On the Field of Constructible Numbers

Course Project for MATH 320: Algebra I

Muhammad Hashir Hassan Khan

2024-10-0111

May 3, 2024

The Greeks posed three mathematical problems in Euclidean geometry that remained unsolved for the better part of 2000 years. They are the following:

- **Doubling the Cube**. Can we construct a cube that has twice the volume of a given constructed cube?
- **Trisecting the Angle**. Can we trisect any constructed angle?
- **Squaring the Circle**. Can we construct a square with the same area as a constructed circle?

This report aims to prove that the answer to all three of the above is a resounding "No!"

We begin with a few preliminary results from abstract algebra and specifically, field theory.

Definition 1. A field K is called an **extension field** of a field F if F is a subfield of K.

We now attempt to construct extension fields when we are given a field F. To do this, recall that $F[x]$ is the field of polynomials with coefficients in F. Now, there may exist a polynomial $p(x) \in F[x]$ such that $p(x)$ has a root which is not in F. For example, $p(x) = x^2 - 2$ is a polynomial in $\mathbb{Z}[x]$ but its roots $\pm\sqrt{2}$ are not integers. The following theorem now allows us to find an extension field of $\mathbb{Z}$:

Theorem 1. *Let F be a field and $p(x)$ a non-constant polynomial in $F[x]$. There exists an extension field E of F and an element $c \in E$ such that c is a root of $p(x)$.*

Proof. Assume that $p(x)$ is an irreducible polynomial in $F[x]$. (If it is reducible, we can factorize it and work with its irreducible factors.) If $p(x)$ is irreducible in $F[x]$, then $\langle p(x)\rangle$ is a maximal ideal of $F[x]$. Therefore, the quotient ring $F[x]/\langle p(x)\rangle$ is a field. Let $J = \langle p(x)\rangle$. Define the ring homomorphism $h : F \to F[x]/J$ as

$$h(a) = J + a,$$

for all $a \in F$. Now, h is a homomorphism because

$$\begin{aligned} h(a+b) &= J + (a+b) = J + a + J + b = h(a) + h(b), \\ h(a \cdot b) &= J + (a \cdot b) = (J + a) \cdot (J + b) = h(a) \cdot h(b). \end{aligned}$$

Since $\mathrm{Ker}(h)$ is an ideal in F and a field only has the trivial ideals, $\mathrm{Ker}(h) = 0$. Therefore, h is injective and hence, h is an isomorphism between its domain and range. We can talk about the element $a \in F$ as the constant polynomial $a \in F[x]$. Then, $J + a$ is a coset of a constant polynomial and F is isomorphic to the subfield of $F[x]/J$ consisting of cosets of constant polynomials. Therefore, $F[x]/J$ is an extension field of F.

We now show that $J + x$ is a root of $p(x) = a_0 + a_1x + \ldots + a_nx^n$ in $F[x]/J$:

$$\begin{aligned}
p(J + x) &= (J + a_0) + (J + a_1)(J + x) + \ldots + (J + a_n)(J + x^n), \\
&= (J + a_0) + (J + a_1x) + \ldots + (J + a_nx^n), \\
&= J + (a_0 + a_1x + \ldots + a_nx^n), \\
&= J + p(x), \\
&= J,
\end{aligned}$$

where in the last line, we used the fact that $p(x) \in J$. Note that we have abused notation slightly by using $p(J + x)$. □

We have now found that a root of $p(x)$ is present in $F[x]/J$ when it was absent in $F[x]$. This field extension of F is denoted by $F(c)$, where c is the root of $p(x)$. This notation comes from the fact that elements in $F(c)$ are polynomials in c. Moving on, let K denote the extension field of F. Then, we can treat K as a vector space with the entries in each vector coming from F. This gives us a natural definition.

Definition 2. The **degree** of an extension field K over its subfield F is the dimension of the F-vector space K. It is denoted by $[K : F]$.

There is a theorem that gives us a way to calculate the degree of our extension field $F(c)$. Before we state it, we need another definition.

Definition 3. The **minimal polynomial** of a field element c over a field F is the irreducible polynomial of the form $p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ which has c as a root and where the a_i's are from F.

We are now in a position to state the theorem.

