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

0 Preliminaries: Fields and Polynomials

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

0.1 Finite Fields

The two main mathematical objects studied in Galois Theory are fields, that we will mostly denote by $\mathbb{F}$, $\mathbb{E}$ or sometimes $\mathbb{K}$, and their corresponding ring of polynomials, $\mathbb{F}[x]$, $\mathbb{E}[x]$ and $\mathbb{K}[x]$ respectively. This subsection will be focused on finite fields and their unexpected properties. Most of the following properties are far from being obvious given the definition of a field.

Definition. Given a field $\mathbb{F}$, we denote by $\operatorname{char}\mathbb{F}$ the least positive integer n such that

$$\underbrace{1+1+\cdots+1+1}_{n}=0$$

and call it the characteristic of $\mathbb{F}$. It there is no such n, we write $\operatorname{char}\mathbb{F}=0$ and say that $\mathbb{F}$ is a field of characteristic 0.

If we replace fields with rings in the definition of the characteristic, we know by our experience that there exist rings of any characteristic. More precisely, given a positive integer n, we have that $\mathbb{Z}/n\mathbb{Z}$ is a ring of characteristic n. This turns out to not be the case for fields.

Theorem 0.1.1. *The characteristic of a field is either a prime number or 0.*

Proof. Let $\mathbb{F}$ be a field and suppose that its characteristic is not 0. Define $n=\operatorname{char}\mathbb{F}$ and suppose that n is a composite number, then there exist positive integers s and t strictly smaller than n such that $n=st$. Define S and T in $\mathbb{F}$ by

$$S=\underbrace{1+1+\cdots+1+1}_{s} \quad \text{and} \quad T=\underbrace{1+1+\cdots+1+1}_{t}.$$

By minimality of n, both S and T are non-zero. However, we can show by induction that S and T satisfy

$$ST=\underbrace{1+1+\cdots+1+1}_{n}=0$$

which is in contradiction with the fact that S and T are both non-zero. Therefore, n cannot be composite, and hence, is a prime number. ∎

From this theorem, we can now understand more precisely the general structure of finite fields. This becomes clearer with the following result.

Corollary. *The cardinality of a finite field is always the power of a prime number.*

Proof. Let $\mathbb{F}$ be a finite field, then its characteristic must be finite since otherwise, $1, 1+1, 1+1+1, ...$ would be an infinite sequence of distinct elements in $\mathbb{F}$. By the previous theorem, there exists a prime number p such that $\operatorname{char}\mathbb{F} = p$. Consider the ring homomorphism $\varphi : \mathbb{Z} \to \mathbb{F}$ generated by $\varphi(1) = 1$, then in general,

$$\varphi(n) = \underbrace{1 + 1 + \cdots + 1 + 1}_{n}.$$

Since $\operatorname{char}\mathbb{F} = p$, then the kernel of φ is $p\mathbb{Z}$. Hence, by the Isomorphism Theorem for ring homomorphisms, the image of φ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. Equivalently, $\mathbb{F}$ contains a copy of $\mathbb{Z}/p\mathbb{Z}$. Therefore, $\mathbb{F}$ can be viewed as a $\mathbb{Z}/p\mathbb{Z}$-vector space since it is closed under scalar multiplication by elements in $\mathbb{Z}/p\mathbb{Z}$. Since $\mathbb{F}$ is finite, then it must be a finite-dimensional vector space which means that $\mathbb{F}$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^n$ as vector spaces for some natural number n. It follows that $\#\mathbb{F} = p^n$. ■

It turns out the converse is also true: there exists a field of cardinality p^n for all prime number p and natural number n. Moreover, any two fields of cardinality p^n are isomorphic. This lets us characterize precisely the finite fields. However, the complete proof of this characterization requires tools that will be introduced in Section 3 on Splitting Fields.

One last property of finite fields concerns the structure of their multiplicative group. The following result will be used in the proof of the Primitive Element Theorem in Section 4.

Theorem 0.1.2. *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, $\alpha^{d_1} = 1$ 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. ■

0.2 Polynomials over Fields

Polynomials are at the heart of Galois Theory because of their numerous properties and their complicated structure. A very useful and well known property of polynomials is how similar their behavior is to the integers. This can be illustrated by the following result.

Theorem 0.2.1 (Euclidean Division)**.** *Given a field $\mathbb{F}$ and polynomials $f, g \in \mathbb{F}[x]$, there exist unique polynomials $q, r \in \mathbb{F}[x]$ such that*

$$f = qg + r$$

with $\deg(r) < \deg(g)$.

Proof. Consider the set

$$S = \{f - qg : q \in \mathbb{F}[x]\}$$

and let r be a polynomial in S with minimum degree, then there exists a $q_0 \in \mathbb{F}[x]$ such that $f = q_0 g + r$. Suppose that $\deg r \geq \deg g$ and write

$$r(x) = a_n x^n + ... + a_0, \qquad g(x) = b_m x^m + ... + b_0,$$

with a_n and b_m different than 0, then we obtain that $r_0(x) = r(x) - a_n b_m^{-1} x^{n-m} g(x)$ is a polynomial of degree strictly smaller than r since the terms of higher degree cancel out in the definition of r_0. It follows that

$$\begin{aligned} r_0(x) &= (f(x) - q_0(x)g(x)) - a_n b_m^{-1} x^{n-m} g(x) \\ &= f(x) - (q_0(x) + a_n b_m^{-1} x^{n-m}) g(x) \\ &\in S \end{aligned}$$

which is impossible since r_0 has a degree strictly smaller than the polynomial r which has minimal in S. It follows that $\deg r < \deg g$. **TODO**: Uniqueness. ■

Another concept that illustrates the similarity between the polynomials and the integers is the greatest common divisor.

Definition (Greatest Common Divisor)**.** Given a field $\mathbb{F}$ and two polynomials $f, g \in \mathbb{F}[x]$, a greatest common divisor of f and g is a polynomial $h \in \mathbb{F}[x]$ that satisfies

1. h is monic (its leading coefficient is 1).
2. h divides both f and g.
3. If a polynomial divides both f and g, then it must divide h.

From this definition, it is not clear whether such a polynomial exists. However, by the following theorem, it exists and is actually unique.

Theorem 0.2.2. *Given a field $\mathbb{F}$ and two polynomials $f, g \in \mathbb{F}[x]$, there exists a unique greatest common divisor h of f and g.*

Proof. Consider the set S defined by

$$S = \{p_1 f + p_2 g : p_1, p_2 \in \mathbb{F}[x]\} \setminus \{0\}$$

and let $h \in \mathbb{F}[x]$ be a monic polynomial of minimum degree in S, then there exist $p_1, p_2 \in \mathbb{F}[x]$ such that $h = p_1 f + p_2 g$. Let's prove that h divides both f and g. By contradiction, if h doesn't divide f, then by the Euclidean Division, there exist $q, r \in \mathbb{F}[x]$ such that

$$f = qh + r$$

where $\deg r < \deg h$ and r is non-zero. However, notice that we obtain

$$r = f - qh = f - q(p_1 f + p_2 g) = [1 - qp_1]f + [-qp_2]g \in S$$

which is impossible since r has a degree strictly smaller than h which is supposed to have the minimum degree in S. It follows that h divides f. The same argument shows that

h also divides g. Finally, let q be a polynomial over $\mathbb{F}$ that divides both f and g, then it must divide both $p_1 f$ and $p_2 g$ which directly implies that q divides $p_1 f + p_2 g = h$. Therefore, h is a greatest common divisor of f and g.

To show that it is unique, simply notice that given two greatest common divisors h_1, h_2 of f, g, we have that h_2 divides both f and g, hence, since h_1 is a common divisor of f and g, then h_2 divides h_1. Similarly, h_1 must divide h_2. It follows that $h_1 = \alpha h_2$ where $\alpha \in \mathbb{F} \setminus \{0\}$. Since both h_1 and h_2 are monic, then we must have $\alpha = 1$ and hence, $h_1 = h_2$. ■

With this theorem, we can now always talk about *the* greatest common divisor of two polynomials. Hence, given a field $\mathbb{F}$ and two polynomials f and g in $\mathbb{F}[x]$, we will denote by $\gcd_{\mathbb{F}}(f, g) \in \mathbb{F}[x]$ their unique greatest common divisor. Moreover, notice that from the proof of the previous theorem, we obtain this really useful property of the gcd.

Corollary. *Given a field $\mathbb{F}$ and two polynomials $f, g \in \mathbb{F}[x]$, there exist $p_1, p_2 \in \mathbb{F}[x]$ such that*

$$\gcd_{\mathbb{F}}(f, g) = p_1 f + p_2 g.$$

Proof. This follows from the construction of the $\gcd_{\mathbb{F}}(f, g)$ in the proof of the previous theorem. ■

It is tempting to drop the notation $\gcd_{\mathbb{F}}(f, g)$ and write the lighter notation $\gcd(f, g)$ instead. However, there are situations where the second notation might be ambiguous. For example, given a field $\mathbb{F}$, two polynomials f and g in $\mathbb{F}[x]$, and a field $\mathbb{E}$ which contains $\mathbb{F}$, then f and g can also be viewed as polynomials in $\mathbb{E}[x]$. In this situation, do we think of $\gcd(f, g)$ as $\gcd_{\mathbb{F}}(f, g)$ or as $\gcd_{\mathbb{E}}(f, g)$? If we think of the gcd of f and g as the monic linear combination $p_1 f + p_2 g$ of least degree, then it's totally conceivable that $\gcd_{\mathbb{E}}(f, g)$ has a degree smaller than $\gcd_{\mathbb{F}}(f, g)$ since we allow p_1 and p_2 to be in $\mathbb{E}[x]$ instead of restricting them to $\mathbb{F}[x]$. However, the next result tells us that this situation will never happen.

Theorem 0.2.3. *Let $\mathbb{F}$ and $\mathbb{E}$ be fields such that $\mathbb{E}$ contains $\mathbb{F}$ and let $f, g \in \mathbb{F}[x]$, then* $\gcd_{\mathbb{F}}(f, g) = \gcd_{\mathbb{E}}(f, g)$.

Proof. First, as we did for f and g, notice that we can also view $\gcd_{\mathbb{F}}(f, g)$ as a polynomial in $\mathbb{E}[x]$. Hence, since $\gcd_{\mathbb{F}}(f, g)$ is a polynomial in $\mathbb{E}[x]$ that divides both f and g, then it must also divide their gcd which is $\gcd_{\mathbb{E}}(f, g)$. It follows that $\gcd_{\mathbb{F}}(f, g)$ divides $\gcd_{\mathbb{E}}(f, g)$. Moreover, recall that there exist polynomials p_1 and p_2 in $\mathbb{F}[x]$ such that $\gcd_{\mathbb{F}}(f, g) = p_1 f + p_2 g$. Since $\gcd_{\mathbb{E}}(f, g)$ divides both f and g, then it must divide both $p_1 f$ and $p_2 g$ which directly implies that $\gcd_{\mathbb{E}}(f, g)$ divides $p_1 f + p_2 g = \gcd_{\mathbb{F}}(f, g)$. Thus, there exists a $\alpha \in \mathbb{E} \setminus \{0\}$ such that $\gcd_{\mathbb{E}}(f, g) = \alpha \gcd_{\mathbb{F}}(f, g)$. Since both polynomials are monic, then $\alpha = 1$ and hence, $\gcd_{\mathbb{F}}(f, g) = \gcd_{\mathbb{E}}(f, g)$. ■

Therefore, given two polynomials f and g, we can indeed drop the notation $\gcd_{\mathbb{F}}(f, g)$ and write $\gcd(f, g)$ instead.

