclidean. □

**Remark 4.2.5.** Considering Remark 4.2.3, the above proof actually sheds light on the Euclidean minimum of the field $K = \mathbb{Q}(\sqrt{-1}, \sqrt{-2}, \sqrt{-11})$. Of all $b \equiv \alpha^4 \pmod{\mathfrak{p}}$, the smallest value for $b$ which is the norm of an element of $\mathcal{O}_K$ is 9. Thus $M(K) \geq 9/N(\mathfrak{p}) = 9/4$.

The above example works out nicely because 2 ramifies completely between a quadratic field and a triquadratic field, and norms are very easy to bound in imaginary quadratic fields. However, 2 is the only prime that can ramify to a fourth power in a triquadratic number field, and even then there are many cases in which 2 will remain unramified, or only ramify to a second power in a triquadratic field. Because of this the application of Proposition 4.2.2 to the triquadratic case is very limited. Considering Remark 4.2.3 we may extend the ideas behind Proposition 4.2.2 so that they are more applicable to the case of triquadratic fields.

**Proposition 4.2.6.** *Let $K/k$ be a finite, abelian, normal extension of number fields of relative degree $n$. Let $\mathfrak{p} \subset \mathcal{O}_k$ be a non-zero prime ideal and let $e$ denote the ramification index of $\mathfrak{p}$ in $\mathcal{O}_K$. If $K$ is norm-Euclidean, then for any $\alpha, \beta \in \mathcal{O}_k \setminus \mathfrak{p}$ with $\beta \equiv \alpha^n \bmod \mathfrak{p}$, there exists $b \in \mathcal{O}_k$ such that*

*(1) $b = N_{K/k}\delta$ for some $\delta \in \mathcal{O}_K$,*

*(2) $b \equiv \beta \bmod \mathfrak{p}$ and*

*(3) $|N_{k/\mathbb{Q}}b| < |N_{k/\mathbb{Q}}\mathfrak{p}|^{n/e}$.*

*Proof.* There exists an ideal $\mathfrak{B} \subset \mathcal{O}_K$ such that $\mathfrak{p}\mathcal{O}_K = \mathfrak{B}^e$. Further, because $K$ is norm-Euclidean, there is a $\gamma \in \mathcal{O}_K$ such that $\mathfrak{B} = \gamma\mathcal{O}_K$ and for $\xi = \alpha/\gamma$ we can find $\eta \in \mathcal{O}_K$ such that $|N_{K/\mathbb{Q}}(\xi - \eta)| < 1$. This implies $|N_{K/\mathbb{Q}}(\alpha - \eta\gamma)| < |N_{K/\mathbb{Q}}\mathfrak{B}|$; put $b = N_{K/k}(\alpha - \eta\gamma)$. Then we find:

(1) By definition, $b = N_{K/k}\delta$ for $\delta = \alpha - \eta\gamma \in \mathcal{O}_K$.

(2) $b \equiv \beta \bmod \mathfrak{p}$: Since $K/k$ is Galois there exists a field $K_E$, $k \subseteq K_E \subseteq K$ such that $K_E$ is the inertia field with respect to the prime ideal $\mathfrak{p} \subset \mathcal{O}_k$; i.e. $[K : K_E] = e$, and $\mathfrak{p}$ is unramified in $K_E/k$. There exists a positive integer $r|n$ such that there are $r$ distinct prime ideals

in $\mathcal{O}_{K_E}$, say $\mathfrak{p}_1, ..., \mathfrak{p}_r$, such that $\mathfrak{p}\mathcal{O}_{K_E} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$. Further, for each $\mathfrak{p}_i$, there exists an irreducible element $q_i \in \mathcal{O}_K$ such that $\mathfrak{p}_i\mathcal{O}_K = (q_i)^e$. Now

$$b = N_{K/k}(\alpha - \eta\gamma) = N_{K_E/k}\left(N_{K/K_E}(\alpha - \eta\gamma)\right).$$

For some unit $u \in \mathcal{O}_K$ we can write $\gamma = uq_1 \cdots q_r$, so

$$b = N_{K_E/k}\left(N_{K/K_E}(\alpha - \eta u q_1 \cdots q_r)\right).$$

Considering the inside norm first we have

$$N_{K/K_E}(\alpha - \eta u q_1 \cdots q_r) = \prod_{\sigma \in \mathrm{Gal}(K/K_E)} (\alpha - \sigma(\eta u q_1 \cdots q_r)),$$

and since each prime ideal $(q_i)$ is the unique prime ideal lying over $\mathfrak{p}_i \subset \mathcal{O}_{K_E}$, each $\sigma \in \mathrm{Gal}(K/K_E)$ will send $q_i$ to an element in the ideal $(q_i)$. Thus

$$N_{K/K_E}(\alpha - \eta u q_1 \cdots q_r) \equiv \alpha^e \bmod (q_1 \cdots q_r).$$

Since both sides of this equation are in $\mathcal{O}_{K_E}$ the congruence holds mod $(q_1 \cdots q_r) \cap \mathcal{O}_{K_E} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$. Additionally, we know that $N_{K/K_E}(\alpha - \eta u q_1 \cdots q_r)$ is an integral element in $\mathcal{O}_{K_E}$, so there exists $\nu \in \mathcal{O}_{K_E}$ and $\rho \in (\mathfrak{p}_1 \cdots \mathfrak{p}_r)$ such that

$$N_{K/K_E}(\alpha - \eta u q_1 \cdots q_r) = \alpha^e + \nu\rho;$$

in particular,

$$b = N_{K/k}(\alpha - \eta\gamma) = N_{K_E/k}\left(N_{K/K_E}(\alpha - \eta\gamma)\right) = N_{K_E/k}\left(\alpha^e + \nu\rho\right).$$

Since each element in $\mathrm{Gal}(K_E/k)$ will permute the $\mathfrak{p}_i$, evaluating the norm $N_{K_E/k}\left(\alpha^e + \nu\rho\right)$ gives us

$$b \equiv (\alpha^e)^{n/e} \bmod (\mathfrak{p}_1 \cdots \mathfrak{p}_r).$$

Now both sides of this congruence are in $\mathcal{O}_k$, so considering the congruence mod $(\mathfrak{p}_1 \cdots \mathfrak{p}_r) \cap \mathcal{O}_k = \mathfrak{p}$ we have $b \equiv \alpha^n \bmod \mathfrak{p}$.

