Project overview

1 The TemplateExercise Problems

Doubling the cube, also known as the Delian problem, is an ancient geometric problem. Given the edge of a cube, the problem requires the construction of the edge of a second cube whose volume is double that of the first, using only a ruler and compass.
Angle trisection is the construction, using only a ruler and compass, of an angle that is one third of a given arbitrary angle.

1.1 Definitions

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 1.1. $\mathcal{G}(\mathcal{M})$ is the set of all real straight lines $\mathcal{G}$, with $|\mathcal{G} \cap \mathcal{M}| \geq 2$.
$\mathcal{C}(\mathcal{M})$ is the set of all circles in $\mathbb{C}$, with center in $\mathcal{M}$ and radius of $\mathcal{C}$ is the distence of two points in $\mathcal{M}$.

Definition 1.2. We define operation that can be used to constructed new Points.

1. $(ZL1)$ is the cut of two lines in $\mathcal{G}(\mathcal{M})$.
2. $(ZL2)$ is the cut of a line in $\mathcal{G}(\mathcal{M})$ and a circle in $\mathcal{C}(\mathcal{M})$.
3. $(ZL3)$ is the cut of two circles in $\mathcal{C}(\mathcal{M})$.

$ZL(\mathcal{M})$ is the set $\mathcal{M}$ combeined with of all points that can be constructed using the operations $(ZL1)$, $(ZL2)$ and $(ZL3)$.

Definition 1.3. We define inductively the the chain

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

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

1.2 Definitions in Lean

Definition 1.4. Let **Point** be an $z \in \mathbb{C}$. For points z_i we write x_i and y_i for $z_i = x_i + \mathbf{i}y_i$.

Definition 1.5. Let $\mathcal{G}$ be a set of Points depending on Point z_1 and z_2.

$$\mathcal{G}_{z_1,z_2} := \{\lambda z_1 + (1-\lambda)z_2 | \lambda \in \mathbb{R}\}$$

Let $\mathcal{C}$ be a set of Points depending on Point z_1 and $r := \|z_2 - z_3\|$.

$$\begin{aligned} \mathcal{C}_{z_1,r} :=& \{x + \mathbf{i}y \in \mathbb{C} | (x - x_1)^2 - (\mathbf{i}y - \mathbf{i}y_1)^2 = r^2 \ \} \\ =& \{x + \mathbf{i}y \in \mathbb{C} | (x - x_1)^2 + (y - y_1)^2 = r^2 \ \} \end{aligned}$$

Definition 1.6. The rules (ZL1), (ZL2) and (ZL3) define the Sets of Points:

1. Z_one_M $\{z \in \mathbb{C} | \exists z_1, \ldots, z_4 \in \mathcal{M} : z \in \mathcal{G}_{z_1,z_2} \cap \mathcal{G}_{z_3,z_4}$ and $z_3 \neq z_1 \neq z_4\}$
2. Z_two_M $\{z \in \mathbb{C} | \exists z_1, \ldots, z_5 \in \mathcal{M} : z \in \mathcal{G}_{z_1,z_2} \cap \mathcal{C}_{z_3,\|z_4-z_5\|}$ and $z_4 \neq z_5\}$
3. Z_three_M $\{z \in \mathbb{C} | \exists z_1, \ldots, z_6 \in \mathcal{M} : z \in \mathcal{C}_{z_1,\|z_2-z_3\|} \cap \mathcal{C}_{z_4,\|z_5-z_6\|}$ and $z_1 \neq z_4, z_2 \neq z_3, z_5 \neq z_6\}$

Therefore $\mathcal{Z}(\mathcal{M})$ is definde as $\mathcal{Z}(\mathcal{M}) := \mathcal{M} \cup$ Z_one_M $\cup$ Z_two_M $\cup$ Z_three_M.

Definition 1.7. We define inductively the the chain

$$M_I : \mathbb{N} \mapsto \mathcal{M} := \begin{cases} \mathcal{M} & \text{if } n = 0 \\ \mathcal{Z}(M_I(n-1)) & \text{if } n > 0 \end{cases}$$

And the set of all constructable points as $\mathcal{M}_\infty = \bigcup_{n \in \mathbb{N}} \mathcal{M}_n$.

1.3 Problem simplification

Let $\mathcal{M} = \{a, b\}$. Let $r := \|a - b\|$ be the distance between a and b. Then a Qube with edge r has volume r^3. There is a cube with volume $2r^3$ if and only if $\sqrt[3]{2} \in \mathcal{M}_\infty$.

Problem 1.8. Let $\mathcal{M} = \{0, 1\}$ Is $\sqrt[3]{2} \in \mathcal{M}_\infty$?

Let $\mathcal{M} = \{a, b, c\}$ with a, b, c not on a line. Let $\alpha := \angle abc$. Then α can be trisected if and only if $\exp(\mathbf{i}\alpha/3) \in \mathcal{M}_\infty$.

Problem 1.9. Let $\mathcal{M} = \{0, 1, \exp(\mathbf{i}\alpha)\}$ Is $\exp(\mathbf{i}\alpha/3) \in \mathcal{M}_\infty$?

