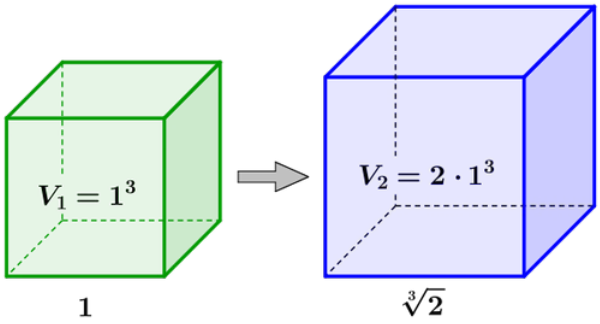

Figure 1: Doubling the Cube (Source: Wikimedia)

Doubling the Cube

Raj Pabari

August 19, 2025

Contents

1 Introduction

As legend has it, when the Delians of Ancient Greece faced a plague circa 430 BCE, they were advised by an oracle to double the size of their cube-shaped altar to the god Apollo. At their disposal were the existing cube, an unmarked straightedge, and a compass capable of drawing circles of a known radius.

For simplicity, we can treat the length of the existing cube (which again, is known a priori) as the unit length of 1. With this unit convention, notice that the original cube has volume $1^3 = 1$ cubic unit, and the goal is to produce a cube of volume 2 cubic units. This cube would necessarily have sides of length $\sqrt[3]{2}$ units because $\ell^3 = 2$ if and only if $\ell = \sqrt[3]{2}$.

Thus, the precise question that the Delians tried to solve was: given a line segment of length 1, is it possible to produce a line segment of length $\sqrt[3]{2}$ with a finite sequence of operations with an unmarked straightedge and compass?

The Ancient Greeks were able to solve many such problems of this form. With a finite sequence of compass and straightedge operations, they were able to bisect angles, construct regular polygons, and solve quadratic equations. On face, the problem of doubling the cube seemed very similar to these problems they had already solved. However, despite their best efforts, the Delians could not find a valid construction, and the problem remained unsolved.

As time went on, mathematicians came up with other tools that allowed them to double the cube (for instance, by allowing compass and straightedge operations and the intersection of parabolas), but never were able to accomplish the task with just a compass and straightedge. It was not until much later that it was proven that doubling the cube with a compass and straightedge alone is actually impossible.

In this paper, we prove that doubling the cube is impossible. At a high level, the proof characterizes the field of lengths that can be constructed with a finite sequence of compass and straightedge operations, then argues that this field of constructible lengths cannot contain the length $\sqrt[3]{2}$.

The bulk of this paper (Section 2) is devoted to proving a number of intermediate results. For instructive purposes, we will often opt to prove more general propositions, then explicitly apply these propositions to the problem of doubling the cube as corollaries. Given these intermediate results, the impossibility of doubling the cube immediately follows; we will briefly combine them in Section 3 to conclude the paper.

2 Intermediate Results

2.1 Constructible Numbers

What distances (eg. real numbers) can we construct with a compass and straightedge? Clearly, some real distances (such as e) are hard to construct, while other real distances (such as 2) are trivial to construct. In this section, we formalize the notion of constructibility.

Definition 1. *Suppose we start with the line segment connecting* $(0, 0)$ *and* $(1, 0)$*. If, after some finite sequence of compass and straightedge operations, we arrive at a coordinate pair* $(x, y) \in \mathbb{R}^2$*, then* x *and* y *are constructible. These compass and straightedge operations are –*

(a) Drawing a line between two constructed points

(b) Drawing a circle with center at a previously constructed point and radius equal to the distance between two previously constructed points

(c) Marking the intersection of two straight lines

(d) Marking the intersection of a straight line and circle

(e) Marking the intersection of two circles

We'll denote the set of constructible numbers as $C \subset \mathbb{R}$.

Notice that, despite distances being positive, we can still reach negative x-values with the above operations. We now provide another simple characterization of C.

Proposition 1. *C is a field such that $\mathbb{Q} \subset C$.*

Proof. First, let $c \in C$ be a constructible length and let $(x, 0)$ be a coordinate we've reached in our sequence of compass and straightedge operations. For any coordinate pair $(x, 0) \in \mathbb{R}^2$ we've constructed, see that we can construct $(x + c, 0)$ and $(x - c, 0)$. We do this by putting the center of the compass at $(x, 0)$ and drawing a circle of radius c. Then the upper intersection of the line passing through $(0, 0)$ and $(x, 0)$ with this circle is the $(x + c, 0)$ and the lower intersection is $(x - c, 0)$.

