6-2019

Geometric Constructions, Origami, and Galois Theory

Julia Greene
Union College - Schenectady, NY

Geometric Constructions, Origami, and Galois Theory

By

Julia Greene

* * * * * * * * *

Submitted in partial fulfillment
of the requirements for
Honors in the Department of Mathematics

UNION COLLEGE
June, 2019

Abstract

GREENE, JULIA Geometric Constructions, Origami, and Galois Theory. Department of Mathematics, June 2019.

ADVISOR: George Todd

Geometric constructions using an unmarked straightedge and a compass have been studied for thousands of years. In these constructions, we can draw circles and lines starting with any two points, and we can create new points where they intersect. An n-gon is said to be constructible if can be constructed in a finite number of steps using these guidelines. We begin with constructions of several n-gons, and examine the field theory behind geometric constructions. Galois theory then provides a precise classification of which n-gons are constructible and which are not. Next is an exploration of origami construction, which examines a single-fold construction axiom, and establishes the classification of origami-constructible n-gons. For example, a heptagon is not constructible using traditional construction techniques, but it is constructible using origami. Finally, we investigate new axioms, which might allow for additional constructions, and examine their implications.

Contents

Chapter 1

Introduction to Constructions

The ancient Greeks were extremely interested in constructions that could be achieved with an unmarked straightedge and a compass. There are several rules for constructions starting with any two points. We will call them C_1, C_2, C_3, C_4 and C_5. They are:

- C_1: A circle can be created centered at any point and through another.
- C_2: A line can be drawn through any two points.
- C_3: A point can be created where any two lines intersect.
- C_4: A point can be created where a line intersects a circle.
- C_5: A point can be created where any two circles intersect.

For example, we can construct a regular triangle starting with any two points. Given A and B, where the distance between them is 1, we can draw a circle centered at A that goes through B. Similarly, we can draw a circle centered at B that goes through A. Then we have that the radius of each of these circles is 1. Now, label the point where the two circles intersect, C. Drawing lines $\overline{AB}$, $\overline{BC}$, and $\overline{AC}$ yields a triangle. Each line has length 1 since that is the radius of the circle, and so we have a regular triangle. This can be seen in Figure 1.1.

We have just seen the simple construction of a triangle, but we ultimately want to know exactly which polygons can and cannot be constructed. We will begin exploring this question by using a straightedge and compass to construct several different n-gons. Then we will analytically prove that each one is actually a regular n-gon.

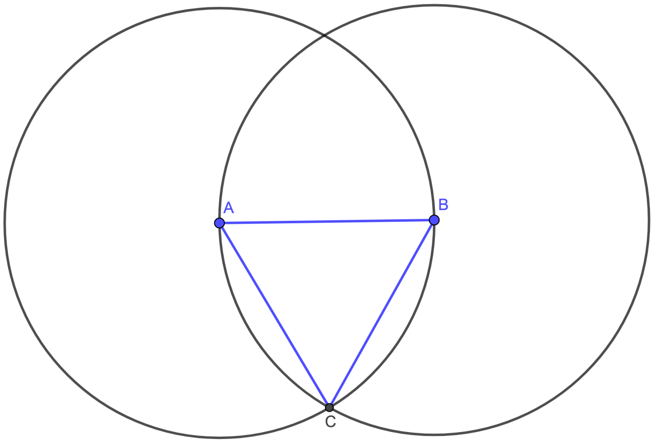

Figure 1.1: Basic Triangle Construction

Chapter 2

Polygon Constructions

In this chapter, we will construct a pentagon, triangle, square, hexagon and octagon using C_1, C_2, C_3, C_4 and C_5. Then we will prove that they are regular polygons, which will show that they are constructible.

2.1 Pentagon Construction

We will start by constructing a regular pentagon using the following steps.

Start with two points, A and B, and say that the distance between them is 1. Then, draw a circle centered at A that goes through B. This circle has radius 1. Draw another circle centered at B that goes through A, which also has radius 1.

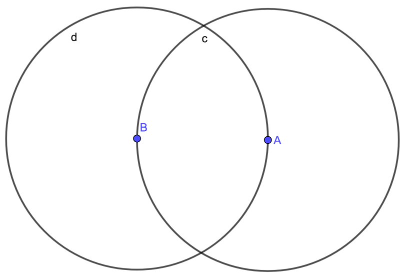

Figure 2.1: Pentagon Construction 1

Call the bottom point of intersection between these two circles, C. Next, draw a line through C and A. Name the point where this line intersects the circle centered at A, D. Then draw a line through B and D. Call the point where this line intersects the circle centered at B, E. This can be seen in Figure 2.2.

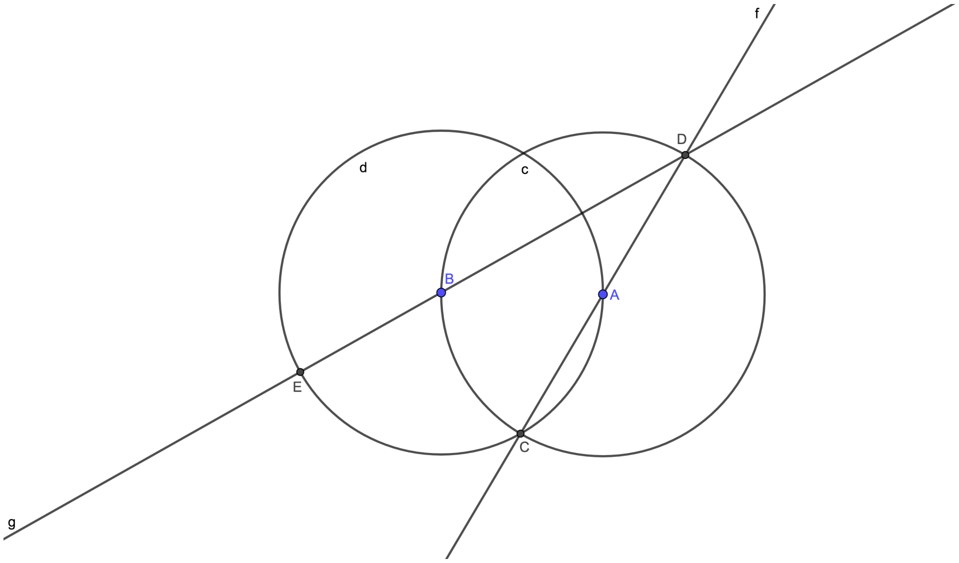

Figure 2.2: Pentagon Construction 2

Next, set the compass length as the distance between C and E.[1] Now, draw a circle centered at A with this radius. Draw a line through C and B, and label the point where it intersects this new circle, F. Then draw an arc centered at E through F, as in Figure 2.4. Draw a point where this arc intersects the circle centered at B. This is point H in Figure 2.5.

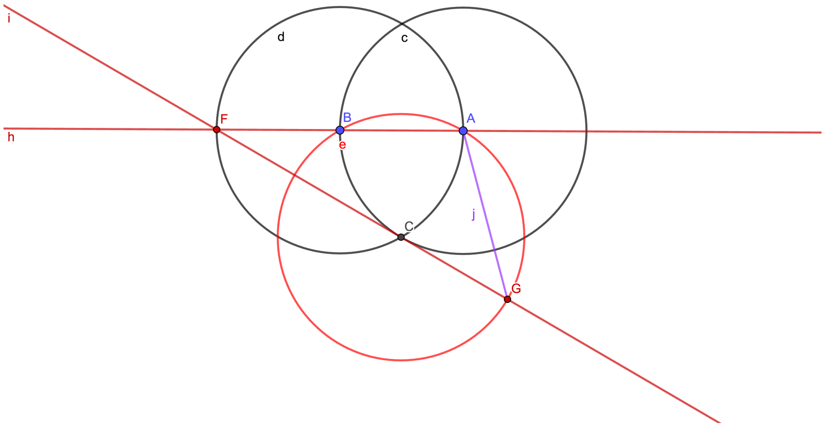

Figure 2.3: How to Construct Length $\overline{EC}$

[1] We can do this since it is a constructible length. We could construct it by following the same steps, but starting with points B and C. Then A is the point of intersection between them. This can be seen in Figure 2.3.

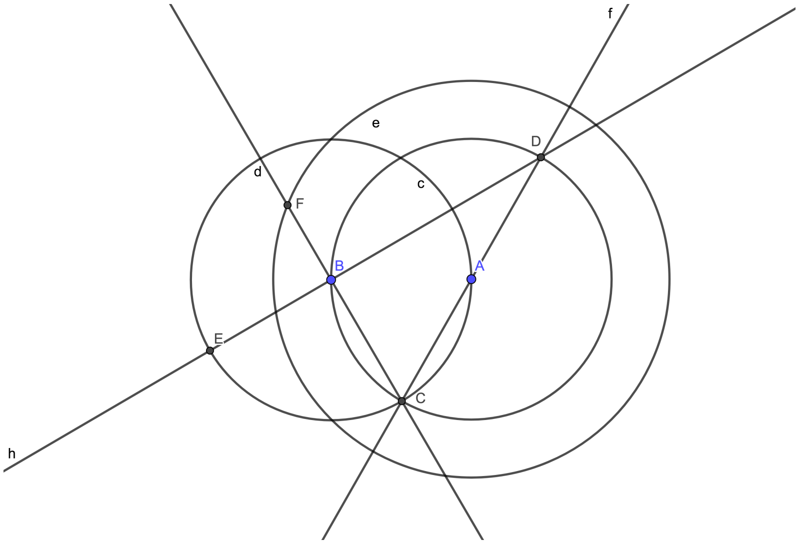

Figure 2.4: Pentagon Construction 3

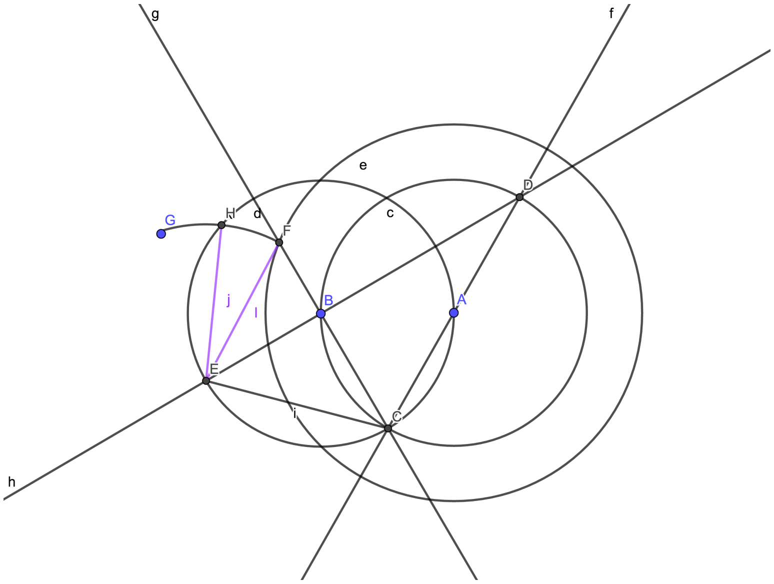

Figure 2.5: Pentagon Construction 4

Now, draw an arc with the same radius centered at H. Continue this process around the circle until there is a pentagon inscribed in the circle centered at B. This can be seen in Figure 2.6. We will prove that this is a regular pentagon.

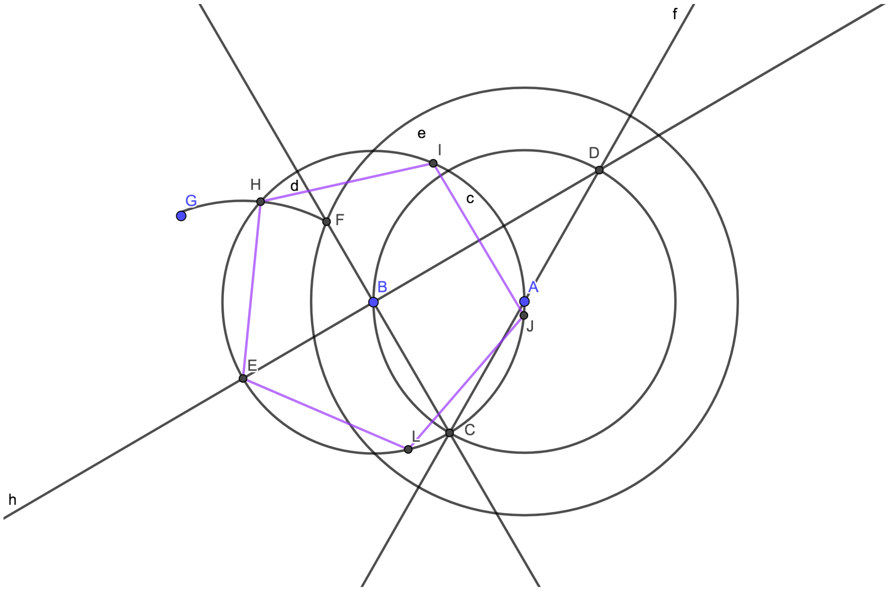

Figure 2.6: Pentagon Construction 5

Theorem 2.1.1. *This construction yeilds a regular pentagon.*

Proof. To show that we have constructed a regular pentagon, we want to find the length of one of the edges and then show that a regular pentagon would have the same edge length. We know that $\overline{EH}$ is the same length as $\overline{EF}$ since they were constructed from the same arc, so we will find the length of the line $\overline{EF}$. We can do this analytically.

