Formalisation of constructable numbers

Ludwig Monnerjahn

Geboren am 03.09.2002 in Berlin

12.09.2024

Bachelorarbeit Mathematik

Betreuer: Prof. Dr. Floris van Doorn

Zweitgutachter: Prof. Dr. Philipp Hieronymi

Mathematisches Institut

Mathematisch-Naturwissenschaftliche Fakultät der

Rheinischen Friedrich-Wilhelms-Universität Bonn

Abstract

The Bachelor's thesis addresses the formalisation of ancient construction problems, with a particular focus on the "Impossibility of Trisecting the Angle and Doubling the Cube". This is the eighth theorem published by Freek Wiedijk in the '100 Theorems' compendium, which serves to allow for a comparison of different theorem provers. For this, the theorem prover Lean is utilised. As a result, this paper is devoted to the problems and solutions that arise when formalising ancient construction problems and proves the impossibility of doing so using Galois' theory.

Zusammenfassung in deutscher Sprache

Die Bachelorarbeit befasst sich mit der Formalisierung antiker Konstruktionsprobleme, wobei der Schwerpunkt auf der „Unmöglichkeit der Dreiteilung des Winkels und der Verdoppelung des Würfels“ liegt. Dies ist das achte Theorem, das Freek Wiedijk in dem im Rahmen von „100 Theorems“ veröffentlichten Kompendium veröffentlicht hat, das dazu dient, einen Vergleich verschiedener Theorembeweiser zu ermöglichen. Hierfür wird der Theorembeweiser Lean verwendet. Die vorliegende Arbeit widmet sich daher den Problemen und Lösungen, die bei der Formalisierung alter Konstruktionsprobleme auftreten, und beweist die Unmöglichkeit, dies mit der Galois-Theorie zu tun.

Contents

Acknowledgment

I would like to express my gratitude to my advisor, Prof. Dr. Floris van Doorn, for his help during all those times when Lean and I had a different understanding of what a sufficient proof looks like. Additionally, I am grateful for the encouragement to maintain a broader perspective and to focus on tangible outcomes, as otherwise I would still be engaged in the process of defining a line.

I would like to express my gratitude to Prof. Jan Schröer for providing the impetus for me to attempt to formalise this topic through his stimulating lecture on the subject.

Furthermore, I would like to express my gratitude to my friend Joshua Hendriks, who had to endure an initial, imperfect iteration of this thesis and identify areas for improvement.

Finally, I would like to thank Leo Diedering for giving me an idea on how to structure my thesis.

Chapter 1

Introduction in the topic of the Bachelor Thesis

This paper formalises the proof of "The Impossibility of Trisecting the Angle and Doubling the Cube" in ruler and compass construction. The Github repository with the code and bluebrint can be found here : `https://github.com/Louis-Le-Grand/Formalisation-of-constructable-numbers`

1.1 Construction Problems

The straightedge and compass constructions were developed by the ancient Greeks. It consists of an initial set $\mathcal{M}$ of constructed points, a ruler that has no measurements and can draw indefinite lines through at least two existing points, and a compass, the centre of which is an already constructed point and the radius of which is the distance between two already constructed points. To construct new points, take the intersection of two lines, two circles or a line and a circle. The set of all possible intersections is called $\mathcal{M}_\infty$. In order to construct a line or a circle, it is necessary that our initial set contain at least two points. Consequently, we can normalise our set and assume that $0, 1 \in \mathcal{M}$.

We may now proceed to define the problem of doubling a cube. The volume of a cube is equal to the cube of the length of an edge, which may be expressed as a^3, where a is the length of an edge. Therefore, a cube with a doubled volume, $2 \cdot a^3$, has an edge length of the cube root of two times the length of the original edge. If we now take the cube with a length of one, the problem is as follows:

Problem 1.1 (Doubling the Cube)**.** *Given the set $\mathcal{M} = \{0, 1\}$, can we construct the point $\sqrt[3]{2}$, i.e. is $\sqrt[3]{2} \in \mathcal{M}_\infty$?*

A similar approach allows the problem of trisecting angles to be simplified. If we take two points on the real axis and a third point on the unit circle, this defines an angle. Thus we need the points 0, 1 and $e^{i\alpha}$. The trisection intersects the unit circle at $e^{i\alpha/3}$. Therefore the problem can be described as follows:

Problem 1.2 (Trisecting the Angle)**.** *Given the set* $\mathcal{M} = \{0, 1, e^{\imath \cdot \alpha}\}$*, can we construct the point* $e^{\imath \cdot \frac{\alpha}{3}}$*, i.e. is* $e^{\imath \cdot \frac{\alpha}{3}} \in \mathcal{M}_\infty$*?*

1.2 Motivation

The subject of this formalisation is the eighth theorem of Freek Wiedijk's list of "100 Theromes", entitled "The Impossibility of Trisecting the Angle and Doubling the Cube" [8]. This is a list of theorems based on an online list from 1999 of the 100 most significant theorems in mathematics [1], which is used for comparative purposes with respect to different theorem provers. The list provides a concise overview of the most important theorem provers, showcases fields in which theorems can be used, and also presents some smaller programs that have formalised theorems that had not yet been formalised in any other environment. Notably, the aforementioned theorem had not yet been formalised in Lean [3].

1.3 Lean, Theorem Prover and Mathlib

Lean is a functional programming language that can be utilised as an interactive theorem prover. The Lean Project was initiated by Leonardo de Moura at Microsoft Research Redmond in 2013 and represents a long-term research endeavour, published under the Apache 2.0 licence.

In order to verify a theorem, it is necessary to find proof. Computers can be of assistance in two distinct ways: firstly, through interactive theorem proving, which verifies the correctness of a proof step by step; and secondly, through automated theorem proving, which attempts to find a proof for a given statement. Lean represents a hybrid of these two approaches. It is an interactive theorem prover, but it incorporates automated tools and methods to assist in the construction of a fully specified axiomatic proof.[2]

Mathlib is a library of mathematical content for the Lean programming language. It is a community-developed project, created by a large number of contributors and covering a substantial breadth of mathematical topics. To ascertain which areas are encompassed by MathLib, one may refer to the following link: `https://leanprover-community.github.io/mathlib-overview.html`.

Outline of the Thesis

The following three chapters present the blueprint for my formalisation. Consequently, the document includes a number of elementary lemmas and details that are not typically documented in such a manner. However, a few statements and most of the auxiliary lemmas are not included in the blueprint. The structure of this formalisation is based on the lecture "Einführung in die Algebra" by Jan Schröer (WS 22/23).

Chapter 2

Basic Constructions with Ruler and Compass

2.1 Defining lines, circles and the set of constructable points

First we need to define what construction using a ruler and compass means. We will use $\mathbb{C}$ as plane of drawing and $\mathcal{M} \subset \mathbb{C}$ as the set of constructed points.

Definition 2.1 (Line)**.** *A line $L := (x, y)$ is defined by two points $x, y \in \mathbb{C}$ with $x \neq y$ and a set*

$$l := \{\lambda x + (1 - \lambda)y \mid \lambda \in \mathbb{R}\}.$$

We say two lines are equal if their generated set is equal.

Remark 2.2. *To express lines in the most general way, they are stated without the requirement that $x \neq y$, which allows for trivial lines. The condition is only included in the lemmas that require it.*

Definition 2.3 (Circle)**.** *A circle $C := (c, r)$ is defined by a center c with $c \in \mathbb{C}$, a radius $r \in \mathbb{R}_{\geq 0}$ and the set:*

$$c := \{z \in \mathbb{C} \mid \|z - c\| = r\}.$$

We say two circles are equal if their underlying sets are equal.

Lemma 2.4. *If we have two circles $C_1 = (c_1, r_1)$, $C_2 = (c_2, r_2)$ and we have $c_1 \neq c_2$ or $r_1 \neq r_2$ then the circles aren't equal.*

Definition 2.5 (Set of lines)**.** *$\mathcal{L}(\mathcal{M})$ is the set of all real straight lines l, with $|l \cap \mathcal{M}| \geq 2$. As a set this is:*

$$\mathcal{L}(\mathcal{M}) := \{l \mid l = \{x, y\} \text{ with } x, y \in \mathcal{M} \wedge x \neq y\}.$$

Definition 2.6 (Set of circles)**.** *$\mathcal{C}(\mathcal{M})$ is the set of all circles in $\mathbb{C}$, with center in $\mathcal{M}$ and radius of $\mathcal{C}$ which is the distance of two points in $\mathcal{M}$. As an equation this is:*

$$\mathcal{C}(\mathcal{M}) := \{c \mid c = \langle c,\ dist\ r_1 r_2\rangle \text{ with } c, r_1, r_2 \in M\}.$$

Definition 2.7 (Rules to construct a point)**.** *We define operations that can be used to construct new points.*

1. *(ILL) is the intersection of two different lines in $\mathcal{L}(\mathcal{M})$.*
2. *(ILC) is the intersection of a line in $\mathcal{L}(\mathcal{M})$ and a circle in $\mathcal{C}(\mathcal{M})$.*
3. *(ICC) is the intersection of two different circles in $\mathcal{C}(\mathcal{M})$.*

$ICL(\mathcal{M})$ is the union of all points that can be constructed using the operations (ILL), (ILC) and (ICC) and $\mathcal{M}$.

Definition 2.8 (Set of constructable points)**.** *We inductively define the chain*

$$\mathcal{M}_0 \subseteq \mathcal{M}_1 \subseteq \mathcal{M}_2 \subseteq ...$$

with $\mathcal{M}_0 = \mathcal{M}$ and $\mathcal{M}_{n+1} = ICL(\mathcal{M}_n)$
and call $\mathcal{M}_\infty = \bigcup_{n\in\mathbb{N}} \mathcal{M}_n$ the set of all constructable points.

Remark 2.9. *The set of lines, circles and their intersection icc, ilc, icc are monoton, i.e. for $N \subseteq M$ is $\mathcal{L}(\mathcal{N}) \subseteq \mathcal{L}(\mathcal{M})$,….*

2.2 Properties of Lines

In light of the fact that a considerable proportion of the forthcoming project will entail the manipulation of lines and the absence of an existing formalisation from MathLib, it is imperative to illustrate the fundamental properties that will be utilised throughout the remainder of the project.

Lemma 2.10. *The set of points of a line l is not defined by one position vector, i.e. for every $\alpha \in l$ $\{\lambda x + (1-\lambda)y \mid \lambda \in \mathbb{R}\} = \{\lambda x + \lambda y + \alpha \mid \lambda \in \mathbb{R}\}$.*

Proof. Two sets are equal if they have the same elements. Since α is in l, there exists a λ_α such that $\alpha = \lambda_\alpha x + (1-\lambda_\alpha)y$.

"⇒:" Let $z = \lambda_0 x + (1-\lambda_0)y$ (i.e. $z \in \{\lambda x + (1-\lambda)y \mid \lambda \in \mathbb{R}\}$), we have to show that $z \in \{\lambda x + \lambda y + \alpha \mid \lambda \in \mathbb{R}\}$, which is equivalent to the existence of λ such that $z = \lambda x + \lambda y + \alpha$. If we use $\lambda = \lambda_0 - \lambda_\alpha$ we get

$$(\lambda_0 - \lambda_\alpha)x + ((\lambda_0 - \lambda_\alpha))y + \alpha \overset{\alpha=\lambda_\alpha x+(1-\lambda_\alpha)y}{=} \lambda_0 x - \lambda_0 y + y = z$$

⇐: Let z be in $\{\lambda x + (\lambda)y + \alpha \mid \lambda \in \mathbb{R}\}$, if we use $\lambda = \lambda_0 + \lambda_\alpha$ we get

$$(\lambda_0+\lambda_\alpha)x+(1-(\lambda_0+\lambda_\alpha))y = \lambda_0 x-\lambda_0 y+\lambda_\alpha x-\lambda_\alpha y+y \overset{\alpha=\lambda_\alpha x+(1-\lambda_\alpha)y}{=} \lambda_0(x-y)+\alpha = z$$

□

Definition 2.11 (parallel)**.** *Two lines l_1 and l_2 are parallel if they have the same slope, i.e. $\exists r \in \mathbb{C} : l_1 = \{x + r \mid x \in l_2\}$.*

Lemma 2.12 (Parallel defined by basis)**.** *If the basis of two lines is moved by the same amount, i.e $l_1.z_1 - l_2.z_1 = l_1.z_2 - l_2.z_2$, then they are parallel.*

Proof. We have to lines l_1, l_2 with basis z_1, z_2 and $l_1.z_1 - l_2.z_1 = l_1.z_2 - l_2.z_2$. To show that they are parallel we have to show that

$$\exists r : l_1 = \{z + r \mid z \in l_2\}.$$

To make it easier to read we define $a := l_1.z_1$, $b := l_1.z_2$, $x := l_2.z_1$ and $y := l_2.z_2$. Upon unravelling the definition, it becomes evident that we need to show that $\exists t : t \cdot a + (1-t) \cdot b = z \iff \exists s : s \cdot x + (1-s)y + (a-x) = z$.
$\Rightarrow$: Claim $s = \frac{t(a-b)}{x-y}$ is a solution.

