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 only take notes 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 Preliminaries

This section was not part of the lectures but I chose to include it in my notes. The goal is to make an inventory of the non-obvious results used latter that would break the rythm if explained in the middle of the following sections.

- Kronecker Construction
- Properties of the minimal polynomial over $\mathbb{F}$ of an element in the field extension $\mathbb{E}$.
- Given $f, g \in \mathbb{F}[x]$, the difference between the gcd as polynomials over $\mathbb{F}$ and polynomials over $\mathbb{E}$. Prove that they are equal and hence, the gcd only depends on the ground field. To prove this, $g_{\mathbb{F}}$ divides $g_{\mathbb{E}}$ since it is a polynomial in $\mathbb{F}[x] \subset \mathbb{E}[x]$ which divides both f and g. Moreover, $g_{\mathbb{E}}$ divides $g_{\mathbb{F}}$ since $g_{\mathbb{F}}$ can be written as a linear combination of f and g. Thus, since they are monic, it follows that $g_{\mathbb{E}} = g_{\mathbb{F}}$.
- The cardinality of a field is always a power of a prime.

1.1 Fields

TODO

Theorem. *Let $\mathbb{F}$ be a finite field, then $\mathbb{F}^\times$ is a cyclic group.*

Proof. Since $\mathbb{F}^\times$ is a finite abelian group, then we can apply the Fundamental Theorem of Finitely Generated Abelian Groups to obtain that

$$\mathbb{F}^\times \cong \mathbb{Z}^{d_1} \times \cdots \times \mathbb{Z}^{d_t}$$

where d_i divides d_{i+1} for all $i \in [\![1, t-1]\!]$. It follows that $\mathbb{F}^\times$ contains an element of order d_t (take $(0, 0, ..., 0, 1)$) and every element has an order that divides d_t. Thus, $\alpha^n = 1$ for all $\alpha \in \mathbb{F}^\times$. Consider the polynomial $p(x) = x^{d_t} - 1 \in \mathbb{F}[x]$, notice that it has at most $\deg p = d_t$ roots and that it all the elements of $\mathbb{F}^\times$ are roots so $\#\mathbb{F}^\times \leq d_t$. Moreover, since $\mathbb{F}^\times$ contains an element of order d_t, then it has a subgroup of cardinality d_t which shows that $d_t \leq \#\mathbb{F}^\times$. Thus, combining the two previous inequalities, $\mathbb{F}^\times$ is a group of cardinality d_t which contains an element of order d_t, it follows that $\mathbb{F}^\times$ is cyclic. ■

1.2 Irreducible Polynomials

TODO

Proposition. *$g(x)$ irreducible if and only if $x^n g(1/x)$ irreducible.*

1.3 Formal Derivative and Multiple Roots

Definition (Formal Derivative)**.** *Given a field $\mathbb{F}$ and a polyomial $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{F}[x]$, we define the polynomial $f'(x) = \sum_{i=0}^{n-1} (i+1) a_{i+1} x^i \in \mathbb{F}[x]$ and call it the formal derivative of f.*

Proposition. *Given two polynomials $f, g \in \mathbb{F}[x]$, their respective formal derivatives satisfy the following properties:*

1. $(f+g) = f' + g'$.
2. $(fg)' = f'g + fg'$.
3. $(f^n)' = nf'f^{n-1}$.

Proof. 1. **TODO**

2. **TODO**

3. **TODO**

■

Theorem. *Given a field $\mathbb{F}$, a polynomial $f \in \mathbb{F}[x]$ and a root $\alpha \in \mathbb{F}$ of f, then $(x-\alpha)^2$ divides f if and only if $f'(\alpha) = 0$.*

Proof. **TODO** ■

2 Fields Extensions

2.1 Definitions and Examples

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 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 rings 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 $n \cdot m$. ■

2.2 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. Using fields, we can say that a number is constructible if it is contained in a sequence of quadratic extensions of $\mathbb{Q}$.*

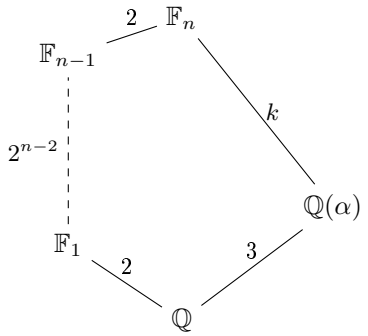
The set of constructible elements by ruler and compass is an extension of $\mathbb{Q}$ of infinite degree. The goal is to characterize this extension.

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

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

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 $[F_{i+1} : F_i] = 2$ 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:



By the Multiplicativity of the degree, it follows that $2^n = 3k$ which is clearly a contradiction. Therefore, by contradiction, α is not constructible. ■

Example:

- (Duplicating the cube) It is equivalent to determine if $\alpha = \sqrt[3]{2}$ is constructible. Notice that α is a root of $p(x) = x^3 - 2$ which is irreducible in $\mathbb{Q}$ so α cannot be constructible.

- (Trisection of angle) To prove that it is impossible to trisect angles, let's show in particular that it is impossible to trisect the angle $\theta = 2\pi/3$. Equivalently, let's determine if $\alpha = \cos(2\pi/9)$ is constructible. Recall the following trigonometric identity:

$$\cos(\theta) = 4\cos^3\left(\frac{\theta}{3}\right) - 3\cos\left(\frac{\theta}{3}\right)$$

  which gives us that α is a root of the polynomial $4x^3 - 3x + \frac{1}{2}$. Equivalently, α is a root of the polynomial $p \in \mathbb{Q}[x]$ where $p(x) = 8x^3 - 6x + 1$. Let's prove that p is irreducible over $\mathbb{Q}$. Notice that it is equivalent to prove that the polynomial $q(x) = x^3 - 6x^2 + 8$ is irreducible. Since q has coefficients in $\mathbb{Z}$, then it suffices to show that q is irreducible over $\mathbb{Z}$. To do so, suppose that there exist integers a, b, c such that $q(x) = (x + a)(x^2 + bx + c)$. Regrouping the terms gives us that $ac = 8$ so $a = \pm 1, \pm 2, \pm 4, \pm 8$. However, notice that if we plug-in any of these numbers into q, we never get 0, a contradiction. Therefore, p is irreducible so α is not constructible.

3 Automorphism Group

Definition (Algebraic Numbers)**.** *Let $\mathbb{E}/\mathbb{F}$ be a finite extension. An element $\alpha \in \mathbb{E}$ is algebraic over $\mathbb{F}$ if α 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 $x^2 + 1 \in \mathbb{Q}[x]$.