We are given that $1 \in C$. Let $a \in \mathbb{Z}$. Then, note that $|a| = \underbrace{1 + \ldots + 1}_{a \text{ times}}$. If $a \geq 2$, we can use the above with $x = 1, c = 1$ to construct $(2, 0)$, then $(3, 0)$, and so on until we reach $(a, 0)$. If $a \leq -1$, we can start with $x = 0$ with a center at the point $(0, 0)$ and keeping $c = 1$, can construct the points $(-1, 0), (-2, 0)$, and continue until we reach $(-a, 0)$.

We've thus shown that $\mathbb{Z} \subseteq C$. In order to conclude the proof, it remains to show C is closed under addition, subtraction, multiplication, and division. This will validate that C is a field and show that $\mathbb{Q} \subseteq C$. The latter follows because rational numbers are of the form $\frac{p}{q}$ for $p, q \in \mathbb{Z}$, $q \neq 0$, so if $\mathbb{Z} \subseteq C$ and C is closed under division then $\mathbb{Q} \subseteq C$.

Given $a, b, c \in C$, we can easily construct the points $(a, 0)$ and $(b, 0)$. In the first paragraph of this proof, we therefore showed that $a - b$ and $a + b$ are in C (let $x = a$ and $c = b$). To show closure under multiplication and division, consider Figure 2. Because the angle of the triangle does not matter, Figure 2 is constructible by drawing a line of length a on one line and lines of length b, c on any other non-parallel line. From here, we can draw a line from C to A, and use the straightedge to draw a parallel line through B. The intersection of this with the line through OA will be our point X; we've thus constructed Figure 2. Because all the angles are equal, triangle OCA is similar to triangle OBX. Thus, we have that $\frac{x}{a} = \frac{b}{c}$, which implies that $x = \frac{ab}{c}$. Setting $c = 1$ allows us to construct $x = ab$, and setting $b = 1$ allows us to construct $x = \frac{a}{c}$ for nonzero c. □

It's worth noting that the containment $\mathbb{Q} \subset C$ is strict. For instance, consider the right triangle of leg length 1, then the hypoteneuse has length $\sqrt{2} \notin Q$. In a sense, the proof that doubling the cube is impossible hinges on the "size" of C relative to $\mathbb{Q}$, a notion which we will soon make precise.

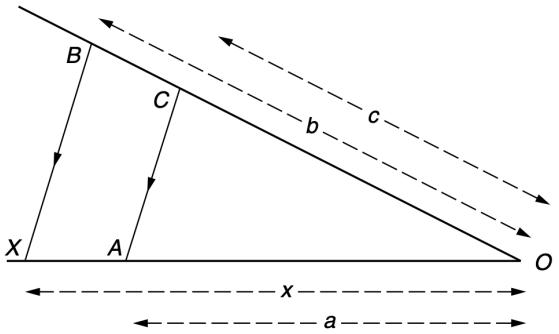

Figure 2: Constructing products and quotients of constructible numbers (Source: [1], Figure 13.2)

2.2 Rational Roots

Consider the equation $x^3 - 2 = 0$. Notice that $x = \sqrt[3]{2} \notin \mathbb{Q}$ is a solution, but are there any rational roots of $p(x) = x^3 - 2$? In this section, we will show that there are none, which will be very important later.

Proposition 2. *Consider a polynomial $p(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$. If $\frac{r}{s} \in \mathbb{Q}$ is a rational root of $p(x)$ such that r and s are relatively prime, then $r \mid a_0$ and $s \mid a_n$.*

Proof. We know that $\frac{r}{s}$ is a root of $p(x)$, thus it follows that

$$\begin{aligned} 0 &= p\left(\frac{r}{s}\right) \\ \implies 0 &= a_0 + a_1\left(\frac{r}{s}\right) + \cdots + a_n\left(\frac{r}{s}\right)^n \\ \implies 0 &= a_0 s^n + a_1 r s^{n-1} + \cdots + a_n r^n \\ \implies a_0 s^n &= -(a_1 r s^{n-1} + \cdots + a_n r^n) \\ \implies a_0 s^n &= -r(a_1 s^{n-1} + \cdots + a_n r^{n-1}) \end{aligned}$$

Which implies that $r \mid a_0 s^n$. We know that r, s are relatively prime, thus $r \nmid s^n$ which implies $r \mid a_0$ as desired. A similar argument holds to show that $s \mid a_n$. □

