Cyclotomic Euclidean Number Fields

Reza Akhtar

Senior thesis

Submitted to the Department of Mathematics
In partial fulfillment of the requirements
For the Degree of Bachelor of Arts with Honors

24th March, 1995

Acknowledgements

I would like to express my gratitude to my advisor, Barry Mazur, for his guidance and criticism of my work, also to Hendrik Lenstra of the University of California, Berkeley for providing me with many of the references which I have used in writing this thesis. In addition, I would like to thank Michael Zieve (Berkeley), Larry Roberts (University of British Columbia), Bill Bradley, and Leonid Fridman for giving me numerous useful suggestions regarding the content of this work, helping me with typsetting, and editing drafts. Finally, I extend my thanks to all the mathematics teachers I have had, beginning with my mother, for preparing me to undertake this challenging yet rewarding task.

Contents

1 Introduction

This thesis is concerned with an abstraction of an ancient problem, which we henceforth refer to as *euclidean division*. To be specific, a euclidean division of an integer a by a nonzero integer b is an expression of the form $a = bq + r$, where q and r are integers and r is strictly less than b. The justification for this nomenclature is derived from the fact that the existence of a euclidean division of any integer a by any nonzero integer b is exactly what drives the so-called *euclidean algorithm* for finding the greatest common divisor of a and b. Although the proof of the existence of a euclidean division of any integer a by a nonzero integer b is trivial, the problem becomes much more interesting when abstracted into a more general setting.

Now let R be an arbitrary integral domain: what would the analogous definition of euclidean division be? In particular, with what do we replace the notion of absolute value? We need some concept of size, which is supplied by a *euclidean function*

$$\sigma : R - \{0\} \longrightarrow \mathbf{N}$$

Then we say that R is a *euclidean domain* if there exists a euclidean function σ such that

- For all $a, b \in R - \{0\}$, $\sigma(ab) \geq \sigma(a)$
- For all $a \in R$, $b \in R - \{0\}$, there exist $q, r \in R$ such that $a = bq + r$ and either
  1. $r = 0$ or
  2. $\sigma(r) < \sigma(b)$

Having formulated such a definition, the natural task at hand is the classification of euclidean domains. This is indeed a daunting problem, and, needless to say, it has not yet been solved. To give an illustration of its complexity, consider the following scenario: any integral domain R is either a euclidean domain or is not; in the former case, we might be able to get a proof if we are lucky enough to stumble upon a euclidean function which works—in the latter case, however, it is no light matter to prove that *no* euclidean function exists. In spite of these difficulties, significant progress has been made towards the solution of the problem for special classes of integral domains. In isolated cases, the problem has been solved completely; take, for example, the rings of integers in imaginary quadratic number fields [Mo 49]. In most others, however, only partial results have been achieved.

The objective of this thesis is to investigate a special case of the abovementioned problem. Attention will be restricted to the ring R of algebraic integers in a cyclotomic field extension K of the rational numbers $\mathbf{Q}$; furthermore, we will strengthen the hypothesis on σ to the point of saying that the absolute value of the field norm (restricted to $R - \{0\}$) must also be a euclidean function. Rings which satisfy the above are called *euclidean for the norm*, or simply *norm-euclidean*. It is worth mentioning that the first hypothesis in the definition of a euclidean function is sometimes excluded; however, since it is required to prove the theorems of Chapter 4, we will retain it. As we will see later, the absolute value of the field norm (restricted to the non-zero algebraic integers) automatically satisfies this condition.

Having stated my purpose, I would like to emphasize that the focus of this thesis is the question of the existence of euclidean properties. Cyclotomic rings are being studied only as an example of how one approaches the solution of the classification problem; historically, they happen to have been the first rings to be studied in this context. I intend to survey the main results achieved throughout history towards the solution of this (specialized) problem—consequently, multiple proofs of certain results will be given. It is hoped that this approach will serve to illustrate the diversity of perspectives that can be adopted in investigating the classification problem.

Much of the modern work done towards the solution of the classification problem for cyclotomic rings relies on a variety of constructions from various fields of mathematics, primarily from algebraic number theory. Although I have assumed a basic knowledge of the algebra of groups, ideals, rings, fields, and Galois theory, I have tried to include most of the necessary definitions and lemmas from algebraic number theory, in order to make this report as self-contained as possible. As a result, it has become somewhat longer than initially expected; hence, I have included all the major results in the body of the thesis, and have reserved the appendices for proofs of minor propositions and lemmas.

Following the introduction, the second chapter will survey the history and motivation behind the problem, while the third will provide the reader with the basic notions involved. The fourth chapter, which is quite independent of the rest of the thesis, introduces an equivalent characterization of euclidean domains; the reader can safely skip this chapter, as it contains few results directly relevant to the classification problem for cyclotomic rings. The same results are reproven in Chapter 6 using alternative techniques. The fifth chapter is where the analysis seriously begins; we provide several conditions necessary for a ring to be a euclidean domain, thereby eliminating all but finitely many cyclotomic rings from consideration. The sixth chapter presents, in summary, proofs that specific cyclotomic rings are norm-euclidean, while the seventh chapter is devoted to showing that $\mathbf{Z}[\zeta_{32}]$ is not norm-euclidean. Finally, the concluding chapter comments on cases which have been excluded from discussion.

2 History

As mentioned in the introduction, the concept of euclidean division arose in Euclid's work two and a half thousand years ago, but it was only in the 1840s that people became seriously interested in euclidean domains. Still, they were not interested in euclidean domains *per se*; they wanted to prove Fermat's Last Theorem.

On March 1st, 1847, at the meeting of the Académie des Sciences in Paris, the French mathematician Gabriel Lamé claimed to have succeeded in proving Fermat's Last Theorem. After Lamé had finished presenting his proof, Liouville, who was also present at that meeting, raised a concern: could Lamé justify his assumption that unique factorization held in $\mathbf{Z}[e^{2\pi i/n}]$ for all n?

Lamé and Cauchy did not share Liouville's skepticism, though, and spent the next few months fruitlessly trying to prove that unique factorization held in $\mathbf{Z}[e^{2\pi i/n}]$ for all n. Only two weeks after Lamé's exposition, Wantzel correctly observed that in order to prove that

$\mathbf{Z}[e^{2\pi i/n}]$ is a unique factorization domain, it suffices to show that it is norm-euclidean. He even thought that he had a proof that all such rings were norm-euclidean; unfortunately, it contained an embarrassingly blatant arithmetic flaw. Meanwhile, Cauchy had been working on specific examples, and was able to prove the proposition for the cases

$$n = 3, 4, 5, 6, 7, 8, 9, 10, 12, 14, 15.$$

The matter finally came to an end when the French mathematicians discovered that Kummer had proved, *prior* to Lamé's exposition, that $\mathbf{Z}[e^{2\pi i/23}]$ was *not* a unique factorization domain!

Thus the norm-euclidean question sadly became unfashionable soon after it was proposed; the main problem, of course, was lack of information. If people knew exactly those n for which $\mathbf{Z}[e^{2\pi i/n}]$ was a unique factorization domain, they would have known that it was not even worth trying to prove that $\mathbf{Z}[e^{2\pi i/n}]$ was norm-euclidean for other n; without such information, however, the question was virtually intractable. In any case, it was not entirely neglected; in particular, it gave rise to three important problems, which we henceforth refer to as **P1**, **P2**, and **P3**.

- **P1**. Determine all n such that unique factorization into irreducible elements holds in $\mathbf{Z}[e^{2\pi i/n}]$.
- **P2**. Determine all n such that $\mathbf{Z}[e^{2\pi i/n}]$ is a euclidean domain.
- **P3**. Determine all n such that $\mathbf{Z}[e^{2\pi i/n}]$ is norm-euclidean.

Between 1847 and 1975, numerous attempts were made towards solving **P3**, although most were of an *ad hoc* nature, giving proofs only for specific values of n. **P1** was finally solved in 1975 by Masley and Montgomery. It happens that there are exactly 46 such n; we will discuss this at greater length in Chapter 5. Soon afterward, **P2** was solved by Weinberger under the assumption of the Generalized Riemann Hypothesis; amazingly, it turns out that the same 46 values of n (and no others) satisfy this condition. Thus, the solution of **P1** gave mathematicians a sense of direction so sorely lacking in the 1840s, and has since given rise to several important results representing partial solutions to **P3**. Nevertheless **P3** remains unsolved, and a description of the attempts made towards its solution is what lies at the heart of this thesis.

3 Basic Definitions

Here we state some definitions and conventions employed throughout the thesis. Only the most basic notions are presented here; a more detailed discussion of background definitions and results is found in the appendices.

Whenever referring to rings, we assume that they are commutative with identity.

The natural numbers $\mathbf{N}$ include 0.

Given $n \in \mathbf{N}$, we define the *Euler function*

$$\phi(n) = |\{a : 1 \leq a \leq n \text{ and } \gcd(a, n) = 1\}|$$

We will reserve the notation ζ_n to represent the complex number $e^{2\pi i/n}$, where $n \in \mathbf{N}$, and refer to the field $\mathbf{Q}(\zeta_n)$ as the *nth cyclotomic field*. For convenience, we refer to $\mathbf{Z}[\zeta_n]$ as the *nth cyclotomic ring*.

Let R be any ring. The *group of units* of R, denoted $R^\times$, is defined to be

$$\{r \in R : \text{ there exists } s \in R \text{ such that } rs = 1\}$$

A ring R is called an *integral domain* if

$$a, b \in R \text{ and } ab = 0 \Rightarrow a = 0 \text{ or } b = 0$$

Equivalently, $ac = bc \Leftrightarrow a = b$.

Definition 3.1 *An integral domain R is called a* euclidean domain *if there exists a function*

$$\sigma : R - \{0\} \longrightarrow \mathbf{N}$$

(called a euclidean function*) such that*

- *For all $a, b \in R - \{0\}$, $\sigma(ab) \geq \sigma(a)$*
- *For all $a \in R$, $b \in R - \{0\}$, there exist $q, r \in R$ such that $a = bq + r$ and either*
  1. *$r = 0$ or*
  2. *$\sigma(r) < \sigma(b)$*

Now let K be a number field (a finite extension of $\mathbf{Q}$). Define

$$Hom(K, \mathbf{C}) = \{\phi : K \longrightarrow \mathbf{C} \mid \phi \text{ is a homomorphism of fields}\}$$

Let $x \in K$ be any element and define the *trace*

$$Tr_{K/\mathbf{Q}}(x) = \sum_{\sigma \in Hom(K,\mathbf{C})} \sigma(x)$$

and the *norm*

$$N_{K/\mathbf{Q}}(x) = \prod_{\sigma \in Hom(K,\mathbf{C})} \sigma(x)$$

When there is no danger of ambiguity, we write Tr_K or simply Tr for $Tr_{K/\mathbf{Q}}$ and N_K or N for $N_{K/\mathbf{Q}}$. Note that for Galois extensions $K/\mathbf{Q}$,

$$Hom(K, \mathbf{C}) = Gal(K/\mathbf{Q})$$

Let R be the ring of algebraic integers in K. Being a subring of a field, R is an integral domain; sometimes we refer to R as a *number ring*.

Definition 3.2 *R is* euclidean for the norm *or* norm-euclidean *if for all $a \in R$ and $b \in R - \{0\}$ there exist $q, r \in R$ such that $a = bq + r$ and $N(r) < N(b)$, where N denotes the absolute value of the field norm $N_{K/\mathbf{Q}}$. In such a case, we say that the field K is* euclidean.

The following proposition follows directly from definitions and from the multiplicativity of the norm:

Proposition 3.3 *R is norm-euclidean $\Rightarrow$ R is a euclidean domain.*

One might well ask if the converse to Proposition 3.3 holds. The answer, far from obvious, is no. Clark [Cl 94] has shown that the ring of integers of the quadratic number field $\mathbf{Q}(\sqrt{69})$ is euclidean but not norm-euclidean.

4 The Structure of Euclidean Domains

The definition of a euclidean domain is rather cumbersome, and it is difficult to prove results about euclidean domains wihout resorting to more sophisticated methods. In 1948, Theodore Motzkin proved a remarkable theorem which gives an equivalent condition for an arbitrary integral domain R to be a euclidean domain—a condition which in some cases can be checked by a straightforward computation. Motzkin's theorem is all the more suprising because it relies solely on definitions; no algebraic or analytic number theory enters into his proof. We state the theorem here (with proof), but caution the reader that it serves only as an illustration of the general structure of euclidean domains—it has few applications (to my knowledge) to the solution of **P3**. Before stating Motzkin's Theorem, we need one definition.

Let R be an integral domain.

Definition 4.1 *Given a subset $P \subseteq R - \{0\}$, the* derived set *of P, denoted P', is defined as $\{b \in P :$ there exists $a \in R$ such that $a + bR \subseteq P\}$*

The ith derived set of P is denoted $P^{(i)}$; by convention, $P^{(0)} = P$.

Theorem 4.2 *Let $P_0 = R - \{0\}$. Then R is a euclidean domain if and only if*

$$\bigcap_{i=0}^{\infty} P_0^{(i)} = \emptyset$$

In order to prove Theorem 4.2, we need some more definitions.

Definition 4.3 *A subset $P \subset R - \{0\}$ is called a* product subset *(of $R - \{0\}$) if it is closed under multiplication in $R - \{0\}$, i.e. $P(R - \{0\}) \subseteq P$*

The following proposition is immediate from the definitions.

Proposition 4.4 *If P is a product subset, then P' is also a product subset.*

Definition 4.5 *A* euclidean chain *(in R) is a sequence $P_0, P_1, \ldots$ of product subsets such that*

1. $P_0 = R - \{0\}$

2. $P_i \supseteq P_{i+1}$ *for all* $i \geq 0$

3. $P_i' \subseteq P_{i+1}$ *for all* $i \geq 0$

4. $\bigcap_{i=0}^{\infty} P^{(i)} = \emptyset$

If $P_0, P_1, \ldots$ and $Q_0, Q_1, \ldots$ are two euclidean chains, then $P_0, P_1, \ldots$ is said to be *faster* than $Q_0, Q_1, \ldots$ if for all i, $P_i \subseteq Q_i$. If a euclidean chain $P_0, P_1, \ldots$ is faster than all other chains $R_0, R_1, \ldots$, we say that $P_0, P_1, \ldots$ is the *fastest* chain on R.

Theorem 4.2 is really a corollary of the following more general theorem.

Theorem 4.6 *There is a bijective correspondence between euclidean chains in* R *and euclidean functions on* $R - \{0\}$

Proof.

Given a euclidean chain $P_0, P_1, \ldots$ and $x \in R - \{0\}$, define

$$\sigma(x) = \max\{i : x \in P_i \text{ and } x \notin P_{i+1}\}$$

Now choose any $a \in R$ and $b \in R - \{0\}$. If $a = 0$ or $\sigma(a) < \sigma(b)$, write $a = 0 \cdot b + a$. Otherwise, assume that $\sigma(a) \geq \sigma(b)$, and suppose, towards a contradiction, that σ is not a euclidean function. Then, for every $q \in R$ and some $a \in R$, $b \in R - \{0\}$, $\sigma(a - bq) \geq \sigma(b)$, so by definition, $b \in P'_{\sigma(b)}$, and since $P_0, P_1, \ldots$ is a euclidean chain, $P'_{\sigma(b)} \subseteq P_{\sigma(b)+1}$, so $\sigma(b) \geq \sigma(b) + 1$, contradiction.