- π 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 $\alpha \in \mathbb{E}$ and 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 $\beta_0, ..., \beta_n \in \mathbb{F}$ such that $\beta_0 + \beta_1\alpha + \beta_2\alpha^2 + ... + \beta_n\alpha^n = 0$. Thus, if we let $p(x) = \beta_0 + \beta_1 x + ... + \beta_n x^n \in \mathbb{F}[x]$, then $p(\alpha) = 0$ which proves that α is algebraic over $\mathbb{F}$. ■

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

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

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 α has only finitely many translates by the action of $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$. By the previous Lemma, we know that α is algebraic so there is a polynomial $a_n x^n + ... + a_0 \in \mathbb{F}[x]$ satisfied by α. 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 σ on both sides of the previous equation gives us

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

Using the fact that σ preserves addition and multiplication, we get

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

Finally, since σ 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 α 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 α has a finite orbit. ■

Remark: Notice that the same proof can be applied if $\mathbb{E}/\mathbb{F}$ is an 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 σ on the generators, then we know the behavior of σ on $\mathbb{E}$. Since there are finitely many generators and each generator has a finite orbit, then there are finitely many possible σ. ■

Example:

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

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

  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 $\mathbb{F}[\alpha]/(p)$ is an integral domain which is also a finite vector space. Therefore, it is a field and we get that

$$\mathbb{E} = \mathbb{F}(\alpha) = \mathbb{F}[\alpha] \cong \mathbb{F}[x]/(p).$$

Remark: Any homomorphism $\phi : \mathbb{E} \to \mathbb{E}$ is automatically injective. If $[\mathbb{E} : \mathbb{F}] < \infty$, then ϕ is also surjective since it can also be seen as an injective linear transformation.

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

Proof. Let's prove by induction on n that $\#\operatorname{Hom}_{\mathbb{F}}(\mathbb{K}, \mathbb{E}) \leq [\mathbb{K} : \mathbb{F}]$ where $\mathbb{K} = \mathbb{F}(\alpha_1, ..., \alpha_n)$. For the case $n = 1$, we have $\mathbb{K} = \mathbb{F}(\alpha)$ for some element α. We already observed that each $\varphi \in \operatorname{Hom}_{\mathbb{F}}(\mathbb{K}, \mathbb{E})$ is completely determined by where it maps α. Moreover, we know that φ must map α to a root of the minimal polynomial $p \in \mathbb{F}[x]$ of α so there are at most $\deg p$ elements in $\operatorname{Hom}_{\mathbb{F}}(\mathbb{K}, \mathbb{E})$. In other words, $\#\operatorname{Hom}_{\mathbb{F}}(\mathbb{K}, \mathbb{E}) \leq \deg p$. Finally, we also observed that $\mathbb{K} \cong \mathbb{F}[x]/(p)$ so $[\mathbb{K} : \mathbb{F}] = \deg p$. Therefore, $\#\operatorname{Hom}_{\mathbb{F}}(\mathbb{K}, \mathbb{E}) \leq [\mathbb{K} : \mathbb{F}]$.

For the Induction Step, suppose that it holds for a natural number n and consider case $n+1$. We have $\mathbb{K} = \mathbb{F}(\alpha_1, ..., \alpha_{n+1})$ and define $\mathbb{F}' = \mathbb{F}(\alpha_1, ..., \alpha_n)$. By the Induction Hypothesis, we know that $\#\operatorname{Hom}_{\mathbb{F}}(\mathbb{F}', \mathbb{E}) \leq [\mathbb{F}' : \mathbb{F}]$. If $\mathbb{F}' = \mathbb{K}$, then we are done by the Induction Hypothesis, otherwise, we have $\mathbb{K} = \mathbb{F}'(\alpha_{n+1})$. If we define $d_1 = [\mathbb{F}' : \mathbb{F}]$ and $d_2 = [\mathbb{K} : \mathbb{F}']$, we can visualize the set up so far by the following diagram:

$$\begin{array}{c} \mathbb{K} \\ \big| \, d_2 \\ \mathbb{F}' \\ \big| \, d_1 \\ \mathbb{F} \end{array}$$

Let $g \in \mathbb{F}'[x]$ be the minimal polynomial of α_{n+1}, then $\deg g = [\mathbb{K} : \mathbb{F}'] = d_2$. Write g as

$$g(x) = \lambda_{d_2} x^{d_2} + \lambda_{d_2-1} x^{d_2-1} + ... + \lambda_1 x + \lambda_0.$$

where the λ_i's are in $\mathbb{F}'$. We can easily notice that any element of $\operatorname{Hom}_{\mathbb{F}}(\mathbb{K}, \mathbb{E})$ restricted to $\mathbb{F}'$ is an element of $\operatorname{Hom}_{\mathbb{F}}(\mathbb{F}', \mathbb{E})$. Hence, to have an estimation on the size of $\operatorname{Hom}_{\mathbb{F}}(\mathbb{K}, \mathbb{E})$, we can determine in how many ways each element of $\operatorname{Hom}_{\mathbb{F}}(\mathbb{F}', \mathbb{E})$ can be extended to an element of $\operatorname{Hom}_{\mathbb{F}}(\mathbb{K}, \mathbb{E})$. Fix a $\varphi \in \operatorname{Hom}_{\mathbb{F}}(\mathbb{F}', \mathbb{E})$ and let $\varphi_0 \in \operatorname{Hom}_{\mathbb{F}}(\mathbb{K}, \mathbb{E})$ be an extension of φ. Notice that for all

$$K = a_0 + a_1 \alpha_{n+1} + ... + a_{d_2-1} \alpha_{n+1}^{d_2-1}$$

in $\mathbb{K} = \mathbb{F}'(\alpha_{n+1})$ where the a_i's are in $\mathbb{F}'$, we can apply φ_0 to get

$$\varphi_0(K) = \varphi_0(a_0) + \varphi_0(a_1)\varphi_0(\alpha_{n+1}) + ... + \varphi_0(a_{d_2-1})\varphi_0(\alpha_{n+1})^{d_2-1}.$$

Using the fact that $\varphi_0|_{\mathbb{F}'} = \varphi$, we get

$$\varphi_0(K) = \varphi(a_0) + \varphi(a_1)\varphi_0(\alpha_{n+1}) + ... + \varphi(a_{d_2-1})\varphi_0(\alpha_{n+1})^{d_2-1}.$$

Since the previous equation expresses $\varphi_0(K)$ in terms of $\varphi_0(\alpha_{n+1})$ for an arbitrary $K \in \mathbb{K}$, then to extend φ to φ_0, it suffices chose where α_{n+1} gets mapped to. From that, recall that $g(\alpha_{n+1}) = 0$ and apply φ_0 on both sides to obtain

$$\varphi(\lambda_{d_2})\varphi_0(\alpha_{n+1})^{d_2} + ... + \varphi(\lambda_1)\varphi_0(\alpha_{n+1}) + \varphi(\lambda_0) = 0.$$

Thus, if we define $\varphi g \in \mathbb{E}[x]$ as the polynomial g with the coefficients λ_i replaced by the coefficients $\varphi(\lambda_i)$, we get that $(\varphi g)(\varphi_0(\alpha_{n+1})) = 0$. It follows that φ_0 must map α_{n+1} to a root of φg which has degree d_2. Since φ_0 is only determined by its value at α_{n+1}, then φ can have at most d_2 extensions in $\mathrm{Hom}_{\mathbb{F}}(\mathbb{K}, \mathbb{E})$. Therefore, by the Induction Hypothesis, since there are at most d_1 elements in $\mathrm{Hom}_{\mathbb{F}}(\mathbb{F}', \mathbb{E})$, then by the multiplicativity of the degree:

$$\#\,\mathrm{Hom}_{\mathbb{F}}(\mathbb{K}, \mathbb{E}) \leq d_1 d_2 = [\mathbb{F}' : \mathbb{F}][\mathbb{K} : \mathbb{F}'] = [\mathbb{K} : \mathbb{F}].$$