(3) Using the fact that $b = N_{K/k}(\alpha - \eta\gamma)$, we have

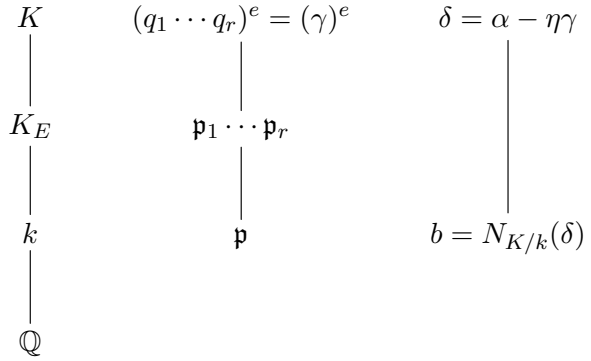
$$|N_{k/\mathbb{Q}}b| = |N_{k/\mathbb{Q}}N_{K/k}(\alpha - \eta\gamma)| = |N_{K/\mathbb{Q}}(\alpha - \eta\gamma)|,$$

and we have used the norm-Euclidean property to ensure that $|N_{K/\mathbb{Q}}(\alpha - \eta\gamma)| < |N_{K/\mathbb{Q}}\mathfrak{B}|$. Putting these facts together, we have

$$\begin{aligned} |N_{k/\mathbb{Q}}b| &< |N_{K/\mathbb{Q}}\mathfrak{B}| \\ &= |N_{k/\mathbb{Q}}(N_{K_E/k}(N_{K/K_E}(\mathfrak{B})))| \\ &= |N_{k/\mathbb{Q}}(N_{K_E/k}(\mathfrak{p}\mathcal{O}_{K_E}))| \\ &= |N_{k/\mathbb{Q}}(\mathfrak{p}^{[K_E:k]})| \\ &= |N_{k/\mathbb{Q}}(\mathfrak{p})|^{n/e}. \end{aligned}$$

□

**Remark 4.2.7.** It is helpful for the reader to keep the following diagram in mind when applying Proposition 4.2.6:




As mentioned in the previous section, there are exactly 17 imaginary triquadratic fields with class number 1. These are the fields $\mathbb{Q}(\sqrt{-a_1}, \sqrt{-a_2}, \sqrt{-a_3})$ with the 3-tuples $(a_1, a_2, a_3)$ given in the following table:

| $(a_1, a_2, a_3)$ | $(a_1, a_2, a_3)$ | $(a_1, a_2, a_3)$ | $(a_1, a_2, a_3)$ | $(a_1, a_2, a_3)$ |
|---|---|---|---|---|
| $(1, 2, 3)$ | $(1, 3, 5)$ | $(1, 7, 19)$ | $(2, 3, 7)$ | $(3, 7, 15)$ |
| $(1, 2, 5)$ | $(1, 3, 7)$ | $(1, 7, 35)$ | $(2, 3, 10)$ | $(3, 11, 6)$ |
| $(1, 2, 11)$ | $(1, 3, 11)$ | $(1, 7, 91)$ | $(2, 7, 10)$ | $(3, 11, 19)$ |
| | $(1, 3, 19)$ | | | $(3, 11, 187)$ |

**Remark 4.2.8.** Note that some of the tuples in this table are written differently than in Chapter 3. These are re-written for convenience when applying the arguments below but are equivalent to the fields found in Chapter 3; for example $\mathbb{Q}(\sqrt{-1},\sqrt{-7},\sqrt{-35}) = \mathbb{Q}(\sqrt{-1},\sqrt{-7},\sqrt{-5})$, so the tuple $(1,7,35)$ in the table above corresponds to the tuple $(1,7,5)$ in the previous chapter.

**Lemma 4.2.9.** *Applying Proposition 4.2.6 to* $K = \mathbb{Q}(\sqrt{-a_1},\sqrt{-a_2},\sqrt{-a_3})$, $k = \mathbb{Q}(\sqrt{-a_3})$, *a prime ideal* $\mathfrak{p} \in \mathcal{O}_k$ *and the corresponding inertia field* $K_E = \mathbb{Q}(\sqrt{-a_2},\sqrt{-a_3})$, *we can exclude the following fields:*

| $(a_1,a_2,a_3)$ | $\alpha$ | $\mathfrak{p}$ | $b \bmod \mathfrak{p}$ |
|---|---|---|---|
| $(1,7,19)$ | $\frac{1}{2}(1+\sqrt{-19})$ | $(2)$ | $\frac{1}{2}(\pm 1-\sqrt{-19})$, $\frac{1}{2}(\pm 3-\sqrt{-19})$, $\frac{1}{2}(\pm 5-\sqrt{-19})$ |
| $(1,3,19)$ | $\frac{1}{2}(1+\sqrt{-19})$ | $(2)$ | $\frac{1}{2}(\pm 1\pm\sqrt{-19})$, $\frac{1}{2}(\pm 3\pm\sqrt{-19})$, $\frac{1}{2}(\pm 5\pm\sqrt{-19})$ |
| $(1,7,91)$ | $\frac{1}{2}(1+\sqrt{-91})$ | $(2)$ | $\frac{1}{2}(\pm 1\pm\sqrt{-91})$ |

*Proof.* We will look at the details of the proof that $K := \mathbb{Q}(\sqrt{-1},\sqrt{-7},\sqrt{-19})$ is not norm-Euclidean. The proofs for the other fields listed in the table above are similar.