Conversely, given a euclidean function σ on R, define $P_i = \{x \in R - \{0\} : \sigma(x) \geq i\}$. It is easily verified that P_i is a product subset for each i; thus, given $b \in P_i'$, choose a such that $a + bR \subseteq P_i$. Using the fact that σ is a euclidean function, write $a = bq + r$ with $\sigma(r) < \sigma(b)$. Since $a + bR \subseteq P_i$, $\sigma(r) = \sigma(a - bq) \geq i$; whence $\sigma(b) \geq i + 1$, so $P_i' \subseteq P_{i+1}$, as desired. Finally, if $\bigcap_{i=0}^{\infty} P^{(i)} \neq \emptyset$, then there is an element $x \in R - \{0\}$ such that $\sigma(x) \geq i$ for all i, which is impossible; hence $\bigcap_{i=0}^{\infty} P^{(i)} = \emptyset$, and so $P_0, P_1, \ldots$ is a euclidean chain.

The following proposition follows immediately from definitions.

Proposition 4.7 *If* $P_0, P_1, \ldots$ *is any euclidean chain in* R*, then there exists a fastest chain* $R_0, R_1, \ldots$ *given by*

$$R_i = P_0^{(i)}$$

We remark that under the hypotheses of the above proposition, Theorem 4.6 provides us with a euclidean function corresponding to the fastest chain; we refer to this function as the *fastest algorithm* on $R - \{0\}$.

From here, the proof of Theorem 4.2 is very straightforward. The sequence $P_0, P_0^{(1)}, \ldots$, where $P_0 = R - \{0\}$, automatically satisfies posulates (i), (ii), and (iii) of Definition 4.5. So $\bigcap_{i=0}^{\infty} P_0^{(i)} = \emptyset$ if and only if $P_0, P_0^{(1)}, \ldots$ is a euclidean chain if and only if there exists a fastest algorithm on $R - \{0\}$, if and only if (by Proposition 4.7) there exists a euclidean function on $R - \{0\}$.

Example 1

Consider $\mathbf{Z}$, the ring of integers. We verify that the absolute value function is a euclidean function on $\mathbf{Z}$ by showing that the sequence R_i defined by

$$R_0 = \mathbf{Z} - \{0\}$$

$$R_n = \mathbf{Z} - \{0, \pm 1, \ldots, \pm(n-1)\}$$

is a euclidean chain. Properties (i), (ii), and (iv) follow easily from the construction; to see that $R_i' \subseteq R_{i+1}$ it suffices to show that $i \notin R_i'$. If $i \in R_i'$, then there exists $a \in \mathbf{Z}$ such that $a + i\mathbf{Z} \subseteq R_i = \mathbf{Z} - \{0, 1, \ldots, i-1\}$, which is clearly impossible, since $\mathbf{Z} - R_i$ contains a representative of every coset of $i\mathbf{Z}$ in $\mathbf{Z}$. Hence $\mathbf{Z}$ is a euclidean domain.

Computing the fastest algorithm on $\mathbf{Z}$ (See Fig. 1) yields the euclidean chain:

$$P_0 = \mathbf{Z} - \{0\}$$

$$P_0^{(i)} = \mathbf{Z} - \{0, \pm 1, \ldots, \pm(2^i - 1)\}$$

which corresponds to the euclidean function $\phi(n) = \lfloor \log_2 |n| \rfloor$.

Example 2

For our next example, we consider the ring $\mathbf{Z}(\zeta_4) = \mathbf{Z}[i] = \{a + bi : a, b \in \mathbf{Z}\}$ and the function $\sigma : \mathbf{Z}[i] \longrightarrow \mathbf{N}$ given by

$$\sigma(a + bi) = a^2 + b^2$$

We can prove that $\mathbf{Z}[i]$ is a euclidean domain by verifying that the chain

$$R_0 = \mathbf{Z}[i] - \{0\}$$

$$R_n = \mathbf{Z}[i] - \{x \in \mathbf{Z}[i] : |x|^2 \leq n - 1\}$$

is euclidean. The verification is routine and similar to Example 1, so we omit it here for reasons of brevity. If we compute the fastest chain (See Fig. 2) on $\mathbf{Z}[i]$, we obtain

$$P_0 = \mathbf{Z} - \{0\}$$

$$P_0^{(n)} = \mathbf{Z}[i] - \{x \in \mathbf{Z}[i] : |x|^2 \leq n\}$$

which corresponds to the euclidean function $\phi(n) = |n|^2 - 1$. This raises an interesting open question:

Question 4.8 *Let R be the ring of integers in a number field K, and let N denote the absolute value of the field norm. If ϕ is the fastest algorithm on R, under what conditions is $\phi = N - 1$?*

Example 3 As a final example of the use of Motzkin's theorem, we show that the ring $\mathbf{Z}[\sqrt{-5}]$ is *not* a euclidean domain. The following definition will lead to an alternate characterization of the sets P_0' and P_0'', which in turn will simplify the proof:

Definition 4.9 *A non-unit b is called a* side divisor *of $a \in R$ if b divides $a + e$, where $e \in R^\times \cup \{0\}$. If b is a side divisor of every $a \in R$, b is called a* universal side divisor.

Observe that for any ring R, with $P_0 = R - \{0\}$, the set P_0' can also be expressed as

$$P_0' = R - (R^\times \cup \{0\})$$

Furthermore, if U is the set of universal side divisors, then

$$P_0'' = P_0' - U$$

Returning to $R = \mathbf{Z}[\sqrt{-5}]$, note that the only units of R are ± 1. Furthermore, 2 is irreducible, and the only side divisors of 2 and $\pm 2, \pm 3$. However, neither of these is a side divisor of $\sqrt{-5}$, so there are no universal side divisors. Hence $P_0'' = P_0'$ and so

$$\bigcap_{n=0}^{\infty} P_0^{(n)} \neq \emptyset$$

Therefore $\mathbf{Z}[\sqrt{-5}]$ is not a euclidean domain.

It is worth noting that the proof that $\mathbf{Z}[\sqrt{-5}]$ is not a euclidean domain depended strongly on the paucity of units in the ring; few units generally imply few side divisors of any particular element, and hence few (or possibly no) universal side divisors. Motzkin [Mo 49] uses this principle to determine completely the imaginary quadratic fields whose rings of integers are euclidean domains. We will return to the matter of units in the conclusion.

5 Some Necessary Conditions for a Field to be Euclidean

In this section, we begin our description of the results which have aided mathematicians in their attempts to solve **P3**. This particular chapter will be devoted to the demonstration of several basic results from algebraic number theory, which, coupled with a powerful result of Masley and Montgomery, reduce **P3** to a much more tractable (but still nontrivial) problem. To be precise, we will show that there are only thirty values of n, $n \not\equiv 2 \pmod 4$ such that $\mathbf{Z}[\zeta_n]$ *could* be a euclidean domain (and hence norm-euclidean). Before beginning our discussion, though, we need a few definitions. Let R be an integral domain.

Definition 5.1 *An element $x \in R$ is called* irreducible *if $y, z \in R$ and $x = yz$ together imply that exactly one of y, z is a unit.*

Definition 5.2 *An element $x \in R - R^\times$ is called* prime *if $a, b \in R$ and $p \mid ab$ implies $p \mid a$ or $p \mid b$.*

Definition 5.3 Existence of factorizations *(EOF) holds in R if for every $x \in R$, the factorization of x into irreducible elements terminates after finitely many steps.*

Definition 5.4 *R is called a* unique factorization domain *(UFD) if:*

- *EOF holds in R*
- *If $b_1 \cdots b_n$ and $c_1 \cdots c_m$ represent two factorizations of $a \in R$ into irreducible elements, then $m = n$ and there exists a permutation σ of $\{1, \ldots, n\}$ such that $b_i = u_i c_{\sigma(i)}$, where $u_i \in R$ is a unit.*

Definition 5.5 *An ideal $I \subseteq R$ is called* principal *if $I = (r)$ for some $r \in R$.*

Definition 5.6 *R is called a* principal ideal domain *(PID) if every ideal of R is principal.*

Definition 5.7 *Let K be the field of fractions of R. Then $t \in K$ is said to be* integral *over R if it satisfies a monic polynomial in $R[x]$; that is,*

$$t^n + a_{n-1}t^{n-1} + \ldots + a_0 = 0 \text{ for some } a_i \in R$$

Definition 5.8 *R is said to be* integrally closed *if there are no elements of $K - R$ which are integral over R.*

We are now in a position to state our goal, which is to prove

Theorem 5.9 *Let R be an integral domain. Then*

1. *R is a euclidean domain $\Rightarrow$ R is a PID*
2. *R is a PID $\Rightarrow$ R is a UFD*
3. *Let R be the ring of integers in an algebraic number field K. Then R is a UFD $\Rightarrow$ R is a PID.*
4. *Let R be any subring of an algebraic number field K which is also a unique factorization domain. Then R is integrally closed.*

The proof of (1), (2), and (4) are found in Appendix B; while not difficult, they are routine and somewhat unrelated to the subject of discussion. The proof of (3), while historically relevant, is only of peripheral interest to us, so we omit it. We summarize the results of Theorem 5.9 and Proposition 3.3 as follows:

R norm-euclidean $\Rightarrow R$ is a euclidean domain $\Rightarrow R$ is a PID $\Rightarrow R$ is a UFD $\Rightarrow R$ is integrally closed

With Theorem 5.9 at our disposal, we now have enough to evaluate our progress towards each of the problems **P1**, **P2**, and **P3**. In particular, we know that if a cyclotomic ring is norm-euclidean, it *must* be a PID and a UFD. The next theorem is a powerful result from analytic number theory, which we state here without proof. It allows us, in conjunction with Theorem 5.9 (2) and (3), to determine exactly which cyclotomic rings admit unique factorization.

Theorem 5.10 *(Masley and Montgomery, 1975) There are precisely 30 values of* n, $n \not\equiv 2 \pmod 4$ *for which* $\mathbf{Z}[\zeta_n]$ *is a principal ideal domain. These are*

$$n = 1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84$$

Historically, at least, the proof of the above theorem was a milestone in the solution of **P3**. It helps us understand why Cauchy and Wantzel were willing to believe that unique factorization held in all cyclotomic rings—the smallest counterexample, $n = 23$, has $\phi(23) = 22$. It also explains the lack of attention given to the problem between 1847 and 1975—all previous attempts towards finding a general solution had failed; solutions for specific cases were interesting in their own right, but nobody knew how many (or even whether there were finitely or infinitely many) cases to check. Thus, the majority of solutions accomplished during this time period (1847-1975) were of an *ad hoc* nature; subsequent to the proof of Theorem 5.10, though, several valiant attempts (some of them quite successful) were made towards proving that $\mathbf{Z}[\zeta_n]$ is norm-euclidean for n in the above list. At present, about half of the cases have been checked; all but one have been found to be norm-euclidean, and the remaining cases are untreated, to the best of my knowledge. The next chapter provides an overview of some of the methods which have been employed to show that specific cyclotomic fields are euclidean.

6 Some Sufficient Conditions for a Field to be Euclidean

As mentioned in the previous section, the current chapter, which is truly the heart of this thesis, will survey the work done towards the solution of **P3**, using the results of the previous chapter. As mentioned before, the reader will find that certain cases are proven more than once—the repetition is intentional, and is intended to demonstrate how more sophisticated techniques can simplify the solution of already-solved problems, or extend an older idea to accomplish the solution of a wider class of problems. The most beautiful aspect of the solutions presented here is that almost all of them rely upon geometric intuition of the sort described in Chapter 4. The following table gives an idea of the relative difficulty of the problem for various values of n, as measured by when (chronologically) the solution was achieved.

n	$\phi(n)$	*Date of first proof*	*Name of mathematician*
1	1	300 B.C.	Euclid
4	2	1801	Gauss
5	4	1844	Kummer
7	6	1844	Kummer
3	2	1847	Wantzel
9	6	1847	Cauchy
15	8	1847	Cauchy
8	4	1850	Eisenstein
12	4	1850	Eisenstein
20	8	1975	H. W. Lenstra
11	10	1975	H. W. Lenstra
16	8	1977	Ojala
24	8	1978	H. W. Lenstra
13	12	1988	McKenzie

Based on the table above, it can be inferred that $\phi(n)$, which by Proposition A.1 is the degree of the field extension $\mathbf{Q}(\zeta_n)/\mathbf{Q}$, is a fairly good measure of the complexity of the problem of determining whether or not $\mathbf{Q}(\zeta_n)$ is euclidean. We shall, therefore, describe the various methods of solution in roughly increasing order of $\phi(n)$. Before beginning, though, we need the following extremely important proposition, which gives an alternate characterization of norm-euclidean rings.

Proposition 6.1 *Let R be the ring of integers in a number field K. Then R is norm-euclidean if and only if for every $y \in K$ there exists $x \in R$ such that $N(y-x) < 1$.*

Proof.

Suppose R is norm-euclidean. Then given $y \in K$, write $y = a/b$, where $a, b \in R,\ b \neq 0$. Since R is norm-euclidean, there exist $q, r \in R$ such that $a = bq + r$ and $N(r) < N(b)$. Divide the equation by b to obtain $a/b = q + r/b$. We claim that by choosing $x = q \in R$, $N(y-x) < 1$. Clearly

$$N(y-x) = N(a/b\ -\ q) = N(r/b) = N(r)/N(b) < 1$$

using multiplicativity of the norm and our assumption that $N(r) < N(b)$.

Conversely, assume that for every $y \in K$ there exists $x \in R$ such that $N(y-x) < 1$. Then, given $a \in R$ and $b \in R - \{0\}$, choose $q \in R$ such that $N(a/b\ -\ q) < 1$, and let $r = a - bq$. Then

$$N(r) = N(a - bq) = N(b(a/b - q)) = N(b)N(a/b - q) < N(b)$$

as desired.

In all of the examples which follow, $K = \mathbf{Q}(\zeta_n)$ and $R = \mathbf{Z}[\zeta_n]$.

6.1 Geometric Techniques

The following two examples illustrate the manner in which intuition derived directly from the geometry of the rings in question can be used to construct a proof that such rings are norm-euclidean. The fields are embedded inside a familiar normed vector space, and known facts about the "topological" norm of the vector space is used to draw conclusions about the value of the "algebraic" field norm. The proofs presented here are significantly less cumbersome than their counterparts in Chapter 4.

$\mathbf{n = 1}$, $\phi(\mathbf{n}) = \mathbf{1}$

Here $K = \mathbf{Q}$, $R = \mathbf{Z}$, and the norm $N_{\mathbf{Q}/\mathbf{Q}}$ is the absolute value function. Consider $\mathbf{Q}$ embedded in $\mathbf{R}$ in the usual manner.

Choose $a \in R$ and $b \in R - \{0\}$, and set $q = \lfloor a/b \rfloor$ and $r = a - bq$; we need to show that $|r| < |b|$. Since by definition, $|a/b - \lfloor a/b \rfloor| < 1$, multiplying through by $|b|$ gives $|a - b\lfloor a/b \rfloor| = |a - bq| = |r| < |b|$.

Note that the key fact used above was that the greatest integer function (floor) of $x \in \mathbf{Q}$ lies at a distance of at most 1 from x. We could just as well have used the ceiling $\lceil\ \rceil$ function, and the proof would have been equally valid. The next example, though similar in spirit to this one, will show that we do not always have this freedom.

$\mathbf{n = 4}$, $\phi(\mathbf{n}) = \mathbf{2}$

Now we have $K = \mathbf{Q}(i)$, $R = \mathbf{Z}[i]$, and $N(a+bi) = a^2 + b^2$. If we consider the canonical embedding of K into the complex plane $\mathbf{C}$, then the norm of a point corresponds precisely to the square of its modulus. Gauss's original proof for this case used the methods of the last example; to simplify matters for ourselves, we will exploit the result of Proposition 6.1.

