Galois Theory - Week 5 - Degree, the Tower Law and Greek Constructions

Antonio León Villares

February 2023

Contents

Based on the notes by Tom Leinster, Chapter 5

1 Extensions as Vector Fields

1.1 Definition: Degree of an Extension

> *The **degree** of a **field extension** $M : K$ (denoted $[M : K]$) is the **dimension** of M as a **vector space** over K.*
> *(Definition 5.1.1)*

- **How can we think of M as a vector space over K?**
  - **addition** is the same as over M:
    $$m_1, m_2 \in M \ : \ m_1 + m_2 \in M$$
  - we define **scalar multiplication** via:
    $$k \in K, m \in M \ : \ k \cdot m = km \in M$$
    where we use the fact that K is a **subfield** of M
  - in a sense we are **forgetting** how to multiply elements of M together, unless they are in K
- **What intuition does the notion of degree hold about the "size" of fields?**
  - **extensions** with larger **degree** can be thought of as **bigger**
  - for instance, consider:
    $$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$
    $$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 \mid a, b, c \in \mathbb{Q}\}$$
  - we can see that:
    $$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$$
    since $\mathbb{Q}(\sqrt{2})$ has $\{1, \sqrt{2}\}$ as a basis over $\mathbb{Q}$ (clearly linearly independent, since one is rational and the other is irrational, and we only allow scalar multiplication by rationals)
  - similarly:
    $$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$$

1.1.1 Proposition: Degree 1 Iff Field Extends Itself

> *Let K be a field, and $M : K$ be an extension. Then:*
> $$[M : K] = 1 \iff M = K$$
> *(Example 5.1.3, i)*

Proof. Let $M = K$. Then certainly $\{1_M\}$ is a basis, since:

$$\forall m \in M \ : \ m = 1_M \cdot m$$

so:

$$[M : K] = 1$$

Alternatively, let $[M : K] = 1$. This means that the basis only contains a single element, which WLOG we may assume to be $\{1_M\}$. But then this implies that every element of M is $a \cdot 1_M = a$ for some $a \in K$, so $M = K$

□

1.1.2 Examples of Degrees

- every field M contains a non-zero element 1_M, which certianly must be part of a basis. Hence:

  $$\forall M : K, \ [M : K] \geq 1$$

- if $z \in \mathbb{C}$, then:

  $$\exists x, y \in \mathbb{R} \ : \ z = x + iy$$

  Hence, $\{1, i\}$ forms a basis of $\mathbb{C}$ over $\mathbb{R}$, and:

  $$[\mathbb{C} : \mathbb{R}] = 2$$

- $K(t)$ is the field of rational expressions over some field K. Clearly:

  $$1, t, t^2, \ldots$$

  are linearly independent over K, and generate each element of $K(t)$. Thus, $K(t)$ is an infinite-dimensional vector space over K, and:

  $$[K(t) : K] = \infty$$

1.2 Theorem: Algebraics/Transcendentals Define a Basis for Extensions

*Let $K(\alpha) : K$ be a **simple extension**. Then:*

1. *Let:*
   - *α be **algebraic** over K*
   - *$m \in K[t]$ be the **minimal polynomial** of α*
   - $\deg(m) = n$

   Then:

   $$1, \alpha, \ldots, \alpha^{n-1}$$

   *is a **basis** of $K(\alpha)$ over K, such that:*

   $$[K(\alpha) : K] = \deg(m) = n$$

2. *If α is **transcendental** over K, then:*

   $$1, \alpha, \alpha^2, \ldots$$

   *are **linearly independent** over K, and so:*

   $$[K(\alpha) : K] = \infty$$

(Theorem 5.1.5)

Proof.

(1)

If $\alpha \in K$, then $K(\alpha) = K$, so $\{1\}$ is a basis, as required.

Hence, assume that $\alpha \notin K$. In particular, it is thus clear that:

$$1, \alpha, \ldots, \alpha^{n-1}$$

is linearly independent over K (otherwise, the minimal polynomial would have degree less than n). To show that it forms a basis, it is sufficient to show that any element of $K(\alpha)$ can be expressed as a **unique** K-linear combination of $1, \alpha, \ldots, \alpha^{n-1}$.

Recall from last week:

*Let K be a **field**. Then:*

1. *Let $m \in K[t]$ be **monic** and **irreducible**. Let:*

$$\pi(t) = \alpha \in K[t]/\langle m \rangle$$

*be the **image** of t under the **canonical homomorphism**:*

$$\pi : K[t] \to K[t]/\langle m \rangle$$

*Then, α has a **minimal polynomial** m over K, and $K[t]/\langle m \rangle$ is **generated** by α over K ($K[t]/\langle m \rangle = K(\alpha)$).*

2. *The element t of the field $K(t)$ is **transcendental** over K, and $K(t)$ is **generated** by t over K.*

(Lemma 4.3.1)

*Let K be a **field**.*

1. *Let $m \in K[t]$ be a **monic, irreducible** polynomial. Then:*

$$\exists M : K,\ \exists \alpha \in M\ :\ M = K(\alpha)$$

*where α is **algebraic**, and has a **minimal polynomial** m over K. Moreover, if (M_1, α_1) and (M_2, α_2) are 2 such pairs, there is **exactly one isomorphism**:*

$$\varphi : M_1 \to M_2$$

over K, such that $\varphi(\alpha_1) = \alpha_2$.

2. *There exists an **extension** $M : K$ and a **transcendental** $\alpha \in M$, such that:*

$$M = K(\alpha)$$

*Moreover, if (M_1, α_1) and (M_2, α_2) are 2 such pairs, there is **exactly one isomorphism**:*

$$\varphi : M_1 \to M_2$$

over K, such that $\varphi(\alpha_1) = \alpha_2$.

(Theorem 4.3.16)

This tells us that without loss of generality, we may take:

$$K(\alpha) = K[t]/\langle m \rangle \qquad \alpha = \pi(t)$$

where π is the canonical homomorphism.

Now, π is surjective, so:

$$\forall x \in K(\alpha) = K[t]/\langle m \rangle\,,\ \exists f \in K[t]\ :\ \pi(f) = x$$

For any such f, recall that we can write it as:

$$f = qm + r$$

where $q, r \in K[t]$ are **unique**, and $\deg(r) < n$. In particular:

$$f(t) - r(t) = q(t)m(t) \iff f - r \in \langle m \rangle$$

and r is a unique such polynomial. Equivalently, we thus have **unique** $a_0, \ldots, a_{n-1} \in K$, such that:

$$f(t) - \sum_{i=0}^{n-1} a_i t^i \in \langle m \rangle$$

However, this means that f, r are in the same equivalence class under the canonical homomorphism, so:

$$\pi(f) = \pi\left(\sum_{i=0}^{n-1} a_i t^i\right)$$

(alternatively, $\pi(m) = 0 \in K[t]/\langle m \rangle$, from which the equality follows). Moreover, by definition $\pi(t) = \alpha$, so:

$$\pi(f) = \sum_{i=0}^{n-1} a_i \alpha^i$$

Thus, we can express any $\pi(f) \in K(\alpha)$ using a **unique** linear combination of $1, \ldots, \alpha^{n-1}$, and thus, this linearly independent set forms a basis for $K(\alpha)$ over K, as required.