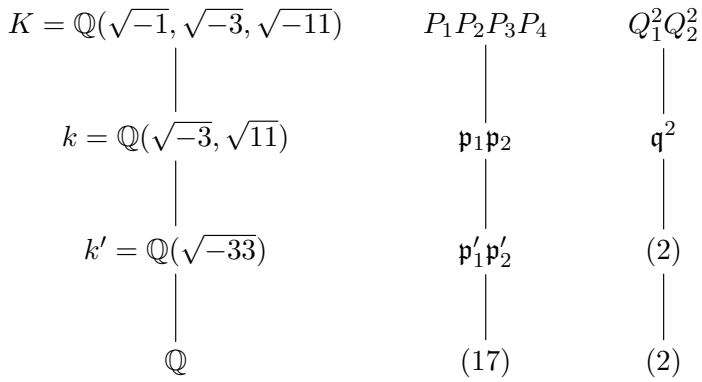
Choose the subfield $k$ to be $\mathbb{Q}(\sqrt{-19})$. If we choose $\mathfrak{p} = (2)$, a prime ideal in $\mathcal{O}_k$, then the inertia field is $K_E = \mathbb{Q}(\sqrt{-7},\sqrt{-19})$. Choose $\alpha = \frac{1}{2}(1+\sqrt{-19})$, then $\alpha^4 = \frac{1}{2}(31-9\sqrt{-19})$. Now $e = [K : K_E] = 2$ so $n/e = 4/2 = 2$ and $|N_{k/\mathbb{Q}}(\mathfrak{p})|^2 = 16$, and the options for $b \in \mathcal{O}_k$ with $|N_{k/\mathbb{Q}}(b)| < 16$ are $b_1 := \frac{1}{2}(-1-\sqrt{-19})$, $b_2 := \frac{1}{2}(3-\sqrt{-19})$ and $b_3 := \frac{1}{2}(-5-\sqrt{-19})$. Computing these norms we have that $N_{k/\mathbb{Q}}(b_1) = 5$, $N_{k/\mathbb{Q}}(b_2) = 7$ and $N_{k/\mathbb{Q}}(b_2) = 11$. However, considering how 5, 7 and 11 factor in $\mathcal{O}_K$ we see that there are no elements in $\mathcal{O}_K$ with absolute norm 5, 7 or 11; thus no possible $b$ satisfies condition 1 of Proposition 4.2.3, so $K$ is not norm-Euclidean.

□

**Lemma 4.2.10.** *The field* $K = \mathbb{Q}(\sqrt{-1},\sqrt{-3},\sqrt{-11})$ *is not norm-Euclidean.*

*Proof.* In order to prove this, we are going to consider an element which generates a prime ideal lying over (17) in $\mathcal{O}_K$, modulo an ideal lying over (2) in $\mathcal{O}_K$.

Let $k = \mathbb{Q}(\sqrt{-3}, \sqrt{11})$ and $k' = \mathbb{Q}(\sqrt{-33})$. For prime ideals $P_1, P_2, P_3, P_4, Q_1, Q_2 \subset \mathcal{O}_K$, $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{q} \subset \mathcal{O}_k$ and $\mathfrak{p}_1', \mathfrak{p}_2' \in \mathcal{O}_{k'}$ we have the following factorizations of (2) and (17) in the rings of integers of these fields:




Assume that these prime ideals are named such that $\mathfrak{p}_1\mathcal{O}_K = P_1P_2$. Since $K$ has class number 1, there exist irreducible elements which generate these ideals. Choose $p_1, p_2, q_1, q_2 \in \mathcal{O}_K$ such that $P_i = (p_i)$ and $Q_i = (q_i)$ for $i = 1, 2$, and also such that $\sigma(p_1) = p_2$ and $\sigma(q_1) = q_2$, where $\sigma$ denotes the automorphism of $K$ which fixes $k$.

If $\mathcal{O}_K$ is norm-Euclidean, then the residue class of $p_1$ mod $Q_1Q_2$ must contain an element $r \in \mathcal{O}_K$ such that $|N_{K/\mathbb{Q}}(r)| < N_{K/\mathbb{Q}}(Q_1Q_2) = 16$. Any element of this residue class is of the form $p_1 + xq_1q_2$ for some $x \in \mathcal{O}_K$, and

$$\begin{aligned} N_{K/k}(p_1 + xq_1q_2) &= p_1\sigma(p_1) + p_1\sigma(xq_1q_2) + \sigma(p_1)xq_1q_2 + xq_1q_2\sigma(xq_1q_2) \\ &= p_1p_2 + q_1q_2\left[p_1\sigma(x) + p_2x + x\sigma(x)q_1q_2\right]. \end{aligned}$$

Now this norm lies in $\mathcal{O}_k$, and we know that $p_1p_2\mathcal{O}_k = \mathfrak{p}_1$ and $q_1q_2\mathcal{O}_k = \mathfrak{q}$. Denote by $p, q$ the irreducible elements of $\mathcal{O}_k$ which are given by $p := p_1p_2$ and $q := q_1q_2$. Then $(p) = \mathfrak{p}_1$, $(q) = \mathfrak{q}$ and

$$N_{K/k}(p_1 + xq_1q_2) \equiv p \bmod \mathfrak{q};$$

for $y \in \mathcal{O}_k$ write $N_{K/k}(p_1 + xq_1q_2) = p + yq$. Then, letting $\tau$ be the automorphism of $k$ which fixes

$k'$, we have

$$\begin{aligned} N_{K/k'}(p_1 + xq_1q_2) &= N_{k/k'}\left(N_{K/k}(p_1 + xq_1q_2)\right) \\ &= N_{k/k'}(p + yq) \\ &= p\tau(p) + p\tau(yq) + \tau(p)yq + \tau(yq)yq. \end{aligned}$$

Now since $\mathfrak{p}_1$ is the only prime ideal in $\mathcal{O}_k$ lying over $\mathfrak{p}_1' \subset \mathcal{O}_{k'}$, then $p \in \mathfrak{p}_1$ implies that $\tau(p) \in \mathfrak{p}_1$. Thus $p\tau(p) \in \mathfrak{p}_1'^2$ when $p\tau(p)$ is considered as an element of $\mathcal{O}_{k'}$. Further, we can easily see that $N_{k'/\mathbb{Q}}(p\tau(p)) = 17^2$ by considering the splitting of the prime (17) in the fields we are working in. Also note that $p\tau(p) \neq 17$, because $(17) \not\subseteq \mathfrak{p}_1'^2 \subseteq (p\tau(p))$ as (17) is unramified in $\mathcal{O}_{k'}$. Therefore, $p\tau(p)$ must be some element of $\mathcal{O}_{k'}$ which is not equal to 17 yet has norm equal to $17^2$. The only such elements which fit this description are $\pm 16 \pm \sqrt{-33}$. Thus,

$$N_{K/k}(p_1 + xq_1q_2) = \pm 16 \pm \sqrt{-33} + p\tau(yq) + \tau(p)yq + yq\tau(yq).$$