Proof.

$$\begin{aligned}
& & z = s \cdot x + (1-s)y + (a-x) & \quad | z = t \cdot a + (1-t) \cdot b \\
\Leftrightarrow & & t \cdot a + (1-t) \cdot b = s \cdot x + (1-s)y + (a-x) & \\
\Leftrightarrow & & t \cdot a - t \cdot b + b = s \cdot x - s \cdot y + y + (a-x) & \quad | -y \\
\Leftrightarrow & & t \cdot a - t \cdot b + b - y = s \cdot x - s \cdot y + (a-x) - y & \quad | a - x = b - y \\
\Leftrightarrow & & t \cdot a - t \cdot b = s \cdot x + s \cdot y & \\
\Leftrightarrow & & t(a-b) = s(x-y) & \quad | s := \frac{t(a-b)}{x-y} \\
\Leftrightarrow & & t(a-b) = \frac{t(a-b)}{x-y}(x-y) & \\
\Leftrightarrow & & t(a-b) = t(a-b) &
\end{aligned}$$

□

"$\Leftarrow$:" Claim $t = \frac{s(x-y)}{a-b}$ is a solution.

Proof.

$$\begin{aligned}
& t \cdot a + (1-t)b = z & \quad | z := s \cdot x + (1-s)y + (a-x) \\
\Leftrightarrow \quad & t \cdot a - t \cdot b + b = s \cdot x - s \cdot y + y + (a-x) & \quad | -y; a - x = b - y \\
\Leftrightarrow \quad & t(a-b) = s(x-y) & \quad | t := \frac{s(x-y)}{a-b} \\
\Leftrightarrow \quad & \frac{s(x-y)}{a-b}(a-b) = s(x-y) &
\end{aligned}$$

□

□

Definition 2.13. *The direction vector of a line l is the vector $l.z_1 - l.z_2$.*

Definition 2.14. *Two lines l_1 and l_2 are* parallel' *if there exists a k such that $l_1.z_1 - l_1.z_2 = k \cdot (l_2.z_1 - l_2.z_2)$.*

Lemma 2.15 (Parallel imp parallel')**.** *If two lines l_1 and l_2 are parallel' they are parallel.*

Remark 2.16. *The other direction holds as well, but is not needed.*

Proof. Let l_1 and l_2 be two lines with $l_1.z_1 - l_1.z_2 = k \cdot (l_2.z_1 - l_2.z_2)$. We have to show that $l_1 = \{z + r \mid z \in l_2\}$, i.e. $\exists r : l_1 = \{z + r \mid z \in l_2\}$.
First we remark that $k \neq 0$ since $l_1.z_1 \neq l_1.z_2$. We define $r := y_1 - y_2$ and show that $l_1 = \{z + r \mid z \in l_2\}$. For z to be in l_1 is equivalent to $z = \lambda x_1 + (1 - \lambda)y_1$ for some λ_0. For z to be in $\{x + y_1 - y_2 \mid z \in l_2\}$ is wquivalent to the existence of λ such that

$$z = \lambda x_2 + (1-\lambda)y_2 + y_1 - y_2 = \lambda(x_2 - y_2) + y_1 \overset{\lambda=\lambda_0 * k}{=} \lambda_0 k(x_2 - x_2) - y_1 \overset{x_1 - y_1 = k(x_2 - y_2)}{=} \lambda_0(x_1 - y_1) + y_1.$$

□

Lemma 2.17 (Parallel imp equal)**.** *If two lines l_1 and l_2 are parallel' and intersect, then they are equal.*

Proof. Let $z \in l_1 \cap l_2$. Then we use lemma 2.10 to get $l_1 = l_2 \Leftrightarrow \{\lambda(x_1 - y_1) \mid \lambda \in \mathbb{R}\} = \{\lambda(x_2 - y_2) + z \mid \lambda \in \mathbb{R}\}$. Since for every λ we have $\lambda(x_1 - y_2) + x = \lambda \cdot k(x_2 - y_2) + z$ we get $l_1 = l_2$. □

2.3 The Set M_∞

In order to work with the set of constructable points, it is necessary to have some basic lemmas at one's disposal. While these may appear to be trivial on paper, they are invaluable when undertaking a formalisation.

Lemma 2.18 ($\mathcal{M} \subseteq ICL(\mathcal{M})$)**.** *Every set M is included in the constructable points of M, i.e.*

$$M \subseteq ICL(M)$$

Proof. Follows from the definition of $ICL(M)$. □

Lemma 2.19 ($\mathcal{M}_i$ Monoton)**.** *The set $\mathcal{M}_i$ is monoton, i.e.*

$$\mathcal{M}_i \subseteq \mathcal{M}_{i+1}.$$

This can be generalised to

$$\forall m : \forall n \leq m : \mathcal{M}_n \subseteq \mathcal{M}_m.$$

Proof. Follows from the definition of $\mathcal{M}_i$. □

Lemma 2.20 ($\mathcal{M}$ in $\mathcal{M}_i$)**.** *The set $\mathcal{M}$ is in $\mathcal{M}_i$, i.e.*

$$\mathcal{M} \subseteq \mathcal{M}_i.$$

Proof. Combining the fact that $\mathcal{M}_0 = \mathcal{M}$ 2.8 and the monotonity of $\mathcal{M}_i$ 2.19 we get the result. □

Lemma 2.21 ($\mathcal{M}_i$ in $\mathcal{M}_\infty$)**.** *The set $\mathcal{M}_i$ is in $\mathcal{M}_\infty$, i.e.*

$$\mathcal{M}_i \subseteq \mathcal{M}_\infty.$$

Proof. Follows from the definition of $\mathcal{M}_\infty$. □

Lemma 2.22 ($\mathcal{M}$ in $\mathcal{M}_\infty$)**.** *The set $\mathcal{M}$ is in $\mathcal{M}_\infty$.*

Proof. Combining $\mathcal{M} \subseteq \mathcal{M}_i$ 2.20 and $\mathcal{M}_i \subseteq \mathcal{M}_\infty$ 2.21 we get the result. □

Lemma 2.23 ($\mathcal{M}_\infty$ iff $\mathcal{M}_i$)**.** *A point z is in $\mathcal{M}_\infty$ if and only if z is in $\mathcal{M}_i$ for some i.*

Proof. Follows from the definition of $\mathcal{M}_\infty$. □

Corollary 2.24 ($L(\mathcal{M}_\infty)$ iff $L(\mathcal{M}_i)$)**.** *A line l is in $\mathcal{L}(\mathcal{M}_\infty)$ if and only if l is in $\mathcal{L}(\mathcal{M}_i)$ for some i.*

Proof. Follows from 2.23 and the fact that every line in $\mathcal{L}(\mathcal{M}_\infty)$ is defined by two points in $\mathcal{M}_\infty$. □

Corollary 2.25 ($C(\mathcal{M}_\infty)$ iff $C(\mathcal{M}_i)$)**.** *A circle c is in $\mathcal{C}(\mathcal{M}_\infty)$ if and only if c is in $\mathcal{C}(\mathcal{M}_i)$ for some i.*

Proof. Follows from 2.23 and the fact that every circle in $\mathcal{C}(\mathcal{M}_\infty)$ is defined by three points in $\mathcal{M}_\infty$. □

To construct new points in the next section2.4 we still need to show that every intersection of lines and circles is in $\mathcal{M}_\infty$.

Lemma 2.26 (Intersection of lines in $\mathcal{M}_\infty$)**.** *For two lines $l_1, l_2 \in \mathcal{L}(\mathcal{M}_\infty)$ is $l_1 \cap l_2 \in \mathcal{M}_\infty$.*

Proof. By corollary 2.24 and the monotonity of $\mathcal{M}_i$ 2.19 we get that there exists an n such that $l_1, l_2 \in \mathcal{L}(\mathcal{M}_n)$. Therfore $l_1 \cap l_2 \in \mathcal{M}_{n+1} \overset{2.21}{\subseteq} \mathcal{M}_\infty$. □

Remark 2.27. *To formalise the lemmas 2.23, 2.24 and 2.25 one should use filters in Lean.*

Lemma 2.28 (Intersection of line and circle in $\mathcal{M}_\infty$)**.** *For a line $l \in \mathcal{L}(\mathcal{M}_\infty)$ and a circle $c \in \mathcal{C}(\mathcal{M}_\infty)$ is $l \cap c \in \mathcal{M}_\infty$.*

Proof. By corollary 2.24 and 2.25 we get that there exists an n such that $l \in \mathcal{L}(\mathcal{M}_n)$ and $c \in \mathcal{C}(\mathcal{M}_n)$. Therfore $l \cap c \in \mathcal{M}_{n+1} \overset{2.21}{\subseteq} \mathcal{M}_\infty$. □

Lemma 2.29 (Intersection of circles in $\mathcal{M}_\infty$)**.** *For two circles $c_1, c_2 \in \mathcal{C}(\mathcal{M}_\infty)$ it follows that $c_1 \cap c_2 \in \mathcal{M}_\infty$.*

Proof. By corollary 2.25 we get that there exists an n such that $c_1, c_2 \in \mathcal{C}(\mathcal{M}_n)$. Therfore $c_1 \cap c_2 \in \mathcal{M}_{n+1} \overset{2.21}{\subseteq} \mathcal{M}_\infty$. □

2.4 Basic constructions

It is now possible to construct fundamental points in M_∞ using a compass and ruler, which can subsequently be employed to create a field structure and special properties on M_∞. Consequently, the following constructions are based on the assumption that $M \subseteq \mathbb{C}$ with $0, 1 \in M$.

Lemma 2.30 (Negative complex numbers)**.** *For $z \in M_\infty$ it follows that $-z \in M_\infty$.*

This construction is taken from [6].
To get the point $-z$ we can use the second intersection of the line through 0 and z with the circle with center 0 and radius $\|z\|$.2.1

Proof. Define $l = \{0, z\}$ and $c = \{0,\ \text{dist}\ (0, z)\}$.
By assumption $0, z \in M_\infty$, so $l \in \mathcal{L}(\mathcal{M}_\infty)$ and $c \in \mathcal{C}(\mathcal{M}_\infty)$.
Claim 1: $-z$ is in l.

Proof. By the definition of $l := \{\lambda 0 + (1-\lambda)z \mid \lambda \in \mathbb{R}\}$ with $\lambda = 2$ we get $2 \cdot 0 + (1-2)z = -z$. □

Claim 2: $-z$ is in c.

Proof. Unfolding the definition of $c := \{x \in \mathbb{C} \mid \|x - 0\| = \text{dist}\ (0\ z)\}$. By the definition of the distance we get $\|0 - (-z)\| = \text{dist}\ (0\ z)$. □

By claim 1 and 2 we get that $-z \in l \cap c$. Futhermore $-z$ is in M_∞, after lemma 2.28. □

Lemma 2.31 (Addition of complex numbers)**.** *For $z_1, z_2 \in M_\infty$ it follows that $z_1 + z_2 \in M_\infty$.*

This construction is taken from [6].
One can construct the point $z_1 + z_2$ by drawing a circle with center z_1 and radius $\|z_2\|$ and a circle with center z_2 and radius $\|z_1\|$ and taking the intersection of the two circles.2.2

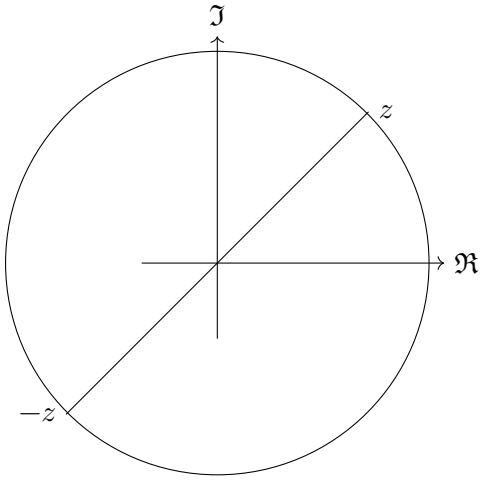

Figure 2.1: Construction of $-z$

Proof. First we have the case that $z_1 \neq z_2$.
Define $c_1 = \{z_1,\ \text{dist}\ (0\ z_2)\}$ and $c_2 = \{z_2,\ \text{dist}\ (0\ z_1)\}$.
By assumption $0, z_1, z_2 \in M_\infty$, so $c_1, c_2 \in \mathcal{C}(\mathcal{M}_\infty)$ and since $z_1 \neq z_2$ we get $c_1 \neq c_2$.
Claim 1: $z_1 + z_2$ is in c_1.

