

# COMPASS AND STRAIGHTEDGE APPLICATIONS OF FIELD THEORY

SPENCER CHAN

ABSTRACT. This paper explores several of the many possible applications of abstract algebra in analysing and solving problems in other branches of mathematics, particularly applying field theory to solve classical problems in geometry. Seemingly simple problems, such as the impossibility of angle trisection or the impossibility of constructing certain regular polygons with a compass and straightedge, can be explained by results following from the notion of field extensions of the rational numbers.

## CONTENTS

1. Introduction	1
2. Fields	2
3. Compass and Straightedge Constructions	4
4. Afterword	8
Acknowledgments	8
References	8

## 1. INTRODUCTION

Trisecting the angle, doubling the cube, and squaring the circle are three famous geometric construction problems that originated from the mathematics of Greek antiquity. The problems were considered impossible to solve using only a compass and straightedge, and it was not until the 19th century that these problems were indeed proven impossible. Elementary geometric arguments alone could not explain the impossibility of these problems. The development of abstract algebra allowed for the rigorous proofs of these problems to be discovered. It is important to note that these geometric objects can be *approximated* through compass and straightedge constructions. Furthermore, they are completely constructible if one is allowed to use tools beyond those of the original problem. For example, using a marked ruler or even more creative processes like origami (i.e. paper folding) make solving these classical problems possible. For the purposes of this paper, we will only consider the problems as they were originally conceived in antiquity.

In this paper, we will first build up a basic understanding of field theory before moving onto its geometric applications. In section 2, we will start by defining two important algebraic objects, rings and field, and discussing their basic properties. In section 3, we will explore the applications of the theory in solving the classical geometric problems mentioned above.

---

*Date:* September 15, 2014.

## 2. FIELDS

**Definition 2.1** (Ring). A ring is a set  $R$  endowed with two binary operations  $+$  and  $\times$  called addition and multiplication. Together they respect the following axioms:

- (1)  $(R, +)$  forms an abelian group with identity denoted by 0.
- (2)  $\times$  is associative:  $x \times (y \times z) = (x \times y) \times z$  for all  $x, y, z \in R$ .
- (3) The distributive law holds:  
 $x \times (y + z) = (x \times y) + (x \times z)$  and  
 $(x + y) \times z = (x \times z) + (y \times z)$  for all  $x, y, z \in R$ .

If  $\times$  is commutative, then  $R$  is called a commutative ring. If there exists an element  $1 \in R$  such that  $1 \times x = x \times 1 = x$  for all  $x \in R$ , then the ring  $R$  is said to have an identity. All the rings we will work with in this paper will be commutative and have an identity.

**Theorem 2.2** (Rational Roots). *Let  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$  be a polynomial of degree  $n$  and an element of the ring  $\mathbb{Z}[x]$  so that each coefficient  $a_i$  is an integer. If  $p/q$  is a rational number where  $p$  and  $q$  are coprime and  $p/q$  is a root of  $f(x)$ , then  $p$  divides the constant term  $a_0$  and  $q$  divides the leading coefficient  $a_n$ .*

*Proof.* By the hypothesis  $p/q$  is a root, so we have

$$0 = f(p/q) = a_n (p/q)^n + a_{n-1} (p/q)^{n-1} + \dots + a_0.$$

Multiplying  $f(x)$  by  $q^n$  yields

$$0 = a_n p^n + a_{n-1} p^{n-1} q + \dots + a_0 q^n.$$

Through simple algebraic manipulation we find  $q$  divides  $a_n p^n$

$$a_n p^n = -q(a_{n-1} p^{n-1} + \dots + a_0 q^{n-1}).$$

The proposition states that  $p$  and  $q$  are relatively prime, so  $q$  must also divide  $a_n$ . We can similarly solve the equation for  $a_0 q^n$  to find  $p$  divides  $a_0$ .  $\square$

**Definition 2.3** (Field). A field is a commutative ring  $F$  containing the identity 1 not equal to 0 and where every non-zero element  $x \in F$  has a multiplicative inverse.

**Example 2.4.** Not all rings are fields. Fields possess multiplicative inverses, allowing for division—except for division by zero—whereas not all rings possess multiplicative inverses. The ring of polynomials  $\mathbb{R}[x]$  over the real numbers is not a field, as the element  $x$  does not have a multiplicative inverse— $1/x$  is not a polynomial, after all!

