Spring 5-2016

Origami Constructions of Rings of Algebraic Integers

Juergen Desmond Kritschgau
Bates College, jkritsch@bates.edu

Origami Constructions of Rings of Algebraic Integers

Jürgen Desmond Kritschgau

Origami Constructions of Rings of Algebraic Integers

An Honors Thesis

Presented to the Department of Mathematics

Bates College

in partial fulfillment of the requirements for the

Degree of Bachelor of Arts

by

Jürgen Desmond Kritschgau

Lewiston, Maine

3.28.2016

"Das Ergebnis habe ich schon, jetzt brauche ich nur noch den Weg,

der zu ihm führt."–Gauß

Contents

List of Figures

Acknowledgments

This thesis is not part of the meteoric rise of a rockstar, but it was fated. There are a lot of people that pushed me and helped me along even when I didn't ask for it.

The story starts with Gabriel Edge and Jacqui Gardner. They were both my high school math teachers, and some how they knew how much I liked math before I did. In fact, I think I tried to resist liking math despite how much fun their classes were.

Next, I have to thank an economics professor for dumbing down an economic model. Apparently, the class didn't know enough linear algebra to see the full blown model. I concluded that I was in the wrong class and quickly changed my focus to math.

I would like to thank Budapest and all the friends I made there. The problems I saw that summer reminded me that math is so much more than the entry level calculus classes make it out to be. The fun problems with creative solutions reminded me of high school geometry. Doing homework in Budapest with my roommates felt like solving puzzles, not doing computations. In particular, I have to thank James

Ronan, James Drain, and Nicolas Paskal for begin more disappointed in my grades than I was.

Coming back from Budapest, I knew I would have to make more math friends at Bates. In particular, I spent more time with Tom Sacchetti and Larissa Sambel. They both read drafts of my thesis and gave me good feed back. However, the time we spent solving problems and being excited by cool proofs as by far their most important contribution to my math experience.

I need to thank SUAMI 2015 for giving me a fun problem to look at, and Adriana Salerno for advising me through the thesis writing process. Additionally, I want to thank Peter Wong for teaching Abstract Algebra II. The impact that class had on my mathematical maturity and my thesis will be obvious. Furthermore, I appreciate everything anyone involved in the Bates mathematics department in the last four years had done for my mathematical life. I look forward to reconnecting with them at conferences in the future.

Finally, I cannot thank my parents, sister, and friends enough. Their support throughout my life has been and will be the most important factor in anything I do.

CHAPTER 1

Introduction

In origami, the artist uses intersections of folds as reference points to make new folds. This kind of construction can be extended to points on the complex plane. That is, given a set of reference points and a set of lines we can fold along, we can construct new reference points by adding intersections of lines to our set of reference points. These *Origami Constructions* are the subject of my thesis.

The order in which I present information is supposed to be the path of least resistance. However, that is not the order in which I engaged with the material. The chronological beginning of my thesis is with the paper: *Origami Rings* by Joe Buhler, Steve Butler, Warwick de Launey, and Ron Graham. Some friends of mine were working with origami rings over the summer, and I became curious. In order to understand the proofs and implications in the paper, I had to do some digging. Though I had already had classes that dealt with a lot of the algebra involved, I still needed to look things up frequently and find a thread that showed why the results in *Origami Rings* were novel.

After getting enough background information, I set out to extend these results.

The first chapter of my thesis will cover all of the background information required to understand the proofs in [**1**] and why they are important. In particular, start with basic ring theory, and show how the theory is motivated by the problem of solving polynomials. This narrative will result in an exploration of rings of algebraic integer rings in different extensions of the rational numbers. Most of this chapter consists of theorems and proofs from [**2**]. All of the proofs have been rewritten in my own words and I filled in some gaps in the logic. Most of the lemmas, were left as "exercises for the reader". I did those exercises and included the proofs. The sections on quadratic field extensions is mostly from [**3**]; some of the section on cyclotomic fields also comes from [**3**]. However, due to the target audience of that book, and the relative level of ease, those proofs had lots of holes for me to fill.

The second chapter is entirely a reconstruction of [**1**]. As in the background chapter, I make an effort to rewrite as many of the proofs in my own words. In many cases, the authors suggested a proof by induction, and left the details out almost completely. I have filled these in. The major result of [**1**] is that the origami constructions yield

rings that are very close to the rings of algebraic integers for cyclotomic fields.

In the third chapter, I begin to explore how the assumptions for the origami rings paper can be relaxed, while still getting a ring under the origami construction. This chapter is heavily guided by the logic of discovery. My hope is that this chapter shows how I came to formulate a new theorem that I prove in the fourth chapter. If these results are not new, I at least arrived at them independently.

CHAPTER 2

Background

The goal of this chapter is to provide background information and motivation for origami ring constructions. Section 1 deals with complex numbers and is attributed primarily to [**4**]. Sections 2 through 5 contains work done in [**2**]. The contributions of [**3**] are mostly contained in section 6, however, there is some overlap of sources in section 5.

1. Complex Numbers

The major parts of my thesis will deal with numbers in the complex plane. There is some notation and background knowledge about the complex numbers that will be extremely helpful down the line.

First, we define the complex plane $\mathbb{C} = \{x + \imath y | x, y \in \mathbb{R}\}$ where $\imath^2 = -1$. For each $z \in \mathbb{C}$ we can define $\bar{z} \in \mathbb{C}$ to be the conjugate of z. In particular, if $z = x + \imath y$, then $\bar{z} = x - \imath y$. The reason we like conjugates of complex numbers is that $z\bar{z} = x^2 + y^2 \in \mathbb{R}$. One case of conjugates is particularly near and dear to a mathematician's heart,

namely,

$$(x + \imath)(x - \imath) = x^2 + 1.$$

It is worth noting that conjugacy distributes. Let $p = a + \imath b$ and $q = c + \imath d$. Then

$$\begin{aligned}
\overline{p + q} &= \overline{a + \imath b + c + \imath d} \\
&= \overline{a + c + \imath(b + d)} \\
&= a + c - \imath(b + d) \\
&= a - \imath b + c - \imath d \\
&= \bar{p} + \bar{q}
\end{aligned}$$

Addition in the complex numbers is defined as follows

$$(a + \imath b) + (c + \imath d) = a + c + \imath(b + d)$$

In other words, addition is component wise.

Multiplication in the complex numbers is defined as

$$(a + \imath b)(c + \imath d) = ac - bd + \imath(ad + bc)$$

This is essentially the foil method. We define the modulus of a complex number as $|z| = \sqrt{x^2 + y^2}$ where $z = x + \imath y$.

Multiplying complex numbers by foiling them is cumbersome. Therefore, we would like to find a different notation that is easier to manage. Recall the following series expansions from calculus:

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

$$\cos(x) = \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n}}{(2n)!}$$

$$\sin(x) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1} x^{2n-1}}{(2n-1)!}$$

In particular, notice that

$$\cos(x) + \sin(x) = \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n}}{(2n)!} + \sum_{n=1}^{\infty} \frac{(-1)^{n-1} x^{2n-1}}{(2n-1)!} = \sum_{n=0}^{\infty} \frac{x^n}{n!} = e^x$$

Furthermore, recall the equations for polar coordinates

$$x = r\cos\theta$$

$$y = r\sin\theta$$

where $r = \sqrt{x^2 + y^2}$. The result is that $x + \imath y = \cos\theta + \imath \sin\theta$ for some θ. We define the *argument* of z as follows:

$$\arg z = \{\theta \in \mathbb{R} : |z|\cos\theta + \imath|z|\sin\theta = z\}$$

Notice that $\arg z$ is not well-defined. To make up for this we define the *principal argument* of z as follows:

$$\text{Arg } z = \{\theta \in (-\pi, \pi] : |z| \cos\theta + \imath |z| \theta = z\}$$

We can combine all of these facts to naturally rewrite complex numbers in *exponential form*. In particular, given $z = x + \imath y$ we have,

$$\begin{aligned} z &= x + \imath y \\ &= |z| \cos\theta + \imath |z| \sin\theta \\ &= |z| \left[\sum_{n=0}^{\infty} \frac{(-1)^n \theta^{2n}}{(2n)!} + \imath \sum_{n=1}^{\infty} \frac{(-1)^{n-1} \theta^{2n-1}}{(2n-1)!} \right] \end{aligned}$$

Notice that $\imath^{2n} = (-1)^n$ and $(-1)^{n-1} \imath^{2n-1} = -\imath$ or $\imath$

$$\begin{aligned} &= |z| \left[\sum_{n=0}^{\infty} \frac{\imath^{2n} \theta^{2n}}{(2n)!} + \sum_{n=1}^{\infty} \frac{(-1)^{n-1} \imath^{2n-1} \theta^{2n-1}}{(2n-1)!} \right] \\ &= |z| \sum_{n=0}^{\infty} \frac{(\imath\theta)^n}{n!} \\ &= |z| e^{\imath\theta} \end{aligned}$$

In particular, we have the following equation.

(Euler's Formula) $$e^{\imath\theta} = \cos\theta + \imath \sin\theta$$

Notice that when $\theta = \pi$ we have

$$e^{\imath\pi} + 1 = 0$$

which relates the constants $e, \imath, \pi, 1, 0$ to each other. However, the major impact of Euler's Formula is that we can find roots of polynomials more easily.

Euler's formula makes it easy to find zeros of polynomials in the complex numbers. Let's consider an example:

$$z^n - 1 = 0$$

If we rewrite $z = re^{\imath\theta}$, where $r = |z|$ and $z \neq 0$, then we have the equations

$$z^n - 1 = 0$$

$$(re^{\imath\theta})^n = 1$$

$$r^n e^{\imath n\theta} = 1$$

$$e^{\imath n\theta} = \frac{1}{r^n}.$$

Notice that $|e^{\imath n\theta}| = 1$, therefore, we know that $r = 1$.

$$e^{\imath n\theta} = 1$$

$$\cos n\theta + \imath \sin n\theta = 1$$

Since the imaginary component of 1 is 0, we know that $\sin n\theta = 0$. Thus, we can reduce the equation to

$$\cos n\theta = 1$$

$$n\theta = 2\pi k \text{ for } k \in \mathbb{Z}$$

$$\theta = \frac{2\pi k}{n} \text{ for } k \in \mathbb{Z}.$$

The result is that all complex solutions to $z^n - 1 = 0$ are of the form $e^{\imath\theta}$ where $\theta = \frac{2\pi k}{n}$ for some $k \in \mathbb{Z}$. Notice that $z^n - 1$ has more zeros in $\mathbb{C}$ than it does in $\mathbb{R}$. In particular, we can see that $z^n - 1$ has n distinct zeros in $\mathbb{C}$. This is nice because the degree of $z^n - 1$ is also n. However, this is not true in $\mathbb{R}$. In fact, all we can say is that if m is the number of solutions to $z^n - 1$ in $\mathbb{R}$ then $m \leq \deg z^n - 1$. The implication is that the real numbers are not as complete as the complex numbers. In particular, we cannot solve all polynomials with real coefficients in the real numbers. The remainder of the background section will formalize how we get from the real numbers to the complex numbers in a natural way.

2. Rings, Integral Domains, Fields, and Factor Rings

Polynomials require both addition and multiplication. That is, if $f(x)$ is a polynomial, then $f(a)$ with $a \in R$ must be defined. Since

polynomials often multiply and add elements together, we need to make sure that addition and multiplication are defined over a set R. In particular, we have the following definition of a *ring*.

DEFINITION 2.1. A *ring* R is a set with two binary operations, addition and multiplication, such that for all $a, b, c \in R$:

(1) $a + b = b + a$

(2) $(a + b) + c = a + (b + c)$

(3) There is an additive identity, $0 \in R$

(4) for all $a \in R$, there exists $-a \in R$ such that $a + (-a) = 0$

(5) $a(bc) = (ab)c$

(6) $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$

Here are a few examples of rings and properties of rings. The integers, $\mathbb{Z}$ are a ring under normal addition and multiplication. However, $\mathbb{Z}$ also has a multiplicative identity. We call the multiplicative identity the *unity* of $\mathbb{Z}$ and we say that $\mathbb{Z}$ is a ring with unity. Furthermore, $\mathbb{Z}$ has two units, namely 1 and -1. That is 1 and -1 are the only two elements in $\mathbb{Z}$ with a multiplicative inverse.

Next consider $\mathbb{Z}[x]$. This is the ring of polynomials with integer coefficients. The typical element in $\mathbb{Z}[x]$ has the form

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

where $a_i \in \mathbb{Z}$ and $a_n \neq 0$. Notice that these rings are *commutative*. That is, $ab = ba$ for all elements in the ring. This is not true in general.

In some sense, rings are the bare minimum amount of structure required to solve a polynomial. Since not all rings are created equal, it would be nice if we had many of them. One natural place to look for a new ring is within an old ring. In particular, looking at subsets of a ring is a good place to start.

DEFINITION 2.2. A subset S of a ring R is a subring of R if S is itself a ring with the operations inherited from R.

Consider the Gaussian integers denoted as $\mathbb{Z}[\imath]$. A typical Gaussian integer is of the form $a + b\imath$ where $a, b \in \mathbb{Z}$. The Gaussian integers are a subring of the complex numbers $\mathbb{C}$.

Rings were meant to be a generalization of the integers. That is, any set that was a ring would have the same properties as the integers. However, this is not true. There are properties of the integers that are not true of all rings. The most obvious one is that the integers are commutative. However, there are other important properties of the integers that we would like to abstract.

DEFINITION 2.3. A *zero-divisor* is a nonzero element a of a commutative ring R such that there is a nonzero element $b \in R$ with $ab = 0$.

The definition of zero-divisors lets us define integral domains.

DEFINITION 2.4. An *integral domain* is a commutative ring with unity and no zero-divisors.

In other words, a commutative ring is an integral domain if it has unity, and if $ab = 0$ for some a, b, then either $a = 0$ or $b = 0$. Obviously, the integers, rational numbers, and real numbers are integral domains. We can use this fact to show that the Gaussian integers are also an integral domain.

PROOF. Assume that $|r_1|e^{\imath\theta_1}$ and $|r_2|e^{\imath\theta_2}$ are elements in $\mathbb{Z}[\imath]$ such that $|r_1||r_2|e^{\imath\theta_1\theta_2} = 0$. Notice that $e^{\imath\theta_1\theta_2} \neq 0$. This implies that $|r_1||r_2| = 0$. Since $|r_1|, |r_2| \in \mathbb{R}$ either $|r_1| = 0$ or $|r_2| = 0$. Therefore, either $|r_1|e^{\imath\theta_1} = 0$ or $|r_2|e^{\imath\theta} = 0$. Thus, $\mathbb{Z}[\imath]$ is an integral domain. □

It is worth noting that this proof generalizes to show that $\mathbb{Z}[\sqrt{m}]$ is an integral domain for any $m \in \mathbb{Z}$. This will be nice to know later.

The reason we like integral domains is because they make it easy to solve polynomial equations. For example, consider

$$x^2 - 2x - 3 = 0$$

We can factor the polynomial to get

$$(x - 3)(x + 1) = 0$$

Now if we restrict x to be either an integer, rational, or real number then we know that

$$(x-3)(x+1)=0$$

if and only if either

$$x-3=0$$

or

$$x+1=0$$

since the integers, rationals, and reals are all integer domains.

However there is an even more fundamental use for integer domains, namely, the cancellation law.

THEOREM 2.1 (Cancellation). Let a, b, c belong to an integral domain. If $a \neq 0$ and $ab = ac$, then $b = c$.

PROOF. Assume that a, b, c belong to an integral domain, $a \neq 0$ and $ab = ac$. This implies that $ab - ac = 0$. Furthermore, $a(b-c) = 0$. Since a, b, c belong to an integral domain, we know that either $a = 0$ or $b - c = 0$. However, $a \neq 0$ by assumption, therefore, $b - c = 0$ and $b = c$. Thus, the theorem is proven. □

Another property that would make solving equations much easier is if every element in a ring was a unit. This would allow us to divide

by multiplying both sides of an equation by the inverse of an element. Fortunately, such beautiful things exist and they are called *fields*.

DEFINITION 2.5. A field F is a commutative ring with unity in which every nonzero element is a unit.

We will come back to fields because they arise naturally in ring theory. For groups, we can take a normal subgroup, and create a factor group. That is, we create a new group which is essentially the way elements of the normal subgroup behave in the context of the larger group. We can extend this idea to rings as well. However, it will not suffice to take a subring to create a factor ring. Instead, we need *ideals*.

DEFINITION 2.6. A subring A of a ring R is called a (two sided) *ideal* of R if for every $r \in R$ and every $a \in A$ both ra and ar are in A.

In essence, an ideal I of a ring R defines equivalence classes of elements in R in a similar way that reducing numbers by modulo n defines equivalence classes of integers. That is, ideals identify sets of elements with the same remainder within a ring. The idea here is that ideals *absorb* elements from R, the way mod n absorbs n's out of other integers. That is, if we apply any element from r multiplicatively to

the entire set A, we do not change the set A. This is important for showing that multiplication for a factor ring is well defined.

Like cosets for groups, ideals let us look at how elements in a ring interact given their equivalence class. That is, factor rings are rings where we factor out by an equivalence class.

DEFINITION 2.7. Let A be a two sided ideal of R. Then we call $R/A = \{r + A | r \in R\}$ a factor ring.

It is nontrivial to show that factor rings actually exist. This is because multiplication does not fall out of the definition of a factor ring as nicely as addition follows from the definition of a factor group. However, multiplication in a factor ring will be reminiscent of multiplication in modular groups.

