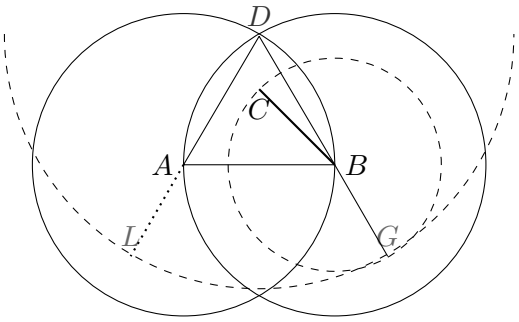
BASIC (ABSTRACT) ALGEBRA II
CONSTRUCTIBLE NUMBERS

THERON BOERNER

Contents

1. Introduction

We assume a modern compass that can copy distances, equivalent to a collapsing compass as shown:



In general, we follow the outline of [Cox04].

2. Constructible Numbers

We borrow our axioms from [Cox04, p.255]. Two constructions can be performed with our compass and straightedge.

(C1) Given two points $\alpha \neq \beta$ we can draw the line both α and β.
(C2) Given two points $\alpha \neq \beta$ and a point γ we can draw a circle of radius $\alpha\beta$ centered at γ.

These allow for the creation of new points:

(P1) The intersection of two lines.
(P2) The intersection of a line and a circle.
(P3) The intersection of two circles.

We start with only two points: 0 and 1.

Definition 2.1. We say a number is **constructible** if it can be made by finite applications of (C1), (C2), (P1), (P2), and (P3), starting from 0 and 1.

Example 2.2. The integers are constructible. Thus the horizontal axis is constructible.

Proof. We proceed by induction. Let $P(n)$ be the statement that $n \in \mathcal{C}$. We proceed by induction. **Base case.** 0 and 1 exist. **Inductive Step.** Suppose $P(n)$ for some n. (C1) line through 0 and n; (C2) $r = 1$ at n; (P2) $n+1$ exists. Thus we've shown $P(n)$ implies $P(n+1)$. Thus we've proven $P(n)$ for $n \geq 0$. Similarly, $P(n)$ is true for $n < 0$. The complete proof is graphically represented in Fig. 1. □

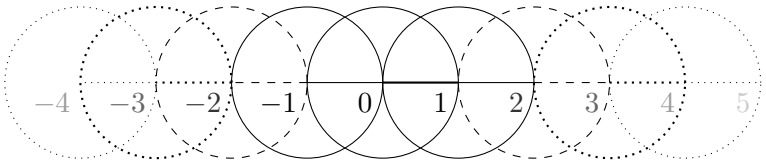


Figure 1. Construction of $\mathbb{Z}$ using straightedge and compass, starting from 0 and 1.

Example 2.3. $i\mathbb{Z} \subset \mathcal{C}$. Thus, the vertical axis is constructible.

Proof. We start with $-1, 0, 1 \in \mathcal{C}$ by the previous example. It suffices to show that if we can construct i then we are done because the argument to construct $i\mathbb{Z}$ is symmetric to the previous proof. Fig. 2 shows our strategy. (C2) $r = 1$ at 0; (C2) $r = 1$ at 1; (P3) two points u and d; (C1) u to d; (P1) $0.5 \in \mathcal{C}$; (C3) $r = 1.5$ at 1; (C3) $r = 1.5$ at -1; (P3) two points u and d; (P1) u to d; (P2) $i \in \mathcal{C}$. □

Date: March 9, 2022.

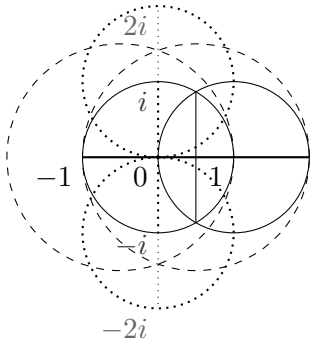


FIGURE 2. Construction of $i\mathbb{Z}$.