This concludes our proof by induction. To prove the actual claim, notice that since $\mathbb{E}$ is a finite extension, then it can be written as $\mathbb{F}(\alpha_1, ..., \alpha_n)$ where $\alpha_1, ..., \alpha_{[\mathbb{E}:\mathbb{F}]}$ is the basis of $\mathbb{E}$ as a $\mathbb{F}$-vector space. Therefore, we can plug-in $\mathbb{K} = \mathbb{E}$ to get

$$\#\,\mathrm{Aut}(\mathbb{E}/\mathbb{F}) = \#\,\mathrm{Hom}_{\mathbb{F}}(\mathbb{E}, \mathbb{E}) \leq [\mathbb{E} : \mathbb{F}]$$

which proves our claim. ■

4 Galois Extensions

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:

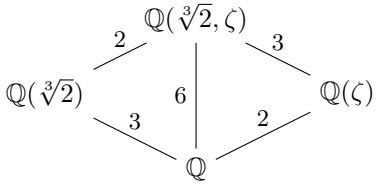
- Take $\mathbb{E} = \mathbb{C}$ and $\mathbb{F} = \mathbb{R}$, then $[\mathbb{E} : \mathbb{F}] = 2$. Moreover, beside the identity from $\mathbb{C}$ to $\mathbb{C}$, we know that the conjugation map is contained in $\mathrm{Aut}(\mathbb{C}/\mathbb{R})$. Therefore, $\mathrm{Aut}(\mathbb{C}/\mathbb{R})$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

- Take $\mathbb{F} = \mathbb{Q}$ and $\mathbb{E} = \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$, 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.

- Let ζ be a cube root of 1 distinct than 1, then the minimal polynomial of ζ over $\mathbb{Q}$ can be found by writing

  $$\zeta^3 - 1 = 0 \implies (\zeta - 1)(\zeta^2 + \zeta + 1) = 0 \implies \zeta^2 + \zeta + 1 = 0$$

  and noticing that $x^2 + x + 1$ is irreducible oever $\mathbb{Q}$ (since it is irreducible over $\mathbb{R}$). It follows that the minimal polynomial of ζ is $p(x) = x^2 + x + 1$. Hence, $\mathbb{Q}(\zeta) \subset \mathbb{C}$ is an extension of $\mathbb{Q}$ of degree 2. Similarly, if we consider the extension $\mathbb{Q}(\sqrt[3]{2}, \zeta) = \mathbb{Q}(\sqrt[3]{2})(\zeta)$ of $\mathbb{Q}(\sqrt[3]{2})$, then p stays irreducible so this extension also has degree 2. Therefore, by the following diagram and by the multiplicativity of the degree, $\mathbb{Q}(\sqrt[3]{2}, \zeta)$ is an extension of $\mathbb{Q}(\zeta)$ of degree 2:



Let's count the number of elements in $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2},\zeta)/\mathbb{Q})$. Let $\phi \in \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2},\zeta)/\mathbb{Q})$, then $\varphi(\zeta)$ must be a root of x^2+x+1 so $\varphi(\zeta)$ can be mapped to ζ and $\overline{\zeta}$. Similarly, $\sqrt[3]{2}$ must be mapped to a root of x^3-2. But since $\zeta^3=1$, then $\varphi(\sqrt[3]{2})$ can be $\sqrt[3]{2}$, $\zeta\sqrt[3]{2}$ or $\overline{\zeta}\sqrt[3]{2}$. Since φ is only determined by $\varphi(\zeta)$ and $\varphi(\sqrt[3]{2})$, then there are 6 elements in $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2},\zeta)/\mathbb{Q})$. Therefore, it is a Galois extension.

- Let's determine the structure of $G = \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2},\zeta)/\mathbb{Q})$. Since it has cardinality 6, then it is either $\mathbb{Z}/6\mathbb{Z}$ or S_3. Let's show that it is S_6 by showing that no element has order 6. Let $\varphi \in G$, if $\varphi(\zeta)=\zeta$ or $\varphi(\sqrt[3]{2})=\sqrt[3]{2}$, then φ has at most order 3. Hence, the only possible candidates for an element of order 6 in G are φ_1 and φ_2 where $\varphi_1(\zeta)=\varphi_2(\zeta)=\overline{\zeta}$, $\varphi_1(\sqrt[3]{2})=\zeta\sqrt[3]{2}$ and $\varphi_2(\sqrt[3]{2})=\overline{\zeta}\sqrt[3]{2}$. Notice that in both cases, $\overline{\zeta}$ is mapped to ζ because it can only be mapped to a root of $x^2+x+1=(x-\zeta)(x-\overline{\zeta})$ and if it was mapped to $\overline{\zeta}$, then it would break the fact that it is injective. Hence,

$$\varphi_1^2(\zeta)=\varphi_1(\overline{\zeta})=\zeta \quad \text{and} \quad \varphi_1^2(\sqrt[3]{2})=\varphi_1(\zeta)\varphi_1(\sqrt[3]{2})=\overline{\zeta}\zeta\sqrt[3]{2}=\sqrt[3]{2}$$

and

$$\varphi_2^2(\zeta)=\varphi_2(\overline{\zeta})=\zeta \quad \text{and} \quad \varphi_2^2(\sqrt[3]{2})=\varphi_2(\overline{\zeta})\varphi_2(\sqrt[3]{2})=\zeta\overline{\zeta}\sqrt[3]{2}=\sqrt[3]{2}$$

so $\varphi_1^2=\varphi_2^2=id$. Thus, both φ_1 and φ_2 have order 2. It follows that G has no element of order 6 so G must be S_3.

Galois Extensions can be seen as field extensions on which we can be read off a lot of structure and properties from the symmetries. The next theorem justifies this way of thinking about Galois extensions. In the next propositions and definitions, fix a field $\mathbb{F}$, a finite Galois extension $\mathbb{E}$ and denote by G the Galois Group of $\mathbb{E}/\mathbb{F}$.

Notation: $\mathbb{E}^G = \{\alpha \in \mathbb{E} : g(\alpha)=\alpha \text{ for all } g \in G\}$ is the set of fixed points of G.