PROOF. Let A be an ideal of a ring R. Since A is a normal subgroup of the group R, the additive properties of the factor ring R/A are obvious. Furthermore, we do not need to check that multiplication is associative or distributive because these properties follow from the fact that multiplication in R/A is inherited from R. Suppose we have elements $s + A = s' + A$ and $t + A = t' + A$. That is, s and s' are different representatives for the same coset. Similarly, t and t' are different representatives for the same coset. By definition of ideals,

there exists an element $a \in A$ such that $s = s' + a$. Similarly, there exists an element $b \in A$ such that $t = t' + b$. Consider,

$$st = (s' + a)(t' + b)$$

$$st = s't' + s'b + at' + ab$$

$$st + A = s't' + s'b + at' + ab + A$$

Notice that $s'b, at', ab$ are all elements in A, and are absorbed by A. Therefore, we have the following:

$$st + A = s't' + A$$

This means that multiplication is well defined in factor rings. That is, we can take different representatives for a coset and still get the same element back if we multiply using that representative.

We can see that this proof relies on the fact that A can absorb any ra, ar where $r \in R$ and $a \in A$. Thus, the proof would fail if there existed an $ar \notin A$. Therefore, we are entitled to the fact that R/A is a ring if and only if A is an ideal of R. □

Let's look at an example of a factor ring. Consider the polynomial ring with real coefficients

$$\mathbb{R}[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 | a_n \neq 0, a_i \in \mathbb{R}\}$$

Notice that$\langle x^2+1\rangle = \{f(x)(x^2+1)|f(x) \in \mathbb{R}[x]\}$ is an ideal by definition. We call it the principle ideal generated by x^2+1. Let's examine the typical element in $\langle x^2+1\rangle$.

Let $f(x) \in \mathbb{R}[x]$ be arbitrary but fixed. Consider, $f(x)+\langle x^2+1\rangle$. By the division algorithm, we know that there exists $q(x), r(x) \in \mathbb{R}[x]$ such that $q(x)(x^2+1)+r(x) = f(x)$. Notice that the degree of $r(x)$ must be strictly less than 2. Now,

$$f(x)+\langle x^2+1\rangle = q(x)(x^2+1)+r(x)+\langle x^2+1\rangle$$

Notice that $q(x)(x^2+1) \in \langle x^2+1\rangle$, so we have

$$f(x)+\langle x^2+1\rangle = r(x)+\langle x^2+1\rangle$$

where $r(x)$ is of the form $ax+b$, $a, b \in \mathbb{R}$.

Notice that we treat $x^2+1+\langle x^2+1\rangle$ the same as $0+\langle x^2+1\rangle$. This implies that

$$x^2+\langle x^2+1\rangle = -1+\langle x^2+1\rangle$$

In other words, $x+\langle x^2+1\rangle$ behaves just like $\imath \in \mathbb{C}$. The result is that we can define a ring isomorphism between $\mathbb{R}[x]/\langle x^2+1\rangle$ and $\mathbb{C}$. In particular, consider $\varphi : \mathbb{R}[x]/\langle x^2+1\rangle \to \mathbb{C}$ given by

$$\varphi(ax+b+\langle x^2+1\rangle) = b+a\imath$$

Furthermore, a ring can have many ideals. For example, any element a in a commutative ring R will define an ideal of R. In particular $\langle a \rangle = \{ba | b \in R\}$ is an ideal of R. Furthermore, every integral domain is commutative by definition. It is no surprise that there are some ideals we care about more than others, because the corresponding factor rings are nicer. Let's take a look at some nice ideals.

DEFINITION 2.8. A *prime ideal* A of a commutative ring R is a proper ideal of R such that $a, b \in R$ and $ab \in A$ implies that $a \in A$ or $b \in A$.

Prime ideals are nice because their factor rings are integral domains. In particular, we have the following theorem.

THEOREM 2.2. Let R be a commutative ring with unity and let A be an ideal of R. Then R/A is an integral domain if and only if A is prime.

DEFINITION 2.9. A *maximal* ideal A of a commutative ring R is a proper ideal of R such that, whenever B is an ideal of R and $A \subset B \subset R$, then $B = A$ or $B = R$.

This is where we naturally stumble upon fields. In particular, we have the following theorem.

THEOREM 2.3. Let R be a commutative ring with unity and let A be an ideal of R. Then R/A is a field if and only if A is maximal.

For the proofs of Theorems 2.2 and 2.3 refer to [**2**] pg. 268. Showing that an ideal is maximal is tough. However, the general strategy is to show that adding any element from $I - R$ to I requires adding all elements from $I - R$ to I. The obvious question is for which $a \in R$ is $\langle a \rangle$ an ideal. This is the topic of the next section.

3. Polynomial Rings and Field Extensions

Though most undergraduates are familiar with polynomials with real coefficients over x as functions, we can also consider polynomials as elements of a ring. In particular, we will use the following abstract approach to polynomials.

DEFINITION 2.10. Let R be a commutative ring. The set of formal symbols

$$R[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 | a_i \in R, n \in \mathbb{N}\, a_n \neq 0\}$$

is called the ring of polynomials over R in the indeterminate x.

Under this definition, two polynomials $p(x)$ and $q(x)$ are considered equivalent if and only if for all $n \in \mathbb{N}$, the nth coefficient of $p(x)$ is the same as the nth coefficient of $q(x)$.

As one might think, the properties of $R[x]$ are in part determined by the properties of R. In particular, we care about the properties of $R[x]$ when R is a field. The next theorem shows that we have a division algorithm for $F[x]$ when F is a field. Recall the analogy between factoring by ideals and looking at the integers under modulo p. When we define $n \cong k \mod p$ we mean that there exists unique $q, r \in \mathbb{Z}$ such that $n = qp + r$ and $r = k$. Having a division algorithm for polynomial rings will help formalize the analogy from factoring by ideals and "moding out" by p.

THEOREM 2.4. Let F be a field and let $f(x)$ and $g(x) \in F[x]$ with $g(x) \neq 0$. Then there exist unique polynomials $q(x)$ and $r(x) \in F[x]$ such that $f(x) = g(x)q(x) + r(x)$ and either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

PROOF. Notice that the theorem is trivial if $f(x) = 0$ or $\deg f(x) < \deg g(x)$. In particular, $f(x) = 0g(x) + f(x)$. Thus we will assume that $n = \deg f(x) \geq \deg g(x) = m$. Let a_i be the coefficient of x^i in $f(x)$. Define b_i similarly. We will proceed by strong induction.

Base Case: Let $N = 1$. The base case is taken care of by the case we examined at the beginning of the proof. That is, if $f(x) = 0$ or $\deg f(x) < \deg g(x)$, then $f(x) = 0g(x) + f(x)$. Assume that $f(x) = c$

where $c \in F$ and $g(x) = d$ where $d \in F$. Since F is a field, there exists a unique element $\frac{c}{d} \in F[x]$ such that $f(x) = g(x)\frac{c}{d}$. In this case, $r(x)$ is 0 and the base case is satisfied.

Induction Hypothesis: For all $f(x)$ such that $n < N$, we have $q(x), r(x) \in F[x]$ such that $f(x) = g(x)q(x) + r(x)$ and $\deg r(x) < \deg g(x)$.

Induction Step: Let N be fixed. Assume $\deg f(x) = N$. Using long division, we get

$$f_1(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x)$$

Notice that $\deg f_1(x) < N$. Either $f_1(x) = 0$ or $\deg f_1(x) < \deg f(x)$. In either case, apply the induction hypothesis to $f_1(x)$ to get

$$f_1(x) = q_1(x)g(x) + r_1(x)$$

We combine equations to get

$$f(x) = q_1(x)g(x) + a_n b_m^{-1} x^{n-m} g(x) + r_1(x)$$

$$= (q_1(x) + a_n b_m^{-1} x^{n-m})g(x) + r_1(x)$$

Therefore, we have found $q(x) = q_1(x) + a_n b_m^1$ and $r(x) = r_1(x)$ such that $f(x) = q(x)g(x) + r(x)$, concluding the induction step.

Uniqueness: We must still show that each factorization is unique. Suppose

$$f(x) = q(x)g(x) + r(x)$$

and

$$f(x) = q'(x)g(x) + r'(x)$$

By subtracting these two equations from each other we get

$$g(x)(q(x) - q'(x)) = r(x) - r'(x)$$

Either $r(x) - r'(x) = 0$ or $\deg r(x) - r'(x) \geq \deg g(x)$. The latter is impossible, therefore, $r(x) - r'(x) = 0$ which implies that $r(x) = r'(x)$. This in turn implies that $g(x)(q(x) - q'(x)) = 0$. Since $g(x) \neq 0$ by assumption, we have $q(x) = q'(x)$. This completes the proof. □

Recall we are interested in finding elements $f(x) \in R[x]$ such that $\langle f(x) \rangle$ is a nice ideal. In particular, we want $\langle f(x) \rangle$ to be a maximal ideal of $R[x]$. The corollaries of Theorem 2.4 will provide the infrastructure for a characterization of a maximal ideal of a polynomial ring. We will prove each corollary in turn. The proofs for these corollaries and the required lemmas are going to come fast and furious. Each proof builds on the previous corollary.

COROLLARY 2.4.1. Let F be a field, $a \in F$, and $f(x) \in F[x]$. Then $f(a)$ is the remainder in the division of $f(x)$ by $x - a$.

PROOF. Let F be a field, $a \in F$, and $f(x) \in F[x]$. By Theorem 2.4, there exists $q(x), r(x) \in F[x]$ such that

$$f(x) = q(x)(x - a) + r(x)$$

Consider $f(a)$. Notice that $q(a)(a-a) = 0$. Therefore, we have $f(a) = r(a)$. □

COROLLARY 2.4.2. Let F be a field, $a \in F$, and $f(x) \in F[x]$. Then a is a zero of $f(x)$ if and only if $x - a$ is a factor of $f(x)$.

PROOF. Let F be a field, $a \in F$, and $f(x) \in F[x]$. By Theorem 2.4, there exists $q(x), r(x) \in F[x]$ such that

$$f(x) = q(x)(x - a) + r(x)$$

Assume that $f(a) = 0$. By Corollary 2.4.1, we have $r(a) = 0$. This implies that $f(x) = q(x)(x - a)$. Assume $f(x) = q(x)(x - a)$ for some $q(x) \in F[x]$. This implies that $f(a) = q(a)(a - a) = 0$. Thus, both directions of the corollary have been shown. □

To prove the next corollary we will need the following two lemmas.

LEMMA 2.1 (Degree Rule). Let D be an integral domain and $f(x), g(x) \in D[x]$. Then $\deg(f(x) \cdot g(x)) = \deg f(x) + \deg g(x)$.

PROOF. Let D be an integral domain and $f(x), g(x) \in D[x]$. Let $n = \deg f(x)$ and $m = \deg g(x)$. By definition of degree, the exponent of x in the leading term of $f(x)$ and $g(x)$ is n and m respectively. By definition of polynomial ring multiplication, the leading term of $f(x) \cdot g(x) = a_n b_m x^{m+n}$. Since D is an integral domain $a_n b_m \neq 0$. Therefore,

$$\deg f(x) \cdot g(x) = m + n = \deg f(x) + \deg g(x)$$

proving the degree rule. □

LEMMA 2.2. Let $f(x)$ belong to $F[x]$, where F is a field. Let a be a zero of $f(x)$ with multiplicity k, and write $f(x) = (x - a)^k q(x)$. If $b \neq a$ is a zero of $q(x)$, then b has the same multiplicity as a zero of $q(x)$ as it does for $f(x)$.

PROOF. Let $f(x)$ belong to $F[x]$, where F is a field. Let a be a zero of $f(x)$ with multiplicity k, and write $f(x) = (x - a)^k q(x)$. Assume $b \neq a$ is a zero of $q(x)$ with multiplicity n. By Corollary 2.4.2, $(x - b)$ divides $q(x)$ n times. That is $q(x) = (x-b)^n \bar{q}(x)$ for some $\bar{q}(x) \in F[x]$.

We can use this equation to see that

$$f(x) = (x-a)^k(x-b)^n\bar{q}(x)$$

Thus, by Corollary 2.4.2, we know that b is a zero of $f(x)$ with multiplicity n. □

COROLLARY 2.4.3. A polynomial of degree n over a field has at most n zeros, counting multiplicity.

PROOF. Let F be a field. Let $f(x) \in F[x]$ and $n = \deg f(x)$. We will prove this corollary by strong induction on the degree n.

Base Case: Assume $n = 0$. This suggests that $f(x) = a$ where $a \neq 0$ and $a \in F$. Thus, $f(x)$ does not have any zeros.

Induction Hypothesis: Let $f(x) \in F[x]$ such that $\deg f(x) \leq N$. Then $f(x)$ has at most N zeros, counting multiplicity.

Induction Step: Let $\deg f(x) = N + 1$. Assume that $a \in F$ is a zero of $f(x)$ with multiplicity k. By Corollary 2.4.2, we have

$$f(x) = (x-a)^k q(x)$$

for some $q(x) \in F[x]$. By Lemma 2.1

$$\deg f(x) = \deg(x-a)^k \deg q(x) = k + \deg q(x)$$

If $k = N + 1$ we are done. Otherwise, we know that $0 < \deg q(x) < N+1$. Therefore, we can apply the induction hypothesis to $q(x)$ to find that $q(x)$ has at most $\deg q(x)$ zeros. By Lemma 2.2, we know that any zero of $q(x)$ is a zero of $f(x)$ with the same multiplicity. Therefore, $f(x)$ has at most $k + \deg q(x)$ zeros. Notice that $k + \deg(x) = N + 1$. Thus, $f(x)$ has at most $N + 1$ zeros and the induction step is complete. □

Now that we have a division algorithm for polynomials over a field, it is natural to ask if every polynomial in a field can be factored. Like prime numbers in the integers, there are polynomials that cannot be factored. We call these polynomials irreducible. As it turns out, irreducible polynomials will give us maximal ideals of their polynomial ring.

DEFINITION 2.11. Let D be an integral domain. A polynomial $f(x)$ from $D[x]$ that is neither the zero polynomial nor a unit in $D[x]$ is said to be *irreducible over* D if, whenever $f(x)$ is expressed as a product $f(x) = g(x)h(x)$, with $g(x), h(x) \in D[x]$, then $g(x)$ or $h(x)$ is a unit in $D[x]$.

Notice, that if F is a field, then every element in $F[x]$ is either 0 or a unit. Thus, $f(x)$ being irreducible over a field F is equivalent to saying that $f(x)$ cannot be written as the product of two lower degree

polynomials in $F[x]$. The following theorem and its corollary will show that every irreducible polynomial over a field F, will give us an ideal I whose corresponding factor ring is also a field. In order to prove Theorem 2.5, we need the following lemma:

LEMMA 2.3. If A is an ideal of a ring R and 1 belongs to A, then $A = R$.

PROOF. Let A be an ideal of a ring R and assume that $1 \in A$. By definition of ideal, $ra \in A$ for all $r \in R$ and $a \in A$. Since $1 \in A$, it follows that there exists $a^{-1} \in R$. Let $r \in R$ be arbitrary. Notice that $r = ra^{-1}a \in A$ by definition. Therefore, it follows that $r \in A$ and $R \subset A$. Furthermore, $A \subset R$ by definition of ideal. Therefore, $A = R$ proving the result. Thus, if $1 \in A$, then $A = R$. □

The utility of Lemma 2.3 comes from its contrapositive in the context of polynomial rings. In particular, if $A = \langle a(x) \rangle$ where $a(x) \in R[x]$ and A is maximal in $R[x]$, then $A \neq R[x]$ by definition. Therefore, by Lemma 2.3 $a(x)$ is not a unit. Recall that in order for $a(x)$ to be irreducible, $a(x)$ cannot be a unit.

THEOREM 2.5. Let F be a field and let $p(x) \in F[x]$. Then $\langle p(x) \rangle$ is a maximal ideal in $F[x]$ if and only if $p(x)$ is irreducible over F.

PROOF. Let F be a field and let $p(x) \in F[x]$. Assume that $\langle p(x) \rangle$ is a maximal ideal. Since neither $\{0\}$ nor $F[x]$ are maximal ideals by definition, $p(x) \neq 0$ and $p(x)$ is not a unit. If $p(x)$ where a unit, then $1 \in \langle p(x) \rangle$, and $\langle p(x) \rangle = F[x]$ by Lemma 2.3. We will proceed by contraction. Assume that $p(x)$ is reducible. That is $p(x) = g(x)h(x)$ for some $g(x), h(x) \in F[x]$ such that $\deg g(x), \deg h(x) < \deg p(x)$. This implies that $\langle p(x) \rangle \subseteq \langle g(x) \rangle \subseteq F[x]$. Since $\langle p(x) \rangle$ is maximal, there are two cases: either $\langle p(x) \rangle = \langle g(x) \rangle$ or $\langle g(x) \rangle = F[x]$.

Case I: Assume $\langle p(x) \rangle = \langle g(x) \rangle$. This implies that $\deg g(x) = \deg p(x)$, which is a contradiction.

Case II: Assume that $\langle g(x) \rangle = F[x]$. By the degree rule, this implies that $\deg g(x) = 0$ and $\deg h(x) = \deg p(x)$, which is a contradiction.

In either case, we have a contradiction. Therefore, $p(x)$ is irreducible.

Now assume that $p(x)$ is irreducible over F. Let I be an ideal of $F[x]$ such that $\langle p(x) \rangle \subseteq I \subseteq F[x]$. Since $F[x]$ is a principle ideal domain, $I = \langle g(x) \rangle$ for some $g(x) \in F[x]$. Therefore, we have that $p(x) = g(x)h(x)$ for some $h(x) \in F[x]$. Since $p(x)$ is irreducible, either $g(x)$ or $h(x)$ is a constant. If $g(x)$ is a constant, then $\langle g(x) \rangle = F[x]$. If

$h(x)$ is a constant, then $\langle p(x)\rangle = \langle g(x)\rangle$. Therefore, $\langle p(x)\rangle$ is maximal by definition. Thus, the theorem has been shown. □

COROLLARY 2.5.1. Let F be a field and $p(x)$ be an irreducible polynomial over F. Then $F[x]/\langle p(x)\rangle$ is a field.