An important concept in field theory is the notion of extending a field so that it becomes a larger field by adding or *adjoining* elements to it.

**Definition 2.5** (Field extension). Let  $K$  be a field containing  $F$ .  $K$  is a field extension of  $F$  and is denoted  $K/F$ . This is read “ $K$  over  $F$ ”.

**Example 2.6.**  $\mathbb{Q}$ ,  $\mathbb{R}$ , and  $\mathbb{C}$  are all examples of fields, and specifically they are classified as number fields. A number field is any finite extension of the field  $\mathbb{Q}$  of rational numbers. We see rather obviously that  $\mathbb{R}$  is an extension field of  $\mathbb{Q}$ , and  $\mathbb{C}$  is an extension field of  $\mathbb{R}$ . Shortly we will define that extent, or the *degree*, to which the field is extended.

**Definition 2.7** (Algebraic element). Let  $K$  be a field extension of  $F$ . Let  $\alpha$  be an element of  $K$ . The element  $\alpha$  is algebraic over the field  $F$  if it is a root of a monic polynomial

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

where each coefficient  $a_i$  is an element of  $F$ . Note that  $f(\alpha) = 0$ .

**Definition 2.8** (Transcendental element). An element is transcendental over a field  $F$  if it is not algebraic over  $F$ , i.e. it is not the root of a polynomial in the form as shown above.

**Definition 2.9** (Irreducible polynomial for  $\alpha$  over  $F$ ). Let  $K$  be a field extension of  $F$ . Let  $\alpha$  be an element of  $K$  that is algebraic over  $F$ .  $f$  is the irreducible polynomial for  $\alpha$  over  $F$  if  $f$  is the lowest-degree monic polynomial in  $F[x]$  in which  $\alpha$  is a root.

**Definition 2.10** (Degree of a field extension). The degree of a field extension  $K/F$  is the dimension of  $K$  as a vector space over  $F$ . The degree is denoted by  $[K : F]$ .

**Example 2.11.**  $[\mathbb{C} : \mathbb{R}] = 2$ , since  $(1, i)$  is a basis for the complex numbers. However,  $\mathbb{R}$  extends  $\mathbb{Q}$  infinitely, i.e.  $[\mathbb{R} : \mathbb{Q}] = \infty$ . Such an extension is called a *transcendental extension*. We will encounter another important transcendental extension at the end of the paper.

**Lemma 2.12.** *Let  $K/F$  be a field extension.  $[K : F] = 1$  if and only if  $K = F$ .*

*Proof.* Let the dimension of  $K$  as a vector space over  $F$  be 1. For every nonzero element  $\alpha \in K$ ,  $\alpha$  will form an  $F$ -basis. If we choose 1 as a basis, then every element of  $K$  will be in  $F$ .  $\square$

**Theorem 2.13** (Multiplicativity of the degree). *Let  $F \subset K \subset L$  be a tower of fields. Then  $[L : F] = [L : K][K : F]$ . Consequently, the degrees  $[L : K]$  and  $[K : F]$  divide the degree  $[L : F]$ .*

*Proof.* Let  $V = (v_1, \dots, v_n)$  be a basis for  $L$  over  $K$ , and let  $U = (u_1, \dots, u_m)$  be a basis for  $K$  over  $F$ . From the definition of degree of a field extension, we have  $[L : K] = n$  and  $[K : F] = m$ . We wish to show  $W = (v_i u_j)$  is a basis for  $L$  over  $F$ . Consider the element  $l \in L$ . Since  $V$  is a basis for  $L$  over  $K$ , we can write  $l$  as a linear combination

$$l = \sum_{i=1}^n \alpha_i v_i$$

where each  $\alpha_i$  is in  $K$ . Now, since  $U$  is a basis for  $K$  over  $F$ , we can write each  $\alpha_i$  as a linear combination

$$\alpha_i = \sum_{j=1}^m \alpha_{ij} u_j$$

where each  $\alpha_{ij}$  is in  $F$ . Thus,  $l$  can be written as the linear combination

$$l = \sum_{i,j} \alpha_{ij} v_i u_j$$

Therefore,  $W$  spans  $L$  as a vector space over  $F$ . Finally, we need to show  $W$  is linearly independent over  $F$ . Suppose there are scalars  $\alpha_{ij}$  in  $F$  satisfying

$$\sum_{i,j} \alpha_{ij} v_i u_j = 0.$$

Define  $\alpha_i = \sum_j \alpha_{ij} u_j$ . Then  $\alpha_i$  is in the field  $K$  and  $l = 0$ . We know that  $V$  is linearly independent over  $K$ , so for every  $i$ , we have

$$\alpha_i = \sum_{j=1}^m \alpha_{ij} u_j = 0.$$

We know furthermore  $U$  is linearly independent over  $F$ , so it follows  $\alpha_{ij} = 0$ , for every  $i$  and  $j$ . Therefore,  $W$  is linearly independent and forms a basis for  $L$  over  $F$ .  $\square$

