GEOMETRIC CONSTRUCTIONS AND ALGEBRAIC FIELD EXTENSIONS

JENNY WANG

Abstract. In this paper, we study field extensions obtained by polynomial rings and maximal ideals in order to determine whether solutions exist to three ancient Greek construction problems: squaring the circle, doubling the cube, and trisecting an angle.

Contents

1. Introduction

Much of Ancient Greek mathematics was based in geometry. One particular point of interest was determining which geometric elements could be constructed using only an unmarked straightedge and a compass. It is a quick classroom exercise, for example, to construct congruent circles and perpendicular lines. The constructibility of some other elements, however, is less immediate. Can we construct a square with the same area as any given circle? Given a cube, can we construct a second cube with twice the volume? Can we trisect any given angle? To answer these questions, we turn to the study of algebraic structures.

Given the geometric nature of the Greek construction problems, it is understandable if the motivation for studying polynomial rings and field extensions is not entirely apparent. The aim of this paper, however, is to build a fundamental understanding of polynomial rings, maximal ideals, and algebraic extensions in order to determine the possibility (or impossibility) of certain constructions without having to explicitly construct the elements themselves.

We begin by proving some relevant results about principal ideal domains and polynomial division. In the next few sections, we will determine how to construct and classify field extensions before finally revisiting the geometric construction problems.

It should be noted that discussion of rings in this paper will be restricted to commutative rings. Imposing this condition does not detract from the validity of the results eventually obtained and simplifies notation for the reader.

2. Principal Ideal Domains and Polynomial Division

We begin with some important properties of polynomial rings and integral domains. The reader is assumed to be familiar with the conventional notion of long division of polynomials. Given any polynomial as our dividend, we know how to divide it by a non-zero polynomial to get a quotient and remainder. With a restriction only on the degree of the remainder, the Division Algorithm ensures both the existence and uniqueness of the quotient and remainder. We can thus formalize the basic polynomial division with the following theorem:

Theorem 2.1 (Division Algorithm)**.** *Let F be a field and f and g polynomials in $F[x]$, where g is non-zero. Then there exist unique q, r also in $F[x]$ such that*

(1) $f(x) = q(x)g(x) + r(x)$ *and*
(2) $\deg(r) < \deg(g)$

This theorem will prove to be crucial in proving many useful results about principal ideal domains and field extensions. Suppose, for example, we are given any two polynomials f and g in a polynomial ring $F[x]$, where g is non-zero. The Division Algorithm guarantees the existence of two more polynomials q and r so that f can be written as the product of q and g, plus a remainder r.

In the special case that the remainder has degree zero, then we say that f is a multiple of g. This basic idea is the conceptual foundation of our discussion of principal ideal domains, as principal ideals in $F[x]$ consist of nothing more than multiples of a given polynomial.

We claim that for any field F, the polynomial ring $F[x]$ is a principal ideal domain - meaning every ideal in the ring $F[x]$ is a principal ideal. The proof relies on the existence of a division algorithm in $F[x]$.

Theorem 2.2. *Let F be a field. For any ideal I in $F[x]$, $I = (a(x))$ for some $a(x) \in F[x]$*

Proof. If $I = \{0\}$, we have that $I = (0)$ so $a(x)$ is the zero polynomial and $I = (a(x))$.

Now consider when $I \neq \{0\}$. We claim that I is generated by a polynomial of minimal degree in the ideal, call it $a(x)$. Note that the existence of a polynomial with minimal degree is guaranteed by the Well-Ordering Principle. Now, because $I \neq \{0\}$, $a(x)$ is not the zero polynomial. By Theorem 2.1, for any $f(x) \in I$, there exist unique $q(x), r(x) \in F[x]$ such that $f(x) = q(x)a(x) + r(x)$ where $\deg(r(x)) < \deg(a(x))$.