Now since $\mathfrak{q}$ is the only prime ideal lying over (2) in $\mathcal{O}_k$, then $q \in \mathfrak{q}$ implies that $\tau(q) \in \mathfrak{q}$. Also, $\mathfrak{q} \cap \mathcal{O}_{k'} = (2)$, so we have the congruence

$$N_{K/k'}(p_1 + xq_1q_2) \equiv \pm 16 \pm \sqrt{-33} \bmod (2).$$

Clearly, there are no elements $r \in \mathcal{O}_{k'}$ in this residue class such that $|N_{k'/\mathbb{Q}}(r)| < N_{K/\mathbb{Q}}(Q_1Q_2) = 16$; the elements of smallest norm are $\pm\sqrt{-33}$, which have norm equal to $-33$. Therefore $K = \mathbb{Q}(\sqrt{-1}, \sqrt{-3}, \sqrt{-11})$ cannot be norm-Euclidean.

□

## 4.3 The Limitations of This Method

Since Proposition 4.2.6 uses a subfield $k$ of a number field $K$ to understand whether or not $K$ is norm-Euclidean, it is natural to ask about the relationship between the Euclidean minimum of $k$ and that of $K$. In particular, it seems that if the subfields of $K$ are norm-Euclidean, then it may be more likely that $K$ is norm-Euclidean as well.

If we take $K$ to be an arbitrary number field and $k$ to be a norm-Euclidean subfield of $K$, with a prime $\mathfrak{p} \subset k$ then for any choice of $\alpha$, the Euclideanity of $k$ guarantees that there exists $b \equiv \alpha^n \bmod \mathfrak{p}$ such that $|N_{k/\mathbb{Q}}b| < |N_{k/\mathbb{Q}}\mathfrak{p}|$, so we will always be able to find $b$ satisfying conditions (2) and (3) of the proposition in this case. Therefore, the only way to use this proposition in order to show that $K$ is not Euclidean is to assure that there is no possible value for $b$ satisfying (2) and (3) which is also the relative norm of some element of $\mathcal{O}_K$.

An example of when this proposition can be used to show that a field is not Euclidean, despite the presence of Euclidean subfields is when $K = \mathbb{Q}(\sqrt{-7}, \sqrt{-11})$. Both of the imaginary quadratic subfields, $\mathbb{Q}(\sqrt{-7})$ and $\mathbb{Q}(\sqrt{-11})$ are Euclidean; take $k := \mathbb{Q}(\sqrt{-11})$. Then the prime $\mathfrak{p} := (7)$ ramifies completely in $K/k$. If we let $\alpha = 2 + \sqrt{-11}$ then

$$\alpha^2 \equiv \frac{7 + \sqrt{-11}}{2} \bmod \mathfrak{p}.$$

If we choose $b = \frac{7+\sqrt{-11}}{2}$ then $N_{k/\mathbb{Q}}(b) = 15$ which is clearly smaller than $N_{k/\mathbb{Q}}(7)^2 = 49$. However, the primes lying over 3 and 5 in $\mathcal{O}_k$ remain inert in $K/k$, which means that this choice for $b$ cannot be the relative norm of any element in $\mathcal{O}_K$. Any other choice for $b$ has norm which is too large, so Proposition 4.2.2 implies that $K$ is not Euclidean.

In our situation, Proposition 4.2.6 is more powerful than 4.2.2, so we are going to look at Proposition 4.2.6, and consider the limitations on it. First, since we are only considering imaginary triquadratic fields, I am going to re-state this proposition, tailored directly to the fields in question.

**Proposition 4.3.1.** *Let $K$ be an imaginary triquadratic number field and $k$ an imaginary quadratic subfield of $K$. Let $\mathfrak{p} \subset \mathcal{O}_k$ be a non-zero prime ideal which is a square in $K$. Let $K_E$ denote the imaginary biquadratic field which is the inertia field of $\mathfrak{p}$; that is the field such that all of the ramification of $\mathfrak{p}$ occurs between $K_E$ and $K$. If $K$ is norm-Euclidean, then for any $\alpha, \beta \in \mathcal{O}_{K_E} \setminus \mathfrak{p}$ with $\beta \equiv \alpha^2 \bmod \mathfrak{p}$, there exists $b \in \mathcal{O}_{K_E}$ such that*

*(1) $N_{K_E/\mathbb{Q}}(b) = N_{K/\mathbb{Q}}(\delta)$ for some $\delta \in \mathcal{O}_K$,*

*(2) $b \equiv \beta \bmod \mathfrak{p}$ and*

*(3)* $|N_{K_E/\mathbb{Q}}b| < |N_{K_E/\mathbb{Q}}\mathfrak{p}|$.

**Remark 4.3.2.** This proposition is using a combination of $K_E$ and $k$ in place of where the original proposition just uses $k$. Esentially, $k$ is still playing the same role as before, but we want to study elements in $K_E$ as often as possible, because we can usually glean more information about our element $b$ through looking at the image of $b$ in a larger field, like $K_E$, rather than pulling it all the way down to $k$.

**Remark 4.3.3.** Here is a summary of why the changes to Proposition 4.2.6 which appear in Proposition 4.3.1 are present:

(1) The subfield $k$ will always be an imaginary quadratic field, because it is very simple to bound the norms of elements in such a field. In any imaginary quadratic field, there are a finite number of integers with norm equal to any given nonnegatve rational integer. In the case of real quadratic fields and (real or imaginary) biquadratic fields, there are infinitely many integers of any possible non-zero norm.

(2) The ideal $\mathfrak{p}$ should always be a prime in $\mathcal{O}_k$ which is ramified in $\mathcal{O}_K$. The reason we must take $\mathfrak{p}$ to be ramified is that otherwise we would simply be doing the division algorithm on elements of $\mathcal{O}_K$.