Corollary 1. *The polynomial $p(x) = x^3 - 2$ has no rational roots.*

Proof. By Proposition 2, any rational root $\frac{r}{s}$ of $p(x)$ must satisfy $r \mid a_0 = -2$ and $s \mid a_3 = 1$, in other words that $r \in \{\pm 1, \pm 2\}, s \in \{\pm 1\}$. This implies that $\frac{r}{s} \in \{\pm 1, \pm 2\}$, however evaluating $p(x)$ at each of these possible values yields no solution. Thus, there are no rational roots of $p(x)$. □

2.3 Preliminaries on Field Extensions

In this section, we define and characterize field extensions to give us the machinery to analyze the set of constructible numbers.

Definition 2. *Let F be a field and $G \subset F$ be a subfield. F is called a field extension of G.*

It immediately follows from the definition that C is a field extension of $\mathbb{Q}$.

Proposition 3. *Let F be a field and $K \supset F$ be an extension. K is a vector space over F.*

Proof. Note that because K is itself a field, it is commutative and has inverses. The rest of the properties follow from the fact F is a subfield of K –

(a) K and F share the same additive and multiplicative identities $0, 1 \in F$

(b) Let $\lambda, \mu \in F$ and $k, \ell \in K$, then $\lambda, \mu \in K$ implies that $\lambda(k + \ell) = \lambda k + \lambda \ell$ and $(\lambda + \mu)k = \lambda k + \mu k$

(c) Let $\lambda, \mu \in F$ and $k \in K$, then $\lambda, \mu \in K$ implies that $(\lambda\mu)k = \lambda(\mu k)$

□

Proposition 3 tells us a lot about the structure of a field extension. The next definition uses the vector space characterization of a field extension to introduce the aforementioned notion of "size" of a field extension, and we follow it with an important property.

Definition 3. *Let F be a field and $K \supset F$ be an extension. The degree of K over F, denoted $[K : F]$, is the dimension of K considered as a vector space over F.*

As a remark, the degree of a field extension could be infinite, but we'll restrict our attention in this paper to extensions of finite dimension.

Proposition 4. *Let L be a field and $L \supset K \supset F$ be subfields. Then, $[L : F] = [L : K][K : F]$.*

Proof. Let $\{u_1, \ldots, u_m\}$ be a basis for L over K and let $\{v_1, \ldots, v_n\}$ be a basis for K over F. We claim that $B := \{u_i v_j \mid i \in \{1, \ldots, m\}, j \in \{1, \ldots, n\}\}$ is a basis of L over F.

We show that B spans L. For all $\ell \in L, \ell = \sum_{i=1}^{m} \lambda_i u_i$ for some choices of $\lambda_i \in K$. Similarly, though, each of these $\lambda_i \in K$ can be decomposed as $\lambda_i = \sum_{j=1}^{n} \mu_{ij} v_j$ for some $\mu_{ij} \in F$ depending on λ_i. Thus, we can write

$$\ell = \sum_{i=1}^{m} \lambda_i u_i = \sum_{i=1}^{m} \sum_{j=1}^{n} \mu_{ij} v_j u_i$$

implying that ℓ is a linear combination of the elements in our basis B. Now, suppose that $\sum_{i=1}^{m} \sum_{j=1}^{n} \mu_{ij} v_j u_i = 0$. Because $\mu_{ij} v_j \in K$, and the u_i form a basis of L over K (and are linearly independent as a result), $\sum_{j=1}^{n} \mu_{ij} v_j = 0$ for each i. However, the v_j form a basis of K over F, implying that for all i and j, $\mu_{ij} = 0$. Thus, we've established that B is a linearly independent set of vectors that span the space L over the field F, and $[L : F] = |B| = mn = [L : K][K : F]$. □

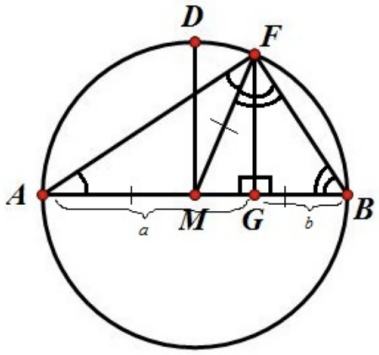

Figure 3: Constructing geometric mean of a and b (Source: [2], Figure 4)

2.4 A Condition for Constructibility

In this section, we introduce a characterization of the constructible numbers we introduced above. Intuitively, see that $\sqrt{2}$ is the hypoteneuse of a right triangle with leg lengths $1 \in \mathbb{Q} = K_0$. The constructible number $\sqrt[4]{2}$ is then the hypoteneuse of a right triangle with leg length $\sqrt{2} \in K_1 \supset K_0$ for some field extension K_1. Similarly, if we can further extend $\mathbb{Q}$ in this fashion finitely many times, we'll still obtain constructible numbers. We provide a brief lemma then a formalization of this intuition.