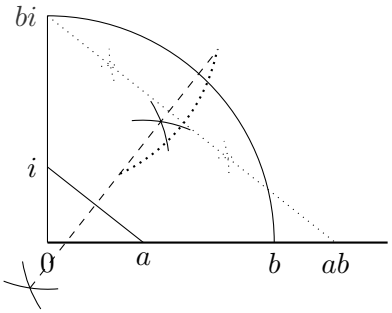


FIGURE 3. Construction of $ab \in \mathbb{R} \cap \mathcal{C}$ from $ab \in \mathbb{R} \cap \mathcal{C}$.

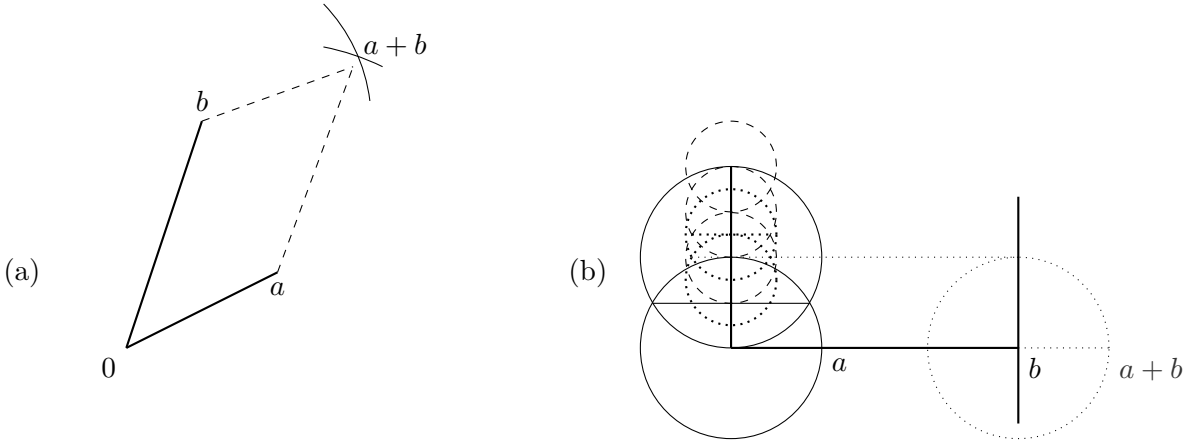


FIGURE 4. (a) Addition of two non-colinear vectors. Drawing the circle of radius $|a|$ around b and vice versa gives the point $a+b$. (b) Addition of two co-linear vectors. A parallel line can be constructed $|a|$ away from b. This gives $a+b$ by extension of the line and a circle.

Proposition 2.4. *$\mathcal{C} \cap \mathbb{R}$ is a subfield of $\mathbb{R}$.*

Proof. By construction, $0, 1 \in \mathcal{C}$. Additive closure is shown by Fig. 4. Multiplicative closure is shown by Fig. 3. Multiplicative inverses are shown by Fig. 5. The additive inverse for $a \in \mathcal{C}$ is constructed by the intersection of the line through 0 and a and the circle of radius $|a|$ around the origin. Thus, we have shown $\mathcal{C}$ is a subfield of $\mathbb{C}$. □

Proposition 2.5. *If $a, b \in \mathbb{R}$ then $\alpha = a + bi \in \mathcal{C}$ iff $a, b \in \mathcal{C}$.*

Proof. In the forward direction the perpendiculars are dropped to get a and bi and the circle is constructed of radius $|bi|$ around the origin to construct b. Likewise in the reverse direction we use b and the circle to construct bi and then then add together a and bi by the formation of perpendiculars against the two axes at a and bi. (See Fig. 6 for a graphical proof.) □

Proposition 2.6. $\alpha \in \mathcal{C} \implies \sqrt{\alpha} \in \mathcal{C}$.