For the moment, in this subsection, we focused our attention on the gcd and its properties. Another polynomial will turn out to be very important in the following sections, way more than the gcd of two polynomials. For the rest of this subsection, fix the fields $\mathbb{F}$ and $\mathbb{E}$ where $\mathbb{E}$ contains $\mathbb{F}$.

Definition (Minimal Polynomial)**.** Let $\alpha \in \mathbb{E}$, then we call minimal polynomial of α any monic non-zero polynomial m_α in $\mathbb{F}[x]$ of least degree such that $m_\alpha(\alpha) = 0$.

It is easy to guess that a minimal polynomial is actually unique given a $\alpha \in \mathbb{E}$. Let's prove it using the following useful property of minimal polynomials.

Proposition 0.2.4. *Let $\alpha \in \mathbb{E}$, let $p \in \mathbb{F}[x]$ be a minimal polynomial of α and let $f \in \mathbb{F}[x]$ be such that $f(\alpha) = 0$, then p divides f.*

Proof. By the Euclidean Division, there exist polynomials $q, r \in \mathbb{F}[x]$ such that $f = qp+r$ where $\deg r < \deg p$. If r is non-zero, then

$$r(\alpha) = f(\alpha) - q(\alpha)p(\alpha) = 0$$

which is impossible since r is a non-zero polynomial of degree strictly smaller than the minimal polynomial of α. Thus, by contradiction, r must be the zero polynomial which implies that $f = qp$. Therefore, p divides f. ■

Corollary. *Let $\alpha \in \mathbb{E}$, then α has a unique minimal polynomial.*

Proof. Let p_1 and p_2 be minimal polynomials of α, then $p_1(\alpha) = 0$ implies that p_2 divides p_1 by the previous theorem. Similarly, p_1 divides p_2. It follows that $p_1 = cp_2$ for a $c \in \mathbb{F} \setminus \{0\}$. Since both polynomials are monic, then $c = 1$ and so $p_1 = p_2$. ■

Given a $\alpha \in \mathbb{E}$, we can now talk about *the* minimal polynomial of α. The following corollary is very useful, intuitive and can be proved very simply using the previous propositions.

Corollary. *Let $f \in \mathbb{F}[x]$ and $\alpha \in \mathbb{F}$ be a root of f, then $(x - \alpha)$ divides f.*

Proof. If we take $\mathbb{E} = \mathbb{F}$ and consider the minimal polynomial of α, then we know that by uniqueness, it must be $(x - \alpha) \in \mathbb{F}[x]$ since α is a root, it has minimal degree (the minimal polynomial cannot have degree smaller than 1) and it is monic. Therefore, by a previous proposition, $(x - \alpha)$ must divide f. ■

One last property that we will prove in this section is the following.

Proposition 0.2.5. *The minimal polynomial of $\alpha \in \mathbb{E}$ is irreducible.*

Proof. Let $\alpha \in \mathbb{E}$ and let p denotes its minimal polynomial. Let $g \in \mathbb{F}[x]$ be a monic divisor of p, then there exists a monic polynomial $h \in \mathbb{F}[x]$ such that $p = gh$. It follows that $g(\alpha)h(\alpha) = p(\alpha) = 0$. If $g(\alpha) = 0$, then p divides g and so $p = g$. If $h(\alpha) = 0$, then p divides h which implies that $p = h$ and so $g = 1$. Since the only monic divisors of p are 1 and itself then p is irreducible. ■

0.3 Irreducible Polynomials over $\mathbb{Q}$

Determining if a polynomial in $\mathbb{Q}[x]$ is irreducible will become an important task in the following sections. Let's prove in this subsection a few theorems that will make our life easier. The first two proofs are taken from the book *Fields and Galois Theory* by James Milne.

Theorem 0.3.1. *Let f be an irreducible polynomial in $\mathbb{Z}[x]$, then f is irreducible as a polynomial over $\mathbb{Q}$.*

Proof. By contradiction, suppose that f is not irreducible over $\mathbb{Q}$, then there exists polynomials $g, h \in \mathbb{Q}[x]$ such that $f = gh$ with

$$g(x) = a_0 + \cdots + a_k x^k, \quad \text{and} \quad h(x) = b_0 + \cdots + b_l x^l$$

where $k, l < \deg f$. Since the coefficients of g and h are in $\mathbb{Q}$, there must be a least positive integer n such that $nf = g'h'$ where $g', h' \in \mathbb{Z}[x]$. Notice that n must be strictly greater than 1 because otherwise, it would contradict the fact that f is irreducible over $\mathbb{Z}$. Thus, let p be a prime factor of n, let's prove that p divides all the coefficients of either g' or h'.

By contradiction, if not all coefficients in g' and h' are divisible by p, then there must be integers i and j such that p divides $a_0, ..., a_{i-1}$ but not a_i and divides $b_0, ..., b_{j-1}$ but not b_j. Notice that the coefficient of x^{i+j} in nf is

$$a_0 b_{i+j} + a_1 b_{i+j-1} + \cdots + a_i b_j + \cdots + a_{i+j-1} b_1 + a_{i+j} b_0$$

and it must be divisible by p since the coefficients of nf are all divisible by n. It follows that

$$a_0 b_{i+j} + \cdots + a_i b_j + \cdots + a_{i+j} b_0 \equiv 0 \pmod{p} \tag{1}$$

Beside $a_i b_j$, all the other terms of this sum must be divisible by p since it either contains an a_k with $k \in \{0, ..., i-1\}$ or a b_k with $k \in \{0, ..., j-1\}$. Thus, equation (1) becomes $a_i b_j \equiv 0 \pmod{p}$ which implies by Gauss's Lemma that p must divide a_i or b_j. This is in contradiction with the definition of i and j. Therefore, p must divide all the coefficients of g' or h'. Without loss of generality, if p divides all the coefficients in g', then we can write $g'' = pg'$ where $g'' \in \mathbb{Z}[x]$ to get that

$$\left(\frac{n}{p}\right) f = g''h'.$$

However, this contradicts the minimality of n and so by contradiction, f must be irreducible over $\mathbb{Q}$. ■

This theorem implies another very important one which is probably the most well known irreducibility result for polynomials over $\mathbb{Q}$.

Theorem 0.3.2 (Eisenstein's Criterion)**.** *Let $f(x) = a_0 + ... + a_n x^n$ be a polynomial in $\mathbb{Z}[x]$. Suppose that there exists a prime number p such that p divides $a_0, a_1, ..., a_{n-1}$ but not a_n and p^2 does not divide a_0, then f is irreducible over $\mathbb{Q}$.*

Proof. By the previous theorem, it suffices to prove that f is irreducible over $\mathbb{Z}$. By contradiction, suppose that $f = gh$ where

$$g(x) = b_0 + \ldots b_r x^r, \quad \text{and} \quad h(x) = c_0 + \cdots + c_s x^s$$

with $r, s < n$. Since p divides $a_0 = b_0 c_0$, then p must divide b_0 or c_0. Moreover, p^2 does not divide $b_0 c_0$ so if either p divides b_0 but not c_0 or the opposite. Without loss of

generality, suppose that p divides b_0 but not c_0. Let's prove by induction that p divides b_k for all $k \in \{0, ..., r\}$. We already showed the base case. Suppose now that p divides $b_0, ..., b_{k-1}$, consider the coefficiet a_k. Since $k \leq r < n$, then p divides a_k. It follows that

$$a_k = b_0c_k + \cdots + b_{k-1}c_1 + b_kc_0 \equiv 0 \pmod{p}.$$

Beside b_kc_0, all the terms are divisible by p since they contain b_i with $i \in \{0, ..., k-1\}$. Thus, our equation becomes $b_kc_0 \equiv 0 \pmod{p}$. Since p doesn't divide c_0, then p must divide b_k. Therefore, by induction, p divides all the b_k's. In particular, for $k = r$, we get that p divides b_r. But since $a_n = b_rc_s$, then p divides a_n, a contradiction. Therefore, f must be irreducible over $\mathbb{Z}$, and hence, over $\mathbb{Q}$. ■

The last proposition is different in nature from the two previous ones since it doesn't let us conclude directly that a certain polynomial is irreducible over $\mathbb{Q}$. However, it lets us sometimes simplify the problem by determining the irreducibility of another polynomial on which we may apply other irreducibility tests.

Proposition 0.3.3. *Given a polynomial, $f(x) \in \mathbb{F}[x]$ of degree n, $f(x)$ irreducible if and only if the polynomial $x^n f(1/x) \in \mathbb{F}[x]$ is irreducible.*

Proof. Suppose that f is not irreducible, then there exist polynomials $g, h \in \mathbb{F}[x]$ of degree $s, t < n$ respectively satisfying $f = gh$. It follows that

$$x^n f(1/x) = x^n g(1/x)h(1/x) = [x^s g(1/x)][x^t h(1/x)].$$

It follows that $x^n f(1/x)$ is not irreducible over $\mathbb{F}$. To prove the converse, simply repeat the argument with $x^n f(1/x)$ instead f since the map $\mathbb{F}[x] \to \mathbb{F}[x] : g(x) \mapsto x^{\deg g} g(1/x)$ has order 2. ■

Given a polynomial $g(x)$ of degree n, the polynomial $x^n g(1/x)$ is simply the polynomial g where the order of the coefficient is reversed. Notice that the previous proposition applies to any field $\mathbb{F}$ and not just $\mathbb{Q}$.

0.4 Formal Derivatives and Multiple Roots

Another aspect of polynomials that will become important is the multiplicity of a root of a polynomial. This subsection's goal is to create a link between the multiplicity of a root and the roots of the formal derivative of a polynomial. We are talking about the formal derivtive and not simply the derivative to emphasize that th formal derivative has nothing to do with limits and rates of change, it is purely formal.

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

Proposition 0.4.1. *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. In the following proofs, assume that

$$f(x) = \sum_{k=0}^{n} a_k x^k, \qquad \text{and} \qquad g(x) = \sum_{k=0}^{m} b_k x^k.$$

1. To make the notation simpler, let $N = \max(n, m)$ and think of f and g as polynomials of degree N where the leading coefficient might be zero. We have that $f+g$ is the polynomial $(f+g)(x) = \sum_{k=0}^{N}(a_k + b_k)x^k$. Hence, its Formal Derivative is given by

$$(f+g)'(x) = \sum_{k=0}^{N-1}(k+1)(a_{k+1} + b_{k+1})x^k$$

which implies that

$$(f+g)'(x) = \sum_{k=0}^{N-1}(k+1)a_{k+1}x^k + \sum_{k=0}^{N-1}(k+1)b_{k+1}x^k = f'(x) + g'(x).$$

Therefore, $(f+g)' = f' + g'$.

