# MATH 457 Notes : Galois Theory

Samy Lahlou

These notes are based on lectures given by Professor Henri Darmon at McGill University in Winter 2025. The subject of these lectures is Representation Theory and Galois Theory but I chose to take notes only for the Galois Theory part.
As a disclaimer, it is more than possible that I made some mistakes. Feel free to correct me or ask me anything about the content of this document at the following address : samy.lahloukamal@mcgill.ca

## Contents

# 1 Fields Extensions

**Definition** (Field Extension)**.** *If and $\mathbb{E}$ and $\mathbb{F}$ are fields, we say that $E$ is an extension of $F$ if $F$ is a subfield of $E$.*

**Remark:** If $\mathbb{E}$ is an extension of $\mathbb{F}$, then $\mathbb{E}$ is also a vector space over $\mathbb{F}$.

**Definition.** *Given a fields $\mathbb{E}$ and $\mathbb{F}$ and $\alpha \in \mathbb{E}$ where $\mathbb{E}$ is an extension of $\mathbb{F}$, we denote by $\mathbb{F}[\alpha]$ the ring generated by $\mathbb{F}$ and $\alpha$, i.e., $\mathbb{F}[\alpha]$ is the intersection of all the fields containing both $\mathbb{F}$ and $\alpha$. Similarly, we denote by $\mathbb{F}(\alpha)$ the field generated by $\mathbb{F}$ and $\alpha$. Hence, there is a natural inclusion from $\mathbb{F}[\alpha]$ to $\mathbb{F}(\alpha)$.*

**Definition.** *The degree of $\mathbb{E}$ over $\mathbb{F}$ is the dimension of $\mathbb{E}$ as a $\mathbb{F}$ vector space. It is written as $[\mathbb{E} : \mathbb{F}]$. If the degree is finite, we say that $\mathbb{E}/\mathbb{F}$ is finite.*

**Example:**

- $[\mathbb{C} : \mathbb{R}] = 2$ since $\mathbb{R} \subset \mathbb{C}$ and $\mathbb{C}$ is a 2-dimensional $\mathbb{R}$-vector space.
- $[\mathbb{C} : \mathbb{Q}] = \infty$ since $\mathbb{Q} \subset \mathbb{C}$ and $\mathbb{C}$ is an $\infty$-dimensional $\mathbb{Q}$-vector space. Using the Axiom of Choice, we can construct a basis for this vector space, it is called the Hamel basis.
- Let $\mathbb{F}$ be a field and $\mathbb{E} = \mathbb{F}[x]/(p)$ where $p$ is an irreducible polynomial of degree $n$, then
$$\mathbb{E} = \{a_0 + a_1 x + ... + a_{n-1} x^{n-1}\}$$
so $[\mathbb{E} : \mathbb{F}] = n$ since $\mathbb{E}$ contains $\mathbb{F}$ (the constant polynomials) and has basis $\{1, x, ..., x^{n-1}\}$.
- Let $\mathbb{F}$ be a field and $\mathbb{E} = \mathbb{F}(x)$ be the fraction field of $\mathbb{F}[x]$, then $[\mathbb{E} : \mathbb{F}] = \infty$.
- Given an irreducible polynomial $p$ over $\mathbb{Q}$ and a root $\alpha$ of $p$, then
$$\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(p)$$
is an extension of $\mathbb{Q}$ of degree $\deg p$. The isomorphism $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(p)$ comes from the valuation map $ev_\alpha : \mathbb{Q}[x]/(p) \to \mathbb{Q}(\alpha)$.