We need to show that for $a+bi \in \mathbf{Q}(i)$, we can find $a'+b' \in \mathbf{Z}[i]$ such that $N((a+bi) - (a'+b'i)) < 1$. (See Fig. 3) It turns out that it is sufficient to choose a' to be an integer closest in value to a, i.e. $a' = \lfloor a + 1/2 \rfloor$, and also $b' = \lfloor b + 1/2 \rfloor$. For then, $|a - a'|$ and $|b - b'|$ are both no larger than $1/2$, so

$$N((a+bi) - (a'+b'i)) = N((a-a') + (b-b')i) = |(a-a') + (b-b')|^2 = (a-a')^2 + (b-b')^2$$

$$\leq (1/2)^2 + (1/2)^2 = 1/2 < 1$$

6.2 Using inequalities

A considerable number of results can be obtained by refining the techniques of 6.1 slightly, and by using inequalities to one's advantage; virtually all of the results obtained before 1975 relied on this approach. In the proof of the case $n = 4$ above, we managed to bound $N((a + bi) - (a' + b'i))$ above (strictly) by any $\alpha > 1/2$; we only need to do this for $\alpha = 1$, thereby suggesting an inherent flexibility in the proof. The next two examples are fairly representative of the style of reasoning developed by the early French mathematicians and continued until the 1970s.

$\mathbf{n = 3}$, $\phi(\mathbf{n}) = \mathbf{2}$

In our proof of the case $n = 3$, we will follow Wantzel's line of reasoning, using Proposition 6.1 to simplify the argument. We have $K = \mathbf{Q}(\zeta_3)$, $R = \mathbf{Z}[\zeta_3]$, and $N(a + b\zeta_3) = a^2 - ab + b^2$. Given any element $x = a + b\zeta_3 \in K$, where $a, b \in \mathbf{Q}$, we choose $a' = \lfloor a + 1/2 \rfloor$ and $b' = \lfloor b + 1/2 \rfloor$ as before. Then

$$N((a+b\zeta_3)-(a'+b'\zeta_3)) = (a-a')^2-(a-a')(b-b')+(b-b')^2 \leq |a-a'|^2+|a-a'||b-b'|+|b-b'|^2$$
$$< (1/2)^2 + (1/2)(1/2) + (1/2)^2 = 3/4 < 1$$

$\mathbf{n = 5}$, $\boldsymbol{\phi(n) = 4}$

The following proof, due to Branchini, is found in [Ch 25]. Given $a, b \in R$, $b \neq 0$, write $a/b = C + \alpha$, where $C \in R$, and $\alpha \in K$. Write

$$\alpha = a_0 + a_1\zeta_5 + a_2{\zeta_5}^2 + a_3{\zeta_5}^3 + a_4{\zeta_5}^4$$

By adding or subtracting 1 to or from the various coefficients of α and performing the inverse operation on C, we can assume that the coefficients of α all have absolute value less than or equal to $1/2$. Furthermore, at least three of the five coefficients will have the same sign; assume (without loss of generality) that this sign is positive, and that the three coefficients are a_0, a_1, and a_2. In view of the relation

$$1 + \zeta_5 + {\zeta_5}^2 + {\zeta_5}^3 + {\zeta_5}^4 = 0$$

we can write

$$\alpha = (a_0 - 1/4) + (a_1 - 1/4)\zeta_5 + (a_2 - 1/4){\zeta_5}^2 + (a_3 - 1/4){\zeta_5}^3 + (a_4 - 1/4){\zeta_5}^4$$
$$= b_0 + b_1\zeta_5 + b_2{\zeta_5}^2 + b_3{\zeta_5}^3 + b_4{\zeta_5}^4$$

It is clear that the first three terms have coefficients less than or equal to $1/4$ in absolute value; by adding or subtracting 1 to the coefficients of the other two terms and performing the inverse operation on C, we can assume that they are less than or equal to $1/2$ in absolute value.

Now let σ denote the automorphism of K defined by $\zeta_5 \mapsto {\zeta_5}^{-1}$. Then, by an easy computation,

$$\alpha\sigma(\alpha) + \sigma^2(\alpha)\sigma^3(\alpha) = 1/2 \sum_{0 \leq i < j \leq 4} (b_i - b_j)^2$$

Furthermore,

$$\sum_{0 \leq i < j \leq 4} (b_i - b_j)^2 = 5\sum_{i=0}^{4} b_i^2 - (\sum_{i=0}^{4} b_i)^2 \leq 5\sum_{i=0}^{4} b_i^2$$

so

$$\alpha\sigma(\alpha) + \sigma^2(\alpha)\sigma^3(\alpha) \leq 5/2 \sum_{i=0}^{4} b_i^2 \leq 5/2 \cdot 11/16 = 55/32$$

Lastly, we apply the arithmetic-geometric mean inequality to conclude that

$$N(\alpha) = \alpha\sigma(\alpha)\sigma^2(\alpha)\sigma^3(\alpha) \leq (55/64)^2 < 1$$

It is interesting to observe that the above proof closely resembles both the original proof of Kummer (see [Len 79]) in his correspondence with Kronecker, and a more contemporary proof by Ouspensky [Ou 09], which was published before Kummer's correspondence was made public.

$\mathbf{n = 8}$, $\boldsymbol{\phi(\mathbf{n}) = 4}$

In our last example of an *ad hoc* proof, we turn to an elegant result of Masley. Throughout this example, we write ζ for ζ_8, and N_n for $N_{\mathbf{Q}(\zeta_n)/\mathbf{Q}}$. In light of the inclusion of fields

$$\mathbf{Q} \subseteq \mathbf{Q}(\zeta_4) \subseteq \mathbf{Q}(\zeta_8)$$

we define, for $x \in \mathbf{Q}(\zeta_8)$ the *relative norm*

$$N_{8/4}(x) = \prod_{\sigma \in Gal(\mathbf{Q}(\zeta_8)/\mathbf{Q}(\zeta_4))}$$

Thus $N_8 = N_4 \cdot N_{8/4}$. Given $T = t_0 + t_1\zeta + t_2\zeta^2 + t_3\zeta^3 \in K$, choose $S = s_0 + s_1\zeta + s_2\zeta^2 + s_3\zeta^3 \in R$ such that for all i, $0 \leq i \leq 3$, $|s_i - t_i| \leq 1/2$. To simply notation, write $a = t_0 - s_0$, $b = t_1 - s_1$, $c = t_2 - s_2$, $d = t_3 - s_3$. We observe that

$$N_{8/4}(T - S) = (a + b\zeta + c\zeta^2 + d\zeta^3)(a + b\zeta^5 + c\zeta^{10} + d\zeta^{15})$$

Using the relation $\zeta^4 + 1 = 0$, the above reduces to

$$(a + b\zeta + c\zeta^2 + d\zeta^3)(a - b\zeta + c\zeta^2 - d\zeta^3)$$

which after further simplication becomes

$$(a^2 + 2bd - c^2) + (d^2 + 2ac - b^2)i$$

Thus

$$N_8(T - S) = N_4((a^2 + 2bd - c^2) + (d^2 + 2ac - b^2)i)$$

which reduces to

$$(a^2 + c^2)^2 + (b^2 + d^2)^2 + 4bd(a^2 - c^2) + 4ac(d^2 - b^2)$$

Since a, b, c, d all have absolute value less than or equal to $1/2$, each of the quantities $a^2, b^2, c^2, d^2, |ac|, |bd|$ has absolute value less than or equal to $1/4$. Thus all four terms in the last expression for $N_8(T - S)$ are between 0 and $1/4$, inclusive. However, if $(a^2 + c^2)^2$ actually equals $1/4$, then $a^2 + c^2 = 1/2$, which forces $a^2 = c^2 = 1/4$, and so the third term vanishes. In any case, $N_8(T - S) < 1$, and so $K = \mathbf{Q}(\zeta_8)$ is euclidean.

The literature is full of similar demonstrations that particular cyclotomic fields are euclidean; see [Ch 25] for some especially ingenious solutions. Unfortunately, the arguments usually become quite unintuitive and somewhat hard to follow, particularly when $\phi(n) > 4$. An important landmark in the history of the euclidean problem was the development of a more general criterion—a condition which, when satisfied by *any* number field, would guarantee that field to be euclidean. The condition, due to H.W. Lenstra, will allow us to prove (by a few simple computations) that $\mathbf{Q}(\zeta_1)$, $\mathbf{Q}(\zeta_3)$, $\mathbf{Q}(\zeta_5)$, and $\mathbf{Q}(\zeta_7)$ are euclidean. Because the condition is general, it does not exploit the geometry of cyclotomic fields, and we cannot use it to prove that $\mathbf{Q}(\zeta_n)$ is euclidean for higher n. This task will be left to a later section.

6.3 Lenstra's condition for general number fields

The statement and proof of Lenstra's condition (outlined in [Len 77]) rely heavily on packing- theoretic concepts which, though concise, do not provide the unfamiliar reader with an intuitive idea of why the condition is sufficient. For this reason, we defer the topic of Lenstra's condition in favor of a discussion of its ancestor, Hurwitz's Theorem.

In this section, we let K denote an algebraic number field of degree n and discriminant Δ over $\mathbf{Q}$, and R the ring of algebraic integers in K. K being a separable extension of $\mathbf{Q}$, we write $K = \mathbf{Q}(\gamma)$ for some $\gamma \in \mathbf{C}$. Let $g(x)$ be the irreducible monic polynomial (in $\mathbf{Q}[x]$) for γ, and denote by $\alpha_1, \ldots, \alpha_r$ its real roots. Since its complex roots come in conjugate pairs, let $\beta_1, \ldots, \beta_s$ represent a choice of one root from each pair.

Now we embed K inside $\mathbf{R}^r \times \mathbf{C}^s$ as follows:

For $1 \leq i \leq r$, let σ_i denote the homomorphism $K \longrightarrow \mathbf{C}$ defined by $\gamma \mapsto \alpha_i$; likewise, for $1 \leq j \leq s$, let τ_j denote the homomorphism defined by $\gamma \mapsto \beta_j$. Now consider $\Phi : K \longrightarrow \mathbf{R}^r \times \mathbf{C}^s$ defined by

$$\Phi(x) = (\sigma_1(x), \ldots, \sigma_r(x), \tau_1(x), \ldots, \tau_s(x))$$

Then the function $N : \mathbf{R}^r \times \mathbf{C}^s \longrightarrow \mathbf{R}$ defined by

$$N(x) = \prod_{i=1}^{r} |x_i| \cdot \prod_{j=1}^{s} |x_j|^2$$

is (when restricted to $\Phi(K)$), the absolute value of the field norm. Next, we identify each copy of $\mathbf{C}$ with $\mathbf{R}^2$ via the map $\Psi : \mathbf{C} \longrightarrow \mathbf{R}^2$ sending

$$a + bi \mapsto (a + b, a - b)$$

thus identifying the image $\Phi(K) \subseteq \mathbf{R}^r \times \mathbf{C}^s$ with a subset of $\mathbf{R}^n$. We use the following proposition later, but as its proof is unrelated to the present topic of discussion, we omit it. (See [La 64] for a proof)

Proposition 6.2 *The image of $F = \Psi(\Phi(R))$ of R, a lattice in $\mathbf{R}^n$, has a fundamental domain of volume (Lebesgue measure) equal to $|\Delta|^{1/2}$.*

We are now in a position to state Hurwitz's theorem:

Theorem 6.3 *Let K be a number field, R its ring of integers. Then there is an integer $M > 1$ such that for all $\xi \in K$, there exists $\kappa \in R$ and j, $0 < j < M$, such that $N(j\xi - \kappa) < 1$.*

We note that R is norm-euclidean if and only if we can choose $M = 2$.

Consider K embedded in $\mathbf{R}^n$ by the map $\Psi \circ \Phi$. Since R is a lattice in $\mathbf{R}^n$, choose a basis $\theta_1, \ldots, \theta_n$ for R. Now let

$$F = \{a_1\theta_1 + \ldots a_n\theta_n : 0 \leq a_i < 1\}$$

Clearly, we can write $K = F + R$. Since the set F is open, and the function N is continuous

on $\mathbf{R}^n$, we can choose a neighborhood U of the origin in $\mathbf{R}^n$ such that for all $u, v \in U$, $N(u - v) < 1$. We now let ξ be an element of K, and consider the translates

$$i\xi + U,\ i = 1, 2, \ldots$$

For each i, we construct a set $(i\xi + U)^*$ by replacing each element ϵ of $i\xi + U$ by $\epsilon' \in F$, where $\epsilon' = \epsilon - \rho$ for some $\rho \in R$. (In other words, we are bringing each element of $i\xi + U$ into F by subtracting an appropriate ring element) Each set $(i\xi + U)^*$ has the same volume as U, and they are all contained in F. So if we consider $M > \mu(F)/\mu(U)$, then at least two sets $(i\xi + U)^*$ and $(i'\xi + U)^*$, $1 \leq i < i' \leq M$, will intersect. That is, there exist elements $u, v \in U$ and translation factors $\lambda, \lambda' \in R$ such that

$$i\xi + u - \lambda = i'\xi + v - \lambda'$$

Setting $\kappa = \lambda' - \lambda$ and $j = i' - i$ gives us

$$N(j\xi - \kappa) = N(i'\xi - \lambda' - i\xi + \lambda) = N(u - v) < 1$$

This proves Hurwitz's theorem.

As mentioned above, we need to be able to choose $M = 2$ to show that R is norm-euclidean. Therefore, unless we can find an appropriate U such that $\mu(U) > \mu(F)/2$, we cannot conclude that the ring is norm-euclidean. In the worst case, the ring might be norm-euclidean, but no such U may exist. To overcome this problem, Lenstra suggested replacing the sequence $1, 2, \ldots M$ with elements $\omega_1, \omega_2, \ldots, \omega_M \in R$ such that $\omega_i - \omega_j \in R^\times$ for all $i \neq j$. Copying the argument above, one could conclude that there is an integer $M > 1$ such that for each $\xi \in K$ there exists $\kappa \in R$ and i, j, $0 < i < j < M$ such that

$$N((\omega_i - \omega_j)\xi - \kappa) < 1$$

By inverting $\omega_i - \omega_j$, we obtain

$$N(\xi - \kappa(\omega_i - \omega_j)^{-1}) = N((\omega_i - \omega_j)\xi - \kappa)N((\omega_i - \omega_j)^{-1}) = N((\omega_i - \omega_j)\xi - \kappa) \cdot 1 < 1$$

and so R is norm-euclidean. Thus a sufficient condition for R to be norm-euclidean is simply the existence of a sufficiently long sequence $\omega_1, \ldots \omega_m$ such that the differences $\omega_i - \omega_j$ are units for all $i \neq j$. We formalize this in the statement of Lenstra's theorem, which we state after the following definition; readers unfamiliar with packing theory are advised to review the definitions in Appendix C before proceeding further.

Definition 6.4 *A sequence $\{\omega_1, \ldots, \omega_n\}$ of elements of R is called* unit-differential *if for all i, j, $i \neq j$, $\omega_i - \omega_j \in R^\times$. As a convention, we reserve the letter M to refer to*

$$sup\{m : \text{ there exists a unit-differential sequence in } R \text{ of length } m\}$$

Theorem 6.5 *Let K be an algebraic number field of degree n and discriminant Δ over $\mathbf{Q}$; let N be the absolute value of the field norm. Let $U \subseteq \mathbf{R}^n$ be a bounded Lebesgue measurable set with positive Lebesgue measure such*

$$N(u - v) < 1 \text{ for all } u, v \in U$$

and let $\delta^*(U)$ denote the center packing constant of U. Then K is euclidean if

$$M > \delta^*(U) \cdot |\Delta|^{1/2}$$

Proof.