Proof. By the definition of $c_1 := \{x \in \mathbb{C} \mid \|x - z_1\| = \ \text{dist}\ (0\ z_2)\}$ and of the distance we get $\|z_1 - (z_1 + z_2)\| = \ \text{dist}\ (0\ z_2)$. □

Claim 2: $z_1 + z_2$ is in c_2.

Proof. Using that c_2 ia definded as $c_2 := \{x \in \mathbb{C} \mid \|x - z_2\| = \ \text{dist}\ (0\ z_1)\}$ and the definition of the distance we get $\|z_2 - (z_1 + z_2)\| = \ \text{dist}\ (0\ z_1)$. □

By claim 1 and 2 we get that $z_1 + z_2 \in c_1 \cap c_2$. Futhermore $z_1 + z_2$ is in M_∞, after lemma 2.29.

If we have $z_1 = z_2$ we can define $c_1 = \{z_1,\ \text{dist}\ (0\ z_1)\}$ and $l = \{0, z_1\}$ and get that $z_1 + z_2 = z_1 + z_1 \in c_1 \cap l$.

□

Corollary 2.32 (Subtraction of complex numbers)**.** *For $z_1, z_2 \in M_\infty$ it follows that $z_1 - z_2 \in M_\infty$.*

Proof. By lemma 2.30 and 2.31 we get $z_1 - z_2 = z_1 + (-z_2) \in M_\infty$. □

Corollary 2.33 (Construction of parallel lines)**.** *For $l \in \mathcal{L}(\mathcal{M}_\infty)$ and $z \in M_\infty$ it follows that $\exists l' \in \mathcal{L}(\mathcal{M}_\infty)$ with $z \in l'$ and $l \| l'$.*

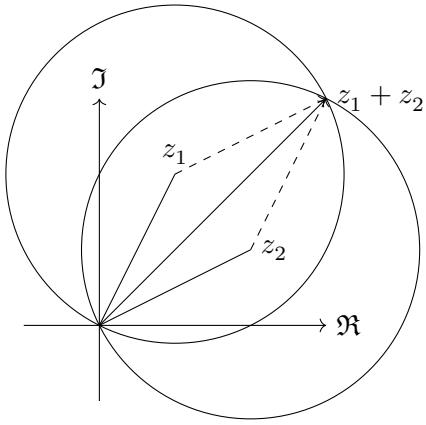

Figure 2.2: Construction of $z_1 + z_2$

Proof. Let l be a line through $x, y \in \mathcal{M}_\infty$ and $z \in \mathcal{M}_\infty$.
After corollary 2.32 we get $z - x \in \mathcal{M}_\infty$ and therfore $z - x + y \in \mathcal{M}_\infty$2.31.
Define $l' = \{z, z - x + y\}$, then $l' \in \mathcal{L}(\mathcal{M}_\infty)$ and since a line is defined by two points and we moved them the same distance $(z - x)$ l' is parallel to l.2.12 □

Lemma 2.34 (Complex conjugation)**.** *For $z \in M_\infty$ it follows that $\overline{z} \in M_\infty$.*

This construction is taken from [6].
Draw two circles one with center 0 and radius $\|z\|$ and a second with center 1 and radius $\|z - 1\|$ and take the intersection of the two circles.2.3

Proof. Define $c_1 = \{0,\ \text{dist}\ (0, z)\}$ and $c_2 = \{1,\ \text{dist}\ (1, z)\}$.
By assumption $0, 1, z \in M_\infty$, so $c_1, c_2 \in \mathcal{C}(\mathcal{M}_\infty)$.
Claim 1: $\overline{z}$ is in c_1.

Proof. The definition of c_1 can be written in the following form:

$$\{x \in \mathbb{C} \mid \|x - 0\| = \ \text{dist}\ (0\ z)\}.$$

Using the definition of the distance, we obtain the following result:

$$\|0 - \overline{z}\| = \|\overline{z}\| = \|z\| = \ \text{dist}\ (0\ z).$$

□

Claim 2: $\overline{z}$ is in c_2.

Proof. From the definition of $c_2 := \{x \in \mathbb{C} \mid \|x - 1\| = \ \text{dist}\ (1\ z)\}$ and the definition of the distance, we can derive the following:

$$\|1 - \overline{z}\| = \|\overline{z} - 1\| = \sqrt{(\mathfrak{R}(\overline{z}) - 1)^2 + \mathfrak{I}(\overline{z})^2} = \sqrt{(\mathfrak{R}(z) - 1)^2 + \mathfrak{I}(z)^2} = \|z - 1\| = \ \text{dist}\ (1\ z).$$

□

By claim 1 and 2 we get that $\overline{z} \in c_1 \cap c_2$. Futhermore $\overline{z}$ is in M_∞, after lemma 2.29. □

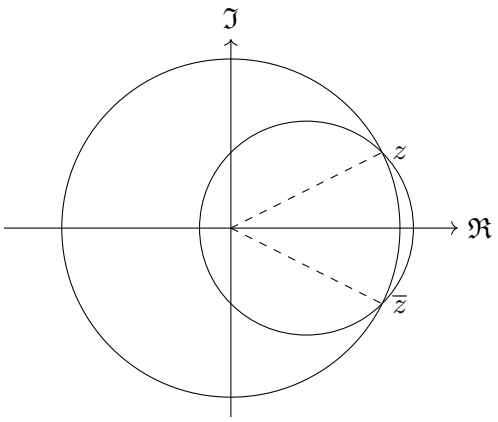

Figure 2.3: Construction of $\overline{z}$

Lemma 2.35 (Construction $\imath r \in \mathcal{M}_\infty$)**.** *For $r \in \mathbb{R} \cap M_\infty$ it follows that $\imath \cdot r \in M_\infty$.*

The first step is to construct the imaginary axis, which is achieved by drawing a line, designated as l, that passes through two circles with centres at -1 and 1 and radii of 2. The second step is to construct the point, designated as $\imath r$, which is achieved by drawing a circle with a centre at 0 and a radius of r, and taking the intersection with the imaginary axis. (Fig2.4)

Proof. First we construct the imaginary axis. Define $c_1 = \{-1, 2\}$ and $c_2 = \{1, 2\}$.
Claim 1: $c_1, c_2 \in \mathcal{C}(\mathcal{M}_\infty)$

Proof. By assumption and lemma 2.30 we get $-1, 1 \in M_\infty$. Using dist $(-11) = 2$ we get $c_1, c_2 \in \mathcal{C}(\mathcal{M}_\infty)$, by the definition of the circle. □

Claim 2: $\imath\sqrt{3}$ and $-\imath\sqrt{3}$ are in $c_1 \cap c_2$.

Proof. Unfolding the definition of $c_1 := \{x \in \mathbb{C} \mid \|x + 1\| = 2\}$ and $c_2 := \{x \in \mathbb{C} \mid \|x - 1\| = 2\}$. By the definition of the distance we get $\| - \imath\sqrt{3} + 1\| = \sqrt{1+3} = 2$ and $\|\imath\sqrt{3} - 1\| = \sqrt{1+3} = 2$. □

Now we define $l = \{\imath\sqrt{3}, -\imath\sqrt{3}\}$.
Claim 3: $l \in \mathcal{L}(\mathcal{M}_\infty)$

Proof. By claim 2 and 2.29 we get $\imath\sqrt{3}, -\imath\sqrt{3} \in M_\infty$, so $l \in \mathcal{L}(\mathcal{M}_\infty)$. □

To get $\imath r$ we define $c = \{0, |r|\}$.
Claim 4: $\imath r$ is in $c \cap l$.

Proof. It is clear that $\imath r \in c$. Now using the definition of l and $\lambda = \frac{r}{2\sqrt{3}+\frac{1}{2}}$ we get $(\frac{r}{2\sqrt{3}+\frac{r}{2}})\imath\sqrt{3} + (1 - \frac{r}{2\sqrt{3}+\frac{r}{2}})(-\imath\sqrt{3}) = \imath r$. □

Therfore $\imath r \in M_\infty$ after lemma 2.28. □

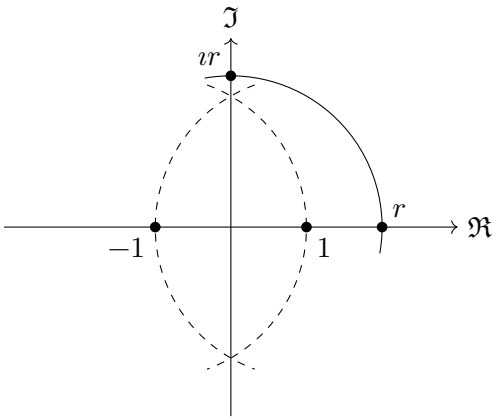

Figure 2.4: Construction of $\imath r$

Corollary 2.36 (Construction of $\imath$)**.** $\imath \in M_\infty$.

Proof. By lemma 2.35 with $r = 1$ and the definition of $\mathcal{M}$ we get $\imath \in M_\infty$. □

Lemma 2.37 (Construction of real part)**.** *For $z \in M_\infty$ it follows that $z.re \in M_\infty$.*

To get the point $z.re$ we draw a line through z and $\overline{z}$. Then $z.re$ is the intersection with the real line, defined by 0 and 1.2.5

Proof. Without loss of generality we can assume that $z \in \mathbb{C} \setminus \mathbb{R}$.
Define the lines $l = \{z, \overline{z}\}$ and $l_{\mathfrak{R}} = \{1, 0\}$.
By using Lemma 2.34, they are in $\mathcal{L}(\mathcal{M}_\infty)$.
To show that $z.re \in l \cap l_{\mathfrak{R}}$ we use $t := 1/2$ for l and $t := z.re$ for $l_{\mathfrak{R}}$. □

Lemma 2.38 (Construction of imaginary part)**.** *For $z \in M_\infty$ it follows that $z.im \in M_\infty$.*

To get the point $z.im$ we draw a line through z and $z - 1$. Now we get $\imath \cdot z.im$ by taking the intersection with the imaginary line, defined by 0 and $\imath$. To get $z.im$ draw a circle trough $\imath \cdot z.im$ and take the intersection with the real line.2.6

Proof. Define the lines $l = \{z, z - 1\}$ and $l_{\mathfrak{I}} = \{\imath, 0\}$.
Now it is analog to the proof of lemma 2.37, that $z.im \cdot \imath \in l \cap l_{\mathfrak{I}}$.

