Constructible Polygons

Aaryan, Dylan, Helena, Jordi, Stephen

T-Shirt Talk, PROMYS 2022

1 Introduction

THE resolution of plane geometry problems with a straight-edge and a compass dates back to ancient Greece. These problems consist in constructing idealized geometric objects using only these two objects. In particular, there are 5 Euclidean commandments we are allowed to perform:

1. Create a line between two existing points.

2. Create a circle through one point with the center at another point.

3. Create a point from the intersection of two lines.

4. Create one or two points from the intersection(s) of a line and a circle.

5. Create one or two points from the intersection(s) of two circles.

In the plane, a line is determined by any two points on the line (different points) and a circle is determined by its center and any point contained in it.

The problems of straightedge-and-compass construction consist of using those tools to construct new geometric figures from other geometrical figures. More precisely: given a set of points in the plane $\{P_i \mid i \in I\}$, construct a point Q or a geometric figure via intersection and circles drawn from the given points or other previously constructed points.

Example 1.0.1. *Some easy constructions that can be obtained using a straight-edge and a compass are*

1. *the midpoint of two given points,*

2. *the perpendicular line at a point on a line.*

3. *the parallel line to a given line that passes through a given point.*

4. *the bisection of an angle.*

For many years, people tried to to solve the following three classical problems:

1. *Squaring the circle:* constructing a square with the same area of a given circle.

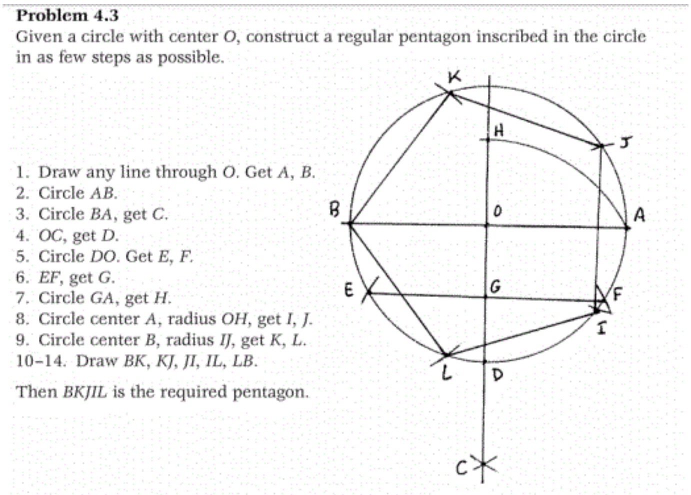
2. *Doubling the cube:* constructing a cub with twice the volume of a given cube.

3. *Trisection of an angle:* dividing a given angle into three equal angles.

Another classical problem that will be the main topic of these notes, is

4. *Construction of a regular polygon with n sides.*

For example, Figure 1 shows how to construct a regular pentagon.



Problem 4.3
Given a circle with center *O*, construct a regular pentagon inscribed in the circle in as few steps as possible.

1. Draw any line through *O*. Get *A*, *B*.
2. Circle *AB*.
3. Circle *BA*, get *C*.
4. *OC*, get *D*.
5. Circle *DO*. Get *E*, *F*.
6. *EF*, get *G*.
7. Circle *GA*, get *H*.
8. Circle center *A*, radius *OH*, get *I*, *J*.
9. Circle center *B*, radius *IJ*, get *K*, *L*.

10–14. Draw *BK*, *KJ*, *JI*, *IL*, *LB*.

Then *BKJIL* is the required pentagon.

K
H
J
B
O
A
E
G
F
I
L
D
C

Figure 1: Construction of a regular pentagon

Exercise 1.0.2. *Show that if we can construct a regular polygon of n sides, then we can construct a polygon of $2n$ sides. Show that if we can construct a polygon of m sides, and* $\gcd(m, n) = 1$*, we can construct a polygon of mn sides.*

The question still remains to characterize all possible constructible regular polygons.

Q:. *For what n is the n-sided regular polygon constructible?*

2 Constructible Lengths and Numbers

PROBLEMS of straight-edge and compass construction can be translated, introducing coordinates, to the construction of certain real or complex numbers, thought as points in the real line or the complex plane, starting from other given points. This interpretation translates a geometric problem into an algebraic problem and allows us to work with field extensions and apply Galois theory.