(2)

Using Theorem 4.3.16, Part 2, we can see that if α is transcendental, then $K(\alpha)$ is isomorphic to $K(t)$. But we saw above that $1, t, t^2, \ldots$ is a basis for $K(t)$, and $[K(t) : K] = \infty$, so the result follows.

□

1.2.1 Examples

- if $\alpha \in \mathbb{C}$ is algebraic over $\mathbb{Q}$ with a quadratic minimal polynomial, then:

  $$\mathbb{Q}(\alpha) = \{a + b\alpha \mid a, b \in \mathbb{Q}\}$$

  We already saw this:

  - $\sqrt{2}$ is algebraic with minimal polynomial $t^2 - 2$
  - i is algebraic with minimal polynomial $t^2 - 1$

- if p is prime, then $e^{2\pi i/p}$ has minimal polynomial $1 + t + \ldots + t^{p-1}$, so:

  $$[\mathbb{Q}(e^{2\pi i/p}) : \mathbb{Q}] = p - 1$$

- consider the polynomial $1 + t + t^2$ over $\mathbb{Z}_2$. If α is a root, then:

  $$\mathbb{Z}_2(\alpha) = \{a + b\alpha \mid a, b \in \mathbb{Z}_2\} = \{0, 1, \alpha, 1 + \alpha\}$$

  Notice, since $1 + \alpha + \alpha^2 = 0$, then if we apply the Frobenius automorphism (and noting that $p = 2$ is prime and $\mathbb{Z}_2(\alpha)$ has characteristic 2)

  $$x \mapsto x^p$$

  then:

  $$\alpha^2 = -1 - \alpha = 1 + \alpha$$
  $$(1 + \alpha)^2 = 1^2 + \alpha^2 = \alpha$$

- notice, this Theorem tells us that if $\alpha \in M$ is algebraic over K with minimal polynomial m of degree n, the set $\{1, \alpha, \ldots, \alpha^{n-1}\}$ forms a **basis** for $K(\alpha)$, such that:

$$\left\{ \sum_{i=0}^{n-1} a_i \alpha^i \mid a_i \in K \right\}$$

will be a **subfield** of M (since $K(\alpha)$ is by definition of the smallest subfield of M containing $K \cup \{\alpha\}$). This is not obvious at all: this implies that, for instance, the set is closed under taking reciprocals!

1.3 Corollaries

1.3.1 Definition: Degree of Elements

*Let $M : K$ be a **field extension**, with $\alpha \in M$. Then, the **degree** of α over K is:*

$$\deg_K(\alpha) = [K(\alpha) : K]$$

Alternatively:

$$\deg_K(\alpha) = \deg(m)$$

where m is the minimal polynomial of α in $K[t]$ (this follows from Theorem 5.1.5 above).

1.3.2 Corollary: Finite Degree Iff Algebraic

*Let $M : K$ be a **field extension** with $\alpha \in M$. Then:*

$$\deg_K(\alpha) < \infty \iff \alpha \text{ is algebraic over } K$$

(Corollary 5.1.10)

Proof. This is immediate from the Theorem above, and using the fact that $\deg_K(\alpha) = [K(\alpha) : K]$. □

1.3.3 Example: Field Extension Containing $\sqrt[3]{2}$

Let ξ be the **real** cube root of 2. Last week we argued that:

$$\mathbb{Q}(\xi) \neq \{a + b\xi \mid a, b \in \mathbb{Q}\}$$

Proving this directly is messy. However, now we know that the minimal polynomial of ξ is $t^3 - 2$, so:

$$\deg_{\mathbb{Q}}(\xi) = 3$$

In particular, this means that $Q(\xi)$ is a 3-dimensional vector field over $\mathbb{Q}$, so the set $\{1, \xi\}$ won't be a basis.

In fact, this is a rather elegant proof that $2^{2/3}$ can't be written as a $\mathbb{Q}$-linear combination of 1 and $2^{1/3}$!

1.3.4 Corollary: Degree of Chained Extensions

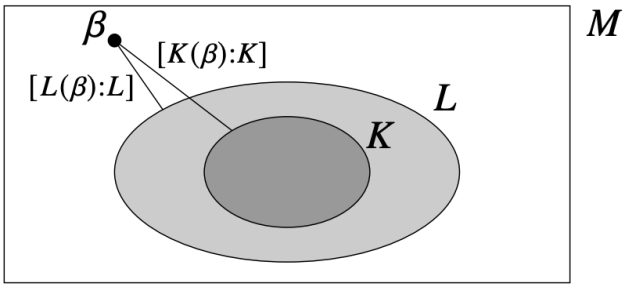
*Let $M : L : K$ be **field extensions**, and $\beta \in M$. Then:*

$$[L(\beta) : L] \leq [K(\beta) : K]$$

(Corollary 5.1.12)

---

*This isn't immediately obvious, but can be understood intuitively. Since $L : K$, L contains a copy of K. Hence, the **minimal polynomial** of β in L will have **at most** the same degree as the minimal polynomial of β in K (since L has "more" elements, we can potentially construct a polynomial of smaller degree with β as a root). Pictorially:*



Proof. If $[K(\beta) : K] = \infty$ (i.e if β is transcendental), then the result follows.

Otherwise, β will be algebraic over K, so let $m \in K[t]$ be its minimal polynomial. Since $L : K$, m is certainly an annihilating polynomial of β over L. In particular, we must have that the degree of the minimal polynomial p of β over L is at most $deg(m)$, so:

$$[L(\beta) : L] = deg(p) \leq deg(m) = [K(\beta) : K]$$

as required.

□

1.3.5 Corollary: Element in Field from Polynomial of Algebraics

*Let $M : K$ be a **field extension**. Let:*

$$\alpha_1, \ldots, \alpha_n \in M$$

*where each α_i is **algebraic** over K, and:*

$$\deg_K(\alpha_i) = d_i$$

Then:

$$\forall \alpha \in K(\alpha_1, \ldots, \alpha_n),\ \exists c_{r_1,\ldots,r_n} \in K\ :\ \alpha = \sum_{r_1,\ldots,r_n} c_{r_1,\ldots,r_n} \prod_{i=1}^{n} \alpha_i^{r_i}$$

where:

$$r_i \in [0, d_i - 1]$$

(Corollary 5.1.14)

This is conceptually difficult, so it is easier to ground it with an example.

Consider the case $n = 2$. We have an extension $M : K$, and 2 algebraic elements $\alpha_1, \alpha_2 \in M$. Say:

$$\deg_K(\alpha_1) = d_1 \quad \deg_K(\alpha_2) = d_2$$

Then, each element of $K(\alpha_1, \alpha_2)$ can be expressed as:

$$\sum_{r=0}^{d_1-1} \sum_{s=0}^{d_2-1} c_{rs} \alpha_1^r \alpha_2^s$$

where $c_{rs} \in K$ are some coefficients.

For example, recall how:

$$\mathbb{Q}(\sqrt{2}, i) = \{a + b\sqrt{2} + ci + d\sqrt{2}i \mid a, b, c, d \in \mathbb{Q}\}$$

Since:

$$\deg_{\mathbb{Q}}(\sqrt{2}) = \deg_{\mathbb{Q}}(i) = 2$$

any element of $\mathbb{Q}(\sqrt{2}, i)$ can be written as:

$$\sum_{r=0}^{1} \sum_{s=0}^{1} c_{rs} \sqrt{2}^r i^s = c_{00} + c_{01} i + c_{10}\sqrt{2} + c_{11}\sqrt{2}i$$

as expected.