Rearranging, we get

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

As $f(x)$ and $a(x)$ are both in the ideal, it follows that $r(x) \in I$ as well. However, by the condition on degree of r by the division algorithm and the minimality of the degree of $a(x)$, it must be that $r(x)$ is the zero polynomial. Hence for any $f \in I$,

$f(x) = q(x)a(x)$ for some $q(x) \in F[x]$. Therefore $I = (a(x))$ for any ideal I in $F[x]$. □

Once it is established that every ideal in a given ring is generated by a single element, there arises an important correspondence between prime and maximal ideals. Given a prime ideal (p) in a principal ideal domain, we will show there are no proper ideals that contain (p) except (p) itself - meaning it is by definition a maximal ideal.

Theorem 2.3. *In a principal ideal domain, every prime ideal is maximal.*

Proof. Consider a prime ideal I of a ring R. If R is a principal ideal domain, then $I = (p)$ for some $p \in R$. In order to show that (p) is maximal, it is sufficient to show that any ideal containing (p) is either (p) itself or the entire ring R.

So let (m) be an ideal containing (p). Then $p = m \cdot r$ for some $r \in R$. As (p) is prime, either $m \in (p)$ or $r \in (p)$. In the case that $m \in (p)$, we have that $(m) \subset (p)$ and $(m) \supset (p)$, so $(m) = (p)$.

In the case that $r \in (p)$, then we have $r = s \cdot p$ for some element s in the ring R. Substituting, we can see that $r = s \cdot (m \cdot r)$ so $1 = s \cdot m$. Then 1 is in the ideal (m), so (m) is necessarily the entire ring. We have thus shown that there do not exist any proper ideals of R containing (p) a prime ideal, and hence it is maximal. □

3. Field Extensions

This discussion of polynomial rings, maximal ideals, and fields is motivated by the existence of polynomials with no roots in a given field. In general, given a polynomial $p(x)$ in the ring $F[x]$ for any given field F, does there exist a solution to $p(x) = 0$ that lies in F? If not, does there exist a field extension of F in which $p(x) = 0$ has a solution?

Consider the classic example: the polynomial $x^2 + 1 = 0$ has no solutions over $\mathbb{R}$. It is easy to see that there are no numbers in $\mathbb{R}$ that satisfy this equation - but over the complex numbers, both i and $-i$ are solutions. It is also crucial to notice that the complex numbers, conventionally of the form $a + bi$, contain a “copy” of the real number line - namely, when $b = 0$.

These concepts are generalized and formalized in this section. Given any polynomial with no roots over a given field, we would like to be able to construct a field extension that both contains solutions to the equation and preserves the structure of the original field.

Definition 3.1. Let K be a field. A **subfield** of K is a subset F of K that is closed under the field operations of K. The larger field K is said to be a **(field) extension** of F.

We would like now to use the fact that a polynomial ring $F[x]$ is a principal ideal domain in order to discuss the construction of field extensions.

Theorem 3.2. *Let R be a ring and I an ideal of R. Then I is maximal if and only if R/I is a field.*

The proof for this theorem follows from two important results: one is a characterization of fields of having only trivial ideals and the other is a correspondence that exists between ideals of a ring R containing an ideal I and ideals of the quotient group R/I. The first result is simply a consequence of the fact that every nonzero element in a field is a unit. The second result is precisely the Lattice Isomorphism Theorem for rings.

Proposition 3.3. *A ring R is a field if and only if the only ideals of R are $\{0\}$ and R.*

Proof. Suppose that R is a field. Note that $\{0\}$ is always an ideal of any ring, so $\{0\}$ is an ideal of R. By definition of a field, every nonzero element of R is a unit, so every non-zero ideal contains a unit. 1 generates the entire ring, so the only nonzero ideal is the entire ring R.

Now suppose that the only ideals of R are $\{0\}$ and R. Let an element $a \in R$ be nonzero. Then the ideal generated by a is R by assumption: $(a) = R$. An ideal is the whole ring if and only if the unit is in the ideal, so $1 \in (a)$, which means there exists an element $b \in R$ such that $ab = 1$. Then it follows that a is a unit. As every nonzero element in R is a unit, it must be that R is a field. □

Proposition 3.4 (Lattice Isomorphism Theorem)**.** *Let I be an ideal of a ring R. There exists an inclusion-preserving bijection between ideals of R containing I and the ideals of the quotient group R/I.*

With these two results, the proof of Theorem 3.2 follows with straightforward application of definitions and these propositions.