We want to find the distance between points E and F, so we must find the coordinates of each point. Let A be the origin. We know that the larger circle centered at A has radius $\sqrt{2}$ since it was constructed with a radius of $\overline{EC}$. We know $\overline{EC} = \sqrt{2}$ since $\measuredangle EBC$ is a right triangle and each of the legs has length 1. Thus, the circle centered at point A that goes through F has equation,

$$x^2 + y^2 = 2.$$

Then we want to find the point where this circle intersects with the line that goes through points B and C. We know that this line has slope $-\sqrt{3}$ and goes through the point $(-1, 0)$, thus has equation

$$y = -\sqrt{3}x - \sqrt{3}.$$

Then, finding the point where the circle intersects this line, we have

$$x^2 + \left(-\sqrt{3}x - \sqrt{3}\right)^2 = 2$$

$$x^2 + 3x^2 + 6x + 3 = 2$$

$$4x^2 + 6x + 1 = 0.$$

And applying the quadratic formula, we have that $x = \dfrac{-6 \pm \sqrt{20}}{8}$. But then, we must have that $x = \dfrac{-6 - \sqrt{20}}{8} = \dfrac{-3 - \sqrt{5}}{4}$, since the x value of F must be less than -1, since it is to the left of B. Then we have that $\dfrac{-3-\sqrt{5}}{4} < -1$, while $\dfrac{-3+\sqrt{5}}{4} > -1$. Thus,

$$F = \left(\frac{(-3 - \sqrt{5})}{4}, \sqrt{-3}\left(\frac{-3-\sqrt{5}}{4} \right) - \sqrt{3} \right).$$

Similarly, we can find the coordinates of E, by finding the point where the circle

$$(x+1)^2 + y^2 = 1$$

intersects with the line through B and D, which has equation,

$$y = \frac{1}{\sqrt{3}}x + \frac{1}{\sqrt{3}}.$$

Then we have,

$$\begin{aligned} (x+1)^2 + \left(\frac{1}{\sqrt{3}}x + \frac{1}{\sqrt{3}} \right)^2 &= 1 \\ x^2 + 2x + \frac{1}{3}x^2 + \frac{2}{3}x + \frac{1}{3} &= 0 \\ 4x^2 + 8x + 1 &= 0. \end{aligned}$$

Applying the quadratic formula, we have that $x = \dfrac{-8 \pm \sqrt{48}}{8}$. But then, we must have that $x = \dfrac{-8 - \sqrt{48}}{8} = \dfrac{-2 - \sqrt{3}}{2}$ since as before, we must have the x value of E less than -1. Thus,

$$E = \left(\frac{(-2 - \sqrt{3})}{2}, \frac{1}{\sqrt{3}}\left(\frac{-2-\sqrt{3}}{2} \right) + \frac{1}{\sqrt{3}} \right).$$

Then, applying the distance formula we can find the length of $\overline{EF}$ by finding the distance between E and F.

$$\text{Let } \alpha = \left(\frac{(-3-\sqrt{5})}{4} \right) - \left(\frac{(-2-\sqrt{3})}{2} \right).$$

$$\text{And let } \beta = \left(\sqrt{-3}\left(\frac{-3-\sqrt{5}}{4} \right) - \sqrt{3} \right) - \left(\frac{1}{\sqrt{3}} \left(\frac{-2-\sqrt{3}}{2} \right) + \frac{1}{\sqrt{3}} \right).$$

Then we have that

$$d(E,F) = \sqrt{\alpha^2 + \beta^2}$$

$$= \sqrt{\frac{2(5-\sqrt{5})}{4}} = \sqrt{\frac{5-\sqrt{5}}{2}}.$$

We can now check to see that if we do have a regular pentagon, each edge length would be $\sqrt{\frac{5-\sqrt{5}}{2}}$. Given a regular pentagon, each of the interior angles should be $\frac{2\pi}{5}$. Then, bisecting one of these angles gives us a right triangle, which bisects the edge. Thus, we know that the edge length is equal to $2(\sin\frac{\pi}{5})$, which can be seen in Figure 2.7.

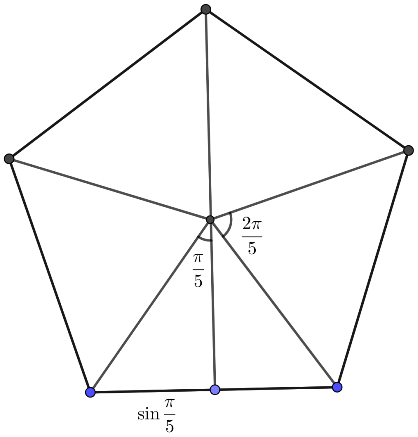

Figure 2.7: Length of Pentagon Edge

Now using the identity,

$$\sin(5\theta) = 16\sin^5\theta - 20\sin^3\theta + 5\sin\theta,$$

which can be obtained using the Bromwich formula A.0.1, we must have that

$$\sin(\pi) = 16\sin^5\left(\frac{\pi}{5}\right) - 20\sin^3\left(\frac{\pi}{5}\right) + 5\sin\left(\frac{\pi}{5}\right).$$

Now if we let $x = \sin(\frac{\pi}{5})$, we can solve for x to find our edge length. This gives us that

$$\sin(\pi) = 0 = 16x^5 - 20x^3 + 5x = x(16x^4 - 20x^2 + 5).$$

And solving for x^2, we have

$$x^2 = \frac{20 \pm \sqrt{80}}{32} = \frac{5 \pm \sqrt{5}}{8}.$$

And we know it must be $\dfrac{5-\sqrt{5}}{8}$ since $\sin(\frac{\pi}{5}) < \sin(\frac{\pi}{4}) = \frac{\sqrt{2}}{2}$. Hence, $x = \sin\left(\dfrac{\pi}{5}\right) = \sqrt{\dfrac{5-\sqrt{5}}{8}} = \frac{1}{2}\sqrt{\dfrac{5-\sqrt{5}}{2}}$. Then since the edge length is equal to $2\sin\left(\dfrac{\pi}{5}\right) = 2x$ we have that the edge length is

$$2\left(\frac{1}{2}\right)\sqrt{\frac{5-\sqrt{5}}{2}} = \sqrt{\frac{5-\sqrt{5}}{2}}.$$

Thus we have constructed a regular pentagon.

□

2.2 Triangle Construction

We can construct a triangle as in Figure 2.8, and we will show that this is a regular triangle. We can find the edge length of the triangle analytically by finding the two points where the circles intersect, and then finding the distance between them. We have that the circle centered at B, the origin, has the equation $x^2 + y^2 = 1$ and the circle centered at A has equation $(x+1)^2 + y^2 = 1$. Thus we can set the two equal to find the points where they intersect. We then have that $x^2 + y^2 = 1$ implies that $y^2 = 1 - x^2$. So plugging in we have

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

$$\text{Thus, } x^2 + 2x + 1 + 1 - x^2 = 1.$$

$$\text{Implying, } 2x + 2 = 1 \Rightarrow 2x = -1.$$

And so we have that, $x = -\frac{1}{2}$. Then we can plug x in to find that $y = \pm\sqrt{\dfrac{3}{4}} = \pm\dfrac{\sqrt{3}}{2}$, so our two points of intersection are $\left(-\dfrac{1}{2}, \dfrac{\sqrt{3}}{2}\right)$ and $\left(-\dfrac{1}{2}, -\dfrac{\sqrt{3}}{2}\right)$. Now, since each of these points is a vertex of the triangle, we need to determine the distance between them to find the edge length. Using the distance formula we have,

$$d\left(\left(-\frac{1}{2}, \frac{\sqrt{3}}{2}\right), \left(-\frac{1}{2}, -\frac{\sqrt{3}}{2}\right)\right)$$

$$= \sqrt{\left(-\frac{1}{2} - -\frac{1}{2}\right)^2 + \left(\frac{\sqrt{3}}{2} - -\frac{\sqrt{3}}{2}\right)^2}$$

$$= \sqrt{\frac{2\sqrt{3}^2}{2}}$$

$$= \sqrt{3}.$$

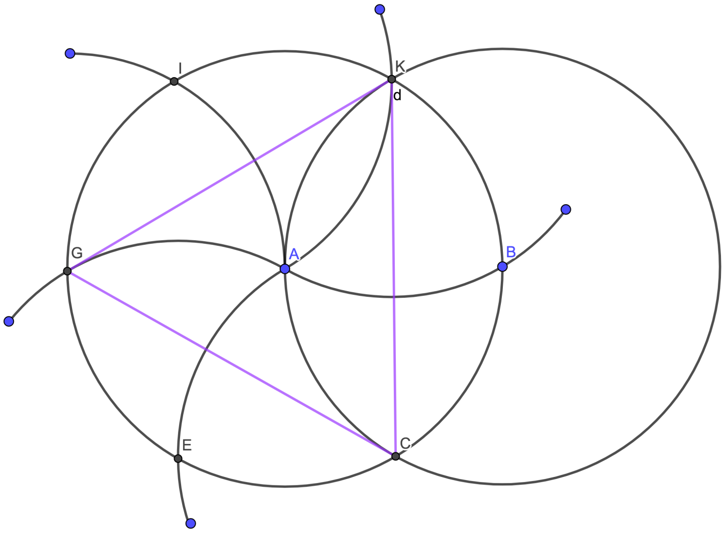

Figure 2.8: Triangle Construction

We can now check that this is a regular triangle. If so, each of the interior angles would be $\frac{2\pi}{3}$. Then, we can bisect one of these angles to be $\frac{\pi}{3}$ by dropping a perpendicular. And thus, the edge length would be equal to $2\sin\frac{\pi}{3}$. We will use the identity $\sin 3\theta = 3\sin\theta - 4\sin^3\theta$, which we get from the Bromwich formula A.0.1. This gives us that

$$0 = \sin\pi = 3\sin\left(\frac{\pi}{3}\right) - 4\sin^3\left(\frac{\pi}{3}\right).$$

If we let $x = \sin\left(\frac{\pi}{3}\right)$, we have

$$0 = 3x - 4x^3 = x(4x^2 - 3).$$

Thus, $x = \frac{\sqrt{3}}{2} = \sin(\frac{\pi}{3})$. Hence, our edge length is $2\sin\frac{\pi}{3} = 2\left(\frac{\sqrt{3}}{2}\right) = \sqrt{3}$, and so we have a regular triangle, as desired.

2.3 Square Construction

We can construct a square inscribed in a circle, as in Figure 2.9, and find the edge length analytically. Say that point A is the origin and point B has coordinates $(1, 0)$. Then the equation of the circle centered at A is $x^2 + y^2 = 1$ and the circle centered at B has equation $(x-1)^2 + y^2 = 1$. Then since the distance between A and B is 1, we must have that the point between them is $\left(\frac{1}{2}, \frac{1}{2}\right)$ and the radius of the circle which goes through both A and B is $\frac{1}{2}$. This then gives us the at the slope of line h is 1 and the slope of line i is -1. Then to find the edge length, we will find where line h intersects with the circle centered at A and where line i intersects with the circle centered at A.

We have that the equation for h is $y = x$ and the equation for i is $y = -x$. Starting with h, when we plug its equation into $x^2 + y^2 = 1$, we have

$$x^2 + x^2 = 2x^2 = 1.$$

And so,

$$x^2 = \frac{1}{2}.$$

And so this circle intersects with line h when $x = \dfrac{1}{\sqrt{2}}$ and when $x = -\dfrac{1}{\sqrt{2}}$. We will use the positive value, which is point I in Figure 2.9. Plugging the x-value back into $y = x$, we have that point I has coordinates $\left(\dfrac{1}{\sqrt{2}}, \dfrac{1}{\sqrt{2}}\right)$. Similarly, to find the point where i intersects with the circle centered at A, we will plug the equation $y = -x$ into $x^2 + y^2 = 1$. This gives us,

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

Thus, as before we have that this circle intersects with line i when $x = \dfrac{1}{\sqrt{2}}$ and when $x = -\dfrac{1}{\sqrt{2}}$. Again, we will use the positive value, which is point J in Figure 2.9. Plugging this back in, the coordinates of point J are $\left(\dfrac{1}{\sqrt{2}}, -\dfrac{1}{\sqrt{2}}\right)$. We can now find the distance between these two points. The distance formula yields:

$$\begin{aligned} d(I, J) &= \sqrt{\left(\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}\right)^2 + \left(\frac{1}{\sqrt{2}} - -\frac{1}{\sqrt{2}}\right)^2} \\ &= \sqrt{0^2 + \left(\frac{2}{\sqrt{2}}\right)^2} \\ &= \frac{2}{\sqrt{2}} \\ &= \sqrt{2}. \end{aligned}$$

Thus, our constructed square has an edge length of $\sqrt{2}$.

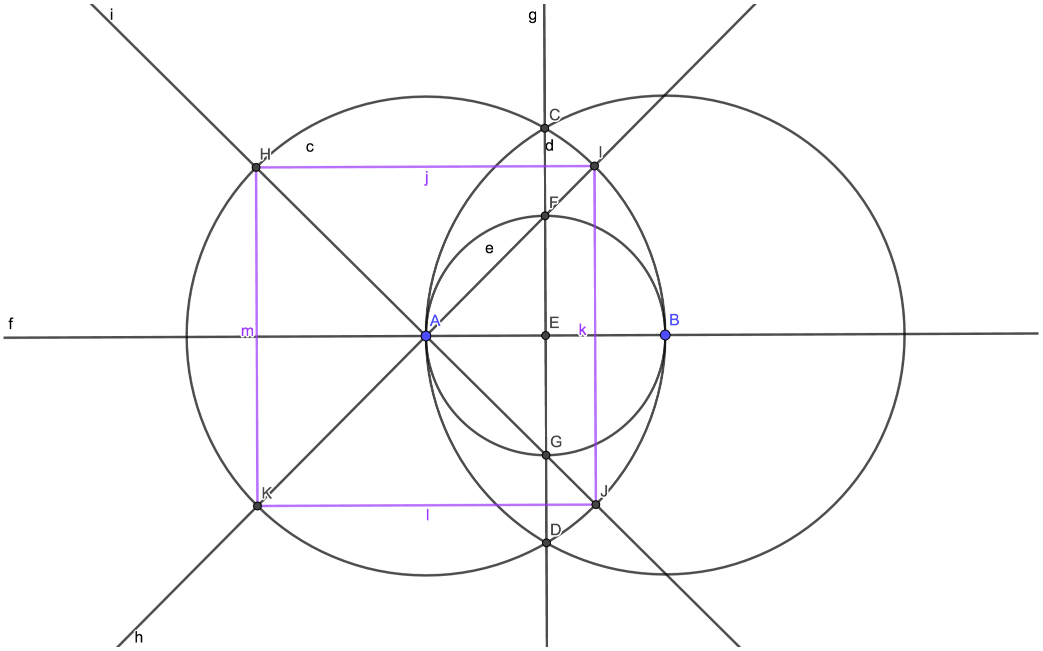

Figure 2.9: Square Construction

Now we can check that this is actually a square. If so, each of the interior angles would be $\frac{2\pi}{4}$. As we did with the triangle, we can then bisect one of these angles by dropping a perpendicular, which gives us an angle of $\frac{\pi}{4}$. Thus, the edge length would be equal to $2\sin\left(\frac{\pi}{4}\right)$. Now using the identity $\sin(4\theta) = \cos\theta(4\sin\theta - 8\sin^3\theta)$, which can be found using the Bromwich formula A.0.1, we have

$$0 = \sin\pi = \cos\left(\frac{\pi}{4}\right)\left(4\sin\left(\frac{\pi}{4}\right) - 8\sin^3\left(\frac{\pi}{4}\right)\right)$$

$$= \frac{\sqrt{2}}{2}\left(4\sin\left(\frac{\pi}{4}\right) - 8\sin^3\left(\frac{\pi}{4}\right)\right).$$

So if we let $x = \sin\left(\frac{\pi}{4}\right)$ then,

$$0 = -8x^3 + 4x.$$

$$\text{Thus } 0 = -4x(2x^2 - 1).$$

This gives us that $x = \frac{1}{\sqrt{2}} = \sin\left(\frac{\pi}{4}\right)$. And then $2\sin\left(\frac{\pi}{4}\right) = \frac{2}{\sqrt{2}} = \sqrt{2}$. Thus the edge length is $\sqrt{2}$, as desired.