2. Let's compute $(fg)'$ and $f'g + fg'$ separately to obtain the desired formula. First, using the product formula for polynomials, we have

$$(fg)' = \left(\sum_{k=0}^{n+m}\left(\sum_{i=0}^{k} a_i b_{k-i}\right)x^k\right)' = \sum_{k=0}^{n+m-1}\left((k+1)\sum_{i=0}^{k+1} a_i b_{k+1-i}\right)x^k. \quad (1)$$

For the second expression, we obtain

$$f'g + fg' = \left(\sum_{k=0}^{n-1}(k+1)a_{k+1}x^k\right)\left(\sum_{k=0}^{m} b_k x^k\right) + \left(\sum_{k=0}^{n} a_k x^k\right)\left(\sum_{k=0}^{m-1}(k+1)b_{k+1}x^k\right).$$

Again, using the product formula, we get

$$f'g + fg' = \sum_{k=0}^{n+m-1}\left[\left(\sum_{i=0}^{k}(i+1)a_{i+1}b_{k-i}\right) + \left(\sum_{i=0}^{k} a_i(k-i+1)b_{k-i+1}\right)\right]x^k.$$

By reindexing the first sum inside the square brackets and merging the two sums, we can simplify the expression into

$$f'g + fg' = \sum_{k=0}^{n+m-1}\left((k+1)\sum_{i=0}^{k+1} a_i b_{k+1-i}\right)x^k.$$

Therefore, combining the previous inequality with equation (1), we obtain the desired formula.

3. Let's prove it by induction on n. The base case is trivial. Suppose that $(f^n)' = nf'f^{n-1}$, then by the product formula:

$$(f^{n+1})' = (f^n f)' = (f^n)'f + f^n f' = nf'f^n + f^n f' = (n+1)f'f^n$$

which proves it for the case $n+1$. Therefore, by induction, the formula holds for all n.

■

Notice that all of these properties are the usual properties of the usual derivative in $\mathbb{R}^n$, but we were able here to prove them only using the formula for the derivative a polynomial. This can be explained by the fact that we use precisely these properties of the usual derivative to find the formula for the derivative of a polynomial. With these formula, we are now ready to to prove the link between the formal derivative an the multiplicity of a root of a polynomial.

Theorem 0.4.2. *Given a field $\mathbb{F}$, a polynomial $f \in \mathbb{F}[x]$ and a root $\alpha \in \mathbb{F}$ of f, then α is a root of multiplicity 1 if and only if $f'(\alpha) \neq 0$.*

Proof. Let's prove equivalently that $(x-\alpha)^2$ divides f if and only if $f'(\alpha) = 0$. If $(x-\alpha)^2$ divides f, then we can write $f(x) = (x-\alpha)^2 g(x)$ with $g \in \mathbb{F}[x]$. It follows by the product rule and the power rule that $f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x)$. Thus, α is a root of f'. Conversely, write $f(x) = (x-\alpha)^r h(x)$ where $r \geq 1$ and $\gcd(h, (x-\alpha)) = 1$, i.e., r is the largest integer such that $(x-\alpha)^r$ divides f, then its formal derivative is given by

$$f'(x) = r(x-\alpha)^{r-1}h(x) + (x-\alpha)^r h'(x).$$

Since $f'(\alpha) = 0$, then taking $x = \alpha$ gives us $r(x-\alpha)^{r-1} = 0$. By contradiction, if $r = 1$, $r(x-\alpha)^{r-1} = 1$ which can never be zero in a field. Thus, r must be greater than or equal to 2. It follows that $(x-\alpha)^2$ divides f. ■

This theorem can probably be generalized, but this version is the only one we will need really.

0.5 Constructing Fields

Since fields play an important role in Galois Theory, it will be crucial to be able to construct fields with the appropriate properties in the appropriate situations such as proofs or counterexamples. Hopefully, most of the time, we will use the same construction technique over and over. This technique relies on a theorem about rings and ideals which, because of its importance, I will state and prove even if it was already studied in Algebra 3.

Theorem 0.5.1. *Let R be a commutative ring and I be an ideal, then I is a maximal ideal if and only if R/I is a field.*

Proof. Suppose that I is a maximal ideal and let $a + I \in (R/I) \setminus \{I\}$, then $a \notin I$. Thus, the ideal $(a) + I$ properly contains I which, by maximality, implies that $(a) + I = R$. Thus, there is a $b \in R$ and $i \in I$ such that $ba + i = 1$. Equivalently, $(b+I)(a+I) = 1+I$. Therefore, $a + I$ has a multiplicative inverse in R/I and so R/I is a field.

Suppose now that R/I is a field and let J be an ideal of R containing I properly, then there exists a $a \in J \setminus I$. It follows that $(a+I)$ must have a multiplicative inverse $(b+I)$. Thus, $(b+I)(a+I) = 1+I$ which is equivalent to $ba+i = 1$ for some $i \in I$. Since J contains both I and a, then $1 = ba+i \in J$. Therefore, $J = R$ and so I must be maximal. ■

By reading the statement of Theorem 0.5.1, it is now clear how to construct fields given a ring and a maximal ideal. However, this theorem is a bit too general since in practice we will only apply it to a more restrained class of rings: the polynomials rings. But to do so, for a fixed field $\mathbb{F}$, we need a way to identify the maximal ideals of $\mathbb{F}[x]$. An important property of $\mathbb{F}[x]$ is the fact that it is a Principal Ideal Domain (PID), meaning that every ideal is generated by a single element.

Theorem 0.5.2. *Given $f \in \mathbb{F}[x]$, the set $(f) = \{qf : q \in \mathbb{F}[x]\}$ is an ideal. Moreover, any ideal of $\mathbb{F}[x]$ is of this form.*

Proof. The first part of this theorem is not hard to prove. For the second part, let I be an ideal of $\mathbb{F}[x]$ and let f be a non-zero polynomial in I of minimal degree. By properties of ideals, all the multiples of f must be in I so $(f) \subset I$. Now, let $g \in I$, then by the Euclidean Division, there is are polynomials $q, r \in \mathbb{F}[x]$ such that $g = qf + r$ with $\deg r < \deg f$. If r is non-zero, then we get that $r = g - qf \in I$. But it implies that r is a polynomial in I of degree strictly smaller than f which contradicts the minimality of the degree of f. Thus, r is zero so $q = qf \in (f)$. It follows that $(f) = I$. ■

We can characterize precisely the maximal ideals of $\mathbb{F}[x]$.

Theorem 0.5.3. *The maximal ideals of $\mathbb{F}[x]$ are precisely the ideals of the form (f) where $f \in \mathbb{F}[x]$ is irreducible.*

Proof. Suppose that I is a maximal ideal of $\mathbb{F}[x]$, by Theorem 0.5.2, we have that $I = (f)$ where $f \in \mathbb{F}[x]$. Let g be a monic divisor of f of degree strictly smaller than f, then there exists a $h \in \mathbb{F}[x]$ such that $f = gh \in (g)$. It follows that $(f) \subset (g)$. Moreover, (f) is a proper subset of (g) since $g \notin (f)$. Thus, by maximality, $(g) = \mathbb{F}[x]$. It follows that g must have degree 0 since otherwise, every non-zero polynomial in $\mathbb{F}[x]$ would have degree greater than 1. Thus, since g is monic and of degree 0, then $g = 1$. It follows that the only monic divisors of f are f itself and 1 so f must be irreducible.

Suppose now that f is irreducible and let I be an ideal of $\mathbb{F}[x]$ which contains (f) properly. By Theorem 0.5.2, we have $I = (g)$ for some $g \in \mathbb{F}[x]$. Consider the gcd of f and g, since $\gcd(f, g)$ is monic and divides f, then it is either equal to f or 1. If $\gcd(f, g) = f$, then it would imply that f divides g and so that $(g) \subset (f)$ which is impossible since (f) is properly contained in (g). Hence, $\gcd(f, g) = 1$. Recall now that the gcd of two polynomials must be a linear combination of the two polynomials so there exist $p_1, p_2 \in \mathbb{F}[x]$ such that $1 = p_1 f + p_2 g$. By properties of ideals, we have that $1 = p_1 f + p_2 g \in (g)$ and so $(g) = \mathbb{F}[x]$. Therefore, (f) must be maximal since the only ideals that properly contain it is $\mathbb{F}[x]$. ■

From the two previous results, we have a clear method for constructing new fields using polynomials.

Theorem 0.5.4. *Let $f \in \mathbb{F}[x]$ be an irreducible polynomial of degree greater than 1, then $\mathbb{F}[x]/(f)$ is a field containing a subfield isomorphic to $\mathbb{F}$. Moreover, $\mathbb{F}[x]/(f)$ contains a root of the polynomial f.*

Proof. Since f is irreducible, then by Theorem 0.5.3, (f) is a maximal ideal of $\mathbb{F}[x]$. Hence, by Theorem 0.5.1, $\mathbb{F}[x]/(f)$ is a field. Since the degree of f is greater than 1, then the map $\mathbb{F} \to \mathbb{F}[x] : x \mapsto x + (f)$ is injective and so $\mathbb{F}$ is isomorphic to a subfield of $\mathbb{F}[x]/(f)$. Finally, since we can view $\mathbb{F}$ as a subfield of $\mathbb{F}[x]/(f)$, then we can view f as a polynomial over $\mathbb{F}[x]/(f)$. Moreover, by induction and using properties of elements in a quotient ring, $q(g + (f)) = q(g) + (f)$ for all $q \in (\mathbb{F}[x]/(f))[t]$ and $g \in \mathbb{F}[x]$. It follows that $f(x + (f)) = f(x) + (f) = 0 + (f)$ and so $x + (f)$ is a root of f in $\mathbb{F}[x]/(f)$. ■

1 Field Extensions

1.1 Definitions and Examples

In this section, let's make clear the idea of a field extension. The process of extending a field arises for example when we study a polynomial over a field $\mathbb{F}$ but the polynomial has no roots in $\mathbb{F}$. We can then extend $\mathbb{F}$ to a larger field which also contains roots of the polynomial. Notice that in this situation, $\mathbb{F}$ is a subfield of the larger field. In general, field extensions of $\mathbb{F}$ are simply the fields which contains $\mathbb{F}$ as a subfield. This leads to the following definition.

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.

There are different ways of extending a given field $\mathbb{F}$. If $\mathbb{E}$ is an extension of $\mathbb{F}$ and $\alpha \in \mathbb{E} \setminus \mathbb{F}$, then a common way of extending $\mathbb{F}$ is to consider the smallest field containing both $\mathbb{F}$ and α. We denote by $\mathbb{F}(\alpha)$ the field generated by both $\mathbb{F}$ and α. To make the definition more precise, we can view $\mathbb{F}(\alpha)$ as the intersection of all the fields containing $\mathbb{F} \cup \{\alpha\}$. Hence, $\mathbb{F}(\alpha)$ is the smallest field in the sense that any extension of $\mathbb{F}$ containing α is also an extension of $\mathbb{F}(\alpha)$. We can also view $\mathbb{F}(\alpha)$ as the set of rational functions $\mathbb{F}(x)$ evaluated at $x = \alpha$, hence the notation. It follows that we have a surjective map $ev_\alpha : \mathbb{F}(x) \to \mathbb{F}(\alpha) : f(x) \mapsto f(\alpha)$.