Proof. Let I be a non-zero maximal ideal of R. Suppose, for contradiction, that there exists a proper ideal J/I of R/I, so $J/I \subset R/I$. Then by the Lattice Isomorphism Theorem, there exists corresponding ideal J of R containing I. By assumption, $J/I \neq R/I$ so $J \neq R$. Then J is a proper ideal of R containing I. This contradicts the fact that I is maximal. It must be that there are no proper ideals of R/I. Hence if I is maximal, the only ideals of R/I are $\{0\}$ and the entire quotient ring R/I, so R/I is a field.

Now suppose R/I is a field, where I is an ideal of R. Then its only ideals are $\{0\}$ and the whole quotient ring R/I. Again, by Lattice Isomorphism Theorem, there exists a single corresponding non-zero ideal J such that $I \subset J \subset R$. The correspondence from the Isomorphism Theorem, however, implies that J must be the entire ring R, so there are no proper ideals of R that contain I except I itself. Hence I is a maximal ideal. □

The quotient ring corresponding to a maximal ideal of a ring, therefore, is a field. We now return to the original motivation of the section in order to examine what the maximal ideals of a polynomial ring look like. The example we considered was a question about whether a polynomial had roots in a given field - namely, whether we could factor $p(x)$ into linear factors. More generally, however, we can consider irreducible polynomials to be polynomials in $F[x]$ that cannot be written as the product of two non-constant polynomials with coefficients also in F. Irreducible polynomials over a polynomial ring $F[x]$ necessarily do not have roots in F, as that would require the polynomial to be able to be decomposed into at least one linear factor.

Consider now the ideal generated by an irreducible polynomial $p(x)$. This ideal consists of all the multiples of $p(x)$, which factor uniquely into $p(x)q(x)$ for $q(x)$ in the ring. Note that the uniqueness of the factorization comes from the irreducibility of $p(x)$. Then by definition, the ideal $(p(x))$ is prime. From this observation and Theorem 2.3, the following theorem is immediate:

Theorem 3.5. *For $p(x)$ an irreducible polynomial in $F[x]$, $(p(x))$ is a prime ideal. As $F[x]$ is a principal ideal domain, it follows that $(p(x))$ is a maximal ideal.*

Corollary 3.6. *For an irreducible polynomial $p(x) \in F[x]$, the quotient ring $F[x]/(p(x))$ is a field.*

To find a root to the polynomial $p(x)$ in K, let $\theta := x \mod p(x)$. It is clear that θ is an element of K. We see that θ is always going to be a root of $p(x)$ in K:

$$\begin{aligned} p(\theta) &= p(x) \mod p(x) \\ &\equiv 0 \pmod{p(x)} \end{aligned}$$

Corollary 3.7. *Let $p(x)$ be an irreducible polynomial in $F[x]$ for any field F. Then $K := F[x]/(p(x))$ is a field extension of F containing a root of $p(x)$*

We have thus shown the existence of a field in which the multiples of $p(x)$ are sent to $0 \in K$. It is true, then, that $p(x)$ has a root in this new field. However, the objective set forth in the beginning of this section was two-fold: the field we are looking for must also preserve the original structure of F. In order to verify that K is indeed a field extension that satisfies both conditions, it is necessary to check that K contains an isomorphic copy of F. To do this, we need only the following theorem:

Proposition 3.8. *Let F, K be fields. A field homomorphism $\varphi : F \to K$ is either injective or identically zero.*

To see the validity of this statement, consider the kernel of a homomorphism. From the first isomorphism theorem, we know that $ker(\varphi)$ is an ideal of F. By Proposition 3.3 the only ideals of a field are $\{0\}$ and the entire field, which correspond to the image being injective and identically zero, respectively.