2.4 Hexagon Construction

Now, we will construct a hexagon inscribed in a circle as in Figure 2.10. Given points A and B, which have a distance of 1 between them, this hexagon is constructed by drawing a circle centered at A which goes through B and then a circle centered at B which goes through A. Then, using B and the two points of intersection between the circles, each new vertex is created by centering a circle at a vertex and drawing it through point A. Then since the radius of the circle centered at B is equal to 1, we have that the edge length between points B and C, as in Figure 2.10, is 1.

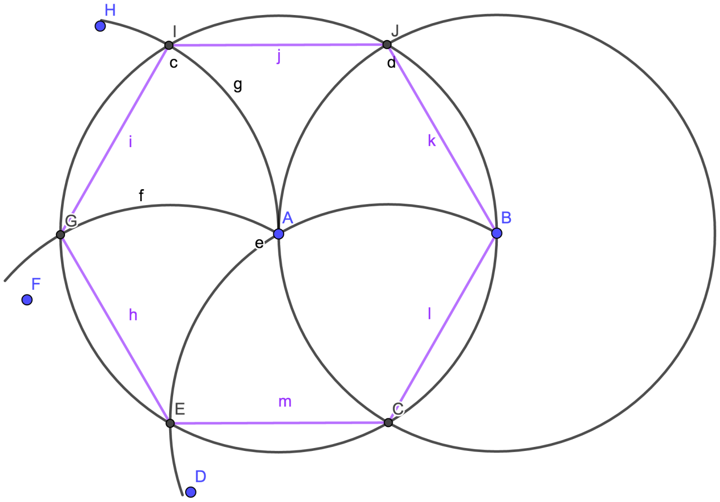

Figure 2.10: Hexagon Construction

As we did with the pentagon, triangle and square, we will now check that this is a regular hexagon. Assuming it is, each interior angle is $\frac{2\pi}{6}$ radians, and so we can bisect this angle by dropping a perpendicular. This gives us a side length of $2\sin\frac{\pi}{6}$. We will use the identity $\sin(6\theta) = \cos\theta(6\sin\theta - 32\sin^3\theta + 32\sin^5\theta)$, which comes from the Bromwich formula A.0.1, to show that $2\sin\frac{\pi}{6} = 1$. This identity gives us that

$$\sin(\pi) = \cos\left(\frac{\pi}{6}\right)\left(6\sin\left(\frac{\pi}{6}\right) - 32\sin^3\left(\frac{\pi}{6}\right) + 32\sin^5\left(\frac{\pi}{6}\right)\right).$$

Thus,

$$0 = \cos\left(\frac{\pi}{6}\right)\left(6\sin\left(\frac{\pi}{6}\right) - 32\sin^3\left(\frac{\pi}{6}\right) + 32\sin^5\left(\frac{\pi}{6}\right)\right).$$

And so,

$$0 = 6\sin\left(\frac{\pi}{6}\right) - 32\sin^3\left(\frac{\pi}{6}\right) + 32\sin^5\left(\frac{\pi}{6}\right).$$

Now, if we let $x = \sin\left(\frac{\pi}{6}\right)$, we have that

$$0 = 32x^5 - 32x^3 + 6x = 2x(16x^4 - 16x^2 + 3).$$

Factoring gives us that $x = \frac{1}{2} = \sin\left(\frac{\pi}{6}\right)$. And thus, the edge length is $2\sin\frac{\pi}{6} = 2x = 2\left(\frac{1}{2}\right) = 1$, as desired. Therefore, we have constructed a regular hexagon.

2.5 Octagon Construction

Next we are going to construct an octagon, which can be seen in Figure 2.11. As before, we will find a side length analytically and verify that this side length indicates that it is a regular octagon. We will find the distance between points B and N in Figure 2.11. Say that point A is the origin, so the circle centered there has equation $x^2 + y^2 = 1$. Then B has coordinates $(1, 0)$. We will now find the coordinates of point N. As with our square construction, we know the line that goes through both A and N has a slope of 1, and therefore has equation $y = x$. Then, setting it equal to our circle, $x^2 + y^2 = 1$, we have that point N has coordinates $\left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right)$. We will now find the distance between points B and N. The distance formula yields:

$$d(B,N) = \sqrt{\left(1 - \frac{1}{\sqrt{2}}\right)^2 + \left(0 - \frac{1}{\sqrt{2}}\right)^2} = \sqrt{\left(\frac{\sqrt{2}-1}{\sqrt{2}}\right)^2 + \left(-\frac{1}{\sqrt{2}}\right)^2}$$

$$= \sqrt{\left(\frac{(\sqrt{2}-1)^2 + 1}{2}\right)}$$

$$= \frac{\sqrt{(\sqrt{2}-1)^2 + 1}}{\sqrt{2}}$$

$$= \frac{\sqrt{(2 - 2\sqrt{2} + 1) + 1}}{\sqrt{2}}.$$

$$\text{Thus, } d(B,N) = \frac{\sqrt{4 - 2\sqrt{2}}}{\sqrt{2}} = \frac{\sqrt{2}\sqrt{2(2-\sqrt{2})}}{2}$$

$$= \frac{2\sqrt{2-\sqrt{2}}}{2} = \sqrt{2-\sqrt{2}}.$$

Therefore, the edge length is $\sqrt{2-\sqrt{2}}$.

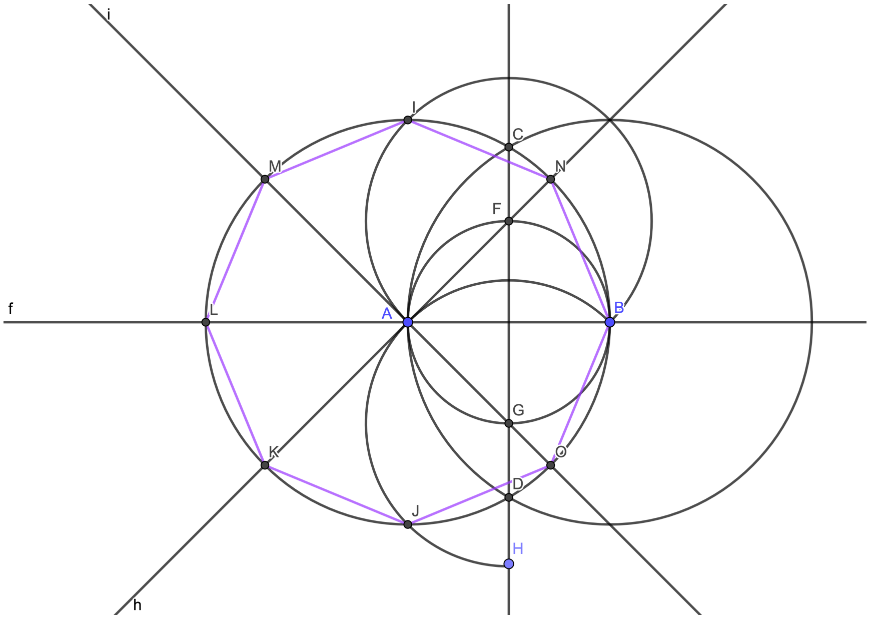

Figure 2.11: Octagon Construction

We will now verify that it is a regular octagon using the identity $\sin(8\theta) = 8\cos\theta(\sin\theta - 10\sin^3\theta + 24\sin^5\theta - 16\sin^7\theta)$, which can be found with the Bromwich formula A.0.1. We have that

$$\sin(\pi) = 8\cos\left(\frac{\pi}{8}\right)\left(\sin\left(\frac{\pi}{8}\right) - 10\sin^3\left(\frac{\pi}{8}\right) + 24\sin^5\left(\frac{\pi}{8}\right) - 16\sin^7\left(\frac{\pi}{8}\right)\right).$$

Thus,

$$0 = \sin\left(\frac{\pi}{8}\right) - 10\sin^3\left(\frac{\pi}{8}\right) + 24\sin^5\left(\frac{\pi}{8}\right) - 16\sin^7\left(\frac{\pi}{8}\right).$$

And if we let $x = \sin\left(\frac{\pi}{8}\right)$, we have

$$0 = x(1 - 10x^2 + 24x^4 - 16x^6)$$

$$\text{Thus, } 0 = -(2x^2 - 1)(8x^4 - 8x^2 + 1).$$

And using the quadratic formula on $(8x^4 - 8x^2 + 1)$ we get that $x = \dfrac{\sqrt{2-\sqrt{2}}}{2}$. Thus, the edge length is $2\sin\dfrac{\pi}{8} = 2x = 2\left(\dfrac{\sqrt{2-\sqrt{2}}}{2}\right) = \sqrt{2-\sqrt{2}}$, as desired.

2.6 Heptagon Construction

We were able to construct a triangle, square, pentagon, hexagon, and octagon. However, we did not construct a regular heptagon. For an n-gon to be constructible, we would be able to construct the length $\sin\left(\frac{2\pi}{n}\right)$. Thus, if we were able to construct a heptagon, we would construct a length of $\sin\left(\frac{2\pi}{7}\right)$. This is equal to a length of

$$\frac{1}{2}\sqrt{\frac{1}{3}\left(7-\sqrt[3]{\frac{7+21\sqrt{-3}}{2}}-\sqrt[3]{\frac{7-21\sqrt{-3}}{2}}\right)}.$$

We will later return to the constructibility of this length.

Chapter 3

Field Extensions

We now know that we can construct a regular triangle, square, pentagon, hexagon and octagon. Given a straightedge and compass construction of an n-gon, we can determine whether that polygon is a regular polygon, and therefore if the specific n-gon is constructible. However, we want to be able to precisely determine which n-gons are constructible and which n-gons are not. To do this, we need an algebraic classification of the field of constructible numbers. We know that all constructions are completed through a finite number of steps, and the creation of new points involves intersecting 2 lines, 2 circles or a line and a circle. We will prove the following theorem.

Theorem 3.0.1. *Let r be a constructible number. Then $[\mathbb{Q}(r) : \mathbb{Q}] = 2^k$ for some integer k.*

Proof. Suppose r is constructible. Then we can construct r through a finite number of steps which involve the intersections of lines and circles. We will look at each of these steps individually.

We will first look at the case in which 2 lines are intersected. Suppose that a_1, a_2, b_1, b_2, c_1 and $c_2 \in \mathbb{Q}$. Then consider the lines l and m, where l is given by

$$ax + by + c = 0,$$

and m is the line

$$dx + ey + f = 0.$$

Taking their intersection, we get the point $\left(\frac{ce - bf}{bd - ae}, \frac{af - cd}{bd - ae}\right)$, which is a another point in the field $\mathbb{Q}$, thus this is a degree 1 extension. Now if a, b, c, d, e and f are points of $\mathbb{Q}$, we can look at the intersection of the circles, c_1 and c_2, where c_1 is

$$x^2 + y^2 + ax + by + c = 0,$$

and c_2 is

$$x^2 + y^2 + dx + ey + f = 0.$$

Setting $c_1 = c_2$ we have the line,

$$(a-d)x + (b-e)y + (c-f) = 0,$$

where $(a-d), (b-e)$ and $(c-f)$ are all points of $\mathbb{Q}$. Therefore, we have another degree 1 extension. Lastly, we will look at the intersection of a line l and a circle c, such that $a, b, c, d, e, f \in \mathbb{Q}$ and l is the line

$$ax + by + c = 0,$$

and c is the circle

$$x^2 + y^2 + dx + ey + f = 0.$$

If we let $l = c$ and solve for x we get

$$(b^2 + a^2)x^2 + (2ac + db^2 - aeb)x + (c^2 - ceb + fb^2) = 0.$$

Let $\alpha = (b^2 + a^2)$, $\beta = (2ac + db^2 - aeb)$, and $\gamma = (c^2 - ceb + fb^2)$. Thus, our solution is $x = \dfrac{-\beta \pm \sqrt{\beta^2 - 2\alpha\gamma}}{2\alpha}$, where $\sqrt{\beta^2 - 2\alpha\gamma}$ is constructible. Hence, the points of intersection of l and c are in the field extension $\mathbb{Q}(\sqrt{\beta^2 - 2\alpha\gamma})$ which is a degree 2 extension of $\mathbb{Q}$.

Then since each one of the steps for a construction is a degree 1 or 2 extension, and a construction must occur in a finite number of steps, multiplying the degree of each step gives us an extension of 2^k for some k. Thus, we have that $[\mathbb{Q}(r) : \mathbb{Q}] = 2^k$ for some integer k, as desired.

□

Corollary 3.0.2. *If an n-gon is constructible then* $\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right) : \mathbb{Q}\right] = 2^k$ *for some integer* k.

Proof. Suppose that some n-gon is constructible. Then the length $\cos\left(\dfrac{2\pi}{n}\right)$ must be constructible for the same reason that $\sin\left(\dfrac{2\pi}{n}\right)$ is constructible in our examples in Chapter 2. Therefore, by Theorem 3.0.1 we must have that $\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right) : \mathbb{Q}\right] = 2^k$ for some integer k, as desired. □

We can now use the information we have on field extensions to prove whether a length is constructible or not using its minimal polynomial as in Definition A.0.40. For example, we saw that the length of a pentagon edge is $\sqrt{\dfrac{5-\sqrt{5}}{2}}$, so we must adjoin $\mathbb{Q}$ with $\sqrt{\dfrac{5-\sqrt{5}}{2}}$, which is a degree 4 extension. Then we also have that its minimal polynomial of $\sqrt{\dfrac{5-\sqrt{5}}{2}}$ is $x^4 - 5x^2 + 5$ which is a degree 4 polynomial.