Choose $x \in K$. We want to find $y \in R$ such that $N(x-y) < 1$. Let $\omega_1, \ldots \omega_m$ be a unit-differential sequence of elements of R, with $m > \delta^*(U) \cdot |\Delta|^{1/2}$. By definition of δ^*, this is equivalent to stating that

$$m \cdot \mu(U)/|\Delta|^{1/2} > \delta(U)$$

Now consider the system $\mathbf{U} = (U + \omega_i x + \alpha)_{1 \le i \le m, \alpha \in R}$ of translates of U. Using Lemma C.9, we calculate

$$\rho_+(\mathbf{U}) = m \cdot \mu(U)/|\Delta|^{1/2}$$

so

$$\rho_+(\mathbf{U}) > \delta(U)$$

which implies (by definition of δ) that $\mathbf{U}$ is *not* a packing of U.

Hence, there exist distinct pairs (i, α) and (j, β), with $1 \le i, j, \le m$ and $\alpha, \beta \in R$ such that $(U + \omega_i x + \alpha) \cap (U + \omega_j x + \beta) \neq \emptyset$; that is, for some $u, v \in U$,

$$u + \omega_i x + \alpha = v + \omega_j x + \beta$$

If $i = j$ then $\beta - \alpha = u - v$, and since $\beta - \alpha \in R$, $N(\beta - \alpha) \in \mathbf{Z}$ by Proposition A.5 (3); on the other hand, $\beta - \alpha = u - v \in U$ forces $N(u - v) < 1$, and so we must have $\beta = \alpha$, which contradicts the distinctness of the pairs (i, α) and (j, β). Thus $i \neq j$, so $\omega_i - \omega_j \in R^\times$. Set

$$y = (\beta - \alpha)/(\omega_i - \omega_j)$$

Then

$$N(x - y) = N((u - v)/(\omega_i - \omega_j)) = N(u - v) \cdot 1 = N(u - v) < 1$$

This concludes the proof of Theorem 6.5.

The following corollary gives an explicit bound for M.

Corollary 6.6 *Let $K = \mathbf{Q}(\gamma)$ be an algebraic number field of degree n and discriminant Δ over $\mathbf{Q}$; let s be one half the number of non-real complex roots of the irreducible polynomial for γ. Then K is euclidean if*

$$M > (n!/n^n) \cdot (4/\pi)^s \cdot |\Delta|^{1/2}$$

Proof.

Choose

$$U = \{(x_j)_{j=1}^{r+s} \in \mathbf{R}^r \times \mathbf{C}^s : \sum_{j=1}^{r} |x_j| + 2 \sum_{j=r+1}^{r+s} |x_j| < n/2\}$$

One can verify that $N(u - v) < 1$ for all $u, v \in U$ using the arithmetic-geometric inequality. A classical computation (see [La 64]) gives

$$\mu(U) = (n^n/n!) \cdot (\pi/4)^s$$

Combining this with the inequality

$$\delta(U) \le 1$$

of Corollary C.8 and then using Theorem 6.5 suffices to show that K is euclidean.

We are finally ready to use Corollary 6.6 to prove that certain specific cyclotomic fields are euclidean. Consider the field $\mathbf{Q}(\zeta_p)$, where p prime. Consideration of the (unit-differential) sequence

$$(\zeta_p^i - 1)/(\zeta_p - 1),\ i = 1, \ldots, p$$

shows that $M \geq p$. For $p = 2, 3, 5, 7, 11$, the bound of Corollary 6.6 is equal to $1, 1.103, 1.70, 4.13, 58.96$ respectively, so we obtain proofs that $\mathbf{Q}(\zeta_p)$ is euclidean for $p = 2, 3, 5, 7$. Could we hope for a better lower bound on M when $p \geq 11$? In fact, we cannot; the reason for this is summarized by the following proposition.
Define

$$L = \min\{|R/I| :\ I \subset R \text{ is a proper ideal}\}$$

Proposition 6.7 $2 \leq M \leq L \leq 2^n$

Proof.

Since the sequence $\{0, 1\}$ is always unit-differential, $2 \leq M$. Consideration of the ideal $2R$ shows that $L \leq 2^n$, so L is always finite. Now suppose that $M > L$; that is, there exists a unit-differential sequence of length greater than L. Then, if I satisfies $|R/I| = L$, at least two elements of the sequence lie in the same coset of I in R. This implies that their difference (which is a unit) lies in the ideal I, contradiction.

Since the element $1 - \zeta_p \in \mathbf{Q}(\zeta_p)$ has norm p, the ideal it generates will have index p in R, so $L \leq p$. Combining this with the proposition and the explicit bound $M \geq p$ gives $M = L = p$, so we can do no better using the bounds of Corollary 6.6.

We now turn our attention to other results of Lenstra which prove that a much larger class of cyclotomic fields is euclidean.

6.4 Lenstra's result for cyclotomic fields

In this section we prove a detailed theorem, also due to H. W. Lenstra [Len 75], which extends the results proved above, though by a distinctly different method. We state the theorem below and prove it in stages.

Theorem 6.8 *Suppose $\phi(m) \leq 10$, $m \neq 16$, $m \neq 24$. Then $\mathbf{Z}[\zeta_m]$ is norm-euclidean.*

Our previous analysis has been centered around the norm function N; in this section, we develop a richer concept of size by introducing another measure on fields.

Let K denote an algebraic number field of degree d over $\mathbf{Q}$, and write $K_{\mathbf{R}}$ for $K \otimes_{\mathbf{Q}} \mathbf{R}$, which, as an $\mathbf{R}$-algebra, is isomorphic to $\mathbf{R}^r \times \mathbf{C}^s$, where r, s are as defined in the previous section.

Definition 6.9 *The* general measure $\mu : K_{\mathbf{R}} \to R$ *is given by*

$$\mu(x) = \sum_{\sigma \in Hom(K, \mathbf{C})} |\sigma(x)|^2$$

Let R be the ring of integers in K. As a subset of $K_{\mathbf{R}}$, R is a lattice.

Definition 6.10 *The* fundamental domain *is defined by*

$$F = \{x \in K_{\mathbf{R}} \mid \mu(x) \leq \mu(x-y) \text{ for all } y \in R\}$$

We remark that F is a compact subset of $K_{\mathbf{R}}$ satisfying

$$F + R = K_{\mathbf{R}}$$

Definition 6.11 *Let*

$$c = \max\{\mu(x) |\, x \in F\}$$

A number c' is called a bound *for F if $c' \geq c$. A bound c' for F is termed* usable *if for every $x \in F \cap K$ such that $\mu(x) = c'$ there exists a root of unity $u \in R$ such that $\mu(x-u) = c'$.*

The motivation for the apparently arbitrary definition of usability above comes from the following lemma and proposition. For the remainder of the section we assume that any roots of unity in K are actually contained in R; this condition (which is weaker than integral closure) is necessary (by Theorem 5.9) to show that K is euclidean.

Lemma 6.12 *Suppose $x \in K$ satisfies $|\sigma(x)|^2 = 1$ and $|\sigma(x-u)|^2 = 1$ for some root of unity $u \in R$ and homomorphism $\sigma \in Hom(K, \mathbf{C})$. Then $x \in R$.*

Proof.

Let $y = \sigma(-xu^{-1}) \in \mathbf{C}$; it is easy to check, given the assumptions, that $y\overline{y} = 1$ and $y + \overline{y} = -1$, so y is a cube root of unity. Since $\sigma : K \to \mathbf{C}$ is injective, $-xu^{-1}$ must be a cube root of unity in K, too. Our hypotheses indicate that $-xu^{-1} \in R$, so

$$x = (-u)(-xu^{-1}) \in R$$

as desired.

Proposition 6.13 *If d is a usable bound for F, then R is norm-euclidean.*

Proof.

Let $x \in K$ be any element; we need to find $y \in R$ such that $N(x-y) < 1$. Since $F + R = K_{\mathbf{R}}$, it suffices to show this for all $x \in F$. The case $x = 0$ is handled trivially, so assume $x \neq 0$. Clearly $\mu(x) \leq d$, since d is a usable bound. If the inequality is strict, we can take $y = 0$. In the case of equality, usability of d implies that $\mu(x) = \mu(x-u) = d$ for some root of unity $u \in R$. Thus, by the arithmetic-geometric inequality and the definitions of N and μ,

$$N(x)^2 \leq (\mu(x)/d)^d = 1$$

and

$$N(x-u)^2 \leq (\mu(x-u)/d)^d = 1$$

If at least one of the above inequalities is strict, then we can take either $y = 0$ or $y = u$. If both are equalities, then, by the equality condition of the arithmetic-geometric inequality,

$$|\sigma(x)|^2 = |\tau(x)|^2 \text{ and } |\sigma(x-u)|^2 = |\tau(x-u)|^2$$

for all $\sigma, \tau \in Hom(K, \mathbf{C})$. Also, since

$$\prod_\sigma |\sigma(x)|^2 = N(x)^2 = 1 = N(x-u)^2 = \prod_\sigma |\sigma(x-u)|^2$$

we must have

$$|\sigma(x)|^2 = |\sigma(x-u)|^2 = 1 \text{ for all } \sigma$$

Then Lemma 6.12 implies that $x \in R$, which contradicts $x \in F - \{0\}$.

In the discussion above, we gave a sufficient condition for a field to be euclidean. Below, we will show how satisfiability of this condition for one field can give us information about satisfiability in other fields. We now pass to the specific case of cyclotomic fields. When referring to the field $K = \mathbf{Q}(\zeta_m)$ with ring of integers $R = \mathbf{Z}[\zeta_m]$, we write μ_m for μ, F_m for F, and c_m for c. We denote by Tr_m the extension of the trace function to $K_\mathbf{R}$. Our next goal is to prove

Proposition 6.14 *Let n be a positive divisor of m, and define*

$$e = \phi(m)/\phi(n)$$

Then $c_m \leq e^2 c_n$. Also, if c' is a usable bound for F_n, then $e^2 c'$ is a usable bound for F_m.

In order to prove Proposition 6.14 we introduce the *relative trace* function $Tr_{nm} : \mathbf{Q}(\zeta_m) \to \mathbf{Q}(\zeta_n)$ defined by

$$Tr_{nm}(x) = \sum_{\sigma \in Gal(\mathbf{Q}(\zeta_m)/\mathbf{Q}(\zeta_n))} \sigma(x)$$

Clearly, Tr_{nm} extends naturally to $\mathbf{Q}(\zeta_m)_\mathbf{R}$; also

$$Tr_m = Tr_n \circ Tr_{nm}$$

To derive the inequality of Proposition 6.14, we need to express μ_m in terms of μ_n; this is accomplished by the following two lemmas.

Lemma 6.15 *Let $x \in \mathbf{Q}(\zeta_m)_\mathbf{R}$, $y \in \mathbf{Q}(\zeta_n)_\mathbf{R}$. Then*

$$\mu_m(x) - \mu_m(x-y) = e(\mu_n(1/e \cdot Tr_{nm}(x)) - \mu_n(1/e \cdot Tr_{nm}(x) - y))$$

Proof.

Observe that for any k,

$$\mu_k(x) = \sum_{\sigma \in Hom(\mathbf{Q}(\zeta_k), \mathbf{C})} \sigma(x)\overline{\sigma(x)} = Tr_k(x\overline{x})$$

Then

$$\begin{aligned}
&e(\mu_n(1/e \cdot Tr_{nm}(x)) - \mu_n(1/e \cdot Tr_{nm}(x) - y)) \\
&= e \cdot Tr_n(1/e \cdot Tr_{nm}(x)\overline{y} + 1/e \cdot Tr_{nm}(\overline{x})y - y\overline{y}) \\
&= Tr_n(Tr_{nm}(x)\overline{y} + Tr_{nm}(\overline{x})y - ey\overline{y}) \\
&= Tr_n(Tr_{nm}(x\overline{y}) + Tr_{nm}(\overline{x}y) - Tr_{nm}(y\overline{y})) \\
&= Tr_m(x\overline{y} + \overline{x}y - y\overline{y}) = \mu_m(x) - \mu_m(x-y)
\end{aligned}$$

Lemma 6.16 *Given* $x \in \mathbf{Q}(\zeta_m)_{\mathbf{R}}$,

$$\mu_m(x) = 1/m \cdot \sum_{j=1}^{m} \mu_n(Tr_{nm}(x\zeta_m^j))$$

Proof.

For convenience of notation, we let $G = Gal(\mathbf{Q}(\zeta_m)/\mathbf{Q}(\zeta_n))$

$$\begin{aligned}
&\sum_{j=1}^{m} \mu_n(Tr_{nm}(x\zeta_m^j)) \\
&= \sum_{j=1}^{m} \mu_n(\sum_{\sigma\in G} \sigma(x\zeta_m^j)) \\
&= Tr_n(\sum_{j=1}^{m} \sum_{\sigma\in G} \sum_{\tau\in G} \sigma(x)\sigma(\zeta_m^j)\tau(\overline{x})\tau(\zeta_m^{-j})) \\
&= Tr_n(\sum_{\sigma\in G} \sum_{\tau\in G} \sigma(x)\tau(\overline{x})(\sum_{j=1}^{m}(\sigma(\zeta_m)\tau(\zeta_m)^{-1})^j))
\end{aligned}$$

The inner sum vanishes when $\sigma \neq \tau$ and equals m when $\sigma = \tau$. Thus the above expression is equal to

$$Tr_n(\sum_{\sigma\in G} \sigma(x)\sigma(\overline{x})m) = m \cdot Tr_n(Tr_{nm}(x\overline{x})) = m \cdot Tr_m(x\overline{x}) = m \cdot \mu_m(x)$$

Proof of Proposition 6.14

Let $x \in F_m$ be any element; we need to show that $\mu_m(x) \leq e^2 c_n$. For any $y \in \mathbf{Z}[\zeta_m]$, Lemma 6.15 implies that $1/e \cdot Tr_{nm}(x) \in F_n$, since both sides of the equality must be nonpositive. Replacing x by $x\zeta_m^j \in F_m$, we obtain that $1/e \cdot Tr_{nm}(x\zeta_m^j) \in F_n$. Thus

$$\mu_n(Tr_{nm}(x\zeta_m^j)) = e^2 \cdot \mu_n(1/e \cdot Tr_{nm}(x\zeta_m^j)) \leq e^2 \cdot c_n$$

which proves that $c_m \leq e^2 \cdot c^n$. Now assume that c' is a usable bound for F_n, and let $x \in F_m \cap \mathbf{Q}(\zeta_m)$ satisfy $\mu_m(x) = e^2 \cdot c'$. This forces $c' = c_n$ and

$$\mu_n(1/e \cdot Tr_{nm}(x\zeta_m^j)) = c_n = c' \text{ for all } j \in \mathbf{Z}$$

Taking $j = 0$,

$$\mu_n(1/e \cdot Tr_{nm}(x)) = c'$$

and by usability of c' for F_n, there is a root of unity $u \in \mathbf{Z}[\zeta_n]$ such that

$$\mu_n(1/e \cdot Tr_{nm}(x) - u) = c'$$

Finally, we apply Lemma 6.15 with $y = u$ to obtain

$$\mu_m(x - u) = \mu_m(x) = e^2 \cdot c'$$

therefore proving usability of c' for F_m.

