Constructibility: Abstract Algebra in Geometry

Diana Harambas

PROMYS, July 2023

Contents

1 Motivation **2**

2 Necessary background **3**
2.1 Fields, field extensions and the Tower Law 3
2.2 Simple extensions and minimal polynomials 4
2.3 Quadratic extensions 5

3 Constructible real numbers and regular n-gons **6**
3.1 Constructibility criteria for real numbers 6
3.2 Constructibility criteria for regular n-gons 8

4 Classical impossible constructions **9**
4.1 Trisecting the 60° angle 9
4.2 Squaring a circle 10

5 References **10**

1 Motivation

Revisiting the concepts from elementary geometry, we can all remember what midpoints and angle bisectors are and how we can construct these using a ruler/straight edge and a compass.

For example, when constructing the midpoint M of segment $\overline{AB}$ (drawn using the straight edge), we start by creating two circles of radius AB, one centred at A and one at B with the compass. They will intersect in two points, let's call them C and D. Then, we can construct $\overline{CD}$ using the ruler. One can check that intersection $\overline{AB} \cap \overline{CD} = \{M\}$ will be the midpoint of $\overline{AB}$.

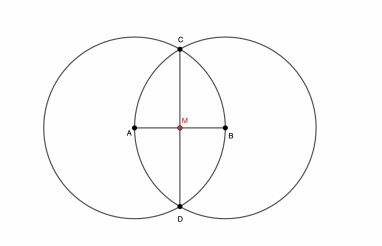

Figure 1: Constructing the midpoint of a segment

In order to bisect an angle $\angle X$, we construct a circle (of arbitrary radius) with the centre in X using the compass, and call the intersections with the sides Y, Z as in the figure below. Then, draw two additional circles, one centred at Y with radius XY and the other centred at Z with radius XZ. These circles would intersect at T and one can prove that XT is the bisector of $\angle X$.

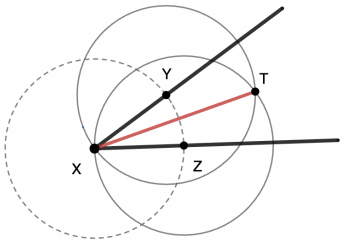

Figure 2: Bisecting an angle

Seeing these examples, the following questions come to mind:

Can all elements be constructed similarly, using only a pair of compasses and a ruler? How can we check this without long geometric proofs?

Before introducing the algebraic background needed to answer these questions, let's introduce some useful definitions.

Definition 1.1 (Ruler-and-compass constructions)**.**

A figure is considered to be a ruler-and-compass construction if it is built as a finite sequence of the following possible operations on a given set of points P_0 in the Euclidean plane $\mathbb{R}^2$:

1. Draw a straight line between two points of P_0 (using the unmarked ruler).

2. Draw a circle (using the pair of compasses), whose centre is a point in P_0 and its radius is equal to the distance between some two distinct points in the set P_0.

3. Mark the intersection points of any two lines, circles or line and circle - these points are said to be *constructible*.

Definition 1.2 (Constructible real numbers)**.** *A real number α is constructible using the ruler-and-compass operations if one can draw a segment of length $|\alpha|$ starting with a unit segment (which is already constructed with a compass and straight edge).*

2 Necessary background

In order to see some tricks on finding out if a number is constructible or not, and furthermore if certain figures are ruler-and-compass constructions, we need some ideas from Field Theory.

2.1 Fields, field extensions and the Tower Law

Definition 2.1 (**Fields**)**.**

A set with two operations $(F, +, \cdot)$ is a field if it satisfies the following properties (for both $+, \cdot$):

- F is closed under both operations
- associativity
- distributivity
- commutativity
- there exist distinct additive (0) and multiplicative (1) identities
- every element has a unique additive inverse
- every "non-zero" element has a unique multiplicative inverse

For example, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ are fields, but $(\mathbb{Z}, +, \cdot)$ is not (it is only a ring - remember the ring axioms discussed in the Number Theory lectures).

Definition 2.2 (**Subfields**).

Let K be a subset of the field F. It is a subfield if:

- $0, 1 \in K$
- for any $x \neq 0 \in K$, then $-x, x^{-1} \in K$
- for any $x, y \in K$, then $x + y, xy \in K$

Proposition 2.3. *Any subfield of* $\mathbb{C}$ *contains* $\mathbb{Q}$.

Now that we defined the basic notions, let's take a look at something a bit more advanced that is key to our future constructibility theorems.