3.1 The Three Problems of Antiquity

There are three classic problems of antiquity involving straightedge and compass constructions. The ancient Greeks knew that any angle could be bisected, but worked to determine if an angle could be trisected. The two other problems were "doubling the cube" and "squaring the circle." Keeping in mind that a length, x, is constructible if $[\mathbb{Q}(x):\mathbb{Q}] = 2^k$ for some k, we can now show that all three of these problems are impossible using only a straightedge and compass.

Example 3.1.1. *Angle Trisection*

An angle cannot be trisected.

Proof. We will show that some angle θ cannot be trisected. Let $\theta = \frac{\pi}{3}$. Then, if we could trisect this angle, it would result in three equal angles of size $\frac{\pi}{9}$. Thus, we would be able to construct the length, $\cos\left(\frac{\pi}{9}\right)$. We will find the minimal polynomial of $a = \cos\left(\frac{\pi}{9}\right)$ to show that a is not constructible, which implies that we cannot trisect this angle. First, we will prove that $\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$. We know that $e^{i\theta} = \cos(\theta) + i\sin(\theta)$, so we have,

$$\begin{aligned}
\cos(3\theta) &= \frac{e^{i3\theta} + e^{-i3\theta}}{2} = \frac{(e^{i\theta})^3 + (e^{-i\theta})^3}{2} \\
&= \frac{(\cos\theta + i\sin\theta)^3 + (\cos\theta - i\sin\theta)^3}{2} \\
&= \sum_{k=0}^{3}\binom{3}{k}\frac{\cos^k\theta(i\sin\theta)^{3-k} + \cos^k\theta(-i\sin\theta)^{3-k}}{2} \\
&= \sum_{k=0}^{3}\binom{3}{k}\cos^k\theta\sin^{3-k}\theta\frac{i^{3-k} + (-i^{3-k})}{2} \\
&= \sum_{k=0}^{3}\binom{3}{k}\cos^k\theta\sin^{3-k}\theta\cos\left(\frac{1}{2}(3-k)\pi\right) \\
&= \sin^3\theta(0) - 3\cos\theta\sin^2\theta + \cos^2\theta\sin\theta(0) + \cos^3\theta \\
&= \cos^3\theta - 3\cos\theta\sin^2\theta = \cos^3\theta - 3\cos\theta(1-\cos^2\theta) \\
&= \cos^3\theta - 3\cos\theta + 3\cos^3\theta \\
&= 4\cos^3\theta - 3\cos\theta.
\end{aligned}$$

Now, we can find the minimal polynomial for $a = \cos\left(\frac{\pi}{9}\right)$. Using the identity for $\cos\left(\frac{\pi}{3}\right)$ we have that

$$\cos\left(\frac{3\pi}{9}\right) = 4\cos^3\left(\frac{\pi}{9}\right) - 3\cos\left(\frac{\pi}{9}\right).$$

Then if we let $x = \cos\left(\frac{\pi}{9}\right)$ we have,

$$\cos\left(\frac{\pi}{3}\right) = 4x^3 - 3x.$$

And since $\cos\left(\frac{\pi}{3}\right) = \frac{1}{2}$, we have

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

Thus, $8x^3 - 6x - 1$ has $\cos\left(\frac{\pi}{9}\right)$ as a root. There is no prime in which Theorem A.0.42, Eisenstein's Criterion, allows us to verify that this is the minimal polynomial. However, we can check that this is the minimal polynomial by shifting by -1. We can do this because given a polynomial, $f(x)$, if we shift by a value, a, we have $f(x+a)$, which simply shifts the graph horizontally. This does not affect the shape of the graph, and therefore, if $f(x+a)$ is irreducible, we must have that $f(x)$ is irreducible. Now, we see that

$$8(x-1)^3 - 6(x-1) - 1 = 8(x^3 - 3x^2 + 3x - 1) - 6(x-1) - 1$$

$$= 8x^3 - 24x^2 + 18x - 3.$$

Which is irreducible by Eisenstein's Criterion, Theorem A.0.42, with $p = 3$. Thus $8x^3 - 6x - 1$ must be the minimal polynomial for $a = \cos\left(\frac{\pi}{9}\right)$. But, this polynomial has degree 3, and so $\left[\mathbb{Q}\left(\cos\left(\frac{\pi}{9}\right)\right) : \mathbb{Q}\right] = 3$ and $3 \neq 2^k$ for any value k. Therefore, $\cos\left(\frac{\pi}{9}\right)$ is not constructible and so we cannot trisect this angle. Thus, given an arbitrary angle θ, we cannot trisect it using the rules of straightedge and compass constructions.

□

Example 3.1.2. *Squaring a Circle*

Given a circle of radius 1, we cannot construct a square with the same area.

Proof. Suppose we have a circle with radius 1, and for contradiction assume that we can construct a square with the same area. Since the radius of our circle is 1, the area of the circle must be $\pi(1)^2 = \pi$. Then we know that we can construct a square with area π, thus the length of its edges is constructible. Let s be the side length of the square. Then we know that $s^2 = \pi$, so $s = \sqrt{\pi}$. Then since s is constructible, we know that $\sqrt{\pi}$ is constructible. This implies that we can construct π, since if we can construct $\sqrt{\pi}$, we can construct $(\sqrt{\pi})(\sqrt{\pi}) = \pi$. But, since π is transcendental, we know that $\mathbb{Q}(\pi)/\mathbb{Q}$ is not algebraic and π is not the root of any polynomial with rational coefficients. Hence, $[\mathbb{Q}(\pi) : \mathbb{Q}]$ is infinite. But, if π was constructible, we would have that $[\mathbb{Q}(\pi) : \mathbb{Q}] = 2^k$ for some integer k, thus we have a contradiction, and we cannot square a circle. □

Example 3.1.3. *Doubling the Cube*

Given a cube with side length 1, we cannot construct a cube with twice the volume.

Proof. Suppose we have a cube with side length 1. Then we have that the volume of this cube is $1^3 = 1$. We will show that we cannot construct a cube with twice this volume. Suppose we can. Then we want to construct a cube with volume 2. If this cube is contructible, its side length, s must be constructible. Then, since the volume of the cube is 2, we know that $s^3 = 2$, thus $s = \sqrt[3]{2}$. We then have that the minimal polynomial of $\sqrt[3]{2}$ is $x^3 - 2$, since $\sqrt[3]{2}$ is a root and it is irreducible by Eisenstein's criterion, Theorem A.0.42, using $p = 2$. Then, since $x^3 - 2$ has degree 3, we know that $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, and $3 \neq 2^k$ for any k. Thus, s is not constructible, and we cannot construct a cube with twice the volume of our original cube. □

Chapter 4

Galois Theory

We are now able to show which extensions yield a constructible length, but we wish to classify exactly which n-gons are constructible. We can use Galois Theory to do this.

We know that if a polygon is constructible, then its edge length is constructible. Then the length $\cos\left(\frac{2\pi}{n}\right)$ is constructible, as in Corollary 3.0.2. We will use this to prove the Constructibility Criterion of a Regular n-gon in Theorem 4.1.1.

We first need some definitions and theorems of Galois Theory. The following can be found in Chapters 32 and 33 of Gallian's book [6].

Definition 4.0.1. *Roots of Unity are solutions to $x^n - 1 = 0$. $G_n = \{x | x^n - 1 = 0\}$ is a finite group under multiplication.*

For example, we have that $G_3 = \{x|x^3 - 1 = 0\} = \left\{1, \frac{1 \pm \sqrt{-3}}{2}\right\}$ and $G_4 = \{x|x^4 - 1 = 0\} = \{1, -1, i, -i\}$.

Definition 4.0.2. *A generator for G_n is a primitive n^{th} root of unity.*

Definition 4.0.3. *Fix n and let $\omega_1, \omega_2, ..., \omega_{\varphi(n)}$ be the primitive n^{th} roots of unity. Then $\Phi_n(x) = (x - \omega_1)(x - \omega_2)...(x - \omega_{\varphi(n)})$ is called the n^{th} cyclotomic polynomial over $\mathbb{Q}$.*

Note that Φ_n has degree $\varphi(n)$, where $\varphi(n)$ is Euler's phi-Function.

Theorem 4.0.4. *For every positive integer n, $x^n - 1 = \prod_{d|n} \Phi_d(x)$. In particular, for p prime, $x^p - 1 = (x - 1)(x^{p-1} + x^{p-2} + ... + x^2 + x + 1)$.*

Theorem 4.0.5. *If $n \in \mathbb{N}$, then*

(i) $\Phi_n(x) \in \mathbb{Z}[x]$

(ii) $\Phi_n(x)$ *is irreducible over* $\mathbb{Z}$.

Theorem 4.0.6. *Let ω be a primitive n^{th} root of unity. Then, Gal$(\mathbb{Q}(\omega)/\mathbb{Q}) \cong U(n)$.*

Definition 4.0.7. *Let E be an extension field of F. Then an automorphism of E is an isomorphism from E to E.*

For example, $\text{Aut}(\mathbb{C}/\mathbb{R}) = \{\text{id}, \tau\}$, $\tau(a+bi) = a - bi$.

Definition 4.0.8. *The Galois Group of E over F, denoted Gal(E/F) is the set of automorphisms of E which take every element of F to itself. That is,*

$$Gal(E/F) = \{\phi : E \to E \mid \phi \text{ is an automorphism}, \ \phi(x) = x, \forall x \in F\}.$$

Lemma 4.0.9. *If $n \in \mathbb{N}$, $\omega = e^{\frac{2\pi i}{n}}$, then $\mathbb{Q}(\cos(\frac{2\pi}{n})) \subseteq \mathbb{Q}(\omega)$.*

Lemma 4.0.10. *Consider an extension E over $\mathbb{Q}$. Then for every automorphism, ϕ of E, $\phi(x) = x$ for all $x \in \mathbb{Q}$.*

Proof. Let ϕ be an automorphism of E, and let $x \in \mathbb{Q}$. Since $x \in \mathbb{Q}$, we have $x = \frac{m}{n}$ where $m, n \in \mathbb{Z}$. We want to show that $\phi(x) = x$. Since 1 is a unit, we must have that the automorphism $\phi(1) = 1$. Then we have that

$$\phi(n) = \phi((n)(1)) = \phi\underbrace{(1+1+...+1)}_{\text{n times}} = \underbrace{\phi(1)+\phi(1)+...+\phi(1)}_{\text{n times}} = n(\phi(1)) = (n)(1) = n.$$

Similarly, $\phi(m) = m$. We also have that

$$\phi(1) = \phi\left(n\frac{1}{n}\right) = \phi(n)\phi\left(\frac{1}{n}\right) = n\phi\left(\frac{1}{n}\right) = 1.$$

So we must have that $\phi\left(\frac{1}{n}\right) = \frac{1}{n}$. Now, combining our results, we have that

$$\phi(x) = \phi\left(\frac{m}{n}\right) = \phi\left(m\frac{1}{n}\right) = \phi(m)\phi\left(\frac{1}{n}\right) = m\left(\frac{1}{n}\right) = \frac{m}{n} = x.$$

Hence, $\phi(x) = x$, as desired. □

Example 4.0.11. *Let Gal$(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = G$.*

Then, by Lemma 4 we have that $\phi(x) = x$ for all $x \in \mathbb{Q}$ and for all $\phi \in G$. Thus

$$\begin{aligned}\phi(a+b\sqrt{2}) &= \phi(a) + \phi(b)\phi(\sqrt{2}) \\ &= a + b\phi(\sqrt{2}).\end{aligned}$$

Thus, $\phi(x)$ is completely determined by $\phi(\sqrt{2})$. Then we see that,

$$2 = \phi(2) = \phi(\sqrt{2}\sqrt{2}) = (\phi(\sqrt{2}))^2.$$

So, $\phi(\sqrt{2}) = \pm\sqrt{2}$ and we have that G has 2 elements, the identity mapping and the mapping which sends $a + b\sqrt{2}$ to $a - b\sqrt{2}$. Hence, $|G| = 2$, and $G \cong \mathbb{Z}/2\mathbb{Z}$.

Theorem 4.0.12 (The Fundamental Theorem of Galois Theory). *Let F be $\mathbb{Q}$ or an extension of $\mathbb{Q}$. If E/F is the splitting field for some polynomial in $F[x]$ (E/F is a Galois extension), then*

$$\varphi : \{F \subseteq K \subseteq E\} \mapsto \{H | H \leq Gal(E/F)\}$$
$$K \longmapsto Gal(E/F)$$

is one-to-one. We also have the following four facts:

1. $[E : K] = |Gal(E/K)|$ *and* $[K : F] = |Gal(E/F)|/|Gal(E/K)|$
2. *If K is the splitting field of some polynomial in $F[x]$ then,*
$$Gal(K/F) \cong \frac{Gal(E/F)}{Gal(E/K)}$$
3. $K = E_{Gal(E/K)}$
4. *If $H \leq Gal(E/F)$ then $H = Gal(E/E_H)$*

We now have the information we need to prove our constructability criterion. To characterize constructible n-gons, we will prove the following:

4.1 Constructibility Criterion

Theorem 4.1.1 (Constructability Criterion). *A regular n-gon is constructible if and only if $n = 2^k p_1 p_2 ... p_t$ where $k \geq 0$ and each p_i is a prime of the form $p_i = 2^{m_i} + 1$ for some m_i.*

Proof. ($\Rightarrow$) Suppose that a regular n-gon is constructible. We will show that $n = 2^k p_1 p_2 ... p_t$ where $k \geq 0$ and p_i is a prime such that $p_i = 2^{m_i} + 1$. Since our n-gon is constructible, by Corollary 3.0.2, $\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right) : \mathbb{Q}\right] = 2^k$. Now by Lemma 4.0.9, we know that $\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right) \subseteq \mathbb{Q}(\omega)$ where $\mathbb{Q}(\omega)$ is an extension of $\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)$ and $\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)$ is an extension of $\mathbb{Q}$. Then, since $\Phi_n(x)$, which has degree $\varphi(n)$, is the minimal polynomial of ω we have that $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n)$. Then, by field theory we know that

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = \left[\mathbb{Q}(\omega) : \mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right] \cdot \left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right) : \mathbb{Q}\right].$$

Then by the Fundamental Theory of Galois theory, which is Theorem 4.0.12, we have that

$$\varphi(n) = \left|\text{Gal}(\mathbb{Q}(\omega))/\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right| \cdot \left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right].$$