Having derived a bound for c_m in terms of c_n (where $m \mid n$), our next task is to compute an explicit bound for c_n; we do this when n is a prime number and then use Proposition 6.14 to estimate c_m.

To this end, let $n \geq 2$ be an integer, and let V be an $(n-1)$-dimensional $\mathbf{R}$-vector space with generators e_i, $1 \leq i \leq n$, subject only to the relation $\sum_{i=1}^{n} e_i = 0$. Define a positive definite quadratic form q on V by

$$q(x) = \sum_{1 \leq i < j \leq n} (x_i - x_j)^2, \text{ where } x = \sum_{i=1}^{n} x_i e_i$$

Let $(\ ,\ ): V \times V \to \mathbf{R}$ represent the symmetric bilinear form induced by q, that is:

$$(x, y) = 1/2 \cdot (q(x + y) - q(x) - q(y))$$

Then it is routine to check that

$$(x, x) = q(x) \text{ for } x \in V$$

$$(e_i, e_i) = n - 1 \text{ for } 1 \leq i \leq n$$

$$(e_i, e_j) = -1 \text{ for } 1 \leq i < j \leq n$$

The subgroup $L \subseteq V$ generated by $\{e_i : 1 \leq i \leq n\}$ is a lattice of rank $n - 1$ in V. Its fundamental domain

$$E = \{x \in V : q(x) \leq q(x - y) \text{ for all } y \in L\}$$

is a compact subset of V, and we define

$$b = \max\{q(x) : x \in E\}$$

The following proposition is proved in Appendix D; the proof relies solely on linear algebra. We do not present it here for reasons of length and relevance to the material under discussion.

Proposition 6.17 *The set of points $x \in E$ for which $q(x) = b$ is*

$$Z = \{1/n \cdot \sum_{i=1}^{n} i e_{\sigma(i)} : \sigma \text{ is a permutation of } \{1, 2, \ldots n\}\}$$

Furthermore,

$$b = (n^2 - 1)/12$$

The next proposition relates the linear algebraic construction above to the geometry of cyclotomic fields.

Proposition 6.18 *Let n be a prime number. Then $c_n = (n^2 - 1)/12$ is a usable bound for F_n.*

Proof.

The $\mathbf{R}$-algebra $\mathbf{Q}(\zeta_n)_{\mathbf{R}}$ is generated by the n elements ζ_n^i, $1 \leq i \leq n$, on which the only relation (by primality of n) is $\sum_{i=1}^n \zeta_n^i = 0$. Moreover, given $x_i \in \mathbf{R}$, $1 \leq i \leq n$, we have

$$\begin{aligned} & \mu_n(\sum_{i=1}^n x_i \zeta_n^i) \\ = & Tr_n(\sum_{i=1}^n \sum_{j=1}^n x_i x_j \zeta_n^{i-j}) \\ = & n \cdot \sum_{i=1}^n x_i^2 - \sum_{i=1}^n \sum_{j=1}^n x_i x_j \\ = & \sum_{1 \leq i < j \leq n} (x_i - x_j)^2 \end{aligned}$$

Thus, the quadratic spaces $(\mathbf{Q}(\zeta_n)_{\mathbf{R}}, \mu_n)$ and (V, q) are isomorphic; the isomorphism is given by

$$\zeta_n^i \mapsto e_i \text{ for } 1 \leq i \leq n$$

$\mathbf{Z}[\zeta_n]$ corresponds to L; therefore F_n corresponds to E and

$$c_n = b = (n^2 - 1)/12$$

Furthermore, the set of $x \in F_n$ for which $\mu_n(x) = c_n$ is given by

$$S = \{1/n \sum_{i=1}^n i \zeta_n^{\sigma(i)} : \sigma \text{ is a permutation of } \{1, 2, \ldots, n\}\}$$

Choose any x in this set and its associated permutation σ. Setting $\sigma(0) = \sigma(n)$ to ease notation,

$$x - \zeta_n^{\sigma(n)} = 1/n \sum_{i=0}^{n-1} i \zeta_n^{\sigma(i)} = 1/n \sum_{j=1}^n j \zeta_n^{\sigma(j-1)} \in S$$

Hence $\mu_n(x - \zeta_n^{\sigma(n)}) = c_n$, and so c_n is usable.

Proof of Theorem 6.8

$c_1 = 1/4$ is clearly a (usable) bound for F_1, so using Proposition 6.14 and Proposition 6.18,

$$\begin{aligned} c_1 = 1/4 < 1 = \phi(1) \\ c_3 = 2/3 < 2 = \phi(3) \\ c_4 \leq 1/4 \cdot 2^2 = 1 < 2 = \phi(4) \\ c_5 = 2 < 4 = \phi(5) \\ c_7 = 4 < 6 = \phi(7) \\ c_8 \leq 1/4 \cdot 4^2 = 4 = \phi(8) \end{aligned}$$

$$
\begin{aligned}
c_9 &\leq 2/3 \cdot 3^2 = 6 = \phi(9) \\
c_{11} &= 10 = \phi(11) \\
c_{12} &\leq 1/4 \cdot 4^2 = 4 = \phi(12) \\
c_{15} &\leq 2 \cdot 2^2 = 8 = \phi(15) \\
c_{20} &\leq 2 \cdot 2^2 = 8 = \phi(20)
\end{aligned}
$$

which proves Theorem 6.8.

We have seen how bounding the general measure on a fundamental domain of the lattice $R \subseteq K_{\mathbf{R}}$ and using the existence of roots of unity in the field is sufficient to show that certain fields are euclidean. In our last example, we will show how to handle the special case $\phi(m) = 8$, using properties of a well-known lattice.

6.5 Using Properties of Γ_8

The analysis which we describe below (also due to H. W. Lenstra; see [Len 78]), is, in a more general form, applicable to certain non-cyclotomic number fields; however, we will be concerned only with its application to the cyclotomic case. The method of attack is somewhat similar to that of the last section; an isomorphism is set up between two quadratic spaces, one of which has a degree 8 field extension K as the underlying vector space. Known information about the other quadratic space is then used to draw conclusions about the ring of integers in K.

We introduce the lattice Γ_8 by given two equivalent constructions.

- $\mathbf{\Gamma}_8$ is the subgroup of $\mathbf{Q}^8$ generated by $(1/2, \ldots, 1/2)$ and the elements $x \in \mathbf{Z}^8$ such that $\sum_{i=1}^{8} x_i \equiv 0 \pmod 2$.
- $\mathbf{\Gamma}_8$ is the subset of $\mathbf{Q}^8$ consisting of 8-tuples $(x_1, \ldots, x_8)$ satisfying
  1. $2x_i \in \mathbf{Z}$
  2. $x_i - x_j \in \mathbf{Z}$
  3. $\sum_{i=1}^{n} x_i \in 2\mathbf{Z}$

The criterion to be used is the following:

Theorem 6.19 *Let F be a cyclotomic extension of degree 8 over $\mathbf{Q}$; further, let F be an imaginary quadratic extension of an intermediate totally real field K; that is, $\mathbf{Q} \subseteq K \subseteq F$. If $\Delta_{K/\mathbf{Q}} < 8^4 = 4096$, then F is euclidean.*

Proof.

The first step of the proof is to verify the following lemma, which will be used later to establish a connection between the ring of integers R in F and the lattice $\mathbf{\Gamma}_8$.

Lemma 6.20 *Let V be a $\mathbf{Q}$-vector space of dimension 8, endowed with a positive definite quadratic form f. Let $(\ ,\ )$ refer to the bilinear form associated with f defined by*

$$(x, y) = 1/2 \cdot (f(x + y) - f(x) - f(y))$$

If $E \subseteq V$ is a subgroup, free of rank 8 over $\mathbf{Z}$ such that

1. *For all $x \in V$, $x \in E$ if and only if $(x, y) \in \mathbf{Z}$ for all $y \in E$.*

2. *$f(x) \in 2\mathbf{Z}$ for all $x \in E$*

Then for every $x \in V$ there exists $y \in E$ such that $f(x - y) \leq 1$.

Proof.

It is easy to see from the definitions that any E satisfying the conditions of the lemma must be isomorphic to $\mathbf{\Gamma}_8$ (as a quadratic space). Hence it suffices to prove the lemma for $E = \mathbf{\Gamma}_8$ and $V = \mathbf{\Gamma}_8 \otimes \mathbf{Q}$. This can be done using a computer.

Returning to the proof of Theorem 6.19, let F, K be fields satisfying the hypotheses of the theorem. Let σ denote the non-trivial automorphism of F which fixes K, and δ the different of F over $\mathbf{Q}$. Define $f : F \to \mathbf{Q}$ by

$$f(x) = Tr_F(x\sigma(x)/\delta)$$

which is easily seen to be a positive definite quadratic form on F, whose associated bilinear form is given by

$$(x, y) = Tr_F(x\sigma(y)/\delta)$$

Let R be the ring of integers in F. Given $x \in F$, clearly $(x, y) \in \mathbf{Z}$ for all $y \in R$ if and only if $Tr_F((x/\delta) \cdot y) \in \mathbf{Z}$ for all $y \in R$ if and only if $x \in \mathbf{Z}$, by Corollary A.10. Noting that σ is an automorphism of order 2,

$$f(x) = 2 \cdot Tr_K(x\sigma(x)/\delta) \in 2\mathbf{Z} \text{ for } x \in R$$

Now calculate

$$N_F(z) = N_K(z\sigma(z)) = N_K(\delta) \cdot N_K(z\sigma(z)/\delta) = \Delta \cdot \prod_{\tau \in Gal(K/\mathbf{Q})} \tau(z\sigma(z)/\delta)$$

Each of the factors in the product is nonnegative, so applying the arithmetic-geometric inequality, we obtain

$$0 \leq N_F(z) \leq \Delta \cdot (\sum_{\tau} \tau(z\sigma(z)/\delta)/4)^4 = \Delta \cdot f(z)^4 \cdot 8^{-4}$$

Finally, we show that R is norm-euclidean. Given $a, b \in R$, $b \neq 0$, use Lemma 6.20 to choose $y \in R$ such that $f(a/b - y) \leq 1$. Then, using our hypothesis that $\Delta < 4096$ and the inequalities above,

$$N_F(a/b - y) \leq \Delta \cdot 8^{-4} < 1$$

and R is norm-euclidean.

We now turn to the application of Theorem 6.19 to specific fields. We note that $\phi(15) = \phi(20) = \phi(24) = 8$ and that we have

$$F = \mathbf{Q}(\zeta_{15}), \quad K = \mathbf{Q}(\zeta_{15} + \zeta_{15}^{-1}), \quad \Delta = 1125$$

$$F = \mathbf{Q}(\zeta_{20}), \quad K = \mathbf{Q}(\zeta_{20} + \zeta_{20}^{-1}), \quad \Delta = 2000$$

$$F = \mathbf{Q}(\zeta_{24}), \quad K = \mathbf{Q}(\zeta_{24} + \zeta_{24}^{-1}), \quad \Delta = 2304$$

Thus we have obtained new proofs that $\mathbf{Q}(\zeta_{15})$ and $\mathbf{Q}(\zeta_{20})$ are euclidean, and our first proof that $\mathbf{Q}(\zeta_{24})$ is euclidean.

7 A Non-euclidean Cyclotomic Field

In what follows, we give a short proof (due to H.W. Lenstra) that $\mathbf{Q}(\zeta_{32})$ is not euclidean. We claim, in particular, that there are no elements q, r in $\mathbf{Z}[\zeta_{32}]$ such that

$$1 + (1+\zeta)^5 = q(1+\zeta)^6 + r$$

Using Proposition A.5 (1), we compute $N(1+\zeta) = 2$, so

$$N(1+\zeta)^6 = 64$$

Lemma 7.1 *Every element in* $\mathbf{Z}[\zeta_{32}]$ *which is prime to* $1+\zeta$ *has norm equivalent to* 1 (mod 32)*.*

Proof.

Fix an element $z \in R = \mathbf{Z}[\zeta_{32}]$; assume also that z is irreducible and prime to $1+\zeta$. Then for every $y \in R$, let $\overline{y}$ represent its coset in $R/(z)$. Divide both sides of the identity

$$x^{32} - 1 = \prod_{i=1}^{32}(x - \zeta^i)$$

by $(x-1)$ to obtain

$$1 + x + \ldots + x^{31} = \prod_{i=1}^{31}(x - \zeta^i)$$

Substitute $x = 1$ in this identity, to obtain

$$32 = \prod_{i=1}^{31}(x - \zeta^i)$$

so taking residues yields

$$\overline{32} = \prod_{i=1}^{31}\overline{(1-\zeta^i)}$$

Because z is prime to $1+\zeta$, we can assume that $\overline{32} \neq \overline{0}$; hence it follows that $\overline{\zeta^i} \neq \overline{1}$ or all i. Thus the residues $\overline{\zeta^i}$ of ζ^i are distinct for all i.

Finally, we observe that the elements $\{\overline{\zeta^i} : 0 \leq i \leq 31\}$ form a subgroup of order 32 of the multiplicative group of $R/(z)$. However, using Proposition A.5 (9), we find that this multiplicative group has order $p^k - 1$ for some p, k, and so

$$N(z) = |R/(z)| = p^k \equiv 1 \pmod{m}$$

So if we can find q, r such that

$$1 + (1+\zeta)^5 = q(1+\zeta)^6 + r$$

with $N(r) < 64$, Lemma 7.1 and Proposition A.5 (6) and (9) tell us that r is either a unit or a product of prime powers, each equivalent to 1 (mod 32). These conditions force $N(r) = 1$. It is known [Ka 88] that the unit group of $\mathbf{Z}[\zeta_{32}]$ is generated by

$$(1-\zeta^i)/(1-\zeta), \text{ where } 1 \leq i \leq 8$$

We examine the residues of each of these elements in the multiplicative group M of the ring

$$\mathbf{Z}[\zeta]/((1+\zeta)^6)$$

Since

$$(2) = ((1+\zeta))^{16}$$

as ideals, we observe that

$$\mathbf{Z}[\zeta]/((1+\zeta)^6) = \mathbf{Z}/\mathbf{2Z}[\zeta]/((1+\zeta)^6)$$

thereby greatly simplifying computation. Finally, it can be shown (by direct computation) that the subgroup M generated by the residues of these units has order 16 and hence does not contain the residue of $1 + (1+\zeta)^5$, giving a contradiction.

8 Other Techniques

Most of the proofs presented in previous sections, while insightful, were of a conventional character. A notable exception to this pattern is Ojala's proof that $\mathbf{Q}(\zeta_{\mathbf{16}})$ is norm-euclidean, which used a UNIVAC 1108 system [Oj 77].

Ojala first imposes an equivalence relation on the field, and then shows that it suffices to check the condition of Proposition 6.1 for one representative of each equivalence class. By using various inequalities, he manages to show that for all such representatives x, there exists $y \in \{0, 1, i, 1+i\}$ such that $N(x-y) < 1$.

Summarizing the results hitherto achieved towards the solution of **P3**, we know that for all but thirty values of n, $n \not\equiv 2 \pmod 4$, $\mathbf{Z}[\zeta_n]$ is not norm-euclidean; in fact, it is not even a euclidean domain. On the other hand, among these thirty values, we know that fourteen are norm-euclidean and one is not; the other fifteen remain unclassified at this stage. Because $\phi(n) \geq 12$ for all such n, it seems unlikely that the methods of sections 6.3 and 6.4 could handle such cases; it is conceivable, though, that Ojala's idea could be modified to provide proofs for other such values of n if there is sufficient rationale to believe that such fields are in fact euclidean.