Lemma 1. *If $a \geq 0$ is constructible, $\sqrt{a}$ is also constructible.*

Proof. We use the geometric mean construction from Figure 3 with $b = 1$ and a a constructible number. We draw a line of length $a + 1$ with endpoints A, B. We label the point of distance a away from A and 1 away from B as G, and label the midpoint $\frac{a+1}{2}$ as M. Then we draw a circle with center M and radius $\frac{a+1}{2}$. From here, we draw a line from G perpendicular to AB, and label the intersection of this line with the circle as F – we claim that FG is a line segment of length $\sqrt{a}$.

To help prove this, we'll draw line segment MF, which is a radius of the circle and thus has length $\frac{a+1}{2}$. Then triangles ΔAMF and ΔBMF are isosceles, which implies that $m\angle BFM = m\angle FBM$ and $m\angle AFM = m\angle FAM$. From here it follows that

$$180^\circ = m\angle BFM + m\angle FBM + m\angle AFM + m\angle FAM = 2m\angle FAM + 2m\angle FBM$$

$$\implies 90^\circ = m\angle FAM + m\angle FBM = m\angle BFA$$

Thus, triangle ΔBFA is right. Notice that AF is the hypoteneuse of right triangle ΔFGA which implies its length is $AF = \sqrt{a^2 + FG^2}$ and similarly BF is the hypoteneuse of right triangle ΔFGB and thus has

length $\sqrt{1^2 + FG^2}$. From the pythagorean theorem applied to right triangle ΔBFA,

$$\begin{aligned} AB^2 &= AF^2 + BF^2 \\ \implies (a+1)^2 &= a^2 + FG^2 + 1 + FG^2 \\ \implies a^2 + 2a + 1 &= a^2 + FG^2 + 1 + FG^2 \\ \implies 2a &= 2FG^2 \\ \implies \sqrt{a} &= FG \end{aligned}$$

□

Proposition 5. *Let $x \in \mathbb{R}$. If there exists a sequence of fields such that $K_n \subset \mathbb{R}$, $x \in K_n$, and $K_n \supseteq K_{n-1} \supseteq \cdots \supseteq K_0 = \mathbb{Q}$, and $[K_i : K_{i-1}] = 2$ or 1 for $i \in \{1, \ldots, n\}$, then x is constructible.*

Proof. For a finite set $X = \{x_1, \ldots, x_\ell\}$, let $\mathbb{Q}(X)$ denote the set $\{q_0 + q_1 x_1 + \cdots + q_\ell x_\ell \mid q_i \in \mathbb{Q} \text{ for } i \in \{0, \ldots, \ell\}\}$. If the elements of X have been previously constructed, then all $x \in \mathbb{Q}(X)$ are trivially constructible because they are just rational multiples of constructed elements. In other words, $\mathbb{Q}(X) \subset C$. For $i \in \{2, \ldots, n\}$, we'll denote the set of numbers that have been constructed at each of the intermediate steps as X_i, then each $K_i = \mathbb{Q}(X_i)$.

We'll complete the proof by induction on n, the amount of intermediate constructible numbers used in the construction of x. As a base case, we start with $n = 2$, then we have that $X_2 = \{0, 1\}$ and $K_2 = \mathbb{Q}(X_2) = \mathbb{Q}$, which implies that $[K_2 : \mathbb{Q}] = 1$.

Now, suppose as the inductive hypothesis that for all $n \in \mathbb{N}$, we have that all $x \in \mathbb{R}$ that are constructed with n intermediate constructible numbers are such that $x \in \mathbb{Q}(X_n) \supseteq \cdots \supseteq \mathbb{Q}(X_0)$ and $[\mathbb{Q}(X_i) : \mathbb{Q}(X_{i-1})] \in \{1, 2\}$ for all $i \in \{1, \ldots, n\}$. We'll show that the field extension $\mathbb{Q}(X_{n+1})$ containing each of the compass and straightedge operations of previously constructed points in X_n (see Definition 1) is such that $[\mathbb{Q}(X_{n+1}) : \mathbb{Q}(X_n)] \in \{1, 2\}$.