Proof. We proceed by induction.

(1) **Base Case (n = 1)**

(We skip $n = 0$, since this is trivial)

The case $n = 1$ is what we've been considering up until now (simple field extensions), for which we know that, by using Theorem 5.1.5:

> *Let $K(\alpha) : K$ be a **simple extension**. Then:*
>
> 1. *Let:*
>
> - *α be **algebraic** over K*
> - *$m \in K[t]$ be the **minimal polynomial** of α*
> - $\deg(m) = n$
>
> *Then:*
>
> $$1, \alpha, \ldots, \alpha^{n-1}$$
>
> *is a **basis** of $K(\alpha)$ over K, such that:*
>
> $$[K(\alpha) : K] = \deg(m) = n$$
>
> 2. *If α is **transcendental** over K, then:*
>
> $$1, \alpha, \alpha^2, \ldots$$
>
> *are **linearly independent** over K, and so:*
>
> $$[K(\alpha) : K] = \infty$$
>
> *(Theorem 5.1.5)*

$1, \alpha, \ldots, \alpha^{deg_K(\alpha)-1}$ forms a basis for $K(\alpha)$ over K, so the result follows for $n = 1$.

(2) **Inductive Hypothesis:** $n \leq k$

Now, assume the claim is true for any $n \in [1, k]$; that is, for any $\alpha \in K(\alpha_1, \ldots, \alpha_k)$, we have that:

$$\alpha = \exists c_{r_1,\ldots,r_n} \in K \ : \ \alpha = \sum_{r_1,\ldots,r_k} c_{r_1,\ldots,r_k} \prod_{i=1}^{k} \alpha_i^{r_i}$$

where

$$\deg_K(\alpha_i) = d_i \qquad r_i \in [0, d_i - 1]$$

(3) **Inductive Step:** $n = k + 1$

Now, let:

$$\alpha \in K(\alpha_1, \ldots, \alpha_{k+1})$$

Notice, since $K(\alpha_1, \ldots, \alpha_k)$ is a field, we may also write:

$$\alpha \in (K(\alpha_1, \ldots, \alpha_k))(\alpha_{k+1})$$

Notice, this is a simple extension:

$$(K(\alpha_1, \ldots, \alpha_k))(\alpha_{k+1}) : K(\alpha_1, \ldots, \alpha_k)$$

and since α_{k+1} is algebraic, again by Theorem 5.1.5, we may write:

$$\alpha = \sum_{r=0}^{d_{k+1}-1} c_r \alpha_{k+1}^r$$

where:

$$d_{k+1} = \deg_K(\alpha_{k+1}) \geq \deg_{K(\alpha_1,\ldots,\alpha_k)}(\alpha_{k+1})$$

and:

$$c_0, \ldots, c_{d_{k+1}-1} \in K(\alpha_1, \ldots, \alpha_k)$$

But them, we can apply the inducitve hypothesis for each c_r:

$$c_r = \sum_{r_1,\ldots,r_k} c_{r_1,\ldots,r_k} \prod_{i=1}^{k} \alpha_i^{r_i}$$

so:

$$\alpha = \sum_{r=0}^{d_{k+1}-1} \left(\sum_{r_1,\ldots,r_k} c_{r_1,\ldots,r_k} \prod_{i=1}^{k} \alpha_i^{r_i} \right) \alpha_{k+1}^r = \sum_{r_1,\ldots,r_{k+1}} c_{r_1,\ldots,r_{k+1}} \prod_{i=1}^{k+1} \alpha_i^{r_i}$$

as required.

□

2 The Tower Law

2.1 Theorem: The Tower Law

The Tower Law is invaluable when dealing with extensions which involve adjoining multiple elements.

*Let $M : L : K$ be **field extensions**.*

1. *If:*
   - *$(\alpha_i)_{i \in I}$ is a **basis** of L over K*
   - *$(\beta_j)_{j \in J}$ is a **basis** of M over L*

   *then, $(\alpha_i \beta_j)_{(i,j) \in I \times J}$ is a **basis** for M over K.*
2. $$M : K \text{ is } \textbf{finite} \iff M : L \text{ and } L : K \text{ are } \textbf{finite}$$
3. $$[M : K] = [M : L][L : K]$$

(Theorem 5.1.17)

Proof. Notice, it is sufficient to prove (1), since (2), (3) follow immediately.

To this end, we claim that $(\alpha_i\beta_j)_{(i,j)\in I\times J}$ is a linearly independent, spanning set of M over K.

> *A family $(a_i)_{i\in I}$ to be **finitely supported** if the set:*
>
> $$\{i \in I \mid a_i \neq 0\}$$
>
> *is **finite***

Let $(c_{ij})_{(i,j)\in I\times J}$ be a finitely supported family of elements of K, such that:

$$\sum_{i,j} c_{ij}\alpha_i\beta_j = 0$$

In particular, this means that for any $j \in J$:

$$\sum_i c_{ij}\alpha_i \in L$$

(as α_i forms a basis of L over K). Thus, and using the fact that $(\beta_j)_{j\in J}$ is linearly independent over L:

$$\sum_{i,j} c_{ij}\alpha_i\beta_j = 0 \iff \sum_j \left(\sum_i c_{ij}\alpha_i\right)\beta_j = 0 \iff \sum_i c_{ij}\alpha_i = 0$$

However, $(\alpha_i)_{i\in I}$ is linearly independent over K, so:

$$\forall i \in I, \forall j \in J,\ c_{ij} = 0$$

Hence:

$$\sum_{i,j} c_{ij}\alpha_i\beta_j = 0 \iff c_{ij} = 0$$

so

$$(\alpha_i\beta_j)_{(i,j)\in I\times J}$$

is linearly independent over K, as required.

Now, we show it is a spanning set. Let $e \in M$. $(\beta_j)_{j\in J}$ spans M over L, so:

$$e = \sum_j d_j\beta_j$$

for some finitely supported family $(d_j)_{j\in J} \in L$. But then, $(\alpha_i)_{i\in I}$ spans L over K, so for each $j \in J$:

$$d_j = \sum_i c_{ij}\alpha_i$$

for some finitely supported family $(c_{ij})_{i\in I}$ of K. Hence:

$$e = \sum_j \sum_i c_{ij}\alpha_i\beta_j$$

as required.

□

2.1.1 Example: Tower Law for Degree of Complicated Extensions

Consider the extension $\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}$. We know that this is in fact a simple extension, since:

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$$

If we wanted to find the degree of $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ we'd need to find the minimal polynomial of $\sqrt{2}+\sqrt{3}$ which isn't immediately obvious.