Before concluding, a word is in order regarding the problem **P2**. Consideration of number fields of small degree might lead one to think that there are many rings of integers which are principal ideal domains but not euclidean domains; for example, Motzkin [Mo 49] proves that the ring of integers in $\mathbf{Q}(\sqrt{-d})$ is a euclidean domain if and only if

$$d = 1, 2, 3, 7, \text{ or } 11$$

However, it has been determined by Baker and Stark [Ar 91] that this ring is a principal ideal domain if and only if

$$d = 1, 2, 3, 7, 11, 19, 43, 67, 163$$

thus giving examples of euclidean domains which are not principal ideal domains. On the other hand, Weinberger [Len2 80] has proved the following astonishing result.

Theorem 8.1 *Let R be the ring of integers in a number field K, and assume that R has infinitely many units. Then, under the assumption of the Generalized Riemann Hypothesis (GRH), R is a euclidean domain if and only if it is a principal ideal domain.*

If GRH is true, one might question the worth of studying euclidean domains. On the other hand, the exhibition of a number field whose ring of integers has infinitely many units, is a principal ideal domain, but is *not* a euclidean domain would be an amusing way to disprove GRH.

We pause no longer at the question of **P2**, intriguing as it may be. **P3**, on the other hand, remains as challenging a problem as it was when the French mathematicians of the 1840s first formulated it. The many problems it has spawned (see [Lem 94]) have inspired over 150 years of mathematical research, and continue to occupy the research interests of prominent mathematicians to this day—it is hoped that this survey has provided the reader with a glimpse of the exciting mathematics associated with this problem.

A Background Definitions and Results

In this section, we give some results from cyclotomic field theory and algebraic number theory, many of them familiar, which are used throughout the thesis.

A.1 Cyclotomic Fields

Let $K = \mathbf{Q}(e^{2\pi i/n})$. We will write ζ_n for $e^{2\pi i/n}$, so $K = \mathbf{Q}(\zeta_n)$; when there is no danger of ambiguity, we will also replace ζ_n by ζ. We begin with an elementary result from Galois theory.

Proposition A.1 *$K / \mathbf{Q}$ is a Galois extension of degree $\phi(n)$, whose Galois group consists of automorphisms defined by sending $\zeta \longrightarrow \zeta^d$, where $1 \leq d \leq n$ and $\gcd(d, n) = 1$.*

The following corollary is then an immediate consequence of the tower law for field extensions:

Corollary A.2 *If $m \mid n$, then*

$$[\mathbf{Q}(\zeta_n) \,:\, \mathbf{Q}(\zeta_m)] = \phi(n)/\phi(m)$$

The next proposition, simple but surprising, helps reduce the amount of analysis we have to do:

Proposition A.3 *Suppose n is odd. Then*

$$\mathbf{Q}(\zeta_n) = \mathbf{Q}(\zeta_{2n})$$

Proof.

Since $\zeta_{2n}^2 = \zeta_n$, $\mathbf{Q}(\zeta_n) \subseteq \mathbf{Q}(\zeta_{2n})$. To see the other inclusion, multiply ζ_{2n} twice by $-1 = e^{\pi i} = e^{n \cdot 2\pi i/2n}$ to get

$$\zeta_{2n} = -e^{n \cdot 2\pi i/2n} \cdot e^{2\pi i/2n} = -e^{(n+1)\pi i/2n} = -e^{((n+1)/2)(2\pi i/n)} = -\zeta_n^{(n+1)/2} \in \mathbf{Q}(\zeta_n)$$

The following theorem is an important result about the algebraic structure of cyclotomic fields; because its proof involves more advanced algebraic number theory than is discussed in this thesis, we omit it here, and instead refer the interested reader to [Ri 72].

Theorem A.4 *The ring of algebraic integers in $\mathbf{Q}(\zeta_n)$ is $\mathbf{Z}[\zeta_n]$.*

A.2 Properties of the Norm

Now let K be any (finite) Galois extension of $\mathbf{Q}$, and R the ring of algebraic integers in K. Let $G = Gal(K/\mathbf{Q})$. The following proposition gives a few important properties of the field norm.

Proposition A.5 *Let N denote the field norm $N_{K/\mathbf{Q}}$.*

1. *Given $y \in K$, let $f(x) \in R[x]$ be the monic irreducible polynomial for y. If*

$$f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$$

then $N(y) = a_0^{[K:\mathbf{Q}]/d}$

2. *$y \in K \Rightarrow N(y) \in \mathbf{Q}$*

3. *$y \in R \Rightarrow N(y) \in \mathbf{Z}$*

4. *If $K = \mathbf{Q}(\zeta_n)$ for some $n \geq 0$ then $y \in K \Rightarrow N(y) \geq 0$.*

5. *$y \in R - \{0\} \Rightarrow |N(y)| = |R/(y)|$*

6. *For all $x, y \in K$, $N(xy) = N(x)N(y)$*

7. *$N(y) = 0 \Leftrightarrow y = 0$*

8. *$N(y) = \pm 1 \Leftrightarrow y \in R^\times$*

9. *If R is a principal ideal domain and $y \in R$ is irreducible, then $|N(y)| = p^r$ for some prime $p \in \mathbf{Z}$ and some $r \in \mathbf{N}$, $r \geq 1$*

Proof.

1. Given $y \in R$, let $f(x) \in R[x]$ be the monic irreducible polynomial for y. Write

$$f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$$

where $a_i \in \mathbf{Q}$ for all i, $0 \leq i \leq d-1$.

Let $O_y = \{\sigma(y) : \sigma \in G\}$. We claim that $f(x) = g(x)$, where

$$g(x) = \prod_{s \in O_y} (x - s)$$

Certainly O_y is fixed (as a set) by the action of G, so $g(x)$ is thereby fixed by G; so $g(x) \in \mathbf{Q}[x]$ and since $g(x)$ clearly has y as a root, $g(x)$ divides the irreducible polynomial $f(x)$ for y. By definition of irreducibility, $g(x) = f(x)$. Now $N(y) = \prod_{\sigma \in G} \sigma(y)$ and each element of O_y appears exactly $[K : \mathbf{Q}]/\mathbf{d}$ times in the above product. However, expanding $g(x)$ and equating its constant coefficient to that of $f(x)$ implies that $a_o = \prod_{s \in O_y} s$, whence

$$N(y) = \prod_{\sigma \in G} \sigma(y) = \prod_{s \in O_y} s^{[K\,:\,\mathbf{Q}]/d} = a_o^{[K\,:\,\mathbf{Q}]/d}$$

2. This follows immediately from (1).

3. If $y \in R$, it satisfies a monic irreducible polynomial $f(x) \in \mathbf{Q}[x]$. For any $\sigma \in G$, $\sigma(y)$ has the same irreducible polynomial, which is monic, so $\sigma(y)$ is also integral over $\mathbf{Q}$; hence $\sigma(y) \in R$. Hence $N(y) = \prod_{\sigma \in G} \sigma(y) \in R$. By (2), $N(y) \in \mathbf{Q}$, so $N(y) \in R \cap \mathbf{Q} = \mathbf{Z}$.

4. If $n = 2$, the field extension is trivial, so the proposition follows immediately. Assume $n \neq 2$. Recalling that G consists of automorphisms defined by sending $\zeta \longrightarrow \zeta^d$, where $1 \leq d \leq n$ and $\gcd(d, n) = 1$, we note that $\gcd(d, n) = 1 \Leftrightarrow \gcd(n - d, d) = 1$. So to every automorphism $\sigma \in G$ we associate a unique automorphism $\tau \in G$ such that $\sigma(\zeta) = \tau(\zeta^{-1})$. We claim that $\sigma \neq \tau$. If this were not the case, and j is chosen such that $\sigma(\zeta) = \zeta^j$, then $j \equiv -j \pmod{n}$, so $j \equiv n/2 \pmod{n}$ and $\sigma(\zeta) = \zeta^{n/2}$. Since σ is an automorphism, ζ and $\zeta^{n/2}$ must have the same order in the group of nth roots of unity; hence they both have order 2, which means that $n = 2$, contradiction. Since $\sigma(\zeta) = \tau(\zeta^{-1})$, $\tau(y) = \overline{\sigma(y)}$, and the automorphisms come in conjugate pairs, so choosing a set $\sigma_1, \ldots, \sigma_{\phi(n)/2}$ of representatives from each pair, we have

$$N(y) = \prod_{\sigma \in G} \sigma(y) = \prod_{i=1}^{\phi(n)/2} \sigma_i(y)\overline{\sigma_i(y)} = \prod_{i=1}^{\phi(n)/2} |\sigma_i(y)|^2$$

which is clearly nonnegative.

5. Fix $y \in R - \{0\}$. Let $d = \phi(n)$ and choose an enumeration $\sigma_1, \ldots, \sigma_d$ of G such that σ_1 represents the identity automorphism. Then define a descending chain of ideals

$$I_0 \supseteq I_1 \supseteq \ldots \supseteq I_d$$

by:

$$I_0 = R$$
$$I_1 = (\sigma(y))$$
$$I_j = (\sigma_1(y) \cdots \sigma_j(y))$$

for $1 \leq j \leq d$. Note that $I_d = (N(y))$. By (3), $|N(y)| = z \in \mathbf{Z}$, and since R is a free module of rank d over $\mathbf{Z}$, it follows that $R/(N(y)) = R/(z)$ is finite; in fact $|R/N(y)| = z^d$.

It is clear that $|I_i/I_{i+1}| = |I_j/I_{j+1}|$ for any i, j such that $0 \leq i, j \leq d - 1$. Hence,

$$z^d = |R/(N(y))| = |R/I_1| \cdots |I_{d-1}/I_d| = |R/I_1|^d = |R/(y)|^d$$

whence $|R/(y)| = z = |N(y)|$.

6.
$$N(xy) = \prod_{\sigma \in G} \sigma(xy) = \prod_{\sigma \in G} \sigma(x)\sigma(y) = \prod_{\sigma \in G} \sigma(x) \prod_{\sigma \in G} \sigma(y) = N(x)N(y)$$

7. If $y = 0$, then $\sigma(y) = 0$ for all $\sigma \in G$, so $N(y) = 0$. Conversely, $N(y) = \prod_{\sigma \in G} \sigma(y) = 0$, and the fact that $N(y)$ is in the field (integral domain) $\mathbf{Q}$ implies that $\sigma(y) = 0$ for some $\sigma \in G$. Hence $y = \sigma^{-1}(\sigma(y)) = 0$.

8. If $N(y) = \pm 1$, then by (5), $|R/(y)| = 1$, so (y) is the unit ideal, and y is a unit. Conversely, if y is a unit, then $|R/(y)| = |N(y)| = 1$.

9. Let $y \in R$ be irreducible. Then, since R is a PID, (y) is a maximal ideal of R, and so $R/(y)$ is a field. Since $|R/(y)| = |N(y)|$ (by part 5) is finite, $R/(y)$ is a finite field; hence its order is a positive prime power.

A.3 Different and Discriminant

Let K be a finite Galois extension of $\mathbf{Q}$, with Galois group G. K is separable, so we can apply the primitive element theorem to write $K = \mathbf{Q}(\alpha)$ for some $\alpha \in \mathbf{C}$. Let R be the ring of algebraic integers in K. We are about to introduce two very important number-theoretic quantities associated to a field extension—the *different* and its more prominent sister, the *discriminant*.

Definition A.6 *The* different $\delta_{K/\mathbf{Q}}$ *is equal to*

$$\prod_{\substack{\sigma in G \\ \sigma \neq id}} (\alpha - \sigma(\alpha))$$

When there is no danger of ambiguity, we will simply write δ for the different.
The next proposition follows directly from Definition A.6.

Proposition A.7 *Let K, α be as above, and let $f(x) \in \mathbf{Q}[x]$ be the monic irreducible polynomial for α. Then $\delta = f'(\alpha)$.*

Proof.
Since $K = \mathbf{Q}(\alpha)$, α has degree $[K : \mathbf{Q}]$ over $\mathbf{Q}$; hence its monic irreducible polynomial $f(x) \in \mathbf{Q}[x]$ has degree $[K : \mathbf{Q}] = |G|$. Writing $f(x) = \prod_{\sigma \in G}(x - \sigma(\alpha))$, we differentiate (formally) using Leibniz's rule and substitute α for x. All terms in the sum but one vanish; that term is equal to

$$\prod_{\substack{\sigma \in G \\ \sigma \neq id}} (\alpha - \sigma(\alpha)) = \delta$$

Definition A.8 *Let $K/\mathbf{Q}$ be a finite extension, and let R be the ring of integers in K. The* dual *of R (denoted R^*) is*

$$R^* = \{x \in K : Tr(xR) \subseteq R\}$$

We remark that the bilinear form $(x, y) = Tr(xy)$ is nondegenerate.

Lemma A.9 *Let $K = \mathbf{Q}(\alpha)$ be a finite extension of $\mathbf{Q}$ of degree n, and assume that*

$$f(x) = (x - \alpha)(b_0 + b_1 x + \ldots + b_{n-1}x^{n-1}) \in K[x]$$

is the monic irreducible polynomial for α. Then the dual basis (relative to the bilinear form $(\ ,\ )$) corresponding to the basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$ of K is

$$\{b_0/f'(\alpha), \ldots, b_{n-1}/f'(\alpha)\}$$

Proof.
Let $\alpha = \alpha_1, \ldots \alpha_n$ be the roots of f in $\mathbf{C}$; they are distinct because f is irreducible over $\mathbf{Q}[x]$. Now consider the polynomial

$$P_r(x) = \sum_{i=1}^{n} \alpha_i^r / f'(\alpha_i) \prod_{j \neq i}(x - \alpha_j)$$

Since $f'(\alpha_i) = \prod_{j \neq i}(\alpha_i - \alpha_j)$, it follows that for all i,

$$P_r(\alpha_i) = \alpha_i^r$$

$P_r(x)$ is a polynomial of degree at most $n-1$; hence it is determined by its values at the n distinct points $\alpha_1, \ldots, \alpha_n$. It follows that $P_r(x) = x^r$.

Now given any polynomial $g(x) = \sum_{i=1}^n a_i x^i \in K[x]$, write

$$Tr(g) = \sum_{i=1}^{n} Tr(a_i)x^i \in \mathbf{Q}[x]$$

From above, we write

$$x^r = P^r(x) = \sum_{i=1}^{n} \alpha_i^r / f'(\alpha_i) \prod_{j \neq i}(x - \alpha_j) = Tr(f(x)\alpha^r/(x-\alpha)f^\alpha)$$

$$= Tr((b_0 + b_1 x + \ldots + b_{n-1}x^{n-1})\alpha^r / f'(\alpha))$$

Equating coefficients of powers of x in the last equation, we see that $Tr((b_i/f'(\alpha))\alpha^r) = \delta_{ir}$, which proves the lemma.

Corollary A.10 *Suppose that $K = \mathbf{Q}(\alpha)$ is a finite extension of $\mathbf{Q}$, and $B = \mathbf{Z}[\alpha]$, where α is integral over $\mathbf{Z}$. Let f be as in Lemma A.9. Then*

$$B^* = f'(\alpha)^{-1}B = \delta^{-1}B$$

Proof.