PROOF. The corollary follows from the previous theorem and Theorem 2.3. □

Notice, that if we have a polynomial $p(x) \in F[x]$ that is irreducible over F, and $\deg p(x) = 1$, then $p(x)$ has exactly 1 zero. In particular, if $\deg p(x) = 1$ then $p(x)$ is of the form $ax + b$ where $a, b \in F$. Since F is a field, $-a^1 b \in F$ and is a zero of $p(x)$. However, if $\deg p(x) \geq 2$ and $p(x)$ is irreducible over F, then $p(x)$ will have strictly fewer than $\deg p(x)$ zeros in F. This follows from Corollary 2.4.2. That is, if a is a zero of $p(x)$ then $(x - a)$ is a factor of $p(x)$. However, if $p(x)$ has a factor, then it is reducible. Thus, irreducible polynomials over a field F cannot have any zeros in the field F. Notice that we are beginning to address the problem raised at the end of section 1. In particular, it is weird that $x^2 + 1$ has two zeros in $\mathbb{C}$, but no zeros in $\mathbb{R}$. Part of this mystery has been solved: $x^2 + 1$ doesn't have any zeros in $\mathbb{R}$ because it is irreducible over R. We still have to explain how $x^2 + 1$ gets zeros in $\mathbb{C}$. This is where *field extensions* come in.

DEFINITION 2.12. A field E is an extension field of a field F if $F \subseteq E$ and the operations of F are those of E restricted to F.

Recall the factor ring $\mathbb{R}[x]/\langle x^2+1\rangle$. Notice that x^2+1 is irreducible over $\mathbb{R}$. However, x^2+1 has a zero in $\mathbb{R}[x]/\langle x^2+1\rangle$, namely, $x+\langle x^2+1\rangle$. Furthermore, we showed that $\mathbb{R}[x]/\langle x^2+1\rangle \cong \mathbb{C}$. Here is the kicker, $\mathbb{C}$ is an extension field of $\mathbb{R}$. The remainder of this section will formalize this fact, and generalize it to other irreducible polynomials over a field F.

THEOREM 2.6. Let F be a field and let $f(x)$ be a nonconstant polynomial in $F[x]$. Then there is an extension field E of F in which $f(x)$ has a zero.

PROOF. Let $f(x) \in F[x]$ where F is a field. By Theorem 2.4, $f(x)$ must have an irreducible factor $p(x)$. By Lemma 2.2, if we can find a zero for $p(x)$, then we have found a zero for $f(x)$. That is, we want to construct a field E such that $p(x)$ has a zero in E. Consider $F[x]/\langle p(x)\rangle$. We know that $F[x]/\langle p(x)\rangle$ is a field by Corollary 2.5.1. Notice that the map $\phi : F \to F[x]/\langle p(x)\rangle$ given by $\phi(a) = a + \langle p(x)\rangle$ is an isomorphism between F and elements of $F[x]/\langle p(x)\rangle$ of the form $a + \langle p(x)\rangle$ where $a \in F$. That is, F is isomorphic to a subfield of $F[x]/\langle p(x)\rangle$.

Now we must show that $p(x)$ has a zero in $F[x]/\langle p(x)\rangle$. Consider

$$p(x + \langle p(x)\rangle) = p(x) + \langle p(x)\rangle$$

$$= 0 + \langle p(x)\rangle$$

Thus, we have shown that $F[x]/\langle p(x)\rangle$ is a field extension of F in which $f(x)$ has a zero. □

Theorem 2.6 lets us find at least one zero of an irreducible polynomial. However, this is only part of our goal. We want to be able to find all zeros of a polynomial such that the number of zeros in a field is the same as the polynomial's degree. This kind of field is a *splitting field* of a polynomial.

DEFINITION 2.13. Let E be an extension field of F and let $f(x) \in F[x]$. We say that $f(x)$ splits in E if $f(x)$ can be factored as a product of linear factors in $E[x]$. We call E the splitting field for $f(x)$ over F if $f(x)$ splits in E but in no proper subfield of E.

Finding the splitting field for polynomial $f(x)$ over F amounts to applying Theorem 2.6 enough times to find all of the zeros. In particular, we get the following theorem:

THEOREM 2.7. Let F be a field and let $f(x)$ be a nonconstant element in $F[x]$. Then there exists a spiting field E for $f(x)$ over F.

PROOF. Let F be a field and let $f(x)$ be a nonconstant element in $F[x]$. We will use strong induction on $n = \deg f(x)$.

Base Case: Assume $\deg f(x) = 1$. This implies that $f(x) = ax+b$ for some $a, b \in F$. Thus, F is a splitting field for $f(x)$ over F.

Induction Hypothesis: If $\deg f(x) \leq N$, then there exists a splitting field E for $f(x)$ over F.

Induction Step: Assume that $\deg f(x) = N+1$. By Theorem 2.6, there exists an extension E of F such that $f(a_1) = 0$ for some $a_1 \in E$. By the division algorithm, we can write

$$f(x) = (x - a_1)q(x)$$

for some $q(x) \in E[x]$. Notice, that by Lemma 2.1 $\deg q(x) = N$. Therefore, we may apply the induction hypothesis to $q(x)$ to find an extension field K that contains all zeros of $q(x)$ over E. Call these zeros, $a_2, \ldots, a_{N+1}$. By Lemma 2.2, all the zeros of $q(x)$ are also zeros of $f(x)$. Thus, $K = F(a_1, \ldots, a_{N+1})$ is a splitting field for $f(x)$ over F, and the induction step is complete. □

Theorem 2.7 lets us find a spitting field for any polynomial $f(x)$ over a field F. However, we still don't know exactly what these fields look like. Of course they are of the form $F[x]/\langle p(x)\rangle$. But given the fact that we must repeatedly extend fields by factoring out maximal

ideals, the exact structure of these fields gets pretty messy. Before we can show that the splitting fields for $f(x)$ over F is $F(a_1, \ldots, a_n)$ — $F(a_1, \ldots, a_n)$ is the smallest field containing all elements of F and $a_1, \ldots a_n$— we need two lemmas. The first lemma relates particular representatives of elements in $F[x]/\langle p(x)\rangle$ to elements in $F[x]$. The second lemma shows that $\langle p(x)\rangle$ is the kernel for the homomorphism from $F[x]$ to the factor ring $F[x]/\langle p(x)\rangle$.

LEMMA 2.4. Let F be a field and let $p(x), f(x), g(x) \in F[x]$ such that $\deg f(x) < \deg p(x)$ and $\deg g(x) < \deg p(x)$. If $f(x) + \langle p(x)\rangle = g(x) + \langle p(x)\rangle$ then $f(x) = g(x)$.

PROOF. Let F be a field and let $p(x), f(x), g(x) \in F[x]$ such that $\deg f(x) < \deg p(x)$ and $\deg g(x) < \deg p(x)$. Assume that $f(x) + \langle p(x)\rangle = g(x) + \langle p(x)\rangle$. Since $\deg f(x), \deg g(x) < \deg p(x)$, there is nothing for $\langle p(x)\rangle$ to absorb. This suggest that

$$f(x) + \langle p(x)\rangle = a_n x^n + \cdots a_1 x + a_0 + \langle p(x)\rangle$$

where $a_i \in F$ and $a_n \neq 0$. Similarly,

$$g(x) + \langle p(x)\rangle = b_m x^m + \cdots b_1 x + b_0 + \langle p(x)\rangle$$

where $b_i \in F$ and $b_m \neq 0$. Combining the equations yields,

$$a_n x^n + \cdots a_1 x + a_0 + \langle p(x)\rangle = b_m x^m + \cdots b_1 x + b_0 + \langle p(x)\rangle$$

which implies that $n = m$ and $a_i = b_i$. Thus, $f(x) = g(x)$. □

LEMMA 2.5. Let F be a field and let $p(x)$ be irreducible over F. If E is a field that contains F and there is an element a in E such that $p(a) = 0$, then the map $\phi : F[x] \to E$ given by $\phi(f(x)) = f(a)$ is a ring homomorphism with kernel, $\langle p(x) \rangle$.

PROOF. Let F be a field and let $p(x)$ be irreducible over F. Assume that $E \supset F$ and that there exists $a \in E$ such that $p(a) = 0$. Let $\phi : F[x] \to E$ be given by $\phi(f(x)) = f(a)$. Let $f(x), g(x) \in F[x]$.

First, we will show that ϕ preserves addition. Clearly,

$$\phi(f(x) + g(x)) = f(a) + g(a).$$

Second, we will show that ϕ preserves multiplication. Consider

$$\begin{aligned}
\phi(f(a)g(a)) &= \phi(c_n b_m x^{n+m} + \cdots + c_0 b_0) \\
&= c_n b_m a^{n+m} + \cdots + c_0 b_0 \\
&= (c_n a^n + \cdots + c_0)(b_n a^m + \cdots b_0) \\
&= \phi(f(a)) + \phi(g(a).
\end{aligned}$$

Therefore, $\phi : F[x] \to E$ is a ring homomorphism.

Now, let $f(x) \in \langle p(x) \rangle$. By definition, $f(x) = h(x)p(x)$ for some $h(x) \in F[x]$. Consider

$$\begin{aligned} \phi(f(x)) &= \phi(h(x)p(x)) \\ &= h(a)p(a) \\ &= h(a)0 \\ &= 0 \end{aligned}$$

Thus, $\langle p(x) \rangle$ is the kernel of ϕ and the lemma has been shown. □

THEOREM 2.8. Let F be a field and let $p(x) \in F[x]$ be irreducible over F. If a is a zero of $p(x)$ in some extension E of F, then $F(a)$ is isomorphic to $F[x]/\langle p(x) \rangle$. Furthermore, if $\deg p(x) = n$, then every member of $F(a)$ can be uniquely expressed in the form

$$c_{n-1}a^{n-1} + cn - 2a^{n-2} + \cdots + c_1 a + c_0$$

where $c_0, \ldots, c_{n-1} \in F$.

PROOF. Let F be a field and let $p(x) \in F[x]$ be irreducible over F. Assume that a is a zero of $p(x)$ in some extension E of F. Let $\phi : F[x] \to F(a)$. By Lemma 2.5, we know that $\langle p(x) \rangle \subset \ker \phi$. By Theorem 2.5, we know that $\langle p(x) \rangle$ is a maximal ideal of $F[x]$. In other words, $\ker \phi$ is either $\langle p(x) \rangle$ or $F[x]$. Notice that $1 \notin \ker \phi$ by

Lemma 2.3. This implies that $\ker \phi \neq F[x]$. Therefore, $\ker \phi = \langle p(x) \rangle$. Thus, by the First Isomorphism Theorem for Rings, we have that $F[x]/\langle p(x) \rangle \cong \phi(F[x])$. Notice that $\phi(F[x])$ contains all of F and the element a. The smallest such field is $F(a)$, therefore, by Corollary 2.5.1 $F[x]/\langle p(x) \rangle \cong F(a)$.

By Lemma 2.4, we know that the typical element in $F[x]/\langle p(x) \rangle$ is uniquely given by

$$c_{n-1}x^{n-1} + cn - 2x^{n-2} + \cdots + c_1 x + c_0 + \langle p(x) \rangle$$

where $c_i \in F$. Notice that the isomorphism ϕ takes $c_i x^i + \langle p(x) \rangle$ to $c_i a^i$. Thus, the theorem has been shown. □

Theorem 2.8 gives us the last result we need to explain why $x^2 + 1$ has two zeros over $\mathbb{C}$. To summarize, we have shown that every polynomial has a splitting field over which it has as many zeros as its degree. Using field extensions, we can find splitting fields and identify their elements. In particular, the splitting field for a polynomial $p(x)$ where $p(x)$ is irreducible over F is $F(a_1, \ldots, a_n)$, the field of polynomials with coefficients in F over the variables $a_1, \ldots, a_n$.

4. Algebraic Extensions

DEFINITION 2.14. Let E be an extension field of a field F and let $a \in E$. We call a *algebraic over* F if a is the zero for some nonzero polynomial in $F[x]$. If a is not algebraic over F, it is called *transcendental over* F. Similarly, an extension E of F is called *algebraic* extension of F if every element of E is algebraic over F. If E is not an algebraic extension of F, it is called a *transcendental* extension of F. An extension of F of the form $F(a)$ is called a simple extension of F.

THEOREM 2.9. Let E be an extension field of F and let $a \in E$. If a is transcendental over F, then $F(a) \cong F(x)$. If a is algebraic over F, then $F(a) \cong F[x]/\langle p(x)\rangle$, were $p(x)$ is a polynomial in $F[x]$ of minimum degree such that $p(a) = 0$. Moreover, $p(x)$ is irreducible over F.

PROOF. Let E be an extension field of F and let $a \in E$. Let $\phi : F[x] \to E$ be given by $\phi(f(x)) = f(a)$.

Assume that a is transcendental over F. By definition of transcendental, $f(a) \neq 0$ for all nonzero polynomials in $F[x]$. This implies that $\ker \phi = \{0\}$. Therefore, we can define an isomorphism $\phi' : F(x) \to F(a)$ where

$$\phi\left(\frac{f(x)}{g(x)}\right) = \frac{f(a)}{g(a)}$$

Assume that a is algebraic over F. By definition of algebraic, $f(a) = 0$ for some $f(x) \in F[x]$. This suggests that $\ker \phi \neq \{0\}$. There are two cases: either $f(x)$ is irreducible over F, or it is not.

Case I: Let $f(x)$ be irreducible over F. Then $\langle f(x) \rangle$ is a maximal ideal of $F[x]$ and $\langle f(x) \rangle = \ker \phi$. By the First Isomorphism Theorem, $\phi' : F[x]/\langle f(x) \rangle \to F(a)$ given by $\phi'(f(x) + \langle f(x) \rangle) \to f(a)$ is an isomorphism. Furthermore, notice that if $f(x)$ wasn't of minimum degree such that $f(a) = 0$, then $\langle f(x) \rangle$ would not be maximal.

Case II: Let $f(x)$ be reducible over $F[x]$. By definition, there exists $g(x), h(x) \in F[x]$ such that $f(x) = g(x)h(x)$ and $\deg f(x) > \deg g(x), \deg h(x) \geq 1$. Since F is a field, either $g(a) = 0$ or $h(a) = 0$. Without loss of generality, we may assume that $g(a) = 0$. Notice that if $g(x)$ is irreducible, then we are done by **Case I**. Otherwise, we may repeat the arguments of **Case II**. Notice this process must bottom out because we are every time we factor $f(x)$ (or $g(x)$), we are reducing the degree of the polynomial we are considering. Thus, we are done with this case.

Therefore, all statements of the theorem have been proven. □

THEOREM 2.10. If a is algebraic over a field F, then there is a unique monic irreducible polynomial $p(x)$ in $F[x]$ such that $p(x) = 0$.

PROOF. Assume that a is algebraic over a field F. By Theorem 2.9, there exists an irreducible polynomial of minimal degree, $p(x) \in F[x]$ such that $p(a) = 0$. Let b be the leading coefficient of $p(x)$. Since F is a field, there exists an element $b^{-1} \in F[x]$. The polynomial $b^{-1}p(x)$ is monic and unique by construction. □

THEOREM 2.11. Let a be algebraic over F, and let $p(x)$ be the minimal polynomial for a over F. If $f(x) \in F[x]$ and $f(a) = 0$, then $p(x)$ divides $f(x)$ in $F[x]$.

PROOF. Let a be algebraic over F, and let $p(x)$ be the minimal polynomial for a over F. By Theorem 2.10, $p(x)$ is unique. Assume that $f(x) \in F[a]$ and $f(a) = 0$. Recall ϕ from the proof of Theorem 2.9. We apply this theorem to $p(x)$ to get that, $\langle p(x) \rangle$ is the kernel of ϕ. Since $f(a) = 0$, $f(a) \in \langle p(x) \rangle$. By definition of ideal, there exists $g(x) \in F[x]$ such that $g(x)p(x) = f(x)$. Therefore, $p(x)$ divides $f(x)$ by definition. □

5. Cyclotomic Fields

Irreducible polynomials aren't the only polynomials that don't have as many zeros as their degree. In particular, if a polynomial has an irreducible factor, then it will not have as many zeros as its degree. In section 1 we saw an example of this kind of polynomial, namely $x^n - 1$.

In fact, this is an entire family of polynomials that don't have n zeros over $\mathbb{Q}$.

DEFINITION 2.15. The irreducible factors of $x^n - 1$ over $\mathbb{Q}$ are called the cyclotomic polynomials.

From complex analysis we know that the complex zeros of the polynomial $x^n - 1$ are $\langle e^{\imath \frac{2\pi}{n}} \rangle = \{1, e^{\imath \frac{2\pi}{n}}, e^{\imath \frac{4\pi}{n}}, e^{\imath \frac{6\pi}{n}}, \ldots, e^{\imath \frac{(n-1)2\pi}{n}}\}$. In other words $\mathbb{Q}(e^{\imath \frac{2\pi}{n}})$ is the splitting field for $x^n - 1$ over $\mathbb{Q}$. Any generator of the cyclic group $\langle e^{\imath \frac{2\pi}{n}} \rangle$ is called a primitive nth root of unity. In particular, $e^{\imath k \frac{2\pi}{n}}$ where k is relatively prime to n is a generator of $\langle e^{\imath \frac{2\pi}{n}} \rangle$. Let $\phi(n)$ denote the number of integers $0 < k < n$ such that k and n are relatively prime.

DEFINITION 2.16. We can then define the nth cyclotomic polynomial as the polynomial $\Phi_n = (x - \omega_1)(x - \omega_2) \cdots (x - \omega_{\phi(n)})$ where ω_i are the nth primitive roots of unity.

Notice that the nth cyclotomic polynomial is monic. That is, the leading coefficient is 1. Since we are interested in cyclotomic field extensions over $\mathbb{Q}$, we need to show that the cyclotomic polynomials are irreducible over $\mathbb{Q}$. First, we will show that the pth cyclotomic polynomial where p is prime is irreducible over $\mathbb{Q}$. This result is actually a corollary of Eisenstein's Criterion for irreducibility.

THEOREM 2.12 (Eisenstein's Criterion (1850)). Let

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$$

If there is a prime p such that $p \not| a_n, p|a_{n-1}, \ldots, p|a_0$ and $p^2 \not| a_0$, then $f(x)$ is irreducible over $\mathbb{Q}$.