### 3. COMPASS AND STRAIGHTEDGE CONSTRUCTIONS

Now that we have developed sufficient theory, we will begin to explore algebra's connections to classical geometry. But before jumping into the major results from the application of field theory to geometry, we must first understand the basic rules of compass and straightedge constructions:

**Definition 3.1** (Three Rules of Construction). The following are basic rules of compass and straightedge constructions.

- (1) We always begin with two points in the Cartesian plane—these points are constructed. We can treat the points as being unit distance 1 apart with one point  $p_0 = (0, 0)$  being the origin and the other point  $p_1 = (1, 0)$  being a point along the x-axis. This simplification is possible since geometric operations with a compass and straightedge are invariant under scaling and translation.
- (2) Given two points  $p_0$  and  $p_1$ , we can either draw a line through the two points or a circle centred at one of the points intersecting the other point. The subsequent line or circle are constructed.
- (3) Points of intersection between any constructed lines or circles are constructed.

**Lemma 3.2** (Elementary compass and straightedge Constructions). *Using only the three rules of construction, the following geometric objects are constructible using a finite number of steps with a compass and straightedge:*

- (1) Parallel lines
- (2) 90-degree angles and perpendicular bisectors
- (3) Angle bisectors
- (4) Midpoints of lines

One can consult any high school geometry textbook to review the actual process for creating the familiar constructions listed above. We will use these basic constructions to discuss problems in constructing more complex objects.

**Proposition 3.3.** *Given the basic rules of compass and straightedge construction, all distances of rational length are constructible. In other words, all rational numbers are constructible.*

*Proof.* Suppose we start with a line segment between the points  $p_0 = (0, 0)$  and  $p_1 = (1, 0)$ . Constructing the integers through addition and subtraction is obvious. Simply measure out the line segment with the compass, score an arc with centre at either  $p_0$  or  $p_1$ , and construct a line segment between the arc's centre and any point on the arc. Repeat the procedure as necessary. Multiplication and division

FIGURE 1. Multiplication by similar triangles

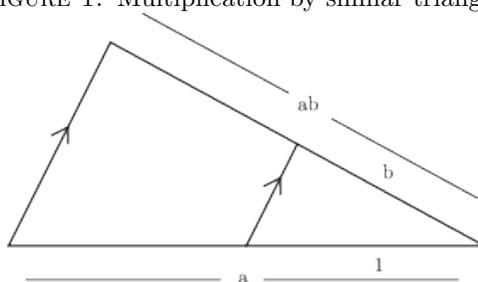
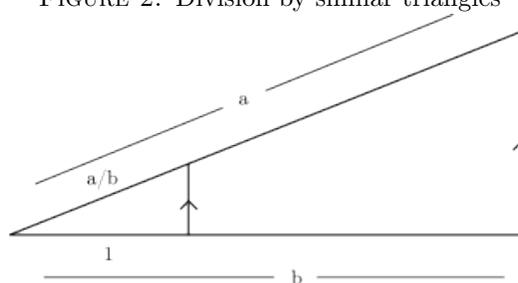


FIGURE 2. Division by similar triangles



of two numbers involves the construction of similar triangles in which the smaller triangle has at least one side of unit length. While we will not discuss their explicit construction, similar triangles need only be constructed from the elementary techniques listed in lemma 3.2. At the very least, similar triangles require the construction of parallel lines. Therefore, all rational numbers are constructible.  $\square$

*Remark 3.4.* Not only are all of the rational numbers constructible, but also all of the square roots of rational numbers are constructible. Simply construct a semicircle with a radius of unit length plus the rational number of which you wish to take the square root. Then construct a perpendicular line through the radius at unit length from the circumference of the circle.