By the lemma above, $B^* = f'(\alpha)^{-1}M$, where M is the $\mathbf{Z}$-submodule of K generated by $b_0, \ldots, b_{n-1}$. Write

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \text{ where } a_i \in \mathbf{Z}$$

Comparing this with

$$f(x) = (x - \alpha)(b_{n-1}x^{n-1} + \ldots + b_0)$$

we see that

$$\begin{aligned} b_{n-1} &= 1 \\ b_{n-2} - \alpha &= a_{n-1} \\ b_{n-3} - \alpha b_{n-2} &= a_{n-2} \\ &\vdots \end{aligned}$$

Clearly, $M \subseteq \mathbf{Z}[\alpha]$. To see the other inclusion, note that the first equation implies that $1 \in M$; that is, $\mathbf{Z} \subseteq M$. Using this fact, the second equation implies that $\alpha \in M$. In the third equation, we have $\alpha b_{n-2} \in M$, so multiplying the second equation by α gives $\alpha^2 \in M$.

Continuing in this manner, we conclude that $\alpha^i \in M$ for all i, $1 \leq i \leq n-1$, so $\mathbf{Z}[\alpha] \subseteq M$. Thus $M = \mathbf{Z}[\alpha] = B$.

We note that R is free as a $\mathbf{Z}$-module. Choose a basis (generating set) $W = \{w_1, \ldots, w_d\}$ for R as a $\mathbf{Z}$-module. Let $\{\sigma_1, \ldots, \sigma_d\}$ be any fixed enumeration of G, and define

$$a_{ij} = \sigma_i(w_j)$$

Definition A.11 *The* discriminant *of an extension field $K/\mathbf{Q}$ with respect to the basis W is*

$$\Delta^W_{K/\mathbf{Q}} = (\det(a_{ij}))^2$$

Now suppose $V = \{v_1, \ldots, v_d\}$ is another basis for R as a $\mathbf{Z}$-module. Then there exists an invertible matrix $M = (m_{ij})$ such that $v_i = M(w_i)$ for all i. Then

$$\Delta^V_{K/\mathbf{Q}} = (\det(\sigma_i(v_j)))^2 = (\det(\sigma_i(\sum_{k=1}^{d} m_{kj} w_k)))^2$$

$$= (\det \sum_{k=1}^{d} m_{kj}\sigma_i(w_j))^2 = (\det M(\sigma_i(v_j)))^2 = (\det M)^2 \Delta^W_{K/\mathbf{Q}}$$

Since M is an invertible matrix, its determinant must be a unit; hence we see from the above that the discriminant is defined (uniquely) up to the square of a unit. Since the only units in $\mathbf{Z}$ are ± 1, the discriminant is thus independent of the choice of basis; we henceforth refer to the discriminant as $\Delta_{K/\mathbf{Q}}$.

Proposition A.12 *Let $K = \mathbf{Q}(\alpha)$ be as above. Then*

$$\Delta_{K/\mathbf{Q}} = (-1)^{n(n-1)/2} \prod_{\substack{\sigma_i, \sigma_j \in G \\ i \neq j}} (\sigma_i(\alpha) - \sigma_j(\alpha))$$

Proof.

Consider the basis $W = \{1, \alpha, \ldots, \alpha^{d-1}\}$ of R as a module over $\mathbf{Z}$. Then

$$\Delta_{K/\mathbf{Q}} = (\det(\sigma_i(\alpha^{j-1})))^2 = (\det(\sigma_i(\alpha^{j-1})))^2$$

The determinant which needs to be computed is a Vandermonde determinant, and has value

$$\prod_{i<j} (\sigma_i(\alpha) - \sigma_j(\alpha))$$

so

$$\Delta_{K/\mathbf{Q}} = \prod_{i<j} (\sigma_i(\alpha) - \sigma_j(\alpha))^2$$

We can now write each squared term in the product as

$$(-1)(\sigma_i(\alpha) - \sigma_j(\alpha))(\sigma_j(\alpha) - \sigma_i(\alpha))$$

to get

$$\Delta_{K/\mathbf{Q}} = (-1)^{n(n-1)/2} \prod_{\substack{\sigma_i, \sigma_j \in G \\ i \neq j}} (\sigma_i(\alpha) - \sigma_j(\alpha))$$

The next proposition is apparent from Definition A.6 and Proposition A.12.

Proposition A.13 $\Delta_{K/\mathbf{Q}} = N(\delta_{K/\mathbf{Q}})$

Combining the above with Proposition A.7 yields

Corollary A.14 *Let $K = \mathbf{Q}(\alpha)$ be as above, and let $f(x) \in \mathbf{Q}[x]$ be the monic irreducible polynomial for α. Then*

$$\Delta_{K/\mathbf{Q}} = \prod_{\sigma \in G} f'(\sigma(\alpha))$$

B Proof of Theorem 5.9

We first prove Theorem 5.9 (1), as it is the easiest. Let R be a euclidean domain, with euclidean function σ, and let $I \subseteq R$ be any ideal. If $I = \{0\}$, I is certainly principal, so assume $I \neq \{0\}$, and consider $S = \{\sigma(i) : i \in I\}$. Being a subset of $\mathbf{N}$, S has a smallest element m; choose $j \in I$ such that $\sigma(j) = m$. Now given $a \in I$, use the fact that R is a euclidean domain to write $a = qj + r$. Since $a \in I$ and $j \in I$, $a - qj = r \in I$, and because $\sigma(j)$ is minimal, $\sigma(r) < \sigma(j)$ is impossible, so it must be the case that $r = 0$, and hence that $a = qj$. Thus, $I = (j)$ and R is a PID.

We now begin our proof of (2). Let R be any principal ideal domain. The proof that R is a UFD is not hard, but relies on a number of facts, which we outline below.

Definition B.1 *An integral domain R is called* Noetherian *if there is no infinite ascending sequence of (distinct) principal ideals.*

Lemma B.2 *R is Noetherian $\Leftrightarrow$ EOF holds in R.*

Proof.

If EOF does not hold in R then there exists an element $x \in R$ and a sequence of factorizations

$$x,\ y_1 x_1,\ y_1 y_2 x_2, \ldots$$

of x, which gives rise to an infinite ascending sequence

$$(x) \subseteq (x_1) \subseteq \ldots$$

of distinct principal ideals. Conversely, if

$$(a_1) \subseteq (a_2) \subseteq \ldots$$

is such a sequence, then the generator of (a_{i+1}) must divide the generator of a_i, so we get a nonterminating factorization

$$a_1 = b_1 a_2 = b_1 b_2 a_3 = \cdots$$

Proposition B.3 *Let R be an integral domain in which EOF holds. Then every prime element $p \in R$ is irreducible.*

Proof.

Suppose that $p \in R$ is prime and that $p \mid a$ for some $a \in R$. Now use EOF to write

$$a = c_1 \cdots c_k$$

as a product of irreducible elements. By induction on the definition of prime, $p \mid c_j$ for some $1 \leq j \leq k$. Thus, $c_j = yp$ for some $y \in R$, and since c_j is irreducible, one of y, p is a unit. Since p is prime, y must be a unit; so p, too, is irreducible.

Lemma B.4 *Let R be an integral domain in which EOF holds. Then R is a UFD if and only if every irreducible element is prime.*

Proof.

Suppose that R is a UFD, and, towards a contradiction, that p is an irreducible element which is not prime. Then there exist $a, b \in R$ such that $p \mid ab$, but $p \nmid a$ and $p \nmid b$. Then p appears in the factorization of ab into irreducible elements, but not in the factorization of a or b, contradiction.

Conversely, suppose that every irreducible element is prime, but that R is not a UFD. Then there exists $x \in R$ such that $p_1 p_2 \cdots p_n$ and $q_1 q_2 \cdots q_m$ are distinct factorizations of x into irreducible elements. Assume (without loss of generality) that $n \leq m$ and that $p_1 \neq u q_j$ for all $1 \leq j \leq m$ and all units $u \in R^\times$. Then by induction on the definition of prime, $p_1 \mid q_j$ for some $1 \leq j \leq m$, but since q_j is irreducible, it must be the case that $up_1 = q_j$ for some unit u, contradiction.

We note that to check that any PID R is a UFD, we need to verify that factorization of elements into irreducible factors is unique up to units, which by Lemma B.4 is equivalent to proving that every irreducible element is prime, *and* that EOF holds in R. We first check that every irreducible element is prime.

Proposition B.5 *Let R be a PID. Then every irreducible element of R is prime.*

Proof.

Suppose $p \in R$ is irreducible, and $p \mid ab$; it follows that (p) is a maximal ideal. Now consider $(p, a) \supseteq (p)$ and $(p, b) \supseteq (p)$. If $(p, a) = (p)$, then $(a) \subseteq (p)$, so $p \mid a$ and we are done; similarly if $(p, b) = (p)$. Since (p) is maximal, the only other possibility is that $(p, a) = (p, b) = (1) = R$. Then there exist $x, y, v, w \in R$ such that

$$1 = xp + ya$$

and

$$1 = vp + wb$$

Multiplying the two expressions gives

$$1 = xvp^2 + (xwb + vya)p + wyab$$

However, since $p \mid ab$, the right hand side is divisible by p, but clearly the left hand side is not, contradiction.

Finally, we show that EOF holds in R, thereby proving (2).

Proof of Theorem 5.9 (2)

By Lemma B.2, it suffices to show that R is Noetherian. Let

$$(a_1) \subseteq (a_2) \subseteq \cdots$$

be an infinite ascending sequence of principal ideals. We claim that $I = \bigcup_{i \in \mathbf{N}} (a_i)$ is an ideal. To see this, let $u, v \in I$, $r \in R$. Then there exists $n \in \mathbf{N}$ such that $u, v \in (a_n)$. Since a_n is an ideal, $u + v$ and ru are both in (a_n), and hence in I.

Since R is a PID, there exists $b \in R$ such that $I = (b)$ for some $b \in R$. Clearly, $b \in I$, so $b \in (a_m)$ for some $m \in \mathbf{N}$. Hence for any $k \in \mathbf{N}$, $(b) \subseteq (a_m) \subseteq (a_{m+k}) \subseteq I = (b)$. This forces $(a_m) = (a_{m+k})$ for all such k, so the elements of the sequence are not distinct. Hence EOF holds in R, and we conclude that R is a UFD.

Proof of Theorem 5.9 (4)

The proof of Theorem 5.9 (4) relies solely upon the lemma proven below. Combining this result with Theorem 5.9 (2), we note that since the ring of integers R_0 is the smallest integrally closed subring of K, it is also the smallest possible euclidean domain; in other words, every subring R of K which is a euclidean domain must contain R_0.

Lemma B.6 *Every UFD is integrally closed.*

Proof.

Let R be a UFD, and let K be its field of fractions. If R is not integrally closed then there exists $t \in K - R$ such that t is a solution of a monic irreducible polynomial

$$x^d + a_{d-1}x^{d+1} + \ldots + a_0$$

Writing $t = m/n$, with $m, n \in R$, $n \neq 0$, and $\gcd(m, n) = 1$,

$$(m^d/n^d) + a_{d-1}(m^{d-1}/n^{d-1}) + \ldots + a_0 = 0$$

Multiplying through by n^d and rearranging terms yields

$$-m^d = a_{d-1}m^{d-1}n + \ldots + a_0 n^d = n(a_{d-1}m^{d-1} + \ldots a_0 n^{d-1})$$

so n divides m^d, contradiction.

C Packing Theory

The following discussion follows Rogers' text closely.

Definition C.1 *Let $U \subseteq \mathbf{R}^n$ be a set with finite positive Lebesgue measure $\mu(U)$. Given a sequence $\{a_i\}_{i \in I}$ of points of $\mathbf{R}^n$, define the* system of translates *of U relative to $\{a_i\}$ (denoted $\mathbf{U}$) to be*

$$\mathbf{U} = \{S : S = U + a_i,\ i \in I\}$$

Definition C.2 *A sequence of subsets $S_1, S_2, \ldots$ of $\mathbf{R}^n$ is said to form a* packing *if $S_i \cap S_j = \emptyset$ for all $i \neq j$.*

Definition C.3 *Let $C \subseteq \mathbf{R}^n$ be a half-open, half-closed cube of sidelength s, centered at the point $x = (x_1, \ldots, x_n)$; that is,*

$$C = \{(y_1, \ldots, y_n) : y_i - s/2 \leq x_i < y_i + s/2 \text{ for all } i\}$$

and let $\mathbf{U}$ be a system of translates (of some Lebesgue measurable set U with positive Lebesgue measure) relative to some sequence $\{a_i\}_{i \in I}$. We then define the densities

$$\rho_+(\mathbf{U}, C) = 1/\mu(C) \sum_{(U+a_i) \cap C \neq \emptyset} \mu(U + a_i)$$

and

$$\rho_-(\mathbf{U}, C) = 1/\mu(C) \sum_{U+a_i \subseteq C} \mu(U + a_i)$$

In more generality, we define

$$\rho_+(\mathbf{U}) = \limsup_{s(C) \to \infty} \rho_+(\mathbf{U}, C)$$

and

$$\rho_-(\mathbf{U}) = \liminf_{s(C) \to \infty} \rho_-(\mathbf{U}, C)$$

With U as above, let D denote the set of systems of translates $\mathbf{U}$ of U such that $\rho_+(\mathbf{U}) < \infty$.

Definition C.4 *Let U and D be as above, and let $D' \subseteq D$ be the set of systems of translates which form packings into U. We define the* packing density

$$\delta(U) = \sup_{\mathbf{U} \in D'} \rho_+(\mathbf{U})$$

Definition C.5 *Given U as above, and letting μ denote Lebesgue measure, define the* center packing constant

$$\delta^*(U) = \delta(U)/\mu(U)$$

The following proposition is an immediate consequence of Definition C.3.

Proposition C.6 *With U and $\mathbf{U}$ as above, $\rho_-(\mathbf{U}) \leq \rho_+(\mathbf{U})$*

The next lemma provides an important characterization of packings.

Lemma C.7 *Suppose U and $\mathbf{U}$ are as above, and that $\mathbf{U}$ forms a packing. Then*

$$\rho_+(\mathbf{U}) \leq 1$$

Proof.

Denote by $s(U)$ the sidelength of some cube containing U. Choose $x \in \mathbf{R}^n$ and a cube C (of sidelength $s(C)$) centered at x. Then all of the translates $U + a_i$ which intersect C

lie in the cube C', centered at x with sidelength $s(C) + 2s(U)$. Since $\mathbf{U}$ is a packing, the sets $U + a_i$ and $U + a_j$ are mutually disjoint if $i \neq j$. Then

$$\sum_{(U+a_i)\cap C\neq\emptyset} \mu(U + a_i) \leq [s(C) + 2s(U)]^n$$

Dividing both sides by $\mu(C) = [s(C)]^n$ gives

$$\rho_+(\mathbf{U}, C) \leq [1 + 2s(U)/s(C)]^n$$

so

$$\rho_+(\mathbf{U}) \leq \limsup_{s(C)\to\infty} [1 + 2s(U)/s(C)]^n = 1$$

The following corollary is an easy consequence of the lemma and Definition C.4.

Corollary C.8 *Let U and $\mathbf{U}$ be as above. Then $\delta(U) \leq 1$.*

The next lemma is used in the proof of Theorem 6.5.