2 Properties of the the set of constructable points

Definition 2.1. The degree of x over K is

$$[x : K] := \text{degree}(\mu_{x,K})$$

with $\mu_{x,K}$ the minimal polynomial of x over K.
The degree of L/K is the dimension of L as a K-vector space and is denoted by

$$[L : K].$$

Theorem 2.2. *Let L/K be a simple field extension with $L = K(x)$. Then*

$$[L : K] = [x : K].$$

Proof. In Mathlib: theorem IntermediateField.adjoin.finrank □

Definition 2.3. Let $(M) \subseteq \mathbb{C}$ with $0, 1 \in \mathcal{M}$

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

with $\overline{\mathcal{M}} := \{\overline{z} = x - \mathbf{i}y \mid z = x + \mathbf{i}y \in \mathcal{M}\}$.

Theorem 2.4. *Let $\mathcal{M} \subseteq \mathbb{C}$ with $0, 1 \in \mathcal{M}$ and $K_0 := \mathbb{Q}(\mathcal{M} \cup \overline{\mathcal{M}})$. Then for $z \in \mathcal{M}_\infty$ is equvalent:*

1. $z \in \mathcal{M}_\infty$

2. *There is an $n \in \mathbb{N}$ and a chain*

$$K_0 = L_0 \subset L_1 \subset \cdots \subset L_n \subset \mathbb{C}$$

of subfields of $\mathbb{C}$ such that $z \in L_n$ and $[L_i : L_{i-1}] = 2$ for $1 \leq i \leq n$

In this case $[K_0(z) : K_0] = 2^m$ for some $0 \leq m \leq n$.

Proof. TODO □

3 Doubling the cube with a compass and straightedge

The Problem of doubling the cube is equivalent to the question if $\sqrt[3]{2} \in \mathcal{M}_\infty$. Since $\mathcal{M} = \{0, 1\}$, we know that $K_0 = \mathbb{Q}$. Therfore we need examine if $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2^m$.

Theorem 3.1. *$P := X^3 - 2$ 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 Rational, 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 have shown in **??** that $\zeta_3 \sqrt[3]{2}$ and $\zeta_3^2 \sqrt[3]{2}$ are not real numbern and in **??** $\sqrt[3]{2}$ is not rational.
So P is irreducible over $\mathbb{Q}$. □

Theorem 3.2. *The cube can't be doubled using a compass and straightedge.*

Proof. We know that $K_0 = \mathbb{Q}$ and the problem is equivalent to $\sqrt[3]{2} \in \mathcal{M}_\infty$.
2.4 tells us that it is sufficient to show that $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \neq 2^m$ for some $0 \leq m$. Since $\sqrt[3]{2}$ is not a rational number, we know that $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \geq 2$. TODO
We know that $P := X^3 - 2$ is irreducible over $\mathbb{Q}$ 3.1 and $P(\sqrt[3]{2}) = 0$, therefore $P = \mu_{\sqrt[3]{2}, \mathbb{Q}}$. So with 2.2 we know $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ and $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \neq 2^m$ for some $0 \leq m$. □

3.1 Doubling the cube with a compass and straightedge in Lean

4 Angle trisection

Let $\mathcal{M} = \{0, 1, \exp(\mathbf{i}\alpha)\}$ with $\alpha \in (0, 2\pi)$. Therfore we know that

$$K_0 = \mathbb{Q}(\mathcal{M} \cup \overline{\mathcal{M}}) = \mathbb{Q}(\exp(\mathbf{i}\alpha))$$

We need to examine if $\exp(\mathbf{i}\alpha/3) \in \mathcal{M}_\infty$. Since 2.4 that for an postive answer it is nessary that $[\mathbb{Q}(\exp(\mathbf{i}\alpha/3)) : \mathbb{Q}] = 2^m$ for some $0 \leq m$.
Since $\exp(\mathbf{i}\alpha/3)$ is zero of $X^3 - \exp(\mathbf{i}\alpha)$, we know that $[\mathbb{Q}(\exp(\mathbf{i}\alpha/3)) : \mathbb{Q}] \leq 3$. Therfore it is equivalent

1. $\exp(\mathbf{i}\alpha/3) \notin \mathcal{M}_\infty$
2. $\text{degree}(\mu_{\exp(\mathbf{i}\alpha/3), \mathbb{Q}}) = 3$

3. $X^3 - \exp(\mathbf{i}\alpha/3)$ is irreducible over $\mathbb{Q}$

Lemma 4.1. *If $r \in \mathcal{M}_n$, then $\sqrt{r} \in \mathcal{M}_\infty$.*

Proof. TODO ☐

Lemma 4.2 (Rational root theorem)**.**

Theorem 4.3. *The angle $\pi/3 = 60°$ can't be trisected using a compass and straightedge.*

Proof. We know

$$\exp(\mathbf{i}x) = \cos(x) + \mathbf{i}\sin(x) \quad \forall x \in \mathbb{R}$$

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

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

Since we know that $\sqrt{r} \in \mathcal{M}_\infty$ for $r \in \mathcal{M}_n$ 4.1 we see that $\exp(\mathbf{i}\alpha) \in \mathcal{M}_\infty$ for $\mathcal{M} = \{0, 1\}$.
So we will work with $K_0 = \mathbb{Q}$.
TODO
We now $\cos(\alpha/3)$ is zero of

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

Suppose f is reducible over $\mathbb{Q}$, then f has a rational zero a. According to the rational root theorem, **??** TODO we know that every zero is in

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

Man can check that none of these numbers is a zero of f. TODO 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. ☐