Lemma. *$\mathbb{E}^G$ is a subfield of $\mathbb{E}$ which contains $\mathbb{F}$.*

Proof. All the elements of $\mathbb{F}$ are fixed by all the elements of G so $\mathbb{F} \subset \mathbb{E}^G$. Moreover, by definition, we already know that $\mathbb{E}^G \subset \mathbb{E}$. Hence, it remains to show that $\mathbb{E}^G$ is a subfield of $\mathbb{E}$, i.e., that $\mathbb{E}^G$ contains 0, 1, is closed under addition, multiplication and respective inverses. Since $\mathbb{F} \subset \mathbb{E}^G$, then in particular $0,1 \in \mathbb{E}^G$. Since the elements of G are field homomorphisms, then for all $x,y \in \mathbb{E}^G$ and $\varphi \in G$, we have $\varphi(x+y)=\varphi(x)+\varphi(y)=x+y$ and $\varphi(xy)=\varphi(x)\varphi(y)=xy$ so $\mathbb{E}^C$ is closed under addition and multiplication. Similarly, for all $x,y \in \mathbb{E}^G$ with $y \neq 0$ and $\varphi \in G$, we have $\varphi(-x)=-\varphi(x)=-x$ and $\varphi(y^{-1})=\varphi(y)^{-1}=y^{-1}$ so $\mathbb{E}^G$ is closed under additive and multiplicative inverses. Therefore, $\mathbb{E}^G$ is a subfield of $\mathbb{E}$. ∎

Theorem. $\mathbb{E}^G = \mathbb{F}$.

Proof. By the previous lemma, we have the following tower of extensions

$$\begin{array}{c} \mathbb{E} \\ \big| d_2 \\ \mathbb{E}^G \\ \big| d_1 \\ \mathbb{F} \end{array}$$

where $d_1 = [\mathbb{E}^G : \mathbb{F}]$ and $d_2 = [\mathbb{E} : \mathbb{E}^G]$. Let's show that $d_1 = 1$. Consider the set $\mathrm{Aut}(\mathbb{E}/\mathbb{E}^G)$, then it must contain G. Moreover, by the last theorem of the previous section, $\#\,\mathrm{Aut}(\mathbb{E}/\mathbb{E}^G) \leq d_2 = [\mathbb{E} : \mathbb{E}^G] \leq [\mathbb{E} : \mathbb{F}]$. Thus, we obtain:

$$[\mathbb{E} : \mathbb{F}] = \#G \leq \#\,\mathrm{Aut}(\mathbb{E}/\mathbb{E}^G) \leq [\mathbb{E} : \mathbb{F}]$$

which implies that $\#\,\mathrm{Aut}(\mathbb{E}/\mathbb{E}^G) = [\mathbb{E} : \mathbb{E}^G] = d_1 d_2 \leq d_2$. It follows that $d_1 = 1$. ■

Theorem. *If f is an irreducible polynomial in $\mathbb{F}[x]$ which has a root in $\mathbb{E}$, then f splits completely into linear factors in $\mathbb{E}[x]$.*

Proof. Let $r \in \mathbb{E}$ be a root of f, then it is easy to see (using the Euclidean Algorithm) that f is the minimal pokynomial of r over $\mathbb{F}$. Consider the orbit $\{r_1, ..., r_n\}$ of r under the action of G on $\mathbb{E}$ and define the polynomial $g(x) = \prod(x - r_i) \in \mathbb{E}[x]$. Notice that if we expand the product, we get that $g(x) = x^n - \sigma_1 x^{n-1} + ... + (-1)^n \sigma_n$ where the σ_i's are the elementary symmetric functions in $r_1, ..., r_n$. It follows that for all $1 \leq i \leq n$, $\sigma_i \in \mathbb{E}^G = \mathbb{F}$ since by symmetry σ_i is fixed by all the elements of G. Thus, $g \in \mathbb{F}[x]$ with $g(r) = 0$ so it follows by minimality of f that f divides g. Therefore, in $\mathbb{E}[x]$, f divides a product of linear factors so f must itself be a product of linear factors. Hence, f splits completely in $\mathbb{E}[x]$. ■

Terminology: If a field extension has the property that any irreducible polynomial with the polynomial ring of the ground field with a root in the extension splits completely in the polynomial ring of the extension, we say that the extension is normal.

Using this terminology, the previous theorem states that any Galois extension is normal.

5 Splitting Fields

5.1 Existence and Uniqueness

Definition. *Given a field $\mathbb{F}$ and a polynomial $f \in \mathbb{F}[x]$, a splitting field of f is an extension $\mathbb{E}/\mathbb{F}$ satisfying*

(a) f factors into linear factors in $\mathbb{E}[x]$.

(b) E is generated as a field by the roots $r_1, ..., r_n$ of f.

Theorem (Existence)**.** *Given a field $\mathbb{F}$ and a polynomial f, there exists an extension $\mathbb{E}/\mathbb{F}$ which is a splitting field of f.*

Proof. Let's prove it by induction on the degree of f. For the base case, $n = 1$, if f has degree 1, then its unique root r must be in $\mathbb{F}$ already so $\mathbb{E} = \mathbb{F}(r) = \mathbb{F}$ is a splitting field of f. For the Inductive Step, assume that the statement holds for polynomials of degree n and suppose that f has degree $n+1$. Let p be an irreducible factor of f and construct the field $L = \mathbb{F}[x]/(p) = \mathbb{F}(r_0)$ which contains a root r_0 of p. It follows that $f(x)$ can be written as $(x - r)g(x)$ in $L[x]$ where g has degree n. Hence, by applying the inductive hypothesis, we can construct a splitting field $\mathbb{E}/L$ of g. It follows that $g(x)$ can be written as $(x - r_1)\dots(x - r_n)$ in $\mathbb{E}[x]$ so $f(x)$ splits completely into $(x - r_0)(x - r_1)\dots(x - r_n)$ in $\mathbb{E}[x]$. Moreover, since $\mathbb{E}$ is generated by L and the roots of g, then

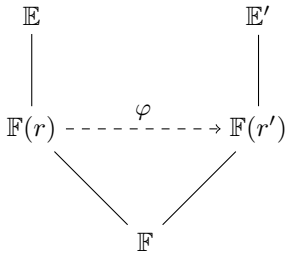
$$\mathbb{E} = L(r_1, ..., r_n) = \mathbb{F}(r_0)(r_1, ..., r_n) = \mathbb{F}(r_0, r_1, ..., r_n)$$

which proves that $\mathbb{E}$ is generated by the roots of f. Therefore, by induction, we can always construct a splitting field given a field $\mathbb{F}$ and a polynomial $f \in \mathbb{F}[x]$. ■

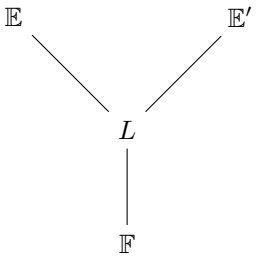
Remark: It is very hard to compute the degree of a splitting field since it depends very subtly on the structure of f. However, by the multiplicativity of the degree, the degree of the splitting field must be smaller than $(\deg f)!$.

