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 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 1.4. *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 $\alpha := \angle(b - a, c - a)$. Then α can be trisected if and only if, there is a point $d \in \mathcal{M}_\infty$ so that $\angle(b - a, d - a) = \alpha/3$. Using a "standard" $\mathcal{M} = \{0, 1, \exp(\boldsymbol{i}\alpha)\}$ gives us the following problem.

Problem 1.5. *Let* $\mathcal{M} = \{0, 1, \exp(\boldsymbol{i}\alpha)\}$*. Is* $\exp(\boldsymbol{i}\alpha/3) \in \mathcal{M}_\infty$*?*

1.3 Properties of the the set of constructable points

Definition 1.6. 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 1.7. *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 1.8. 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 1.9. *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 $0 \leq m \leq n$.

Remark 1.10. Theorem **??** tells us that it is sufficient to show that $[K_0(z) : K_0] \neq 2^m$ for some $0 \leq m$, witch we will use to show that $\sqrt[3]{2} \notin \mathcal{M}_\infty$ and $\exp(\mathbf{i}\alpha/3) \notin \mathcal{M}_\infty$ for some α.

Proof of Theorem **??***.* TODO □

1.4 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 1.11. *$P := X^3 - 2$ 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 know that $\zeta_3 \sqrt[3]{2}$ and $\zeta_3^2 \sqrt[3]{2}$ are not real numberns and $\sqrt[3]{2}$ is not rational. So P is irreducible over $\mathbb{Q}$. □

Theorem 1.12. *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 $\sqrt[3]{2} \in \mathcal{M}_\infty$.
?? tells us that it is sufficient to show that $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \neq 2^m$ for some $0 \leq m$.
We know that $P := X^3 - 2$ is irreducible over $\mathbb{Q}$ **??** and $P(\sqrt[3]{2}) = 0$, therefore $P = \mu_{\sqrt[3]{2},\mathbb{Q}}$. So with **??** we know $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ and $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \neq 2^m$ for some $0 \leq m$. □

1.5 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 **??** 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 $\mathbb{Q}$

Theorem 1.13. *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 $r \in \mathcal{M}_n$ we see that $\exp(\mathbf{i}\alpha) \in \mathcal{M}_\infty$ for $\mathcal{M} = \{0, 1\}$.
So we will work with $K_0 = \mathbb{Q}$.
We also now that if $x \in \mathcal{M}_\infty$, then $x.real, x.imag \in \mathcal{M}_\infty$. So we focus on $\cos(\alpha/3)$, witch 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, 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 is 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. □

2 Proof in Lean

2.1 Definitions in Lean

We have priviously defined the set of constructable points over lines and circles. We will now define the set of constructable points over the complex numbers.

Definition 2.1. 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 2.2. 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 2.3. 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 2.4. 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 $\mathcal{M}_\infty = \bigcup_{n \in \mathbb{N}} \mathcal{M}_n$.

3 Conclusion on proofing in Lean

Lean is great for proving general theorems, but it is not the best tool for proving specific problems. Proving construction problems with ruler and compass often requires working with complex numbers and field extensions or explicit polynomials. These are not computable in Lean. Therefore, proving these problems in Lean is a very long process. The witch can be seen in endless lines of commented out code.
But Zulip was a great help. The community is very helpful and the response time is very short.

3.1 What would help to prove these problems in Lean

It would be helpful if polynomial and field extensions were computable in Lean. Also, it would be helpful if there were more lemmas and theorems about complex numbers, because there are few lemma witch are helpful, but are only shown for Real numbers.
Also, it would be helpful if there were Tatict for computing explicit goals, like [1].
And an overview of the existing ‘Tatitcts‘’ or somthing like ‘Tatict¿ witch shows you all the Taticts that are available and could be usful for the current goal.

3.2 What still needs to be done

Tidying up the code and making it more readable would help a lot. Also lemma and theorems that are used can be generalised and statet outside of the specific problem or proof. So that they can be reused in other proofs.
Also there are some lemmas that are not yet proven:

[1] https://leanprover.zulipchat.com/narrow/stream/113489-new-members/topic/.E2.9C.94.20Eval.20of.20polynomial/near/420729

Real Component In M Inf

If $z \in \mathcal{M}_\infty$, then $z.real \in \mathcal{M}_\infty$. Witch can be proven by using the line trough z and $\overline{z}$ and the fact and the fact that you can halve distances. Or by using $real(z) = z + \overline{z}$.

Classfication Z In M Inf

The Formalisation of the construction problems with ruler and compass is not yet complete. The proof of Theorem **??** and the underlying lemmma over $\mathcal{M}_\infty$ are still missing. Here we need to describe differnt Points as soloitions and painstakingly prove that they are not in $\mathcal{M}_\infty$.

Classfication Z In M Inf 2m

To prove that $z \in \mathcal{M}_\infty$ implies $[K_0(z) : K_0] = 2^m$ for some $0 \leq m \leq n$. We use **??**, **??** and the degreeformular for field extensions.

Pi Third Not In M Inf

To finsih the proof it is nessary to show why it is sufficient to use the polynomial $f := 8X^3 - 6X - 1$ over $\mathbb{Q}$. Witch is esay to stat by using $\exp(\mathbf{i}x) = \cos(x) + \mathbf{i}\sin(x) \quad \forall x \in \mathbb{R}$, $\cos(\pi/3) = \frac{1}{2}$, $\sin(\pi/3) = \frac{\sqrt{3}}{2}$ and the fact that $\sqrt{r} \in \mathcal{M}_\infty$ for $r \in \mathcal{M}_n$. But since you can't compute $\mathcal{K}_{\text{inf}}$ or $\mathcal{M}_{\text{inf}}$ in Lean, it is hard prove that $M_{\text{inf}} = \mathbb{Q}_{\text{inf}}$ so one can use the minimal polynomial of $\cos(\pi/3)$ over $\mathbb{Q}$.