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 α, i.e., $\mathbb{F}[\alpha]$ is the intersection of all the fields containing both $\mathbb{F}$ and α. Similarly, we denote by $\mathbb{F}(\alpha)$ the field generated by $\mathbb{F}$ and α. 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 ∞-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 α 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 λ_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 (+, -, ×, division) and square roots.*

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 α is not constructible by ruler and compass.*

Proof. Suppose that α is constructible, then there are finite field extensions

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

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 $\alpha = \cos(2\pi/9)$:

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