Definition 2.4 (**Field extensions**). *If K is a subfield of the field L, then we can say that L is an extension field of K. To symbolize this, we often write L/K ("L over K").*

Definition 2.5 (**Degree of a field extension**). *For L/K, the degree $[L : K]$ is the dimension of L as a $K-$vector space.*

For example, when looking at $L = \mathbb{Q}(i)$ and $K = \mathbb{Q}$, we get $[L : K] = 2$.

Another example of finite degree is for $L = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ and $K = \mathbb{Q}$, where $[L : K] = 4$, because elements of L have form $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ (the $\sqrt{6}$ is necessary for ensuring that L is closed under multiplication), with $a, b, c, d \in \mathbb{Q}$.

However, $[\mathbb{R} : \mathbb{Q}] = \infty$.

Introducing field extensions and their degree, it's only natural to look for formulas that help compute the degree of more "complicated" extensions. Therefore, we introduce an important theorem, known as the Tower Law (or Tower Rule).

Theorem 2.6 (**Tower Law**). *Let $K \subseteq L \subseteq M$ be subfields of $\mathbb{C}$, then*

$$[M : K] = [M : L] \cdot [L : K].$$

Corollary 2.7 (**Extended Tower Law**). *For $K_0 \subseteq K_1 \subseteq ... \subseteq K_n$ subfields of $\mathbb{C}$, we have*

$$[K_n : K_0] = [K_n : K_{n-1}] \cdot [K_{n-1} : K_{n-2}] \cdot ... \cdot [K_1 : K_0].$$

2.2 Simple extensions and minimal polynomials

To better understand how the Tower Law applies in compass-and-ruler constructions and how we can "repeatedly extend" a field, we should go back to the easiest type of field extensions and spend some time analysing them:

Definition 2.8 (**Simple extensions**). *If L/K is a field extension, we say that L is a simple extension of K if there exists some $\alpha \in L$ such that $L = K(\alpha)$.*

Definition 2.9 (**Algebraic vs transcendental**). *If $L = K(\alpha)$ is a simple extension, where α is a root of some non-zero polynomial in $K[x]$ (with coefficients in K), then we say that α is algebraic over K. If there is no such polynomial for which α is a root, then α is transcendental over K.*

Now, in order to further explore the differences between algebraic and transcendental L/K extensions, we need to define some new notions, such as the minimal polynomial of α over K, where $\alpha \in L$ is algebraic.

Definition 2.10 (**The minimal polynomial**). *Let L/K be a field extension and let $\alpha \in L$ be algebraic over K. The minimal polynomial of α over K is the unique monic polynomial $m \in K[x]$, of smallest degree, and such that $m(\alpha) = 0$.*

Note : A monic polynomial is a polynomial with the leading coefficient 1.

For example, in the field extension $\mathbb{C}/\mathbb{R}$, i has minimal polynomial $m(x) = x^2 + 1$. For $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $m(x) = x^3 - 2$.

Let's bring back the degree of an extension and see how $[K(\alpha) : K]$ behaves in case α is transcendental or algebraic.

Theorem 2.11. *Let $K(\alpha)/K$ be a simple field extension. If α is transcendental over K, then $[K(\alpha) : K] = \infty$. Else, $[K(\alpha) : K] = deg(m)$, where m is the minimal polynomial of α over K.*

Note : The proof of this theorem requires some linear algebra knowledge (and some ideas about polynomial rings and isomorphism), so it might be harder to follow if one has no experience with it.

Proof. Let α be algebraic over K and have the minimal polynomial m of degree n. Then we know that $K(\alpha)$ is isomorphic to $K[x]/m(x)$, which must have a K-basis of n elements (since $deg(m) = n$ and only polynomials of smaller degree exist in $K[x]/m(x)$). Being isomorphic, that implies that $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ is a basis of $K(\alpha)$, and therefore, $[K(\alpha) : K] = n = deg(m)$.

If α is transcendental over K, then $\{1, \alpha, \alpha^2, ..., \alpha^n, ...\}$ is linearly independent over K, because otherwise α must be a root of some polynomial in $K[x]$ (i.e., α algebraic). With that being said, since $\{1, \alpha, \alpha^2, ..., \alpha^n, ...\}$ is an infinite linearly independent set, $[K(\alpha) : K] = \infty$.
QED

Corollary 2.12. *A simple extension is algebraic if and only if it is finite (has a finite degree).*

Proposition 2.13. *L/K is a finite extension if and only if L is algebraic over K and there exist finitely many $\alpha_1, \alpha_2, ..., \alpha_n \in L$ such that $L = K(\alpha_1, \alpha_2, ..., \alpha_n)$.*

2.3 Quadratic extensions

Finally, let's introduce quadratic extensions (these would be the most helpful in the next section).