Lemma C.9 *Let $U \subseteq \mathbf{R}^n$ be a bounded set with positive Lebesgue measure, and let $C \subseteq \mathbf{R}^n$ be a closed cube with edges in the directions parallel to the basis vectors; let T be a non-singular affine transformation. If $a_1, \ldots a_E \in \mathbf{R}^n$ are any points and $b_1, b_2, \ldots$ is any enumeration of the lattice $[s(C)\mathbf{Z}]^n \subseteq \mathbf{R}^n$, then let*

$$\mathbf{K} = \{U + a_i + b_j\}\ i = 1, \ldots, E;\ j = 1, 2, \ldots$$

Denote by $T\mathbf{K}$ the system

$$\{T(U + a_i + b_j)\}\ i = 1, \ldots, E;\ j = 1, 2, \ldots$$

Then

$$\rho_+(\mathbf{K}) = \rho_+(T\mathbf{K}) = \rho_-(\mathbf{K}) = \rho_-(T\mathbf{K}) = E\mu(U)/\mu(C)$$

Proof.

First we note that the addition of any vector b_j of the abovementioned lattice to any of the points a_i leaves the systems $\mathbf{K}$ and $T\mathbf{K}$ unchanged; hence, we can assume that each translate $U + a_i$ intersects the cube C. Also, because T is affine, the system $T\mathbf{K}$ is the system of translates of the set $T(U)$ by the vectors $T(a_i + b_j) - T(0)$ for $i = 1, \ldots, E$; $j = 1, 2, \ldots$.

Writing $s(T(U))$ for the sidelength of any cube containing $T(U)$, let G denote a half-open, half-closed cube of sufficiently large sidelength, satisfying $s(G) > 2s(T(C))+2s(T(U))$, and let G' and G'' denote the cubes concentric with G having sidelengths

$$s(G) - 2s(T(U))$$

and

$$s(G) - 2s(T(U)) - 2s(T(C))$$

respectively. Then since the sets $T(C+b_j)$ cover the whole space, each point of the cube G'' lies in some set $T(C+b_k)$, which, given the assumption that $s(G) - 2s(T(U)) > 2s(T(C))$, lies completely within G'. Reordering the b_j if necessary, let $\{1, \ldots, D\}$ be the set of values of j for which $T(C+b_j) \subseteq G'$. Then we have

$$D\mu(T(C)) = \sum_{j=1}^{D} \mu(T(C+b_j)) \geq \mu(G'') = [s(G) - 2s(T(C)) - 2s(T(U))]^n \tag{1}$$

Now, since each set $U + a_i$ intersects C and $T(C + b_j)$ lies completely in G' for $j = 1, \ldots, D$, $T(U + a_i + b_j)$ intersects G' exactly when $i = 1, \ldots, E$ and $j = 1, \ldots, D$. Since G' has sidelength $s(G) - 2s(T(U))$, this implies that each of the sets $T(U + a_i + b_j)$ lies completely in G for the above values of i and j. Thus,

$$\rho_-(T\mathbf{K}, G) \geq 1/\mu(G) \sum_{i=1}^{E} \sum_{j=1}^{D} \mu(T(U + a_i + b_j)) = ED\mu(T(U))/\mu(G)$$

Using equation 1,

$$\rho_-(T\mathbf{K}, G) \geq E \cdot \mu(T(U))/\mu(T(C)) \cdot [1 - 2s(T(C))/s(G) - 2s(T(U))/s(G)]^n$$

Now we use the fact that T is affine non-singular to write this as

$$\rho_-(T\mathbf{K}, G) \geq E \cdot \mu(U)/\mu(C) \cdot [1 - 2s(T(C))/s(G) - 2s(T(U))/s(G)]^n$$

Since this holds for all G with $s(G)$ sufficiently large, it follows that

$$\rho_-(T\mathbf{K}) = \liminf_{s(G)\to\infty} \rho_-(T\mathbf{K}, G) \geq E \cdot \mu(U)/\mu(C)$$

In an entirely analogous way, one can show that

$$\rho_+(T\mathbf{K}) \leq E \cdot \mu(U)/\mu(C)$$

Combining this with Proposition C.6 yields

$$\rho_-(T\mathbf{K}) = \rho_+(T\mathbf{K}) = E\mu(U)/\mu(C)$$

Taking the special case in which T is the identity gives the desired result.

D Proof of Proposition 6.17

In our discussion we have defined a special subgroup $L \subseteq V$; it is convenient to give an alternate characterization of it in terms of the quadratic form q and its associated bilinear form. Towards this goal, we introduce the following lemma:

First, define $M = \{1, 2, \ldots, m\}$. Given $A \subseteq M$, define

$$e_A = \sum_{i \in A} e_i$$

Lemma D.1 *Suppose $y \in L$ satisfies $y \neq e_A$ for all $A \subseteq M$. Then there exists $z = \pm e_j \in L$ such that*

$$q(z) + q(y - z) < q(y)$$

Proof.

Write

$$y = \sum_{i=1}^{n} m_i e_i$$

with $m_i \in \mathbf{Z}$. Using the relation $\sum_{i=1}^{n} e_i = 0$, we can assume that

$$0 \leq \sum_{i=1}^{n} m_i \leq n - 1$$

For $z = \pm e_j$, we have

$$\begin{aligned} 1/2 \cdot (q(y) - q(z) - q(y - z)) \\ = (y, z) - (z, z) \\ = \pm(nm_j - \sum_{i=1}^{n} m_i) - (n - 1) \end{aligned}$$

If this quantity is positive for some j, then the lemma is proven. Thus we can assume that it is nonpositive for all j and both choices of sign. Then for $1 \leq j \leq n$, we have

$$nm_j \leq (\sum_{i=1}^{n} m_i) + (n - 1) \leq 2n - 2 < 2n,$$

$$nm_j \geq (\sum_{i=1}^{n} m_i) - (n - 1) \geq -n + 1 > -n,$$

so $m_j \in \{0, 1\}$ for all j, and so $y = e_A$ for some $A \subseteq M$, a contradiction.

The following lemma gives the characterization of E in terms of q and its associated bilinear form.

Lemma D.2 *Let $x \in V$. Then $x \in E$ if and only if $(x, e_A) \leq 1/2 \cdot q(e_A)$ for all $A \subseteq M$.*

Proof.

The "only if" direction comes from the construction of E; in the other direction, we can assume that $(x, e_A) \leq 1/2 \cdot q(e_A)$ for all $A \subseteq M$, then use induction on Lemma D.1 to prove that $(x, y) \leq 1/2 \cdot q(y)$ for all $y \in L$.

The next step in the proof is to characterize the points at which q is maximized.

Lemma D.3 *Suppose $x_o \in E$ satisfies $q(x_0) = b$. Then there exist $n - 1$ distinct proper non-empty subsets $A(i) \subset M$, $1 \leq i \leq n - 1$ such that x_0 is the unique solution of the system of equations:*

$$(x, e_{A(i)}) = 1/2 \cdot q(e_{A(i)}),\ 1 \leq i \leq n - 1$$

Proof.

Set

$$S = \{A \subset M \ : \ (x_0, e_A) = 1/2 \cdot q(e_A)\}$$

We assert that the dimension of the span of

$$\{e_A \ : \ A \in S\}$$

is exactly equal to $n-1$, that is, the dimension of the vector space V. If this is not the case, then there is some nonzero vector orthogonal to every vector of S; that is, there exists $z \in V - \{0\}$ such that

$$(z, e_A) = 0$$

for all $A \in S$. By scaling z by some real number, we can assume that

$$(x_0, z) \geq 0$$

and

$$(z, e_A) \leq 1/2 \cdot q(e_A) - (x_0, e_A) \text{ for all } A \subseteq M, \ \ A \notin S.$$

By the last inequality, we have $(x_0 + z, e_A) \leq 1/2 \cdot q(e_A)$ for all $A \subseteq M$; by Lemma D.2, $x_0 + z \in E$. However, our stipulation that $(x_0, z) \geq 0$ forces

$$q(x_0 + z) = q(x_0) + q(z) + 2(x_0, z) \geq q(x_0) + q(z) > q(x_0)$$

contradicting our assumption that $q(x_0) = b = \max\{q(x) : x \in E\}$.

Thus, the dimension of the span of $\{e_A \ : \ A \in S\}$ is $n-1$, so there are $n-1$ subsets $A(i) \in S$ such that $\{e_{A(i)} \ : \ 1 \leq i \leq n-1\}$ is linearly independent over $\mathbf{R}$. Then clearly x_0 is the unique solution of the system

$$(x, e_{A(i)}) = 1/2 \cdot q(e_{A(i)}).$$

Our final task is to characterize the subsets $A(i)$ of the previous lemma; it turns out that they are related to each other by a linear ordering.

Lemma D.4 *Let $x_0 \in E$ and let $A, B \subseteq M$ satisfy*

$$(x_0, e_A) = 1/2 \cdot q(e_A) \text{ and } (x_0, e_B) = 1/2 \cdot q(e_B)$$

Then $A \subseteq B$ or $B \subseteq A$

Proof.

Let $C = A - B$ and $D = B - A$. If $C = \emptyset$ or $D = \emptyset$, the lemma is proven; suppose that $C \neq \emptyset \neq D$. Then, if (by contradiction) $C \cap D = \emptyset$, we have

$$(e_{A \cap B}, e_{A \cup B}) - (e_A, e_B) = -(e_C, e_D) = |C| \cdot |D| > 0.$$

Thus,

$$\begin{aligned}(x_0, e_{A\cap B}) + (x_0, e_{A\cup B}) &= (x_0, e_A) + (x_0, e_B)\\ &= 1/2 \cdot q(e_A) + 1/2 \cdot q(e_B)\\ &= 1/2 \cdot q(e_A + e_B) - (e_A, e_B)\\ &> 1/2 \cdot q(e_{A\cap B} + e_{A\cup B}) - (e_{A\cap B}, e_{A\cup B})\\ &= 1/2 \cdot q(e_{A\cap B}) + 1/2 \cdot q(e_{A\cup B})\end{aligned}$$

Hence for at least one of $X = A \cap B$, $X = A \cup B$ we have $(x_0, e_X) > 1/2 \cdot q(e_X)$, which contradicts our choice of $x_0 \in E$.

Proof of Proposition 6.17

Let $x_0 \in E$ be a point such that $q(x_0) = b$, and let $\{A(i) : 1 \leq i \leq n-1\}$ be the system of $n-1$ subsets given by Lemma D.3. By Lemma D.4, there is a linear ordering, given by set inclusion, on this system. This is only possible if, after reindexing the vectors e_i and the sets $A(i)$, we have

$$A(i) = \{i+1, \ldots, n\}, \text{ for } 1 \leq i \leq n-1$$

We have $x_0 \in E$, so by Lemma D.2, we can compute

$$\sum_{j=i+1}^{n} (x_0, e_j) = 1/2 \cdot q(e_{A(i)}) = 1/2 \cdot i(n-i), \text{ for } 1 \leq i \leq n-1$$

Now choose a representation $x_0 = \sum_{j=1}^n x_j e_j$ such that $\sum_{j=1}^n x_j = 0$. Then we calculate

$$(x_0, e_j) = (\sum_{i=1}^{n} x_i e_i, e_j) = -\sum_{i=1}^{n} x_i + (n-1)x_j = nx_j$$

and the system of equations becomes

$$\sum_{j=i+1}^{n} nx_j = 1/2 \cdot i(n-i) \text{ for } 0 \leq i \leq n-1$$

This implies that

$$nx_i = i - 1/2(n+1) \text{ for } 1 \leq i \leq n$$

and so

$$x_0 = 1/n \cdot \sum_{i=1}^{n} ie_i$$

We reindexed the e_i once above, so $x_0 \in Z$, where Z is as in the statment of Proposition 6.17. By permuting the e_i, one obtains in a similar way that every element $x \in Z$ satisfies $q(x) = b$. Finally, we compute

$$b = \sum_{1\leq i<j\leq n} (i-j)^2/n^2 = (n^2-1)/12$$

References

[Ar 91] M. ARTIN, *Algebra*, Prentice-Hall, 1991.

[Ch 25] T. CHELLA, Dimostrazione dell'esistenza di un algoritmo delle divisioni successive per alcuni corpi circolari, *Annali di Matematica pura ed applicata*, (4) 1, 1924, pp. 199-218.

[Cl 94] D. CLARK, A Quadratic Field that is Euclidean but not Norm-euclidean, *Manuscripta Mathematica*, 83, 1994, pp. 327-330.

[Ed 77] H. M. EDWARDS, *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory*, Springer-Verlag, 1977.

[IR 90] K. IRELAND and M. ROSEN, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, 1990.

[Ka 88] G. KARPILOVSKY, *Unit Groups of Classical Rings*, Clarendon, 1988.

[La 93] S. LANG, *Algebra*, Addison-Wesley, 1993.

[La 64] S. LANG, *Algebraic Numbers*, Addison-Wesley, 1964.

[Lem 94] F. LEMMERMEYER, The Euclidean Algorithm in Algebraic Number Fields, preprint, 1994.

[Len 75] H. W. LENSTRA, Jr., Euclid's Algorithm in Cyclotomic Fields, *J. London Math. Soc.*, (2) 10, 1975, pp.457-465.

[Len 77] H. W. LENSTRA, Jr., Euclidean Number Fields of Large Degree, *Inventiones Mathematicae*, (38), 1977, pp. 237-254.

[Len 78] H. W. LENSTRA, Jr., Quelques exemples d'anneaux euclidiens, *Comptes Rendus de l'Académie des Sciences*, 286, 1978, pp. 683-685.

[Len 79] H. W. LENSTRA, Jr., Euclidean Number Fields 1, *The Mathematical Intelligencer*, (2) 1, 1979, pp 6-15.

[Len1 80] H. W. LENSTRA, Jr., Euclidean Number Fields 2, *The Mathematical Intelligencer*, (2) 2, 1980, pp.73-77.

[Len2 80] H. W. LENSTRA, Jr., Euclidean Number Fields 3, *The Mathematical Intelligencer*, (2) 2, 1980, pp.99-103.

[Lev 90] W. J. LEVEQUE, *Elementary Theory of Numbers*, Dover, 1990.

[Lo 77] R. LONG, *Algebraic Number Theory*, Marcel Dekker, 1977.

[Ma 75] J. M. MASLEY, On Euclidean Rings of Integers in Cyclotomic Fields, *J. Reine Angew. Math.*, 272, 1975, pp. 45-48.

[MaM 76] J. M. MASLEY and H. L. MONTGOMERY, Cyclotomic Fields with Unique Factorization, *J. Reine Angew. Math.*, 286/287, 1976, pp. 248-256.

[Mo 49] T. MOTZKIN, The Euclidean Algorithm, *Bull. Amer. Math. Soc.*, 55, 1949, pp. 1142-1146.

[Oj 77] T. OJALA, Euclid's Algorithm in the Cyclotomic Field $\mathbf{Q}(\zeta_{16})$, *Mathematics of Computation*, 31, No. 137, January 1977, pp. 268-273.

[Ou 09] J. OUSPENSKY, Note sur les nombres entiers dependant d'une racine cinquième de l'unité, *Math. Ann.*, 66, 1909, pp. 109-112.

[Ri 72] P. RIBENBOIM, *Algebraic Numbers*, John Wiley and Sons, 1972.

[Ro 64] C. A. ROGERS *Packing and Covering*, Cambridge University Press, 1964.

[Sa 71] P. SAMUEL, About Euclidean Rings *J. Algebra*, 19, 1971, pp. 282-301.

[Se 73] J-P. SERRE, *A Course in Arithmetic*, Springer-Verlag, 1973.

[Va 85] F. J. VAN DER LINDEN, *Euclidean Rings with Two Infinite Primes*, Mathematisch Centrum, 1985.

[Wa 82] L. C. WASHINGTON, *Introduction to Cyclotomic Fields*, Springer-Verlag, 1982.