**Theorem** (Multiplicativity of the degree)**.** *Given three fields $\mathbb{K} \subset \mathbb{F} \subset \mathbb{E}$, we have*
$$[\mathbb{E} : \mathbb{K}] = [\mathbb{E} : \mathbb{F}][\mathbb{F} : \mathbb{K}].$$

*Proof.* If one of the degree is infinite, the proof is trivial, hence, assume that the degrees are finite. Call $[\mathbb{E} : \mathbb{F}] = n$ and $[\mathbb{F} : \mathbb{K}] = m$. Let $\alpha_1, ..., \alpha_n \in \mathbb{F}$ be a basis for $\mathbb{E}$ as a $\mathbb{F}$-vector space and $\beta_1, ..., \beta_m \in \mathbb{K}$ be a basis for $\mathbb{F}$ as a $\mathbb{K}$-vector space. Notice that for all $a \in \mathbb{E}$, there exist elements $\lambda_1, ..., \lambda_n \in \mathbb{F}$ such that
$$a = \lambda_1 \alpha_1 + ... + \lambda_n \alpha_n$$
is the unique representation of $a$ as a linear combination of the basis $\alpha_1, ..., \alpha_n$. But for each $\lambda_i$, we know that there exist elements $\lambda_{i1}, ..., \lambda_{im} \in \mathbb{K}$ such that
$$\lambda_i = \lambda_{i1}\beta_1 + ... + \lambda_{im}\beta_m$$

. Thus,

$$a = \sum_{i=1}^{n} \sum_{j=1}^{m} \lambda_{ij} \alpha_i \beta_j.$$

Therefore, $\{\alpha_i \beta_j\}_{i,j}$ is a $\mathbb{K}$ basis for $\mathbb{E}$. Hence, it follows that the dimension of $\mathbb{E}$ as $K$-vector space is $n \cdot m$. ■

## 2 Ruler and Compass Constructions

**Definition.** *A complex number is constructible by ruler and compass if it can be obtained from rational numbers by successive applications of field operations (+, -, $\times$, division) and square roots. Using fields, we can say that a number is cinstructible if it is contained in a sequence of quadratic extensions of $\mathbb{Q}$.*

The set of elements constructible by ruler and compass is an extension of $\mathbb{Q}$ of infinite degree. The goal is to characterize the set of numbers which can be constructible by ruler and compass.

**Theorem.** *If $\alpha \in \mathbb{R}$ is a root of an irreducible cubic polynomial over $\mathbb{Q}$, then $\alpha$ is not constructible by ruler and compass.*

*Proof.* Suppose that $\alpha$ is constructible, then there are finite field extensions

$$\mathbb{Q} \subset \mathbb{F}_1 \subset ... \subset \mathbb{F}_n$$

with $\mathbb{F}_{i+1} = \mathbb{F}_i(\sqrt{a_i})$ for some $a_i \in \mathbb{F}_i$. Hence, for all $i$, we have that $[F_{i+1} : F_i]$ since $\{1, \sqrt{a_i}\}$ is a basis for $F_{i+1}$ as a $\mathbb{F}_i$-vector space. Thus, by multiplicativity of the degree, $[\mathbb{F}_n : \mathbb{Q}] = 2^n$. Moreover, we know that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ so we get the following diagram : **TODO**. Contradiction. ■

**Example:**

- (Duplicating the cube) $p(x) = x^3 - 2$ and $\alpha = \sqrt[3]{2}$ cannot be constructible.
- (Trissection of angle) $p(x) = x^3 - 3x + \frac{1}{2}$ and $\alpha = \cos(2\pi/9)$:

$$\cos(3\theta) = \cos^3\theta - 3\cos(\theta)(1 - \cos^2\theta)$$

**Definition** (Algebraic Numbers)**.** *Let $\mathbb{E}/\mathbb{F}$ be a finite extension. An element $\alpha \in \mathbb{E}$ is algebraic over $\mathbb{F}$ if $\alpha$ is the root of a polynomial in $\mathbb{F}[x]$.*

**Example:**

- $\sqrt{2} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$ since it solves the polynomial $x^2 - 1 \in \mathbb{Q}[x]$.
- $i \in \mathbb{C}$ is algebraic over $\mathbb{Q}$ since it solves the polynomial $x^2 + 1 \in \mathbb{Q}[x]$.
- $\pi$ is not algebraic over $\mathbb{Q}$ but it is algebraic over $\mathbb{Q}(\pi^3)$.
- The set of $\alpha \in \mathbb{R}$ which are algebraic over $\mathbb{Q}$ is countable (Cantor).