Theorem (Uniqueness)**.** *Given a field $\mathbb{F}$, a polynomial $f \in \mathbb{F}[x]$ and two splitting fields $\mathbb{E}$ and $\mathbb{E}'$ of f over $\mathbb{F}$, then $\mathbb{E}$ and $\mathbb{E}'$ are isomorphic as extensions of $\mathbb{F}$, i.e., there exists a field isomorphism from $\mathbb{E}$ to $\mathbb{E}'$ that fixes $\mathbb{F}$.*

Proof. Let's proceed by induction on $n = \deg f$. For the base case, if $\deg f = 1$, then we simply have $\mathbb{E} = \mathbb{F} = \mathbb{E}'$ so we are done. Assume now that the claim holds for n and suppose that $\deg f = n + 1$. Let $p \in \mathbb{F}[x]$ be an irreducible factor of the polynomial f, let r be a root of p in $\mathbb{E}$ and let r' be a root of p in $\mathbb{E}'$. We have the following diagram:



Notice that both $\mathbb{F}(r)$ and $\mathbb{F}(r')$ are isomorphic to $\mathbb{F}[x]/(p)$ so in particular, $\mathbb{F}(r) \cong \mathbb{F}(r')$. Let $\varphi : \mathbb{F}(r) \to \mathbb{F}(r')$ be such an isomorphism. Hence, if we let $L = \mathbb{F}(r) = \mathbb{F}(r')$, our diagram becomes



It follows that $\mathbb{E}$ and $\mathbb{E}'$ can be seen of splitting fields of a polynomial in $L[x]$ of degree n so by the inductive hypothesis, $\mathbb{E}$ and $\mathbb{E}'$ are isomorphic as extensions of L. Therefore, $\mathbb{E}$ and $\mathbb{E}'$ are isomorphic as extensions of $\mathbb{F}$. ■

We can now talk about *the* splitting field of a polynomial f over a field $\mathbb{F}$. The next theorem justifies the link between splitting fields and Galois extensions.

Proposition. *If $\mathbb{E}/\mathbb{F}$ is Galois, then $\mathbb{E}$ is the splitting field of a polynomial $f \in \mathbb{F}[x]$.*

Proof. Since $[\mathbb{E} : \mathbb{F}] < \infty$, then we can let $\alpha_1, ..., \alpha_n$ be a finite set of generators for $\mathbb{E}/\mathbb{F}$. Since every element of $\mathbb{E}$ is algebraic over $\mathbb{F}$, then we can let $f_1, ..., f_n$ be irreducible polynomials in $\mathbb{F}[x]$ having respective roots $\alpha_1, ..., \alpha_n$ and define $f = f_1 \cdot \cdots \cdot f_n$. In $\mathbb{E}[x]$, all the f_i's factor completely and therefore so does f. Moreover, the roots of f in $\mathbb{E}$ generate $\mathbb{E}$ so $\mathbb{E}$ is the splitting field of f over $\mathbb{F}$. ■

5.2 Application to Finite Fields

Recall that if $\mathbb{F}$ is a finite field, then it must have a charachteristic equal to a prime number p which implies that $\mathbb{F}$ contains a copy of $\mathbb{Z}/p\mathbb{Z}$. From this, we can see $\mathbb{F}$ as a vector space over $\mathbb{Z}/p\mathbb{Z}$ which implies that $\#\mathbb{F}$ must be a power of p. However, given any prime power p^n can we construct fields of cardinality p^n ? Are they necessarily isomorphic one to another ?

Theorem. *Given a prime p and a natural number n, there is a unique field of cardinality p^n up to isomorphism.*

One possible approach would be to find a polynomial $f \in \mathbb{F}_p[x]$ which is irreducible of degree n and construct $\mathbb{F} = \mathbb{F}_p[x]/(f)$ which is the desired field. However, it is not clear that there exists such a polynomial f or there might be several of them. We will not use this approach in the proof. The theory of splitting fields we developed gives us the perfect tools to prove this theorem.

Proof. Let $\mathbb{F}$ be the splitting field of $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$, let's show that $\mathbb{F}$ has cardinality p^n. First, notice that f has distinct roots in $\mathbb{F}$ since its formal derivative is identically -1 (so no multiple roots). Since f splits completely in $\mathbb{F}$, then f has p^n roots $\alpha_1, ..., \alpha_{p^n}$. But notice that the roots of f in $\mathbb{F}$ form a field which contains $\mathbb{F}_p$. It follows that $\mathbb{F} = \mathbb{F}_p(\alpha_1, ..., \alpha_{p^n})$ is simply the set of roots of f in $\mathbb{F}$. Therefore, $\mathbb{F}$ has cardinality p^n which proves the existence part of the claim.

Now, let $\mathbb{F}'$ be a field of cardinality p^n, then $\mathbb{F}'$ must have characteristic p (because we know that $\#\mathbb{F}' = q^m$ where q is its characteristic which is a prime number, $q^m =$

$p^n \implies \text{char}(\mathbb{F}') = p$). It follows that $\mathbb{F}'$ contains $\mathbb{F}_p$ as a subfield so it is an extension of $\mathbb{F}_p$. Moreover, notice that all the elements of $\mathbb{F}'$ are roots of the polynomial $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$ so f splits completely in $\mathbb{F}'$ (since $\#\mathbb{F}' = \deg f$). And finally, since the elements of $\mathbb{F}'$ are precisely the roots of the f, then we can say that $\mathbb{F}'$ is generated by the roots of f. It follows that $\mathbb{F}'$ is the splitting field of f over $\mathbb{F}$. By uniqueness of the splitting field, we have that $\mathbb{F}' \cong \mathbb{F}$. Since every field of cardinality p^n is isomorphic to $\mathbb{F}$, then the field of cardinality p^n is unique up to isomorphism. ■

Let's now determine if $\mathbb{F}_q$ (where $q = p^n$) is a Galois extension of $\mathbb{F}_p$. To do so, we need to determine the number of automorphisms in the automorphism group $\text{Aut}(\mathbb{F}_q/\mathbb{F}_p)$. To understand this group, we will heavily rely on the important observation that in $\mathbb{F}_q$, $(x+y)^p = x^p + y^p$. This equation means that taking the pth power is not only well-behaved for multiplication but also for addition in $\mathbb{F}_q$. This motivates the following proposition and definition.

Proposition. *The map $\mathbb{F}_q \to \mathbb{F}_q : x \mapsto x^p$ is an automorphism.*

Proof. First, notice that this map trivialy preserves multiplication but also preserves addition by our previous discussion. Hence, it remains to show that it fixes $\mathbb{F}_p$. To see why it is the case, recall Fermat's Little Theorem which states that for any $x \in \mathbb{F}_p^\times$, $x^{p-1} = 1$. Multiplying by x on both sides gives us $x^p = x$ for all $x \in \mathbb{F}_p^\times$. Since this equation is also satisfied by $x = 0$, then the map fixes F_p. ■

Definition (Frobenius Automorphism)**.** *The map $\varphi : \mathbb{F}_q \to \mathbb{F}_q$ defined by $x \mapsto x^p$ is called the Frobenius Automorphism. Indeed, by the previous proposition, $\varphi \in Aut(\mathbb{F}_q/\mathbb{F}_p)$.*

The Frobenius Automorphism, gives us a concrete element in $\text{Aut}(\mathbb{F}_q/\mathbb{F}_p)$. This lets us understand the group $\text{Aut}(\mathbb{F}_q/\mathbb{F}_p)$ as shown by the following theorem where the Frobenius Automorphism plays a crucial role.