Consider two given points P_0 and P_1 in the plane. We can fix a coordinate system by setting $P_0 = (0,0)$ and $P_1 = (1,0)$. The x axis is the line that passes through these points and the y axis is its perpendicular line that passes through P_0. Once the axis are defined, any point in the plane is identified with a pair (x, y) of real numbers or with the complex number $x + iy$.

Given a coordinate system, the problems of straight-edge and compass construction can be translated in terms of complex numbers in the following way: given complex numbers $\{z_i \in \mathbb{C} \mid i \in I\}$, we ask whether a complex number $w \in \mathbb{C}$ can be obtained from the points z_i using only a straight-edge and a compass. If the answer is positive, we say that *w is constructible from the points z_i*.

Definition. We say that a real or complex number is **constructible** if it is constructible from the points 0 and 1.

Lemma 2.0.1. *A complex number is constructible if, and only if,*

(i) its real and imaginary parts are constructible, or also

(ii) its absolute value and its argument (as an angle) are constructible.

Proof. Note that the real and imaginary axis can be drawn from 0 and 1. Suppose $z = x + iy \in \mathbb{C}$ is constructible. To construct its real part, draw the line parallel to the imaginary axis that passes through z. Its intersection with the real axis is x. Analogously, we construct iy. The intersection of the circle of center 0 that passes through iy with the real axis are the poits y and $-y$. Conversely, form y we can draw iy. The parallel lines to the axis that passes through x and iy intersect in z.

Given $z \in \mathbb{C}$, its absolute values as the intersection of the circle with center 0 that passes through z and the real axis (on the positive part). Constructing its argument means drawing two lines which form an angle of $\arg(z)$. The line passing through 0 and 1 and the line passing through 0 and z satisfy this property. Conversely, given $r = |z|$ and two lines which form an angle α, via translation and homothety, we can suppose that α is given by the numbers 1, 0 and ω. Then, z

can be constructed as the intersection of the circle with center 0 that passes though r and the line that passes through 0 and ω. □

Lemma 2.0.2. *The classical problems can be translated in:*

- *Squaring of a circle* $\iff$ *constructing* $\sqrt{\pi}$.
- *Doubling of a cube* $\iff$ *constructing* $\sqrt[3]{2} \in \mathbb{R}$.
- *Trisecting of an angle* $\iff$ *given* $a \in [-1, 1]$, *construct a real root of the polynomial* $4x^3 - 3x - a$.
- *Constructing of a regular polygon with* n *sides* $\iff$ *constructing* $\cos(2\pi/n)$ $\iff$ *constructing* $e^{2\pi i/n}$.

Proof. The first two equivalences are pretty evident. For the third one, note that give an angle α is equivalent (by intersecting with the unit circle) to give its cosine. Hence, the trisection of an angle consist in constructing the number $\cos(\alpha)$ given the number $\cos(3\alpha)$. Let $a = \cos(3\alpha)$. Using the trigonometric addition and double-angle formulae we obtain

$$a = \cos(2\alpha)\cos(\alpha) - \sin(2\alpha)\sin(\alpha), \qquad \cos(2\alpha) = 2\cos^2(\alpha) - 1, \qquad \sin(2\alpha) = 2\sin(\alpha)\cos(\alpha),$$

and thus

$$a = \left(2\cos^2(\alpha) - 1\right)\cos(\alpha) - 2\sin^2(\alpha)\cos(\alpha) = 4\cos^3(\alpha) - 3\cos(\alpha)$$

From this, we get that $\cos(\alpha)$ is a root of the polynomial $4x^3 - 3x - a$.

For the last equivalence, we can suppose we wish to construct the regular n-gon inside the unit circle having 1 as one of its vertices. Then, the adjacent vertex will be $e^{2\pi i/n}$. Reversely, if we are given $e^{2\pi i/n}$, we can calculate all the vertices of the n-gon by calculating the powers of $e^{2\pi i/n}$ (we will see in Theorem 2.0.3 that this can be done). One can easily check that constructing $e^{2\pi i/n}$ is equivalent to constructing $\cos(2\pi/n)$. □

Theorem 2.0.3. *The set real constructible numbers is a subfield of* $\mathbb{R}$. *The set of constructible numbers is a subfield of* $\mathbb{C}$.