It is easier to just use the Tower Law. Indeed, let:

$$M = \mathbb{Q}(\sqrt{2},\sqrt{3}) \qquad L = \mathbb{Q}(\sqrt{2}) \qquad K = \mathbb{Q}$$

Then clearly:

$$M : L : K$$

so by the Tower Law:

$$\begin{aligned} & [M:K] = [M:L][L:K] \\ \implies & [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}] \\ \implies & [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]\cdot 2 \end{aligned}$$

Moreover, recall that:

> *Let $M : L : K$ be **field extensions**, and $\beta \in M$. Then:*
>
> $$[L(\beta):L] \leq [K(\beta):K]$$
>
> *(Corollary 5.1.12)*

Using $L = \mathbb{Q}(\sqrt{2}), K = \mathbb{Q}, \beta = \sqrt{3}$ then implies that:

$$[L(\sqrt{3}):L] \leq [K(\sqrt{3}):K] \implies [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})] \leq [\mathbb{Q}(\sqrt{3}):\mathbb{Q}] = 2$$

Moreover, since $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ it is clear that:

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) \neq \mathbb{Q}(\sqrt{2})$$

so:

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})] > 1$$

(recall, $[M:K] = 1 \iff M = K$). Hence, we must have that:

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})] = 2$$

such that:

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = 4$$

Moreover, by closure under multiplication, we know that:

$$\{1,\sqrt{2},\sqrt{3},\sqrt{6}\} \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$$

This is a linearly independent set of 4 elements; since $\mathbb{Q}(\sqrt{2},\sqrt{3})$ has dimension 4, it must be a basis, so:

$$\alpha \in \mathbb{Q}(\sqrt{2},\sqrt{3}) \implies \alpha = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$

2.2 Corollaries of the Tower Law

2.2.1 Corollary: Divisibility of Degree for Stacked Extensions

Let:

$$M : L_1 : L_2 : K$$

be ***field extensions****. If* $M : K$ *is* ***finite*** *then* $[L_1 : L_2]$ *divides* $[M : K]$*. (Corollary 5.1.19)*

Proof. Just apply the Tower Law twice:

$$[M : K] = [M : L_1][L_1 : K] = [M : L_1][L_1 : L_2][L_2 : K]$$

□

2.2.2 Exercises

1. *[Exercise 5.1.20]* **Show that a field extension whose degree is a prime number must be simple. This might remind you of the fact that a group of prime order is cyclic.**

2.2.3 Corollary: Upper Bound on Degree for Adjoined Extensions

Let $M : K$ *be a* ***field extension*** *and:*

$$\alpha_1, \ldots, \alpha_n \in M$$

Then:

$$[K(\alpha_1, \ldots, \alpha_n) : K] \leq [K(\alpha_1) : K] \ldots [K(\alpha_n) : K]$$

(Corollary 5.1.21)

Proof. Applying the Tower Law, and defining $L_i = K(\alpha_1, \ldots, \alpha_i)$:

$$\begin{aligned} & [K(\alpha_1, \ldots, \alpha_n) : K] \\ =& [K(\alpha_1, \ldots, \alpha_n) : K(\alpha_1, \ldots, \alpha_{n-1})] \ldots [K(\alpha_1, \alpha_2) : K(\alpha_1)][K(\alpha_1) : K] \\ =& [L_{n-1}(\alpha_n) : L_{n-1}] \ldots [L_1(\alpha_2) : L_1][K(\alpha_1) : K] \end{aligned}$$

Then, recall:

*Let $M : L : K$ be **field extensions**, and $\beta \in M$. Then:*

$$[L(\beta) : L] \leq [K(\beta) : K]$$

(Corollary 5.1.12)

from which we get:

$$[K(\alpha_1, \ldots, \alpha_n) : K] \leq [K(\alpha_1) : K] \ldots [K(\alpha_n) : K]$$

as required.

□

3 Algebraic Extensions

3.1 Definition: Finitely Generated Field Extension

*The **field extension** $M : K$ is **finitely generated** if:*

$$\exists Y \subseteq M \ : \ |Y| < \infty \text{ and } M = K(Y)$$

(Definition 5.2.1)

3.2 Definition: Algebraic Field Extension

*The **field extension** $M : K$ is **algebraic** if every element of M is **algebraic** over K.*

---

*Recall, α is **algebraic** over K **if and only if** $K(\alpha) : K$ is **finite** (this is Corollary 5.1.19). Thus, if a **field extension** is **algebraic**, we can think of it as some kind of **finiteness condition**.*
(Definition 5.2.2)

3.3 Proposition: Finite Extensions are Finitely Generated and Algebraic

Let $M : K$ be a ***field extension****. Then, the following are equivalent:*

1. *$M : K$ is* ***finite***
2. *$M : K$ is* ***finitely generated and algebraic***
3. *for some* ***finite*** *set $\{\alpha_1, \ldots, \alpha_n\}$ of algebraic elements of M over K:*

$$M = K(\alpha_1, \ldots, \alpha_n)$$

(Proposition 5.2.4)

Proof.

(1) $\implies$ (2)

Assume that $M : K$ is finite.

We begin by showing that $M : K$ is finitely generated. Since $M : K$ is finite, we have a basis $\alpha_1, \ldots, \alpha_n$ of M over K. Notice, any subfield L of M containing K will be a K-linear subspace of M, so:

$$\alpha_1, \ldots, \alpha_n \in L \implies L = M$$

In particular, the **only** subfield of M containing:

$$K \cup \{\alpha_1, \ldots, \alpha_n\}$$

is M itself:

$$M = K(\alpha_1, \ldots, \alpha_n)$$

Thus, $M : K$ is finitely generated.

It is also algebraic. Let $\alpha \in M$. Notice, by the Tower Law, and since $M : K$ is finite, and we have that $M : K(\alpha) : K$, it follows that in particular $K(\alpha) : K$ is finite, so α must be algebraic (Corollary 5.1.10). Hence, $M : K$ is algebraic.

(2) $\implies$ (3)

Assume that $M : K$ is finitely generated and algebraic over K. Then there exists a finite set $\{\alpha_1, \ldots, \alpha_n\}$ such that:

$$M = K(\alpha_1, \ldots, \alpha_n)$$

But since M is algebraic, each of the $\alpha_1, \ldots, \alpha_n$ must also be algebraic in K, as required.

(3) $\implies$ (1)

Assume that we have algebraic α_i over K, such that:

$$M = K(\alpha_1, \ldots, \alpha_n)$$

Then, by the second Corollary of the Tower Law:

$$[M : K] = [K(\alpha_1, \ldots, \alpha_n) : K] \leq [K(\alpha_1) : K] \ldots [K(\alpha_n) : K]$$

Since α_i are algebraic, then:

$$\forall i \in [1, n] \ : \ [K(\alpha_i) : K] < \infty$$

so:

$$[M : K] < \infty$$

as required.

□

3.3.1 Corollary: Finite, Simple Extensions are Algebraic

*Let $K(\alpha) : K$ be a **simple extension**. The following are equivalent:*

1. $$[K(\alpha) : K] < \infty$$
2. *$K(\alpha) : K$ is **algebraic***
3. *α is **algebraic** over K*

(Corollary 5.2.6)

Proof.

- (1) $\implies$ (2) is the above Proposition (Proposition 5.2.4)
- (2) $\implies$ (3) is immediate from the definition of an algebraic extension
- (3) $\implies$ (1) is again immediate from the above Proposition (Proposition 5.2.4)

□

3.3.2 Proposition: Algebraics Over Rationals are a Subfield of Complex Numbers

> *The set of* ***algebraic numbers*** *over* $\mathbb{Q}$ *(denoted* $\overline{\mathbb{Q}}$*) is a* ***subfield*** *of* $\mathbb{C}$*. (Proposition 5.2.7)*

Proof. We have that $\alpha \in \mathbb{C}$ is algebraic if and only if $\mathbb{Q}(\alpha) : \mathbb{Q}$ is finite. In other words:

$$\overline{\mathbb{Q}} = \{\alpha \mid \alpha \in \mathbb{C}, [\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty\}$$

Now, let $\alpha, \beta \in \overline{\mathbb{Q}}$. Then, by the Second Corollary of the Tower Law:

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] \leq [\mathbb{Q}(\alpha) : \mathbb{Q}][\mathbb{Q}(\beta) : \mathbb{Q}] < \infty$$

Importantly, we thus know that $\mathbb{Q}(\alpha, \beta)$ is finite.