In some cases, it might be useful to simply consider the smallest ring containing both $\mathbb{F}$ and α. In such cases, we denote the smallest ring containing $\mathbb{F}$ and α by $\mathbb{F}[\alpha]$ and define it in the same way as $\mathbb{F}(\alpha)$ but replacing fields with rings. Again, we can identify elements of $\mathbb{F}[\alpha]$ with polynomials in $\mathbb{F}[x]$ evaluated at $x = \alpha$. This gives us that $ev_\alpha : \mathbb{F}[x] \to \mathbb{F}[\alpha] : f(x) \mapsto f(\alpha)$ is surjective. By the Isomorphism Theorem, if we denote by K the kernel of ev_α, we obtain that $\mathbb{F}[x]/K \cong \mathbb{F}[\alpha]$. Since the kernel is an ideal of $\mathbb{F}[x]$ and $\mathbb{F}[x]$ is a Principal Ideal Domain, then there is a polynomial $f \in \mathbb{F}[x]$ such that $K = (f)$ which gives us $\mathbb{F}[x]/(f) \cong \mathbb{F}[\alpha]$.

In general, if $\mathbb{E}$ is an extension of $\mathbb{F}$, then $\mathbb{E}$ is also a vector space over $\mathbb{F}$. This leads to the following definition.

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. If the degree is 2, we can also say that $\mathbb{E}$ is a quadratic extension of $\mathbb{F}$.

Example:

- If we view $\mathbb{C}$ as a field extension of $\mathbb{R}$, then it is an extension of degree 2 since the field of complex numbers is 2-dimensional $\mathbb{R}$-vector space. Using the previously defined notation, it follows that $[\mathbb{C} : \mathbb{R}] = 2$.

- If we view $\mathbb{C}$ as a field extension of $\mathbb{Q}$, then it is an infinite-degree extension since the field of complex numbers is not a finite-dimensional vector space of $\mathbb{Q}$ (which can be shown using an argument on the cardinality). It follows that $[\mathbb{C} : \mathbb{Q}] = \infty$. 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 consider the field $\mathbb{E} = \mathbb{F}[x]/(p)$ as an extension of $\mathbb{F}$ where p is an irreducible polynomial of degree $n \geq 1$, then

  $$\mathbb{E} = \{a_0 + a_1 x + ... + a_{n-1} x^{n-1}\}.$$

  It is easy to see from this representation of $\mathbb{E}$ that $\mathbb{E}$ is n-dimensional vector space over $\mathbb{F}$ with basis $1, ..., x^{n-1}$. Hence, $[\mathbb{F}[x]/(p) : \mathbb{F}] = n$.

- Let $\mathbb{F}$ be a field and $\mathbb{E} = \mathbb{F}(x)$ be the fraction field of $\mathbb{F}[x]$, then $[\mathbb{E} : \mathbb{F}] = \infty$ since the set $\{1, x, x^2, ...\}$ in $\mathbb{F}(x)$ is infinite and linearly independent.

- Let p be an irreducible polynomial over $\mathbb{Q}$ of degree greater than 1, then $\mathbb{Q}[x]/(p)$ is an extension of $\mathbb{Q}$ which contains a root α of p. Consider the surjective homomorphism $ev_\alpha : \mathbb{Q}[x] \to \mathbb{Q}[\alpha] : f(x) \mapsto f(\alpha)$, then the First Isomorphism Theorem tells us that $\mathbb{Q}[x]/K \cong \mathbb{Q}[\alpha]$ where K is the kernel of ev_α. To determine K, notice that the minimal polynomial of α must divide p, but since p is irreducible, then by uniqueness, p must be the unique polynomial of α. It follows that any element in K is divisible by p and all multiples of p are in K. Thus, $K = (p)$ and so $\mathbb{Q}[x]/(p) \cong \mathbb{Q}[\alpha]$. Since p is irreducible, then $\mathbb{Q}[x]/(p)$ must be a field and so $\mathbb{Q}[\alpha]$ must be a field as well. Therefore, $Q[\alpha] = \mathbb{Q}(\alpha)$.

The following theorem relates the degree of iterated field extensions with the degrees of the individual extensions. In other words, if $\mathbb{K}$ is an extension of $\mathbb{E}$ which is itself an extension of $\mathbb{F}$, then $\mathbb{K}$ is an extension of $\mathbb{F}$ and $[\mathbb{K} : \mathbb{F}]$ can be found by only knowing $[\mathbb{K} : \mathbb{E}]$ and $[\mathbb{E} : \mathbb{F}]$.

Theorem 1.1.1 (Multiplicativity of the degree)**.** *Given three fields $\mathbb{F} \subset \mathbb{E} \subset \mathbb{K}$, we have*

$$[\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathbb{E}][\mathbb{E} : \mathbb{F}].$$

Proof. If $[\mathbb{K} : \mathbb{E}]$ or $[\mathbb{E} : \mathbb{F}]$ is infinite, then the proof is trivial since in both cases, we can find an infinite set of linearly independent vectors in $\mathbb{K}$ as a $\mathbb{F}$-vector space. Hence, we can assume that the degrees are finite. Define $n = [\mathbb{K} : \mathbb{E}]$, $m = [\mathbb{E} : \mathbb{F}]$, let $\alpha_1, ..., \alpha_n \in \mathbb{K}$ be a basis for $\mathbb{K}$ as a $\mathbb{E}$-vector space and $\beta_1, ..., \beta_m \in \mathbb{E}$ be a basis for $\mathbb{E}$ as a $\mathbb{F}$-vector space. Notice that for all $a \in \mathbb{K}$, there exist scalars $\lambda_1, ..., \lambda_n \in \mathbb{E}$ 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 scalars $\lambda_{i1}, ..., \lambda_{im} \in \mathbb{F}$ 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 $\mathbb{F}$ basis for $\mathbb{K}$. Hence, it follows that the dimension of $\mathbb{K}$ as a $\mathbb{F}$-vector space is $n \cdot m = [\mathbb{K} : \mathbb{E}][\mathbb{E} : \mathbb{F}]$. ■

1.2 Application to Ruler and Compass Constructions

(**TODO**Ajouter des dessins de constructions pour mieux comprendre les explications. **TODO**)

It feels like we haven't accomplished much beside setting and proving the preliminaries for Galois Theory and proving the theorem on the muliplicity of the degree. However, we already have the tools now to solve some of the oldest problems in mathematics. More precisely, in this subsection, we are going to focus on three problems in classical geometry which remained unsolved for millenials.

Concerning the historical context behind these problems, it is important to understand that most of Greek geometry was based on geometric constructions which only used a ruler with no markings and a compass. Methods to construct the usual two dimensional figures (triangles, squares, ...) only using these two tools were known at that time. Moreover, these two tools are very useful when proving theorems about some constructible shapes since the proof can follow the, usually, easy steps of construction of the constructible shape. However, there were three problems for which no constructions using only ruler and compass was found. Let's state them properly:

1. **Trisecting the angle** - Given any angle θ, is it possible to construct the angle $\theta/3$?

2. **Doubling the cube** - Given a cube of side length 1, is it possible to construct a cube of side length 2 ?

3. **Squaring the circle** - Given a circle of radius 1, is it possible to construct a square of area equal to that of the circle ?

To translate these problems into our framework of Abstract Algebra, let's try to determine precisely what we mean by constructible. We say that an angle θ is constructible if it possible to draw two intersecting straightlines with an angle of intersection of θ. Similarly, we say that a number x is constructible if we can construct two points on the plane with distance x. If x is constructibility, we will consider that $-x$ is also constructible.

On the two dimensional plane with no marks, we will assume that we are able to construct two distinct points A and B for which we define the length of the segment AB to be our unit. We will call this length 1. Since we constructed the two points A and B, then we say that 1 is constructible. Similarly, extending the segment AB into a straight line, and using the compass, we can create a new point C on the straight line of distance 1 from B and of distance 2 from A. Then 2 is also constructible since we constructed two points having distance 2, namely, A and C.

By induction, we can easily show that we can construct any positive integer in this way, and hence, every integer. Moreover, I will not prove it but we can actually construct every positive rational number. This comes from the fact that given two constructible numbers, we can also construct their sum, their multiplication, their subtraction and

division using constructions that I will not show here. Therefore, the subset of $\mathbb{R}$ of constructible numbers is a field that contains $\mathbb{Q}$.

It turns out that given a positive constructible number, there is ruler and compass construction that lets us construct its square root. Moreover, we can prove that the four usual operations and taking the square root are precisely the operations we can apply to constructible numbers. Thus, if we forget about the visual interpretation of constructible numbers and allow constructible numbers to be complex, the following definition shoud be well motivated now.

Definition. A complex number is constructible by ruler and compass if it can be obtained from the rationals by successive applications of field operations (+, -, $\times$, $\div$) and square roots. Using the terminology we developed previously, we can say that a number is constructible if it is contained in a sequence of quadratic extensions of $\mathbb{Q}$.

Thus, the field of constructible numbers is an extension of $\mathbb{Q}$ of infinite degree since we can create an infinite tower of quadratic extension from $\mathbb{Q}$. Now that the notion of constructibility is clear and well defined, let's rephrase the three problems into our modern framework. Given an angle θ formed by the two straightlines L_1 and L_2, we can easily construct the number $\cos\theta$ by taking a point P_1 on L_1 at distance 1 from the intersection P of L_1 and L_2 and projecting the new point onto the L_2 to create the point P_2. The distance between P and P_2 is $\cos\theta$. Conversely, if we assume that $\cos\theta$ is a constructible number for some θ, then we can easily construct the angle θ by reversing the previous construction. It follows that an angle θ is constructible if and only if the number $\cos\theta$ is constructible. Similarly, if we find a construction to double the cube, then we would be able to construct its side length which is $\sqrt[3]{2}$. Thus, the problem of doubling the cube is equivalent to the problem of determining whether $\sqrt[3]{2}$ is a constructible number or not. Finally, constructing a square of area equal to the area of the unit circle is equivalent to constructing a square of side length $\sqrt{\pi}$. Thus, we need to determine whether $\sqrt{\pi}$ is constructible or not. Since taking square roots and squaring constructibles are valid operations, then it is equivalent to determining whether π is constructible or not. Therefore, the three problems can now be restated in terms of constructibility of real numbers:

1. **Trisecting the angle** - Is $\cos(\theta/3)$ constructible given that $\cos\theta$ is constructible?
2. **Doubling the cube** - Is $\sqrt[3]{2}$ constructible ?
3. **Squaring the circle** - Is π constructible ?

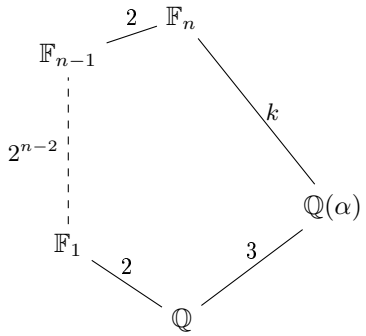
The following theorem gives a very easy and useful unconstructibility test.

Theorem 1.2.1. *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. ■

This test is sufficient to prove that it is impossible to trisect arbitrary angles or to duplicate the cube. Let's prove it in the form of two corollaries.