The homomorphism φ is not identically zero, as it must map the identity of F to the identity of K, thus it is an injective map. K contains an isomorphic copy of F. Again, in the example of the complex numbers $\mathbb{C}$, the reals are all the complex numbers $a + bi$ with $b = 0$.

Thus the field constructed with the ideal generated by an irreducible polynomial satisfies both criteria originally set forth: the new field now contains (1) a root polynomial $p(x)$ and (2) an isomorphic copy of the original field F.

It is useful to view the field extension as a vector space over the original field. Because F is a subfield of K and K is a field itself, we have that K is closed under both addition and multiplication by scalars from base field F. From this, we can quantify the "size" of a field extension:

Definition 3.9. Let K be a field extension of base field F. Then the **degree** of a field extension, denoted $[K : F]$, is the dimension of the vector space K over F.

So if we can find a basis for K, then we would be able to better conceptualize what the elements in K look like, as everything in K could be written as a linear combination of the elements in the basis.

Theorem 3.10. *Let $p(x) \in F[x]$ be an irreducible polynomial of degree n over F, call it K. Let $\theta := x \mod p(x)$. Then*

$$1, \theta, \theta^2, ..., \theta^{n-1}$$

form a basis of K as a vector space over F. Then the elements of K can be expressed as polynomials in θ:

$$K = \{a_0 + a_1\theta + ... + a_{n-1}\theta^{n-1}\big|a_0, a_1, ..., a_{n-1} \in F\}$$

Proof. To check that $1, \theta, \theta^2, ..., \theta^{n-1}$ span K, consider $a(x) \in F[x]$. The Division Algorithm ensures the existence of unique $q(x), r(x) \in F[x]$ such that

$$a(x) = q(x)p(x) + r(x)$$

where $\deg r(x) < n$. By this, $a(x) \equiv r(x) \pmod{p(x)} \in K$. By the degree restriction on r, we know that r can be written as a linear combination of $1, x, x^2, ..., x^{n-1}$ - whose images are precisely $1, \theta, \theta^2, ..., \theta^{n-1}$. Hence any element in K can be written as a linear combination of powers of θ less than n.

Now we must check that $1, \theta, \theta^2, ..., \theta^{n-1}$ are linearly independent. Suppose there exist $b_0, b_1, ..., b_{n-1} \in F$ such that

$$b_0 + b_1\theta + ... + b_{n-1}\theta^{n-1} = 0$$

Equivalently,

$$b_0 + b_1x + ... + b_{n-1}x^{n-1} \equiv 0 \pmod{p(x)}$$

This is equivalent to saying that $p(x)$ divides the polynomial on the left hand side. This cannot be the case for nontrivial coefficients, however, as the polynomial $p(x)$ is of degree n and the left hand side polynomial is of lower degree. Thus all coefficients $b_0, b_1, ..., b_{n-1}$ must be 0, and so the powers of θ are linearly independent.

The set $\{1, \theta, \theta^2, ...\theta^{n-1}\}$ span K and are linearly independent, so they form a basis for K. □

The key to the proof of the previous theorem is understanding the relationship between an element and its image under the field homomorphism that sends an element $x \in F$ to $x \mod p(x) \in K$.

Note that when $p(x) \in F[x]$ is degree n, then the degree of the extension $[K : F]$ is also n.

4. Algebraic Extensions

We would like now to consider field extensions from a slightly different (but fundamentally related) point of view. In the previous section, we constructed a field by taking the quotient of a polynomial ring by an irreducible polynomial. Now we want to extend a field by adjoining F a subfield of K with a single element $\alpha \in K$. We can think of this action in terms of the intersection of fields, since the intersection of subfields is still a subfield. Of all the intersections of fields containing F and fields containing α, we denote $F(\alpha)$ to be the smallest field extension of F containing both F and α. Given that we can adjoin a subfield F with an element of K, what is relationship of this field extension to the ones discussed in the previous section? It would make sense to begin by considering a polynomial $p(x)$ for which α is a root.

Definition 4.1. Let α be an element in K. We say that α is **algebraic** over F if α is the root of some nonzero polynomial $p(x)$ in $F[x]$. Otherwise, we say that α is **transcendental**.