(a) Given two points $(a_1, b_1), (a_2, b_2)$ where each of the coordinates is in X_n, the line connecting them is $\frac{y-b_1}{b_2-b_1} = \frac{x-a_1}{a_2-a_1}$, and all points along this line are linear combinations of elements in X_n. Thus, drawing a line between two points gives elements in $\mathbb{Q}(X_n)$, a field extension X_{n+1} of degree 1.

(b) The circle with center (a_1, b_1) and radius equal to the distance between (a_2, b_2) and (a_3, b_3) is $(x - a_1)^2 + (y - b_1)^2 = (a_2 - a_3)^2 + (b_2 - b_3)^2$, similarly because all points are just linear combinations of elements in X_n we arrive at a field extension of degree 1.

(c) Suppose we have two lines $wx + vy = b_1$ and $tx + uy = b_2$ for $w, v, t, u, b_1, b_2 \in X_n$. Then, their intersection is at the point $x = \frac{b_1 u - b_2 v}{wu - tv} \in X_n$, $y = \frac{b_2 w - b_1 t}{wu - tv} \in X_n$, so we've again produced a field extension of degree 1.

(d) Given a circle $(x - h)^2 + (y - k)^2 = r^2$ and a line $ax + by = c$ for $h, k, r, a, b \in X_n$, we have that $y = \frac{-a}{b}x + \frac{c}{b}$ which has coefficients in X_n. Thus we are looking for solutions of the quadratic equation $(x - h)^2 + (\frac{-a}{b}x + \frac{c}{b} - k)^2 = r^2$, which has solutions of the form $x = \frac{-\ell \pm \sqrt{\ell^2 - 4jk}}{2j}$ for some $\ell, j, k \in X_n$

with nonnegative discriminant (solutions for the y values give something similar). Because $\ell^2 - 4jk$ is constructible, by Lemma 1, we have that $\sqrt{\ell^2 - 4jk}$ is also constructible. Depending on the value of the discriminant, the degree of the field extension containing these solutions may be either 1 or 2 – either $\sqrt{\ell^2 - 4jk} \in X_n$ or we need to add it as a basis vector to span the field extension $\mathbb{Q}(X_{n+1})$.

(e) Given two circles $x^2 + y^2 + ax + by + c$ and $x^2 + y^2 + a'x + b'y + c'$ for $a, a', b, b', c, c' \in \mathbb{Q}(X_k)$, they intersect at at most two points. Thus, we can instead consider the interesection of one circle and the line connecting their points of intersection, this line being $(a - a')x + (b - b')y + (c - c') = 0$. See that this is exactly the situation we considered in the previous case, thus the field extension from applying this operation has degree 1 or 2.

This concludes our induction because we've shown that no matter which compass and straightedge operation is applied to those already constructed, $[\mathbb{Q}(X_{n+1}) : \mathbb{Q}(X_n)] \in \{1, 2\}$. □

This was an involved proof, but it gives us the key condition that we will use for the final result of doubling the cube. It is worth explicitly emphasizing the condition we've arrived at as a corollary.

Corollary 2. *Let $c \in \mathbb{R}$ and $\mathbb{Q}(c) = \{q_0 + q_1 c \mid q_0, q_1 \in \mathbb{Q}\}$. Then, if $2 \nmid [\mathbb{Q}(c) : \mathbb{Q}]$ and $[\mathbb{Q}(c) : \mathbb{Q}] \neq 1$, c is not constructible.*

Proof. We prove the contrapositive of this statement. Let c be constructible, then by Proposition 5 we know that there exists some sequence $K_n \supseteq K_{n-1} \supseteq \cdots \supseteq K_0 = \mathbb{Q}$ such that $c \in K_n$ and $[K_i : K_{i-1}] \in \{1, 2\}$ for $i \in \{1, \ldots, n\}$. Notice further that $\mathbb{Q} \subseteq \mathbb{Q}(c) \subseteq K_n$ and each of these are fields. Thus, we can apply Proposition 4 to see that, for some $\ell \geq 0$,

$$[K_n : \mathbb{Q}(c)][\mathbb{Q}(c) : \mathbb{Q}] = [K_n : \mathbb{Q}] = [K_n : K_{n-1}][K_{n-1} : K_{n-2}] \cdots [K_1 : K_0] = 2^\ell$$

which implies that $[\mathbb{Q}(c) : \mathbb{Q}] = 1$ or $2 \mid [\mathbb{Q}(c) : \mathbb{Q}]$ as desired. □

As mentioned earlier, if we can apply Corollary 2 to show that $\sqrt[3]{2}$ is not constructible, we will have demonstrated impossibility of doubling the cube. The remainder of the document is dedicated to doing exactly this.