Or,

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] = \frac{\varphi(n)}{\left|\text{Gal}(\mathbb{Q}(\omega))/\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right|}.$$

We also know that $\mathrm{Gal}(\mathbb{Q}(\omega))/\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right) \leq \mathrm{Gal}(\mathbb{Q}(\omega))/\mathbb{Q})$. Now, let $H = \mathrm{Gal}(\mathbb{Q}(\omega))/\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)$ and let $G = \mathrm{Gal}(\mathbb{Q}(\omega))/\mathbb{Q})$. Then we have that $H \leq G$. Now by the definition of the Galois group, Definition 4.0.8, we know that for all $\sigma \in H$, $\sigma(\omega) = \omega^k$ for some k, and $\sigma\left(\cos\left(\frac{2\pi}{n}\right)\right) = \cos\left(\frac{2\pi}{n}\right)$. But, $\omega = e^{\frac{2\pi i}{n}} = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$. Thus,

$$\sigma(\omega) = \sigma\left(\cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)\right)$$

$$= \sigma\left(\cos\left(\frac{2\pi}{n}\right)\right) + \sigma(i)\sigma\left(\sin\left(\frac{2\pi}{n}\right)\right).$$

We also have that $\sigma(\omega) = \omega^k = \cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right)$. Hence, $\cos\left(\frac{2\pi}{n}\right) = \cos\left(\frac{2\pi k}{n}\right)$, which occurs when $k = 1$ or $k = n-1$, and so we must have $|H| = 2$. Then, we have that

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] = \frac{\varphi(n)}{|H|} = \frac{\varphi(n)}{2}.$$

And by our supposition, we know that $\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] = 2^k$, so we have that $\varphi(n) = 2^{k-1}$ hence $\varphi(n)$ must be a power of 2. Now suppose that $p_1^{n_1}p_2^{n_2}...p_t^{n_t}$ is the prime factorization of n. Then as shown on page 163 of Tattersall's book [10] Euler's phi-function is multiplicative. Thus,

$$2^k = \varphi(n) = \varphi(p_1^{n_1})\varphi(p_2^{n_2})...\varphi(p_t^{n_t})$$
$$= ((p_1-1)(p_1^{n_1-1}))((p_2-1)(p_2^{n_2-1}))...((p_t-1)(p_t^{n_t-1})).$$

So, we must have that for each $i = 1, ..., t$ either $p_i = 2$ or, $n_i = 1$ and $p_i - 1 = 2^{m_i}$, which implies that $p_i = 2^{m_i} + 1$, for some m_i, as desired.

($\Leftarrow$) Suppose that $n = 2^k p_1 p_2 ... p_t$ where $k \geq 0$ and each p_i is a prime of the form $p_i = 2^{m_i} + 1$ for some m_i. We want to show that an n-gon is constructible by showing that

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] = 2^k \text{ for some k.}$$

We know that

$$\varphi(n) = [\mathbb{Q}(\omega) : \mathbb{Q}] = |\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}|.$$

Then, by the Fundamental Theorem of Galois Theory, we know that

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] = |\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}| \,/\left|\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right|.$$

Then we have that,

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] = \varphi(n)/\left|\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right|.$$

Then we know from ($\Rightarrow$) that

$$\left|\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right| = 2.$$

So,

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] = \left|\text{Gal}\left(\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right)\right| = \varphi(n)/2.$$

Then we know that

$$\begin{aligned}\varphi(n) &= \varphi(2^k p_1 p_2 ... p_t)\\ &= \varphi(2^k)\varphi(p_1)\varphi(p_2)...\varphi(p_t)\\ &= 2^{k-1}(p_1^{1-1}(p_1-1))...(p_t^{1-1}(p_t-1)).\end{aligned}$$

Thus we have that

$$\varphi(n)/2 = 2^{k-2}(p_1-1)...(p_t-1).$$

Where $p_i = 2^{m_i}+1$. So we must have

$$\begin{aligned}\varphi(n)/2 &= 2^{k-2}(2^{m_1})(2^{m_2})...(2^{m_t})\\ &= 2^k \text{ for some k.}\end{aligned}$$

Hence,

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] = 2^k \text{ for some k.}$$

And so we have that this n-gon is constructible. □

We can now exactly characterize constructible polygons. We know that an n-gon is constructible if and only if $n = 2^k p_1 p_2 ... p_t$ where $k \geq 0$ and p_i is a prime such that $p_i = 2^{m_i}+1$. We have already seen that a triangle, square, pentagon, hexagon, and octagon are all constructible, but we can now say that a 17-gon is constructible as well as a 257-gon. In addition, even though we may not necessarily know how to construct a given n-gon with a straightedge and compass, we can determine whether or not it is possible.

Chapter 5

Origami

We will now use origami, or paper folding, to study some constructions that are not possible with only a straightedge and compass. In this section, the previous construction rules apply but we will add a new rule which allows us to create lines by folding the paper. Cox [3] gives us the following definition of a line constructed by origami.

Definition 5.0.1. *Given two points $a_1 \neq a_2$ not lying on lines $l_1 \neq l_2$, we can draw a new line l, called an origami line which reflects point a_1 to a new point b_1 lying on l_1 and reflects a_2 to a point b_2 on l_2. We will call this axiom, O_6.*

In this section, the rules of construction are as follows:
Starting with any two points,

- C_1: A circle can be created centered at any point and through another.
- C_2: A line can be drawn through any two points.
- C_3: A point can be created where any two lines intersect.
- C_4: A point can be created where a line intersects a circle.
- C_5: A point can be created where any two circles intersect.
- O_6: An origami line can be drawn as outlined in Definition 5.0.1.

Example 5.0.2. *We can trisect an angle using origami.*

We begin with a square piece of origami paper, created from lines j, k, l and m in Figure 5.1. Call the point of intersection between m and j point P_1. Then, draw a line through P_1, which is line n in our figures, that creates an arbitrary angle that we will call θ. This is angle $\measuredangle AP_1D$ in Figure 5.1. We will trisect this angle.

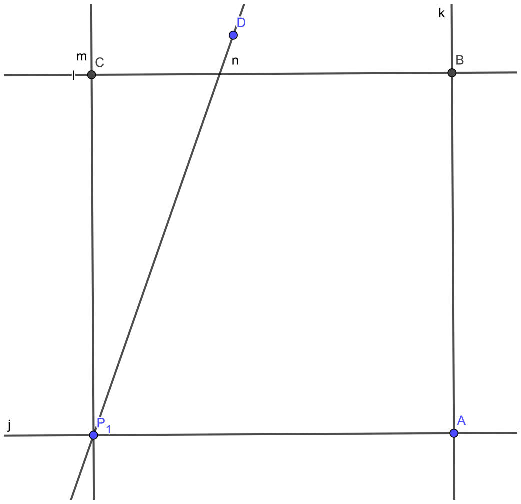

Figure 5.1: Origami Trisect 1

We will now make an origami line as in Definition 5.0.1 by reflecting P_1 to a point called P_2 on line m and point A to a new point, called F, on line k. Our origami line p is parallel to line j since j is perpendicular to both m and k. This line is the dotted line in in Figure 5.2.

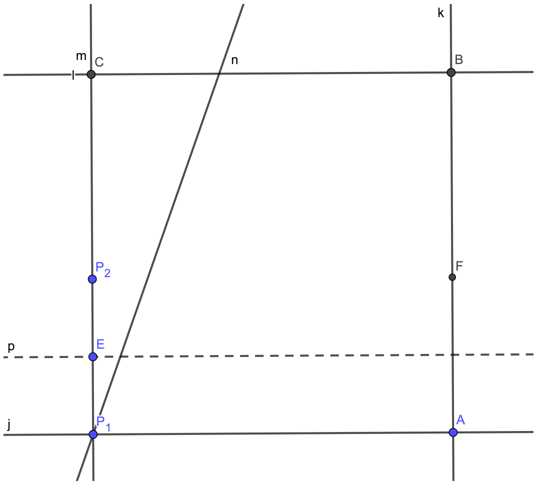

Figure 5.2: Origami Trisect 2

Now draw a line through points P_2 and F as in Figure 5.3.

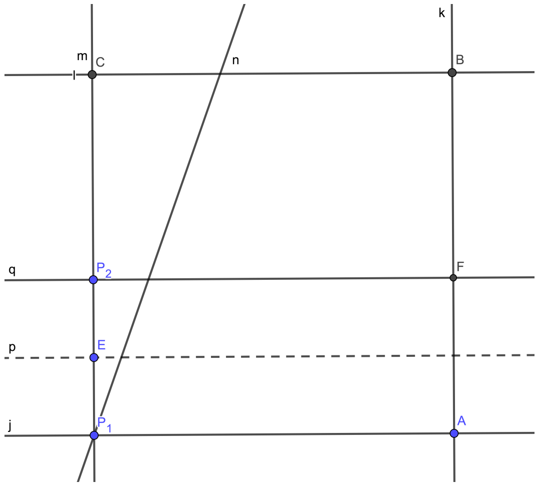

Figure 5.3: Origami Trisect 3

We will now fold another line. Fold the paper to reflect point P_1 to a new point on line p, called Q_1 and P_2 to a new point on line n, called Q_2. This can be seen as the dotted line r in Figure 5.4.

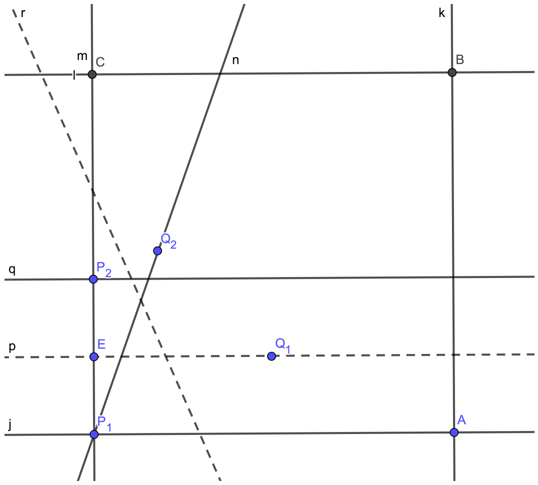

Figure 5.4: Origami Trisect 4

Lastly, we will draw a line through points P_1 and Q_1. It is easy to check that the angle created between lines j and this new line, s, is $\frac{\theta}{3}$ by folding the paper twice. We can also check that the angle is $\frac{\theta}{3}$ using the properties of similar triangles. Thus we have trisected our angle, and it can seen in Figure 5.5.

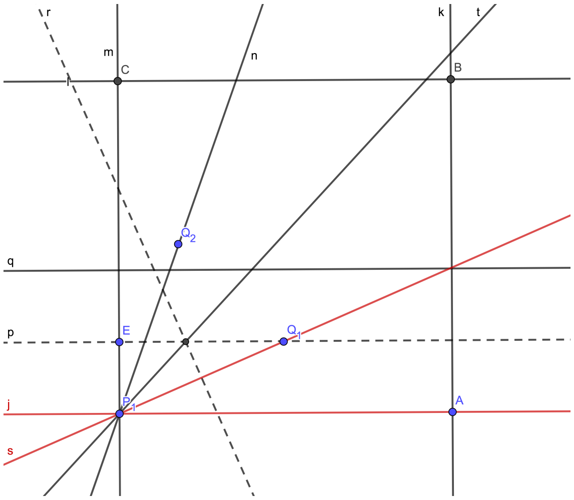

Figure 5.5: Origami Trisect 5

As we saw in Example 5.0.2, the rules of origami allow constructions that were previously impossible. We want to think about what allows us to create new lines by folding and what implications this leads to in terms of constructibility.

The lines we are creating can actually be represented as simultaneous tangents to parabolas. Start with a point P called the focus, and a line l, the directrix, as in Figure 5.6

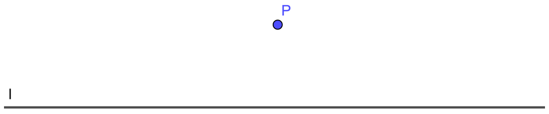

Figure 5.6: Simultaneous Tangents 1

Then, by definition, a parabola is all the points which are equidistance from our focus P and the directrix l. For example, we can take any point on the parabola - we use point A in Figure 5.7. Then, we have that the distance from point P to point A is equal to the distance between point A and line l if we drop a perpendicular line from A. This is true for any point on our parabola.

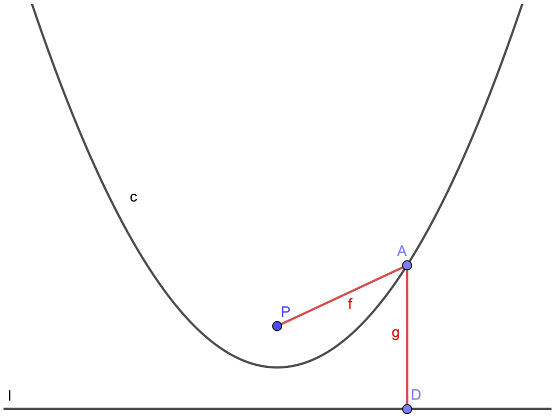

Figure 5.7: Simultaneous Tangents 2

Now consider the tangent line to the parabola at point A as in Figure 5.8. This line can be thought of as an origami line which reflects point P to point D on l.

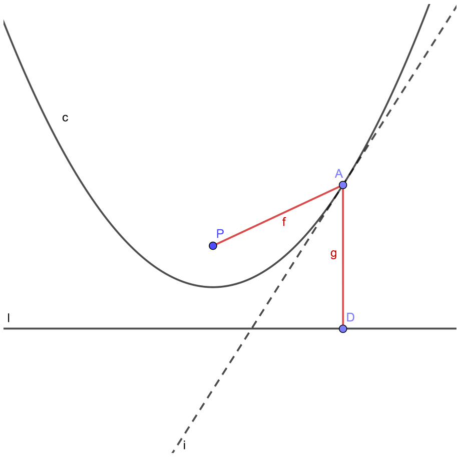

Figure 5.8: Simultaneous Tangents 3

For example, if we return to the example of trisecting an angle, we can look at the origami line in terms of simultaneous tangents. In Figure 5.9, we can draw a parabola with point P_1 as the focus and line p as the directrix. Then we have that the folded line r is tangent at a point which is equidistant to points P_1 and Q_1. Similarly, if we draw a parabola with P_2 as the focus and line n as the directrix, we have that the origami line r is tangent at a point equidistant from P_2 and Q_2.