We have that $\alpha - \beta \in \mathbb{Q}(\alpha, \beta)$, so in particular:

$$[\mathbb{Q}(\alpha - \beta) : \mathbb{Q}] \leq [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] < \infty$$

Thus, since $\mathbb{Q}(\alpha - \beta) : \mathbb{Q}$ is a finite, simple field extension, by the above Corollary it follows that $\alpha - \beta$ is algebraic, so $\alpha - \beta \in \overline{\mathbb{Q}}$. The same argument can be used to show that $\alpha\beta \in \overline{\mathbb{Q}}$. Moreover, it is clear that $0, 1 \in \overline{\mathbb{Q}}$. Hence, $\overline{\mathbb{Q}}$ is a subring of $\mathbb{C}$.

To show it is a subfield, we just need to show that $1/\alpha \in \overline{\mathbb{Q}}$. Clearly, and using the fact that $\mathbb{Q}(\alpha)$ is a field:

$$[\mathbb{Q}(1/\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty$$

so $1/\alpha$ is algebraic, and $1/\alpha \in \overline{\mathbb{Q}}$.

Hence, $\overline{\mathbb{Q}}$ must be a subfield of $\mathbb{C}$, as required.

□

3.3.3 Exercises

1. *[Exercise 5.2.8]* **By imitating the prove above, show that L is a subfield of M, where $M : K$ is a field extension, and L is the set of elements of M algebraic over K.**

4 Ruler and Compass Constructions

4.1 Formalising Ruler and Compass Constructions

- **What constructions are possible in a ruler and compass problem?**
  - we are allowed an **unmarked edge** ("ruler"), and a **compass**
  - if Σ is a subset of the plane:
    - given $A, B \in \Sigma$, we can draw the (infinite) line through A and B
    - given $A, B \in \Sigma$, we can draw the circle with **centre** A passing through B

4.1.1 Definition: Immediately Constructible Points

*A point is **immediately constructible** from Σ if it is a **point of intersection** between:*

- *2 **distinct lines***
- *2 **distinct circles***
- *a **line** and a **circle***

4.1.2 Definition: Constructible Points

*A point C_n is **constructible** from Σ if there is a **finite** sequence of points:*

$$C_1, \ldots, C_n$$

such that:

$$\forall i \in [1, n]\ C_i \text{ is immediately constructible from } \Sigma \cup \{C_1, \ldots, C_{i-1}\}$$

4.2 Field Theory and Constructions

When performing ruler and compass constructions, points of intersection correspond to solutions to linear or quadratic equations (since these are the form of the equations of lines and circles). As such, we expect points like $\sqrt{\sqrt{2}+\sqrt{3}}$ to be constructible, whilst $\sqrt[3]{2}$ shouldn't be (no way a cube root could turn up). We now attempt to formalise this notion in terms of field theory.

4.2.1 Definition: Iterated Quadratic Extension

*Let $K \subseteq \mathbb{R}$ be a **subfield**. The **extension** $K : \mathbb{Q}$ is **iterated quadratic** if there exists from **finite sequence** of **subfields**:*

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = K$$

such that:

$$\forall i \in [1, n],\ [K_i : K_{i-1}] = 2$$

4.2.2 Example of Iterated Quadratic Extensions

The extension:

$$\mathbb{Q}\left(\sqrt{\sqrt{2}+\sqrt{3}}\right) : \mathbb{Q}$$

is **iterated quadratic**, since:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}\left(\sqrt{\sqrt{2}+\sqrt{3}}\right)$$

The fact that $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}\left(\sqrt{\sqrt{2}+\sqrt{3}}\right)$ comes from the fact that closure under multiplication gives:

$$\left(\sqrt{\sqrt{2}+\sqrt{3}}\right)^2 = \sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$$

In fact, a similar argument tells us that there is an interated quadratic extension of $\mathbb{Q}$ containing $\sqrt{\sqrt{5}+\sqrt{7}}$.

4.2.3 Definition: Compositum of Fields

*Let L_1, L_2 be **subfields** of the **field** M. The **compositum** L_1L_2 is the **subfield** of M, generated by $L_1 \cup L_2$.*

---

*That is, the **compositum** is the **smallest subfield** of M containing both L_1 and L_2:*

$$L_1L_2 = L_1(L_2) = L_2(L_1)$$

(Definition 5.3.3)

- **What is the compositum of $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$?**
  - the field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$

4.2.4 Lemma: Degree of a Compositum

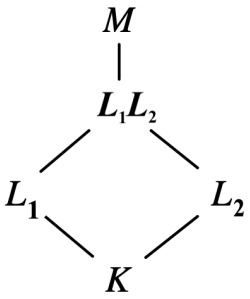
*Let $M : K$ be a **field extension**, such that L_1, L_2 are **subfields** of M **containing** K. Then:*

$$[L_1 : K] = 2 \implies [L_1L_2 : L_2] \in \{1, 2\}$$

More generally, it is the case that:

$$[L_1L_2 : L_2] \leq [L_1 : K]$$

(Lemma 5.3.6)



Proof. We seek to show that:

$$[L_1L_2 : L_2] \leq 2$$

Let $\beta \in L_1 \setminus K$. We can then apply the Tower Law to:

$$L_1 : K(\beta) : K$$

which alongside the hypothesis that $[L_1 : K] = 2$ yields:

$$[L_1 : K] = 2 \implies [L_1 : K(\beta)][K(\beta) : K] = 2$$

Since $\beta \notin K$, we must have that $[K(\beta) : K] \geq 2$, which then implies that $[K(\beta) : K] = 2$, and thus forces:

$$[L_1 : K(\beta)] = 1 \iff L_1 = K(\beta)$$

Using this, we now seek to show that:

$$L_1L_2 = L_2(\beta)$$

Since $L_2 \subseteq L_1L_2$ and $\beta \in L_1 \subseteq L_1L_2$, it is clear that:

$$L_2(\beta) \subseteq L_1L_2$$

Conversely, $L_2(\beta)$ is a subfield of M containing $K(\beta) = L_1$ (since $K \subseteq L_2$) and L_2, so it must contain L_1L_2. Hence, it follows that $L_1L_2 = L_2(\beta)$.

Hence, using Corollary 5.1.12:

$$[L_1L_2 : L_2] = [L_2(\beta) : L_2] \leq [K(\beta) : K] = 2$$

as required.