PROOF. Let

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$$

Assume that there exists a prime p such that $p \not| a_n, p|a_{n-1}, \ldots, p|a_0$ and $p^2 \not| a_0$. We will proceed by contradiction. Assume that $f(x)$ is reducible over $\mathbb{Q}$. Let $\deg f(x) = n$. It is a fact that if a polynomial is reducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$. Therefore, there exists $g(x), h(x) \in \mathbb{Z}[x]$ such that

$$f(x) = g(x)h(x)$$

and $1 \leq \deg g(x), \deg h(x) < n$. Let

$$g(x) = b_r x^r + \cdots + b_0$$

and

$$h(x) = c_s x^s + \cdots + c_0.$$

By assumption $p|a_0$ but $p^2 \not| a_0$. Furthermore, $a_0 = b_0 c_0$. This implies that p can divide at most b_0 or c_0 but not both. Without loss of

generality, assume that $p|b_0$ but $p \not| c_0$. Notice that $p \not| a_n = b_r c_s$ implies that $p \not| b_r$. Let t be the least integer such that $p \not| b_t$. Now consider,

$$a_t = b_t c_0 + b_{t-1} c_1 + \cdots + b_0 c_t$$

Since, $p|b_i$ for $t \geq i \geq 0$, we know that $p|a_t$. In particular, $p|b_t c_0$ which is a contradiction because we assumed that $p \not| b_t$ and $p \not| c_0$. Thus, the theorem is shown. □

COROLLARY 2.12.1. For any prime p, the pth cyclotomic polynomial

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

is irreducible over $\mathbb{Q}$.

PROOF. Consider

$$f(x) = \Phi_p(x+1) = \frac{(x+1)^p - 1}{x + 1 - 1} = (x)^{p-1} + \binom{p}{1}(x)^{p-2} + \cdots + \binom{p}{2}x + \binom{p}{1}$$

Notice, that by Theorem 2.12 $f(x)$ is irreducible over $\mathbb{Q}$. For the sake of contradiction, assume that $\Phi_p(x)$ is reducible over $\mathbb{Q}$. By definition of reducible, there exists $g(x), h(x) \in \mathbb{Q}[x]$ such that $\Phi_p(x) = g(x)h(x)$. However, this implies that $\Phi_p(x+1) = g(x+1)h(x+1)$ would also be a nontrivial factorization of $f(x)$ over $\mathbb{Q}$. This is a contradiction. Therefore, $\Phi_p(x)$ is irreducible over $\mathbb{Q}$. □

We would like to show that the nth cyclotomic polynomial is irreducible over $\mathbb{Q}$ even when n is not prime. To show that the nth cyclotomic polynomial is irreducible over $\mathbb{Q}$, we will show that it is irreducible over $\mathbb{Z}$. For the nth cyclotomic polynomial to be irreducible over $\mathbb{Z}$ it must have coefficients in $\mathbb{Z}$. The proof for this requires induction on n. Since induction on n is nicer for $x^n - 1$ than the nth cyclotomic polynomial, we will relate the former to the latter with the following theorem.

THEOREM 2.13. For every positive integer n, $x^n - 1 = \prod_{d|n} \Phi_d(x)$, where the product runs over all positive divisors d of n.

PROOF. Let n be a positive integer. Notice that both $x^n - 1$ and $\prod_{d|n} \Phi_d(x)$ are monic. That means it suffices to show that both polynomials have the same zeros with the same multiplicity. Let $\omega = e^{\imath \frac{2\pi}{n}}$. By Lagrange's theorem, we know that for all j, $|\omega^j|$ divides $|\langle\omega\rangle| = n$. This implies that $(x-\omega^j)$ is a zero of $\Phi_{|\omega^j|}(x)$. This shows that $(x-\omega^j)$ is a factor for $\prod_{d|n} \Phi_d(x)$, where j is arbitrary. In other words, if $x - \alpha$ is a linear factor of $x^n - 1$, then $x - \alpha$ is a linear factor of $\prod_{d|n} \Phi_d(x)$.

Now, let $d|n$. Assume that $x - \alpha$ is a linear factor of $\Phi_d(x)$. This implies that $\alpha \in \langle\omega\rangle$. Therefore, $\alpha^d = 1$ and $\alpha^n = 1$. Thus, $x - \alpha$ is a

linear factor of $x^n - 1$. That is, every linear factor of $\prod_{d|n} \Phi_d(x)$ is a linear factor of $x^n - 1$. □

Notice that $x^n - 1$ has integer coefficients. So far we know don't much about $\prod_{d|n}$ and $\Phi_d(x)$ except that they are both monic. This leaves open the possibility for $\prod_{d|n}$ and $\Phi_d(x)$ to have rational coefficients. The following lemma shows why this is not the case.

LEMMA 2.6. Let $g(x)$ and $h(x)$ belong to $\mathbb{Z}[x]$ and let $h(x)$ be monic. If $h(x)$ divides $g(x)$ in $\mathbb{Q}[x]$, then $h(x)$ divides $g(x)$ in $\mathbb{Z}[x]$.

PROOF. Let $g(x), h(x) \in \mathbb{Z}[x]$ such that $h(x)$ is monic. Assume that $h(x)$ divides $g(x)$ in $\mathbb{Q}[x]$. By the division algorithm in polynomial rings, this implies that there exists $q(x) \in \mathbb{Q}[x]$ such that $q(x)h(x) = g(x)$. Let $m = \deg q(x)$ and $n = \deg h(x)$. By the degree rule, $m + n = \deg g(x)$. Let g_i, h_i, q_i denote the coefficient of the ith term in $g(x), h(x)$, and $q(x)$ respectively. By the polynomial ring multiplication,

$$g_i = \sum_{\substack{0 \le l \le n \\ 0 \le k \le m \\ l + k = i}} h_l q_k$$

for all $0 \leq i \leq m+n$. We are going to show that q_{m-t} is an integer by induction on t from 0 to m.

Base Case: Consider $t = 0$. We know that $g_{n+m} = h_n q_m$. Since $h_n = 1$, we know that q_m is an integer.

Induction Hypothesis: For all $t < T$, we know that q_{m-t} is an integer.

Induction Step: Consider

$$g_{n+m-(T+1)} = h_n q_{m-(T+1)} + h_{n-1} q_{m-T} + \cdots + h_{n-(T+1)} q_m$$

Note that $h_i = 0$ where $i < 0$. Since all variables in this equation except $q_{m-(T+1)}$ are integers by the induction hypothesis and $h_n = 1$, $q_{m-(T+1)}$ must be an integer. This concludes the proof of the lemma. □

Theorem 2.13 and Lemma 2.6 round out the relationship $x^n - 1 = \prod_{d|n} \Phi_d(x)$. In particular, if any $\Phi_d(x)$ is monic then the others cyclotomic polynomials have integer coefficients. This paves the way for an induction proof for the next theorem.

THEOREM 2.14. For every positive integer n, $\Phi_n(x)$ has integer coefficients.

PROOF. We are going to prove the theorem by induction on n.

Base Case: Consider $\Phi_1(x) = x - 1$. Clearly, $\Phi_1(x)$ only has integer coefficients.

Induction Hypothesis: Assume that for all $n \leq N$, $\Phi_n(x)$ has integer coefficients.

Induction Step: Let $g(x) = \prod_{d|n, d<n} \Phi_d(x)$. Consider

$$x^{N+1} - 1 = \Phi_{N+1} g(x)$$

Since $g(x)$ is monic, we know that Φ_{N+1} has integer coefficients by Lemma 2.6. This concludes the proof of this theorem. □

Now that we know that the *nth* cyclotomic polynomials are elements in $\mathbb{Z}[x]$ it makes sense to ask whether or not they are irreducible over $\mathbb{Z}$. Showing that the *nth* cyclotomic polynomials are irreducible over $\mathbb{Z}$ is actually a stronger theorem than what I want for my thesis. I just care whether they are irreducible over $\mathbb{Q}$. However, Gauss's proof for the irreducibility of the cylotomic polynomials over $\mathbb{Z}$ ties together many of the ideas in Chapter 1. Furthermore, it is by far the craziest proof I have seen in any class at Bates. I think both are compelling reasons to take a look at it. The irreducibility of the cyclotomic polynomials over $\mathbb{Q}$ is a corollary.

THEOREM 2.15. The cyclotomic polynomials $\Phi_n(x)$ are irreducible over $\mathbb{Z}$.

PROOF. Let $f(x) \in \mathbb{Z}[x]$ be a monic irreducible factor of $\Phi_n(x)$. Since $\Phi_n(x)$ is monic and does not have multiple zeros, if all of the zeros of $\Phi_n(x)$ are zeros of $f(x)$, then $\Phi_n(x) = f(x)$ and $\Phi_n(x)$ is irreducible over $\mathbb{Z}$.

Since $\Phi_n(x)$ divides $x^n - 1$ in $\mathbb{Z}[x]$ by definition, and $f(x)$ is a factor of $\Phi_n(x)$, we can write

$$x^n - 1 = f(x)g(x)$$

for some $g(x) \in \mathbb{Z}[x]$. Let ω be an nth root of unity that is a zero of $f(x)$. Since $f(x)$ is irreducible over $\mathbb{Z}$, $f(x)$ is irreducible over $\mathbb{Q}$. This implies that $f(x)$ is a minimal polynomial for ω over $\mathbb{Q}$. Let p be a prime that does not divide n. Since $p \not| n$ we know that ω^p is a generator of $\langle\omega\rangle$ and thus a primitive root of unity. Therefore, by definition

$$0 = (\omega^p)^n - 1 = f(\omega^p)g(\omega^p).$$

Since $\mathbb{Z}[x]$ is an integral domain $f(\omega^p) = 0$ or $g(\omega^p) = 0$.

For the sake of contradiction, assume that $f(\omega^p) \neq 0$. Then $g(\omega^p) = 0$, and ω is a zero of $g(x^p)$. By Theorem 2.11, $f(x)$ divides $g(x^p)$ in $\mathbb{Q}[x]$. Now, by Lemma 2.6 we know that $f(x)$ divides $g(x^p)$ in $\mathbb{Z}[x]$. In particular, $g(x^p) = f(x)h(x)$ for some $h(x) \in \mathbb{Z}[x]$. Let $\bar{g}(x), \bar{f}(x), \bar{h}(x) \in \mathbb{Z}_p[x]$ be obtained by reducing $g(x), f(x), h(x)$ by

modulo p respectively. Notice that $\psi : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ is a ring homomorphism. This implies that $\bar{g}(x) = \bar{f}(x)\bar{h}(x)$ in $\mathbb{Z}_p[x]$. By Fermat's Little Theorem, we have that

$$(\bar{g}(x))^p = \bar{g}(x^p) = \bar{f}(x)\bar{h}(x).$$

Since $\mathbb{Z}_p[x]$ is a unique factorization domain, $\bar{f}(x)$ and $\bar{g}(x)$ are irreducible and have a factor in common. Therefore, we have

$$\bar{f}(x) = k_1(x)m(x)$$

and

$$\bar{g}(x) = k_2(x)m(x)$$

where $k_1(x), k_2(x) \in Z_p[x]$. We can use these equalities to write

$$x^n - 1 = k_1(x)k_2(x)m(x)^2$$

in $\mathbb{Z}_p[x]$. However, this suggests that $x^n - 1$ has multiple zeros in some extension over $\mathbb{Z}_p[x]$. Consider nx^{n-1} the derivative of $x^n - 1$. By the multiple zeros criterion, $x^n - 1$ has multiple zeros if and only if nx^{n-1} and $x^n - 1$ have a factor of positive degree in common in $\mathbb{Z}_p[x]$. Since $p \not| n$, we know that nx^{n-1} does not reduce to zero in $\mathbb{Z}_p[x]$. Furthermore, $\mathbb{Z}_p$ does not have any zero divisors, so nx^{n-1} and $x^n - 1$ cannot share a factor of positive degree. This implies that $x^n - 1$ cannot have multiple zeros, which is a contradiction. Therefore, $f(\omega^p) = 0$.

Thus, if ω is a primitive root of unity and $f(\omega) = 0$, then $f(\omega^p) = 0$ where p is prime and $p \nmid n$.

Let $1 < k < n$ be relatively prime to n. Let $k = p_1 p_2 \cdots p_t$. Since k and n are relatively prime $p_i \nmid n$. Therefore, $\omega, \omega^{p_1}, \omega^{p_1 p_2}, \ldots, \omega^k$ are zeros of $f(x)$. Notice that every zero of $\Phi_n(x)$ is of the form ω^k, where $1 < k < n$ and k is relatively prime to n. Therefore, every zero of $\Phi_n(x)$ is a zero of $f(x)$. Thus, $\Phi_n(x) = f(x)$ which was assumed to be irreducible over $\mathbb{Z}$. □

COROLLARY 2.15.1. The cyclotomic polynomials $\Phi_n(x)$ are irreducible over $\mathbb{Q}$.

PROOF. It is a fact that if a polynomial is reducible over $\mathbb{Z}$, then it is reducible over $\mathbb{Q}$. Therefore, the corollary easily follows from Theorem 2.15. □

The upshot of all of these theorems is that there is a special family of fields called the cyclotomic field extensions over $\mathbb{Q}$. In particular, the *nth* cyclotomic field is the smallest field that contains all the rational numbers and the *nth* roots of unity. By finding cyclotomic fields, we begin to see how we can build the complex numbers out of the rationals. Though this is not a formal treatment of the matter, I picture the

solution being something like this:

$$\mathbb{Q} \subset \mathbb{Q}(\omega_n) \subset \mathbb{Q}(\omega_{2n}) \subset \mathbb{C}$$

where ω_n a primitive nth root of unity, for all $n \in \mathbb{N}$. In this relation, we see that even though the degree of $\mathbb{Q}(\omega_n)$ and $\mathbb{Q}(\omega_{2n})$ is the same, the former is a "smaller" subset of the complex numbers.

6. Quadratic Number Fields

DEFINITION 2.17. Let $p(x) = x^2+m$ be an element in $\mathbb{Q}[x]$ where m is not a perfect square in $\mathbb{Z}$. Then $\mathbb{Q}[x]/\langle p(x)\rangle \cong \mathbb{Q}(\sqrt{m})$ is a quadratic field extension over $\mathbb{Q}$. If $m > 0$, $\mathbb{Q}(\sqrt{m})$ is called a *real* quadratic field extension. If $m < 0$, then $\mathbb{Q}(\sqrt{m})$ is called an *imaginary* quadratic field extension.

THEOREM 2.16. Let $p^2|m$ for some $p, m \in \mathbb{Z}$, where p is not a unit. Then $\mathbb{Q}(\sqrt{m'}) = \mathbb{Q}(\sqrt{m})$ where $p^2m' = m$.

PROOF. Let $p^2|m$ for some $p, m \in \mathbb{Z}$, where p is not a unit. Consider $\mathbb{Q}(\sqrt{m})$. Notice that $\sqrt{m} = p\sqrt{m'}$ where $p^2m' = m$. Therefore, $\mathbb{Q}(\sqrt{m}) \subseteq \mathbb{Q}(\sqrt{m'})$. Let $a + b\sqrt{m'}$ be some element in $\mathbb{Q}(\sqrt{m'})$. Consider the element $\frac{b^{-1}a}{p} + \sqrt{m} \in \mathbb{Q}(\sqrt{m'})$. We know that $\frac{b^{-1}a}{p} + \sqrt{m} = \frac{b^{-1}ap}{p} + p\sqrt{m'}$ and that $\frac{b}{p} \in \mathbb{Q}(\sqrt{m})$. Therefore,

$$\frac{b}{p}(\frac{b^{-1}ap}{p} + p\sqrt{m'}) = a + b\sqrt{m'} \in \mathbb{Q}(\sqrt{m})$$

Thus, $\mathbb{Q}(\sqrt{m}) \supseteq \mathbb{Q}(\sqrt{m'})$, concluding the proof. □

Recall the definition of a prime ideal.

DEFINITION 2.18. A *prime ideal* A of a commutative ring R is a proper ideal of R such that $a, b \in R$ and $ab \in A$ implies that $a \in A$ or $b \in A$.

This is similar to the definition of a prime element.

DEFINITION 2.19. Let a, b, c be elements of an integral domain D. Then we say that a is prime if a is not a unit and $a|bc$ implies either $a|b$ or $a|c$.

In fact, an ideal $\langle a \rangle$ is prime if and only if a is prime. Notice that $\langle x^2 + m \rangle$ is a prime ideal of $\mathbb{Q}[x]$ when $m \in \mathbb{Z}$ is square free. Therefore, $x^2 + m$ is prime in $\mathbb{Q}[x]$. Furthermore, $x^2 + m$ is irreducible in $\mathbb{Q}[x]$ by Theorem 2.12. This implies that $\langle x^2 + m \rangle$ is maximal, allowing us to consider the field $Q[x]/\langle x^2 + m \rangle \cong \mathbb{Q}(\sqrt{m})$. However, notice that $y^2 + m$ (indeterminate y) has a zero in $\mathbb{Q}[x]/\langle x^2 + m \rangle$, and therefore, has a factor; namely $x + \langle x^2 + m \rangle$. Alternatively, we can say that $y^2 + m$ has $y - \sqrt{-m}$ and $y + \sqrt{-m}$ as factors. This suggests that $y^2 + m$ is no longer prime in $\mathbb{Q}(\sqrt{m})$. Now it is interesting to ask which elements are prime in $\mathbb{Q}(\sqrt{m})$. As it turns out the answer depends on m.

DEFINITION 2.20. A complex number is an algebraic integer if and only if it is the root of some monic polynomial with coefficients in $\mathbb{Z}$.

LEMMA 2.7. Let $f(x)$ be a monic polynomial with coefficients in $\mathbb{Z}$, and suppose $f(x) = g(x)h(x)$ where $g(x)$ and $h(x)$ are monic polynomials with coefficients in $\mathbb{Q}$. Then $g(x), h(x) \in \mathbb{Z}[x]$.

Notice that Lemma 2.7 is similar to a lemma we used in a previous section. For a detailed proof of it, refer to page 14 in [**3**].