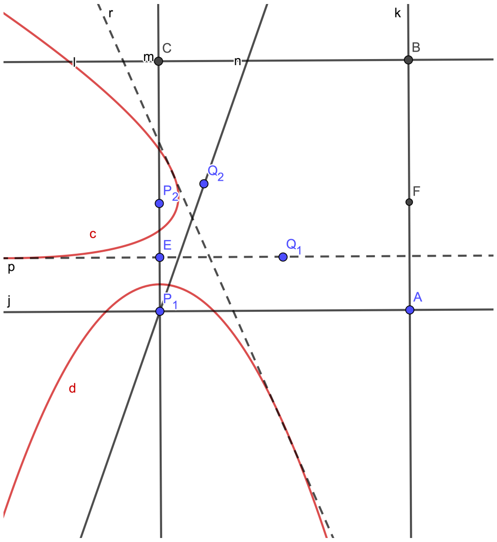

Figure 5.9: Simultaneous Tangents 4

Let $\mathbb{O}$ be the field of numbers which are constructible with origami. We want to be able to exactly describe all origami-constructible numbers. We continue to use the traditional construction rules in addition to origami, so we can still intersect lines and circles to get new points, which are in degree 1 or degree 2 field extensions. We will now look at the new points created with origami lines.

As outlined by Cox, [3] we will look at the simultaneous tangents of two parabolas

$$\left(y-\frac{1}{2}a\right)^2=2bx \text{ and } y=\frac{1}{2}x^2.$$

Starting with $\left(y-\frac{1}{2}a\right)^2=2bx$ we can use its derivative to find the slope of its tangent, which is

$$m=\frac{b}{y-\frac{1}{2}a}.$$

Then we can define a point (x_1,y_1) on the parabola in terms of m, and we have that $(x_1,y_1)=\left(\frac{b}{2m^2},\frac{b}{m}+\frac{a}{2}\right)$. Now looking at $y=\frac{1}{2}x^2$, we can find its derivative to show that the slope of its tangent line is

$$m=x.$$

Thus we have that $(x_2,y_2)=(m,\frac{m^2}{2})$. Now we will look at the slope formula,

$$m=\frac{y_2-y_1}{x_2-x_1}.$$

Using our points (x_1, y_1) and (x_2, y_2), we have

$$m = \frac{\dfrac{m^2}{2} - \left(\dfrac{b}{m} + \dfrac{a}{2}\right)}{m - \dfrac{b}{2m^2}} = \frac{m^4 - 2bm - am^2}{2m^3 - b}.$$

Thus m is the solution to the cubic equation,

$$m^3 + am + b = 0.$$

This gives us the fact that we can now solve any cubic $m^3 + am + b = 0$ where a and b are constructible using the simultaneous tangent of two parabolas.

Then Lee [8] explains how this implies that m is a constructible distance. We can construct m by dropping a perpendicular line which is a distance 1 from a constructible point on the simultaneous tangent line. This can be seen in Figure 5.10.

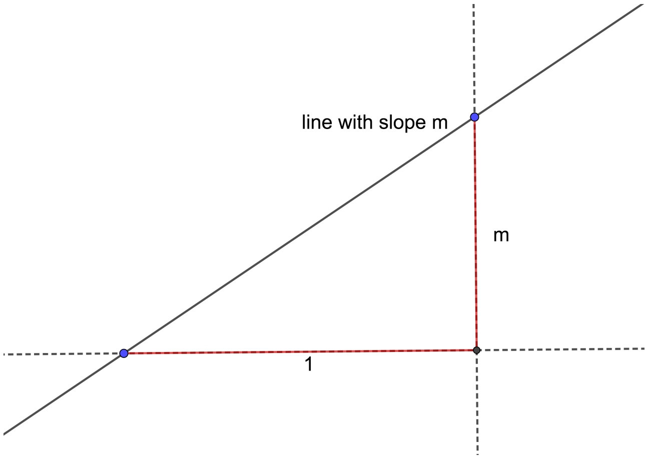

Figure 5.10: Constructing the Distance m

Then since m is the solution of an irreducible degree 3 polynomial, we must have that the degree of the extension from K to $K(m)$ is a degree 3 extension.

Let $x \in \mathbb{O}$. Then we can construct the length x in a finite number of steps using C_1, C_2, C_3, C_4, C_5 and O_6. Then since each of the steps for a construction is a degree 1,2, or 3 extension, multiplying the degree of each step gives us an extension of $2^k 3^j$ for some k. Thus, we have that $[\mathbb{Q}(x) : \mathbb{Q}] = 2^k 3^j$ for some integers k and j.

We can now prove that a heptagon is constructible using origami.

Theorem 5.0.3. *A heptagon is constructible with origami.*

Proof. As we did with the polygons in Chapter 2, in order to show that a heptagon is constructible, we need to adjoin an element to $\mathbb{Q}$ and find the degree of the field extension.

We know by Section 2.6, that if a heptagon is constructible then the length

$$\sin\left(\frac{2\pi}{7}\right) = \frac{1}{2}\sqrt{\frac{1}{3}\left(7 - \sqrt[3]{\frac{7+21\sqrt{-3}}{2}} - \sqrt[3]{\frac{7-21\sqrt{-3}}{2}}\right)}$$

is constructible. Thus, we want to determine if this length is constructible using origami. We can verify that $64x^6 - 112x^4 + 56x^2 - 7$ has $\sin\left(\dfrac{2\pi}{7}\right)$ as a root and using Theorem A.0.42, Eisenstein's Criterion, with $p = 7$ we see that this is the minimal polynomial of $\sin\left(\dfrac{2\pi}{7}\right)$. This polynomial has degree $6 = 2^1 3^1$. Hence, a heptagon is constructible using origami. □

We now want to characterize the n-gons that are constructible using origami.

5.1 Origami Constructibility Criterion

Theorem 5.1.1 (Origami Constructibility Criterion)**.** *A regular n-gon is constructible with origami if and only if $n = 2^a 3^b p_1 p_2 ... p_t$ where $a, b \geq 0$ and each p_i is a prime of the form $p_i = 2^{m_i} 3^{n_i} + 1$ for some m_i and n_i.*

Proof. ($\Rightarrow$) Suppose that a regular n-gon is constructible by origami. We will show that $n = 2^a 3^b p_1 p_2 ... p_t$ where $a, b \geq 0$ and p_i is a prime such that $p_i = 2^{m_i} 3^{n_i} + 1$. Since our n-gon is constructible, we know that $\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right) : \mathbb{Q}\right] = 2^k 3^j$. We know by Lemma 4.0.9 that $\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right) \subseteq \mathbb{Q}(\omega)$ where $\mathbb{Q}(\omega)$ is an extension of $\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)$ and $\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)$ is an extension of $\mathbb{Q}$. Then, since $\Phi_n(x)$, which has degree $\varphi(n)$, is the minimal polynomial of ω we have that $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n)$. Now, by field theory we have that

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = \left[\mathbb{Q}(\omega) : \mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right] \cdot \left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right) : \mathbb{Q}\right]$$

Then by the Fundamental Theory of Galois theory, or Theorem 4.0.12, we have that

$$\varphi(n) = \left|\text{Gal}(\mathbb{Q}(\omega))/\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right| \cdot \left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right],$$

or

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] = \frac{\varphi(n)}{\left|\text{Gal}(\mathbb{Q}(\omega))/\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right|}.$$

We also know that $\text{Gal}(\mathbb{Q}(\omega))/\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right) \leq \text{Gal}(\mathbb{Q}(\omega))/\mathbb{Q})$. Now, let $H = \text{Gal}(\mathbb{Q}(\omega))/\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)$ and let $G = \text{Gal}(\mathbb{Q}(\omega))/\mathbb{Q})$. Then we have that $H \leq G$. Now by the definition of the Galois group, Definition 4.0.8, we know that for all $\sigma \in H$, $\sigma(\omega) = \omega^k$ for some k, and $\sigma\left(\cos\left(\frac{2\pi}{n}\right)\right) = \cos\left(\frac{2\pi}{n}\right)$. But, $\omega = e^{\frac{2\pi i}{n}} = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$. Thus,

$$\sigma(\omega) = \sigma\left(\cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)\right)$$

$$= \sigma\left(\cos\left(\frac{2\pi}{n}\right)\right) + \sigma(i)\sigma\left(\sin\left(\frac{2\pi}{n}\right)\right).$$

We also have that $\sigma(\omega) = \omega^k = \cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right)$. Hence, $\cos\left(\frac{2\pi}{n}\right) = \cos\left(\frac{2\pi k}{n}\right)$, which occurs when $k = 1$ or $k = n - 1$. Thus, $|H| = 2$. Then, we have that

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] = \frac{\varphi(n)}{|H|} = \frac{\varphi(n)}{2}.$$

And by our supposition, we know that $\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] = 2^k 3^j$, so we have that $\varphi(n) = 2^l 3^j$, where $l = k - 1$. Let $q_1^{n_1} q_2^{n_2} ... q_r^{n_r}$ be the prime factorization of n. Then since Euler's phi-function is multiplicative [10] we have that

$$2^l 3^j = \phi(n) = ((q_1 - 1)(q_1^{n_1 - 1}))((q_2 - 1)(q_2^{n_2 - 1}))...((q_r - 1)(q_r^{n_r - 1})).$$

Thus, we must have that $q_i = 2$ or 3 or $q_i - 1 = 2^{m_i} 3^{n_i}$ for some m_i and n_i. Thus, we must have that $n = 2^a 3^b p_1 p_2 ... p_t$ where $p_i = 2^{m_i} 3^{n_i} + 1$.

($\Leftarrow$) Suppose that $n = 2^a 3^b p_1 p_2 ... p_t$ where $a, b \geq 0$ and $p_i = 2^{m_i} 3^{n_i} + 1$. We want to show that an n-gon is constructible by showing that

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] = 2^j 3^k \text{ for some j and k.}$$

We know that

$$\varphi(n) = [\mathbb{Q}(\omega) : \mathbb{Q}] = |\text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}|.$$

Then, by the Fundamental Theorem of Galois Theory, we know that

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] = |\text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}| \,/\, \left|\text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right|.$$

Then we have that,

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] = \varphi(n)/\left|\text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right|.$$

Then we know from ($\Rightarrow$) that

$$\left|\text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right| = 2.$$

So,

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] = \left|\text{Gal}\left(\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right)\right| = \varphi(n)/2.$$

Then we know that

$$\varphi(n) = \varphi(2^a 3^b p_1 p_2 ... p_t)$$
$$= \varphi(2^a)\varphi(3^b)\varphi(p_1)\varphi(p_2)...\varphi(p_t)$$

$$= 2^{a-1}3^{b-1}(p_1^{1-1}(p_1-1))...(p_t^{1-1}(p_t-1)).$$

Then we have that

$$\varphi(n)/2 = 2^{a-2}3^{b-1}(p_1-1)(p_2-1)...(p_t-1).$$

Where $p_i = 2^{m_i}3^{n_i}+1$. So we have that

$$\varphi(n)/2 = 2^{a-2}3^{b-1}(2^{m_1}3^{n_1})(2^{m_2}3^{n_2})...(2^{m_t}3^{n_t})$$

$$= 2^j3^k \text{ for some j and k.}$$

Thus, we have that

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] = 2^j3^k \text{ for some j and k.}$$

And so we have that this n-gon is constructible by origami.

□

We now know exactly which n-gons are constructible using origami. We have shown that a heptagon is constructible, but we also know that a 54-gon and a 22-gon are constructible with origami. We saw that with our traditional construction techniques that the following n-gons are constructible:

$$3, 4, 5, 6, 8, 10, 12, 15, 16, 17....$$

However, we now have that the following are constructible with origami:

$$3, 4, 5, 6, 7, 8, 9, 10, 12, 15, 16, 17, 18, ...$$

We can also return to the three problems of antiquity. We saw that we can trisect an angle with origami in Example 5.0.2, but we can also say that doubling a cube is possible with the addition of O_6 since $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Origami expanded our construction possibilities, and we now want to look at additional construction techniques.

Chapter 6

Geometric Approach to Solving Quintic Equations

We saw in Chapter 5 that an n-gon is constructible by origami if and only if $n = 2^k 3^j p_1 p_2 ... p_t$ where $j, k \geq 0$ and each p_i is a prime number of the form $p_i = 2^l 3^m + 1$. This is because our new origami construction axiom allowed us to construct solutions to cubic equations. We want to extend this further by creating a new construction axiom which would allow us to solve quintic equations. Suppose such an axiom exists. We will call it J_7. Now suppose that $\mathbb{J}$ is the field of numbers that are constructible using $C_1, C_2, C_3, C_4, C_5, O_6$ and J_7. Since J_7 allows us to solve quintic equations, it would give us the following results:

Proposition 6.0.1. *If a length $x \in \mathbb{J}$ then $[\mathbb{Q}(x) : \mathbb{Q}] = 2^a 3^b 5^c$ for some integers a, b and c.*

We have already seen that C_1, C_2, C_3, C_4, C_5 and O_6 give us field extensions of degree 2 and 3. Now with J_7, we have the addition of degree 5 extensions, and therefore we have that $[\mathbb{Q}(x) : \mathbb{Q}] = 2^a 3^b 5^c$.