We know from elementary algebra that given two points  $p_0$  and  $p_1$ , where the coordinates are elements of a subfield  $F$  of the real numbers, the line through the two points is given by a linear equation with coefficients in  $F$ . This is easily seen by writing an equation in point-slope form. Similarly, one can see that if we instead construct a circle centred about  $p_0$  passing through  $p_1$ , the circle is described by a quadratic equation with coefficients in  $F$ , i.e. the standard form of the circle. The situation is slightly more interesting when lines or circles intersect one another.

- Proposition 3.5.**
- i* Given two lines with coefficients in a subfield  $F$  of the real numbers, the points of intersection have coordinates in  $F$ .
  - ii* Given a line and a circle with coefficients in a subfield  $F$  of the real numbers, the points of intersection have coordinates in  $F$  or a real quadratic field extension  $K$  of  $F$ .
  - iii* The result from *ii* is the same given two circles.

- Proof.*
- i Clearly, the coordinates of the point of intersection of two lines are in  $F$ , since the coordinates are found through solving two linear equations.
  - ii In the case of a line and a circle with coefficients in  $F$ , we can solve for one of the variables, say  $y$ , in the linear equation and substitute in the equation for the circle, producing a quadratic equation in  $x$ . Consequently, the coordinates of the point of intersection are at most in a quadratic field extension of  $F$ .
  - iii In the case of two circles, we can subtract the equations of the two circles in standard form, producing an equation like the intersection of the line and circle which we considered in part ii.

□

**Proposition 3.6.** *If  $p$  is some point with coordinates in a field extension  $K \subset \mathbb{R}$  produced by a series of compass and straightedge constructions starting in a subfield  $F \subset K$ , then  $[K : F] = 2^k$  for some integer  $k \geq 0$ .*

*Proof.* Any line or circle constructed through any two points of  $F$  will have coefficients in  $F$ . Thus, points of intersection will have coordinates in  $F$  or at most a degree two field extension of  $F$ . By the multiplicative property of the degree, a finite series of compass and straightedge constructions will produce elements of degree  $2^k$  over  $F$ . □

Now that we have learned the rules of compass and straightedge construction, we have sufficiently filled our toolbox so that we may now look at some famous applications of abstract algebra which provided the solutions to classical problems in geometry that remained unsolved from the time of the ancient Greeks all the way up to the 19th century. We will first discuss angle trisection, followed by squaring the circle, and then end with doubling the cube.

**Lemma 3.7** (Triple angle formula).

$$\cos 3\theta = 4 \cos^3 \theta - 3 \cos \theta$$

**Theorem 3.8.** *Trisecting an angle using only a finite number of compass and straightedge constructions is not possible in general.*

*Proof.* Without loss of generality, we may assume that one side of the angle we wish to trisect lies along the x-axis. If an angle can be constructed, then the point on the unit circle corresponding to the angle from the x-axis can be constructed—in other words, the cosine of the angle can be constructed. Starting with  $\cos \theta$ , we wish to construct the angle  $\cos \frac{\theta}{3}$ . To show that trisection is not possible in general, we will consider the case of trisecting a  $60^\circ$  angle. Let  $\theta = \frac{\pi}{9}$ . Applying the triple angle formula and substituting our value for  $\theta$  we have

$$\cos \frac{\pi}{3} = 4 \cos^3 \frac{\pi}{9} - 3 \cos \frac{\pi}{9}$$

We know  $\cos \frac{\pi}{3} = \frac{1}{2}$ . Let  $\alpha = \cos \frac{\pi}{9}$ . We can rewrite the equation:

$$0 = 4\alpha^3 - 3\alpha - \frac{1}{2}$$

$$0 = 8\alpha^3 - 6\alpha - 1$$

In other words,  $\alpha = \cos \frac{\pi}{9}$  is a root of the polynomial  $8x^3 - 6x - 1 \in \mathbb{Z}[x]$ . By the rational roots theorem,  $\frac{\pm 1}{1, 2, 4, 8}$  are candidates for the rational roots of this polynomial. Through simply checking each candidate, we find that none of the candidates are roots. Consequently, the polynomial is irreducible over  $\mathbb{Q}$ , and in

fact,  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ , which is clearly not a power of 2, so  $\alpha$  is not constructible. Thus, trisecting an angle is impossible in general.  $\square$

**Example 3.9.** While it is not true in general that a given angle can be trisected, some angles, like  $180^\circ$ , are able to be trisected. Taking  $\theta = \frac{\pi}{3}$  and using the same formula above, we find:

$$\cos \pi = 4 \cos^3 \frac{\pi}{3} - 3 \cos \frac{\pi}{3}$$

We know  $\cos \pi = -1$ . Let  $\alpha = \frac{\pi}{3}$ . So we have:

$$0 = 4\alpha^3 - 3\alpha + 1$$

$$0 = (\alpha + 1)(2\alpha - 1)^2$$

The polynomial is reducible over  $\mathbb{Q}$ , and in fact  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 1$ , so  $\mathbb{Q}(\alpha)$  is equal to  $\mathbb{Q}$ . Consequently,  $60^\circ$  is constructible by trisecting a  $180^\circ$  angle.