Definition 2.14 (**Quadratic extensions**). *A simple field extension L/K is quadratic if $[L : K] = 2$.*

Proposition 2.15. *For a quadratic field extension L/K, we can take some $\alpha \in L, \alpha \notin K$ such that $\alpha^2 \in K$ and $L = K(\alpha)$.*

Note : This is equivalent to saying that $L = K(\sqrt{d})$, where $d \in K$ is not a square in the subfield K.

Proposition 2.16. *When looking at $\mathbb{Q}$ as a subfield inside $\mathbb{C}$, the quadratic extensions of $\mathbb{Q}$ are precisely the extensions $\mathbb{Q}(\sqrt{d})$, where $\sqrt{d}$ is irrational.*

3 Constructible real numbers and regular n-gons

Recall the definitions from Section 1. We will now introduce the necessary criteria for proving whether a real number is constructible or not, and later, use this knowledge to check if regular n-gons can or cannot be built using a pair of compasses and a straight edge.

3.1 Constructibility criteria for real numbers

Theorem 3.1. *The set of constructible real numbers is a field.*

Note : The complete proof will be omitted here (or left as an exercise for the reader), but some key ideas for proving closure under addition and additive inverses are working with addition and subtraction of segment lengths and circles with radii of desired length. When it comes to closure under multiplication and multiplicative inverses, one could use the straight edge to build perpendicular lines and, after drawing circles with radii of a given length, look for similar triangles, as they have proportional side lengths.

Proposition 3.2 (**Square root construction**). *Let $\alpha \geq 0$ be a constructible real number, then $\sqrt{\alpha}$ is constructible.*

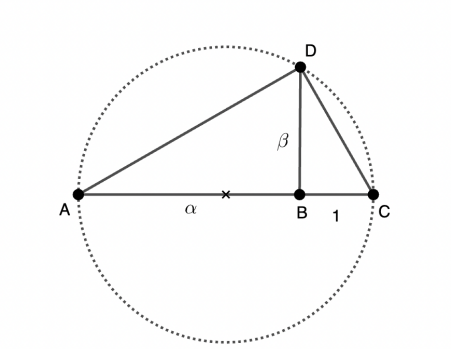

Figure 3: Construction of the square root

Proof. Let $AB = \alpha$ and C on the same segment, such that $BC = 1, AC = \alpha + 1$. Since midpoints can be constructed, we can draw a circle of diameter AB as in the image above.

Using the straight edge, we can construct point D on the circle such that $\overline{BD} \perp \overline{AC}$. Let $BD = \beta$, which implies that the real number β can be constructed.

Using elementary geometry, we can state that ΔDBC is similar to ΔABD. Therefore,

$$\frac{DB}{BC} = \frac{AB}{BD} \Rightarrow \frac{\beta}{1} = \frac{\alpha}{\beta} \Rightarrow \beta = \sqrt{\alpha},$$

leading us to the conclusion that $\sqrt{\alpha}$ is constructible.

QED

The theorem and proposition above, alongside the Tower Law and the knowledge we have from elementary geometry, prepare us for the following theorem:

Theorem 3.3 (**Constructible real numbers**). *Let $\alpha \in \mathbb{R}$. It is constructible if and only if there exists a tower of field extensions*

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq ... \subseteq K_n = \mathbb{Q}(\alpha),$$

with $[K_{i+1} : K_i] \leq 2, \forall i = \overline{0, n-1}$.

Note : The proof below explains all the main ideas, but one could include more detailed steps.

Proof. ($\Rightarrow$) The only operations possible are constructing a line and constructing a circle. Hence, the points that can be constructed (on top of the initial set of points) come from intersecting two lines, intersecting a circle and a line, or intersecting two circles.

Let F be the field we are working in and let $a, b, c, d \in F$. By drawing a line between points of coordinates $(a, b), (c, d)$, we add points (x, y) that satisfy the line equation

$$\frac{x-a}{y-b} = \frac{c-a}{d-b}.$$

In a linear form, the line equation would be of type $Ax + By = C$, where $A, B, C \in F$ as they are rational functions of a, b, c, d. Similarly, the equation of a circle of a given centre and radius has coefficients in F, however it now includes quadratics:

$$(x-a)^2 + (y-b)^2 = r^2,$$

where the above equation describes the circle of centre (a, b) and radius r.