Proposition 6.0.2. *An n-gon is constructible with $C_1, C_2, C_3, C_4, C_5, O_6$ and J_7 if and only if $n = 2^k 3^j 5^l p_1 p_2 ... p_t$ where $j, k, l \geq 0$ and p_i is a prime of the form $p_i = 2^{a_i} 3^{b_i} 5^{c_i} + 1$.*

Proof. ($\Rightarrow$) Suppose that a regular n-gon is constructible by origami. We will show that $n = 2^k 3^j 5^l p_1 p_2 ... p_t$ where $k, j, l \geq 0$ and $p_i = 2^{a_i} 3^{b_i} 5^{c_i} + 1$. Since our n-gon is constructible, we know that $\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right) : \mathbb{Q}\right] = 2^d 3^e 5^f$. We know by Lemma 4.0.9 that $\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right) \subseteq \mathbb{Q}(\omega)$ where $\mathbb{Q}(\omega)$ is an extension of $\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)$ and $\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)$ is an extension of $\mathbb{Q}$. Then, since $\Phi_n(x)$, which has degree $\varphi(n)$, is the minimal polynomial of ω we have that $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n)$. Now, by field theory we know

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = \left[\mathbb{Q}(\omega) : \mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right] \cdot \left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right) : \mathbb{Q}\right].$$

Then by the Fundamental Theory of Galois theory, Theorem 4.0.12, we must have that $\varphi(n) = \left|\mathrm{Gal}(\mathbb{Q}(\omega))/\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right| \cdot \left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right]$, or

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] = \frac{\varphi(n)}{\left|\mathrm{Gal}(\mathbb{Q}(\omega))/\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right|}.$$

We also know that $\mathrm{Gal}(\mathbb{Q}(\omega))/\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right) \leq \mathrm{Gal}(\mathbb{Q}(\omega))/\mathbb{Q})$. Now, let $H = \mathrm{Gal}(\mathbb{Q}(\omega))/\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)$ and let $G = \mathrm{Gal}(\mathbb{Q}(\omega))/\mathbb{Q})$. Then we have that $H \leq G$. Now by the definition of the Galois group, Definition 4.0.8, we know that for all $\sigma \in H$, $\sigma(\omega) = \omega^k$ for some k, and $\sigma\left(\cos\left(\frac{2\pi}{n}\right)\right) = \cos\left(\frac{2\pi}{n}\right)$. But, $\omega = e^{\frac{2\pi i}{n}} = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$. Thus,

$$\sigma(\omega) = \sigma\left(\cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)\right)$$

$$= \sigma\left(\cos\left(\frac{2\pi}{n}\right)\right) + \sigma(i)\sigma\left(\sin\left(\frac{2\pi}{n}\right)\right).$$

We also have that $\sigma(\omega) = \omega^k = \cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right)$. Hence, $\cos\left(\frac{2\pi}{n}\right) = \cos\left(\frac{2\pi k}{n}\right)$, which occurs when $k = 1$ or $k = n-1$. Thus, $|H| = 2$. Then, we have that

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] = \frac{\varphi(n)}{|H|} = \frac{\varphi(n)}{2}.$$

And by our supposition, we know that $\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] = 2^d3^e5^f$, so we have that $\varphi(n) = 2^m3^e5^f$, where $m = d-1$. Let $q_1^{n_1}q_2^{n_2}...q_r^{q_r}$ be the prime factorization of n. Thus

$$2^m3^e5^f = \varphi(n) = ((q_1-1)(q_1^{n_1-1}))((q_2-1)(q_2^{n_2-1}))...((q_r-1)(q_r^{n_r-1})).$$

Therefore, we must have $q_i = 2, 3$ or 5, or $q_i - 1 = 2^{a_i}3^{b_i}5^{c_i}$. Thus, we must have that $n = 2^k3^j5^lp_1p_2...p_t$ where p_i is a prime of the form $p_i = 2^a3^b5^c + 1$.

($\Leftarrow$) Suppose that $n = 2^k3^j5^lp_1p_2...p_t$ where $j, k, l \geq 0$ andp_i is a prime such that $p_i = 2^{a_i}3^{b_i}5^{c_i} + 1$. We want to show that an n-gon is constructible by showing that

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] = 2^d3^e5^f \text{ for some d,e and f.}$$

We know that

$$\varphi(n) = [\mathbb{Q}(\omega) : \mathbb{Q}] = |\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}|.$$

Then, by the Fundamental Theorem of Galois Theory, Theorem 4.0.12, we know that

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] = |\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}| \,/\, \left|\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right|.$$

Thus we have that,

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] = \varphi(n)/\left|\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right|.$$

Then we know from ($\Rightarrow$) that

$$\left|\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right| = 2.$$

So,

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] = \left|\mathrm{Gal}\left(\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right)\right| = \varphi(n)/2.$$

Then we know that

$$\begin{aligned}\varphi(n) &= \varphi(2^k 3^j 5^l p_1 p_2 ... p_t)\\ &= \varphi(2^k)\varphi(3^j)\varphi(5^l)\varphi(p_1)\varphi(p_2)...\varphi(p_t)\\ &= 2^{k-1}3^{j-1}5^{l-1}(p_1^{1-1}(p_1-1))...(p_t^{1-1}(p_t-1)).\end{aligned}$$

Then we have that

$$\varphi(n)/2 = 2^{k-2}3^{j-1}5^{l-1}(p_1-1)(p_2-1)...(p_t-1).$$

Where $p_i = 2^{a_i}3^{b_i}5^{c_i}+1$. So we have that

$$\varphi(n)/2 = 2^{k-2}3^{j-1}5^{l-1}(2^{a_1}3^{b_1}5^{c_1})...(2^{a_t}3^{b_t}5^{c_t})$$

$$= 2^d 3^e 5^f \text{ for some d,e and f.}$$

Hence,

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)/\mathbb{Q}\right] = 2^d 3^e 5^f \text{ for some d,e and f.}$$

And so we have shown that this n-gon is constructible using our original construction techniques, origami, and the addition of J_7. □

We now want to find some axiom which would allow us to solve quintic equations. In Lucero's article [9] a 2-fold axiom is described, in which there are 2 points, A and B and 3 lines, l,m, and n. We can then simultaneously fold 2 lines, α and β. The line α places A onto l and β places B onto m while aligning n and α. Alperin and Lang [2] also describe this 2-fold axiom. This axiom can be used to solve specific quintic equations, however, in general a degree n polynomial can be solved with n-2 simultaneous folds.

We will now look at a new axiom which starts with 3 points and 3 lines. We define J_7 as follows:

Definition 6.0.3. *Consider 3 distinct points, A, B and C, and three distinct lines, l, m and n such that A is not on l, B is not on m and C is not on n. Then a new line i, which we will call a J_7 line, can be drawn which reflects A to a point on l, B to a point on m and C to a point on n. This can be seen in Figures 6.1 and 6.2.*

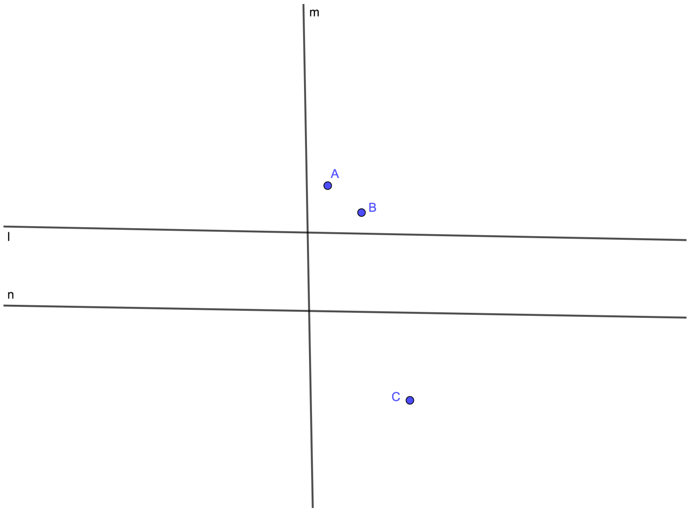

Figure 6.1: J_7 Line 1

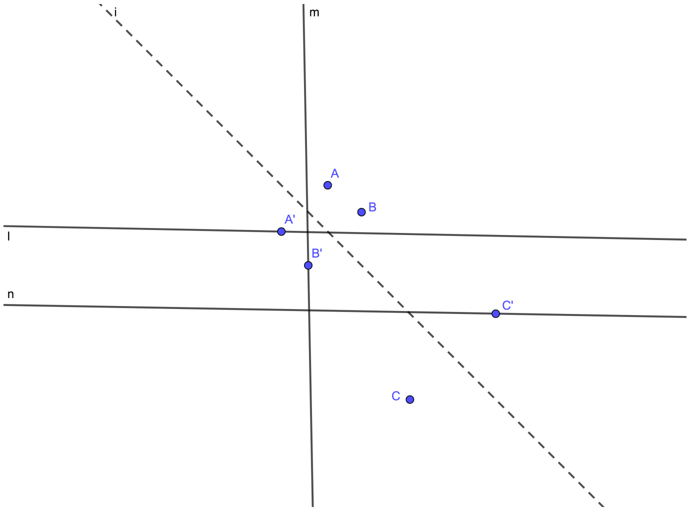

Figure 6.2: J_7 Line 2

Similar to an origami line, we can then see that this line is a simultaneous tangent to three different parabolas, as in Figure 6.3. Each of these parabolas is defined by its focus and directrix and the simultaneous tangent reflects each focus to a new point on the directrix.

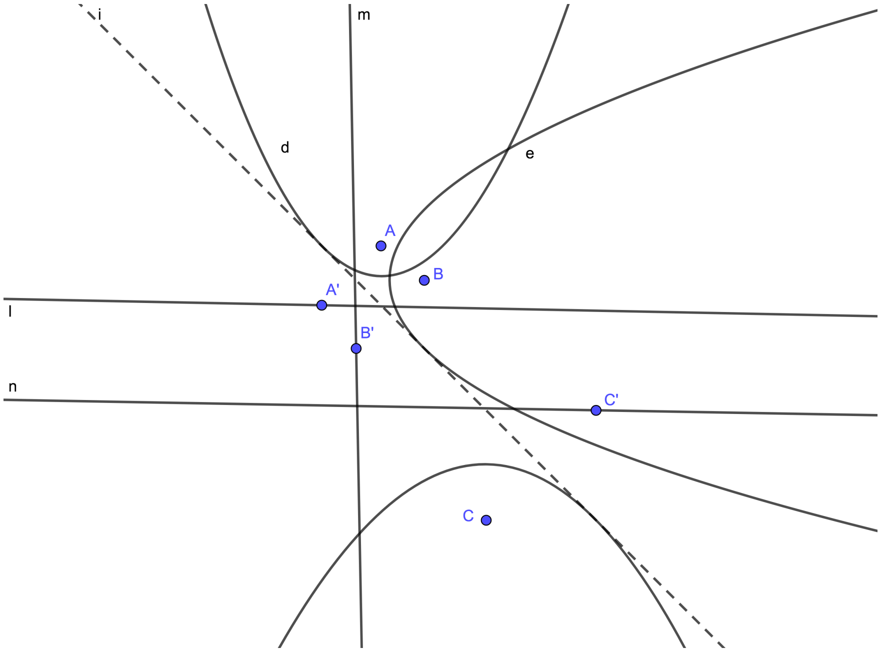

Figure 6.3: J_7 Line 3

As an example, we will now look at the simultaneous tangent of the three parabolas:

$$y = \frac{1}{2}x^2,\ x = \frac{1}{2}y^2, \text{ and } \left(y - \frac{1}{2}a\right)^2 = 2bx.$$

Starting with $y = \frac{1}{2}x^2$, we can find its derivative to show that the slope of its tangent line is

$$m = x.$$

Thus if we want to define a point (x_1, y_1) in terms of this parabola and m, we have that $x_1 = m$ and $y_1 = \frac{m^2}{2}$. We can follow the same process for $x = \frac{1}{2}y^2$. We have that the slope of its tangent is

$$m = \frac{1}{y}.$$

Thus, $(x_2, y_2) = \left(\frac{1}{2m^2}, \frac{1}{m}\right)$. Lastly, we will repeat the same process for $\left(y - \frac{1}{2}a\right)^2 = 2bx$. And we find that the slope of its tangent is

$$m = \frac{b}{y - \frac{1}{2}a}.$$

Then we have that $(x_3, y_3) = \left(\frac{b}{2m^2}, \frac{b}{m} + \frac{a}{2}\right)$.

Now, to find the simultaneous tangent to all three parabolas we want to find the solution for m when

$$\frac{y_2 - y_1}{x_2 - x_1} = \frac{y_3 - y_1}{x_3 - x_1}.$$

So if we plug in our values for $(x_1, y_1), (x_2, y_2)$ and (x_3, y_3) we have

$$\frac{\frac{1}{m} - \frac{m^2}{2}}{\frac{1}{2m^2} - m} = \frac{\frac{b}{m} + \frac{a}{2} - \frac{m^2}{2}}{\frac{b}{2m^2} - m}.$$

Then simplifying we have that

$$\frac{2m - m^4}{1 - 2m^3} = \frac{2bm + am^2 - m^4}{b - 2m^3}.$$

It then follows that

$$2am^5 + (3b - 3)m^4 - am^2 = 0.$$

Thus, m is the solution to a quintic equation.

6.1 Future Work

We have a shown a specific example of how the J_7 axiom allows us to solve a quintic equation. However, using origami we know that we can solve for any cubic equation, $m^3 + am + b = 0$ when a and b are constructible. We want to a similar conclusion using the J_7 fold. We want to be able to solve any quintic, $m^5 + am + b = 0$ where a and b are constructible. We could then look further to find a geometric solution to 7th degree polynomials, as well as looking at a simultaneous tangent to n parabolas where $n \geq 3$.

Bibliography

[1] Roger C Alperin. A mathematical theory of origami constructions and numbers. *New York J. Math*, 6(119):133, 2000.

[2] Roger C Alperin and Robert J Lang. One-, two-, and multi-fold origami axioms. *Origami*, 4:371–393, 2009.

[3] D.A. Cox. *Galois Theory*. Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. Wiley, 2012.

[4] B. Carter Edwards and Jerry Shurman. Folding quartic roots. *Mathematics Magazine*, 74(1):19–25, 2001.

[5] Euclid, T.L. Heath, and D. Densmore. *Euclid's Elements: all thirteen books complete in one volume : the Thomas L. Heath translation*. Green Lion Press, 2002.

[6] J. Gallian. *Contemporary Abstract Algebra*. Cengage Learning, 2016.

[7] Thomas C Hull. Solving cubics with creases: he ork of beloch and lill. *The American Mathematical Monthly*, 118(4):307–315, 2011.

[8] Hwa Young Lee. *Origami-constructible numbers*. PhD thesis, University of Georgia, 2017.

[9] Jorge C Lucero. On the elementary single-fold operations of origami: reflections and incidence constraints on the plane. *arXiv preprint arXiv:1610.09923*, 2016.

[10] James J Tattersall. *Elementary number theory in nine chapters*. Cambridge University Press, 2005.

[11] E.W. Weisstein. *CRC Concise Encyclopedia of Mathematics*. CRC Press, 2002.

Appendix A

Background Information

Bromwich Multiple Angle Formula

In his book, Eric Weisstein [11] outlined Bromwich's multiple angle formula as follows:

Theorem A.0.1. *For any given n value,*

$$\sin(na) = \begin{cases} nx - \dfrac{n(n^2-1^2)x^3}{3!} + \dfrac{n(n^2-1^2)(n^2-3^2)x^5)}{5!} - ... & \text{for } n \text{ odd} \\ n\cos(a)\left[x - \dfrac{(n^2-2^2)x^3}{3!} + \dfrac{(n^2-2^2)(n^2-4^2)x^5}{5!} - ...\right] & \text{for } n \text{ even.} \end{cases}$$

where $x = \sin(a)$.