An extension K/F is said to be algebraic if every element in K is algebraic over F. Here is precisely the correspondence between field extensions and the smallest field containing the subfield F and an element α of the larger field K. In fact, the field $F(\alpha)$ is related to $p(x)$ as described in the following theorem:

Theorem 4.2. *Let $p(x)$ be an irreducible polynomial in $F[x]$ and let $\alpha \in K$ be a root of $p(x)$. Then $F(\alpha) \cong F[x]/(p(x))$.*

This statement requires little more than a surprisingly general condition on polynomials and their roots - it does not specify anything about α beyond the fact that α satisfies $p(x)$. Therefore, the theorem is a statement about an isomorphism that exists between the field $F/(p(x))$ and $F(\alpha)$ for *any* root of the polynomial $p(x)$.

Also note that if α is a root of a polynomial $p(x)$, it is also a root of all multiples of $p(x)$. In order to avoid issues with multiplicity, we would like to consider a polynomial of minimal degree for which α is a root.

Proposition 4.3. *Let F be a subfield of K. Let $\alpha \in K$ be algebraic over F. Then there exists a unique monic irreducible polynomial of minimal degree $m(x) \in F[x]$ such that $m(x)$ divides $a(x)$ if and only if $a(\alpha) = 0$. That is, the minimal polynomial of α exists and divides any polynomial with α as a root.*

Proof. Let $m(x)$ be a polynomial of minimal degree satisfying $m(\alpha) = 0$.

Suppose $m(x)$ divides a polynomial $a(x) \in F[x]$. Then $a(x) = m(x)q(x)$ for some $q(x) \in F[x]$. Evaluation of this equation at α gives us:

$$a(\alpha) = m(\alpha)q(\alpha) = 0 \cdot q(\alpha) = 0$$

.

Now suppose that a polynomial $a(x)$ has α as a root. Dividing by $f(x)$, we have that there exist $q(x), r(x) \in F[x]$ such that

$$a(x) = m(x)q(x) + r(x)$$

Evaluating at α,

$$\begin{aligned} a(\alpha) &= m(\alpha)q(\alpha) + r(\alpha) \\ 0 &= 0 \cdot q(\alpha) + r(\alpha) \\ 0 &= r(\alpha) \end{aligned}$$

The degree of $r(x)$ must be strictly less than the degree of $m(x)$, by the Division Theorem, so it must be that $r(x)$ is the zero polynomial, else it would contradict the minimality of the degree of $m(x)$. It follows that $a(x)$ is divisible by $m(x)$. □

By scaling by a constant, we can ensure that the polynomial of minimal degree satisfying $m(\alpha) = 0$ is monic, and thus unique. This is precisely the minimal polynomial of α over F, denoted $m_{\alpha,F}(x)$. Now when discussing an algebraic element of a field extension, we can talk about *the* corresponding (minimal) polynomial over the base field. Additionally, the degree of the minimal polynomial of α corresponds to the degree of the smallest field extension containing both F and α - which matches the definition given in the introduction.

Proposition 4.4. *Let F be a field and α be algebraic over F. Then $F(\alpha)$ is isomorphic to $F[x]/(m_{\alpha,F}(x))$.*

Proof. Consider the map $\psi : F[x] \to F(\alpha)$ that takes a polynomial $f(x)$ to its evaluation $f(\alpha)$. It is easy to check that ψ is a homomorphism and

$$\ker \psi = \{a(x) \in F[x] \mid a(\alpha) = 0\}$$

From the previous proposition, $a(\alpha) = 0$ if and only if the minimal polynomial divides $a(x)$. So the kernel is the set of multiples of $m_{\alpha,F}(x)$. Hence it is the ideal generated by the minimal polynomial. By the first isomorphism theorem, for any ring homomorphism $\sigma : R \to S$, we have that $\operatorname{Im} \sigma \cong R/\ker \sigma$. Then

$$\operatorname{Im} \psi \cong F[x]/\ker \psi = F[x]/(m_{\alpha,F}(x))$$

Note that every evaluation is just the image of a polynomial $f(x) \in F[x]$, so the homomorphism ψ is surjective - hence the image of ψ is $F(\alpha)$ and thus $F(\alpha)$ is isomorphic to $F[x]/(m_{\alpha,F}(x))$. □