(3) Further, the prime $\mathfrak{p}$ should actually have ramification index of 2 in $K/k$. This is because the only prime which can ramify to a fourth power in $K/k$ is (2), but any cases where this occurs are already proven to not be norm-Euclidean.

(4) Last, condition (1) of the proposition states that our $b$ should satisfy $b = N_{K/k}\delta$ for some $\delta \in \mathcal{O}_K$. In general, if we take any element of $\mathcal{O}_k$ it is very difficult to know if it is in fact equal to the relative norm of some element of $\mathcal{O}_K$. The only realistic way to do this is to look at a weaker condition: If $b = N_{K/k}\delta$ for some $\delta$ in $\mathcal{O}_K$ then this implies that $N_{K_E/\mathbb{Q}}(b) = N_{K/\mathbb{Q}}(\delta)$ for some $\delta \in \mathcal{O}_K$. This is much easier to do, because this only

requires us to understand the splitting and ramification of the rational primes dividing $N_{K/\mathbb{Q}}(\delta)$ in $\mathcal{O}_K$.

**Lemma 4.3.4.** *Let $K$ be an imaginary triquadratic field of class number 1, and $\mathfrak{p}$ be a prime of some imaginary quadratic subfield $k$ of $K$ such that the ramification index of $\mathfrak{p}$ in $K/k$ is equal to 2. Let $K_E$ be the inertia field for $\mathfrak{p}$. For any $\alpha \in \mathcal{O}_{K_E} \setminus \mathfrak{p}$, let $\{b_1, ..., b_n\}$, $n \geq 0$ be the list of elements of $\mathcal{O}_{K_E}$ such that $b_i \equiv \alpha^2 \bmod \mathfrak{p}$ and $N_{K/\mathbb{Q}}(b_i) < N_{K_E/\mathbb{Q}}(\mathfrak{p})$. For each $b_i$, factor $(b_i)$ into a product of ideals $(b_i) = X_i^2 Y_i$, where $Y_i$ is squarefree. If there exists $b_i$ such that all prime ideals dividing $Y_i$ split or ramify in $K/K_E$ then the conditions of Proposition 4.3.1 are satisfied for this particular choice of $\alpha$, $k$ and $\mathfrak{p}$.*

*Proof.* Assume that for a given choice of $k, \mathfrak{p}, \alpha$ there exists an $b \equiv \alpha^2 \bmod \mathfrak{p}$ such that $N_{K/\mathbb{Q}}(b) < N_{K_E/\mathbb{Q}}(\mathfrak{p})$. Then this value of $b$ satisfies conditions (2) and (3) of Proposition 4.3.1, so we only need to prove it satisfies condition (1) as well. Assume that the factorization $X^2Y$ of $(b)$ where $Y$ is squarefree satisfies the condition that all prime ideals dividing $Y$ split or ramify in $K/K_E$. Factor $Y$ into primes, $Y = \mathfrak{p}_1 \cdots \mathfrak{p}_\ell$. For each $\mathfrak{p}_j$ in this factorization, there exists a prime ideal $\mathfrak{q}_j$ of $\mathcal{O}_K$ lying over $\mathfrak{p}_j$ such that $N_{K/\mathbb{Q}}(\mathfrak{q}_j) = N_{K_E/\mathbb{Q}}(\mathfrak{p}_j)$. Let $I \subset \mathcal{O}_K$ be the ideal of $\mathcal{O}_K$ given by $I = X\mathfrak{q}_1 \cdots \mathfrak{q}_\ell$. Since $K$ has class number 1, there exists $\delta \in \mathcal{O}_K$ such that $(\delta) = I$. Thus

$$\begin{aligned} N_{K_\mathbb{Q}}(\delta) &= N_{K/\mathbb{Q}}\left(X_i \mathfrak{q}_1 \cdots \mathfrak{q}_\ell\right) \\ &= N_{K_E/\mathbb{Q}}\left(N_{K/K_E}(X) N_{K/K_E}(\mathfrak{q}_1) \cdots N_{K/K_E}(\mathfrak{q}_\ell)\right) \\ &= N_{K_E/\mathbb{Q}}\left(X^2 \mathfrak{p}_1 \cdots \mathfrak{p}_\ell\right) \\ &= N_{K_E/\mathbb{Q}}(b). \end{aligned}$$

Thus $b$ satisfies condition (1) of the proposition as well. □

For example, take $K = \mathbb{Q}(\sqrt{-1}, \sqrt{-5}, \sqrt{-7})$ and notice that (2) is unramified in $K_E = \mathbb{Q}(\sqrt{5}, \sqrt{-7})$, but clearly ramified in $K$. Also, we know that $M(K_E) = \frac{9}{16}$. Then for any choice of $\alpha \in \mathcal{O}_{K_E}$, there will exist an element $b \equiv \alpha^2 \bmod \mathfrak{p}$ such that $N_{K_E/\mathbb{Q}}(b) \leq 9$. Thus $b$ will have norm equal to either 1, 3, 5, 7 or 9. But $\mathcal{O}_{K_E}$ has no elements of norm 3, 5 or 7, since these primes stay

inert in at least one quadratic subfield of $K_E$. Thus $b$ has norm 1 or 9. If the norm is equal to 1, then we may factor $(b) = X^2Y$ where $X = Y = (1)$, and it is trivially true that all primes dividing $Y$ split in $K/K_E$. If the norm is equal to 9 then $b$ must equal a prime lying over (3), so $(b) = X^2Y$ where $X = (1)$ and $Y$ is a prime lying over (3). Then $Y$ splits in $K/K_E$. Therefore, for any choice of $\alpha$ we will be able to find some $b \equiv \alpha^2 \bmod \mathfrak{p}$ where $b$ satisfies the conditions of Proposition 4.3.1.

The prime (7) also ramifies in $K$, with inertia field $K_E = \mathbb{Q}(\sqrt{-1}, \sqrt{-5})$ and $M(K_E) = \frac{5}{16}$. Since (7) does split in this field, we must consider two cases: both when (7) is inert in a quadratic subfield, and when (7) splits.