Proof. Let's first prove the first statement. By definition 0 and 1 are constructible. Thus it suffices to show that the real constructible numbers are closed under sum, addition and taking inverses. Let's first

Consider two constructible numbers $x, y \in \mathbb{R}$. Then, the numbers $x+y$ and $x-y$ are constructible, as they are the two intersections of the real axis with the circle with center $x = (x, 0)$ passing through the point (x, y) (note that $x+iy = (x, y)$ is easily constructed form x and y). In particular, the additive inverse of a real constructible number is constructible.

Consider now two constructible numbers $a, b \in \mathbb{R}$, $a \neq 0$. Let r be the line passing though $a = (a, 0)$ and $i = (0, 1)$, that has equation $x + ay - a = 0$. Now consider the line s parallel to r that passes through $ib = (0, b)$, that has equation $x + ay - ab$. The intersection of s with the real axis is ab. To calculate $1/a$, take the line t parallel to r that passes though $1 = (1, 0)$, that has equation $x + ay - 1$. Its intersection with the imaginary axis is $(0, 1/a)$. From this we easily get $1/a$.

The second statement follows from Lemma 2.0.1, as the sum and product of complex numbers, as well as their additive and multiplicative inverses, can be determined using field operations with its real and imaginary parts. □

Proposition 2.0.4. *If x is a positive real constructible number, then $\sqrt{x}$ is constructible. If z is a complex constructible number, then its square roots are constructible.*

Proof. Let $x > 0$. The points $(1, \pm\sqrt{x})$ are the two intersections of the vertical line passing through $(1, 0)$ with the circle with center $\left(\frac{1+x}{2}, 0\right)$ passing through $(0, 0)$.

Now let $z \in \mathbb{C}$ be a nonzero constructible number. By Lemma 2.0.1, we can construct $|z|$ and $\arg(z)$. Then $\sqrt{|z|}$ is constructible and as mention in Example 1.0.1 we can bisect the angle $\arg(z)$. From this and applying Lemma 2.0.1 again, we easily obtain the two square roots of z. □

Proposition 2.0.5. *The line and the circle determined by two constructible numbers have equations of the form*

$$aX + bY + c = 0, \qquad X^2 + Y^2 + \alpha X + \beta Y + \gamma = 0$$

where the coefficients are real constructible numbers. In addition, the intersection of lines and circles like these can be calculated form its coefficients using field operations and (at most) one square root.

Proof. Let $z_1 = x_1 + iy_1$ and $z_2 = x_2 + iy_2$ be different constructible numbers. The line passing through this points have equation

$$(y_2 - y_1)X + (x_1 - x_2)Y + (y_1x_2 - x_1y_2) = 0$$

and the circle with center the first point passing through the second point has equation

$$X^2 + Y^2 - 2x_1X - 2y_1Y + \left(2x_1x_2 + 2y_1y_2 - x_2^2 - y_2^2\right) = 0.$$

In both cases, the coefficients are obtain using field operations with real and imaginary parts of z_1 and z_2 and hence are real constructible numbers.

Reciprocally, given two nonparallel lines $a_1X+b_1Y+c_1 = 0$ and $a_2X+b_2Y+C = 0$, the intersection point is

$$\begin{pmatrix} x \\ y \end{pmatrix} = -\begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}^{-1} \begin{pmatrix} c_1 \\ c_2 \end{pmatrix},$$

and thus is coordinates are obtained from the coefficients using field operations.

The intersection points of a line and a circle with given equations are obtained isolating one of the variables in the equation of the line, substituting it in the circle equation, and solving a quadratic equation, that has coefficients obtained form the line and the circle using field operations. If the discriminant of this equation is negative it means that the intersection is empty. If its non-negative, the intersection points are obtained from the coefficients using field operations and one square root.

Finally, given two circles with non-empty intersection, subtracting the two equations we obtain the equation of a line that passes through their intersection point(s). Hence, the intersection of two circles is obtained as the intersection of a line and a circle. □

An important consequence of the two previous propositions is stated in the following theorem.