□

4.2.5 Lemma: Generating Iterated Quadratic Subfields

*Let K and L be **subfields** of $\mathbb{R}$, such that the **extensions**:*

$$K : \mathbb{Q} \qquad L : \mathbb{Q}$$

*are **iterated quadratic**. Then, there is some **subfield** M of $\mathbb{R}$, such that:*

- *the **extension** $M : \mathbb{Q}$ is **iterated quadratic***
- $K, L \subseteq M$

(Lemma 5.3.8)

Proof. Since $K : \mathbb{Q}, L : \mathbb{Q}$ are iterated quadratic, we have that:

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq K_n = K \subseteq \mathbb{R}$$

$$\mathbb{Q} = L_0 \subseteq L_1 \subseteq L_2 \subseteq \ldots \subseteq L_m = K \subseteq \mathbb{R}$$

such that:

$$\forall i, j,\ [K_i : K_{i-1}] = 2 = [L_j : L_{j-1}]$$

Now, consider the chain of subfields of $\mathbb{R}$ given by:

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = K = KL_0 \subseteq KL_1 \subseteq \ldots \subseteq KL_m = KL$$

Then, it is sufficient to show that $M = KL$ is an iterated quadratic extension of K, since $K, L \subseteq KL$ clearly.

We know that for all i:

$$[K_i : K_{i-1}] = 2$$

and similarly that for each j:

$$[L_j : L_{j-1}]$$

Recall Lemma 5.3.6 on the degree of compositums:

*Let $M : K$ be a **field extension**, such that L_1, L_2 are **subfields** of M **containing** K. Then:*

$$[L_1 : K] = 2 \implies [L_1L_2 : L_2] \in \{1, 2\}$$

More generally, it is the case that:

$$[L_1L_2 : L_2] \leq [L_1 : K]$$

(Lemma 5.3.6)

We have that L_j, KL_{j-1} are subfields of $\mathbb{R}$ which both contain L_{j-1} by assumption. Thus, applying the Lemma:

$$[L_j : L_{j-1}] = 2 \implies [L_j(KL_{j-1}) : KL_{j-1}] = [KL_j : KL_{j-1}] \in \{1, 2\}$$

Hence, in the chain of subfields, all the successive degrees are either 1 or 2. Extensions with degree 1 are an equality, which can be ignored. This then yields that $KL : \mathbb{Q}$ is an iterated quadratic extension, which trivially contains K and L.

□

4.3 The Problems Which Stumped the Greeks

4.3.1 Proposition: Iterated Quadratic Extensions Contain Constructible Points

Ruler and compass constructibility involves a set $\Sigma \subseteq \mathbb{R}^2$ of points. For simplicity, we may assume that Σ only contains 2 points, and we can orient the coordinate axes, such that these 2 points have coordinates $(0, 0)$ and $(1, 0)$.

> *Let $(x, y) \in \mathbb{R}^2$. If (x, y) is **constructible** from:*
>
> $$\Sigma = \{(0, 0), (1, 0)\}$$
>
> *then there is an **iterated quadratic extension** of $\mathbb{Q}$ containing both x and y.*
> *(Proposition 5.3.9)*

Proof. We operated inductively on the number of steps n required to construct (x, y) from Σ.

(1) **Base Case:** $n = 0$

If $n = 0$, then $(x, y) \in \Sigma$, so $x, y \in \mathbb{Q}$, which is an iterated quadratic expression of itself.

(2) **Inductive Hypothesis:** $n = k$

Assume that if (x, y) is constructible in k steps from Σ, then there is an iterated quadratic extension of $\mathbb{Q}$ containing both x and y.

(3) **Inductive Step:** $n = k + 1$

Now, assume that (x, y) is constructible in $k + 1$ steps from Σ. If this is the case, by definition, (x, y) must be the intersection point of 2 distinct lines and/or circles, through points which are constructible in at most k steps. By the inductive hypothesis, each of these points must lie in some iterated quadratic extension of $\mathbb{Q}$, so by Lemma 5.3.8:

*Let K and L be **subfields** of $\mathbb{R}$, such that the **extensions**:*

$$K : \mathbb{Q} \qquad L : \mathbb{Q}$$

*are **iterated quadratic**. Then, there is some **subfield** M of $\mathbb{R}$, such that:*

- *the **extension** $M : \mathbb{Q}$ is **iterated quadratic***
- $K, L \subseteq M$

(Lemma 5.3.8)

there is an iterated quadratic extension L of $\mathbb{Q}$ containing all of the points' coordinates. The coefficients in the equations of the lines and/or circles must also lie in L, due to the closure of the field.

We now claim that:

$$\deg_L(x) \in \{1, 2\}$$

If $\deg_L(x) = 1$, then the minimal polynomial of x in L has degree 1, which implies that $x \in L$. Alternatively, $[L(x) : L] = 1 \iff L(x) = L$, so $x \in L$. Otherwise, if $\deg_L(x) = 2$, then by definition $[L(x) : L] = 2$, so $L(x)$ is an iterated quadratic extension of $\mathbb{Q}$ (since L is by inductive hypothesis). The same logic will apply to y, and then using Lemma 5.3.8, we can combine these to create an iterated quadratic extension of $\mathbb{Q}$ containing x, y.

Hence, to show that $\deg_L(x) \in \{1, 2\}$ we consider 3 cases:

1. If (x, y) is the point of intersection of 2 distinct lines, then they satisfy 2 linearly independent equations:

$$\begin{aligned} a_1x + b_1y + c_1 &= 0 \\ a_2x + b_2y + c_2 &= 0 \end{aligned}$$

where $a_i, b_i, c_i \in L$. But then:

$$\begin{aligned} & y = \frac{-c_2 - a_2x}{b_2} \\ \implies & a_1x - b_1\left(\frac{c_2 + a_2x}{b_2}\right) + c_1 = 0 \\ \implies & a_1x - \frac{b_1a_2}{b_2}x = -c_1 + \frac{b_1c_2}{b_2} \\ \implies & x = \frac{-c_1 + \frac{b_1c_2}{b_2}}{a_1 - \frac{b_1a_2}{b_2}} \end{aligned}$$

so $x \in L$, since it is a rational function of the $a_i, b_i, c_i \in L$. Thus:

$$\deg_L(x) = 1$$

2. If (x, y) is the point of intersection of a line and a circle, then:

$$\begin{aligned} ax + by + c &= 0 \\ x^2 + y^2 + dx + ey + f &= 0 \end{aligned}$$

where $a, b, c, d, e, f \in L$. If $b = 0$, then since a can't be 0, we have:

$$x = -\frac{c}{a} \in L$$

Otherwise, we can use the linear equation to solve for y, and plug in the result into the quadratic. This results in a quadratic over L, satisfied by x, so:

$$\deg_L(x) \in \{1, 2\}$$

(the minimal polynomial of x over L must have degree at most 2, since we have a quadratic solved by x)

3. If (x, y) is the point of intersection of 2 circles, then:

$$x^2 + y^2 + d_1 x + e_1 y + f_1 = 0$$
$$x^2 + y^2 + d_2 x + e_2 y + f_2 = 0$$

where $d_i, e_i, f_i \in L$. If we subtract both equations, we get a linear equation that must be satisfied by (x, y), which thus means that (x, y) must satisfy the case of a line and a circle, and so

$$\deg_L(x) \in \{1, 2\}$$

Hence, as required, x, y must lie in an iterated quadratic extension of $\mathbb{Q}$.