Corollary (Doubling the cube)**.** *It is impossible to double the cube.*

Proof. It suffices to show that $\sqrt[3]{2}$ is not constructible. Notice that $\sqrt[3]{2}$ is a root of the cubic polynomial $q(x) = x^3 - 2 \in \mathbb{Q}[x]$. By Eisenstein's Criterion with $p = 2$, q is irreducible. Therefore, $\sqrt[3]{2}$ is not constructible. ■

Corollary (Trisecting the angle)**.** *There exists a constructible angle θ such that the angle $\theta/3$ is not constructible.*

Proof. Consider the angle $\theta = 2\pi/3$ which is constructible since $\cos\theta = -1/2$ is a rational number (and so constructible). To show that $\theta/3$ is not a constructible angle, it suffices to show that $\cos(\theta/3)$ is not 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 $\cos(\theta/3)$ is a root of the polynomial $4x^3 - 3x + \frac{1}{2} \in \mathbb{Q}[x]$. Equivalently, $\cos(\theta/3)$ 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 $\cos(\theta/3)$ is not constructible. ■

Considering the fact that these problems were unsolved for millenials, the simplicity of these proofs really shows the power of modern mathematics and the theory of fields that is being developed here.

1.3 Algebraic Extensions and Squaring the Circle

For the moment, we didn't solve the third problem. What about squaring the circle? It would be difficult to apply Theorem 1.2.1 to π since there is no obvious irreducible cubic polynomial over $\mathbb{Q}$ for which π is a root. This comes from the fact that π is harder to understand as a real number in the sense that we can easily relate $\sqrt[3]{2}$ to some rational numbers by definition and $\cos(2\pi/9)$ by numerous trigonometric identities. However, it is way harder to find such relations for π. In a way, π is more irrational than $\sqrt[3]{2}$ or $\cos(2\pi/9)$. There is a way to formalize this in a more precise way with the following theorem which proof is being omitted for simplicity.

Theorem 1.3.1 (Lindemann - 1882)**.** *π is the root of no polynomial over $\mathbb{Q}$.*

Complex numbers with this property are called *transcendental numbers*. π is far from being the only known transcendental number, Euler's constant e is transcendental as well, and it was proved by Georg Cantor in 1874 that most complex numbers are transcendental. With this information about π, it is clear that we will need more than Theorem 1.2.1 to conclude anything about squaring the circle. It turns out that the transcendentality of π is precisely the information that will let us conclude that squaring the circle is in fact impossible.

Definition (Algebraic Numbers and Algebraic Extensions)**.** Let $\mathbb{E}/\mathbb{F}$ be a field extension, we say that $\alpha \in \mathbb{E}$ is algebraic over $\mathbb{F}$ if α is the root of a polynomial in $\mathbb{F}[x]$. If every α in $\mathbb{E}$ is algebraic over $\mathbb{F}$, then we say that $\mathbb{E}$ is an algebraic extension of $\mathbb{F}$.

For example, $\sqrt{2} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$ since it is a root of $x^2 - 2 \in \mathbb{Q}[x]$. Similarly, $i \in \mathbb{C}$ is algebraic over $\mathbb{Q}$ since it is a root of $x^2 + 1 \in \mathbb{Q}[x]$. From our discussion about π and the previous definition, we can define the notion of transcendence in a more general setting.

Definition (Transcendental Numbers and Transcendental Extensions)**.** Let $\mathbb{E}/\mathbb{F}$ be a field extension, we say that $\alpha \in \mathbb{E}$ is transcendental over $\mathbb{F}$ if α is not algebraic over $\mathbb{F}$. If $\mathbb{E}$ contains a transcendental number over $\mathbb{F}$, we say that $\mathbb{E}$ is a transcendental extension of $\mathbb{F}$. Equivalently, $\mathbb{E}$ is a transcendental extension if it is not an algebraic extension.

The following theorem is of great importance for the problem of squaring the circle but also for the next sections.

Theorem 1.3.2. *Every finite field extension is algebraic.*

Proof. Let $\mathbb{E}/\mathbb{F}$ be a finite field extension of degree n and let $\alpha \in \mathbb{E}$. By definition of the degree of a finite extension, the set $\{1, \alpha, ..., \alpha^n\}$ must be linearly dependent in $\mathbb{E}$ as a $\mathbb{F}$-vector space. 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 $\mathbb{F}$. Since it holds for all $\alpha \in \mathbb{E}$, then $\mathbb{E}$ is an algebraic extension of $\mathbb{F}$. ■

With this theorem, we can easily prove a very powerful unconstructibility test.

Theorem 1.3.3. *If $\alpha \in \mathbb{C}$ is transcendental, then it is unconstructible.*

Proof. Let's show the converse. If $\alpha \in \mathbb{C}$ is constructible, then by definition, it is contained in a finite tower of quadratic extensions of $\mathbb{Q}$. It follows that α is contained in a finite extension of $\mathbb{Q}$. Therefore, α must be algebraic over $\mathbb{Q}$. ■

Corollary (Squaring the Circle)**.** *It is impossible to contruct a square of area π.*

Proof. It suffices to show that π is unconstructible. By Theorem 1.3.1, π is transcendental and so by Theorem 1.3.3, it must be unconstructible. Therefore, it is impossible to contruct a square of area π. ■

Now that we showed how powerful this theory is, let's apply it to even more complicated problems such as expressing algebraic numbers in terms of radicals. It is actually this problem which motivated the theory of groups and fields we are developping here. Notice the similarity between the problem of solving polynomial equations using radicals and problem of determining which numbers are constructible using ruler and compass constructions. Unfortunately, this new problem will require more tools and complicated results that will take some time to develope.

2 Automorphism Group

(**TODO**Rajouter une section qui détail l'algorithme qui permet de déterminer tout les automorphisms d'une extension de degrée finie et l'appliquer à des exemples du cours. Mettre la section en deuxième ou troisième place. **TODO**)

2.1 Definitions and Properties

For now, we only defined notions and proved theorems related to fields. However, for the rest of this document, the theory of groups will play a major role. To motivate the introduction of groups in this theory, consider the situation where we have a ground field $\mathbb{F}$ and we generate the field extension $\mathbb{E}$ by adding the elements $\alpha_1, ..., \alpha_n$ to $\mathbb{F}$, in this situation, we write $\mathbb{E} = \mathbb{F}(\alpha_1, ..., \alpha_n)$ (more precisely, we define $\mathbb{F}(\alpha_1, ..., \alpha_n)$ recurievly by $\mathbb{F}(\alpha_1, ..., \alpha_n) = \mathbb{F}(\alpha_1, ..., \alpha_{n-1})(\alpha_n)$). It turns out that understanding the symmetries between the generators $\alpha_1, ..., \alpha_n$ of $\mathbb{E}$ using what we call *automorphisms* will give us a lot of informations about the structure of $\mathbb{E}$ as an extension of $\mathbb{F}$. Since the theory of groups is perfect when it comes to studying the symmetries of a mathematical objects, groups will play an important role in the next sections. But first, let's define what an automorphism is.

Definition (Automorphism)**.** Let $\mathbb{E}/\mathbb{F}$ be a field extension and $\varphi : \mathbb{E} \to \mathbb{E}$ be a function, then φ is an automorphism if it is a field-homomorphism that fixes every element of $\mathbb{F}$, i.e., $\varphi|_{\mathbb{F}} = id$.

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. The set of all automorphisms of a field extension forms a group under composition. This leads to the next important definition.

Definition (Automorphism Group)**.** Given a field extension $\mathbb{E}/\mathbb{F}$, the group of all automorphisms of $\mathbb{E}/\mathbb{F}$ is called the automorphism group of $\mathbb{E}/\mathbb{F}$ and is denoted by $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$.

Now that we defined the automorphism group of an extension, the following theorem will be helpful to understand the elements in this group and will let us visualize the action of $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$ on $\mathbb{E}$.

Proposition 2.1.1. *If* $[\mathbb{E}:\mathbb{F}]$ *is finite, then* $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$ *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 Theorem 1.3.2, 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

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

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

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

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. ■

Notice that the proof of the previous theorem only used the fact that the extension is finite to deduce that it is algebraic. It follows that the theorem also applies if $\mathbb{E}/\mathbb{F}$ is algebraic but not necessarily finite. In the previous proof, we showed that any automorphism must map an element to a root of any polynomial that the element satisfies. This observation is very important because it gives us some constraints on the automorphisms. For example, from this observation, ny automorphism in $\mathrm{Aut}(\mathbb{F}(\alpha)/\mathbb{F})$ must map α to a root of its minimal polynomial m_α. It turns out that the converse is true, given a root of m_α, there is an automorphism that maps α to this root. This observation will let us generate and manipulate automorphisms more easily. The next theorems will prove a generalization of the previous observation using some new notations that need to be defined first.

Definition. Given a field $\mathbb{F}$ and two field extensions $\mathbb{K}$ and $\mathbb{E}$, we define $\mathrm{Hom}_{\mathbb{F}}(\mathbb{K}, \mathbb{E})$ as the set of field-homomorphisms from $\mathbb{K}$ to $\mathbb{E}$ which fixes every element of $\mathbb{F}$. Notice that $\mathrm{Hom}_{\mathbb{F}}(\mathbb{E}, \mathbb{E}) = \mathrm{Aut}(\mathbb{E}/\mathbb{F})$.

Given a polynomial $p \in \mathbb{K}[x]$ and a homomorphism $\varphi \in \mathrm{Hom}_{\mathbb{F}}(\mathbb{K}, \mathbb{E})$, it will sometimes be useful to consider the polynomial p with coefficients replaced by their evalution by φ. The next definition is used to make the notation lighter and the proofs shorter.

Definition. Let $\mathbb{E}$ be a field extension of $\mathbb{F}$, φ be an element of $\mathrm{Hom}_{\mathbb{F}}(\mathbb{F}, \mathbb{E})$ and p be a polynomial $\mathbb{F}[x]$ which we can write as $a_0 + ... + a_n x^n$, then we denote by $p^\varphi \in \mathbb{E}[x]$ the polynomial $\varphi(a_0) + ... + \varphi(a_n)x^n$.

We can easily show that the using the notation defined above, we have the that $(p_1 + p_2)^\varphi = p_1^\varphi + p_2^\varphi$ and $(p_1 p_2)^\varphi = p_1^\varphi p_2^\varphi$. Since the proofs of these two formulas are straightforward applications of fields and homomorphisms properties, I will omit the proof. Using the ideas of the proof of Theorem 2.1.1, we have the following theorem.