Rings

The following can be found in Chapter 12, "Introduction to Rings," of Gallian's book [6].

Definition A.0.2. *A ring R is a set with two binary operations, addition (denoted by $a+b$) and multiplication (denoted by ab), 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. *That is, there is an element* 0 *in R such that* $a + 0 = a$ *for all a in R.*
4. *There is an element $-a$ in R such that* $a + (-a) = 0$.
5. $a(bc) = (ab)c$.
6. $a(b + c) = ab + ac$ *and* $(b + c)a = ba + ca$.

Example A.0.3. *Let G and H be additive abelian groups. Then the set $Hom(G, H) = \{\varphi : G \to H | \varphi$ is a homomorphism $\}$ is a ring under the operations $(\varphi + \psi)(x) = \varphi(x) + \psi(x)$ for all $x \in G$ and $(\varphi\psi)(x) = (\varphi \circ \psi)(x)$ for all $x \in G$.*

Definition A.0.4. *If $S \subseteq R$, R is a ring, and S is a ring with the same operations as R, then S is called a subring.*

Example A.0.5. *The set of Gaussian integers $\mathbb{Z}[i] = \{\ a + bi | a, b \in \mathbb{Z}\}$ is a subring of the complex numbers $\mathbb{C}$.*

Example A.0.6. *The set $\mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ where $\mathbb{Q}(\sqrt{d}) = \{x + y\sqrt{d} | x, y \in \mathbb{Q}\}$ is either a subring of $\mathbb{R}$ if $d \geq 0$ or a subring of $\mathbb{C}$ if $d < 0$.*

Integral Domains

The following is from Chapter 13, "Integral Domains," in Gallian's book [6].

Definition A.0.7. *A commutative ring with identity and no zero divisors is called an integral domain.*

Example A.0.8. *$\mathbb{R} \oplus \mathbb{R}$ is not an integral domain since it has zero divisors. For example,*

$$(1, 0) \cdot (0, 1) = (0, 0).$$

Theorem A.0.9. *Suppose D is an integral domain. Then if $a, b, c \in D$ and if $a \neq 0$, then $ad = ac \Rightarrow d = c$.*

Definition A.0.10. *If $a \in \mathbb{R}$, R is any ring, and a has a multiplicative inverse, then a is called a unit.*

Example A.0.11. *In $\mathbb{Q}$, every non-zero element is a unit.*

Definition A.0.12. *A field is a commutative ring with identity such that every non-zero element is a unit.*

Theorem A.0.13. *Every finite integral domain is a field.*

Ideals and Factor Rings

The following can be found in Chapter 14, "Ideals and Factor Rings," in Gallian's book [6].

Definition A.0.14. *If $A \subseteq R$ is a subring, then A is called an ideal if for all $r \in R$, and for all $a \in A$, $ra \in A$ and $ar \in A$.*

Theorem A.0.15. *If $A \subseteq R$, then A is an ideal if*

1. $a, b \in A \Rightarrow a - b \in A$
2. $a \in A$ *and* $r \in R \Rightarrow ra \in A$ *and* $ar \in A$.

Example A.0.16. *For any ring R, R and $\{0\}$ are ideals.*

Example A.0.17. *Let $a \in R$ and consider $\langle a \rangle = \{ra | r \in R\}$. This set is an ideal called the principal ideal generated by a.*

Theorem A.0.18. *Let A be a subring of R. Then A is an ideal if and only if $\{r + A | r \in R\}$ is a ring under*

$$(s + A) + (t + A) = (s + t + A)$$

$$(s + A)(t + A) = st + A.$$

Notation. If I is an ideal of R, we write $R/I = \{r + I | r \in R\}$.

Definition A.0.19. *Let A be an ideal of a commutative ring, R, and let $A \neq R$. Then if $ab \in A \Rightarrow a \in A$ or $b \in A$ then we say that A is a prime ideal.*

Definition A.0.20. *If A is a proper ideal of R such that whenever B is an ideal and $A \subseteq B \subseteq R$, implies that $B = A$ or $B = R$ then we call A a maximal ideal.*

Theorem A.0.21. *Suppose R is a commutative ring with identity. Then R/A is an integral domain if and only if A is prime.*

Theorem A.0.22. *Suppose R is a commutative integral domain. Then R/A is a field if and only if A is maximal.*

Ring Homomorphisms

The infromation on Ring Homomorphisms can be found in Chapter 15 of Gallian's book [6].

Definition A.0.23. *Let R,S be rings, and suppose that $\varphi : R \to S$ is a map such that*

$$\varphi(a + b) = \varphi(a) + \varphi(b)$$

$$\varphi(ab) = \varphi(a)\varphi(b).$$

Then we call φ a ring homomorphism.

Example A.0.24. *$\varphi : \mathbb{C} \to \mathbb{R}[x]/\langle x^2 + 1 \rangle$ is a ring homomorphism by the mapping $a + bi \longmapsto (a + bx) + \langle x^2 + 1 \rangle$.*

Example A.0.25. *$\varphi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}[x]/\langle x^2 - 2\rangle$ is a ring homomorphism by the mapping $a + b\sqrt{2} \longmapsto (a + bx) + \langle x^2 - 2\rangle$.*

Polynomial Rings

The following is from Chapter 16, "Polynomial Rings," in Gallian's book [6].

Theorem A.0.26. *If F is a field then $F[x]$ is a euclidean domain.*

Corollary A.0.27. *If F is a field, $a \in F$, $f(x) \in F[x]$, then $f(a) = 0$ if and only if $x - a|f(x)$.*

Theorem A.0.28. *A polynomial of degree n (over a field) has at most n zeros (counting multiplicity).*

Example A.0.29. *In the ring $\mathbb{Z}_{12}$ the polynomial $x^2 + 8$ has four zeros, 2,4,8, and 10.*

Theorem A.0.30. *Let F be a field. Then $F[x]$ is a principal ideal domain.*

Factorization of Polynomials

The following can be found in Chapter 17, "Factorization of Polynomials," of Gallian's book [6].

Theorem A.0.31. *Suppose F is a field, $f(x) \in F[x]$, and $deg(f(x)) \in \{2, 3\}$. Then $f(x)$ is reducible if and only if $f(x)$ has a zero in F.*

Theorem A.0.32. *If F is a field, and $p(x) \in F[x]$, then $\langle p(x)\rangle$ is maximal if and only if $p(x)$ is irreducible over F.*

Proof. ($\Rightarrow$) Suppose that $\langle p(x)\rangle$ is maximal in $F[x]$. We will show that $p(x)$ is irreducible over F. Let $p(x) = g(x)h(x)$ be a factorization of $p(x)$ over F. Then we have that $p(x) \in \langle g(x)\rangle$ so $\langle p(x)\rangle \subseteq \langle g(x)\rangle \subseteq F[x]$. Then since $\langle p(x)\rangle$ is maximal we must have that $\langle p(x)\rangle = \langle g(x)\rangle$ or $\langle p(x)\rangle = F[x]$.

Suppose that $\langle p(x)\rangle = \langle g(x)\rangle$. Then $p(x)$ and $g(x)$ are associates and they are equal up to units, so if $p(x) = g(x)h(x)$, we must have that $h(x)$ is a unit, and so $p(x)$ is irreducible.

Suppose that $\langle g(x)\rangle = F[x]$. Then we must have that $1 \in \langle g(x)\rangle$, thus $g^{-1}(x)g(x) = 1 \in \langle g(x)\rangle$ and so we must have that $g(x)$ is a unit and so $p(x)$ is irreducible.

($\Leftarrow$) Suppose that $p(x)$ is irreducible over F, and let I be an ideal of $F(x)$ such that $\langle p(x)\rangle \subseteq I \subseteq F[x]$. We want to show that $\langle p(x)\rangle$ is maximal by showing that $I = f[x]$ or $I = \langle p(x)\rangle$. Now, since F is a field, we know that $F[x]$ is a principal ideal domain. Thus, $I = \langle g(x)\rangle$ for some $\langle g(x)\rangle \in F[x]$. But, then $p(x) \in \langle g(x)\rangle$, and so $p(x) = g(x)h(x)$ for some $h(x) \in F[x]$. But then, we know that $p(x)$ is irreducible, so we must have that $g(x)$ is a unit or $h(x)$ is a unit.

Suppose $g(x)$ is a unit. Then $g^{-1}(x)g(x) = 1 \in I$, so we must have that $I = F[x]$.

Suppose $h(x)$ is a unit. Then we have that $p(x)$ and $g(x)$ are associates, since they are equal up to units. Hence, $\langle p(x) \rangle = \langle g(x) \rangle$. And so we have that in either case, $\langle p(x) \rangle$ is maximal. □

Extension Fields

The following can be found in Chapter 20, "Extension Fields," of Gallian's book [6].

Theorem A.0.33. *If F is a field and $f(x) \in F[x]$ then there exists E such that $F \subseteq E$ and $f(x)$ has a root in E.*

Proof. Suppose that there exists E such that $F \subseteq E$ and $f(x)$ has a root in E. Since $F[x]$ is a field, it has an irreducible factor, $p(x)$. So, we can let $E = F[x]/\langle p(x) \rangle$. Then we have that the mapping $\varphi : F \to E$ by $\varphi(a) = a + \langle p(x) \rangle$ is injective and per serves multiplication and addition. Then we want to show that $x + \langle p(x) \rangle$ is a root of $p(x)$, and thus a root of $f(x)$. Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_0$. Then we have

$$p(x + \langle p(x) \rangle) = a_n(x + \langle p(x) \rangle)^n + a_{n-1}(x + \langle p(x) \rangle)^{n-1} + ... + a_0$$

$$= a_n(x^n + \langle p(x) \rangle) + a_{n-1}(x^{n-1} + \langle p(x) \rangle) + ... + a_0$$
$$= a_n x^n + a_{n-1}x^{n-1} + ... + a_0 + \langle p(x) \rangle$$
$$= p(x) + \langle p(x) \rangle = 0 + \langle p(x) \rangle.$$

Hence, $x + \langle p(x) \rangle$ is a root of $p(x)$, as desired. □

Definition A.0.34. *Let E be an extension field of F and let $f(x) \in F[x]$ with degree at least 1. We say that $f(x)$ splits in E if there are elements $a \in F$ and $a_1, a_2, ..., a_n \in E$ such that*

$$f(x) = a(x - a_1)(x - a_2)...(x - a_n).$$

We call E a splitting field for $f(x)$ over F if

$$E = F(a_1, a_2, ..., a_n).$$

Algebraic Extensions

The following information is from Chapter 21, "Algebraic Extensions," of Gallian's book [6].

Definition A.0.35. *If E/F (E is a field extension of F) and $\forall u \in E$ we have that $f(u) = 0$ for some $f \in F[x]$ and $f \neq 0$, then we call this extension an algebraic extension.*

Example A.0.36. *$\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is an algebraic extension.*

Example A.0.37. *$\mathbb{C}/\mathbb{R}$ is an algebraic extension.*

Example A.0.38. *$\mathbb{Q}(\Pi)/\mathbb{Q}$ is not algebraic since π is not the root of any polynomial with rational coefficients.*

Theorem A.0.39. *Let E/F and $u \in F$ be algebraic. Let m be a monic polynomial of minimum degree such that $m(u) = 0$. Then*

1. *m is irreducible over $F[x]$*

2. *If $f \in F[x]$, then $f(u) = 0$ iff $m|f$.*

3. *m is unique (with respect to u).*

Proof. First, we will prove that m is irreducible. Suppose not, so m is reducible and we have that $m(x) = g(x)h(x)$ where $g(x)$ and $h(x)$ are not units. Then we must have that $m(u) = g(u)h(u)$ and we know that $m(u) = 0$, so $0 = g(u)h(u)$. But, since F is a field, it is an integral domain and so $f(u) = 0$ or $h(u) = 0$, but then m does not have minimal degree and hence we must have that m is irreducible.

Next, we will show that if $f \in F[x]$, then $f(u) = 0$ iff $m|f$.
($\Rightarrow$) Assume $f(u) = 0$. Then $m(u) = f(u)$. Then we have by the division algorithm that $f(u) = q(u)m(u) + r(u)$ where $deg(r(x)) < deg(m(x))$. But then since $f(u) = 0$, we must either have that $r = 0$ or $r(u) = 0$. But if $r(u) = 0$, this contradicts that m is the minimal polynomial, so we must have that $r = 0$, and thus $m|f$.
($\Leftarrow$) Assume that $m|f$. Then $f(x) = m(x)g(x)$ for some $g \in F[x]$. Thus we have that $f(u) = m(u)g(u)$ so $f(u) = (0)g(u)$ Thus, $f(u) = 0$.

Now to show that m is unique suppose it is not. Then there is another irreducible polynomial, n of minimal degree such that $n(u) = 0$. But then by (2) we have that $m|n$ and $n|m$. Thus $m = n$ and we must have that m is unique.

□

Definition A.0.40. *If u is algebraic over F, then m is called the minimal polynomial of u over F. We also write $d_F(u) = deg(m)$ for the degree of u/F.*

Corollary A.0.41. *If $p \in F[x]$ is monic, irreducible and $p(u) = 0$, then p is the minimal polynomial for u.*

Theorem A.0.42 (Eisenstein's Criterion). *Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$. Then, if p is prime and*

(i) $p \nmid a_n$

(ii) $p|a_{n-1}, ..., a_1, a_0$

(iii) $p^2 \nmid a_0$
Then $f(x)$ is irreducible over $\mathbb{Q}$.

Example A.0.43. *We can check that the minimal polynomial over $\sqrt{1+\sqrt{3}}$ is x^4-2x^2-2. We can see that $\sqrt{1+\sqrt{3}}$ is a root of x^4-2x^2-2, and applying Eisenstein's Criterion with $p=2$, we have that it is the minimal polynomial.*

Theorem A.0.44. *Let E/F and $u \in E$ be algebraic over F with $deg_F(u) = n$. Then,*

1. $F(u) = \left\{ \sum_{i=0}^{n-1} a_i u^i | a_j \in F \right\} = \{f(u)|f \in F[x]\}$.
2. $\{1, u, u^2, ..., u^{n-1}\}$ *is a basis for $F(u)/F$ as vector spaces.*
3. $F(u) \cong F[x]/\langle m \rangle$.