THEOREM 2.17. Let α be an algebraic integer and let $f(x)$ be a monic polynomial over $\mathbb{Z}$ of least degree having α as a root. Then $f(x)$ is irreducible over $\mathbb{Q}$.

PROOF. Let α be an algebraic integer and let $f(x)$ be a monic polynomial over $\mathbb{Z}$ of least degree such that $f(\alpha) = 0$. If $\deg f(x) = 1$ then we are done. Therefore, let $\deg f(x) \geq 2$. For the sake of contradiction, assume that $f(x)$ is reducible in $\mathbb{Q}[x]$. By definition of irreducible, there exist $g(x), h(x) \in \mathbb{Q}[x]$ such that $f(x) = g(x)h(x)$ where $g(x)$ and $h(x)$ are not units. Since $f(x)$ is monic, the product of the leading coefficients of $g(x)$ and $h(x)$ must be one. We can scale both $g(x)$ and $h(x)$ to make both of them monic. By Lemma 2.7, $g(x)$ and $h(x)$ have coefficients in $\mathbb{Z}$. Notice that either $g(\alpha) = 0$ or $h(\alpha) = 0$. In either case, we have a contradiction because we assumed that $f(x)$ is

a least degree polynomial over $\mathbb{Z}$ such that $f(\alpha) = 0$. Therefore, $f(x)$ is irreducible over $\mathbb{Q}$. □

COROLLARY 2.17.1. Let m be a squarefree integer. The set of algebraic integers in the quadratic field $\mathbb{Q}(\sqrt{m})$ is

$$\{a + b\sqrt{m} : a, b \in \mathbb{Z}\} \text{ if } m \equiv 2 \text{ or } 3 \mod 4$$

$$\{\frac{a + b\sqrt{m}}{2} : a, b \in \mathbb{Z}, a \equiv b \mod 2\} \text{ if } m \equiv 1 \mod 4$$

PROOF. Let m be a squarefree integer. Let $r + s\sqrt{m} \in \mathbb{Q}(\sqrt{m})$. We want to find the conditions under which $r + s\sqrt{m}$ is an algebraic integer in $\mathbb{Q}(\sqrt{m})$. If $s \neq 0$ then $p(x) = x^2 - rx + r^2 - ms^2$ is the monic irreducible polynomial over $\mathbb{Z}$. In particular

$$\begin{aligned} p(r + s\sqrt{m}) &= (r + s\sqrt{m})^2 - 2r(r + s\sqrt{m}) + r^2 - ms^2 \\ &= r^2 + s^2m + 2rs\sqrt{m} - 2r^2 - 2rs\sqrt{m} + r^2 - ms^2 \\ &= 0 \end{aligned}$$

Notice that $r + s\sqrt{m}$ is algebraic if and only if it is a zero for a polynomial with coefficients in $\mathbb{Z}$. In other words, $r + s\sqrt{m}$ is algebraic if $-2r \in \mathbb{Z}$ and $r^2 - ms^2 \in \mathbb{Z}$. In order to find possible algebraic integers, we will assume that $-2r \in \mathbb{Z}$ and $r^2 - ms^2 \in \mathbb{Z}$. There are two cases, either $m \equiv 2$ or $3 \mod 4$, or $m \equiv 1 \mod 4$. Notice that if $m \equiv 0 \mod 4$ then m would not be squarefree.

Case I: Assume that $m \equiv 2 \text{ or } 3 \mod 4$. Notice that if $r \in \mathbb{Z}$, then $ms^2 \in \mathbb{Z}$. Since m is squarefree, $s \in \mathbb{Z}$. However, r could equal $\frac{k}{2}$ where $2 \nmid k$. This implies that $\frac{k^2}{4} = ms^2$. Since $2 \nmid k$, we know that $k^2 \equiv 1 \mod 4$. Therefore s^2 must be of the form $\frac{p^2}{4}$. Now the equality

$$\frac{k^2}{4} = \frac{mp^2}{4}$$

only holds if $k^2 \equiv mp^2 \mod 4$. However, $mp^2 \not\equiv 1 \mod 4$. Therefore, r cannot be of the from $\frac{k}{2}$ where $2 \nmid k$. The conclusion of Case I is that if $m \equiv 2 \text{ or } 3 \mod 4$, then the set

$$\{a + b\sqrt{m} : a, b \in \mathbb{Z}\}$$

consists of the algebraic integers of $\mathbb{Q}(\sqrt{m})$.

Case II: Assume that $m \equiv 1 \mod 4$. First, assume that $r \in \mathbb{Z}$. Then $ms^2 \in \mathbb{Z}$. As in Case I, this implies that $s \in \mathbb{Z}$ Second, assume that $\frac{k}{2}$ where $2 \nmid k$. This implies that $\frac{k^2}{4} = ms^2$. Since $m \equiv 1 \mod 4$, this equation is satisfied any time $s = \frac{p}{2}$ where $2 \nmid p$. The result of Case II is that if $m \equiv 1 \mod 4$, then

$$\{\frac{a + b\sqrt{m}}{2} : a, b \in \mathbb{Z}, a \equiv b \mod 2\}$$

consists of the algebraic integers of $\mathbb{Q}(\sqrt{m})$. $\square$

The ring of algebraic integers is closed, and essentially forms the set of primes in the corresponding quadratic field extension. With this in mind, we have a special interest in these rings.

CHAPTER 3

Origami Rings

In origami, the artist uses intersections of folds as reference points to make new folds. This kind of construction can be extended to points on the complex plane. That is, given a set of reference points and a set of lines we can fold along, we can construct new reference points by adding intersections of lines to our set of reference points. This chapter formalizes the notion of an origami construction, and presents known results. All of the work in this chapter is attributed to [**1**], however, the proofs have been rewritten in my own words and some details have been filled in. I created all of the images myself. The only images containing my own work and interpretation are in section 3.

1. Definitions and Notation

We will denote the seed set of our construction as $S \subset \mathbb{C}$. Let $\mathbb{T} \subset \mathbb{C}$ be the set of points on the unit cicle in the complex plane. We let $U \subset \mathbb{T}$ be a set denoting the lines or folds we get to use. The angle between the line containing 0 and $u \in U$ and a the line containing 0 and 1 is the angle along which we may fold. To be more precise, we

can start a fold at any point we have constructed (or from our seed set) and fold along the angle as given by u in the previously stated way.

To formalize what we have just introduced, we can write a line or fold as

$$L_u(p) = \{p + ru | r \in \mathbb{R}\}$$

where p has been constructed or is in S, and u is the angle given by $u \in U$. Here it might be best to think of u as a vector. The intersections and, therefore, new points can be written as

$$I_{u,v}(p, q) = L_u(p) \cap L_v(q)$$

where p, q have been constructed or are in S and u, v are the angles given by $u, v \in U$. Notice that $I_{u,v}(p, q)$ is in essence a point on the complex plane defined by two other points and lines going through them.

DEFINITION 3.1. We let $R(S, U)$ denote the smallest subset of points in $\mathbb{C}$ containing S such that $R(S, U)$ is closed under $I_{v,u}(p, q)$ for $u, v \in U$ and $p, q \in R(S, U)$.

2. Properties of Intersections

Let $S = \{0, 1\}$ and $U \subset \mathbb{T}$. Notice that we have defined a particular seed set. We have chosen this particular seed set because $0, 1$ are nice

elements to have in rings. We will assume that $S = \{0, 1\}$ unless otherwise noted. Furthermore, we will assume that U is a group. There are interesting properties of the $I_{u,v}(p, q)$ operator that are integral for us to prove more theorems about $R(S, U)$. However, before we get into proving the properties of $I_{u,v}(p, q)$ we will express this point algebraically.

Let $u, v \in U$ be two distinct angles. Let p, q be points in $R(S, U)$. Consider the pair of intersecting lines $L_u(p)$ and $L_v(q)$. By definition of these sets, we can express $I_{u,v}(p, q)$ as the point satisfying the equation

$$p + ru = q + sv \tag{3.1}$$

where $r, s \in \mathbb{R}$. By doing some algebra, we can rewrite equation 3.1 as follows:

$$p + ru = q + sv \tag{3.2}$$

$$p + ru - q = sv \tag{3.3}$$

$$v^{-1}(p + ru - q) = s \tag{3.4}$$

Notice that we have v^{-1} in equation 3.4. Recall that we assumed that U is a group, v must have an inverse, v^{-1}. We will also let $v^{-1} = 1/v$.

Since we know that $s \in \mathbb{R}$, we know that $\Im(s) = 0$, where $\Im(x)$ is the imaginary component of x. If we apply $\Im(x)$ to both sides of equation 3.4 and solve for r as follows:

$$0 = \Im(v^{-1}(p + ru - q)) \tag{3.5}$$

$$0 = \Im((p - q)/v) + \Im(ru/v) \tag{3.6}$$

$$\Im(ru/v) = \Im((p - q)/v) \tag{3.7}$$

Since $r \in \mathbb{R}$ we have $\Im(ru/v) = r\Im(u/v)$. We can substitute this back into equation 3.7 and isolate r to get

$$r = \frac{\Im((p - q)/v)}{\Im(u/v)} \tag{3.8}$$

For the sake of simplifying equation 3.8 we will introduce the following notation:

$$[x, y] = x\bar{y} - \bar{x}y = 2i|y|^2\Im(x/y) \tag{3.9}$$

At first, we will be most interested in the part of the equality that contains the $\Im(z)$ operator. Notice that both the top and the bottom parts of the fraction in equation 3.8 are of the form $\Im(x/y)$. More particularly, v is in the denominator inside both $\Im(z)$ operators. This allows us to multiply the left hand side of equation 3.8 by

$$\frac{2\imath|v|^2}{2\imath|v|^2} = 1$$

to get

$$r = \frac{2\imath|v|^2\Im((p-q)/v)}{2\imath|v|^2\Im(u/v)} \tag{3.10}$$

Now we actually apply equation 3.9 to equation 3.10 to get

$$r = \frac{[p-q,v]}{[u,v]} \tag{3.11}$$

Since we have a value for r that depends only on p, q, v, and u we can find the point specified in equation 3.1 without actually solving the equation. That is, the solution to $p + ru = q + sv$ is given by

$$I_{u,v}(p,q) = p + \frac{[p-q,v]}{[u,v]}u \tag{3.12}$$

Unfortunately, the notation introduced in equation 3.9 is opaque despite its aesthetic appeal. Therefore, we will embark on another adventure in algebraic manipulation to get a new equation of $I_{u,v}(p,q)$ from which we can easily derive some crutial properties of points in an origami ring on $\mathbb{C}$.

$$I_{u,v}(p,q) = p + \frac{[p-q,v]}{[u,v]}u \tag{3.13}$$

$$= \frac{p[u,v] + [p-q,v]u}{[u,v]} \tag{3.14}$$

We will now apply equation 3.9 to get

$$I_{u,v}(p,q) = \frac{p(u\bar{v} - \bar{u}v) - \left((p-q)\bar{v} - \overline{(p-q)}v\right)u}{u\bar{v} - \bar{u}v} \tag{3.15}$$

$$= \frac{pu\bar{v} - p\bar{u}v - (p\bar{v}u - q\bar{v}u - \bar{p}vu + \bar{q}vu)}{u\bar{v} - \bar{u}v} \tag{3.16}$$

$$= \frac{pu\bar{v} - p\bar{u}v - p\bar{v}u + q\bar{v}u + \bar{p}vu - \bar{q}vu}{u\bar{v} - \bar{u}v} \tag{3.17}$$

$$= \frac{-p\bar{u}v + q\bar{v}u + \bar{p}vu - \bar{q}vu}{u\bar{v} - \bar{u}v} \tag{3.18}$$

$$= \frac{\bar{p}vu - p\bar{u}v + q\bar{v}u - \bar{q}vu}{u\bar{v} - \bar{u}v} \tag{3.19}$$

The biggest jump in the algebra is arguably from 3.15 to 3.16. The jump comes from the fact that conjugacy of complex numbers

distributes. Returning to equation 3.19, we see that

$$I_{u,v}(p,q) = \frac{\bar{p}vu - p\bar{u}v - \bar{q}vu + q\bar{v}u}{u\bar{v} - \bar{u}v} = \frac{[u,p]}{[u,v]}v + \frac{[v,q]}{[v,u]}u$$

In order to prove some properties about the intersection operator, it is useful to keep the following equation in mind

(Algebraic Closed form of $I_{u,v}(p,q)$)

$$I_{u,v}(p,q) = \frac{u\bar{p}v - \bar{u}pv}{u\bar{v} - \bar{u}v} + \frac{q\bar{v}u - \bar{q}vu}{\bar{u}v - u\bar{v}} = \frac{[u,p]}{[u,v]}v + \frac{[v,q]}{[v,u]}u$$

From the algebraic closed form of the intersection operator, we can easily see that the following properties hold for for $p, q, u, v \in \mathbb{C}$.

Symmetry: $I_{u,v}(p,q) = I_{v,u}(q,p)$

Reduction: $I_{u,v}(p,q) = I_{u,v}(p,0) + I_{v,u}(q,0)$

Linearity: $I_{u,v}(p+q,0) = I_{u,v}(p,0) + I_{u,v}(q,0)$ and $rI_{u,v}(p,0) = I_{u,v}(rp,0)$ where $r \in \mathbb{R}$.

Projection: $I_{u,v}(p,0)$ is a projection of p on the line $\{rv : r \in \mathbb{R}\}$ in the u direction.

Rotation: For $w \in \mathbb{T}$, $wI_{u,v}(p,q) = I_{wu,wv}(wp,wq)$.

3. Examples of Origami Constructions

Constructing a point in an origami set has a very nice visual and geometric interpretation. In figure 3.1, we see how the point 2 can be

generically constructed with the assumption that we have at least three angles, one of which is 1.

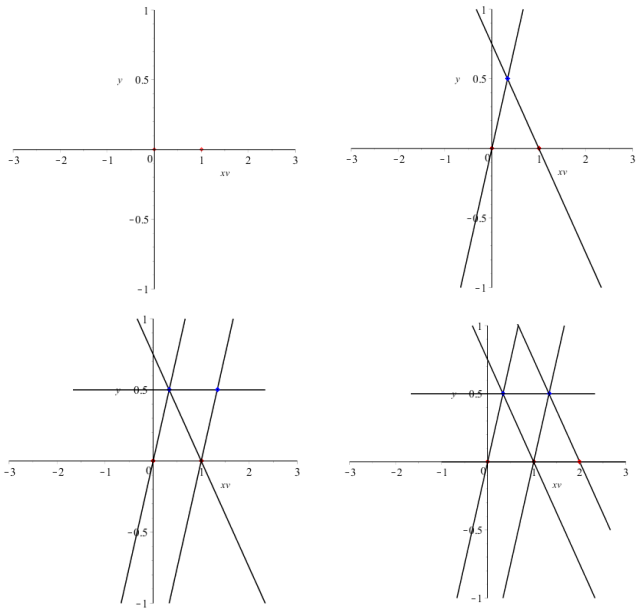

FIGURE 3.1. The construction in this figure shows how 2 can be constructed in any $R(S, U)$.

Of course, when we are trying to close an origami set under the intersection operator, we would like to add points faster than just one by one. In figure 3.2, we can see how an origami set expands. In particular, we can take the seed set S_0 and add all points to S_0 that can be constructed given U to create S_1. Then we have the recurrence relation

$$S_i = \{p = I_{u,v}(q, r) : u, v \in U, q, r \in S_{i-1}\}$$

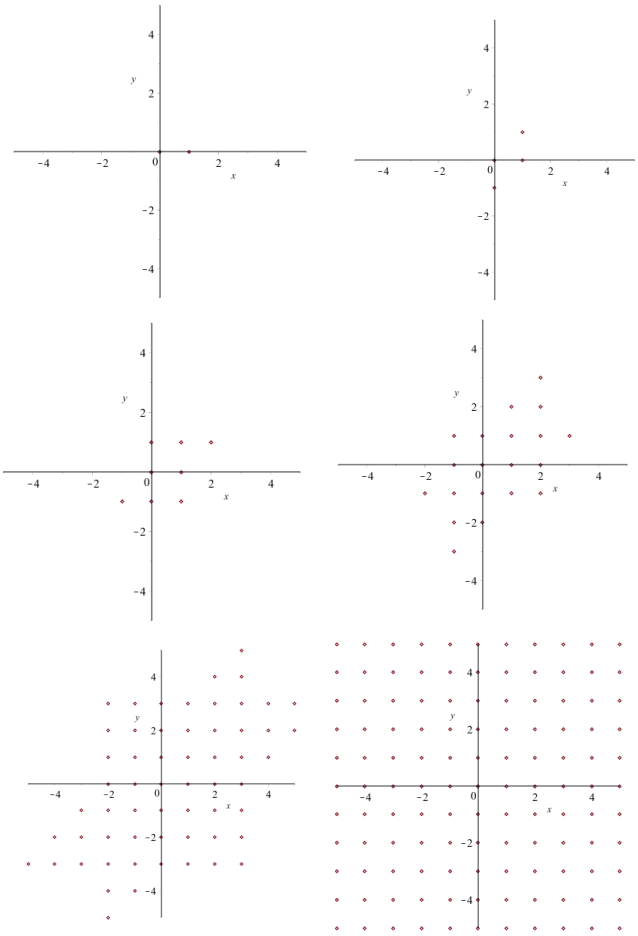

FIGURE 3.2. Here we see how the intersection operator expands the origami set, $R(S, U)$. Each generation adds all points that can be generated from some combination of points and angles from the previous generation. In this example, $S = \{0, 1\}$ and $U = \{1, \imath, e^{\imath \frac{pi}{4}}\}$.

Notice that the set that is closed under the origami operator, is the limit of the sequence S_i. Symbolically, this means that

$$R(S_0, U) = \lim_{n \to \infty} S_n$$

Hopefully, this way of thinking about origami sets is helpful.

4. Proof that $R(S,U)$ is a subring of $\mathbb{C}$

Recall that there are a handful of conditions a set with two binary operators must meet in oder to count as a ring. This section is dedicated to showing that $R(S,U)$ satisfies those conditions.