Theorem 2.0.6. *The constructible numbers are precisely the complex numbers obtained from the rational numbers using field operations and calculating square roots.*

Proof. Note than, since 0 and 1 are constructible, using field operations we easily obtain the rational numbers. Thus, by Theorem 2.0.3 and Proposition 2.0.4, any number obtain from $\mathbb{Q}$ using field operations and square roots will be constructible. Proposition 2.0.5 assures that, in fact, this are all the operations we can do. □

3 Field Extensions and Minimal Polynomials

Theorem 3.0.1. $\cos\left(\frac{2\pi}{n}\right)$ *is constructible* $\implies$ $\phi(n)$ *is a power of 2, where* ϕ *is Euler's totient function.*

LET α be some constructible number. We start with 1, perform some field operations, remaining in $\mathbb{Q}$. At some point, perhaps we take some square root of something that is not a square in $\mathbb{Q}$. Let this value be a. Thus, $\alpha \notin \mathbb{Q}$, but it *could be* in $\mathbb{Q}[\sqrt{a}]$. Suppose we continue doing some field operations with elements in $\mathbb{Q}[\sqrt{a}]$, and then we take the square root of something that is not a square in $\mathbb{Q}[\sqrt{a}]$, let this value be b. Thus, $\alpha \notin \mathbb{Q}[\sqrt{a}]$, but it *could be* in $(\mathbb{Q}[\sqrt{a}])[\sqrt{b}]$.

We continue this process, and at some point it must terminate, since the construction must only use a finite number of steps. We then conclude that $\alpha \in ((\mathbb{Q}[\sqrt{a_1}])[\sqrt{a_2}] \cdots)[\sqrt{a_n}]$.

Definition. Given a field K, a **field extension** L/K (read as "L over K") is a larger field L such that $K \subseteq L$. Yes, writing like that is weird, but it'll be okay. I promise. If K is extended by adjoining the square root of a non-square a, then $K[\sqrt{a}]$ is called a **quadratic field extension**.

Example 3.0.2. *$\mathbb{R}$ is field extension of $\mathbb{Q}$, and $\mathbb{C}$ is a quadratic field extension of $\mathbb{R}$.*

Observation. *Given a field K and a quadratic extension $K[\sqrt{a}]$, we need two representatives from K to represent an element of $K[\sqrt{a}]$.*

Definition. The **degree** of a finite field extension, denoted by $[L : F]$, is defined to be the dimension of L where L is viewed as an F-vector space.

In other words, the degree is the number of representatives from F we need to uniquely identify every element of L.

Example 3.0.3. *Consider the field $\mathbb{Q}(\sqrt{2})$ which we played around a lot with at PROMYS. We can see that it is a field extension over $\mathbb{Q}$, i.e., that $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. Since every element in this field has the form $a + b\sqrt{2}$ for arbitrary $a, b \in \mathbb{Q}$, the clever way of viewing this field is as the linear algebraic span of the set $\{1, \sqrt{2}\}$ over $\mathbb{Q}$. Indeed, this set is a basis of $\mathbb{Q}(\sqrt{2})$ if we view it as a $\mathbb{Q}$-vector space (i.e. a vector space over $\mathbb{Q}$), so we say that $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.*

Lemma 3.0.4. *If E_1 is an m-extension of a field F, and E_2 is an $n-$extension of E_1, then $[E_2 : F] = [E_2 : E_1] \times [E_1 : F] = mn$.*

Proof. We know that every element $\alpha \in E_2$ can be written using n representatives from E_1, i.e:

$$\alpha = a_1 e_1 + a_2 e_2 + \cdots a_n e_n,\ a_i \in E_1, e_i \in E_2 \forall i$$

Moreover, each a_i can be written as:

$$a_i = f_1 b_1 + f_2 b_2 + \cdots f_m b_m, \ f_j \in F, b_j \in E_1 \forall j$$

Substituting each a_i, we get:

$$\begin{aligned} \alpha &= \sum_{i=1}^{n} a_i e_i \\ &= \sum_{i=1}^{n} \left(\sum_{j=1}^{m} f_j b_j \right) e_i \\ &= \sum_{k=1}^{mn} f_k (b_k e_k) \end{aligned}$$

And letting $\alpha_k = b_j e_i$ any pair (i, j), we observe that we need *at least* mn elements to represent every element of E_2, and the big summation above shows that mn elements is sufficient.