2.5 Irreducibility

Corollary 2 gives us a powerful condition to check if a number is constructible. However, it turns out the space $\mathbb{Q}(\sqrt[3]{2}) = \{q_0 + q_1\sqrt[3]{2} \mid q_0, q_1 \in \mathbb{Q}\}$ is a bit unwieldy to analyze directly. In the next section, we will prove that this space is isomorphic to a quotient ring of the form $\mathbb{Q}[x]/(p(x))$, where $(p(x))$ denotes the principal ideal generated by some rational-valued polynomial $p(x)$. However, before introducing the isomorphism it will first be important to understand which choices of $p(x)$ would be such that $\mathbb{Q}[x]/(p(x))$ is a field.

In this section, we define the condition of irreducibility and show that it guarantees exactly this. It should be noted that the notion of irreducibility can be generalized to any integral domain, but that is out of the scope of this paper.

Definition 4. *A polynomial of positive degree $f(x) \in F[x]$ is irreducible over the field F if and only if there do not exist polynomials of strictly lower degree $g(x), h(x) \in F[x]$ such that $f(x) = g(x)h(x)$.*

We next prove an important property of irreducible elements.

Proposition 6. *Let F be a field, $f(x) \in F[x]$, and $(f(x))$ denote the principal ideal generated by $f(x)$. Then, the quotient group $F/(f(x))$ is a field if and only if $f(x)$ is irreducible over F.*

Proof. Suppose that $f(x) \in F[x]$ is irreducible. Let $(f(x)) + g(x) \in F/(f(x))$ be such that $(f(x)) + g(x) \not\equiv (f(x))$. This implies that $f(x), g(x)$ are coprime, and because F is a Euclidean domain we can apply the Euclidean algorithm to write $1 = a(x)f(x) + b(x)g(x)$ for some $a(x), b(x) \in F[x]$. Notice that $a(x)f(x) \in (f(x))$ by definition of a principal ideal, thus

$$a(x)f(x) + b(x)g(x) \equiv b(x)g(x) \equiv 1 \mod (f(x))$$

This congruence implies that $[(f(x)) + b(x)] \cdot [(f(x)) + g(x)] = (f(x)) + b(x)g(x) = (f(x)) + 1$, which is the multiplicative identity in $F[x]/(f(x))$. Thus we've produced a multiplicative inverse of $(f(x)) + g(x)$, concluding the proof that it is a field.

Now, suppose for contradiction $f(x)$ is not irreducible over F. Then, there exist some $g(x), h(x) \in F[x]$ of strictly lower degree such that $f(x) = g(x)h(x)$. Because their degree is strictly lower, it must be the case that $g(x), h(x) \notin (f(x))$, implying that $(f(x)) + g(x) \not\equiv 0 \mod (f(x))$ and $(f(x)) + h(x) \not\equiv 0 \mod (f(x))$. However, notice that

$$[(f(x)) + g(x)] \cdot [(f(x)) + h(x)] = (f(x)) + f(x) = (f(x))$$

and because $(f(x))$ is the zero element of $F[x]/(f(x))$, we've produced zero divisors of $F[x]/(f(x))$, contradicting the assumption that it is a field. □

Corollary 3. *The polynomial $(x^3 - 2)$ is irreducible over $\mathbb{Q}$, and $\mathbb{Q}[x]/(x^3 - 2)$ is a field.*

Proof. It follows from the definition that $p(x) = x^3 - 2 \in \mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$. If $p(x)$ were reducible, we would be able to factor $p(x)$ as $p(x) = (b_1x + b_2)(c_1x^2 + c_2x + c_3)$ where each $b_i, c_i \in \mathbb{Q}$. However, this would imply that $\frac{-b_2}{b_1} \in \mathbb{Q}$ is a rational root of $p(x)$, contradicting Corollary 1. Thus, Proposition 6 implies that $x^3 - 2 \in \mathbb{Q}[x]$ is a field. □

2.6 A Key Isomorphism

We produce here the aforementioned isomorphism, which will be easier to analyze than $\mathbb{Q}(\sqrt[3]{2})$.