From this, it follows directly from Theorem 3.10 that the degree of the minimal polynomial is the degree of the field extension:

$$\deg m_{\alpha,F}(x) = [F[x]/(m_{\alpha,F}(x)) : F] = [F(\alpha) : F]$$

Theorem 4.5. *Let F, K, L be fields such that $F \subseteq K \subseteq L$. Suppose that $[L : K], [K : F] < \infty$. Then*

$$[L : F] = [L : K][K : F]$$

Proof. By Definition 3.9, we know that L is a vector space over K. Let $[L : K] = m$, where $m < \infty$. So given any element $\alpha \in L$,

$$\alpha = \beta_0 + \beta_1 a_1 + ... + \beta_{m-1} a_{m-1}$$

for $\beta_0, \beta_1, ..., \beta_{m-1} \in K$ where the $\{a_0, a_1, ..., a_{m-1}\}$ is any given basis for L. Each β_i, however, is an element of K, which is a vector space over F. Let $[K : F] = n$, where $n < \infty$. Then for any $\beta_i \in K$,

$$\beta_i = \sigma_{i,0} + \sigma_{i,1} b_{i,1} + ... + \sigma_{i,n-1} b_{i,n-1}$$

where $\sigma_{i,j} \in F$. Then $\alpha \in L$ can be written as a linear combination with coefficients in F.

$$\begin{aligned}
\alpha = &\left(\sigma_{0,0} + ... + \sigma_{0,n-1} b_{0,n-1}\right) \\
&+ \left(\sigma_{1,0} + ... + \sigma_{1,n-1} b_{1,n-1}\right) a_1 \\
&\ddots \\
&+ \left(\sigma_{m-1,0} + ... + \sigma_{m-1,n-1} b_{m-1,n-1}\right) a_{m-1}
\end{aligned}$$

From this, we see that L is a vector space over F for which there are mn elements in the basis. Hence $[L : F] = m \cdot n = [L : K][K : F]$. □

5. Impossibility of Geometric Constructions

We now return to the original motivation of the paper, the Greek compass and straightedge construction problems. The goal of this section is to find the correspondences between geometric constructions and algebraic concepts in order to prove the possibility (or impossibility) of certain constructions.

The premise of the compass and straightedge problems is quite simple. Given two points $\{0, 1\}$, unit length is defined to be the shortest distance between the two points. From this, there are then three operations that can be performed to obtain new points:

(1) Connecting two existing points with a straight line
(2) Tracing out a circle with given radius and center
(3) Connecting points where any line(s) or circle(s) intersect

It should be noted that the straightedge is unmarked, but the compass can be used to transfer one length at a time (the compass does not collapse once removed from the surface).

- Given length 1, the length 2 is constructible. It is immediate, by inductive process, that any natural number is also constructible.
- Given that two lengths α, β are constructible, we can also construct $\alpha + \beta$ and $\alpha - \beta$.
- Once we construct parallel lines, we can use similar triangles to construct $\alpha\beta$ and α/β.
- By inscribing a right triangle in a semi-circle, we can also construct square roots of any given length

By these facts, the constructible lengths up until this point are a field, as the set of constructible lengths is closed under addition and multiplication, and every non-zero element is a unit.

In particular, we can think of the construction space as the Cartesian plane - a length, therefore, can be thought of as a correspondence between distance in $\mathbb{R}^2$ and the real numbers. Hence the constructible elements compose some subfield of $\mathbb{R}$ that at least contains $\mathbb{Q}$.

Definition 5.1. A length r is **constructible** if, given two initial points $\{0, 1\}$, it can be constructed through a finite sequence of operations

$$0, 1, r_1, r_2, ..., r_{n-1}, r_n = r$$

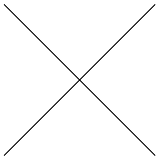
where r_i is the length constructed with the i^{th} operation.