Theorem. *F_q is a Galois extension of $\mathbb{F}_p$. The Galois Group of the extension is $\mathbb{Z}/n\mathbb{Z}$ and is generated by the Frobenius Automorphism.*

Proof. First, we already have that $\text{Aut}(\mathbb{F}_q/\mathbb{F}_p)$ is finite since $\#\,\text{Aut}(\mathbb{F}_q/\mathbb{F}_p) \leq [\mathbb{F}_q : \mathbb{F}_p] = n$. Let's find the order of the Frobenius Automorphism φ, which must be finite by the previous observation. For all $k \in \mathbb{N}$, we have that $\varphi^k(x) = x^{p^k}$. Moreover, since $\mathbb{F}_q^\times$ is cyclic and of order $p^n - 1$, then there is a $\alpha \in \mathbb{F}_q$ such that $\alpha^{p^n} = \alpha$ but $\alpha^{p^k} \neq \alpha$ for all $k < n$. Hence, if we denote by k_0 the order of φ, then we must have $\varphi^{k_0} = id$ and in particular $\alpha^{p^{k_0}} = \varphi^{k_0}(\alpha) = \alpha$. It follows that k_0 must be at least greater than or equal to n. Moreover, since $\mathbb{F}_q^\times$ has $p^n - 1$ elements, then $x^{p^n - 1} = 1$ for all $x \in \mathbb{F}_q^\times$. Equivalently, $\varphi^n(x) = x^{p^n} = x$ for all $x \in \mathbb{F}_q$. Thus, k_0 must be smaller than n. Therefore, k_0 so φ has order n. We obtain the following inequality:

$$n = \#\langle\varphi\rangle \leq \#\,\text{Aut}(\mathbb{F}_q/\mathbb{F}_p) \leq n$$

which lets us conclude that $\#\,\text{Aut}(\mathbb{F}_q/\mathbb{F}_p) = [\mathbb{F}_q : \mathbb{F}_p]$. Therefore, $\mathbb{F}_q/\mathbb{F}_p$ is a Galois extension and its Galois group is cyclic, generated by the Frobenius Automorphism, and hence, isomorphic to $\mathbb{Z}/n\mathbb{Z}$. ■

6 More on Galois Extensions

For the moment, our definition of Galois extensions only applies to finite extensions. However, there is a way of extending this definition to infinite extensions by finding an equivalent definition of Galois extensions that doesn't rely on the finiteness of the degree. Recall that at the end of Section 4, we proved that any Galois extension is normal. Let's make this more precise.

Definition (Normal Extension)**.** *An extension $\mathbb{E}/\mathbb{F}$ is normal if every irreducible polynomial in $\mathbb{F}[x]$ with a root in $\mathbb{E}$ splits into linear factors in $\mathbb{E}[x]$.*

Theorem. *If $\mathbb{E}/\mathbb{F}$ is Galois, then $\mathbb{E}$ is normal over $\mathbb{F}$.*

As we will see, the converse of this theorem is not true. However, we can make it true by adding another assumption on the extension. To make everything clear and precise, we will need to prove the a few theorems.

Definition (Separability)**.** *An extension $\mathbb{E}/\mathbb{F}$ is separable if every irreducible polynomial with a root in $\mathbb{E}$ has no multiple roots.*

Proposition. *If $\mathbb{F}$ has characteristic 0, then every extension of $\mathbb{F}$ is separable.*

Proof. Let $f \in \mathbb{F}[x]$ be an irreducible polynomial with a root $r \in \mathbb{E}$ and suppose that $f(x) = (x-r)^e g(x)$ in $\mathbb{E}[x]$ with $\gcd((x-r), g(x)) = 1$. Consider the formal derivative f' of f and notice that if $e > 1$, then r is again a root of f'. Hence, r is a root of $\gcd(f, f') \in \mathbb{E}[x]$.

$$f(x) = a_n x^n + ... + a_1 x + a_0 \quad \text{and} \quad f'(x) = n a_n x^{n-1} + ... + a_1$$

Recall that f is irreducible in $\mathbb{F}[x]$ so $\gcd(f, f')$ is either f or 1. But since $\gcd(f, f')$ also divides f' which has degree $n-1$, then $\gcd(f, f') = 1$. Therefore, by contradiction, $e = 1$ so α is not a multiple root. ■

The assumption that $\mathbb{F}$ has characteristic 0 was used when asserting that $\deg f' = n - 1$. If $\mathbb{F} = \mathbb{F}_p$ for a prime p and $f(x) = x^p$, then $\deg f' = 0$ so $\gcd(f, f') = f$. When the field don't have characteristic zero, then computing the degree of the formal derivative is not as easy.

Theorem. *If $\mathbb{E}/\mathbb{F}$ is Galois, then it is separable.*

TODO

Proof. Same as for normal. **TODO** ■

Theorem. *If $\mathbb{E}/\mathbb{F}$ is finite, normal and separable, then $\mathbb{E}/\mathbb{F}$ is Galois.*

Proof. Recall our proof that $\#\operatorname{Aut}(\mathbb{E}/\mathbb{F}) \leq [\mathbb{E} : \mathbb{F}]$. We will retrace this proof using the hypothesis of this theorem to replace the inequality with an equality throughout the proof. We will prove by strong induction on $[\mathbb{K} : \mathbb{F}]$ the following statement:

$$\operatorname{Hom}_{\mathbb{F}}(\mathbb{K}, \mathbb{E}) = [\mathbb{K} : \mathbb{F}]$$

where $\mathbb{F} \leq \mathbb{K} \leq \mathbb{E}$. For the Base Case, if $[\mathbb{K} : \mathbb{F}] = 1$, it is trivial (**TODO**). Suppose now that $\mathbb{K}$ is generated by a single element, i.e., $\mathbb{K} = \mathbb{F}(\alpha) = \mathbb{F}[x]/(p)$ with p irreducible, $p(\alpha) = 0$ and $\deg p = [\mathbb{K} : \mathbb{F}]$. But notice that since $\mathrm{Hom}_{\mathbb{F}}(\mathbb{K}, \mathbb{E}) = \mathrm{Hom}_{\mathbb{F}}(\mathbb{F}(\alpha), \mathbb{E})$, then the homomorphisms $\varphi : \mathbb{F}[x]/(p) \to \mathbb{E}$ are precisely the homomorphisms $\varphi : \mathbb{F}[x] \to \mathbb{E}$ where $p(x) \in \ker(\varphi) \implies p(\varphi(x)) = 0$.(**TODO**) Hence,

$$\#\,\mathrm{Hom}_{\mathbb{F}}(\mathbb{K}, \mathbb{E}) = \#\{\text{roots of } p \text{ in } \mathbb{E}\} = \deg p.$$