**Lemma.** *If $\mathbb{E}/\mathbb{F}$ is a finite extension, then every $\alpha \in \mathbb{E}$ is algebraic over $\mathbb{F}$.*

*Proof.* Let $n$ be the degree of $\mathbb{E}/\mathbb{F}$, then the set $\{1, \alpha, \alpha^2, ..., \alpha^n\}$ cannot be linearly independent since it contains $n+1$ elements. Hence, there exist scalars **TODO** ∎

**Definition** (Automorphism Group)**.** *The automorphism group of* $\mathbb{E}/\mathbb{F}$ *is*

$$Aut(\mathbb{E}/\mathbb{F}) = \{\sigma : \mathbb{E} \to \mathbb{E} : \sigma \textit{ preserves the operations and } \sigma|_{\mathbb{F}} = id\}$$

As a consequence, if $\sigma \in \mathrm{Aut}(\mathbb{E}/\mathbb{F})$, then $\sigma(0) = 0$, $\sigma(1) = 1$ and $\sigma(a^{-1}) = \sigma(a)^{-1}$.

**Proposition.** *If* $[\mathbb{E} : \mathbb{F}]$ *is finite then* $Aut(\mathbb{E}/\mathbb{F})$ *acts on* $\mathbb{E}$ *with finite orbits.*

*Proof.* Let $\alpha \in \mathbb{E}$, let's show that $\alpha$ has only finitely many translates by the action of $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$. By the previous Lemma, we know that $\alpha$ is algebraic so there is a polynomial $a_n x^n + ... + a_0 \in \mathbb{F}[x]$ satisfied by $\alpha$. By plugging-in $x = \alpha$, we have

$$a_n \alpha^n + ... a_1 \alpha + a_0 = 0.$$

Let $\sigma \in \mathrm{Aut}(\mathbb{E}/\mathbb{F})$, then applying $\sigma$ on both sides of the previous equation gives us

$$\sigma(a_n \alpha^n + ... a_1 \alpha + a_0) = 0.$$

Using the fact that $\sigma$ preserves addition and multiplication, we get

$$\sigma(a_n)\sigma(a_n)^n + ... + \sigma(a_1)\sigma(\alpha) + \sigma(a_0) = 0.$$

Finally, since $\sigma$ fixes the elements of $\mathbb{F}$, then

$$a_n \sigma(a_n)^n + ... + a_1 \sigma(\alpha) + a_0 = 0.$$

It follows that $\sigma(\alpha)$ must be a root of the same polynomial. Hence, the orbit of $\alpha$ is a subset of the roots of the polynomial that it satisfies (that we fixed at the beginning of the proof). Since polynomials over fields have finitely many roots, then $\alpha$ has a finite orbit. ∎

Notice that the same proof can be applied if $\mathbb{E}/\mathbb{F}$ is a finite extension such that all elements of $\mathbb{E}$ are algebraic over $\mathbb{F}$, i.e., if $\mathbb{E}/\mathbb{F}$ is an algebraic extension.

**Theorem.** *If* $[\mathbb{E} : \mathbb{F}] < \infty$*, then* $\#Aut(\mathbb{E}/\mathbb{F}) < \infty$.

*Proof.* Let $\alpha_1, ..., \alpha_n$ be generators for $\mathbb{E}$ over $\mathbb{F}$, then for all $\sigma \in \mathrm{Aut}(\mathbb{E}/\mathbb{F})$, if we know the behavior of $\sigma$ on the generators, then we know the behavior of $\sigma$ on $\mathbb{E}$. Since there are finitely many generators and each generator has a finite orbit, then there are finitely many possible $\sigma$. ∎

**Example:**

- Suppose that $\mathbb{E}$ is generated over $\mathbb{F}$ be a single element $\alpha$. Let $p \in \mathbb{F}[x]$ be the minimal polynomial of $\alpha$. Consider the evaluation map

$$\begin{aligned} ev_\alpha : \mathbb{F}[x] &\to \mathbb{F}[\alpha] \\ x &\mapsto \alpha \\ f(x) &\mapsto f(\alpha) \end{aligned}$$

  We get that $\ker(ev_\alpha) = (p)$. Hence, by the isomorphism theorem, $\mathbb{F}[\alpha]/(p) \cong \mathbb{F}[\alpha]$. Since $\mathbb{F}[\alpha]$ is an integral domain, then $\mathbb{F}[\alpha]/(p)$ **TODO**

Any homomorphism $\phi : E \to \mathbb{E}$ is automatically injective. If $[\mathbb{E} : \mathbb{F}] < \infty$, then $\phi$ is also surjective.