Proposition 7. *Let F be a field and $c \in F$ be such that there exists a polynomial $p(x) \in F[x]$ satisfying $p(c) = 0$,[1] and furthermore let $p(x) \in F[x]$ be irreducible over F with degree n. Then, where $(p(x))$ denotes the principal ideal generated by $p(x)$ and $F(c) = \{f_0 + f_1c \mid f_0, f_1 \in F\}$, $F[x]/(p(x))$ is isomorphic to $F(c)$.*

[1] This condition is equivalently stated as c being algebraic over F.

Proof. First, we define the homomorphism $\varphi : F[x] \to F(c)$ as $\varphi(q(x)) = q(c)$. The multiplicative identities map to each other, see that $\varphi(1_{F[x]}) = 1_F$. Additionally, for any $q(x), r(x) \in F[x]$, $\varphi(q(x)r(x)) = q(c)r(c) = \varphi(q(x))\varphi(r(x))$ and $\varphi(q(x) + r(x)) = q(c) + r(c) = \varphi(q(x)) + \varphi(r(x))$.

By the first isomorphism theorem, $\text{Ker}\varphi$ is an ideal of $F[x]$. Note that $\varphi(p(x)) = p(c) = 0$, thus $p(x) \in \text{Ker}\varphi$. Furthermore, because $F[x]$ is a principal ideal domain, we know that $\text{Ker}\varphi = (p(x))$. Thus, we can apply the first isomorphism theorem to see that

$$F[x]/\text{Ker}\varphi = F[x]/(p(x)) \cong \text{Im}\varphi \subseteq F(c)$$

By Proposition 6, we know $F[x]/(p(x))$ is a field. Thus, $F(c)$ is an extension field of $\text{Im}\varphi$. Notice that $F \subset \text{Im}\varphi$ (the constant polynomials map to each element of F) and $c \in \text{Im}\varphi$ ($x \in F[x] \mapsto c$). Because $F(c)$ is simply linear combinations of elements in the field and the element $c \notin F$, $\text{Im}\varphi$ spans $F(c)$, implying $[F(c) : \text{Im}\varphi] = 1$ and further implying that $F(c) = \text{Im}\varphi$. We've therefore shown $F[x]/(p(x)) \cong F(c)$. □

Corollary 4. *The space* $\mathbb{Q}(\sqrt[3]{2}) := \{q_0 + q_1\sqrt[3]{2} \mid q_0, q_1 \in \mathbb{Q}\}$ *is isomorphic to* $\mathbb{Q}[x]/(x^3 - 2)$.

Proof. See that the polynomial $p(x) = x^3 - 2 \in \mathbb{Q}[x]$ is such that $p(\sqrt[3]{2}) = 0$. We showed in Corollary 3 that $x^3 - 2$ is irreducible over $\mathbb{Q}$. Thus, Proposition 7 tells us that $\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}[x]/(x^3 - 2)$. □

2.7 Applying Field Extension Theory to $\mathbb{Q}[x]/(x^3 - 2)$

Now that we've shown $\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}[x]/(x^3 - 2)$ and is a field in Corollaries 3 and 4, we will treat it as a field extension of $\mathbb{Q}$ and characterize its degree. First, though, we'll take a closer look at its cosets.

Proposition 8. *Let F be a field and $p(x) \in F[x]$ be of degree n. Then,*

$$F[x]/(p(x)) = \{(p(x)) + r(x) \mid 0 \leq \deg(r(x)) < n\}$$

Proof. Let $(p(x)) + f(x) \in F[x]/(p(x))$ be a coset and let $S := \{(p(x)) + r(x) \mid 0 \leq \deg(r(x)) < n\}$. Because polynomial rings are Euclidean domains, we can apply the Euclidean algorithm to write $f(x) = q(x)p(x) + r(x)$ for some $r(x)$ of degree strictly less than n. Then

$$p(x) + f(x) = p(x) + q(x)p(x) + r(x) \equiv p(x) + r(x) \mod (p(x))$$

thus they are in the same equivalence classes, in other words $(p(x)) + f(x) = (p(x)) + r(x)$. Thus, the equivalence class $(p(x)) + f(x) \in S$, implying that $F[x]/(p(x)) \subseteq S$.