First assume that $\mathfrak{p}$ is a prime lying over (7). Then $N_{K_E/\mathbb{Q}}(\mathfrak{p}) = 7^2 = 49$. Since $M(K_E) = \frac{5}{16}$ then for any choice of $\alpha$ there exists $b \in \mathcal{O}_{K_E}$ such that $b \equiv \alpha^2 \bmod \mathfrak{p}$ and $|N_{K_E/\mathbb{Q}}(b)|/49 < 5/16$. Thus $|N_{K_E/\mathbb{Q}}(b)| \leq 15$; so it must be equal to 1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 12, 13 or 15. Looking at the factorization of primes in $K_E$ we find that the only numbers in this list which can possibly be norms of an element of $K_E$ are 1, 4, 5, or 9. Using an argument similar to the one above for $\mathfrak{p} = (2)$ we know that the conditions of Proposition 4.3.1 will be satisfied if $b$ has norm 1 or 9. Similarly, if $N_{K_E/\mathbb{Q}}(b) = 4$ then $b = X^2Y$ where $X = (1)$ and $Y$ is a prime lying over (2). Then $Y$ splits in $K/K_E$ so the conditions of Proposition 4.3.1 are also satisfied.

Last, if $N_{K_E/\mathbb{Q}}(b) = 5$ then $b = X^2Y$ where $X = (1)$ and $Y$ is a prime lying over (5). But $Y$ is inert in $K/K_E$, so we cannot apply Lemma 4.3.4 to this. However, if $N_{K_E/\mathbb{Q}}(b) = 5$ we can say that

$$b = u \cdot \sigma\left(\frac{1+\sqrt{5}}{2} + \sqrt{-1}\right),$$

where $u$ is a unit of $\mathcal{O}_{K_E}$ and $\sigma \in \mathrm{Gal}(K_E/\mathbb{Q})$. Further, the element of $\mathcal{O}_{K_E}$ given by $\frac{-\sqrt{5}-3\sqrt{-1}+\sqrt{-5}+3}{2}$ is an element of a prime ideal dividing $7\mathcal{O}_{K_E}$. Since

$$u \cdot \sigma\left(\frac{1+\sqrt{5}}{2} + \sqrt{-1}\right) + u \cdot \sigma\left(\frac{-\sqrt{5}-3\sqrt{-1}+\sqrt{-5}+3}{2}\right) = u \cdot \sigma\left(\frac{\sqrt{-5}-\sqrt{-1}}{2} + 2\right)$$

is an element with norm 29, then we know that the equivalence class $\alpha^2 \bmod \mathfrak{p}$ contains an element of norm 29 when $\mathfrak{p} = \left(\sigma\left(\frac{-\sqrt{5}-3\sqrt{-1}+\sqrt{-5}+3}{2}\right)\right)$. And since (29) splits completely in $K$,

this satisfies the conditions of Proposition 4.3.1. The other prime lying over (7) can be written $\mathfrak{p} = \left(\sigma\left(\frac{\sqrt{5}-3\sqrt{-1}-\sqrt{-5}+3}{2}\right)\right)$. Adding $u$ times this to $b$ also gives an element of norm equal to 29.

Next, if $\mathfrak{p} = (7)$ it has norm 2401 and for any $\alpha$, $\alpha^2 \bmod \mathfrak{p}$ contains an element of norm $\leq 750$ and relatively prime to 7. We also must take $k = \mathbb{Q}(\sqrt{-1})$ as this is the only imaginary quadratic subfield of $K_E$ where (7) is inert. Using this information, we may make a preliminary list of possible norms that some element of the congruence class $\alpha^2 \bmod \mathfrak{p}$ must have. This preliminary list should consist of all integers $x$ such that $1 \leq x \leq 750$ which are relatively prime to 7. This list would contain 643 possible norms. Norms from this list can then be eliminated using the following steps:

(1) Remove anything from the list which, based on the splitting and ramification of primes in $K_E$, cannot possibly be a norm. This shrinks the list to 85 possible norms. The Sage code used to do this elimination is below. This block of code looks at all integers $i$ with $1 \leq i \leq 750$ which are not divisible by 7, and only keeps those integers which are norms of elements of $K_E$.

```
#M the Euclidean minimum for K_E
M=5/16
KE.<a> = NumberField([x^2+1,x^2+5])
K.<b> = KE.extension(x^2+7)
prime=7
def get_norms_list():
    pn=[]
    for i in range(1,M*prime^4+1):
        if i%prime!=0:
            possibly_a_norm = True
            norm_factorization = list(factor(i))
            for n_factor in norm_factorization:
                num_KE_factors = len(KE.factor(n_factor[0]))*KE.factor(n_factor[0])[0][1]
                exponent_factor = int(4/num_KE_factors)
```

```
                if n_factor[1]%exponent_factor != 0:
                    possibly_a_norm = False
            if possibly_a_norm:
                pn.append(i)
    return pn
norms_step_1 = get_norms_list()
```

(2) Since $\mathfrak{p} = (7)$ is inert in $k$, elements in the congruence class $\alpha^2 \bmod 7$ must have norms which are squares modulo 7. Eliminating anything which is not a square mod 7, we are left with a list of 47 norms.

```
def squares_mod_7():
    pn=[]
    for norm in norms_step_1:
        if norm%7==1 or norm%7==2 or norm%7==4:
            pn.append(norm)
    return pn
norms_step_2=squares_mod_7()
```

(3) Last, remove 1 and any norms such that all prime factors of that norm split or ramify between $K_E$ and $K$, as per the lemma. This tells us that for any $\alpha \in \mathcal{O}_{K_E} \setminus \{(7)\}$, there exists $b \equiv \alpha^2 \bmod \mathfrak{p}$ such that either $b$ satisfies the lemma, or $N_{K_E/\mathbb{Q}}(b)$ is in the following list:

$$\{25, 100, 205, 225, 305, 400, 445, 505, 625, 725\}.$$

This is done using the Sage code below. Note that 7 is the only prime which ramifies in $K/K_E$. Since our norms list consists only of norms which are relatively prime to 7, we are only interested in whether or not their factors split in $K/K_E$ and need not look at ramification.

```
norms_step_2.remove(1)
```

```
def remove_splitting_norms():
    pn=[]
    for norm in norms_step_2:
            keep_this_norm = False
            norm_factorization = list(factor(norm))
            for n_factor in norm_factorization:
                num_distinct_KE_factors = len(KE.factor(n_factor[0]))
                num_distinct_K_factors = len(K.factor(n_factor[0]))
                if num_distinct_K_factors == num_distinct_KE_factors:
                    keep_this_norm=True
            if keep_this_norm:
                pn.append(norm)
    return pn
norms_step_3=remove_splitting_norms()
```