General case, $\mathbb{K} = \mathbb{F}(\alpha_1, ..., \alpha_t) = \mathbb{F}(\alpha_1, ..., \alpha_{t-1})(\alpha_t) = \mathbb{K}_{t-1}(\alpha_t)$ with $\mathbb{K}_{t-1} \leq \mathbb{K}$. If $[\mathbb{K}_{t-1} : \mathbb{F}] = [\mathbb{K} : \mathbb{E}]$, we are done. Hence, suppose that $[\mathbb{K}_{t-1} : \mathbb{E}] < [\mathbb{K} : \mathbb{E}] = n$, then by strong induction, $\#\,\mathrm{Hom}_{\mathbb{F}}(\mathbb{K}_{t-1}, \mathbb{E}) = [\mathbb{K}_{t-1}, \mathbb{E}]$. There are exactly $[\mathbb{K} : \mathbb{K}_{t-1}]$ extension of **TODO**and $\varphi_0 : \mathbb{K}_{t-1} \to \mathbb{E}$?? **TODO**. Let p be the minimal polynomial of α_t over $\mathbb{K}_{t-1}$, then $\deg p = [\mathbb{K} : \mathbb{K}_{t-1}]$ (why ? **TODO**). Identify $\mathbb{K}$ with $\mathbb{K}_{t-1}[x]/(p)$. If $\varphi|_{\mathbb{K}_{t-1}} = \varphi_0$, then $p(\alpha_t) = 0 \implies \varphi(p(\alpha_t)) = 0 \implies p^{\varphi_0}(\varphi(\alpha_t)) = 0$.

$$p(x) = a_n x^n + ... + a_1 x + a_0$$

$$p^{\varphi_0}(x) = \varphi_0(a_n)x^n + ... + \varphi_0(a_1)x + \varphi_0(a_0) \in \mathbb{E}[x]$$

Let's prove that p^{φ_0} splits into distinct linear factors in $\mathbb{E}[x]$. **TODO**.

$$\begin{aligned}\#\,\mathrm{Hom}(\mathbb{K} : \mathbb{E}) &= \#\,\mathrm{Hom}(\mathbb{K}_{t-1}, \mathbb{E}) \\ &\quad \times \#\{\text{extensions } \varphi \text{ of any } \varphi_0 : \mathbb{K}_{t-1} \to \mathbb{E}\} \\ &= [\mathbb{K}_{t-1} : \mathbb{F}] \times [\mathbb{K} : \mathbb{K}_{t-1}] \\ &= [\mathbb{K} : \mathbb{F}]\end{aligned}$$

Therefore, when $\mathbb{K} = \mathbb{E}$, we get that $\#\,\mathrm{Aut}_{\mathbb{F}}(\mathbb{E}) = [\mathbb{E} : \mathbb{F}]$. ■

To summarize, we have the following theorem:

Theorem. *If $\mathbb{E}/\mathbb{F}$ is a finite extension, then TFAE:*

1. *$\#\,Aut(\mathbb{E}/\mathbb{F}) = [\mathbb{E} : \mathbb{F}]$*
2. *$\mathbb{E}$ is normal and separable over $\mathbb{F}$.*
3. *$\mathbb{E}$ is the splitting field of a separable polynomial over $\mathbb{F}$.*

Notice that Property 2 also makes sens for infinite extensions.

Definition. *An extension $\mathbb{E}/\mathbb{F}$ (not necessarily finite) is said to be Galois if $\mathbb{E}$ is normal and separable over $\mathbb{F}$.*

7 The Galois Correspondence

Proposition. *If $\mathbb{E}/\mathbb{F}$ is Galois and $\mathbb{K}$ is any subfield of $\mathbb{E}$ containing $\mathbb{F}$, then $\mathbb{E}$ is Galois over $\mathbb{F}$.*

Proof. **TODO**By definition, $\mathbb{E}$ is normal and separable over $\mathbb{F}$. To show that $\mathbb{E}$ is normal over $\mathbb{K}$, let $\alpha \in \mathbb{E}$, $g \in \mathbb{K}[x]$ be the minimum polynomial of α and $f \in \mathbb{F}[x]$ be the minimum polynomial of α in $\mathbb{F}[x]$, then f splits completely and g divides f so g splits completely as well. **TODO** ■

Remark: If $\mathbb{E}/\mathbb{F}_p$ is a finite set, then we saw on wednesday (**TODO**) that $\mathbb{E}/\mathbb{F}_p$ is Galois, in fact, cyclic with a canonical generator: $x \mapsto x^p$. If $\mathbb{K} = \mathbb{F}_{p^t}$ and $\mathbb{F}_p \subset \mathbb{K} \subset \mathbb{E}$, then $\mathbb{E}$ is Galois over $\mathbb{K}$. $\mathrm{Gal}(\mathbb{E}/\mathbb{K}) = \langle \delta^t \rangle$ where $\delta^t : x \mapsto x^{p^t}$. This δ^t is called the relative Frobenius element over $\mathbb{K}$. (**TODO**).

If we let $G = \mathrm{Gal}(\mathbb{E}/\mathbb{F})$ and $X = \mathrm{Hom}_{\mathbb{F}}(\mathbb{K}, \mathbb{E})$, then we know that $\#X = [\mathbb{K} : \mathbb{F}]$. But notice that X is a G-set under the rule : if $\varphi \in X = \mathrm{Hom}_{\mathbb{F}}(\mathbb{K}, \mathbb{E})$ and $\delta \in G = \mathrm{Hom}_{\mathbb{F}}(\mathbb{E}, \mathbb{E})$, define $\delta * \varphi$ by the composition of the two functions. X is transitive G-set. Friday, we showed that any $\varphi : \mathbb{K} \to \mathbb{E}$ extends to $\tilde{\varphi} : \mathbb{E} \to \mathbb{E}$. If $\varphi_1, \varphi_2 : \mathbb{K} \to \mathbb{E}$, then $\delta = \tilde{\varphi_1} \circ \tilde{\varphi_2}^{-1} \in G$ makes $\delta\varphi_2 = \varphi_1$. By Orbit-Stabilser, $\#X \times \#\mathrm{Stab}(Id : \mathbb{K} \to \mathbb{E}) = \#G$. But notice that $\mathrm{Stab}(Id : \mathbb{K} \to \mathbb{E})$ is simply $\mathrm{Aut}(\mathbb{E}/\mathbb{K})$ so we get that (by rearranging the equation) $\mathrm{Aut}(\mathbb{E}/\mathbb{K}) = [\mathbb{E} : \mathbb{K}]$.