Now we can project $z.im \cdot \imath$ on the real axis by drawing a circle with center 0 and radius $\|z.im\|$ and taking the intersection with the real axis. □

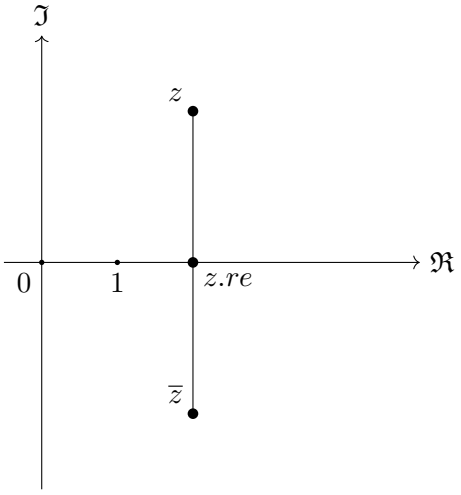

Figure 2.5: Construction of $z.re$

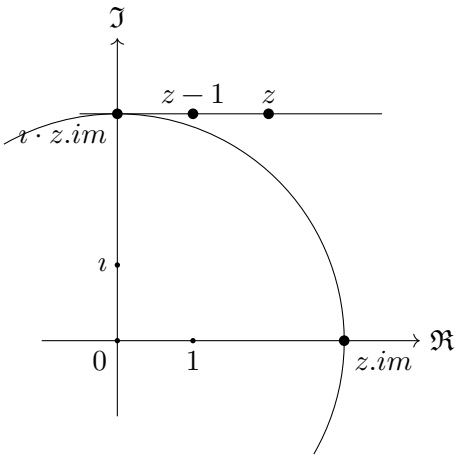

Figure 2.6: Construction of $z.im$

Corollary 2.39 ($z \in M_\infty \Rightarrow z.re, z.im \in M_\infty$)**.** *For $z \in \mathbb{C}$. z is in M_∞ if and only if $z.re, z.im \in M_\infty$.*

Proof. "⇒:" If $z \in M_\infty$ then $z.re, z.im \in M_\infty$ after lemma 2.37 and 2.38.
"⇐:" If $z.re, z.im \in M_\infty$ then $z.re + \imath z.im \in M_\infty$ after lemma 2.31 and lemma 2.35. □

Lemma 2.40 (Multiplication of positve real numbers)**.** *For $a, b \in M_\infty \cap \mathbb{R}$ it follows that $a \cdot b \in M_\infty$.*

This construction is taken from [4].
To get the point $a \cdot b$ we draw a line trough a and $\imath$ and a parallel line through $\imath b$. The intersection of the second line with the real axis is $a \cdot b$.2.7

Proof. Define the three lines $l = \{a + \imath b - \imath, \imath b\}$ and $l_{\mathfrak{R}} = \{1, 0\}$.
Claim 1: $l \in \mathcal{L}(\mathcal{M}_\infty)$

Proof. By assumption $b \in M_\infty$ so after Lemma 2.35 $\imath b \in M_\infty$. Futhermore $l_2 \in \mathcal{L}(\mathcal{M}_\infty)$ after Claim 1 and Lemma 2.33. □

Claim 2: $l_{\mathfrak{R}} \in \mathcal{L}(\mathcal{M}_\infty)$

Proof. By assumption $0, 1 \in M_\infty$, so $l_{\mathfrak{R}} \in \mathcal{L}(\mathcal{M}_\infty)$. □

To show that $a \cdot b \in M_\infty$ we need to show that $l \cap l_{\mathfrak{R}} \in M_\infty$2.26. That $ab \in l_{\mathfrak{R}} \cap l$ is clear after definition $t = ab$. For $ab \in l$ we use $t = b$ and get $t(a + \imath b - \imath) + (1 - t)\imath b \overset{t:=b}{=} ba + \imath b^2 - \imath b + \imath b - \imath b^2 = a \cdot b$. □

Remark 2.41. *This construction uses parallel lines, but it is not needed for the proof of the lemma.*

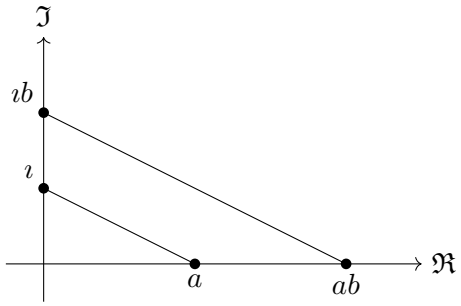

Figure 2.7: Construction of $z_1 \cdot z_2$

Corollary 2.42 (Multiplication of complex numbers)**.** *For $z_1, z_2 \in M_\infty$ it follows that $z_1 \cdot z_2$ in M_∞.*

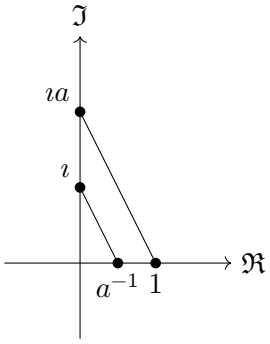

Figure 2.8: Construction of z^{-1}

Proof. Let $z_1 = a + \imath b$ and $z_2 = c + \imath d$. Then

$$z_1 \cdot z_2 = (a + \imath b) \cdot (c + \imath d) = (a \cdot c - b \cdot d) + \imath(a \cdot d + b \cdot c).$$

By combining the Lemmas 2.40, 2.31, 2.32, 2.37 and 2.38 we get that $z_1 \cdot z_2 \in M_\infty$. □

Lemma 2.43 (Invers of a pos real number)**.** *If $a \in M_\infty \cap \mathbb{R}$, then a^{-1} is in M_∞.*

This can be constructed analog to the multiplication of positve real numbers. Using the fact that $a \cdot a^{-1} = 1$. Draw a line through 1 and $\imath a$ and a parallel line through $\imath$. The intersection of the second line with the real axis is a^{-1}. (Fig. 2.8)

Proof. The proof is analogous to that of Lemma 2.40. It requires only two lines: $l = \{1 - \imath z + \imath, \imath\}$ and $l_{\mathfrak{R}} = \{1, 0\}$.
With out loss of generality we can assume that $a \neq 0$.
The fact that they are in $\mathcal{L}(\mathcal{M}_\infty)$ follows analog to the proof of Lemma 2.40.
Thus we have just to show that $z^{-1} \in l$, i.e. $\exists t : t(1 - \imath a + \imath) + (1 - t)I = a^{-1}$

$$t(1 - \imath a + \imath) + (1 - t)\imath \overset{t:=a^{-1}}{=} a^{-1} - a^{-1}\imath a + a^{-1}\imath + \imath - a^{-1}\imath = a^{-1}.$$

The rest follows analog. □

Corollary 2.44 (Inverse of a complex number)**.** *If $z \in M_\infty$, then z^{-1} is in M_∞.*

Proof. For $z \in M_\infty$ we can write $z = a + \imath b$ with $a, b \in \mathbb{R}$. Then

$$z^{-1} = \frac{1}{z} = \frac{\overline{z}}{z\overline{z}} = \frac{a - \imath b}{a^2 + b^2} = (a - \imath b) \cdot (aa + bb)^{-1}.$$

It is now possible to combine the lemmas for addition 2.31, subtraction 2.32, multiplication 2.42 and the corollary for the inverse of a positive real number 2.43 with the part concerning the existence of real and imaginary components 2.39 in order to conclude that $z^{-1} \in M_\infty$. □

Lemma 2.45 (Angle in M_∞)**.** *If $0 \neq z = r \cdot e^{\imath\alpha} \in M_\infty$, then $e^{\imath\alpha} \in M_\infty$.*

For the construction we draw a line through 0 and z and take the intersection with the unit circle. 2.9

Proof. Let l be a line through 0 and z and c be the unit circle. Then $l \cap c = \{e^{\imath\alpha}\}$. The rest follows from the construction of the intersection of a line and a circle2.29. □

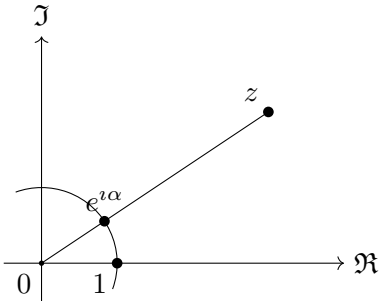

Figure 2.9: Construction of $e^{\imath\alpha}$

Corollary 2.46 (Midpoint in M_∞)**.** *If $z_1, z_2 \in M_\infty$, then $\frac{z_1+z_2}{2} \in M_\infty$.*

Proof. Combining the lemmas for addition2.31, multiplication2.42 and the invers of a complex number2.44 we get that $\frac{z_1+z_2}{1+1} \in M_\infty$. □

Lemma 2.47 (Halving of an angle)**.** *For $\alpha \in [0, 2\pi)$, if $e^{\imath\alpha} \in M_\infty$, then $e^{\imath\frac{\alpha}{2}} \in M_\infty$.*

Proof. For $\alpha \neq 0 \neq \pi$ we take the intersection of the unit circle with the line through 0 and and the mipiont of $e^{\imath\alpha}$ and 1.

For $\alpha = 0$ we get $e^{\imath\frac{\alpha}{2}} = 1$ and for $\alpha = \pi$ we get $e^{\imath\frac{\alpha}{2}} = \imath$.

□

Lemma 2.48 (Construction of radius)**.** *If $z = r \cdot e^{\imath\alpha} \in M_\infty$, then $r \in M_\infty$.*

Remark 2.49. *The radius is the distance from 0 to z, which is the same as $\|z\|$.*

We get the radius by taking the intersection of the real axis with a circle in zero with radius dist $(0, z)$. 2.10

Proof. We use the fact that $r = \|z\| = \sqrt{\mathfrak{R}(z)^2 + \mathfrak{I}(z)^2}$. Since we have spilt r in already constructed parts, we get that $r \in M_\infty$. □

Lemma 2.50 (Root of pos real number)**.** *If $r \in M_\infty \cap \mathbb{R}_{\geq 0}$, then $\sqrt{r}$ is in M_∞.*

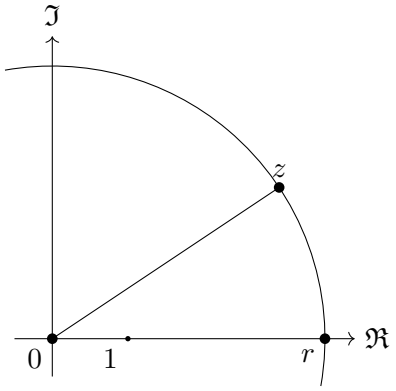

Figure 2.10: Construction of $r = \|z\|$

This construction is taken from [6].
Draw a circle trough 0 and r and a line through 1 parallel to the imaginary axis. Project the intersection to the real axis, using a circle with center 0 and you get $\sqrt{r}$. (Fig. 2.11)

Proof. Without loss of generality we can assume that $r \geq 1$. Otherwise we can use the fact that $\sqrt{r} = \frac{1}{\sqrt{r^{-1}}}$. The initial step is to define the following lines and circles:

$$l_1 := \{z_1 := 1; z_2 := \imath + 1\}$$

$$l_{\mathfrak{R}} := \{z_1 := 0; z_2 := 1\}$$

$$c_1 := \{\text{center} := \tfrac{r}{2}; \text{radius} := \text{ dist } (0, \tfrac{r}{2})\}$$

$$c_2 := \{\text{center} := 0; \text{radius} := \text{ dist } (0, \sqrt{r})\}$$

It can be observed that both l_1 and $l_{\mathfrak{R}}$ are elements of $L(M)$, and that c_1 is an element of $C(M)$. Furthermore, it can be demonstrated that the $\sqrt{r}$ is an element of $l_{\mathfrak{R}} \cap c_2$. Consequently, the only remaining step is to show that c_2 is an element of $C(M)$, which is equivalent to proving that there exists a z in M_∞ that is also an element of c_2. This is possible since 0 is an element of M_∞.
Claim: There exists a $z \in l_1 \cap c_1$, such that $z \in c_2$.

Proof. In accordance with the theorem of Pythagoras, it can be demonstrated that$z = 1 \pm \imath\sqrt{r-1}$. A further application of the Pythagorean theorem yields the following result:

$$\text{dist } (0, z) \overset{z=1+\imath\sqrt{r-1}}{=} \sqrt{1^2 + (\sqrt{r-1})^2} = \sqrt{1 + r - 1} = \sqrt{r} = \text{ dist } (0, \sqrt{r}).$$

□

Therefore, it can be concluded that $\sqrt{r}$ is also constructible.