□

Corollary 3.0.4.1. *In $((\mathbb{Q}[\sqrt{a_1}])[\sqrt{a_2}] \cdots)[\sqrt{a_n}])$, we will need 2^n representatives of $\mathbb{Q}$ to represent every element uniquely.*

Definition. Suppose E is an extension of F. The **minimal polynomial** of $\alpha \in E$ is the smallest polynomial in $F[x]$ for which α is a root. It is denoted $\mathrm{Irr}(\alpha, F, x)$

Exercise 3.0.5. *Show that the degree of a minimal polynomial of any $\alpha \in ((\mathbb{Q}[\sqrt{a_1}])[\sqrt{a_2}] \cdots)[\sqrt{a_n}])$ is at most 2^n.*

Lemma 3.0.6. *If α is constructible, then its minimal polynomial in $\mathbb{Q}[x]$ has degree 2^m for some $m \in \mathbb{N}$.*

Proof. Let α be in $((\mathbb{Q}[\sqrt{a_1}])[\sqrt{a_2}] \cdots)[\sqrt{a_n}])$. Take $\mathbb{Q}[\alpha]$, and consider the sum:

$$q_0 + q_1 \alpha + q_1 \alpha^2 + \cdots,$$

where $q_i \in \mathbb{Q}$. Note that at some point, we must be able to generate all of $\mathbb{Q}[\alpha]$, since by Exercise 3.0.5, α is the root of a polynomial of degree $k \leq 2^n$, and so eventually we will get that:

$$\alpha^k = q_0 + q_1 \alpha + \cdots + q_{k-1} \alpha^{k-1},$$

since that is the definition of α being the root of a degree k polynomial in $\mathbb{Q}[x]$. Note that this means that everything in $\mathbb{Q}[\alpha]$ can be represented using k representatives from $\mathbb{Q}$, thus $[\mathbb{Q}[\alpha] : \mathbb{Q}] = k$.

Moreover, recall that since $\alpha \in ((\mathbb{Q}[\sqrt{a_1}])[\sqrt{a_2}] \cdots)[\sqrt{a_n}])$, then $\mathbb{Q}[a] \subseteq ((\mathbb{Q}[\sqrt{a_1}])[\sqrt{a_2}] \cdots)[\sqrt{a_n}])$.

By Lemma 3.0.4, we deduce that $[\mathbb{Q}[\alpha] : \mathbb{Q}] = k \mid [((\mathbb{Q}[\sqrt{a_1}])[\sqrt{a_2}] \cdots)[\sqrt{a_n}]) : Q] = 2^n$.

Thus, $k \mid 2^n$ and so k must also be a power of 2, as desired. □

Thus, any constructible number has minimal polynomial of degree that is some power of 2. How can we relate this to $\cos\left(\frac{2\pi}{n}\right)$? The answer is: roots of unity.

Fact. *The nth primitive root of unity ζ_n is a complex solution to $x^n - 1 = 0$ in $\mathbb{Q}[x]$, and it holds that:*

$$\zeta_n = e^{2\pi i/n} = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$$

Lemma 3.0.7. *The minimal polynomial of ζ_n has degree $\phi(n)$.*

Proof. Note that we have:

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

However, let d be a (non-1) divisor of n. Then, the powers of ζ_n^d generate the (n/d)th roots of unity. Thus, let $p_1, p_2..p_m$ be the distinct prime divisors of n. Note that their multiples generate all the numbers that are not coprime to n. Thus, $\zeta_n^{p_i}, (\zeta_n^{p_i})^2...$ give us the n/p_i roots of unity, and from this we deduce that:

$$\prod_{k=1}^{n/p_i} (x - (\zeta_n^{p_i})^k) = x^{n/p_i} - 1 \in \mathbb{Q}[x]$$

We can thus divide out by all such factors, and we will be left with all the powers of ζ_n that are coprime to n. Since all the other polynomials we divided out by were in $\mathbb{Q}[x]$, it follows that:

$$\Phi_n := \prod_{k:\gcd(k,n)=1}^{n} (x - \zeta_n^k) \in \mathbb{Q}[x]$$

Observe that the degree of Φ_n is $\phi(n)$. To show that this is the minimal polynomial of ζ_n, we want to show it is irreducible. We outline a sketch proof, and leave the details to the reader.

Let $f(x)$ be a factor of Φ_n such that $f(\zeta_n) = 0$. Then, we make the observation that $f(\zeta_n^p) = 0$ for any prime p coprime to n (show this!). Doing this allows us to generate all ζ_n^k with $\gcd(k, n) = 1$, however. Thus, we deduce that $f(x)$ must have degree $\phi(n)$ and thus must be equal to Φ_n.