**Theorem.** *If $\mathbb{E}/\mathbb{F}$ is any finite extension of fields, then $\#Aut(\mathbb{E}/\mathbb{F}) \leq [\mathbb{E} : \mathbb{F}]$.*

*Proof.* Let $M$ be a fixed estension of $\mathbb{F}$. (??) **TODO**
By induction on the number of generators for $\mathbb{E}$ over $\mathbb{F}$. If $\mathbb{E} = \mathbb{F}(\alpha) = \mathbb{F}[\alpha]$, let $d$ be the degree of extension of $\mathbb{E}$ (which is equal to the degree of the minimal polynomial $p_\alpha \in \mathbb{F}[x]$ of $\alpha$). By definition of $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$, $\phi$ is only determined by its values on $\alpha$. Moreover, $\alpha$ can only be mapped to a root of $p_\alpha$. Since $\alpha$ has at most $d$ roots, then there are at most $d$ possible distinct $\phi$ in $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$. Therefore, $\#\mathrm{Aut}(\mathbb{E}/\mathbb{F}) \leq [\mathbb{E} : \mathbb{F}]$.
Assumer that it holds for $n$ and let's prove it for $n+1$. Let $\mathbb{E} = \mathbb{F}(\alpha_1, ..., \alpha_{n+1})$ and $\mathbb{F}'(\alpha_1, ..., \alpha_n)$. If $\mathbb{F}' = \mathbb{E}$, then we are done. Thus, we have that $\mathbb{E} = \mathbb{F}'(\alpha_{n+1})$. Let $[\mathbb{F}' : \mathbb{F}] = d_1$ and $[\mathbb{E} : \mathbb{F}'] = d_2$. Let $g \in \mathbb{F}'[x]$ be the minimum polynomial of $\alpha_{n+1}$, then $\deg g = d_2$. By the induction hypothesis, we know that $\#\mathrm{Hom}()$ **TODO**!! ∎

**Definition** (Galois Extensions)**.** *An extension $\mathbb{E}/\mathbb{F}$ is a Galois extension if $\#Aut(\mathbb{E}/\mathbb{F}) = [\mathbb{E} : \mathbb{F}]$. In that case, we write $Gal(\mathbb{E}/\mathbb{F})$ to mean $Aut(\mathbb{E}/\mathbb{F})$.*

**Example:**

- Take $\mathbb{E} = \mathbb{C}$ and $\mathbb{F} = \mathbb{R}$, then $[\mathbb{E} : \mathbb{F}] = 2$. Moreover, beside the identity from $\mathbb{C}$ to $\mathbb{C}$, we know that the conjugation map is contained in $\mathrm{Aut}(\mathbb{C}/\mathbb{R})$. Therefore, $\mathrm{Aut}(\mathbb{C}/\mathbb{R})$ contains two maps so $\mathrm{Aut}(\mathbb{C}/\mathbb{R})$ is a Galois extension.

- Take $\mathbb{F} = \mathbb{Q}$ and $\mathbb{E} = \mathbb{Q}(\sqrt[3]{2})$, then the automorphisms in $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$ must map $\sqrt[3]{2}$ to a root of $x^3 - 2$ in $\mathbb{E}$. However, $\sqrt[3]{2}$ is the only element of $\mathbb{Q}(\sqrt[3]{2})$ with this property. Therefore, $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$ only contains the identity map. It follows that this extension is not Galois.

- If we let $\zeta^3 = 1$, then its minimum polynomial is $x^2 + x + 1$. **TODO**