Theorem 2.1.2. *If $\mathbb{F} \subset \mathbb{F}' \subset \mathbb{F}'(\alpha) \subset \mathbb{E}$ are finite extensions of $\mathbb{F}$, then any element φ of $\mathrm{Hom}_{\mathbb{F}}(\mathbb{F}'(\alpha), \mathbb{E})$ is an extension of a $\varphi_0 \in \mathrm{Hom}_{\mathbb{F}}(\mathbb{F}', \mathbb{E})$. Moreover, φ maps α to a root of $m_\alpha^{\varphi_0}$ where m_α is the minimal polynomial of α over $\mathbb{F}'$.*

Proof. Let $\varphi_0 = \varphi|_{\mathbb{F}'}$, it is not hard to show that φ_0 is in $\mathrm{Hom}_{\mathbb{F}}(\mathbb{F}', \mathbb{E})$ so the proof is omitted. Let $m_\alpha \in \mathbb{F}'[x]$ be the minimal polynomial of α and write it as $a_0 + ... + a_n x^n$, then $m_\alpha(\alpha) = 0$ implies that $\varphi(a_0 + ... + a_n \alpha^n) = \varphi(0) = 0$. Using the fact that φ preserves addition and multiplication, we obtain $\varphi(a_0) + ... + \varphi(a_n)\varphi(\alpha)^n = 0$. Using the fact that the a_i's are in $\mathbb{F}'$, we get $\varphi_0(a_0) + ... + \varphi_0(a_n)\varphi(\alpha)^n = 0$ which is equivalent to $m_\alpha^{\varphi_0}(\varphi(\alpha)) = 0$. Thus, α is mapped to a root of $m_\alpha^{\varphi_0}$. ■

As mentionned in a previous discussion, the converse is true. This will be very useful when trying to determine all the homomorphisms of a finite extension.

Theorem 2.1.3. *If $\mathbb{F} \subset \mathbb{F}' \subset \mathbb{F}'(\alpha) \subset \mathbb{E}$ are finite extensions of $\mathbb{F}$ and $\varphi_0 \in \mathrm{Hom}_{\mathbb{F}}(\mathbb{F}', \mathbb{E})$, then each root r of $m_\alpha^{\varphi_0}$ where m_α is the minimal polynomial m_α of α over $\mathbb{F}'$ induces a unique element in $\mathrm{Hom}_{\mathbb{F}}(\mathbb{F}'(\alpha), \mathbb{E})$ that extends φ_0 and that maps α to r.*

Proof. Let $\varphi_0 \in \mathrm{Hom}_{\mathbb{F}}(\mathbb{F}', \mathbb{E})$, let r be a root of $m_\alpha^{\varphi_0}$ and define the function

$$\varphi' : \mathbb{F}'[x]/(m_\alpha) \to \mathbb{E}, \qquad p + (m_\alpha) \mapsto p^{\varphi_0}(r)$$

First, let's prove that φ' is well-defined. Let $p_1, p_2 \in \mathbb{F}'[x]$ be polynomials such that $p_1 + (m_\alpha) = p_2 + (m_\alpha)$, it follows that $p_1 = p_2 + q m_\alpha$ for some $q \in \mathbb{F}'[x]$. Thus,

$$\varphi'(p_1 + (m_\alpha)) = p_1^{\varphi_0}(r) = p_2^{\varphi_0}(r) + q(r)^{\varphi_0} m_\alpha^{\varphi_0}(r) = p_2^{\varphi_0}(r) = \varphi'(p_2 + (m_\alpha))$$

so φ' is well defined. It is not hard to show that φ' preserves addition and multiplication. Recall that $\mathbb{F}'[x]/(m_\alpha) \cong \mathbb{F}'(\alpha)$ by the map

$$f : \mathbb{F}'[x]/(m_\alpha) \to \mathbb{F}'(\alpha), \qquad p + (m_\alpha) \mapsto p(\alpha).$$

Define the function $\varphi = \varphi' \circ f^{-1} : \mathbb{F}'(\alpha) \to \mathbb{E}$ and let's show that it has the desired properties. Since both φ' and f^{-1} preserves addition and multiplication, then so does φ. Let $a \in \mathbb{F}'$, then $f^{-1}(a) = p_a + (m_\alpha)$ where p_a is the constant polynomial with value a. It follows that $\varphi(a) = \varphi'(p_a + (m_\alpha)) = p_a^{\varphi_0}(r) = p_a(r) = a$ so φ extends φ_0. Next, we have that $f(x) = \alpha$ so $\varphi(\alpha) = \varphi'(x + (m_\alpha)) = x^{\varphi_0}(r) = x(r) = r$. Thus, we showed that φ is a homomorphism that maps α to r and that extends φ_0. The last thing we need to prove is that it is unique. Let $\varphi_1 \in \mathrm{Hom}_{\mathbb{F}}(\mathbb{F}'(\alpha), \mathbb{E})$ such that α is mapped to r, then for all $b \in \mathbb{F}'(\alpha)$, we have that

$$\begin{aligned}
\varphi_1(b) &= \varphi_1(c_0 + c_1\alpha + ... + c_m\alpha^m) \\
&= c_0 + c_1\varphi_1(\alpha) + ... + c_m\varphi_1(\alpha)^m \\
&= c_0 + c_1\varphi(\alpha) + ... + c_m\varphi(\alpha)^m \\
&= \varphi(c_0 + c_1\alpha + ... + c_m\alpha^m) \\
&= \varphi(b).
\end{aligned}$$

Since it holds for all $b \in \mathbb{F}'(\alpha)$, then $\varphi_1 = \varphi$. Therefore, φ is unique. ■

From the last two theorems, we obtain a very useful way of understanding the elements in the homomorphism set of a finite field extension generated by one element. We can summarize the two previous theorem as follows:

Theorem 2.1.4. *If $\mathbb{F} \subset \mathbb{F}' \subset \mathbb{F}'(\alpha) \subset \mathbb{E}$ are finite extensions of $\mathbb{F}$, then the elements of $\mathrm{Hom}_{\mathbb{F}}(\mathbb{F}'(\alpha), \mathbb{E})$ are precisely the extensions of the elements φ_0 in $\mathrm{Hom}_{\mathbb{F}}(\mathbb{F}', \mathbb{E})$ that are uniquely determined by the way they map α to a root of $m_\alpha^{\varphi_0}$.*

These theorems may seem obscure and hard to visualize. It is important to keep in mind that they generalize the following simpler version.

Theorem 2.1.5. *Given a finite extension $\mathbb{F}(\alpha)$ of $\mathbb{F}$, each root r of the minimal polynomial in $\mathbb{F}(\alpha)$ induces a unique automorphism that maps α to r, and all the automorphisms are of this form.*

Proof. If we plug-in $\mathbb{F}' = \mathbb{F}$ and $\mathbb{E} = \mathbb{F}(\alpha)$ in Theorem 2.1.4, then $\mathrm{Hom}_{\mathbb{F}}(\mathbb{F}', \mathbb{E}) = \{id\}$ and so we get that every automorphism of $\mathbb{F}(\alpha)/\mathbb{F}$ must map α to a root of m_α and it is uniquely determined by this mapping. ■

With these theorems about the automorphisms and homomorphisms of finite field extensions, we can prove that $\#\,\mathrm{Aut}(\mathbb{E}/\mathbb{F})$ is bounded above by the degree of extension. This can be interpreted by the fact that, as we saw with the previous theorems, the automorphisms are only determined by a few single values and hence, $\#\,\mathrm{Aut}(\mathbb{E}/\mathbb{F})$ cannot be too big.

Theorem 2.1.6. *If $\mathbb{E}/\mathbb{F}$ is a finite field extension, then $\#\,\mathrm{Aut}(\mathbb{E}/\mathbb{F}) \leq [\mathbb{E} : \mathbb{F}]$.*

Proof. Let's prove by induction that $\#\,\mathrm{Hom}_{\mathbb{F}}(\mathbb{K}, \mathbb{E}) \leq [\mathbb{K} : \mathbb{F}]$ 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 know by Theorem 2.1.5 that each $\varphi \in \mathrm{Hom}_{\mathbb{F}}(\mathbb{K}, \mathbb{E})$ 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 $\mathrm{Hom}_{\mathbb{F}}(\mathbb{K}, \mathbb{E})$. In other words, $\#\,\mathrm{Hom}_{\mathbb{F}}(\mathbb{K}, \mathbb{E}) \leq \deg p$. Finally, we also observed that $\mathbb{K} \cong \mathbb{F}[x]/(p)$ so $[\mathbb{K} : \mathbb{F}] = \deg p$. Therefore, $\#\,\mathrm{Hom}_{\mathbb{F}}(\mathbb{K}, \mathbb{E}) \leq [\mathbb{K} : \mathbb{F}]$.

For the induction step, suppose that the inequality holds for all extensions generated by n elements, and consider the case $n + 1$. We have $\mathbb{K} = \mathbb{F}(\alpha_1, ..., \alpha_{n+1})$ so we can define $\mathbb{F}' = \mathbb{F}(\alpha_1, ..., \alpha_n)$. By the induction hypothesis, we know that $\#\,\mathrm{Hom}_{\mathbb{F}}(\mathbb{F}', \mathbb{E}) \leq [\mathbb{F}' : \mathbb{F}]$. If $\mathbb{F}' = \mathbb{K}$, then we are done by the induction hypothesis, otherwise, we have $\mathbb{K} = \mathbb{F}'(\alpha_{n+1})$ with $\alpha_{n+1} \notin \mathbb{F}'$. 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 $m_{\alpha_{n+1}} \in \mathbb{F}'[x]$ be the minimal polynomial of α_{n+1}, then $\deg m_{\alpha_{n+1}} = [\mathbb{K} : \mathbb{F}'] = d_2$. We can easily notice that any element of $\mathrm{Hom}_{\mathbb{F}}(\mathbb{K}, \mathbb{E})$ restricted to $\mathbb{F}'$ is an element of

$\mathrm{Hom}_{\mathbb{F}}(\mathbb{F}', \mathbb{E})$. Hence, to have an estimation on the size of $\mathrm{Hom}_{\mathbb{F}}(\mathbb{K}, \mathbb{E})$, we can determine in how many ways each element of $\mathrm{Hom}_{\mathbb{F}}(\mathbb{F}', \mathbb{E})$ can be extended to an element of $\mathrm{Hom}_{\mathbb{F}}(\mathbb{K}, \mathbb{E})$. By Theorem 2.1.4, we have that each φ_0 in $\mathrm{Hom}_{\mathbb{F}}(\mathbb{F}', \mathbb{E})$ can be extended in at most $\deg m_{\alpha_{n+1}}^{\varphi_0} = \deg m_{\alpha_{n+1}} = d_2$ ways. Therefore, 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. ■

2.2 Galois Extensions

Theorem 2.1.6, shows that there are at most $[\mathbb{E} : \mathbb{F}]$ automorphisms in the automorphism group of a finite extension. Is it possible to prove that there in fact exactly $[\mathbb{E} : \mathbb{F}]$ automorphisms in the automorphism group ? To answer this question, consider the situation where $\mathbb{E}$ is generated by a single element α, then $[\mathbb{E} : \mathbb{F}]$ is equal to the degree of the minimal polynomial of α. By Theorem 2.1.5, we know that there are as much automorphisms as roots of the minimal polynomial in $\mathbb{E}$. Thus, if the minimal polynomial of α doesn't factor completely into linear terms in $\mathbb{E}$, then $\#\,\mathrm{Aut}(\mathbb{E}/\mathbb{F}) < [\mathbb{E} : \mathbb{F}]$.