Proof. Since 1 is constructible, and r is constructible so also is $1+r$. Then we can bisect this line and draw the circle from this middle point to 0 around this middle point. At 1 we form a line perpendicular to the x-axis. The length from 1 to either of the two points intersecting the circle is $\sqrt{r}$. (See Fig. 7 for a graphical proof.) □

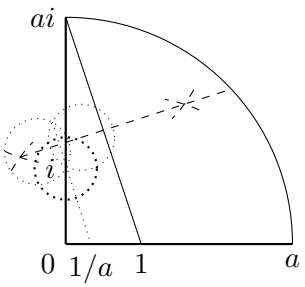


FIGURE 5. Diagram of construction of $1/a \in \mathbb{R} \cap \mathcal{C}$ from $a \in \mathbb{R} \cap \mathcal{C}$.

Proposition 2.7. *$\mathcal{C}$ is a subfield of $\mathbb{C}$.*

Proof. We know that $0, 1 \in \mathcal{C}$. Multiplicative closure can be shown algebraically. Consider $a + bi, c + di \in \mathcal{C}$. By Proposition 2.5 we know that $a, b, c, d \in \mathcal{C}$. Now consider the expanded product:

$$(a + bi)(c + di) = ac - bd + i(ad + bc)$$

Notice that $ac - bd, ad + bc \in \mathbb{R} \cap \mathcal{C}$ since $\mathbb{R} \cap \mathcal{C}$ is a subfield of $\mathbb{C}$. Then by Proposition 2.4 we know that $ac - bd + i(ad + bc) \in \mathcal{C}$. Thus we've shown multiplicative closure.

To show $(a + bi)^{-1} \in \mathcal{C}$ consider the following

$$\frac{1}{a+bi} \cdot \frac{a-bi}{a-bi} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - i\frac{b}{a_2+b_2}.$$

We can construct both $a/(a^2+b^2)$ and $-b/(a^2+b^2)$ because the constructible reals form a subfield. Therefore by Proposition 2.5 we know that $(a + bi)^{-1}$ is constructible.

Hence, $\mathcal{C}$ is a subfield of $\mathbb{C}$. □

3. Some Negative Results

We now turn our attention to three problems of straightedge and compass constructions faced by the ancient Greeks: trisecting an angle, doubling the volume of a cube, and squaring the circle. We will show that these results do not hold in the general case by providing counterexamples

First, we need the following theorem found in Cox [Cox04, Thm. 10.1.6].

Theorem 3.1. *Let $\alpha \in \mathbb{C}$. Then $\alpha \in \mathcal{C}$ iff there are subfields*

$$\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n \subset \mathbb{C}$$

such that $\alpha \in F_n$ and $[F_i : F_{i-1}] = 2$ for $1 \leq i \leq n$.

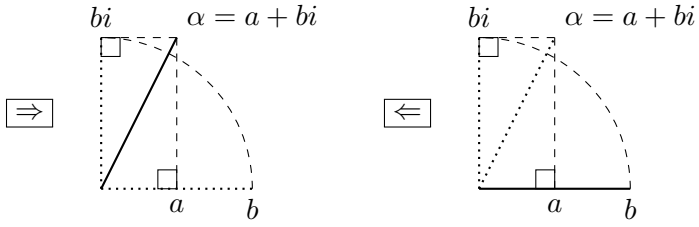


FIGURE 6. $a+bi \in \mathcal{C} \iff a, b \in \mathcal{C}$.

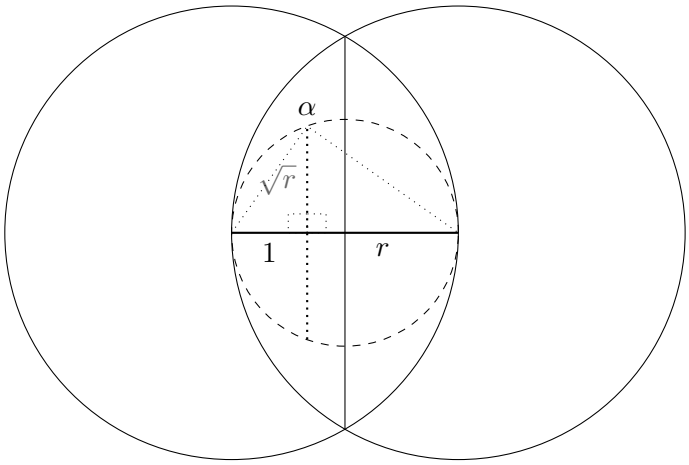


FIGURE 7. Square root is constructible.