□

We now have all the tools to prove the desired theorem.

Proof of Theorem 3.0.1. We want to show that if $\cos\left(\frac{2\pi}{n}\right)$ is constructible, then $\phi(n)$ is a power of 2, let it be 2^m.
We know from Lemma 3.0.6 that the degree of the minimal polynomial of $\cos\left(\frac{2\pi}{n}\right)$ in $\mathbb{Q}[x]$ is a power of 2, by assumption of it being constructible. We now consider $\mathbb{Q}[\cos\left(\frac{2\pi}{n}\right)]$.
Note $\zeta_n \in \mathbb{Q}[i] \not\subseteq \mathbb{Q}[\cos\left(\frac{2\pi}{n}\right)]$. Let's take the following polynomial:

$$x^2 - 2\cos\left(\frac{2\pi}{n}\right)x + 1$$

Observation. *ζ_n is a root of the polynomial above.*

Thus, we conclude that ζ_n has minimal polynomial 2 in $\mathbb{Q}[\cos\left(\frac{2\pi}{n}\right)][x]$, and thus it lies in a quadratic extension of $\mathbb{Q}[\cos\left(\frac{2\pi}{n}\right)]$, which we can denote K for now.

By Lemma 3.0.4, we have that $[K : \mathbb{Q}] = [K : \mathbb{Q}[\cos\left(\frac{2\pi}{n}\right)] \times [\mathbb{Q}[\cos\left(\frac{2\pi}{n}\right)] : \mathbb{Q}] = 2 \times 2^m = 2^{m+1}$.

Finally, by Lemma 3.0.7, we have that $[K : \mathbb{Q}] = \phi(n) = 2^{m+1}$, which is what we wanted to show.

□

4 Group and Galois Theory

We know that in order for an n-sided regular polygon to be constructible, $\phi(n)$ must be some power of 2. However, is the converse true? If we take any n such that $\phi(n) = 2^m$, does there always exist a sequence of constructions or quadratic field extensions that contain that number? The answer is in fact: yes!

Proving this reverse direction, however, requires a lot more mathematical machinery. Here come a blitz of definitions and lemmas for the group theory and Galois theory required to prove the reverse direction. We recommend taking an abstract algebra course to learn more.

Definition. $\alpha \in \mathbb{C}$ is said to be **algebraic** if it is the root of a nonzero polynomial with rational coefficients.

Definition. Let $f \in F[x]$ have degree $n > 0$. Then a field extension $F \subset L$ is a **splitting field** of f over F if

1. $f = c(x - \alpha_1)...(x - \alpha_n)$ where $c \in F$ and $\alpha_i \in L$, and
2. $L = F(\alpha_1, ..., \alpha_n)$.

   We say that $f \in F[x]$ **splits completely** over F.

Example 4.0.1. $\mathbb{Q}(\sqrt{2})$ *is the splitting field of* $f(x) = x^2 - 2$ *over* $\mathbb{Q}$. $\mathbb{Q}(\sqrt{2}, i)$ *is the splitting field of* $g(x) = x^2 + 2$ *over* $\mathbb{Q}$.

Definition. A **group** is a pair $(G, *)$, with $* : G \times G \to G$ a binary operation on G, such that the following properties hold:

- G is **associative** under $*$: for all $a, b, c \in G$,

$$(a * b) * c = a * (b * c).$$

- There exists an **identity element** $e \in G$ such that $e * a = a * e = a$ for all $a \in G$.
- For each element $a \in G$, there exists an **inverse element** $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$.

Definition. If $|G|$ is finite we say the group is **finite**, and **infinite** otherwise. We call $|G|$ the **order** of the group.

Definition. A subset $H \subseteq G$ which is also a group under $*$ is called a **subgroup**.

Definition. A subgroup H of G is called **normal** if for all $g \in G$, $h \in H$, then $ghg^{-1} \in H$.

Example 4.0.2. $\mathbb{Z}$ *is a group under addition, and* $\mathbb{Z}_m$ *is a group under addition mod* m*. The set of symmetries of a regular* n*-gon is a group under composition, which is known as the* ***dihedral group*** D_n*. The subgroup of rotations of the* n*-gon is a normal subgroup of* D_n*.*

Example 4.0.3. *The set of permutations on a set of* n *elements is a group under composition, and is called the* ***symmetric group*** S_n*. The set of even permutations is called the alternating group*

A_n.