This happens for example when $\mathbb{F} = \mathbb{Q}$ and $\mathbb{E} = \mathbb{Q}(\sqrt[3]{2})$. The minimal polynomial of $\sqrt[3]{2}$ in $\mathbb{Q}(\sqrt[3]{2})$ is $x^3 - 2 \in \mathbb{Q}[x]$. The two other roots of the minimal polynomial are complex numbers so $\sqrt[3]{2}$ is the only roots of its minimal polynomial in $\mathbb{Q}(\sqrt[3]{2})$. Therefore, $\#\,\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) < [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$. This shows that $\mathrm{Aut}(\mathbb{E}/\mathbb{F}) = [\mathbb{E} : \mathbb{F}]$ may not always hold. However, we are very interested in the situations where this equation holds since it can be used to deduce a lot of informations about the extension.

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

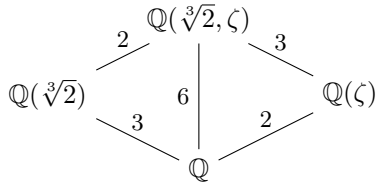
When $\mathbb{E} = \mathbb{C}$ and $\mathbb{R}$, then $[\mathbb{E} : \mathbb{F}] = 2$. Moreover, beside the identify automorphism, the conjugation map is also an automorphism of $\mathbb{C}/\mathbb{R}$. By Theorem 2.1.6, these must be the only automorphisms of $\mathbb{C}/\mathbb{R}$. It follows that $[\mathbb{C} : \mathbb{R}] = 2$ and so $\mathbb{C}/\mathbb{R}$ is a Galois extension.

As before, consider the extension $\mathbb{Q}(\sqrt[3]{2})$ of $\mathbb{Q}$ of degree 3. We already showed that it is not a Galois extension since the extension only contains one root of the minimal polynomial of $\sqrt[3]{2}$. 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 over $\mathbb{Q}$ (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_3 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 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 2.2.1. *$\mathbb{E}^G$ 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 2.2.2. $\mathbb{E}^G = \mathbb{F}$.

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 $d_1 = 1$. ■

By Theorem 2.1.5, the minimal polynomial of α in a Galois extension of the form $\mathbb{F}(\alpha)$ must split completely into linear factors. It turns out that this can be generalized to any irreducible polynomial with a root in the Galois extension.

Theorem 2.2.3. *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 that f is the minimal polynomial 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 $\mathbb{E}[x]$. ■

If a field extension has the property that any irreducible polynomial in 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.

3 Splitting Fields

3.1 Existence and Uniqueness

As we saw in the last section, an interesting property of Galois extensions is the way polynomials in the ground field splits in the Galois extension. In this section, we will explore in more details these situations with the notion of a splitting field, and we will then see how it relates to Galois extensions.

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.

With this definition, it is not clear, even if it might be easy to guess, that such fields always exist. The following theorem answers this matter.

Theorem 3.1.1 (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

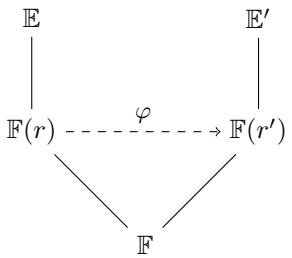
$$\mathbb{E} = L(r_1, ..., r_n) = \mathbb{F}(r_0)(r_1, ..., r_n) = \mathbb{F}(r_0, r_1, ..., r_n)$$

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 $f \in \mathbb{F}[x]$. ■

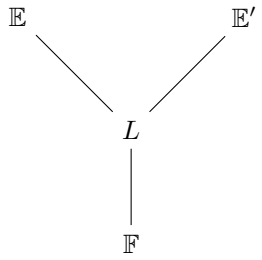
It is very hard to compute the degree of a splitting field since it depends very subtly on the structure of f. However, by the multiplicativity of the degree, the degree of the splitting field must be smaller than $(\deg f)!$. For now, we proved that a splitting field must exist for a field $\mathbb{F}$ and polynomial $f \in \mathbb{F}[x]$, but it turns out that splitting fields of f are isomorphic as field extensions. Let's state it properly and prove it.

Theorem 3.1.2 (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 3.1.3. *If $\mathbb{E}/\mathbb{F}$ is a Galois extension, 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 by Theorem 2.2.3 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 $\mathbb{F}$. ■

3.2 Application to Finite Fields

Recall that if $\mathbb{F}$ is a finite field, then it must have characteristic equal to a prime number p (Theorem 0.1.1) which implies that $\mathbb{F}$ contains a copy of $\mathbb{F}_p$. 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 3.2.1. *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 by Theorem 0.4.2). 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 3.2.2. *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 also holds for $x = 0$, then the map fixes F_p. ■

Definition. 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, $\varphi \in \text{Aut}(\mathbb{F}_q/\mathbb{F}_p)$.

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 3.2.3. *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 $\#\operatorname{Aut}(\mathbb{F}_q/\mathbb{F}_p) = [\mathbb{F}_q : \mathbb{F}_p]$. 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 $\mathbb{Z}/n\mathbb{Z}$. ■

3.3 Characterizing 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 2.2, we proved that any Galois extension is normal. Let's improve it this result and use it to characterize Galois extensions.

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 $\mathbb{E}[x]$.

As we will see, the converse of Theorem 2.2.3 is not true. However, we can make it true by adding another assumption on the extension.

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

The next theorem shows that the seperability of an extension comes for free most of the time since the main applications and examples of this theory is to fields of characteristic zero.

Proposition 3.3.1. *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' by Theorem 0.4.2. Hence, r is a root of $\gcd(f, f') \in \mathbb{F}[x]$.

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

Recall that f is irreducible in $\mathbb{F}[x]$ so $\gcd(f, f')$ is either f or 1 since it divides f. 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 doesn't have characteristic zero, then computing the degree of the formal derivative is not as easy.

Theorem 3.3.2. *If $\mathbb{E}/\mathbb{F}$ is Galois, then it is normal and separable.*

Proof. Let $f \in \mathbb{F}[x]$ be an irreducible polynomial and $r \in \mathbb{E}$ be a root of f. Consider the orbit $r_1, ..., r_n$ of r under the action of the Galois group and define the polynomial $g(x) = (x-r_1)...(x-r_n) \in \mathbb{E}[x]$. If we expand the product which defines g, we get that the coefficients in front of the powers of x are the elementary symmetric polynomials in $r_1, ..., r_n$. Since the r_i's are in the same orbit under the action of the Galois group, then

the coefficients are all fixed by every element of the Galois group, thus, they are in $\mathbb{F}$. It follows that g is a polynomial on $\mathbb{F}$ for which r is a root.

Since r is a root of the irreducible polynomial f, then f must be the minimal polynomial of r. Since g is a polynomial in $\mathbb{F}[x]$ for which r is a root, then f must divide g. It follows that on $\mathbb{E}$, f must split into distinct linear factors since g can be completely split into distinct linear factors. Since it holds for all $f \in \mathbb{F}[x]$ irreducible with a root in $\mathbb{E}$, then $\mathbb{E}/\mathbb{F}$ must be both normal and separable. ■

It turns out that the converse is also true and the proof is very similar to the proof of Theorem 2.1.6 with some additional assumptions that replace inequalities with equalities.

Theorem 3.3.3. *If $\mathbb{E}/\mathbb{F}$ is finite, normal and separable, then $\mathbb{E}/\mathbb{F}$ is Galois.*

Proof. Let's prove by strong induction on the degree that $\#\operatorname{Hom}_{\mathbb{F}}(\mathbb{K},\mathbb{E}) = [\mathbb{K}:\mathbb{F}]$ where $\mathbb{K} \subset \mathbb{E}$ is a finite field extension of $\mathbb{F}$. Notice that the base case $[\mathbb{K}:\mathbb{F}] = 1$ is trivial since in that case, $\mathbb{K} = \mathbb{F}$ and so the only automorphism is the identity.

Suppose now that there is a n such that any extension of $\mathbb{F} \subset \mathbb{K} \subset \mathbb{E}$ of degree strictly smaller than n satisfies $\#\operatorname{Hom}_{\mathbb{F}}(\mathbb{K},\mathbb{E}) = [\mathbb{K}:\mathbb{F}]$. Let $\mathbb{K} \subset \mathbb{E}$ be an extension of $\mathbb{F}$ of degree n and notice that either $\mathbb{K}$ is of the form $\mathbb{F}(\alpha)$ or of the form $\mathbb{F}'(\alpha)$ for some extension $\mathbb{F}'$ of $\mathbb{F}$ different from $\mathbb{F}$. Let's show that in both cases, the equation $\#\operatorname{Hom}_{\mathbb{F}}(\mathbb{K},\mathbb{E}) = [\mathbb{K}:\mathbb{F}]$ holds.

If $\mathbb{K} = \mathbb{F}(\alpha)$, then the degree of $\mathbb{K}/\mathbb{F}$ is simply the degree of the minimal polynomial m_α of α. By Theorem 2.1.4, we have that

$$\#\operatorname{Hom}_{\mathbb{F}}(\mathbb{K},\mathbb{E}) = \#\{\text{roots of } m_\alpha \text{ in } \mathbb{E}\}.$$

But since $\mathbb{E}$ is normal and separable, then m_α splits completely into distinct linear factors and so the number of roots of m_α in $\mathbb{E}$ is simply equal to $\deg m_\alpha$. Therefore, $\#\operatorname{Hom}_{\mathbb{F}}(\mathbb{K},\mathbb{E}) = [\mathbb{K}:\mathbb{F}]$.

If $\mathbb{K} = \mathbb{F}'(\alpha)$ with $\alpha \notin \mathbb{F}'$ and $\mathbb{F}' \neq \mathbb{F}$, then the degree of $\mathbb{F}'/\mathbb{F}$ must be strictly smaller than n and so by the induction hypothesis, $\#\operatorname{Hom}_{\mathbb{F}'}(\mathbb{F}',\mathbb{E}) = [\mathbb{K}:\mathbb{F}]$. By Theorem 2.1.4, the elements in $\operatorname{Hom}_{\mathbb{F}}(\mathbb{K},\mathbb{E})$ are all extensions of elements in $\operatorname{Hom}_{\mathbb{F}}(\mathbb{F}',\mathbb{E})$. Let $\varphi_0 \in \operatorname{Hom}_{\mathbb{F}}(\mathbb{K},\mathbb{E})$, then by the same theorem, φ_0 has as much extensions in $\operatorname{Hom}_{\mathbb{F}}(\mathbb{K},\mathbb{E})$ as there are roots of $m_\alpha^{\varphi_0}$ in $\mathbb{E}$. Let's show that $m_\alpha^{\varphi_0}$ splits into distinct linear factors in $\mathbb{E}[x]$. If we let $m \in \mathbb{F}[x]$ be the minimal polynomial of α over $\mathbb{F}$, we get that m_α divides m. It follows that $m_\alpha^{\varphi_0}$ divides m^{φ_0}. But since m has coefficients in $\mathbb{F}$ and φ_0 fixes the elements of $\mathbb{F}$, then $m^{\varphi_0} = m$. Hence, $m_\alpha^{\varphi_0}$ divides m. Since $\mathbb{E}$ is normal and separable, then m must split completely into distinct linear factors and so does $m_\alpha^{\varphi_0}$. Thus, $m_\alpha^{\varphi_0}$ has as much roots in $\mathbb{E}$ as its degree. But notice that $\deg m_\alpha^{\varphi_0} = \deg m_\alpha = d_2$ so φ_0 has exactly d_2 extensions. It follows that

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

By induction, it holds for all finite extensions $\mathbb{K}$. In particular, it holds for $\mathbb{K} = \mathbb{E}$ which gives us

$$\#\operatorname{Aut}(\mathbb{E}/\mathbb{F}) = [\mathbb{E}:\mathbb{F}].$$

Therefore, $\mathbb{E}$ is a Galois extension. ■

We have found a characterization of Galois extensions as desired at the beginning of the subsection. With this characterization, we can actually deduce a second one. The next theorem summarizes these characterizations into one place.