Proof. ⇐ We have $\mathbb{Q} = F_0 \subset F_1 \cdots \subset F_{n-1} \subset F_n \subset \mathbb{C}$. We can then prove by induction that $F_i \subset \mathcal{C}$.

Base case: $n = 0$. We know that $\mathcal{C}$ is a subfield of $\mathbb{C}$ so that $\mathbb{Q} = F_0 \subseteq \mathcal{C}$.

Inductive step: Suppose that $F_{i-1} \subseteq \mathcal{C}$. We claim that $F_i = F_{i-1}(\sqrt{\alpha_i})$ for some $\alpha_i \in F_i$. We follow Exercise 7.1.12 to prove this claim.[1]

Let $\beta \in F_i \setminus F_{i-1}$. Then Since $[\mathbb{F}_i : \mathbb{F}_{i-1}] = 2$, there exists a, b, c not all zero such that

$$a\beta^2 + b\beta + c = 0$$

Now suppose $a = 0$. If $b\beta + c = 0$ then $b = c = 0$, a contradiction. So $b \neq 0$.

[1] I also used this link to help with the proof https://math.stackexchange.com/a/2494366.

Then $\beta = -\frac{c}{b} \in F$, also gives a contradiction so that $a \neq 0$. Thus, β is a root of

$$f(x) := ax^2 + bx + c = 0.$$

Now we turn $f(x)$ into a monic polynomial:

$$g(x) := x^2 + a^{-1}bx + a^{-1}c = 0$$

giving us the following identity: $x^2 + a^{-1}bx = -a^{-1}c$ and then we complete the square:

$$\begin{aligned}
&(x + b/2a)^2 + a^{-1}c - \frac{b^2}{4a^2} \\
&= x^2 + \frac{bx}{a} + \frac{b^2}{4a^2} + a^{-1}c - \frac{b^2}{4a^2} \\
&= -\frac{c}{a} + \frac{b^2}{4a^2} + a^{-1}c - \frac{b^2}{4a^2} \\
&= 0.
\end{aligned}$$

Letting $\alpha = \beta + b/2a$ we can see that $\alpha^2 \in F_{i-1}$ because $\alpha^2 = -\frac{c}{a} + \frac{b^2}{4a^2}$. We also know that $\alpha \notin F_{i-1}$ and so $[F_{i-1}(\alpha) : F_i] = 2$ implies $F_i = F_{i-1}(\alpha)$. Thus we have proven the claim that $F_i = F_{i-1}(\sqrt{\alpha_i})$ for some $\alpha_i \in F_i$.

Then take $a \in F_i$ we know that $a = f(\sqrt{\alpha_i})$ for some $f(x) \in F_{i-1}[x]$. Since $\sqrt{\alpha_i}$ is constructible by Proposition 2.6 and the constructible numbers form a subfield we therefore know that a is constructible. So $F_i \subseteq \mathcal{C}$.

Thus, by mathematical induction we've proven the reverse direction.

$\boxed{\Rightarrow}$ For the forward direction we have $\alpha in \mathcal{C}$ and we wish to construct telescoping field extensions starting from $\mathbb{Q}$ such that $\alpha = a + bi \in F_n$ and $[F_i : F_{i-1}] = 2$ for $1 \leq i \leq n$.

We proceed by induction on the number of times, N, we use (P1)—(P3) in constructing α.

Base case: Let $F_n = F_0 = \mathbb{Q}$ since we only have 1 and 0.

Inductive Step: Suppose $\alpha = a + bi$ is constructed in $N > 0$ steps so we have $\mathbb{Q} = F_0 \subset \cdots \subset F_n \subset \mathbb{C}$ with successive extensions of degree 2. We have three cases on to consider: one for each of the P's. If the last construction was (P1) then we know that we have the intersection of two lines. We can show through a lot of symbol shuffling that this gives us a system of linear equations with coefficients in F_n which has a unique solution by linear algebra. We must have $a, b \in F_n$ so then $\alpha \in F_n(i)$, which is a degree two extension.