Definition. A finite group G is **solvable** if there exist subgroups $G_0, \ldots, G_n$ such that

$$\{e\} = G_n \subset G_{n-1} \subset ... \subset G_1 \subset G_0 = G$$

and

1. G_i is a normal subgroup of G_{i-1} and
2. $[G_{i-1} : G_i] = p$ for some prime p.

Solvable groups can be infinite too, but we won't talk about those here.

Example 4.0.4. *S_4 is a solvable group. See if you can see why!*

Lemma 4.0.5. *All groups of order p^k for some prime p (p-groups) are solvable.*

Lemma 4.0.6. *Let $F \subset L$ be a finite field extension and let G be its Galois group. Then $F \subset L$ is a Galois extension, i.e. $|G| = [L : F]$, if and only if F is a splitting field over L.*

Definition. A map $\sigma : F \to F$ from a field to itself is called an **automorphism** if it preserves addition and multiplication. In other words, for all $a, b \in F$,

$$\sigma(a + b) = \sigma(a) + \sigma(b),$$

and

$$\sigma(a \cdot b) = \sigma(a) \cdot \sigma(b).$$

Definition. Let $F \subset L$ be a finite field extension. The **Galois group** of $F \subset L$, $\mathrm{Gal}(L/F)$, is the set of automorphisms of L which *fixes* the base field. In other words, it is the set of automorphisms $\sigma : L \to L$ such that $\sigma(a) = a$ for all $a \in F$.

Definition. Given a finite field extension $F \subset L$ and a subgroup $H \subset \mathrm{Gal}(L/F)$, there exists a subfield of L containing F which we call the fixed field:

$$L^H = \{\alpha \in L : \sigma(\alpha) = \alpha, \forall \sigma \in H\}.$$

Exercise 4.0.7. *Show that* $\mathrm{Gal}(L/F)$ *is a group under composition.*

Theorem 4.0.8 (The Galois Correspondence)**.** *Let L be a Galois extension of a field F, and let G be its Galois group. There is a bijective correspondence between subgroups of G and intermediate fields. In particular, this is the arrow given below:*

$$\{\textit{subgroups } H \textit{ of } G\} \longleftrightarrow \{\textit{intermediate fields } K \textit{ of a Galois extension}\}$$

where $H \mapsto K^H$ and $L \mapsto G(K/L)$ are the explicit mappings.

Theorem 4.0.9. *Let $\alpha \in \mathbb{C}$ be algebraic over $\mathbb{Q}$. Let $\mathbb{Q} \subset L$ be a splitting field of Irr$(\alpha, \mathbb{Q}, x)$. Then α is constructible if $[L : \mathbb{Q}] = 2^m$.*

Proof. Let $[L : \mathbb{Q}] = 2^m$ for some m. Then, since $\mathbb{Q}$ is a splitting field of the minimal polynomial of α over L, $\mathbb{Q} \subset L$ is a Galois extension and $|\mathrm{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}] = 2^m$.
Since 2 is prime, $\mathrm{Gal}(L/\mathbb{Q})$ is a p-group, and therefore $\mathrm{Gal}(L/\mathbb{Q})$ is solvable. So there exist subgroups $\{e\} = G_n \subset G_{n-1} \subset ... \subset G_1 \subset G_0 = \mathrm{Gal}(L/\mathbb{Q})$ such that G_i is normal in G_{i-1} and $G_{i-1}/G_i \cong \mathbb{Z}/2\mathbb{Z}$.
By the Galois correspondence, there exist fixed subfields $F_i = L^{G_i}$ such that $\mathbb{Q} = F_0 \subset F_1 \subset ... \subset F_m = L$, where $[F_i : F_{i-1}] = 2$. So, by the Constructible Criterion, α is constructible. □

In fact, this is an "if and only if" statement, however proof of the other direction will be omitted.