THEOREM 3.1. If U is a group and $|U| \geq 3$, then $R(S,U)$ is a subring of $\mathbb{C}$.

IDENTITY AND UNITY. Since $0, 1$ are elements in S, $0, 1$ will definitely be in $R(S,U)$. □

ASSOCIATIVITY AND DISTRIBUTION. Since $R(S,U)$ is a subset of the complex plane, we know that the inherited operations from $\mathbb{C}(+,\cdot)$ are associative and distributive over $R(S,U)$. □

LEMMA 3.1. For any $U \subset T/\{1,-1\}$ such that $|U| \geq 3$, $-1, 2 \in R(S,U)$.

The proof for Lemma 3.1 is best illustrated graphically.

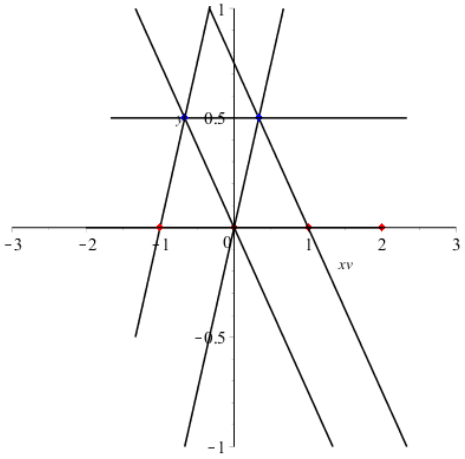

FIGURE 3.3. The construction in this figure shows how -1 can be constructed in any $R(S,U)$.

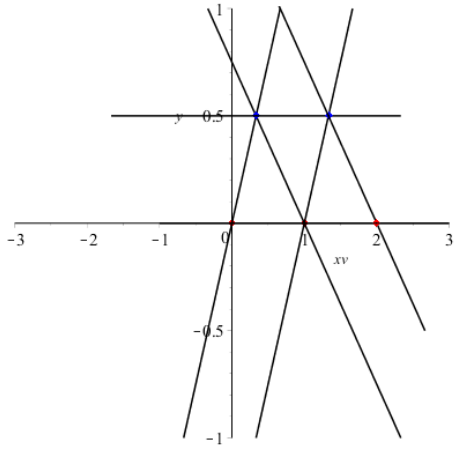

FIGURE 3.4. The construction in this figure shows how 2 can be constructed in any $R(S,U)$.

ADDITIVE CLOSURE. Assume that $p, q \in R(S,U)$. This implies that there exists a sequence of intersections that constructs p and q.

In particular, let

$$p = P(0,1) = I_{u,v}(I_{u',v'}(...), I_{u'',v''}(...))$$

and

$$q = Q(0,1) = I_{u,v}(I_{u',v'}(...), I_{u'',v''}(...)).$$

An example for these constructions is given in figure 3.5. The $0, 1$ in $P(0,1)$ denote that the construction started at $0, 1$. By Lemma 3.1, we know that $2 \in R(S,U)$. Notice that we can construct $p+1 = P(1,2)$, shown on the left of figure 3.6. By the same logic, we can construct $p+q$ by starting from $p, p+1$, shown on the right of figure 3.6. In particular $Q(p, p+1) = p+q$. Thus, $R(S,U)$ is closed under addition. □

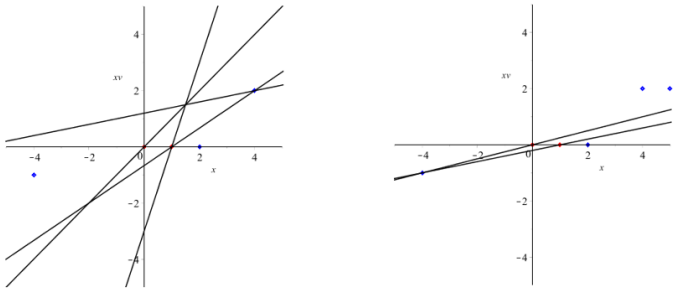

FIGURE 3.5. The graph on the left gives an example of a construction for a point p. The graph on the right gives an example of a construction for a point q.

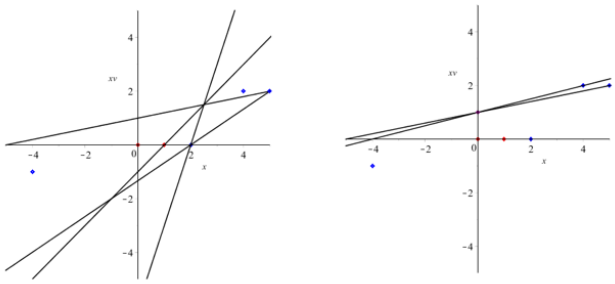

FIGURE 3.6. The graph on the left shows the construction of $p+1$ given the construction for p. The graph on the right shows the construction of $p+q$ given the construction of q and the points $p, p+1$.

ADDITIVE INVERSE. Assume that $p \in R(S,U)$. We want to show that $-p \in R(S,U)$. That is, there exists a construction

$$p = P(0,1) = I_{u,v}(I_{u',v'}(...), I_{u'',v''}(...)).$$

An example is given in figure 3.7. Recall that -1 is an element in $R(S,U)$. Furthermore, we know that

$$I_{u,v}(p,q) = -I_{v,u}(-q,-p)$$

This implies that

$$-p = P(-1,0)$$

This step is illustrated in figure 3.8. Thus, $R(S,U)$ contains additive inverses for all elements. $\square$

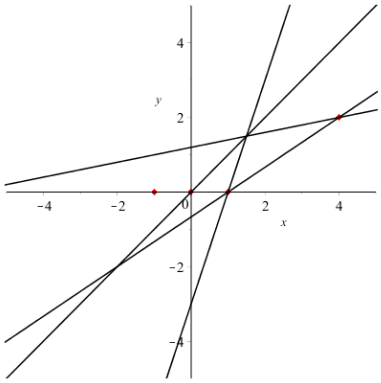

FIGURE 3.7. In this figure we see the construction of some point p.

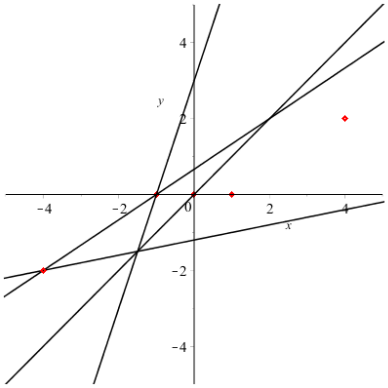

FIGURE 3.8. By reversing the steps of construction, we can use the construction of point p and the initial points $0, -1$ to construct $-p$.

DEFINITION 3.2. We say that a point p is a monomial of length n if p can be written in the form $I_{u_n,v_n}(p_{n-1}, 0)$ such that p_{n-1} is a monomial of length $n-1$. Monomials of length 1 are elementary monomials. Refer to figure 3.9 for an example.

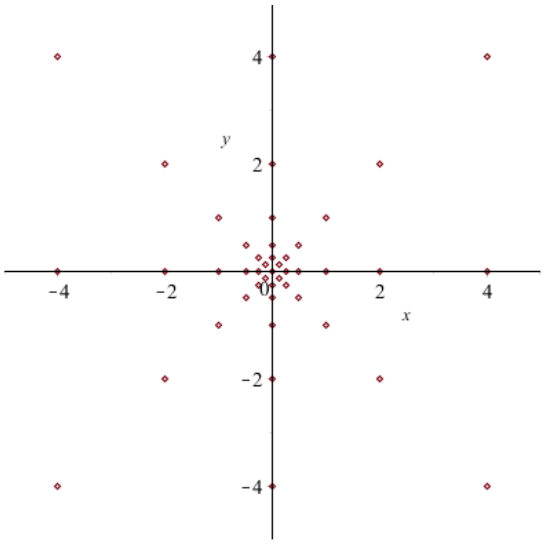

FIGURE 3.9. Monomials for $R(S,U)$ where $U = \{1, e^{\imath\frac{\pi}{4}}, e^{\imath\frac{\pi}{2}}, e^{\imath\frac{3\pi}{4}}\}$.

LEMMA 3.2. The set $R(S,U)$ consists of finite integer linear combinations of monomials.

PROOF. Since $R(S,U)$ is closed under addition and has additive inverses for all elements, it is clear that $R(S,U)$ contains all integer linear combinations of monomials. Therefore, we have that the set of all integer linear combinations of monomials is a subset of $R(S,U)$.

We will show that every element of $R(S,U)$ is a integer linear combination of monomials.

Base Case: If $I_{u,v}(p,q)$ is constructed out of one intersection, then it is an elementary monomial.

Induction Hypothesis: If a point is constructed in n intersections, then it is the linear combination of two monomials length at most n.

Induction Step: Assume $I_{u,v}(p,q)$ can be constructed $n+1$ operations. By linearity and reduction, $I_{u,v}(p,q) = I_{u,v}(p,0) + I_{v,u}(q,0)$. By applying the induction hypothesis to p and q are monomials of length at most n. Therefore, $I_{u,v}(p,q)$ is the linear combination of monomials and is of length at most $n+1$. Thus, we have shown that $R(S,U)$ consists of finite integer linear combinations of monomials. □

LEMMA 3.3. The product of any two monomials is a monomial and all monomials are the product of elementary monomials.

PROOF. We will prove this lemma by induction in each direction. That is, first we will induct on the length of two monomials that we are multiplying together. Second, we will induct on the length of a monomial we will factor into the product of two smaller monomials.

Base Case: Let $p = I_{u,v}(1,0)$ and $q = I_{u',v'}(1,0)$ be elementary monomials. Using the algebraic closed form for the intersection operator, we see that

$$I_{u,v}(1,0)I_{u',v'}(1,0) = \frac{[u,1]}{[u,v]} v I_{u',v'}(1,0)$$

by the rotation property we get

$$I_{u,v}(1,0)I_{u',v'}(1,0) = \frac{[u,1]}{[u,v]}I_{vu',vv'}(v,0)$$

notice that $r = \frac{[u,1]}{[u,v]} \in \mathbb{R}$, so by linearity

$$I_{u,v}(1,0)I_{u',v'}(1,0) = I_{vu',vv'}(rv,0)$$

since $rv = I_{u,v}(1,0)$ and $u, v, u', v' \in U$

$$I_{u,v}(1,0)I_{u',v'}(1,0) = I_{vu',vv'}(I_{u,v}(1,0),0)$$

which is a monomial of length 2. This concludes the base case.

Induction Hypothesis: If m and m' are monomials such that the sum of their length is at most N then mm' is a monomial.

Induction Step: Let $m, m' \in R(S,U)$ such that $m = I_{x,w}(m_0,0)$ is a monomial of length a and $m' = I_{x',w'}(m'_0,0)$ is a monomial of length b such that $a + b = N$. Consider

$$mI_{u,v}(m',0) = rwI_{u,v}(m',0)$$

where $r \in \mathbb{R}$ and $w \in U$. By rotation and linearity, we get

$$mI_{u,v}(m',0) = I_{wu,wv}(rwm',0)$$

$$mI_{u,v}(m',0) = I_{wu,wv}(mm',0).$$

Therefore, we know that if m, m' are monomials, then mm' is a monomial by strong mathematical induction.This is the only place in which U being a group is relevant. In particular, U being a group guarantees that $wu \in U$.

Base Case: Let $p = I_{u,v}(q, 0)$ be a monomial of length 2. Since q must also be a monomial by definition, we have

$$I_{u,v}(q, 0) = I_{u,v}(rw, 0)$$

where $r \in \mathbb{R}$ and $w \in U$. By linearity, we get

$$I_{u,v}(q, 0) = rI_{u,v}(w, 0).$$

Next, rotation gives us

$$I_{u,v}(q, 0) = rwI_{w^{-1}u,w^{-1}v}(1, 0)$$

$$I_{u,v}(q, 0) = qI_{w^{-1}u,w^{-1}v}(1, 0)$$

Notice that q and $I_{w^{-1}u,w^{-1}v}(1, 0)$ are elementary. This concludes the base case.

Induction Hypothesis: If m is a monomial of length at most N, then m is the product of two shorter monomials.

Induction Step: Let $m = I_{u,v}(q, 0)$ be a monomial of length $N+1$. Since q must also be a monomial by definition, we have

$$I_{u,v}(q, 0) = I_{u,v}(rw, 0)$$

where $r \in \mathbb{R}$ and $w \in U$. By linearity, we get

$$I_{u,v}(q, 0) = rI_{u,v}(w, 0).$$

Next, rotation gives us

$$I_{u,v}(q, 0) = rwI_{w^{-1}u,w^{-1}v}(1, 0)$$

$$I_{u,v}(q, 0) = qI_{w^{-1}u,w^{-1}v}(1, 0).$$

Notice that q and $I_{w^{-1}u,w^{-1}v}(1, 0)$ are monomials of length at most N. This is the only place in which U being a group is relevant. In particular, U being a group guarantees that $w^{-}1u \in U$. Therefore, by the induction hypothesis m is the product of two monomials. Thus, we know that if m is a monomial, then it is the product of two shorter monomials by strong mathematical induction.

Combining the results of the two induction proofs, we have that the product of any two monomials is a monomial and any monomial is a product of two monomials. By lemma, 3.2 any monomial is the product of elementary monomials. □

MULTIPLICATIVE CLOSURE. Let $p, q \in R(S,U)$. By Lemma 3.2,

$$p = a_n p_n + a_{n-1} p_{n-1} + \cdots + a_1 p_1$$

and

$$q = b_m q_m + b_{m-1} q_{m-1} + \cdots + b_1 q_1$$

where $a_i, b_i \in \mathbb{Z}$ and p_i, q_i are elementary monomials. Consider

$$\begin{aligned} pq &= (a_n p_n + \cdots + a_1 p_1)(b_m q_m + \cdots + b_1 q_1) \\ &= \sum_{\substack{1 \le i \le n \\ 1 \le j \le m}} a_i b_j p_i q_j \end{aligned}$$

Notice that $a_i b_j \in \mathbb{Z}$. We may apply Lemma 3.3 to each $p_i q_j$ to see that $p_i q_j$ is also a linear combination of monomials. Therefore, we can distribute $a_i b_j$ over $p_i q_j$ to get a really long integer linear combination of monomials. That is, pq is an integer linear combination of monomials. Thus, by Lemma 3.2, $pq \in R(S,U)$.

□

To conclude this section, we have proven Theorem 3.1 by showing that when $|U| \ge 3$ is a group and $S = \{0, 1\}$, then $R(S,U)$ is a subring of the complex numbers.

5. Classifying $R(S,U)$

In order for us to pinpoint exactly which rings $R(S,U)$ can be when U is a group, we need to be more specific about the form of each element in $R(S,U)$. In the remainder of this section, I will let U be a subgroup of $T/\{1,-1\}$ such that $|U| \geq 3$. In particular, we will let U be the cyclic group of angles generated by $e^{\imath\frac{\pi}{n}}$. Now let us examine the algebraic closed form expression for intersections.

Let $u = e^{\imath\pi a}, c = e^{\imath\pi b}$, and $w = e^{\imath\pi c}$. Consider

$$\begin{aligned}
\frac{[u,w]}{[u,v]} &= \frac{e^{\imath\pi a}e^{-\imath\pi c} - e^{-\imath\pi a}e^{\imath\pi c}}{e^{\imath\pi a}e^{-\imath\pi b} - e^{-\imath\pi a}e^{\imath\pi b}} \\
&= \frac{e^{\imath\pi(a-c)} - e^{\imath\pi(c-a)}}{e^{\imath\pi(a-b)} - e^{\imath\pi(b-a)}} \\
&= \frac{\cos(\pi(a-c)) + \imath\sin(\pi(a-c)) - \cos(\pi(c-a)) + \imath\sin(\pi(c-a))}{\cos(\pi(a-b)) - \imath\sin(\pi(a-b)) - \cos(\pi(b-a)) - \imath\sin(\pi(b-a))} \\
&= \frac{\imath\sin(\pi(a-c)) - \imath\sin(\pi(c-a))}{\imath\sin(\pi(a-b)) - \imath\sin(\pi(b-a))} \\
&= \frac{2\imath\sin(\pi(a-c))}{2\imath\sin(\pi(a-b))} \\
&= \frac{\sin(\pi(a-c))}{\sin(\pi(a-b))}.
\end{aligned}$$

The upshot of this break down is that $\frac{[u,w]}{[u,v]}$ is a real number, which is a glossed over fact used in the proofs of lemmas 3.2 and 3.3. However, we get a little more out of this as well. Recall that by Lemma 3.3, every

monomial is the product of elementary monomials. In other words, if p is a monomial, then

$$p = \frac{[u_1, 1]}{[u_1, v_1]} \frac{[u_2, u_1]}{[u_2, v_2]} \cdots \frac{[u_n, u_{n-1}]}{[u_n, v_n]} v_n.$$

Now that we know that $\frac{[u,w]}{[u,v]}$ is a real number, we can see that a monomial is just a scaled point from our group U. This is consistent with figure 3.9.

Now let's integrate this notation with the intersection for a monomial.

$$\begin{aligned} I_{u,v}(1,0) &= \frac{[u,1]}{[u,v]} v \\ &= \frac{u - \bar{u}}{u\bar{v} - \bar{u}v} v. \end{aligned}$$

Notice that $v = \frac{1}{\bar{v}}$. Thus

$$\begin{aligned} I_{u,v}(1,0) &= \frac{u - \bar{u}}{u\bar{v} - \bar{u}v} \frac{1}{\bar{v}} \\ &= \frac{u - \bar{u}}{u\bar{v}^2 - \bar{u}v\bar{v}} \end{aligned}$$

We also know that $u\bar{u} = 1$ since u is on the unit circle. The same holds for v. Hence

$$\begin{aligned} I_{u,v}(1,0) &= \frac{u-\bar{u}}{u\bar{v}^2-\bar{u}}\frac{u}{u} \\ &= \frac{u^2-1}{u^2\bar{v}^2-1} \\ &= \frac{u^2-1}{u^2/v^2-1}. \end{aligned}$$

Since $u, v, -1$ are all in $U \subset T/\{1,-1\}$ factor out by -1 to get

$$I_{u,v}(1,0) = \frac{1-u^2}{1-(u/v)^2}.$$

The result is that every elementary monomial is of the form

$$\frac{1-u}{1-v}$$

where $u, v \in V$ and $V = \{u^2 : u \in U\}$. Using this fact, and lemmas 3.2 and 3.3 Theorem 3.2.