□

4.3.2 Theorem: Constructible, Algebraic Points Have Power of 2 Degree

*Let $(x, y) \in \mathbb{R}^2$. If (x, y) is **constructible** from:*

$$\Sigma = \{(0, 0), (1, 0)\}$$

then:

- *x, y are **algebraic** over $\mathbb{Q}$*
- *their **degrees** over $\mathbb{Q}$ are powers of 2*

(Theorem 5.3.10)

Proof. By the above proposition, there is an iterated quadratic extension M of $\mathbb{Q}$, such that $x \in M$. Hence, by the Tower Law:

$$\exists n \geq 0 \ : \ [M : \mathbb{Q}] = 2^n$$

Moreover, and again by the Tower Law:

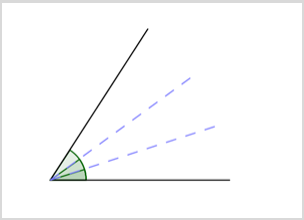
$$[M : \mathbb{Q}] = [M : \mathbb{Q}(x)][\mathbb{Q}(x) : \mathbb{Q}] \implies [\mathbb{Q}(x) : \mathbb{Q}] \mid 2^n$$

Hence, it follows that $\deg_{\mathbb{Q}}(x) < \infty$ (so x will be algebraic), and since it divides 2^n, it must itself be a power of 2, as required.

□

4.3.3 Proposition: Angles Can't be Trisected by Ruler and Compass

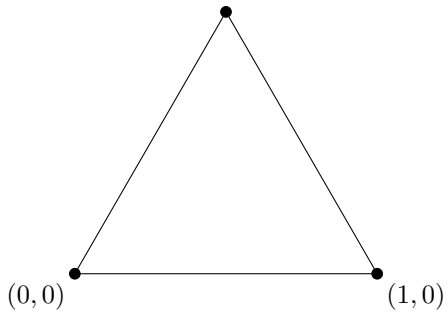
*An angle cannot be **trisected** by ruler and compass.*



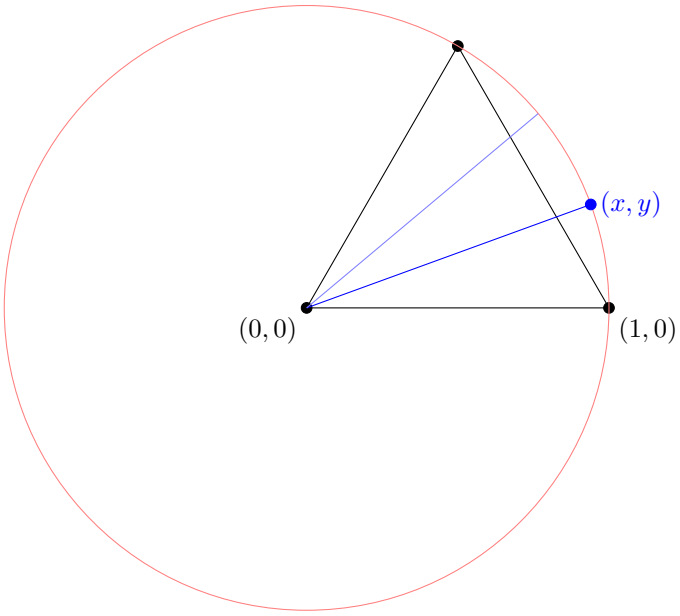
(Proposition 5.3.11)

Proof. Assume that an angle *can* be trisected with ruler and compass.

Using ruler and compass, we can construct an equilateral triangle with $(0,0)$ and $(0,1)$ at its vertices.



Then, we can trisect the angle of the triangle at the vertex $(0,0)$. Let (x,y) be the point where the trisector meets the circle with centre $(0,0)$ going through $(1,0)$:



In particular, this implies that x is constructible, and so, by Theorem 5.3.10 above:

$$\deg_{\mathbb{Q}}(x)$$

must be a power of 2. Simple trigonometry tells us that:

$$x = \cos(\pi/9)$$

Now, there's an identity for cos:

$$\cos(3x) = 4\cos^3(x) - 3\cos(x)$$

Plugging in $x = \pi/9$ and using $\cos(\pi/3) = \frac{1}{2}$:

$$\cos^3(\pi/9) - \frac{3}{4}\cos(\pi/9) - \frac{1}{8} = 0$$

so $x = \cos(\pi/9)$ is a root of:

$$p(t) = t^3 - \frac{3}{4}t - \frac{1}{8}$$

We claim that $p(t)$ is also the **minimal polynomial** of $\cos(\pi/9)$. By Lemma 4.2.10, $m \in \mathbb{Q}[t]$ (a monic polynomial) is the minimal polynomial of α over $\mathbb{Q}$ if and only if m is irreducible over $\mathbb{Q}$, and it annihilates α. To this end, recall the mod p method:

Let:

$$f(t) = a_0 + a_1 t + \ldots + a_n t^n \in \mathbb{Z}[t]$$

Let $\pi : \mathbb{Z} \to \mathbb{Z}_p$ be the canonical homomorphism, and $\pi_* : \mathbb{Z}[t] \to \mathbb{Z}_p[t]$ the resulting induced homomorphism. Define notation:

$$\pi(a) = \bar{a} \qquad \pi_*(f) = \bar{f}$$

If there exists a prime p such that:

- $p \nmid a_n$
- $\bar{f} \in \mathbb{Z}_p[t]$ *is* ***irreducible***

then f is ***irreducible*** *over $\mathbb{Q}$.*
(Proposition 3.3.9)

$p(t)$ is irreducible over $\mathbb{Q}$ if and only if:

$$8p(t) = 8t^3 - 6t - 1$$

is irreducible over $\mathbb{Q}$. Letting $p = 5$, we reduce our polynomial to:

$$\bar{3}\bar{p}(t) = \bar{3}t^3 - t - \bar{1} \in \mathbb{Z}_5$$

Moreover, by Lemma 3.3.1:

Let K be a ***field*** *and $f \in K[t]$. Then:*

1. $$deg(f) \leq 0 \implies f \text{ is } \textbf{not irreducible}$$
2. $$deg(f) = 1 \implies f \text{ is } \textbf{irreducible}$$
3. $$deg(f) \geq 2 \text{ and } f \text{ has a } \textbf{root} \implies f \text{ is } \textbf{reducible}$$
4. $$deg(f) \in \{2, 3\} \text{ and } f \text{ has } \textbf{no root} \implies f \text{ is } \textbf{irreducible}$$

(Lemma 3.3.1)

it follows that it is sufficient to show that $3\bar{p}$ has no roots in $\mathbb{Z}_5$. Indeed:

t	$\bar{3}t^3 - t - \bar{1}$
$\bar{0}$	$\bar{4}$
$\bar{1}$	$\bar{1}$
$\bar{2}$	$\bar{1}$
$\bar{3}$	$\bar{2}$
$\bar{4}$	$\bar{2}$

Hence, $\bar{3}\bar{p}$ has no roots over $\mathbb{Z}_5$, and so, is irreducible. It thus follows that $\cos(\pi/9)$ has $p(t) = t^3 - \frac{3}{4}t - \frac{1}{8}$ as an irreducible, annihilating polynomial over $\mathbb{Q}$, so p must be its minimal polynomial.