Intersecting two lines, we look for solutions that satisfy simultaneously two linear equations. We obtain $x, y \in F$ (y is obtained linearly in terms of x, and x would be a result of addition, subtraction, multiplication or division of the coefficients - which are elements of F, field which is closed under these operations).

Intersecting a line and a circle, we look for solutions that satisfy simultaneously a linear and a quadratic equation. Similarly, we will write y linearly in terms of x and substitute. So, solving for x means getting solutions of a quadratic equation, i.e. x would be at worst in some quadratic extension of F.

The statement above is also true for intersecting two circles: by subtracting one of the quadratic equations from the other, we are left with a linear and a quadratic equation to solve.

Therefore, by adding a new point, the degree of the "most recent" extension that needs to be added to the tower of field extensions will either be 1 or 2.

($\Leftarrow$) Conversely, the key idea here is that all elements obtained by rational functions or by applying the square root (in case we have a quadratic extension) can be constructed. Therefore, by induction, we can obtain that α is constructible.

QED

Corollary 3.4. *Let $\alpha \in \mathbb{R}$ be constructible. Then the degree of the extension $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is a power of 2.*

Corollary 3.5. *Transcendental real numbers are not constructible.*

3.2 Constructibility criteria for regular n-gons

After discussing what constructibility means in real numbers, we should keep the results in mind and explore the criteria for constructing angles and regular n-gons. Let's start with a lemma and a proposition.

Lemma 3.6. *For a real number θ, $cos(\theta)$ is constructible if and only if $sin(\theta)$ is constructible.*

Proof. ($\Rightarrow$) Let's consider the real number $cos(\theta)$ constructible. Recall the identity

$$cos^2(\theta) + sin^2(\theta) = 1,$$

which yields $sin(\theta) = \sqrt{1 - cos^2(\theta)}$. Now by Theorem 3.1 and Proposition 3.2, we conclude that $sin(\theta) = \sqrt{1 - cos^2(\theta)}$ is a constructible real number.

($\Leftarrow$) Similarly, we get that $cos(\theta) = \sqrt{1 - sin^2(\theta)}$ is a constructible real number.

QED

Proposition 3.7. *An angle θ is constructible if and only if $cos(\theta)$ and $sin(\theta)$ are constructible real numbers.*

Note : For the proof, recall that in a right triangle, the ratio of the side opposite to θ and the hypotenuse is $sin(\theta)$, and the ratio of the side adjacent to θ and the hypotenuse is $cos(\theta)$.

These two previously introduced statements are enough to prove the following theorem on regular n-gons:

Theorem 3.8. *A regular n-gon is constructible using only a ruler and a pair of compasses if and only if $cos\frac{2\pi}{n}$ is a constructible real number.*

Proof. ($\Rightarrow$) In a regular n-gon, an exterior angle has measure $\frac{360^\circ}{n}$. Since the n-gon is already constructed, we can also construct the exterior angles by extending the sides using the straight edge. Therefore, $cos(\frac{2\pi}{n})$ is a constructible real number.

Another way to prove this step-by-step is by remembering that an exterior angle of measure $\frac{360^\circ}{n}$, will have the interior angle supplementary to it, measuring $180^\circ - \frac{360^\circ}{n}$, which is already constructed

$$\Rightarrow cos(180^\circ - \frac{360^\circ}{n}) = -cos(\frac{360^\circ}{n}) = -cos(\frac{2\pi}{n})$$

is constructible, and so will $cos(\frac{2\pi}{n})$ be.

($\Leftarrow$) Conversely, the hardest part is constructing the first side of the regular n-gon.

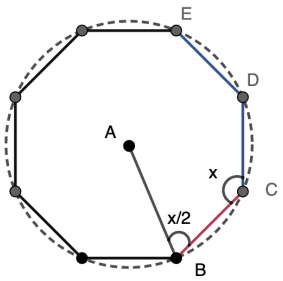

Figure 4: Construction of a regular n-gon

Starting from a unit segment $\overline{AB}$ and drawing the unit circle with centre in A, we can construct point C on the circle such that $\angle ABC = \frac{180^\circ - \frac{360^\circ}{n}}{2}$, because we know that $cos(\frac{2\pi}{n})$ is constructible, which implies that

$$-cos(\frac{2\pi}{n}) = -cos(\frac{360^\circ}{n}) = cos(180^\circ - \frac{360^\circ}{n})$$

is also a constructible real number. Using the half-angle identity and Proposition 3.2, we obtain that $\angle ABC = \frac{180^\circ - \frac{360^\circ}{n}}{2}$ is a constructible angle. Then $\overline{BC}$ will be one side of the n-gon.