□

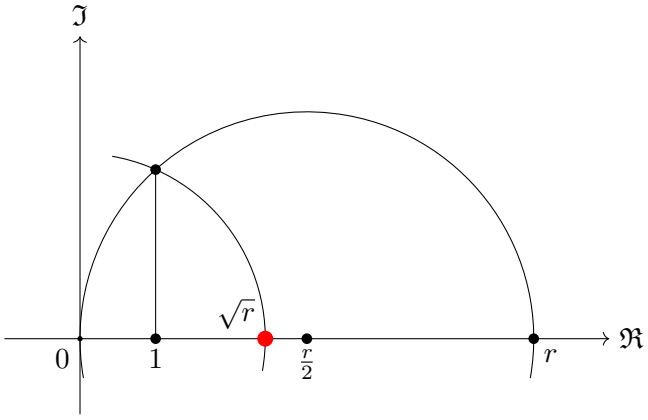

Figure 2.11: Construction of $\sqrt{r}$

Corollary 2.51 (Square root of a complexnumber)**.** *If $z \in M_\infty$, then $\sqrt{z}$ is in M_∞.*

Proof. $z = r \cdot e^{\imath\alpha}$ with $r \in \mathbb{R}_{\geq 0}$ and $\alpha \in \mathbb{R}$. Then $\sqrt{z} = \sqrt{r} \cdot e^{\imath\frac{\alpha}{2}}$. Now we can use Lemma 2.48 and Lemma 2.50 to get that $\sqrt{z} \in M_\infty$. For $e^{\imath\frac{\alpha}{2}}$ we can combine Lemma 2.45 and Lemma 2.47. Now we get that $\sqrt{z} \in M_\infty$, after Lemma 2.40.

□

Chapter 3

Field of constructable Numbers

This chapter develops the field structure on M_∞ and establishes a set of properties that are utilized to establish a criterion for determining the constructability of a point.

3.1 Field M_∞

In this section, we will utilise the constructed points from sectoion 2.4 in order to demonstrate that M_∞ forms a conjugate (3.11) and quartic (3.5) closed field.

Theorem 3.1. *For $M \subseteq \mathbb{C}$ with $0, 1 \in M$. M_∞ is a subfield of $\mathbb{C}$.*

Proof. To show that M_∞ is a subfield of $\mathbb{C}$ we have to show that $0, 1 \in M_\infty$ and M_∞ is closed under addition, multiplication, subtraction and division.

$0, 1$: This follows from $0, 1 \in M$ and Lemma 2.22.

$+$: For $z_1, z_2 \in M_\infty$ we can construct $z_1 + z_2 \in M_\infty$. 2.31

$*$: For $z_1, z_2 \in M_\infty$ we can construct $z_1 \cdot z_2 \in M_\infty$. 2.42

$-$: For $z \in M_\infty$ we can construct $-z \in M_\infty$. 2.30

$^{-1}$: For $z \in M_\infty$ with $z \neq 0$ we can construct $z^{-1} \in M_\infty$. 2.44

□

Remark 3.2. *To prove that M_∞ is a subfield of $\mathbb{C}$ in Lean we have to create a new instance with carrier M_∞.*

Remark 3.3. *Since M_∞ is a subfield of $\mathbb{C}$, M_∞ is a field which is automatically proved in Lean, by* `infer_instance`.

Lemma 3.4. *For $M \subseteq \mathbb{C}$ with $0, 1 \in M$ it holds:*

(i) $\imath \in M_\infty$.

(ii) For $z = x + \imath y \in \mathbb{C}$ the following are equivalent:

1. $z \in M_\infty$.
2. $x, y \in M_\infty$.
3. $x, \imath y \in M_\infty$.

(iii) For $0 \neq z = r\exp(\imath\alpha) \in \mathbb{C}$ the following are equivalent:

1. $z \in M_\infty$.
2. $r, \exp(\imath\alpha) \in M_\infty$.

Proof. This lemma is a direct consequence of section 2.4.

(i): We can apply construction 2.36

(ii): We can apply construction 2.39 and 2.36.

(iii): We can apply construction 2.48 and 2.45.

□

quadratic closed

Definition 3.5 (quadratic closed field)**.** *A field F is called* quadratic closed *if for all $x \in F$ there is a $y \in F$ such that $y^2 = x$.*

Remark 3.6. *An equivalent definition is that F is quadratic closed if $F = \{a^2 \mid a \in F\}$.*

Lemma 3.7. *For $M \subseteq \mathbb{C}$ with $0, 1 \in M$, M_∞ is quadratic closed.*

Proof. It is established that M_∞ is a field (see remark 3.3). Furthermore, the corollary 2.51 provides a root $z^{\frac{1}{2}}$ of $z \in M_\infty$.

$$z^{\frac{1}{2}} * z^{\frac{1}{2}} = {z^{\frac{1}{2}}}^2 = z^{2\cdot\frac{1}{2}} = z.$$

Therefore M_∞ is quadratic closed. □

Conjugate closed

Definition 3.8. *For a Set $M \subset \mathbb{C}$ we define the* conjugate set *of M as*

$$Conj(M) = \{\overline{z} \mid z \in M\}$$

Lemma 3.9. *For two sets $M, N \subset \mathbb{C}$*

$$Conj(M \cup N) = Conj(M) \cup Conj(N).$$

Proof. For $z \in Conj(M \cup N)$ there is a $w \in M \cup N$ such that $\overline{w} = z$, therefore $z = \overline{w} \in Conj(M) \cup Conj(N)$. The other direction is analog. □

Lemma 3.10. *For a set $M \subset \mathbb{C}$ it holds that $Conj(Conj(M)) = M$.*

Proof.

$$Conj(Conj(M)) = Conj(\{\overline{z} \mid z \in M\}) = \{\overline{\overline{z}} \mid z \in M\} = \{z \mid z \in M\} = M.$$

□

Definition 3.11. *We call a subset of* $\mathbb{C}$ conjugate closed *if $M = Conj(M)$.*

Lemma 3.12. *M_∞ is conjugate closed.*

Proof. We can apply construction 2.34 and the fact that $\overline{\overline{z}} = z$ for all $z \in \mathbb{C}$. □

Lemma 3.13. *For $M \subseteq \mathbb{C}$ $M \cup Conj(M)$ is conjugate closed.*

Proof. We can apply Lemma 3.9 and 3.10.

$$Conj(M \cup Conj(M)) = Conj(M) \cup Conj(Conj(M)) = M \cup Conj(M).$$

□

Lemma 3.14. *The set of rational numbers is conjugate closed.*

Proof. For every $r \in \mathbb{Q}$ we have $\overline{r} = r$. □

Lemma 3.15. *For $M, N \subseteq \mathbb{C}$ with $M \subseteq N$ it holds that $Conj(M) \subseteq Conj(N)$.*

Proof. For $z \in Conj(M)$ there is a $w \in M$ such that $\overline{w} = z$ and since $M \subseteq N$ we have $w \in N$ and therefore $z \in Conj(N)$. □

Lemma 3.16. *For a subfield F of $\mathbb{C}$ the conjugate set $Conj(F)$ is a subfield of $\mathbb{C}$.*

Proof. We have to show that $0, 1 \in Conj(F)$ and $Conj(F)$ is closed under addition, multiplication, negation and inversion.

$0, 1$: Since $0, 1 \in F$ and $\overline{0} = 0, \overline{1} = 1$ we have $0, 1 \in Conj(F)$.

$+$: For $z_1, z_2 \in F$ we have $\overline{z_1 + z_2} = \mathfrak{R}(z_1 + z_2) - \imath \cdot \mathfrak{I}(z_1 + z_2) = \mathfrak{R}(z_1) + \mathfrak{R}(z_2) - \imath \cdot (\mathfrak{I}(z_1) + \mathfrak{I}(z_2)) = \overline{z_1} + \overline{z_2}$. Therefore $Conj(F)$ is closed under addition.

$-$: For $z \in F$ we have $\overline{-z} = \mathfrak{R}(-z) - \imath \cdot \mathfrak{I}(-z) = -(\mathfrak{R}(z) - \imath \cdot (\mathfrak{I}(z))) = -\overline{z}$. Therefore $Conj(F)$ is closed under negation.

$*$: Since $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$ we have $Conj(F)$ is closed under multiplication.

$^{-1}$: Since $\overline{z^{-1}} = \overline{z}^{-1}$ we have $Conj(F)$ is closed under inversion.

□

Lemma 3.17. *Let L be a subfield of $\mathbb{C}$, with $L = conj(L)$. For all $z = x + \imath y \in L$ we have $x, \imath y \in L$.*

Proof. Let $z = x + \imath y \in L$. Since L is conjugate closed we know that $\overline{z} = x - \imath y \in L$. This implies

$$\frac{z + \overline{z}}{2} = x \in L$$

and therefore also $\imath y = z - x \in L$. □

Lemma 3.18. *Let L be a subfield of $\mathbb{C}$, with $L = conj(L)$, and $z_1, z_2 \in L$. For $r := \|z_1 - z_2\|$ we get that $r^2 \in L$.*

Proof. For $z_1 = x_1 + \imath y_1$ and $z_2 = x_2 + \imath y_2$ we have

$$r = \|z_1 - z_2\| = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$$

and therefore

$$r^2 = (x_1 - x_2)^2 + (y_1 - y_2)^2$$

After applying Lemma 3.17 we get $r^2 \in L$. □

Lemma 3.19. *Let L be a subfield of $\mathbb{C}$, with $L = conj(L)$. For $i = 1, 2, 3, 4$ let $z_i = x_i + \imath y_i \in L$ with $z_1 \neq z_2$ and $z_3 \neq z_4$. Define*

$$G_1 := \{\lambda z_1 + (1 - \lambda) z_2 \mid \lambda \in \mathbb{R}\},$$
$$G_2 := \{\mu z_3 + (1 - \mu) z_4 \mid \mu \in \mathbb{R}\}.$$

If $G_1 \cap G_2 \neq \emptyset$ and $G_1 \neq G_2$, it is equivalent

- $z \in G_1 \cap G_2$.
- *There are $\lambda, \mu \in \mathbb{R}$ such that:*
  1. $\lambda(x_1 - x_2) + \mu(x_4 - x_3) = x_4 - x_2$
  2. $\lambda(\imath y_1 - \imath y_2) + \mu(\imath y_4 - \imath y_3) = \imath y_4 - \imath y_2$
  3. $z = \lambda z_1 + (1 - \lambda) z_2$

In this case $z \in L$.

Proof. The proof is divided into two parts. Initially, it is demonstrated that z belongs to the intersection of G_1 and G_2, if and only if there exist real numbers $\lambda, \mu \in \mathbb{R}$, such that the equations 1, 2 and 3 are satisfied. Subsequently, it follows that z is an element of L.
Equations 1 and 2 are equivalent to the following:

$$\lambda x_1 + (1 - \lambda) x_2 = \mu x_3 + (1 - \mu) x_4$$

$$\lambda y_1 + (1-\lambda)y_2 = \mu y_3 + (1-\mu)y_4$$

This is the definition of $z \in G_1 \cap G_2$, expressed in terms of its real and imaginary parts.
The third equation is equivalent to $z = \lambda z_1 + (1-\lambda)z_2$. This allows us to conclude that z belongs to G_1 at the point where G_1 and G_2 intersect. Consequently, we can assume that z belongs to the intersection of G_1 and G_2.

Now we can show that z is an element of L.
Since we know that z is equal to $\lambda z_1 + (1-\lambda)z_2$ and $z_1, z_2 \in L$ we only have to show that $\lambda \in L$. Here for we use the equations from the first part of the proof.

$$\begin{aligned} I \qquad & \lambda(x_1 - x_2) + \mu(x_4 - x_3) = x_4 - x_2 \\ II \qquad & \lambda(\imath y_1 - \imath y_2) + \mu(\imath y_4 - \imath y_3) = \imath y_4 - \imath y_2 \end{aligned}$$

Now we solve II for μ

$$\begin{aligned} & \lambda(\imath y_1 - \imath y_2) + \mu(\imath y_4 - \imath y_3) = \imath y_4 - \imath y_2 && \mid -\lambda(\imath y_1 - \imath y_2) \\ \Leftrightarrow \quad & \mu(\imath y_4 - \imath y_3) = \imath y_4 - \imath y_2 - \lambda(\imath y_1 - \imath y_2) && \mid \div \imath(y_4 - y_3) \\ \Leftrightarrow \quad & \mu = \frac{\imath y_4 - \imath y_2 - \lambda(\imath y_1 - \imath y_2)}{\imath y_4 - \imath y_3} \end{aligned}$$

Since we divided by $\imath(y_4 - y_3)$ we need to assume that $y_4 \neq y_3$, so we need to first handle the case $y_4 = y_3$.
If $y_4 = y_3$ we have $\lambda(\imath y_1 - \imath y_2) = \imath y_4 - \imath y_2$ and since $y_4 = y_3$ $y_1 \neq y_2$, because otherwise both Lines would be parallel to the real line and therefore $G_1 = G_2$ or $G_1 \cap G_2 = \emptyset$. Therefore $\lambda = \frac{\imath y_4 - \imath y_2}{\imath y_1 - \imath y_2}$. Using the fact that real part and the imaginary part times $\imath$ are in L 3.17 we have written λ as a fraction of two elements in L. It can thus be concluded that λ is in L, which implies that $z = \lambda z_1 + (1-\lambda)z_2$ is in L.