The problem of the impossibility of trisecting an angle is the same problem as not being able to construct certain regular polygons. For example, since it is impossible to construct a 20-degree angle, it is also impossible to construct a regular 18-gon.

**Theorem 3.10** (Doubling the Cube). *Given the side length of a cube, it is impossible in general to construct a new cube such that the volume of the new cube is twice the volume of the first cube.*

*Proof.* Assume we are given a cube of unit length, so that the volume is one cubed unit. In order to show that it is impossible to construct a cube with a volume of two cubed units, we simply need to show that it is impossible to construct a line segment of length  $\sqrt[3]{2}$ . Clearly,  $\sqrt[3]{2}$  is a root of the irreducible polynomial equation  $f(x) = x^3 - 2$ . Since the irreducible polynomial is of degree three, it is clear  $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ , which is not a power of 2. Thus, doubling the cube is impossible in general.  $\square$

The following two results were solved in 1882 by Ferdinand Lindemann. Lindemann proved that no two polynomials in powers of  $\pi$  with integer coefficients can have the same value. In other words, Lindemann arrived at the following conclusion:

**Theorem 3.11** (Lindemann). *The real number  $\pi$  is transcendental.*

We will assume that this statement is true without proof. The proof is beyond the scope of this paper, and the reader can consult a rigorous analysis textbook if they wish to read a proof.

The transcendence of  $\pi$  immediately solves the problem of squaring the circle.

**Theorem 3.12** (Squaring the Circle). *It is impossible in general to construct a square whose area is the same as a given circle using a finite number of compass and straight edge constructions.*

*Proof.* To prove squaring the circle is not possible in general, we will consider the case of trying to construct a square whose area is equal to that of the unit circle. This problem is equivalent to proving that the number  $\pi$  is not constructible. We use the previous assumption that  $\pi$  is transcendental. Then, the degree of the field extension  $[\mathbb{Q}(\pi) : \mathbb{Q}]$  is not equal to a power of two, but is instead infinite. It follows from proposition 3.6 that  $\pi$  is not constructible. Thus, it is impossible to square the circle in general.  $\square$

## 4. AFTERWORD

The three applications of field theory presented in this paper are only a couple of the many ways in which abstract algebra has helped solve problems in other branches of mathematics. Galois theory, which elaborates upon field theory and connects it with group theory, answers the question of why there is no formula that solves for the roots of a quintic polynomial in terms of its coefficients using only basic algebraic operations. Galois theory can even be applied to answer questions stemming from classical compass and straightedge problems, such as exactly which regular polygons are constructible. For example, we can use Galois theory to show that regular  $p$ -gons, where  $p$  a prime number of the form  $p = 2^{2^n} + 1$ , are constructible. Numbers of that form are known as Fermat Primes. The only known Fermat Primes are 3, 5, 17, 257, 65537. Whether or not there are any more primes of this form remains an open problem in number theory. Any other regular prime-gons, such as polygons of 7, 9, 11, 13, 17,  $\dots$  sides are not constructible with a compass and straightedge. Another paper would investigate how Galois theory allows us to prove such statements and more.

**Acknowledgments.** It is a pleasure to thank my mentor, Drew Moore, for all of the support and guidance in choosing a research topic and, subsequently, editing the drafts of this paper. I am incredibly grateful for his pushing me while I explored mathematical territory previously and entirely unfamiliar to me. I would also like to thank Peter May and all the graduate students and University of Chicago faculty for funding me while I lived in Chicago and for volunteering their time to make the REU possible.

## REFERENCES

- [1] Michael Artin. Algebra. Pearson Prentice Hall. 2011.
- [2] David S. Dummit and Richard M. Foote. Abstract Algebra. John Wiley and Sons, Inc. 2004.
- [3] Heinrich Tietze. Famous Problems of Mathematics. Graylock Press. 1965.