We then construct point D on the circle such that $\angle BCD = 180^\circ - \frac{360^\circ}{n}$ this time (since we are not dealing with a bisector anymore), and will get that $\overline{CD}$ is another side of the n-gon. We repeat this process with the newly created points and sides until we reach B again.

QED

Now, let's look at an example of a regular polygon and check if it can be constructed under the ruler-and-compass construction rules.

A regular **octagon** (regular polygon with 8 sides) is constructible because, for $n = 8$ we have:

$$cos(\frac{2\pi}{8}) = cos(45^\circ) = \frac{\sqrt{2}}{2} \in \mathbb{Q}(\sqrt{2}),$$

with $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, meaning that Theorem 3.3 is satisfied.

4 Classical impossible constructions

Some of the classical constructions, which are impossible to build using the rules from ruler-and-compass constructibility, are trisecting an angle or "squaring" a circle. The Greeks kept wandering for years about how to trisect a 60° angle and for a moment, they thought they found the perfect ruler-and-compass construction. However, it was only a good approximation. Hundreds of years later, after progress in algebra (with the help of Gauss, too), field theory and Galois theory, people were able to prove that these classical figures (and not only) are actually impossible compass-and-ruler constructions.

4.1 Trisecting the 60° angle

Theorem 4.1 (**Wantzel**). *The angle $\frac{\pi}{3}$ cannot be trisected using ruler-and-compass constructions.*

Proof. Since $cos\frac{\pi}{3} = \frac{1}{2}$ and $sin\frac{\pi}{3} = \frac{\sqrt{3}}{2}$ are constructible real numbers, one can indeed construct the $\frac{\pi}{3}$ angle starting from the points $(0, 0)$ and $(1, 0)$.

To trisect it, we need to be able to construct a $\frac{\pi}{9}$ and a $\frac{2\pi}{9}$ angle: we would need to have $\alpha = cos\frac{\pi}{9}$ and $\beta = cos\frac{2\pi}{9}$ constructible real numbers.

From elementary geometry and trigonometry, recall the formula $cos(3\theta) = 4cos^3\theta - 3cos\theta$. Using this for α, we can see that our number must satisfy

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

The polynomial $f(x) = x^3 - \frac{3}{4}x - \frac{1}{8}$ is irreducible over (Q), and it will act as a minimal polynomial for α over $\mathbb{Q}$. Therefore, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, which is not a power of 2. From Theorem 3.3, we conclude that α, and then α, cannot be constructed, which implies that the $\frac{\pi}{3}$ angle cannot be trisected using ruler-and-compass constructions.

QED

4.2 Squaring a circle

Theorem 4.2. *Given a circle, one cannot build a square with the same area as the circle, using ruler-and-compass constructions.*

Proof. Let the circle have radius r (constructible) and surface area πr^2. Suppose we can construct a square with side l (so we assume that l is constructible) such that its area is $l^2 = \pi r^2$. This means that $l/r = \sqrt{\pi}$ is constructible (since both r and l are constructible by our assumption). If $\sqrt{\pi}$ is constructible, then so should π be.

By Theorem 3.3, this means that $[\mathbb{Q}(\pi) : \mathbb{Q}]$ is a finite power of 2. But π is transcendental over $\mathbb{Q}$, which by Theorem 2.11 implies that $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$. Therefore, (as Corollary 3.4 already showed) π is not constructible. So $\sqrt{\pi} = \frac{l}{r}$ is not constructible even if r is.

With this, we conclude that a square with a side length of l such that $l^2 = \pi r^2$ cannot be constructed using only ruler-and-compass rules.

QED

5 References

Stewart, I. (2022). Galois Theory (5th ed.). Chapman and Hall/CRC
Bojorquez, Betzabe, "Geometric Constructions from an Algebraic Perspective" (2015). Electronic Theses, Projects, and Dissertations. 237.
Dummitt, D.S. and Foote, R.M. (2004) Abstract Algebra. 3rd Edition, John Wiley & Sons, Inc.
Davis, I. (2008). Understanding Ruler and Compass Constructions with Field Theory.