Now we insert μ in I and solve for λ.

$$\begin{aligned} & \lambda(x_1 - x_2) + \mu(x_4 - x_3) = x_4 - x_2 && \mid I \leftarrow II \\ \Leftrightarrow \quad & \lambda(x_1 - x_2) + \frac{\imath y_4 - \imath y_2 - \lambda(\imath y_1 - \imath y_2)}{\imath y_4 - \imath y_3}(x_4 - x_3) = x_4 - x_2 && \mid \cdot(\imath y_4 - \imath y_3) \\ \Leftrightarrow & \lambda(x_1 - x_2)(\imath y_4 - \imath y_3) + (\imath y_4 - \imath y_2 - \lambda(\imath y_1 - \imath y_2))(x_4 - x_3) = (x_4 - x_2)(\imath y_4 - \imath y_3) && \mid -(x_1 - x_2)(\imath y_4 - \imath y_3) \\ \Leftrightarrow \quad & \lambda((x_1 - x_2)(\imath y_4 - \imath y_3) - (\imath y_4 - \imath y_2)(x_4 - x_3)) = (x_4 - x_2)(\imath y_4 - \imath y_3) - (\imath y_4 - \imath y_2)(x_4 - x_3) && \mid \div((\imath y_4 - \imath y_3)(x_1 - x_2) - (\imath y_1 - \imath y_2)(x_4 - x_3)) \\ \Leftrightarrow \quad & \lambda = \frac{(x_4 - x_2)(\imath y_4 - \imath y_3) - (\imath y_4 - \imath y_2)(x_4 - x_3)}{(\imath y_4 - \imath y_3)(x_1 - x_2) - (\imath y_1 - \imath y_2)(x_4 - x_3)} \end{aligned}$$

We need to check that the denominator $(y_4 - y_3)(x_1 - x_2) - (y_1 - y_2)(x_4 - x_3)$ is not zero. Assume that its = then we would have $(y_4 - y_3)(x_1 - x_2) = (y_1 - y_2)(x_4 - x_3)$, which is equivalent to $\frac{y_4 - y_3}{x_4 - x_3} = \frac{y_1 - y_2}{x_1 - x_2}$. This would mean that the two lines are parallel and therefore $G_1 = G_2$ or $G_1 \cap G_2 = \emptyset$.
Thus we can assume that the denominator is not zero and therefore we can write λ as a fraction of two elements in L. Therefore λ is in L, wich implies that $z = \lambda z_1 + (1-\lambda)z_2$ is in L.

□

Lemma 3.20. *Let L be a subfield of $\mathbb{C}$, with $L = conj(L)$. For $i = 1, 2, 3$ let $z_i = x_i + \imath y_i \in L$ with $z_1 \neq z_2$, and let $r > 0$ in $\mathbb{R}$ with $r^2 \in L$. Define*

$$G := \{\lambda z_1 + (1-\lambda) z_2 \mid \lambda \in \mathbb{R}\},$$
$$C := \{z = x + \imath y \in \mathbb{C} \mid \|z - z_3\| = r\}.$$

Assume $G \cap C \neq \emptyset$; then the following are equivalent:

- $z \in G \cap C$.
- *There is a $\lambda \in \mathbb{R}$ with $\lambda^2 a + \lambda b + c = 0$ where*

$$a := (x_1 - x_2)^2 + (\imath y_1 - \imath y_2)^2,$$
$$b := 2(x_1 - x_2)(x_2 - x_3) - 2(\imath y_1 - \imath y_2)(\imath y_2 - \imath y_3),$$
$$c := (x_2 - x_3)^2 + (\imath y_2 - \imath y_3)^2 - r^2,$$

  and $z = \lambda z_1 + (1-\lambda) z_2$.

In this case $z \in L(\sqrt{w})$ for an $w \in L$.

Proof. First we have to show $z \in G \cap C$ iff and only iff there exists a $\lambda \in \mathbb{R}$ with $\lambda^2 a + \lambda b + c = 0$ and $z = \lambda z_1 + (1-\lambda) z_2$.

"$\Rightarrow$:" If z belongs to the intersection of G and C, then z satisfies the equations of C and G. Consequently

$$\begin{aligned}
& \|z - z_3\| = r && \mid 0 \leq \|\cdot\| \text{ and } 0 \leq r \\
\Leftrightarrow\ & \|z - z_3\|^2 = r^2 && \\
\Leftrightarrow\ & (x - x_3)^2 + (\imath y - \imath y_3)^2 = r^2 && \mid x = \lambda x_1 - \lambda x_2 + x_2 \text{ and} \\
& && \mid y = \lambda y_1 - \lambda y_2 + y_2 \\
\Leftrightarrow\ & (\lambda x_1 - \lambda x_2 + x_2 - x_3)^2 + && \\
& (\imath(\lambda y_1 - \lambda y_2 + y_2 - y_3))^2 = r^2 && \\
\Leftrightarrow\ & \lambda^2((x_1 - x_2)^2 + (\imath y_1 - \imath y_2)^2) + && \\
& \lambda(2(x_1 - x_2)(x_2 - x_3) - 2(\imath y_1 - \imath y_2)(\imath y_2 - \imath y_3)) + && \\
& (x_2 - x_3)^2 + (\imath y_2 - \imath y_3)^2 = r^2 &&
\end{aligned}$$

"$\Leftarrow$:" Since $z = \lambda z_1 + (1-\lambda) z_2$ we get z in G and can use the equations from the first part of the proof to show that z is in C.

Now we can show that there exists a $w \in L$ such that $z \in L(\sqrt{w})$.
Since we know that $z = \lambda z_1 + (1-\lambda) z_2$ and $z_1, z_2 \in L$ we only have to show that $\lambda \in L(\sqrt{w})$. To do this, we use the equations from the first part of the proof. Since λ is a solution of a quadratic equation we now get that λ is equal to $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$. Since $a, b, c \in L$ we get $w = b^2 - 4ac \in L$ so $\lambda \in L(\sqrt{w})$. Therefore $z = \lambda z_1 + (1-\lambda) z_2$ is in $L(\sqrt{w})$. □

Lemma 3.21. *Let L be a subfield of $\mathbb{C}$, with $L = conj(L)$. For $i = 1, 2$ let $z_i = x_i + \imath y_i \in L$ with $z_1 \neq z_2$ and let $r_i > 0$ in $\mathbb{R}$ with $r_i^2 \in L$. Define*

$$C_1 := \{z = x + \imath y \in \mathbb{C} \mid \|z - z_1\| = r_1\},$$
$$C_2 := \{z = x + \imath y \in \mathbb{C} \mid \|z - z_2\| = r_2\}.$$

Assume $C_1 \cap C_2 \neq \emptyset$ and $C_1 \neq C_2$. Then ther exists $z_1, z_2 \in L$ such that

$$G := \{\lambda z_1 + (1 - \lambda) z_2 \mid \lambda \in \mathbb{R}\}$$

is a real line, and

$$C_1 \cap C_2 = G \cap C_1 = G \cap C_2.$$

For $z \in C_1 \cap C_2$ there is a $w \in L$ such that $z \in L(\sqrt{w})$.

Proof. The initial step is to demonstrate that $z \in C_1 \cap C_2 \Leftrightarrow \exists G, z \in G \cap C_1 \wedge z \in G \cap C_2$.
"$\Rightarrow$": If z is to be in both $G \cap C_1$ and $G \cap C_2$, it must be the case that z is in both C_1 and C_2. Consequently, it is also in $C_1 \cap C_2$.
"$\Leftarrow$": We begin by establishing that $z = x + iy \in C_1 \cap C_2$ is equivalent to:

$$\|z - z_1\| = r_1 \wedge \|z - z_2\| = r_2 \Leftrightarrow 2(x_2 - x_1)x - 2(\imath y_2 - \imath y_1)\imath y = r_1^2 - r_2^2 - x_1^2 + x_2^2 + (\imath y_1)^2 - (\imath y_2)^2$$

The remaining task is to identify two elements in L that satisfy the given equation. This can be achieved by considering three cases: In the initial case, where $x_1 = x_2$, it can be demonstrated that $y_1 \neq y_2$, as otherwise it would follow that $C_1 = C_2$. Here, we can choose

$$z_1 := 1 + \imath\left(\frac{r_1^2 - r_2^2 + (\imath y_2)^2 - (\imath y_1)^2}{-2(y_2 - y_1)}\right)$$
$$z_2 := 0 + \imath\left(\frac{r_1^2 - r_2^2 + (\imath y_2)^2 - (\imath y_1)^2}{-2(y_2 - y_1)}\right)$$

In the second case we have $y_1 = y_2$ and $x_1 \neq x_2$. Here we can choose [1]

$$z_1 := \left(\frac{r_1^2 - r_2^2 + x_2^2 - x_1^2}{2(x_2 - x_1)}\right) + \imath y_1$$
$$z_2 := \left(\frac{r_1^2 - r_2^2 + x_2^2 - x_1^2}{2(x_2 - x_1)}\right) - \imath y_1$$

[1] During the process of formalising this proof, it became evident that for $y_1 = y_2 = 0$ and $L \subseteq \mathbb{R}$, there does not exist a line G with the property that $G \cap C_1 = G \cap C_2 = C_1 \cap C_2$. This error can also be found in the source [6] and was noticed too late, so it could not be corrected in time. The existence of an w such that $z \in L(\sqrt{w})$ is still correct and is the result we are interested in.

For $x_1 \neq x_2$ and $y_1 \neq y_2$ chose

$$z_1 := (\frac{r_1^2 - r_2^2 + x_2^2 - x_1^2 + (\imath y_2)^2 - (\imath y_1)^2 + 2(\imath(y_2) - (\imath y_1))(\imath y_1)}{2(x_2 - x_1)}) + \imath y_1$$
$$z_2 := (\frac{r_1^2 - r_2^2 + x_2^2 - x_1^2 + (\imath y_2)^2 - (\imath y_1)^2 + 2(\imath(y_2) - (\imath y_1))(\imath y_2)}{2(x_2 - x_1)}) + \imath y_2$$

Since the points z_1 and z_2 lie in L, we can conclude that the line G lies in the set of lines of L. This allows us to apply the results stated in lemma 3.20 to obtain w, with the result that z is contained within the set $L(w)$. □

3.2 The Field $\mathcal{K}_0$

This section develops a conjugation-closed field that depends on the set $\mathcal{M}$.

Definition 3.22. *Let $(M) \subseteq \mathbb{C}$ with $0, 1 \in \mathcal{M}$. Define:*

$$K_0 := \mathbb{Q}(\mathcal{M} \cup Conj(\mathcal{M}))$$

Lemma 3.23. *Let K be an conjugation closed intermediate field of $\mathbb{Q}$ and $\mathbb{C}$ and $M \subset \mathbb{C}$ be a subset with $M = conj(M)$. Then $K(M)$ is conjugate closed.*

Proof. In reference 3.16, it was demonstrated that for a field F, the field of complex numbers, $Conj(F)$ is a field. It can thus be concluded that $Conj(K(M))$ is also a field. As both K and M are subsets of $K(M)$, it can be inferred from lemma 3.15 that $Conj(K) \overset{ConjClosed}{=} K$ and $Conj(M) \overset{ConjClosed}{=} M$ are subsets of $Conj(K(M))$. As $K(M)$ is the smallest subfield of $\mathbb{C}$ that includes K and M, it can be concluded that

$$K(M) \subseteq Conj(K(M)).$$

Furthermore, if we apply $Conj$ to both sides and again infer 3.15, we obtain

$$Conj(K(M)) \subseteq Conj(Conj(K(M))) = K(M),$$

which leads to the conclusion that $Conj(K(M)) = K(M)$. □

Corollary 3.24. *For $M \subseteq \mathbb{C}$ with $0, 1 \in M$, K_0 is conjugate closed.*

Proof. By employing the preceding lemma, it is sufficient to demonstrate that $\mathbb{Q}$ and $M \cup Conj(M)$ are conjugate closed, which can be inferred from 3.14 and 3.13 □

Lemma 3.25. *For $M \subseteq \mathbb{C}$ with $0, 1 \in M$ it holds that $K_0 \subseteq M_\infty$.*

Proof. From the definition of $K_0 := \mathbb{Q}(M \cup Conj(M))$, it can be seen that this is the smallest subfield of $\mathbb{C}$ containing both Q and $M \cup Conj(M)$. Consequently, it is sufficient to demonstrate that both $\mathbb{Q}$ and $M \cup Conj(M)$ are contained within M_∞. Since $\mathbb{Q}$ is contained in every subfield of $\mathbb{C}$, it is therefore also contained in M_∞. Furthermore, since M is contained in M_∞ (see 2.22) and M is conjugate closed (3.12), we can conclude that $M \cup Conj(M) \subseteq \mathbb{Q}$. □

3.3 Classification of Constructable Numbers

The following section will demonstrate that for an element to be constructible, the degree over K_0 must be equal to 2^m for some natural number m.