The sequence of constructions can be thought of as a sequence of field extensions whose base field is at least $\mathbb{Q}$, as we showed in the examples above that $\mathbb{Q}$ is constructible. The tower of field extensions would then be:

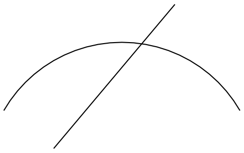
$$\mathbb{Q} \subseteq \mathbb{Q} \subseteq \mathbb{Q}(r_1) \subseteq \mathbb{Q}(r_1, r_2) \subseteq ... \subseteq \mathbb{Q}(r_1, r_2, ..., r_n)$$

To simplify notation, let $\mathbb{Q}(r_1, ..., r_n) =: F_n$.

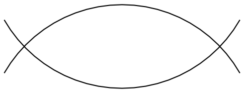
At the k^{th} step in the sequence r_k, we would like to determine whether the construction of a new point extends the field of constructible elements - and if so, by how much? In other words, what is the degree of the field extension F_{k+1} over F_k? We can approach this from a case-by-case basis:



- Intersection of two lines
$$ax + by - c = 0$$
$$dx + ey - f = 0$$
Let F be a field. For $a, b, c, d, e, f \in F$, the solution set (x, y) will also be in F, as it is a system of linear equations.



- Intersection of a line and a circle
$$(x - a)^2 + (y - b)^2 - c^2 = 0$$
$$dx + ey - f = 0$$
Solving for x and y will give either a quadratic expression or a linear expression, depending on the coefficients $a, b, c, d, e, f \in F$.



- Intersection of two circles
$$(x - a)^2 + (y - b)^2 - c^2 = 0$$
$$(x - d)^2 + (y - e)^2 - f^2 = 0$$
Here we can subtract one equation from the other so that the quadratic factors cancel in one of the two equations. Hence it is reduced to the previous case (intersection of a line and a circle).

In the first case, the solution set (x, y) remains in F, so the degree of the extension is 1: $[F_{k+1} : F_k] = 1$. In the second and third cases, if one variable is written in terms of the other, we are left with a quadratic polynomial in the second variable. Adding a point by taking the intersection of a line and a circle, therefore, could be at most a quadratic extension, meaning $[F_{k+1} : F_k]$ is either 1 or 2.

Lemma 5.2. *Let F_i denote the field at the i^{th} iteration of adding points to the base field (as described in Definition 5.1). Then $[F_{i+1} : F_i] \leq 2$.*

This lemma, along with Theorem 4.5, which relates the degrees of intermediate field extensions, gives us the following proposition immediately:

Proposition 5.3. *If r_n is constructible, then $[\mathbb{Q}(r_1, r_2, ..., r_n) : \mathbb{Q}] = 2^k$ for some $k \leq n \in \mathbb{N}$*

Corollary 5.4. *If r_n is constructible, then $[\mathbb{Q}(r_n) : \mathbb{Q}] = 2^m$ for some $m \leq n \in \mathbb{N}$.*

This follows almost immediately from Proposition 5.3 and Theorem 4.5, as

$$[\mathbb{Q}(r_1, ..., r_n) : \mathbb{Q}] = 2^k = [\mathbb{Q}(r_1, ..., r_n) : \mathbb{Q}(r_n)][\mathbb{Q}(r_n) : \mathbb{Q}]$$

With algebraic field extensions and minimal polynomials in mind, we consider the tasks of doubling the cube, trisecting an angle, and squaring the circle.

5.1. **Squaring the Circle.** Given a circle of fixed radius r, is it possible to construct a square with the same area as the circle? Equivalently, is it possible to construct a square with area $2\pi r$ for any $r > 0$? As the base field $\mathbb{Q}$ closed under multiplication, we need only consider whether π is constructible. Notice, however, that π is transcendental over $\mathbb{Q}$, meaning there does not exist a polynomial in $\mathbb{Q}[x]$

for which π is a root. It follows, then, that there does not exist a minimal polynomial for π over $\mathbb{Q}$, so $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$. By Proposition 5.3, π is not constructible - hence the task of squaring the circle is impossible with just a straightedge and compass.