THEOREM 3.2. Let U be a group of angles with at least three elements, and let $V \subset \mathbb{T}$ be the group of squares of angles. Then $R(S,U)$ is the subring of $\mathbb{C}$ consisting of integer linear combinations of monomials, were monomials are products of elements of the form

$$\frac{1-u}{1-v}$$

for $u, v \in V$, $v \neq 1$.

Upon closer examination, we get a much more exciting corollary. Notice that $V \subset \mathbb{Q}(\omega)$ where ω is the generator of U. In other words,

$$\frac{1-u}{1-v}$$

for $u, v \in V$, $v \neq 1$ is a element in the nth cyclotomic field where $n = |U|$. Since the ring $R(S,U)$ consists of integer linear combinations of elements of this form, we can see that $R(S,U)$ is very close to being $\mathbb{Z}[\omega]$.

COROLLARY 3.2.1. For every group $U \subset \mathbb{T}/\{-1,1\}$ with order n, $R(S,U) \subset \mathbb{Q}(\omega_n)$.

We can be even more precise about origami rings generated by U. However, we have quite a bit of work to do before we get there.

THEOREM 3.3. Fix $n > 3$, and let $\omega = e^{\imath\frac{\pi}{n}}$. Let $a, b \not\equiv 0 \mod n$.

a: If n is prime, then $(1-\omega^a)/(1-\omega^b)$ is an algebraic integer.

b: If n is non-prime, then $(1-\omega^a)/(1-\omega^b)$ has denominator dividing n.

c: If n is non-prime and p is a prime divisor of n, then some product of an element of $\mathbb{Z}[\omega]$ by a product of quotients of the form $(1-\omega^a)/(1-\omega^b)$ is equal to $\frac{1}{p}$.

PROOF. (a) Assume that n is prime. Notice that n and b are relatively prime. Therefore, $a + rn = bs$ for some integers r and s. Now consider

$$\begin{aligned}\frac{1-\omega^a}{1-\omega^b} &= \frac{1-\omega^{a+rn}}{1-\omega^b} \\ &= \frac{1-\omega^{bs}}{1-\omega^b} \\ &= -(\omega^{b(s-1)} + \omega^{b(s-2)} + \cdots + \omega^b + 1)\end{aligned}$$

Since this is a polynomial in ω with integer coefficients, it is an element of $\mathbb{Z}[\omega]$. That is, it is algebraic over $\mathbb{Q}(\omega)$. □

PROOF. (b) let n be non-prime. Recall the identity

$$x^n - 1 = \prod_{k=0}^{n-1}(x - \omega^k)$$

Now we can divide both sides by $x - 1$ to get the following

$$\begin{aligned}x^n - 1 &= \prod_{k=0}^{n-1}(x - \omega^k) \\ \frac{x^n - 1}{x - 1} &= \prod_{k=1}^{n-1}(x - \omega^k) \\ x^{n-1} + \cdots + x + 1 &= \prod_{k=1}^{n-1}(x - \omega^k)\end{aligned}$$

Taking the limit as $x \to 1$, we get

$$n = \prod_{k=1}^{n-1}(1-\omega^k)$$

This suggests that $1-\omega^k$ divides n as long as $k \not\equiv 0 \mod n$; in which case $\omega^k = 1$. □

PROOF. (c) Assume that n is not prime and p is a prime divisor of n. Let d be a divisor of n. All we need to show is that (c) holds for the cases $n = pq$ and $n = p^2$ where p, q are prime. Equivalently, we can show that (c) holds for quotients $(1-\omega^a)/(1-\omega^b)$ where a, b are multiples of n/d.

Assume that $n = pq$. Consider

$$n = \prod_{k=1}^{n-1}(1-\omega^k)$$

divide both sides by pq to get

$$\frac{n}{pq} = \prod_{\gcd(k,n)}(1-\omega^k)$$

$$1 = \prod_{\gcd(k,n)}(1-\omega^k)$$

Notice that this suggests that $1-\omega$ is a unit. Let u^{-1} be the inverse of $\prod_{k=1}^{p-1}(1-\omega)$.

$$\prod_{k=1}^{p-1}(1-\omega) = u$$

divide both sides by p

$$\prod_{k=1}^{p-1}\frac{1-\omega}{1-\omega^{qk}} = \frac{u}{p}.$$

Notice that ω^q is a primitive root of unity because q is prime and, therefore, relatively prime to n. Furthermore, u is a unit, so u^{-1} exists. Thus,

$$\frac{1}{p} = \prod_{k=1}^{p-1}\frac{1-\omega}{1-\omega^{qk}}u^{-1}$$

and the claim is shown in the case that $n = pq$.

Assume that $n = p^2$. Given that $p = \prod_{k=1}^{p-1}(1-\omega^k)$ and $p^2 = \prod_{k=1}^{p^2-1}(1-\omega^k)$, consider

$$\prod_{k=1,k\neq p}^{p^2-1} = \frac{1}{p^{p-1}}.$$

Notice, that we can multiply this quotient by p^{p-2} to get $1/p$. For more details turn to [**1**]. This completes the proof. □

We use all of these results to show the next theorem.

THEOREM 3.4 (Buhler, Butler, de Laundey, Graham (2010)). If $n = p$ is prime, then $R(S,U) = \mathbb{Z}[\omega_n]$ where $|U| = n$. If n is non-prime, then $R(S,U) = \mathbb{Z}[\frac{1}{n}, \omega_n]$.

PROOF. Let $n = p$ be prime. Recall that $-1 \in R(S,U)$. Since part (a) of Theorem 3.3 states that all products of elementary monomials are algebraic integers in $\mathbb{Q}(\omega)$ and all elements in $R(S,U)$ are products of elementary monomials, it follows that $R(S,U) = \mathbb{Z}[\omega]$.

Let n be non-prime. In this case, part (b) of Theorem 3.3 shows that $R(S,U) \subset \mathbb{Z}[\frac{1}{n}, \omega]$. Part (c) of Theorem 3.3 shows that every element in $\mathbb{Z}[\frac{1}{n}, \omega]$ in particular $\frac{1}{n}$ can be constructed using the intersection operations. Therefore, it follows that $R(S,U) = \mathbb{Z}[\frac{1}{n}, \omega]$. □

Notice that Theorem 3.4 states that if U is a group, then $R(S,U)$ is almost the ring of algebraic integers for some cyclotomic field. In particular, if the order of U is prime, then we have $R(S,U) = \mathbb{Z}[\omega]$ which is a nice result. However, if the order of U is not a prime, the resulting origami ring is a little bigger than a ring of algebraic integers. That is, if the order of U is not a prime, the origami construction in some sense is over-generating points for it to be a real nice ring.

CHAPTER 4

Converse of the Origami Ring Theorem

The most natural conjecture would be that for every subring R of the complex numbers, there exists a group $U \subset T/\{1, -1\}$ such that $R(S, U) = R$. However, this conjecture is almost trivially false. Consider the Gaussian integers, $\mathbb{Z}[\imath]$. By the contrapositive of Theorem 3.4, there does not exist a $U \subset T/\{1, -1\}$ such that $R(S, U) = \mathbb{Z}[\imath]$. In light of this fact, we ask a different question. For which subrings R of the complex number do there exist sets of angles U such that $R(S, U) = R$? In particular, we are no longer are restricting U to be a group.

1. Exploring the impact of U

Before making a conjecture, we will explore what happens under the intersection operator for arbitrary pairs of angles in a group. This will give us an idea about why requiring U to be a group is so restricting. In particular, we are going to play around with origami rings in reference to the Gaussian integers.

LEMMA 4.1. Let $u, v \in \mathbb{C}$ such that $u \neq v$ and are not of the form $r\imath$ or r for any $r \in \mathbb{R}$. If the sign of the real components of u and v are different but the sign of the imaginary components of u and v are the same, then $I_{u,v}(0,1)$ is not a Gaussian integer.

PROOF. Let $u, v \in \mathbb{C}$ such that $u \neq v$ and are not of the form $r\imath$ or r for any $r \in \mathbb{R}$. Assume that the sign of the real components of u and v are different but the sign of the imaginary components of u and v are the same. This implies that the real component of the intersection $I_{u,v}(0,1)$ is strictly between 0 and 1. Thus, $I_{u,v}(0,1)$ is not a Gaussian integer. □

The result of Lemma 4.1 is if we pick angles that are not parallel to the real or imaginary line, then the first point those angles generate is not in a nice location. With a little bit of visualizing, we can see that for any z such that $\Re(z) \in (0,1)$ there exists u, v such that $I_{u,v}(1,0) = z$. As a result, it is pretty clear why we cannot find a group U such that $R(S,U) = \mathbb{Z}[\imath]$.

THEOREM 4.1. There does not exist a group $U \subset T/\{1,-1\}$ such that $R(S,U)$ is the Gaussian integers.

PROOF. Consider the Gaussian integers as as subring of the complex plane. Let U be a finite subgroup of $T/\{1,-1\}$ such that $R(S,U)$

is the Gaussian integers. Notice that $1 \in U$ because it is the identity. In order for $R(S,U)$ to be non-empty there must exists at least 2 non-identity elements in U; call these two elements u, v. We will let $n \geq 3$ denote the order of U. Given that $|U| \geq 3$, we can find $u, v \in U$ such that $u \neq v$ and neither u nor v are $\imath$ or 1. This implies that $p = I_{u,v}(1,0)$ is not a Gaussian integer by Lemma 4.1. □

The next natural question to ask is whether we can find a subset U of $T/\{-1,1\}$ that is not necessarily a group such that $R(S,U)$ is the Gaussian integers. We find that there does exist such a set of angles, namely,

$$U = \{1, \imath, e^{\imath\frac{\pi}{4}}\}$$

The reasons this set of angles seems to work is that all of the angles are in the first quadrant. We saw in Lemma 4.1 that when we have two angles in $T/\{1,-1\}$ that are not in the same quadrant, then we get a point with the real component in $(0,1)$.

THEOREM 4.2. Let $U = \{1, \imath, e^{\imath\frac{\pi}{4}}\}$. Then $R(S,U)$ is the Gaussian integers.

PROOF. Let $U = \{1, \imath, e^{\imath\frac{\pi}{4}}\}$. We will first show that $I_{u,v}(p,q)$ where $u, v \in U$ is a Gaussian integer if p and q are Gaussian integers. Assume

that $p = a + b\imath$ and $q = c + \imath$ are Gaussian integers. Since U has 3 elements and order matters, there are six cases.

(1) $I_{1,\imath}(p, q) = c + b\imath$

(2) $I_{1,e^{\imath\frac{\pi}{4}}}(p, q) = c - d + b + b\imath$

(3) $I_{\imath,1}(p, q) = a + d\imath$

(4) $I_{\imath,e^{\imath\frac{\pi}{4}}}(p, q) = a + (a - c + d)\imath$

(5) $I_{e^{\imath\frac{\pi}{4}},1}(p, q) = a - b + d + d\imath$

(6) $I_{e^{\imath\frac{\pi}{4}},\imath}(p, q) = c + (-a + b + c)\imath$

Since both p and q are assumed to be Gaussian integers, we can see that all six possible intersections of are also Gaussian integers.

Now, consider $R(S, U)$. Notice that all elements in S are Gaussian integers. Therefore, S_1 consists of Gaussian integers. In fact, this iterative construction will only yield Gaussian integers, because those are the only reference points we ever have. Thus, we have shown that $R(S, U)$ is a subset of the Gaussian integers.

It remains to be shown that any Gaussian integer can be constructed using S and U. Let $a + b\imath$ be a Gaussian integer. Notice, that if we can construct $b\imath$ and $1 + b\imath$ by starting at S, and we can construct a by starting at S, then we can construct $a + b\imath$ by starting at $\{b\imath, 1 + b\imath\}$. We can further reduce the problem by showing that given points $\{n + k\imath, n + 1 + k\imath\}$ we can construct both $n - 1 + k\imath$ and $n + 2 + k\imath$, and that given $\{n + k\imath, n + 1 + k\imath\}$ we can construct $n + (k + 1)\imath$, $n + 1 + (k + 1)\imath$, $n + (k - 1)\imath$, and $n + 1 + (k - 1)\imath$. We will now construct the desired points using the appropriate reference points.

Constructing $n + 2 + k\imath$: Consider

$$I_{\imath,1}(I_{1,e^{\imath\frac{\pi}{4}}}(I_{e^{\imath\frac{\pi}{4}},\imath}(n + k\imath, n + 1 + k\imath), n + 1 + k\imath)), n + 1 + k\imath)$$

Notice that we can evaluate this expression using the six cases enumerated above. In particular, we apply case (6) first to get

$$I_{\imath,1}(I_{1,e^{\imath\frac{\pi}{4}}}(n + 1 + (k + 1)\imath, n + 1 + k\imath), n + 1 + k\imath)$$

Next, we apply case (2) to get

$$I_{\imath,1}(n + 2 + (k + 1)\imath, n + 1 + k\imath)$$

Finally, we use case (3) to get

$$n + 2 + k\imath$$

Constructing $n - 1 + k\imath$: Consider

$$I_{\imath,1}(I_{1,e^{\imath\frac{\pi}{4}}}(I_{\imath,e^{\imath\frac{\pi}{4}}}(n + k\imath, n + 1 + k\imath), n + k\imath), n + k\imath)$$

First, we apply case (4) to get

$$I_{\imath,1}(I_{1,e^{\imath\frac{\pi}{4}}}(n + (k - 1)\imath, n), n)$$

Next, we apply case (2) to get

$$I_{\imath,1}(n - 1 + (k - 1)\imath, n)$$

Finally, we apply case (3) to get

$$n - 1 + k\imath$$

Constructing $n + (k + 1)\imath$ and $n + 1 + (k + 1)\imath$: Consider

$$I_{e^{\imath\frac{\pi}{4}},\imath}(n + k\imath, n + 1 + k\imath)$$

Using case (6) we get

$$n + 1 + (k + 1)\imath$$

Now consider

$$I_{\imath,1}(n + k\imath, n + 1 + (k + 1)\imath)$$

Using case (3) we get

$$n + (k + 1)$$

Constructing $n + (k - 1)\imath$ and $n + 1 + (k - 1)\imath$: Consider

$$I_{\imath,e^{\imath\frac{\pi}{4}}}(n + k\imath, n + 1 + k\imath)$$

Using case (4) we get

$$n + (k - 1)\imath$$

Consider

$$I_{\imath,1}(n + 1 + k\imath, n + (k - 1)\imath$$

Using case (3) we get

$$n + 1 + (k - 1)\imath$$

Thus, we have shown that any Gaussian integer can be constructed using S and U. Combining the previous two results shows that $R(S, U)$ is the Gaussian integers. □

The general construction of the Gaussian integers is similar to the constructions of -1 and 2 in figures 3.3 and 3.4. However, there are two differences worth noting. First, the construction in the proof of Theorem 4.2 is general, not just for a particular point. Second, and

this is more interesting, is that the construction for -1 in the proof of Theorem 4.2 works down and not up. Consider figure 3.4. We can see that constructing -1 uses the inverse of the construction used for 2 and applies it to the points $0, 1$.

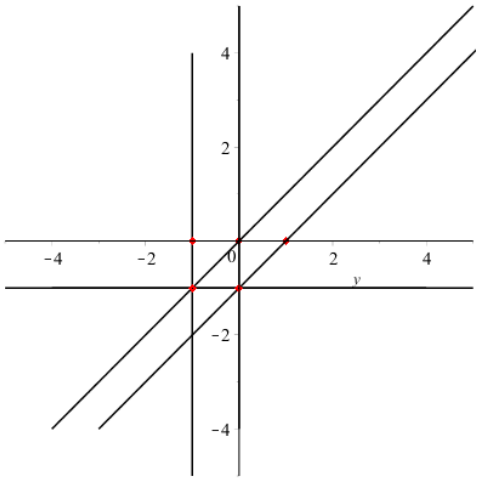

FIGURE 4.1. This construction uses $U = \{1, \imath, e^{\imath\frac{\pi}{4}}\}$ to generate the point -1

2. Revisiting Rings of Algebraic Integers

Let's summarize what we have learned so far about origami rings. At the end of the paper *Origami Rings*, we see Theorem 3.4. This theorem states that if $U \subset T/\{1, -1\}$ with $|U| = n \geq 3$, then $R(S, U) = \mathbb{Z}[\omega]$ for prime n, and $R(S, U) = \mathbb{Z}[\frac{1}{n}, \omega]$ for composite n. These rings are remarkably close to the integer rings for the cyclotomic fields. Notice that the Theorem 4.2 constructs the Gaussian integers, which are

the algebraic integers of $\mathbb{Q}(\imath)$. Algebraic integers are of interest in their own right. Therefore, it would be nice if we could construct as many of them as possible. In particular, I will show that we can construct $\mathbb{Z}[\sqrt{m}]$ for any $\mathbb{Q}(\sqrt{m})$. Recall the following corollary.

COROLLARY. Let m be a squarefree integer. The set of algebraic integers in the quadratic field $\mathbb{Q}(\sqrt{m})$ is

$$\{a + b\sqrt{m} : a, b \in \mathbb{Z}\} \text{ if } m \equiv 2 \text{ or } 3 \mod 4$$

$$\{\frac{a + b\sqrt{m}}{2} : a, b \in \mathbb{Z}, a \equiv b \mod 2\} \text{ if } m \equiv 1 \mod 4$$

I had success in constructing the Gaussian integers with the angle set

$$U = \{1, e^{\imath\frac{\pi}{4}}, \imath\}$$

Notice that $e^{\imath\frac{\pi}{4}}$ is the principal argument for $1+\imath$ which is the Gaussian integer in the first quadrant closest to the origin. A natural question to ask at this point is whether or not other rings of algebraic integers can be constructed as well. With this in mind, we will set out to prove the following theorem in the next section.