Now, suppose we have $(p(x)) + r(x), (p(x)) + s(x) \in S$ such that $(p(x)) + r(x) = (p(x)) + s(x)$. Then, $p(x) \mid r(x) - s(x)$. However, see that the degrees of $r(x)$ and $s(x)$ are strictly less than n, thus their difference also has degree strictly less than n. The only value that $p(x)$ can evenly divide of degree less than n is 0, thus $r(x) - s(x) = 0$ which implies that $r(x) = s(x)$. We've therefore shown each of the equivalence classes in S is distinct.

Thus, for all $r(x) \in F[x]$ of degree strictly less than n, its equivalence class mod $(p(x))$ is in S and we've shown it's different from the other equivalence classes in S. This implies $F[x]/(p(x)) = S$. □

Proposition 9. *Let F be a field and $p(x) \in F[x]$ be an irreducible polynomial of degree n. Then, $F[x]/p(x)$ is a field extension of F, and $[F[x]/p(x) : F] = n$.*

Proof. First, we show that $F[x]/p(x)$ is indeed a field extension of F. We showed in Proposition 6 that $F[x]/p(x)$ is a field. Thus, all that remains to show is that $F \subset F[x]/p(x)$. We claim that F is isomorphic to the set $\{(p(x)) + q \mid q \in F\} \subset F[x]/p(x)$ with the isomorphism $q \mapsto (p(x)) + q$.

The multiplicative identities map to each other because $1 \mapsto (p(x)) + 1$. Next, let $q, r \in F$, then $qr \mapsto (p(x)) + qr = ((p(x)) + q)((p(x)) + r)$ and $q + r \mapsto (p(x)) + (q + r) = ((p(x)) + q) + ((p(x)) + r)$, showing this mapping is a ring homomorphism. Let $(p(x)) + q \in F[x]/p(x)$, then by construction $q \in F$ is such that $q \mapsto (p(x)) + q$ implying surjectivity. We showed injectivity at the end of the proof of Proposition 8, namely $(p(x)) + q = (p(x)) + r \implies q = r$.

From Proposition 8, we also know that $F[x]/(p(x)) = \{(p(x)) + r(x) \mid 0 \leq \deg(r(x)) < n\}$. For all $(p(x)) + r(x) \in F[x]/(p(x))$, where $r(x) = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1}$ for $b_i \in F$, we can write

$$\begin{aligned}(p(x)) + r(x) &= (p(x)) + b_0 + b_1 x + \cdots + b_{n-1}x^{n-1} \\ &= b_0((p(x)) + 1) + b_1((p(x)) + x) + \cdots + b_{n-1}((p(x)) + x^{n-1})\end{aligned}$$

implying $B = \{(p(x))+1, (p(x))+x, \ldots, (p(x))+x^{n-1}\}$ is a basis for $F[x]/(p(x))$. Thus, $\dim F[x]/(p(x)) = |B| = n$, which implies by Definition 3 that $[F[x]/p(x) : F] = n$. □

Corollary 5. $[\mathbb{Q}[x]/(x^3 - 2) : \mathbb{Q}] = 3$

Proof. We showed in Corollary 3 that $x^3 - 2$ is irreducible over $\mathbb{Q}$, and because it is of degree 3 it follows from Proposition 9 that $[\mathbb{Q}[x]/(x^3 - 2) : \mathbb{Q}] = 3$. □

3 Doubling the Cube is Impossible

Given these intermediate results, the impossibility of doubling the cube immediately follows.

Theorem 1. $\sqrt[3]{2}$ *is not constructible.*

Proof. By Corollary 5, we know that $[\mathbb{Q}[x]/(x^3 - 2) : \mathbb{Q}] = 3$. By Corollary 4, $\mathbb{Q}[x]/(x^3 - 2) \cong \mathbb{Q}(\sqrt[3]{2})$, where $\mathbb{Q}(\sqrt[3]{2}) = \{q_0 + q_1\sqrt[3]{2} \mid q_0, q_1 \in \mathbb{Q}\}$. This implies that $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. However, by Corollary 2, this implies that $\sqrt[3]{2}$ is not constructible. □

References

[1] William J. Gilbert and W. Keith Nicholson. Modern algebra with applications. John Wiley & Sons, 2004.

[2] Juan Liu Matt Friehauf, Mikaela Hertel and Stacey Luong. On compass and straightedge constructions: Means. "`https://sites.math.washington.edu/~julia/teaching/445_Spring2013/ConstructionsI.pdf#page=6&zoom=80,-502,802`", 2013.