5.2. **Doubling the Cube.** Given a cube of fixed edge length $a \in \mathbb{Q}$, is it possible to construct a cube with twice the volume? That is, given a length $a > 0$, can a cube be constructed so that each edge is of length $a\sqrt[3]{2}$? To determine the answer to this, consider $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$.

Note that $\sqrt[3]{2}$ is algebraic over $\mathbb{Q}$, as it is the solution to the polynomial $p(x) = x^3 - 2$. It can be checked that the minimal polynomial of $\sqrt[3]{2}$ is precisely $p(x)$, as it is the unique monic polynomial of minimal degree for which $p(\sqrt[3]{2}) = 0$. Then the degree of $\sqrt[3]{2}$ is 3, so it follows that

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$$

This is not a power of 2, so by Proposition 5.3, then $\sqrt[3]{2}$ is not constructible with a straightedge and compass. Hence the task of doubling the cube is impossible.

5.3. **Trisecting an Angle.** Given an angle θ between two lines, is it possible to trisect the angle? In other words, given a non-negative angle θ, is it possible to construct the angle $\frac{\theta}{3}$?

If such a construction were possible, we should be able to trisect any angle, given the original angle. Consider $\theta = 60^\circ$. Suppose now that we are given the task of constructing $\theta' = 20^\circ$. In our all the previous discussion, we were concerned only with constructing lengths, not angles. An angle x is constructible, however, if and only if $\sin x$ and $\cos x$ are both constructible. Determining the constructibility of lengths $\sin\theta'$ and $\cos\theta'$, therefore, will determine whether we can construct θ'.

With trigonometric identities relating sums of angles, we can derive the following relation for any angle x:

$$\cos 3x = 4(\cos x)^3 - 3\cos x$$

For $x = 20$, we have:

$$\frac{1}{2} = \cos 60 = 4(\cos 20)^3 - 3\cos 20$$

If we let $\alpha = \cos 20$, this identity gives a monic polynomial with rational coefficients for which $p(\alpha) = 0$:

$$p(x) := x^3 - \frac{3}{4}x - \frac{1}{8}$$

Thus the angle θ' can be constructed if and only if the field extension $\mathbb{Q}(\alpha)$ has degree 2^k for some nonnegative k over $\mathbb{Q}$

Recall that $\mathbb{Q}(\alpha) \cong \mathbb{Q}(x)/(p(x))$ for α a root of $p(x)$, and the degree of α is the degree of the minimal polynomial of α over $\mathbb{Q}[x]$. If $p(x)$ is irreducible, then it is necessarily the minimal polynomial for $\alpha = \cos\theta'$ over $\mathbb{Q}$. The details are omitted from this paper, but with some basic results about degree three polynomials in $\mathbb{Q}[x]$, it is straightforward to show that $p(x)$ is indeed irreducible over $\mathbb{Q}$.

We have shown, then, that α is of degree 3 over $\mathbb{Q}$, so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, which clearly is not a power of 2. By Theorem 5.3, the angle $\theta' = 20^\circ$ in particular is not constructible from $\theta = 60^\circ$, so it is not possible to trisect any given angle θ given only a straightedge and compass.

We conclude, therefore, that all three of the aforementioned construction problems are impossible given only a straightedge and compass. The results from our study of field extensions allow for an elegant approach to these ancient Greek construction problems. By viewing the constructible elements as a field extension over the rationals, we can consider just the degree of a field extension in order to determine whether an element is not constructible.

6. Acknowledgments

Endless thanks to my mentor, Claudio, for his patience, thoroughness, and guidance throughout the program. I appreciate his immeasurable patience in teaching me all the material and helping me work through the information of this paper. I would also like to thank Professor May and Professor Babai for organizing and teaching the REU - it has been phenomenal to spend the summer learning math.

References

[1] Dummit and Foote. Abstract Algebra, 3rd edition. Wiley, 2003