Theorem 2. *The degree of $F(c)$ over F is equal to the degree of the minimal polynomial of c over F.*

Proof. Let $p(x) = a_0 + a_1x + \ldots + a_nx^n$ be the minimal polynomial of c over F. Then, $p(x)$ has degree n. We will show that the set $C = \{1, c, c^2, \ldots, c^{n-1}\}$ is a basis for the vector space $F(c)$. We first show that C spans $F(c)$. Let $a(c) \in F(c)$ be an arbitrary polynomial. Then, using the Division Algorithm to divide $a(x)$ by $p(x)$, we get $a(x) = p(x)q(x) + r(x)$, where $r(x)$ is a polynomial with degree $\leq n - 1$. Inputting $x = c$, $a(c) = p(c)q(c) + r(c) = 0 + r(c) = r(c)$. Therefore, every polynomial in $F(c)$ has degree $\leq n - 1$ and can be written as $b_0 + b_1c + \ldots + b_{n-1}c^{n-1}$. We now show that the elements in C are linearly independent. Let $d_0 + d_1c + \ldots + d_{n-1}c^{n-1} = 0$. If there is at least one $d_i \in F$ which is non-zero, then c is the root of the resultant polynomial which has degree $\leq n - 1$. But the minimal polynomial of c over F has degree n. We have a contradiction. Therefore, C is a linearly independent set of vectors which spans $F(c)$ and we are done. □

Now that we have our preliminary results, we move onto constructions. We begin by specifying what we mean by construction. Assume that we have two tools in our possession: a collapsible compass and a straightedge. Beginning with two points in the Euclidean plane with coordinates $(0, 0)$ and $(1, 0)$, we want to find out what numbers we can construct. We first try to do this intuitively. What does a straightedge do? It draws a line segment. Assuming that we have an ideal straightedge means that we can extend this line segment indefinitely. What does a compass do? It draws a circle. Assuming that we have an ideal compass means that we can draw a circle of as large a radius as we want. Using these intuitive ideas, we can define what we mean by a constructible number.

Definition 4. A **constructible point** is the point of intersection of two lines, a line and a circle or two circles, each of which has been constructed in a finite number of steps from a given set of two points. A **constructible number** is the x– or y–coordinate of such a point.

We now state a few results without stating their explicit constructions. The reader may consult any standard text to find these.

- If a and b are constructible numbers, then $a+b$ and $a-b$ is constructible.
- If a and b are constructible numbers, then ab and $\frac{a}{b}$ are constructible.
- If a is a constructible number, then $\sqrt{a}$ is constructible.

Going back to the definition, and noting the above, we call a point in the plane constructible if it can be constructed in a finite number of steps from $\mathbb{Q} \times \mathbb{Q}$. To construct our set of constructible numbers, let $P_1 = (a_1, b_1)$ be constructible in one step from $\mathbb{Q} \times \mathbb{Q}$ and $P_i = (a_i, b_i)$ be constructible in one step from $\mathbb{Q} \times \mathbb{Q} \cup \{P_1, P_2, \ldots, P_{i-1}\}$. With each point P_i, we associate a field K_i such that $K_i = K_{i-1}(a_i, b_i)$. The notation makes it clear that K_i is an extension field of K_{i-1} and contains the elements a_i and b_i. We now prove an important result.

Lemma 1. $[K_i, K_{i-1}] = 1, 2$ or 4.

Proof. Using Definition 4, a point can be constructed using 3 methods:

- If it is constructed as an intersection of two lines, we get a linear equation for x and y. Since the degree of a linear equation is 1, $[K_i, K_{i-1}] = 1$.
- If it is constructed as an intersection of a line and a circle or two circles, we get a quadratic equation for both x and y. Since the degree of a quadratic equation is 2, and x may or may not be equal to y, we get $[K_i, K_{i-1}] = 2$ or 4.

$\square$

If J is an extension field of K which in turn is an extension field of L, we have that $[J : L] = [J : K][K : L]$. Using this, we get our most important result.

Lemma 2. $[K : F] = 2^n$ if K is an extension field of F and contains points constructed from F.

We shall use this lemma to answer the three questions posed at the start of this report.

Question 1. Consider a cube of length 1. Clearly, its volume is 1. Doubling the cube would mean that the new volume is 2. Let x be the length of this new cube. Then, we have that $x^3 - 2 = 0$. Clearly, this is a minimal polynomial over $\mathbb{Q}$. Therefore, $[F(x) : \mathbb{Q}] = 3 \neq 2^n$. Therefore, the side length x cannot be constructed.

Question 2. Consider the angle $\theta = \frac{\pi}{9}$. Trisecting $\frac{\pi}{3}$ would give us this angle. Now, if $\frac{\pi}{9}$ is constructible, then the length $\cos\left(\frac{\pi}{9}\right)$ should be constructible. Using $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$ and $\alpha = \cos\theta$, we get $\alpha^3 - \frac{3}{4}\alpha - \frac{1}{8} = 0$. Clearly, this is a minimal polynomial over $\mathbb{Q}$. Therefore, $[F(x) : \mathbb{Q}] = 3 \neq 2^n$ and the side length α cannot be constructed. Hence, there cannot be any general technique for trisecting an angle.

Question 3. Consider a circle of radius 1. Clearly, its area is π. Squaring the circle would mean that we have a square of length $\sqrt{pi}$. But π is transcendental over $\mathbb{Q}$. Therefore, $[F(\pi) : \mathbb{Q}] = \infty \neq 2^n$. Therefore, the side length $\sqrt{\pi}$ cannot be constructed.