Theorem. *The map $\mathbb{K} \mapsto Gal(\mathbb{E}/\mathbb{K})$ is an injection from the subfields of $\mathbb{E}$ containing $\mathbb{F}$ to the subgroups of $Gal(\mathbb{E}/\mathbb{K})$.*

Proof. If we know that $H = \mathrm{Gal}(\mathbb{E}/\mathbb{K})$, then to recover $\mathbb{K}$, we can simply write that $\mathbb{K} = \mathbb{E}^H$ where $\mathbb{E}^H$ is the set of elements in $\mathbb{E}$ fixed by H. **TODO** ■

Corollary. *If $\mathbb{E}/\mathbb{F}$ is a finite Galois extension, then there are finitely many fields K in $\mathbb{E}$ containing $\mathbb{F}$.*

Proof. **TODO**Easy ■

Corollary. *If $\mathbb{E}$ over $\mathbb{F}$ is any finite separable extension, then the same is true: there are finitely many $\mathbb{F} \subset \mathbb{K} \subset \mathbb{E}$.*

Proof. If $\mathbb{E}$ is separable, then it can be generated by the roots $\alpha_1, ..., \alpha_t$ of a separable polynomial (**TODO**) $g_i \in \mathbb{F}[x]$. Hence, we can take the splitting field of $g_1, ..., g_t$ to get a field extension $\tilde{\mathbb{E}}$ that contains $\mathbb{E}$ and that is Galois. Thus, $\mathbb{F} \subset \mathbb{E} \subset \tilde{\mathbb{E}}$ so we can apply the theorem. ■

Remark: The assumpotion that $\mathbb{E}$ is separable over $\mathbb{F}$ is essential. To find a counterexample, take $\mathbb{F} = \mathbb{F}_p(u, v) = \{R(u, v) : R \in \mathbb{F}_p(x, y)\}$. Consider the extensions $\mathbb{E} = \mathbb{F}(\sqrt[p]{u}, \sqrt[p]{v})$ and $\mathbb{K}_\alpha = \mathbb{F}(\sqrt[p]{u} + \alpha\sqrt[p]{v})$ with $\alpha \in \mathbb{F}$.

Theorem (Primitive Element Theorem)**.** *If $\mathbb{E}/\mathbb{F}$ is finite and separable, then $\mathbb{E}$ contains an α such that*

$$\mathbb{E} = \mathbb{F}(\alpha) = \mathbb{F}[\alpha] = \mathbb{F}[x]/(p_\alpha).$$

Proof. Let's prove it by induction on the number of generators. For the Base Case $n = 1$, $\mathbb{E} = \mathbb{F}(\alpha_1)$ so we are done. Consider now the case $n = 2$ and let $\mathbb{E} = \mathbb{F}(\alpha, \beta)$. If $\mathbb{F}$ is finite, the extension $\mathbb{E}^*$ without zero is cyclic (**TODO**). If $\mathbb{F}$ is infinite, for each $t \in \mathbb{F}$, consider the extensions $\mathbb{E}_t = \mathbb{F}(\alpha + t\beta)$. Since there are infinitely many t in $\mathbb{F}$ but only finitely many extensions of $\mathbb{F}$ contained in $\mathbb{E}$. Hence, by the Pigeon Hole Principle, there exist $t_1, t_2 \in \mathbb{F}$ such that $\mathbb{E}_{t_1} = \mathbb{E}_{t_2}$. Let $\mathbb{E}_0 = \mathbb{F}(\alpha + t_1\beta) = \mathbb{F}(\alpha + t_2\beta)$, then notice that $\mathbb{E}_0$ is a field containing both $\alpha + t_1\beta$ and $\alpha + t_2\beta$, so by subtracting the two elements, $\mathbb{E}_0$ also contains $(t_2 - t_1)\beta$. Since $t_2 - t_1$ is a non-zero in $\mathbb{F}$, then it is also in $\mathbb{E}_0$ which proves that $\beta \in \mathbb{E}_0$ by division. From that, we easily get that $\alpha \in \mathbb{E}_0$ as well. It follows that $\mathbb{E}_0 = \mathbb{E}$. From the case $n = 2$, then Inductive Hypothesis follows easily. **TODO** ■

Remark: The separability assumption is key in the statement. Again, consider $\mathbb{F} = \mathbb{F}_p(u,v) = \{R(u,v) : R \in \mathbb{F}_p(x,y)\}$ and the extension $\mathbb{E} = \mathbb{F}(\sqrt[p]{u}, \sqrt[p]{v})$. To find the degree of $\mathbb{E}/\mathbb{F}$, consider first the extension $\mathbb{F}(u^{1/p})$ and notice that the minimal polynomial of $u^{1/p}$ is $x^p - u$ (why ? **TODO**: in the splitting field, $x^p - u = (x - u^{1/p})^p$ so if $x^p - u = gh$, then $g(x) = (x - u^{1/p})^{e_1}$ and $h(x) = (x - u^{1/p})^{e_2}$ for $e_1 + e_2 = p$.) so $[\mathbb{F}(u^{1/p}) : \mathbb{F}] = p$. **TODO**(degree). For each $\alpha \in \mathbb{E}$, we have that $\alpha = R(u^{1/p}, v^{1/p}) = f(u^{1/p}, v^{1/p})/g(u^{1/p}, v^{1/p})$, and hence, $\alpha^p = f(u,v)/g(u,v) \in \mathbb{F}$. It follows that $[\mathbb{F}(\alpha) : \mathbb{F}] \in \{1, p\}$ for all $\alpha \in \mathbb{E}$ so the primitive element theorem fails. This proves that $\mathbb{E}/\mathbb{F}$ has infinitely many distinct subfields.

Let's now prove the converse of the Galois Correspondence.

Proposition. $[\mathbb{E} : \mathbb{E}^H] = \#H$.

Proof. By the Primitive Element Theorem, we know that $\mathbb{E} = \mathbb{E}^H(\alpha)$ for some $\alpha \in \mathbb{E}$. Let's show that α satisfies an irreducible polynomial in $\mathbb{E}^H[x]$ of degree $\#H$. Consider the orbit $\alpha_1, ..., \alpha_n$ of α under the action of H. Notice that by the Stabilizer Theorem. Hence, consider the polynomial $p(x) = \prod(x - \alpha_i) \in \mathbb{E}^H[x]$ of degree $\#H$ which vanishes on α. It remains to show that p is irreducible over $\mathbb{E}^H$. It is the case because H acts transitively on its roots so if there was a decomposition $p = fg$, then it would contradict the transitivity of the action of H on the orbit. It follows that $[\mathbb{E} : \mathbb{E}^H] = \deg p = \#H$. ■

Corollary. $H = Gal(\mathbb{E}/\mathbb{E}^H)$.

Proof. Clearly, H is a subfield **TODO** ■

We can summarize the previous propositions into the following fundamental theorem of Galois Theory.

Theorem (Galois Correspondence)**.** *Given a field $\mathbb{F}$ and a finite Galois extension $\mathbb{E}$, the functions $\mathbb{K} \mapsto Gal(\mathbb{E}/\mathbb{K})$ and $H \mapsto E^H$ are mutually inverse bijections and hence, there is a bijection between the subfields of $\mathbb{E}$ containing $\mathbb{F}$ and the subgroups of $Gal(\mathbb{E}/\mathbb{F})$.*

The Galois correspondence is inclusion reversing: **TODO**

Example:

- Let $\mathbb{E}$ be the splitting field of $x^4 - 2$ and consider $\mathbb{E}_0 = \mathbb{Q}[x]/(r^4 - 2) = \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$. Define $r = \sqrt[4]{2}$. In E_0, the polynomial factorizes:$x^4 - 2 = (x - r)(x + r)(x^2 + r^2)$. **TODO**Hence, the Galois group has order 8. **TODO**Gal$(\mathbb{E}/\mathbb{Q}) = D_8$.