Using this list of integers, we can then find a list of all integers of $K_E$, up to conjugation and multiplication by a unit, with these norms. Considering each of these integers of $K_E$, we find that there exists an element of (7) which can be added to this integer in order to obtain a new integer with norm smaller than $7^4$ such that every prime dividing this new integer splits or ramifies in $K/K_E$, as outlined in the following table:

| norm | integer(s) of $K_E$ | element of (7) | norm of the sum |
|---|---|---|---|
| 25 | $\frac{1}{2}\sqrt{5}+\frac{5}{2}$ | $-\frac{7}{2}\sqrt{5}-\frac{21}{2}$ | 361 |
| 100 | $\frac{1}{2}\sqrt{5}+\frac{1}{2}\sqrt{-5}+\frac{5}{2}\sqrt{-1}+\frac{5}{2}$ | $-\frac{7}{2}\sqrt{5}-\frac{7}{2}\sqrt{-5}-\frac{21}{2}\sqrt{-1}-\frac{21}{2}$ | 1444 |
| 205 | $\sqrt{5}+3\sqrt{-1}+1$ | $-7\sqrt{5}-\frac{7}{2}\sqrt{-5}-\frac{21}{2}\sqrt{-1}-14$ | 261 |
| | $-\sqrt{5}+\sqrt{-5}+2\sqrt{-1}+1$ | $-\frac{7}{2}\sqrt{5}-\frac{21}{2}$ | 149 |
| 225 | $-\sqrt{5}-\frac{3}{2}\sqrt{-5}-\frac{5}{2}\sqrt{-1}$ | $-\frac{7}{2}\sqrt{5}-\frac{21}{2}$ | 421 |
| 305 | $\frac{1}{2}\sqrt{-5}+\frac{1}{2}\sqrt{-1}-4$ | $-\frac{7}{2}\sqrt{5}-\frac{7}{2}$ | 116 |
| | $-\sqrt{5}-\frac{3}{2}\sqrt{-5}+\frac{1}{2}\sqrt{-1}-1$ | $-\frac{7}{2}\sqrt{5}+\frac{7}{2}\sqrt{-5}+\frac{7}{2}\sqrt{-1}-\frac{21}{2}$ | 1229 |
| 400 | $\sqrt{-5}+5\sqrt{-1}$ | $-\frac{7}{2}\sqrt{-5}-\frac{21}{2}\sqrt{-1}$ | 1 |
| 445 | $\frac{1}{2}\sqrt{5}+3\sqrt{-1}+\frac{7}{2}$ | $-\frac{7}{2}\sqrt{5}-\frac{7}{2}\sqrt{-5}-\frac{21}{2}\sqrt{-1}-\frac{21}{2}$ | 81 |
| | $-\frac{1}{2}\sqrt{5}+2\sqrt{-5}+\sqrt{-1}+\frac{1}{2}$ | $-\frac{7}{2}\sqrt{5}+\frac{7}{2}\sqrt{-5}+\frac{21}{2}\sqrt{-1}-\frac{21}{2}$ | 1621 |
| 505 | $\sqrt{5}-\frac{1}{2}\sqrt{-5}+\frac{7}{2}\sqrt{-1}+2$ | $-7\sqrt{5}+\frac{7}{2}\sqrt{-5}+\frac{7}{2}\sqrt{-1}-14$ | 1744 |
| | $-\sqrt{5}+\frac{3}{2}\sqrt{-5}+\frac{3}{2}\sqrt{-1}+2$ | $-\frac{7}{2}\sqrt{5}-\frac{21}{2}$ | 2164 |
| 625 | $\frac{3}{2}\sqrt{5}-3\sqrt{-5}-5\sqrt{-1}+\frac{5}{2}$ | $-\frac{21}{2}\sqrt{5}+\frac{7}{2}\sqrt{-5}+\frac{7}{2}\sqrt{-1}+\frac{35}{2}$ | 261 |
| | $\frac{3}{2}\sqrt{5}+3\sqrt{-5}+5\sqrt{-1}+\frac{5}{2}$ | $-\frac{21}{2}\sqrt{5}+7\sqrt{-5}-28\sqrt{-1}+\frac{35}{2}$ | 1556 |
| 725 | $-\sqrt{5}-\sqrt{-5}-5$ | $\frac{7}{2}\sqrt{-5}+\frac{7}{2}\sqrt{-1}$ | 1621 |

Therefore, Proposition 4.3.1 cannot be used in conjunction with this choice of $K$ if $\mathfrak{p}=(7)$ or $\mathfrak{p}$ is a prime over (7).

The other rational prime which ramifies in $K$ is (5). This ideal has inertia field $K_E=\mathbb{Q}(\sqrt{-1},\sqrt{-7})$ and $M(K_E)=\frac{1}{2}$.

First consider the case where $\mathfrak{p}$ is a prime lying over (5) in $K_E$. Then $N_{K_E/\mathbb{Q}}(5)=25$, and since $M(K_E)=\frac{1}{2}$, for any $\alpha\in K_E\setminus(5)$ there exists an element $b\equiv\alpha^2 \bmod \mathfrak{p}$ with $N_{K_E/\mathbb{Q}}(b)\leq 12$. Looking at the splitting and ramification of primes in $K_E$ to determine which norms are in fact possible, we have that $N_{K_E/\mathbb{Q}}(b)\in\{1,2,4,8,9\}$ However, 1 and 9 can be removed from this list for

the same reasons as before. Thus, if $b$ does not satisfy the lemma, it has norm equal to 2, 4 or 8, and $b$ is not a square. Further, $K$ has no element of norm equal to 2, so in fact the norms 2 and 8 are not possible. Putting this together we can conclude that if there were to exist a value for $b$ satisfying the conditions of the proposition, it would have to satisfy $N_{K_E/\mathbb{Q}}(b) = 4$, and $b$ could not be a square in $\mathcal{O}_{K_E}$. Thus $b = u(1 \pm \sqrt{-1})$ for some unit $u$ of $\mathcal{O}_{K_E}$. But $(5) = (2+\sqrt{-1})(2-\sqrt{-1})$, and $-1 \equiv (1+\sqrt{-1}) \bmod (2+\sqrt{-1})$ and $-\sqrt{-1} \equiv (1+\sqrt{-1}) \bmod ((2-\sqrt{-1})\sqrt{-1})$, so this choice for $b$ is congruent to an element modulo $\mathfrak{p}$ which does satisfy the conditions of the proposition. Therefore, the proposition cannot be used to classify this field as non-norm-Euclidean when $\mathfrak{p}$ is a prime lying over (5).