If the last step was (P2) then we know that. [Soz I'm way too sleep deprived Trevor this is all I can do.]

Having proven both direction we are finished. □

Corollary 3.2 (Cox, Cor. 10.1.8)**.** *If $\alpha \in \mathcal{C}$ then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^m$ for some $m \geq 0$. Thus every constructible number is algebraic over $\mathbb{Q}$, and the degree of its minimal polynomial over $\mathbb{Q}$ is a power of 2.*

Proof. Apply the tower theorem to the telescoping fields given by the previous Theorem to obtain the result. □

Example 3.3. The angle of 40 degrees cannot be constructed and therefore the angle of 120 degrees can not be trisected with a straightedge and compass.[2]

To prove this we first need some theory provided in Cox [Cox04, Ch. 9]. Recall that

$$\zeta_n = e^{2i\pi/n},$$

and

$$x^n - 1 = \prod_{0 \leq i < n} (x - \zeta_n^i).$$

Definition 3.4. The n$^{\text{th}}$ cyclotomic polynomial is defined as

$$\Phi_n(x) := \prod_{\substack{0 \leq i < n \\ \gcd(i,n)=1}} (x - \zeta_n^i)$$

Proposition 3.5 (Cox, Prop. 9.1.5)**.** *$\Phi_n(x)$ is a monic polynomial with integer coefficients and has degree $\varphi(n)$, where $\varphi(n)$ is the Euler totient function. Furthermore, these polynomials satisfy the identity*

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

[2] In AutoCAD this can be performed by constructing a temporary arc using ARC then DIVIDE into 3 pieces.

Theorem 3.6 (Cox, Thm. 9.1.9)**.** *The cyclotomic polynomial $\Phi_n(x)$ is irreduible over $\mathbb{Q}$.*

Now we can prove Example 3.3.

Proof of Example 3.3. If the angle of 40 degrees can be constructed then $\zeta_9 = e^{2\pi i/9}$, the 9th root of unity, is constructible since this is just the vector of distance 1 an angle 40 degrees. The minimal polynomial of ζ_9 is $\Phi_9(x)$ because it is irreducible by Theorem 3.6 and it is monic. We could expand the product in the definition of $\Phi_9(x)$ but this has too many terms to deal with. Instead we use Proposition 3.5 to obtain the factorization:

$$x^9-1 = \Phi_1(x)\Phi_3(x)\Phi_9(x) = (x-1)(x^2-1)\Phi_9(x).$$

Then we divide to obtain

$$\Phi_9(x) = x^6 + x^3 + 1.$$

But $\deg(\Phi_9) = 6$ which is not a power of two. So by Corollary 3.2 the angle 40 degrees is not constructible and thus the angle of 120 degrees cannot be trisected. □

Example 3.7. The number $\sqrt[3]{2}$ cannot be constructed and therefore the unit cube cannot be doubled by straightedge and compass.

Proof. The minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is x^3-2. If this number were constructible then by Corollary 3.2 the minimal polynomial has degree of a power of 2. But 3 is not a power of 2. So $\sqrt[3]{2} \notin \mathcal{C}$. □

Example 3.8. The number $\sqrt{\pi}$ is not constructible and therefore not every circle can be squared as the unit circle has area π.

Proof. Suppose that $\sqrt{\pi}$ is constructible. Then $\sqrt{\pi}^2 = \pi$ is constructible because $\mathcal{C}$ is a field. Then by Corollary 3.2 π is algebraic over $\mathbb{Q}$, a contradiction. □

References

[Cox04] David A. Cox. *Galois Theory*. Pure and Applied Mathematics : A Wiley-Interscience Series of Texts, Monographs, and Tracts. Hoboken, N.J: Wiley-Interscience, 2004. 559 pp. ISBN: 978-0-471-43419-1.