Now we have all the necessary information to prove the following theorem:

Theorem 4.0.10. $\phi(n) = 2^m \implies \zeta_n$*, where ζ_n is the n-th root of unity, is constructible.*

Proof. ζ_n is algebraic over $\mathbb{Q}$ and $\mathbb{Q} \subset L$ is a splitting field of $\mathrm{Irr}(\zeta_n, \mathbb{Q}, x)$. $\varphi(n) = [\mathbb{Q} : \mathbb{Q}]$, so this follows from Theorem 4.0.5. □

5 Synthesis

AT last, we have our main result. We began by showing that any length on the plane that was constructible corresponded to an element of a chain of quadratic field extensions of $\mathbb{Q}$. This allowed us to prove the forward direction. For the reverse direction, we looked at the Galois correspondence between a field extension and its Galois group. This shows us that *anytime* $\phi(n)$ is a power of 2, there is a chain of quadratic extensions corresponding to that nth root of unity, and hence $\cos\left(\frac{2\pi}{n}\right)$. Let us describe our result more in the language of number theory.

Definition. A prime of the form $2^{2^m} + 1$ is known as a **Fermat prime**.

It's useful to show that if $k > 0$ and $2^k + 1$ is prime, then $k = 2^m$ for some $m \in \mathbb{N}$. It is unknown whether the Fermat primes go on forever, or even if there are any more we haven't found yet. The only known Fermat primes are 3, 5, 17, 257, and 65537.

Corollary 5.0.0.1 (Gauss-Wantzel)**.** *A n-sided regular polygon is constructible if and only if n is a product of a power of* 2 *and distinct Fermat primes (including none).*

Proof. If $n = 2^k$, then note that $\phi(2^k) = 2^{k-1}$, meaning we're done. So, assume the factorization of n contains at least one Fermat prime. Then, Since ϕ is multiplicative, we can write

$$\phi(n) = \phi(2^k)\phi(p_1)\cdots\phi(p_j),$$

where $p_1, \ldots, p_j$ are distinct Fermat primes. If $p_i = 2^{2^\ell} + 1$, then $\phi(p_i) = 2^{2^\ell}$, and combining this with our results from before gets us our result.
The reverse direction is left as an exercise, but it's not too bad. □

Gauss proved the 17-gon (or a heptadecagon) was constructible in 1796 at the age of 19. NINETEEN! He was so proud of this result that he wanted to put a 17-gon on his gravestone, but the stonemason declined, saying it looked too much like a circle. There's some kind of metaphor here, but I'm not sure what it is.

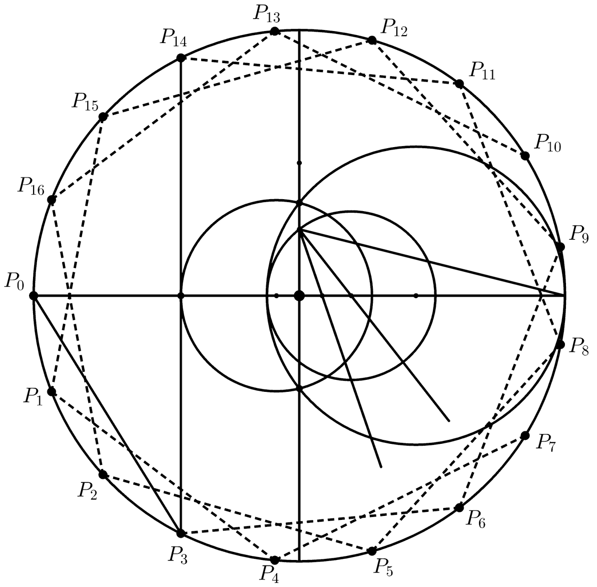
References

[1] Jordi Quer. *Teoria de Galois FME. Curs 2020/21.* 2020.

Carl Friedrich Gauss' blogspot. Also, Ian Stewart's Galois theory textbook contains good chapters on this topic, including proving that H.W. Richmond's 1893 construction (the one on the t-shirt) works.[1] Stewart is also more famous for his pop-math books, which leaves no doubt as to the clarity

[1] Gauss' proof was non-constructive, leaving the actual construction to others. Mathematicians stay winning.

of his writing.



$$\mathbf{Gal}\big(\mathbb{Q}(\boldsymbol{e^{2\pi i/17}})/\mathbb{Q}\big) \cong (\mathbb{Z}/\mathbf{17}\mathbb{Z})^{\times}$$

Figure 2: The t-shirt design, created by Stephen Hu using Geogebra