Lemma 3.26. *Let K, L be subfield of $\mathbb{C}$, with $K \leq L$. Then $[L : K] = 2$ is equivalent to the existence of a $w * w \in K$ with $w \notin K$ and $L = K(w)$.*

Proof. $(ii) \implies (i)$: Let w be as in (ii).Then $\sqrt{w}$ is a root of $X^2 - w \in K[X]$. Since $\sqrt{w} \notin K$ this polynomial is irreducible in $K[X]$. Therefore $[L : K] = 2$.
$(i) \implies (ii)$: Let $[L : K] = 2$ and $\alpha \in L \setminus K$. Then $K(\alpha) = L$ and

$$\mu_{\alpha,K} = X^2 + bX + c \quad b, c \in K$$

This implies

$$\alpha = -\frac{b}{2} \pm \sqrt{\frac{b^2}{4} - c}$$

Now let $w := \frac{b^2}{4} - c \in K$ then we get $L = K(\alpha) = K(\sqrt{w})$. □

Lemma 3.27. *For $z \in \mathbb{C}$ there exists an $n \geq 0$ and a chain*

$$K_0 = L_1 \subset L_2 \subset ... \subset L_n \subset \mathbb{C}$$

of subfields of $\mathbb{C}$ such that $z \in L_n$ and $[L_{i+1} : L_i] = 2$ for $i = 0, ..., n-1$. This is equivalent to:
There is an intermediate field L of $\mathbb{C}/K_0$ with $z \in L$, so that L arises from K_0 by a finite sequence of adjunctions of square roots.

Proof. "⇒:" Let n be the smallest natural number such that there exists a chain of subfields $L_1 \subset L_2 \subset ... \subset L_n$ with $z \in L_n$ and $[L_{i+1} : L_i] = 2$ for $i = 0, ..., n-1$. Now lemma 3.26 gives us that there exists a $w \in L_{n-1}$ such that L_n arises from L_{n-1} by adjoining $\sqrt{w}$.
"⇐:" Let L be an intermediate field of $\mathbb{C}/K_0$ with $z \in L$ and L arises from K_0 by a finte sequence of adjunctions of square roots. Then there exists a chain of subfields $L_1 \subset L_2 \subset ... \subset L_n$ with $z \in L_n$ and $L_{i+1} := L_i(\sqrt{w_i})$ for $i = 0, ..., n-1$. □

Lemma 3.28. *For M_n exists a chain of intermediate fields $K_0 \leq K_1 \leq ... \leq K_n$ such that $M_i \subset K_i$ and $K_i := K_{i-1}(X_i)$ for a set of square roots X_i of elements of K_{i-1}.*

Proof. Induction over n

- Base case $n = 1$:
  $K_0 \leq K_0$ and K_0 is conjugation closed 3.24.
- induction hypothesis:
  Assume that for n there is a chain of conjugation closed intermediate fields $K_0 \leq K_1 \leq ... \leq K_n$ such that $M_i \subset K_i$ and $K_i := K_{i-1}(X_i)$ for a set of square roots X_i of elements of K_{i-1}.

- Inductive step $n \to n+1$:
  For $z \in M_{n+1}$ there are four cases:

$z \in M_n$: By the induction hypothesis $z \in K_n$ and K_n is conjugation closed and arises from K_0 by a sequence of adjunctinos of square roots.

$z \in ILL(M_n)$: By the induction hypothesis $z \in ILL(K_n)$ and using 3.19 we get that $z \in K_n$.

$z \in ILC(M_n)$: By the induction hypothesis $z \in ILC(K_n)$ and using 3.20 there is a $w \in K_n$ such that $z \in K_n(\sqrt{w})$ insert $\sqrt{w}, \overline{\sqrt{w}}$ to X_n.

$z \in ICC(M_n)$: By the induction hypothesis $z \in ICC(K_n)$ and using 3.21 there is a $w \in K_n$ such that $z \in K_n(\sqrt{w})$ insert $\sqrt{w}, \overline{\sqrt{w}}$ to X_n.

□

Theorem 3.29 (constructable iff chain dergee2)**.** *For $z \in \mathbb{C}$, $z \in M_\infty$ is equivalent to:*
There is a $0 \leq n$ and a chain

$$K_0 = L_1 \subset L_2 \subset ... \subset L_n \subset \mathbb{C}$$

of subfields of $\mathbb{C}$ such that $z \in L_n$ and

$$[L_{i+1} : L_i] = 2 \quad for \quad i = 0, ..., n-1.$$

Proof. "⇐:" It can be shown by induction that L_n is contained within M_∞. Therefore, it can be inferred that z is also contained within M_∞.

- Base case $n = 1$:
  $L_1 = K_0 \subseteq M_\infty$ 3.25.

- induction hypothesis:
  Assume that for n: $\forall i < n : L_i \leq L_{i+1} \wedge [L_{i+1} : L_i] = 2$ implies $L_n \subseteq M_\infty$.

- Inductive step $n \to n+1$:
  Given that $[L_{n+1} : L_n] = 2$, it follows from the conclusions of Lemma 3.26 that there exists a $w \in L_n$ with the property that $\sqrt{w} \notin L_n$ and $L_{n+1} = L_n(w)$. By the induction hypothesis, it can be inferred that $L_n \subseteq M_\infty$. Since $w \in L_n \subseteq M_\infty$ and M_∞ is quadratic closed (3.7) $L_n(w) = L_{n+1} \subseteq M_\infty$.

"⇒:" There exists a n such that $z \in M_n$, and we know that there exists a K_n with $M_n \subseteq K_n$ which is derived from K_0 by successive adjoing square roots 3.28. We can conclude that there is a K, which is derived from K_0 by successive adjoining square roots, and that $z \in K$. Since M_i is finite, we get that we adjoin finitely many square roots and so we evoke 3.27.

□

Lemma 3.30. *For $z \in \mathbb{C}$, $z \in M_\infty$ implies there exists a m such that $[z : K_0] = 2^m$.*

Proof. By Theorem 3.29, it can be inferred that there exists a chain of subfields, $K_0 = L_1 \subset L_2 \subset \cdots \subset L_n \subset \mathbb{C}$, with $z \in L_n$ and $[L_i : L_{i+1}] = 2$ for $i = 0, 1, \ldots, n-1$. Moreover, the multiplicativity formula for degrees indicates that the degree of the extension $[L_n : K_0]$ is equal to the product of the degrees of the extensions $[L_n : L_{n-1}] \cdot [L_{n-1} : L_{n-2}] \cdot \ldots [L_2 : L_1]$. Thus, we have that $[L_n : K_0] = 2^n$. The fact that $z \in L_n$ implies that $K_0(z) \subseteq L_n$. It thus follows that the index of the field extension $[L_n : K_0] = [L_n : K_0(z)] \cdot [K_0(z) : K_0]$, which implies that $[K_0(z) : K_0]$ is a divisor of 2^n. □

Corollary 3.31. *For $z \in \mathbb{C}$, if there is no m such that $[z : K_0] = 2^m$ then $z \notin M_\infty$.*

Proof. Contraposition of Lemma 3.30. □

Corollary 3.32. *For $z \in \mathbb{C}$, $z \in M_\infty$ with $[K_0 : \mathbb{Q}] = 2^n$, if there is no m such that $[z : \mathbb{Q}] = 2^m$ then $z \notin M_\infty$.*

Proof. A combination of the multiplicativity formula for degrees and corollary 3.31. □

Chapter 4

Ancient Construction Problems

This chapter will employ the results to demonstrate the impossibility of trisecting the angle and doubling the cube. This formalisation is based on the work conducted during my project in Bonn during the Lean Course WiSe 23/24: `https://github.com/Louis-Le-Grand/LeanCourse23Fork/tree/master/LeanCourse/Project`

4.1 Doubling the cube

The doubling of the cube, also known as the Delian problem, represents an ancient geometric problem. The objective is to construct the edge of a second cube whose volume is double that of the first, using only a ruler and compass, given the edge of a cube. The construction of a second cube with double the volume of the original cube begins with a cube of volume a^3, where a is the length of an edge. Thus, a cube with double the volume $(2 \cdot a^3)$ has an edge length of the cube root of two times the length of the original edge. If we now take the unit cube and reduce $\mathcal{M}$, the problem is as follows:

Problem 4.1. *Let* $\mathcal{M} = \{0, 1\}$.

$$\textit{Is } \sqrt[3]{2} \overset{?}{\in} \mathcal{M}_\infty?$$

Lemma 4.2. *($\sqrt[3]{2}$ is irrational) The third root of* 2 *is an irrational number.*

Proof. The following theorem will be used without proof, as it is already available in MathLib:

Theorem*. *For any* $x \in (\mathbb{R} \setminus \mathbb{Z})$ *if there exist an* $n \in \mathbb{N}_{>0}$ *and* $m \in \mathbb{Z}$ *such that* $m = x^n$*, then* x *is rational.*

The fact that $(\sqrt[3]{2})^3 = 2$, allows us to deduce that the only remaining task is to prove that it is not an integer. This can be observed trough two relations.

$$2^{\frac{1}{3}} < 2 \tag{4.1}$$

$$2^{\frac{1}{3}} > 1 \tag{4.2}$$

□

Lemma 4.3. *$P := X^3 - 2$ is irreducible over $\mathbb{Q}$.*

Proof. Since $\mathbb{Q}$ is *a* subfield of $\mathbb{C}[X]$, we know that

$$X^3 - 2 = (X - \sqrt[3]{2})(X - \zeta_3 \sqrt[3]{2})(X - \zeta_3^2 \sqrt[3]{2})$$

Suppose P is reducible, then

$$X^3 - 2 = (X - a)(X^2 + bX + c), \text{ with } a, b, c \in \mathbb{Q}$$

In particular it has a zero in $\mathbb{Q}$, so there is a rational number a such that $a^3 = 2$. But we know that $\zeta_3 \sqrt[3]{2}$ and $\zeta_3^2 \sqrt[3]{2}$ are not real numbers and $\sqrt[3]{2}$ is not rational 4.2. So P is irreducible over $\mathbb{Q}$. □

Theorem 4.4. *The cube can't be doubled using a compass and straightedge.*

Proof. By applying the corollary 3.31, it is sufficient to proof that no $m \in \mathbb{N}$ exists such that

$$2^m \overset{?}{=} [\sqrt[3]{2} : \mathbb{Q}(0,1)] \overset{0,1 \in \mathbb{Q}}{=} [\sqrt[3]{2} : \mathbb{Q}] = \text{degree}(\mu_{\mathbb{Q}, \sqrt[3]{2}}).$$

Since P is irreducible over $\mathbb{Q}$ **??**, monic and has $\sqrt[3]{2}$ as a zero, we know that $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. And since

$$3 \equiv_2 1 \neq 0 \equiv_2 = 2^m \qquad \forall m \in \mathbb{N}$$

we can conclude that the cube can't be doubled using a compass and straightedge. □

4.2 Trisection of an angle

The trisection of an angle with a compass and ruler can be reduced to the following problem:
Let $\mathcal{M} = \{a, b, c\}$ with a, b, c not on a line and $\alpha := \angle(b - a, c - a)$ be the resulting angle. Then α can be trisected if and only if there is a point $d \in \mathcal{M}_\infty$ such that $\angle(b-a, d-a) = \alpha/3$. The use of a normed set $\mathcal{M} = \{0, 1, e^{i\alpha}\}$ leads to the following problem:

Problem 4.5. *Let $\mathcal{M} = \{0, 1, \exp(\boldsymbol{i}\alpha)\}$.*

$$\textit{Is } \exp(\boldsymbol{i}\alpha/3) \overset{?}{\in} \mathcal{M}_\infty?$$

In this context, since the numbers zero and one are rational numbers, it can be concluded that K_0 is equal to

$$K_0 = \mathbb{Q}(\mathcal{M} \cup Conj(\mathcal{M})) = \mathbb{Q}(e^{\imath\alpha}, \overline{e^{\imath\alpha}}).$$

Given the corollary reference and the fact that $e^{\imath\alpha/3}$ is a zero of $X^3 - e^{\imath\alpha} \in \mathbb{Q}(e^{\imath\alpha}, \overline{e^{\imath\alpha}})[X]$, the following is equivalent:

- $\exp(\mathbf{i}\alpha/3) \notin \mathcal{M}_\infty$
- $\text{degree}(\mu_{e^{\imath\alpha/3},K_0}) = 3$
- $X^3 - e^{\imath\alpha}$ is irreducible over $\mathbb{Q}(e^{\imath\alpha}, \overline{e^{\imath\alpha}})$

The following section will demonstrate that the angle of $\frac{\pi}{3} = 60°$ is not trisectable.