Last, if $\mathfrak{p} = 5$ we have that $k = \mathbb{Q}(\sqrt{-7})$ and must consider possible $b$ values with $N_{K_E/\mathbb{Q}}(b) \leq \frac{1}{2}5^4 = 312.5$. Repeating the same process we used to find possible $b$ values in the case of $\mathfrak{p} = 7$, we find a list of 13 norms which we need to investigate further:

$$\{4, 16, 36, 64, 74, 106, 116, 144, 196, 226, 256, 274, 296\}.$$

For most norms in this list, it is easy to find elements in the ideal (5) which can be added to elements which have these norms and find that the proposition cannot be used with these norms. In fact, we find that the following norms cannot be eliminated through trial and error, by adding or subtracting elements of (5) with small coefficients to them:

| norm | integer(s) of $K_E$ |
|---|---|
| 64 | $\frac{17}{2}\sqrt{7} + \frac{3}{2}\sqrt{-1} + \frac{1}{2}\sqrt{-7} + \frac{45}{2}$ |
| 256 | $-\sqrt{7} + 7\sqrt{-1} + 3\sqrt{-7} - 3$ |
| 296 | $2\sqrt{7} + 28\sqrt{-1} + \frac{21}{2}\sqrt{-7} + \frac{11}{2}$ |
| | $-\frac{7}{2}\sqrt{7} - \frac{7}{2}\sqrt{-1} - \sqrt{-7} - 9$ |

This tells us that if Proposition 4.3.2 were to be useful in proving this number field is not norm-Euclidean, we would have to choose our prime $\mathfrak{p} = 5$ in $k = \mathbb{Q}(\sqrt{-7})$ with intertia field $K_E = \mathbb{Q}(\sqrt{-1}, \sqrt{-7})$. Further, our $\alpha \in \mathcal{O}_{K_E}$ would need to be chosen such that $\alpha^2$ is equivalent,

mod $\mathfrak{p}$, to one of the elements listed in the above table. It is unknown whether or not this is possible, but the author hopes to investigate this number field more closely in the future.

## Bibliography


[1] S. Arno, The imaginary quadratic fields of class number 4, Acta Arith. **60** (1992), 321–334.

[2] Swinnerton-Dyer P.F. Barnes, E.S., The inhomogeneous minima of binary quadratic forms (ii), Acta Mathematica **88** (1952), 279–316.

[3] Parry-C. Brown, E., The imaginary bicyclic biquadratic fields with class-number 1, Journal für die reine und angewandte Mathematik **266** (1974), 118–120.

[4] J.P. Cerri, Inhomogeneous and euclidean spectra of number fields with unit rank strictly greater than 1, Journal für die reine und angewandte Mathematik **592**.

[5] D. Clark, A quadratic field which is euclidean but not norm-euclidean, Manuscripta Math.

[6] H. Cohen, A course in computational algebraic number theory, Springer-Verlag, 1993.

[7] H. Davenport, Multiplicative number theory, Springer, 1980.

[8] L. Dirichlet, Recherches sur les forms quadratiques à coéfficients et à indeterminées complexes, J. Reine Angew. Math. **24** (1842), 291–371.

[9] A. Frölich, Central extensions, galois groups, and ideal class groups of number fields, Contemporary Math **24** (1983), 1–86.

[10] C. F. Gauss, Disquisitiones arithmeticae, 1801.

[11] H. Heilbronn, On the class number in imaginary quadratic fields, Quart. J. Math. Oxford **25** (1934), 150–160.

[12] G. Herglotz, Über einen dirichletschen satz, Math. Zeitschrift **12** (1922), 255–261.

[13] T. Kubota, über den bizyklischen biquadratischen zahlkörper, Nagoya Math. J. **10** (1955), 65–85.

[14] R. Kučera, On the parity of the class number of a biquadratic field, J. Number Theory **52** (1995), 43–52.

[15] F. Lemmermeyer, The euclidean algorithm in algebraic number fields, Expo. Math.

[16] ———, Euclid's algorithm in quartic cm-fields, arXiv:1108.6215v1[math.NT].

[17] ———, Kuroda's class number formula, Acta Arith. **66** (1994), 245–260.

[18] P. Lezowski, euclid (version 1.0), http://www.math.u-bordeaux1.fr/ plezowsk/euclid/index.php.

[19] D. Marcus, Number fields, Springer-Verlag, 1977.

[20] A. Mouhib, On the parity of the class number of multiquadratic number fields, J. Number Theory **129**, 1205–1211.

[21] P. Ribenboim, Classical theory of algebraic numbers, Springer, 2001.

[22] B. Schmal, Diskriminanten, $\mathbb{Z}$-ganzheitsbasen und relative ganzheitsbasen bei multiquadratischen zahlkorpern, Arch. Math. (Basel) **52** (1989), 245–257.

[23] H.M. Stark, A complete determination of the complex quadratic fields of class-number 1, Michigan Math J. **14** (1967), 1–27.

[24] Franciscus Jozef van der Linden, Euclidean rings with two infinite primes, Ph.D. thesis, Centrum voor Wiskunde en Informatica, Amsterdam, 1984.

[25] T. Vaughan, The discriminant of a quadratic extension of an algebraic field., Mathematics of Computation **40** (1983), 685–707.

[26] P. Weinberger, On euclidean rings of algebraic integers, Proc. Symp. Pure Math.

[27] K. Williams, Integers of biquadratic fields, Canad. Math. Bull.