THEOREM. Let $m < 0$ be a squarefree integer. The set of algebraic integers in the quadratic field $\mathbb{Q}(\sqrt{m})$ is $R(S, U)$ where

$$U = \{1, \imath, e^{\imath\theta}\} \text{ if } m \equiv 2 \text{ or } 3 \mod 4$$

$$U = \{1, e^{\imath\theta}, e^{\imath(\pi-\theta)}\} \text{ if } m \equiv 1 \mod 4.$$

Notice that this theorem extends only to $m < 0$ because origami constructions are inherently in the complex plane. If $m \geq 0$ then the corresponding rings of algebraic integers would only have real elements, and thus, cannot be constructed by origami folds.

CHAPTER 5

Constructing Rings of Algebraic Integers for Imaginary $\mathbb{Q}(\sqrt{m})$

In chapter 4, I posit that there are essentially two cases for constructing the algebraic integers for imaginary quadratic extensions. One case seems easier, because it is directly analogous to the construction for the Gaussian integers. However, the second case seems harder. In particular, we need to ensure that the parity of a, b in $\frac{a+b\sqrt{m}}{2}$ is the same. The result is that we need different sets of angles, and that the origami rings develop in different patterns. In the remainder of this chapter I will prove both cases of theorem 5.1. Along the way, we will examine the way each origami ring develops from generation to generation.

1. The $m \equiv 2$ or $3 \mod 4$ Case

The proof for the following lemma is essentially the same as the proof for Theorem 4.2. The key for the proof is that we replace the angle $\frac{\sqrt{2}+\sqrt{2}\imath}{2} = e^{i\frac{\pi}{4}}$ with the principal argument of $1 + \sqrt{m}$.

LEMMA 5.1. Let $m \equiv 2$ or 3 mod 4 and $m < 0$. Let $U = \{1, \imath, e^{\imath\theta}\}$ where θ is the principal argument of $1 + \sqrt{m}$. Then

$$R(S, U) = \{a + b\sqrt{m} : a, b \in \mathbb{Z}\}$$

PROOF. Let $m \equiv 2$ or 3 mod 4 and $m < 0$. Let $U = \{1, \imath, e^{\imath\theta}\}$ where θ is the principal argument of $1 + \sqrt{m}$. First, we will show that $I_{u,v}(p, q) \in Z[\sqrt{m}]$ where $u, v \in U$ and $p, q \in \mathbb{Z}[\sqrt{m}]$. As in the proof for theorem 4.1, there are six cases.

(1) $I_{1,\imath}(p, q) = c + b\sqrt{m}$

(2) $I_{1,e^{\imath\theta}}(p, q) = b + c - d + b\sqrt{m}$

(3) $I_{\imath,1}(p, q) = a + d\sqrt{m}$

(4) $I_{\imath,e^{\imath\theta}}(p, q) = a + (a - c + d)\sqrt{m}$

(5) $I_{e^{\imath\theta},1}(p, q) = a - b + d + d\sqrt{m}$

(6) $I_{e^{\imath\theta},\imath}(p, q) = c + (-a + b + c)\sqrt{m}$

This concludes the proof for the closure of the intersection operator. In other words, as long as our seed set starts with elements in $\mathbb{Z}[\sqrt{m}]$, then the intersections will also be in $\mathbb{Z}[\sqrt{m}]$. We can also express this claim as $R(S,U) \subset \mathbb{Z}[\sqrt{m}]$. It remains to be shown that any element in $\mathbb{Z}[\sqrt{m}]$ is also an element in $R(S,U)$.

Let $a + b\sqrt{m}$ be an element in in $\mathbb{Z}[\sqrt{m}]$. Notice, that if we can construct $b\sqrt{m}$ and $(1+b)\sqrt{m}$ by starting at S, and we can construct a by starting at S, then we can construct $a + b\sqrt{m}$ by starting at $\{b\sqrt{m}, (1+b)\sqrt{m}\}$. We can further reduce the problem by showing that given points $\{n + k\sqrt{m}, n + 1 + k\sqrt{m}\}$ we can construct both $n-1+k\sqrt{m}$ and $n+2+k\sqrt{m}$, and that given $\{n+k\sqrt{m}, n+1+k\sqrt{m}\}$ we can construct both $n + (k-1)\sqrt{m}$ and $n + 1 + (k+1)\sqrt{m}$. We will now construct the desired points using the appropriate reference points.

Constructing $n + 2 + k\sqrt{m}$: Consider

$$I_{\iota,1}(I_{1,e^{\imath\theta}}(I_{e^{\imath\theta},\iota}(n + k\sqrt{m}, n + 1 + k\sqrt{m}), n + 1 + k\sqrt{m}), n + 1 + k\sqrt{m})$$

Notice that we can evaluate this expression using the six cases enumerated above. In particular, we apply case (6) first to get

$$I_{\iota,1}(I_{1,e^{\imath\theta}}(n + 1 + (k+1)\sqrt{m}, n + 1 + k\sqrt{m}), n + 1 + k\sqrt{m})$$

Next, we apply case (2) to get

$$I_{\imath,1}(n+1+(k+1)\sqrt{m}, n+1+k\sqrt{m})$$

Finally, we use case (3) to get

$$n+2+k\sqrt{m}$$

Constructing $n-1+k\sqrt{m}$: Consider

$$I_{\imath,1}(I_{1,e^{\imath\theta}}(I_{\imath,e^{\imath\theta}}(n+k\sqrt{m}, n+1+k\sqrt{m}), n+k\sqrt{m}), n+k\sqrt{m})$$

First, we apply case (4) to get

$$I_{\imath,1}(I_{1,e^{\imath\theta}}(n+(k-1)\sqrt{m}, n+k\sqrt{m}), n+k\sqrt{m})$$

Next, we apply case (2) to get

$$I_{\imath,1}(n-1+(k-1)\sqrt{m}, n)$$

Finally, we apply case (3) to get

$$n-1+k\sqrt{m}$$

Constructing $n+(k+1)\sqrt{m}$ and $n+1+(k+1)\sqrt{m}$: Consider

$$I_{e^{\imath\theta},\imath}(n+k\sqrt{m}, n+1+k\sqrt{m})$$

Using case (6) we get

$$n+1+(k+1)\sqrt{m}$$

Now consider

$$I_{\iota,1}(n + k\sqrt{m}, n + 1 + (k + 1)\sqrt{m})$$

Using case (3) we get

$$n + (k + 1)\sqrt{m}$$

Constructing $n + (k - 1)\sqrt{m}$ and $n + 1 + (k - 1)\sqrt{m}$: Consider

$$I_{\iota,e^{\iota\theta}}(n + k\sqrt{m}, n + 1 + k\sqrt{m})$$

Using case (4) we get

$$n + (k - 1)\sqrt{m}$$

Consider

$$I_{\iota,1}(n + 1 + k\sqrt{m}, n + (k - 1)\sqrt{m})$$

Using case (3) we get

$$n + 1 + (k - 1)\sqrt{m}$$

With this we have shown that $\mathbb{Z}[\sqrt{m}] \subset R(S, U)$, completing the proof. □

2. The $m \equiv 1 \mod 4$ Case

The proof for lemma 5.2 employs the same strategy as the proof for lemma 5.1. However, there is a difference. Generally, the strategy the proof uses is finding general solutions to the possible intersection functions in the component variables of the input points. In the proof of lemma 5.2, we will see that restricting input points to have components with the same parity still does the trick. f

LEMMA 5.2. Let $m \equiv 1 \mod 4$ and $m < 0$. Let $U = \{0, \theta, \pi - \theta\}$ where θ is the principal argument of $\frac{1+\sqrt{m}}{2}$. Then

$$R(S, U) = \{\frac{a + b\sqrt{m}}{2} : a, b \in \mathbb{Z}, a \equiv b \mod 2\} = H$$

PROOF. Let $m \equiv 1 \mod 4$ and $m < 0$. Let $U = \{1, e^{\imath\theta}, e^{\imath(\pi-\theta)}\}$ where θ is the principle argument of $\frac{1+\sqrt{m}}{2}$. First, we will show that $I_{u,v}(p, q) \in H$ where $u, v \in U$ and $p, q \in H$. As in the proof for lemma 5.1, there are six cases.

(1) $I_{1,e^{\imath\theta}}(p, q) = b + c - d + b\sqrt{m}$

(2) $I_{1,e^{\imath(\pi-\theta)}}(p, q) = c + d - b + b\sqrt{m}$

(3) $I_{e^{\imath\theta},1}(p, q) = a - b + d + d\sqrt{m}$

(4) $I_{e^{\imath\theta},e^{\imath(\pi-\theta)}}(p,q) = \frac{(a-b+c+d)+(b-a+c+d)\sqrt{m}}{2}$

(5) $I_{e^{\imath(\pi-\theta)},1}(p,q) = a+b-d+d\sqrt{m}$

(6) $I_{e^{\imath(\pi-\theta)},e^{\imath\theta}}(p,q) = \frac{(a+b+c-d)+(a+b-c+d)\sqrt{m}}{2}$

Notice that if a, b have the same parity, then $a+b$, $a-b$, and $b-a$ are all even. Furthermore, if c is even, then $c+d$, $d-c$, and $c-d$ all have the same parity as d. Using these facts, we can confirm that the closed form of each of the six intersections above result in elements in H as long as p and q are elements in H.

This concludes the proof for the closure of the intersection operator. In other words, as long as our seed set starts with elements in H, then the intersections will also be in H. We can also express this claim as $R(S,U) \subset H$. It remains to be shown that any element in H is also an element in $R(S,U)$.

Let $\frac{a+b\sqrt{m}}{2}$ be an element in in H. Notice, that if we can construct $\frac{b\sqrt{m}}{2}$ and $\frac{(2+b)\sqrt{m}}{2}$ by starting at S, and we can construct $\frac{a}{2}$ by starting at S, then we can construct $\frac{a+b\sqrt{m}}{2}$ by starting at

$$\left\{\frac{b\sqrt{m}}{2}, \frac{(2+b)\sqrt{m}}{2}\right\}$$

We can further reduce the problem by showing that given points

$$\left\{\frac{n+k\sqrt{m}}{2}, \frac{n+2+k\sqrt{m}}{2}\right\}$$

we can construct both $\frac{n-2+k\sqrt{m}}{2}$ and $\frac{n+4+k\sqrt{m}}{2}$, and that given

$$\left\{\frac{n+k\sqrt{m}}{2}, \frac{n+2+k\sqrt{m}}{2}\right\}$$

we can construct both $\frac{n+1+(k-1)\sqrt{m}}{2}$ and $\frac{n+1+(k+1)\sqrt{m}}{2}$. We will now construct the desired points using the appropriate reference points.

Constructing $\frac{n+1+(k-1)\sqrt{m}}{2}$: Consider

$$I_{e^{\imath\theta},e^{\imath(\pi-\theta)}}\left(\frac{n+k\sqrt{m}}{2}, \frac{n+2+k\sqrt{m}}{2}\right)$$

By applying case (4) from above, we see that

$$I_{e^{\imath\theta},e^{\imath(\pi-\theta)}}\left(\frac{n+k\sqrt{m}}{2}, \frac{n+2+k\sqrt{m}}{2}\right) = \frac{n+1+(k-1)\sqrt{m}}{2}$$

Constructing $\frac{n+1+(k+1)\sqrt{m}}{2}$: Consider

$$I_{e^{\imath(\pi-\theta)},e^{\imath\theta}}\left(\frac{n+k\sqrt{m}}{2}, \frac{n+2+k\sqrt{m}}{2}\right)$$

By applying case (6) from above, we see that

$$I_{e^{\imath(\pi-\theta)},e^{\imath\theta}}\left(\frac{n+k\sqrt{m}}{2}, \frac{n+2+k\sqrt{m}}{2}\right) = \frac{n+1+(k+1)\sqrt{m}}{2}$$

Constructing $\frac{n-2+k\sqrt{m}}{2}$: Consider

$$I_{e^{\imath\theta},1}\left(I_{1,e^{\imath(\pi-\theta)}}\left(\frac{n+1+(k+1)\sqrt{m}}{2}, \frac{n+k\sqrt{m}}{2}\right), \frac{n+k\sqrt{m}}{2}\right)$$

By applying case (1) from above, we can reduce the previous expression to

$$I_{e^{\imath\theta},1}\left(\frac{n-1+(k+1)\sqrt{m}}{2}, \frac{n+k\sqrt{m}}{2}\right)$$

We further reduce the expression using case (5) from above. The result is

$$I_{e^{\imath\theta},1}\left(\frac{n-1+(k+1)\sqrt{m}}{2}, \frac{n+k\sqrt{m}}{2}\right) = \frac{n-2+k\sqrt{m}}{2}$$

Constructing $\frac{n+4+k\sqrt{m}}{2}$: Consider

$$I_{e^{\imath(\pi-\theta)},1}\left(I_{1,e^{\pi\theta}}\left(\frac{n+1+(k+1)\sqrt{m}}{2}, \frac{n+2+k\sqrt{m}}{2}\right), \frac{n+2+k\sqrt{m}}{2}\right)$$

By applying case (5) from above, we can reduce the previous expression to

$$I_{e^{\imath(\pi-\theta)},1}\left(\frac{n+3+(k+1)\sqrt{m}}{2}, \frac{n+2+k\sqrt{m}}{2}\right)$$

We further reduce the expression using case (1) from above. The result is

$$I_{e^{\imath(\pi-\theta)},1}\left(\frac{n+3+(k+1)\sqrt{m}}{2}, \frac{n+2+k\sqrt{m}}{2}\right) = \frac{n+4+k\sqrt{m}}{2}$$

With this we have shown that

$$\{\frac{a+b\sqrt{m}}{2} : a, b \in \mathbb{Z}, a \equiv b \mod 2\} \subset R(S,U)$$

completing the proof.

□

3. Putting It All Together

In figure 5.1 we see that when we use $U = \{1, \imath, e^{\imath\theta}\}$ as our angle set, then the origami ring grows into the first and third quadrants, and bleeds into the others. In figure 5.2 we see that when we use $U = \{1, e^{\imath\frac{\pi}{4}}, e^{\imath\frac{3\pi}{4}}\}$ as our angle set, then the origami ring grows along the real line, and slowly bleeds into the rest of the complex plane. Of course, $R(S, U)$ is assumed to be closed under the intersection operator, so the growth pattern doesn't matter in an abstract sense. However, computationally, it means that the number of steps it takes to construct a point is not related to that point's modulus. In fact, we get an entirely different measure of distance if we only consider the number of steps it takes to generate a point.

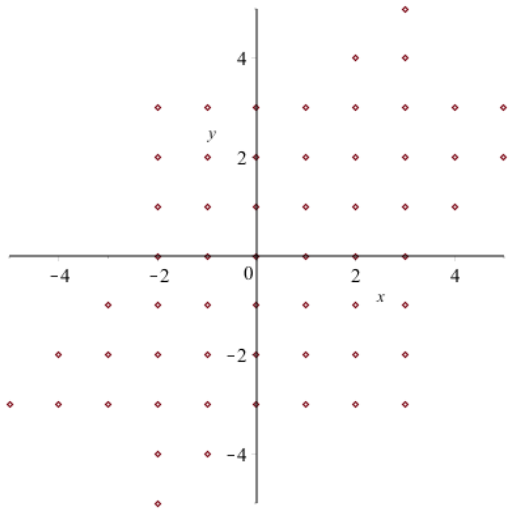

FIGURE 5.1. This graph depicts the first 5 generations of origami points using $U = \{1, \imath, e^{\imath\frac{\pi}{4}}\}$

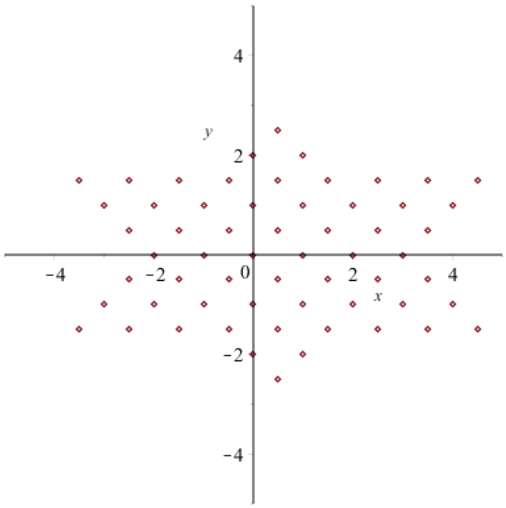

FIGURE 5.2. This graph depicts the first 5 generations of origami points using $U = \{1, e^{\imath\frac{\pi}{4}}, e^{\imath\frac{3\pi}{4}}\}$

Since lemmas 5.1 and 5.2 are just the two cases of theorem 5.1, the proof of the theorem easily follows.

THEOREM 5.1. Let $m < 0$ be a squarefree integer. The set of algebraic integers in the quadratic field $\mathbb{Q}(\sqrt{m})$ is $R(S, U)$ where

$$U = \{1, \imath, e^{\imath\theta}\} \text{ if } m \equiv 2 \text{ or } 3 \mod 4$$

$$U = \{1, e^{\imath\theta}, e^{\imath(\pi-\theta)}\} \text{ if } m \equiv 1 \mod 4$$

Q.E.D.

Bibliography

[1] Joe Buhler, Steve Butler, Warwick de Launey, Ron Graham *Origami rings*, arXiv: 1011.2769v.1 [math.CO] 11 Nov. 2010.

[2] Gallian, Joseph A.. (2010). *Contemporary Abstract Algebra*, 7ed. Brooks/Cole

[3] Marcus, Daniel A..(1997). *Number Fields*. New York, New York: Springer Verlag.

[4] Brown, James W. and Churchill, Ruel V..(2004). *Complex Variables and Applications*. New York, New York: McGraw-Hill.