(you can also check Stack Exchange Post, which gives a more satisfying, albeit complicated, way of finding a minimal polynomial for $\cos(\pi/9)$)

But then, we must have that:

$$\deg_{\mathbb{Q}}(\cos(\pi/9)) = 3$$

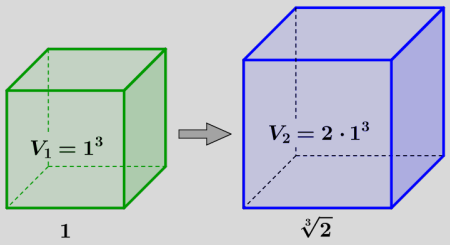
which isn't a power of 2. This is a contradiction, and so, it is impossible to trisect an angle just using ruler and compass. □

4.3.4 Proposition: Cube Can't be Duplicated by Ruler and Compass

*The cube cannot be **duplicated** by ruler and compass.*

---

*That is, given a length, we can't construct a new length whose **cube** is **twice** the cube of the original. In other words if 2 points are a distance L apart, we can't construct 2 new points which are a distance $\sqrt[3]{2}L$ apart.*



(Proposition 5.3.12)

Proof. Assume that we *can* duplicate a cube with ruler and compass.

Then, since $(0, 0)$ and $(1, 0)$ are a distance 1 apart, we can construct from them 2 points A, B a distance $\sqrt[3]{2}$ apart. Using ruler and compass, we can the construct the point $(\sqrt[3]{2}, 0)$:

Hence, since $(\sqrt[3]{2},0)$ is constructible, we must have that:

$$\deg_{\mathbb{Q}}(\sqrt[3]{2})$$

is a power of 2. But we know that the minimal polynomial of $\sqrt[3]{2}$ is t^3-2, so $\deg_{\mathbb{Q}}(2)=3$, a contradiction. Hence, we can't duplicate a cube by using ruler and compass.

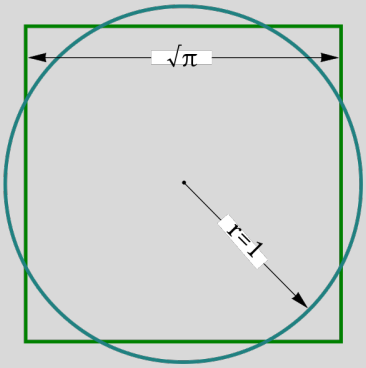
□

4.3.5 Proposition: Circle Can't be Squared by Ruler and Compass

*The circle cannot be **squared** by ruler and compass.*

---

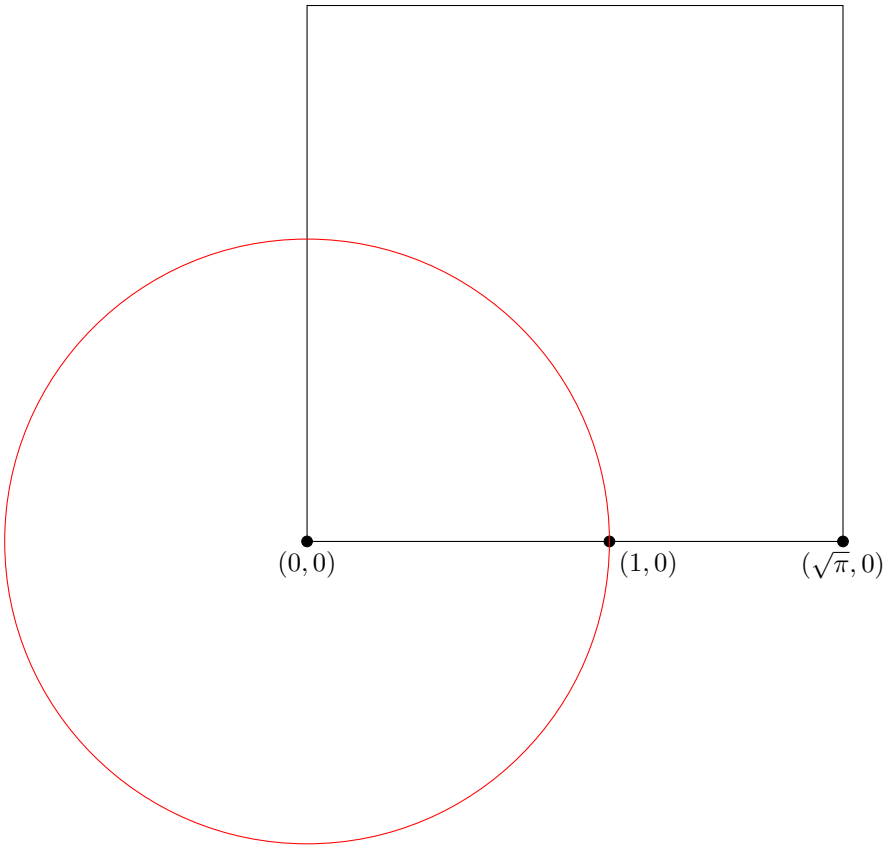
*That is, given a circle, we can't construct a square with the **same area**. in other words, if 2 points are a distance L apart, we can't construct 2 points a distance $\sqrt{\pi}L$ apart.*



(Proposition 5.3.13)

Proof. Assume that we *can* square a circle.

Consider the circle with centre $(0,0)$ going through $(1,0)$ with area π. Then, we can construct a square with side length $\sqrt{\pi}$, and then with ruler and compass, we can construct the point $(\sqrt{\pi},0)$:



However, this implies that $\sqrt{\pi}$ must be algebraic over $\mathbb{Q}$, with $\deg_{\mathbb{Q}}(\sqrt{\pi})$ as a power of 2. In particular, this means that $\sqrt{\pi} \in \overline{\mathbb{Q}}$, which is a subfield, which thus implies that $\pi \in \overline{\mathbb{Q}}$. Thus, we must have that π is algebraic, which is a contradiction, as we know that π is transcendental over $\mathbb{Q}$.

□

4.3.6 Proposition: Constructing Regular N-Sided Polygons

*A **regular, n-sided** polygon is **constructible <u>if and only if</u>**:*

$$n = 2^r p_1 \dots p_k$$

where:

- $r, k \geq 0$
- $p_1, \dots, p_k$ *are **Fermat Primes**, which are primes of the form:*

$$2^u + 1$$

We can show that if $p = 2^u + 1$ is prime, then u must be a power of 2. To this end, we know that if n is

odd:

$$x^n + 1 = (x+1)(x^{n-1} - x^{n-2} + \ldots + 1)$$

Now, let $m = nd$, where n is odd. Then:

$$x^m + 1 = (x^d)^n + 1 = (x^d + 1)((x^d)^{n-1} - (x^d)^{n-2} + \ldots + 1)$$

Hence, the only way for $x^m + 1$ to not be composite (and thus prime) is if m has no odd factors. In other words, m must be some power of 2.

Proof. [This is more of a sketch than a formal proof.]

Let p be prime, and assume that the regular p-sided polygon is constructible. W ecna consider inscirbing the regular p-sided polygon inside the unit circle in $\mathbb{C}$, such that one of its vertices is at 1.

We will have that another vertex will be at $e^{2\pi i/p}$, and since such a vertex is constructible:

$$\deg_{\mathbb{Q}}(e^{2\pi i/p})$$

is a power of 2. Moreover, we saw that $\deg_{\mathbb{Q}}(e^{2\pi i/p}) = p - 1$. Hence, $p - 1$ must be a power of 2, or in other words, p must be a Fermat Prime.

□