Lemma 4.6. *The degree of* $K_0 = \mathbb{Q}(e^{\imath\frac{\pi}{3}}, \overline{e^{\imath\frac{\pi}{3}}})$ *is equal to* 2.

Proof. For all real numbers α, we have that

$$\exp(\imath\alpha) = \cos(\alpha) + \imath\sin(\alpha).$$

For $\alpha = \pi/3$ we get

$$\cos(\alpha) = \frac{1}{2} \qquad \text{and} \qquad \sin(\alpha) = \frac{\sqrt{3}}{2}$$

Therefore $\mathbb{Q}(e^{\imath\frac{\pi}{3}}, \overline{e^{\imath\frac{\pi}{3}}})$ is in $\mathbb{Q}(\imath\sqrt{3})$. And since $\imath\sqrt{3}$ is a zero of $X^2 + 3$, we know that the degree of K_0 less then 2. To show that the degree is not 1, we apply the fact that $\imath\sqrt{3} \notin \mathbb{Q}$. □

Lemma 4.7. *The angle* $\pi/3 = 60°$ *can't be trisected using a compass and straightedge.*

Proof. By utilising the aforementioned lemma 4.6 to apply the corresponding corollary 3.32, we can narrow our focus to the degree over $\mathbb{Q}$. Now we use the fact that if $x \in \mathcal{M}_\infty$, then $x.real, x.imag \in \mathcal{M}_\infty$ 3.4. Thus we focus on $\cos(\alpha/3)$, which the real part $e^{\imath\frac{\pi}{3}}$ and a zero of

$$f \coloneqq 8X^3 - 6X - 1 \in \mathbb{Q}[X]$$

Suppose f is reducible over $\mathbb{Q}$, then f has a rational zero a, since f is of degree 3. According to the rational root theorem, a root rational root of f is of the form $\pm\frac{p}{q}$ with p a factor of the constant term and q a factor of the leading coefficient. So the only possible rational zeros of f are

$$\{\pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm\frac{1}{8}\}.$$

One can check that none of these numbers are a zero of f. So f is irreducible over $\mathbb{Q}$ and $\cos(\alpha/3) \notin \mathcal{M}_\infty$. Therefore

$$\exp(\mathbf{i}\alpha/3) \notin \mathcal{M}_\infty$$

So the angle $\pi/3 = 60°$ can't be trisected using a compass and straightedge. □

Theorem 4.8. *A general angle can't be trisected using a compass and straightedge.*

Proof. Employ the previous lemma with the angle $\pi/3$. □

Chapter 5

A sample of Lean

The following chapter provides a concise overview of the author's experience with lean, the challenges encountered, and the author's approach to formalisation.

However, it will not explain the operational logic of lean nor serve as a guide to learning lean, as this is beyond the scope of this thesis. For those interested in learning more about lean, I recommend consulting the following resources: `https://leanprover-community.github.io/learn.html`

5.1 Blueprint

In order to structure my project, I employ the Lean Blueprint tool, created by Patrick Massot. [5] This tool generates a web version of the LaTeX file, which provides an outline of the project and facilitates the integration of code with the associated documentation. Please refer to Figure 5.1 for an example of the linking. Furthermore, it generates a dependency graph 5.1, which illustrates the extent of formalisation. The presented approach is particularly beneficial for larger-scale projects involving multiple contributors, as evidenced in Terence Tao blog post. [7]

Figure 5.1: Blueprint

- ✓ Indicates the statment is Formalised
- # Links to the proof
- Shows to the proof
- Shows dependency
- L∃∀N Links to the documentation

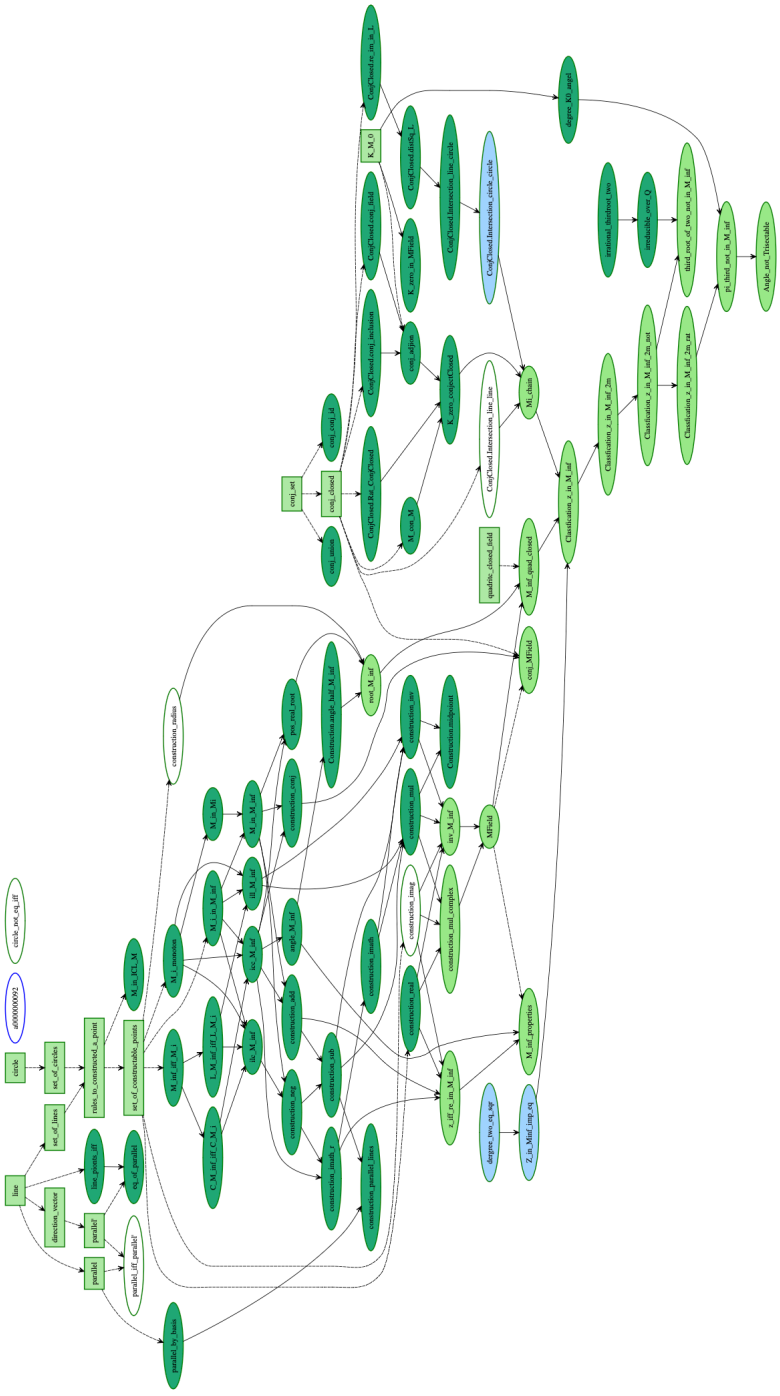

Figure 5.2: Dependency Graph

5.2 A sample of Lean code

The following is a representative sample of the Lean code, which is available in its entirety on the GitHub repository of this project. `https://github.com/Louis-Le-Grand/Formalisation-of-constructable-numbers`

I defined lines as a structure of two points z_1 and z_2. For this structure I then define points by $\{\lambda z_1 + (1-\lambda)z_2 \mid \lambda \in \mathbb{R}\}$ which are all the points the line goes through. I have omitted the condition $z_1 \neq z_2$ because in some settings a line that consists of only one point makes sense.

```
structure line where
    ( z  z :  )

def line.points (l: line) : Set  :=
    {(t :  ) * l. z + (1-t) * l. z | (t :  )}
```

To define the circles, I used c of $\mathbb{C}$ as the centre and r as the radius. For the points, I could refer to spheres already defined in Mathilb, which had the advantage that I could use existing lemmas about them.

```
structure circle where
    (c :  )
    (r :  )

def circle.points (c: circle) := Metric.sphere c.c c.r
noncomputable def circle.points' (c: circle) :=
     (c.c, c. r : EuclideanGeometry.Sphere  )
```

To prove that M_∞ is a subfile of $\mathbb{C}$, I had to define a new object of type subfile of $\mathbb{C}$, and use M_∞ as the subordinate carrier. This is because each object in Lean is a type, and you cannot switch between types.

```
noncomputable def MField (M: Set  )( h: 0   M)( h:  1 M):
        Subfield   where
    carrier := M_inf M
    zero_mem' := by exact M_M_inf M  h
    one_mem' := by exact M_M_inf M  h
    add_mem' := by apply add_M_Inf M  h
    neg_mem' := by apply z_neg_M_inf M  h
    mul_mem' := by apply mul_M_inf M  h  h
    inv_mem' := by apply inv_M_inf M  h  h
```

5.3 Conclusion

The proceeding was an account of the process by which the formalisation of "The Impossibility of Trisecting the Angle and Doubling the Cube" was reached. On the one hand, working with lean demonstrates which aspects have not yet been resolved, during the formalisation process and ensures that all outcomes will be accurate.

However, it requires a more complex proof structure than is typically required, rendering processes that are otherwise straightforward challenging to demonstrate. Consequently, this approach is inherently time-consuming. This has resulted in the following aspects not being completed in time.

In Lemma 3.21, while calculating the existence of the line through the intersection points of the two circles, it was found that for $\Im(c_1) = \Im(c_2) = 0$, the lemma is not true. Due to time limitations, these issues could not be addressed.

In the proof of Theorem 3.29 the fact that it is a finte adjunction of square roots was not proven and the equivalence of Lemma 3.27 is not formalized.

It should be noted that proof of Lemma 3.26 was never forthcoming, as there was a desire to prove the most general setting in order to contribute it to Mathlib. However, due to the limitations of time, this was not feasible.

Nonetheless, I'm glad that I could make a small contribution to the formalization of the 100 theorems in Lean.

Bibliography

[1] Paul Abad and Jack Abad. The hundred greatest theorems. URL: https://web.archive.org/web/20080105074243/http://personal.stevens.edu/~nkahl/Top100Theorems.html.

[2] Jeremy Avigad, Leonardo de Moura, Soonho Kong, and Sebastian Ullrich. Theorem proving in lean 4. URL: https://lean-lang.org/theorem_proving_in_lean4/title_page.html.

[3] Lean Community. URL: https://leanprover-community.github.io/100-missing.html.

[4] D.A. Cox. *Galois Theory*. Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. Wiley, 2012. URL: https://books.google.de/books?id=TshTYrh7MDYC.

[5] Patrick Massot, 2020. URL: https://github.com/PatrickMassot/leanblueprint.

[6] JAN SCHRÖER. Einführung in die algebra. SKRIPT, WS 22/23, BONN, 2023.

[7] Terence Tao, Nov 2023. URL: https://terrytao.wordpress.com/2023/11/18/formalizing-the-proof-of-pfr-in-lean4-using-blueprint-a-short-tour/.

[8] Freek Wiedijk. URL: https://www.cs.ru.nl/~freek/100/index.html.