Theorem 3.3.4. *If $\mathbb{E}/\mathbb{F}$ is a finite extension, then TFAE:*

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

Proof. Property 1 and 2 are equivalent by definition and Property 1 and 3 are equivalent by Theorem 3.3.2 and Theorem 3.3.3. By Proposition 3.1.3, Property 1 implies that $\mathbb{E}$ is the splitting field of a polynomial, however, we didn't prove that this polynomial is separable. Let's prove it by going over the proof of the proposition. Since $[\mathbb{E} : \mathbb{F}] < \infty$, then we can let $\alpha_1, ..., \alpha_n$ be a finite set of generators for $\mathbb{E}/\mathbb{F}$. Let the f_i's be the respective minimal polynomials of the α_i's and define $f = f_1 \cdot \cdots \cdot f_n$ such that the f_i's are distinct: if f_i and f_j are equal, simply remove one of them. In $\mathbb{E}[x]$, all the f_i's factor completely by normality 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 $\mathbb{F}$. To show that f is separable, suppose that it has a multiple root. By separability of $\mathbb{E}$, the f_i's cannot have multiple roots so it must be that $\gcd(f_i, f_j) \neq 1$ for some i and j. Since both are irreducible, then $f_i = \gcd(f_i, f_j) = f_j$ which is in contradiction with our construction of f. Therefore, $\mathbb{E}$ is the splitting field of a separable polynomial.

Let's now prove that Property 4 implies one of Property 1, 2 or 3 to finish the proof. Suppose that $\mathbb{E}$ is the splitting field of a separable polynomial, then f splits completely into distinct linear factors. Moreover, $\mathbb{E}$ is generated by the roots of f. Notice that in the proof of Theorem 3.3.3, the assumption that the extension is normal and separable was here to make sure that the generators are roots of polynomials that splits completely into distinct linear factors. We don't need this assumption anymore since it now follows from the fact that $\mathbb{E}$ is the splitting field of a separable polynomial. Therefore, if rework the proof of Theorem 3.3.3, we obtain that $\mathbb{E}$ is Galois. Therefore, Property 4 implies Property 1. ■

Since Property 2 in the previous theorem also makes sense for infinite extensions, we can now define what it means for an infinite extension to be Galois even though it will not be useful for us here.

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

All the applications of Galois Theory that we will explore at the end of these notes will concern finite extensions but it is still good to keep in mind this new definition.

4 The Galois Correspondence

4.1 The Fundamental Theorem of Galois Theory

The Galois Correspondence is really the Fundamental Theorem of Galois Theory. This theorem makes a connection between the subgroups of the Galois group and the subfields of the Galois extension. It turns out that there is a very deep connection that will let us understand the structure of Galois extensions. However, to prove it, we will need to prove a bunch of theorems first.

Proposition 4.1.1. *If $\mathbb{E}/\mathbb{F}$ is a finite Galois extension and $\mathbb{K}$ is a subfield of $\mathbb{E}$ containing $\mathbb{F}$, then $\mathbb{E}$ is Galois over $\mathbb{K}$.*

Proof. By Theorem 3.3.4, we have that $\mathbb{E}$ is normal and separable over $\mathbb{F}$. Let's show that $\mathbb{E}$ is normal and separable over $\mathbb{K}$. Let $p \in \mathbb{K}[x]$ be an irreducible polynomial which has a root α in $\mathbb{E}$, then p is the minimal polynomial of α over $\mathbb{K}$. If we let $m_\alpha \in \mathbb{F}[x]$ be the minimal polynomial of α over $\mathbb{F}$, then p divides m_α. By normality and separability of $\mathbb{E}$ over $\mathbb{F}$, m_α splits completely into distinct linear factors over $\mathbb{E}$ and so does p. Therefore, $\mathbb{E}$ is normal and separable over $\mathbb{K}$, so it follows from Theorem 3.3.4 that $\mathbb{E}$ is Galois over $\mathbb{K}$. ■

Here is a second proof which uses the theory of Group Actions.

Proof. Let $G = \mathrm{Gal}(\mathbb{E}/\mathbb{F})$ and $X = \mathrm{Hom}_{\mathbb{F}}(\mathbb{K}, \mathbb{E})$, then we know by the proof of Theorem 3.3.3 that $\#X = [\mathbb{K} : \mathbb{F}]$. But notice that X can be seen as a G-set where G acts by composition. This action is transitive since for all $\varphi_1, \varphi_2 \in X$, we have that $\varphi_1 \circ \varphi_2^{-1}$ can be extended to an element in G and so there is a σ such that $\sigma\varphi_2 = \varphi_1$. Thus, by the Orbit-Stabilizer Theorem, $\#X\#\mathrm{Stab}(id) = \#G$ which is equivalent to $[\mathbb{K} : \mathbb{F}]\#\mathrm{Stab}(id) = [\mathbb{E} : \mathbb{F}]$. By the multiplicativity of the degree, we obtain that $\#\mathrm{Stab}(id) = [\mathbb{E} : \mathbb{K}]$. Now, notice that the stabilizer of the identity is precisely $\mathrm{Aut}(\mathbb{E}/\mathbb{K})$. Thus, $\#\mathrm{Aut}(\mathbb{E}/\mathbb{K}) = [\mathbb{E} : \mathbb{K}]$ which proves that $\mathbb{E}$ is Galois over $\mathbb{K}$. ■

In subsection 3.2, we showed that any finite extension $\mathbb{E}$ of $\mathbb{F}_p$ is Galois with a cyclic Galois group generated by the Frobenius automorphism $\delta : x \mapsto x^p$. If $\mathbb{F} \subset \mathbb{K} \subset \mathbb{E}$, then $\mathbb{K} = \mathbb{F}_{p^t}$ and so by the previous theorem, $\mathbb{E}$ must be Galois over $\mathbb{K}$. We can easily see that $\mathrm{Gal}(\mathbb{E}/\mathbb{K})$ is a subgroup of $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ from which we can deduce that $\mathrm{Gal}(\mathbb{E}/\mathbb{K})$ is cyclic and generated by $\delta^t : x \mapsto x^{p^t}$ which is called the relative Frobenius automorphism over $\mathbb{K}$. With this example, we can already start to see the correspondence between the subfields of the Galois extensions and the subgroups of the Galois group. The next theorem is the first direction of this correspondence.

Theorem 4.1.2. *Let $\mathbb{E}$ be a finite Galois extension of $\mathbb{F}$, then the map $\mathbb{K} \mapsto \mathrm{Gal}(\mathbb{E}/\mathbb{K})$ is an injection from the subfields of $\mathbb{E}$ containing $\mathbb{F}$ to the subgroups of $\mathrm{Gal}(\mathbb{E}/\mathbb{K})$.*

Proof. Let $\mathbb{K}_1$ and $\mathbb{K}_2$ be subfields of $\mathbb{E}$ containing $\mathbb{F}$ and suppose that $\mathrm{Gal}(\mathbb{E}/\mathbb{K}_1)$ is equal to $\mathrm{Gal}(\mathbb{E}/\mathbb{K}_2)$. Since $\mathbb{E}$ is Galois over both $\mathbb{K}_1$ and $\mathbb{K}_2$ by Proposition 4.1.1, then by Theorem 2.2.2, we have $\mathbb{K}_1 = \mathbb{E}^{\mathrm{Gal}(\mathbb{E}/\mathbb{K}_1)}$ and $\mathbb{K}_2 = \mathbb{E}^{\mathrm{Gal}(\mathbb{E}/\mathbb{K}_2)}$. It follows that $\mathbb{K}_1 = \mathbb{K}_2$ and so the mapping is injective. ■

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

Proof. By Theorem 4.1.2, the cardinality of the set of subfields of $\mathbb{E}$ containing $\mathbb{F}$ must be smaller than the cardinality of the set of subgroups of $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$. Since $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ is a finite group, then it must have finitely many subgroups. Therefore, there are finitely many subfields of $\mathbb{E}$ containing $\mathbb{F}$. ■

Corollary. *If $\mathbb{E}$ over $\mathbb{F}$ is a finite separable extension, then the same is true: there are finitely many subfields of $\mathbb{E}$ containing $\mathbb{F}$.*

Proof. Since $\mathbb{E}$ is a finite extension, then we can write $\mathbb{E} = \mathbb{F}(\alpha_1, ..., \alpha_n)$. For each i, let $g_i \in \mathbb{F}[x]$ be the minimal polynomial of α_i and define g as the product of the g_i's such that none of the g_i's are equal. Since $\mathbb{E}$ is separable, then all the g_i's are separable. If g isn't separable, then it must be that g_i and g_j have a common root for some i and j. But this implies that their gcd is not 1. Since both are irreducible, it follows that they are both equal to the gcd and hence equal to each other which contradicts our construction of g. Hence, even if $\mathbb{E}$ is not a splitting field, it is generated by some roots of a separable polynomial and hence, it is contained in the splitting field $\mathbb{E}_0$ of a separable polynomial. By Theorem 3.3.4, $\mathbb{E}_0$ is a Galois extension and so by the previous corollary, it must have finitely many subfields containing $\mathbb{F}$. Therefore, since any subfield of $\mathbb{E}$ is a subfield of $\mathbb{E}_0$, there must finitely many subfields of $\mathbb{E}$ containing $\mathbb{F}$. ■

In the previous corollary, the assumption that $\mathbb{E}$ is a separable extension is essential. To see why, let p be a prime number, take $\mathbb{F} = \mathbb{F}_p(x, y)$ and $\mathbb{E} = \mathbb{F}(x^{1/p}, y^{1/p})$. Notice that the field $\mathbb{F}(x)$ of rational functions is isomorphic to $\mathbb{F}(u)$ where u is transcendental over $\mathbb{F}$. Here, it will be more convenient to write u and v instead of x and y and think of them as transcendental elements over $\mathbb{F}$ and $\mathbb{F}(u)$ respectively. Hence, we have $\mathbb{F} = \mathbb{F}_p(u, v)$ and $\mathbb{E} = \mathbb{F}_p(u^{1/p}, v^{1/p})$.

First, notice that $u^{1/p}$ cannot be in $\mathbb{F}$ since otherwise, there would be polynomials **TODO**(change the name of the polynomial p to not confuse with the prime p) $p, q \in \mathbb{F}[x, y]$ such that $uq(u^p, v^p) = p(u^p, v^p)$ which is impossible since no powers are the same. Let's compute the degree of $\mathbb{E}/\mathbb{F}$ by considering the minimal polynomial of $u^{1/p}$ over $\mathbb{F}$. We know that it is a root of the polynomial $p(t) = t^p - u \in \mathbb{F}[t]$. If we let $g, h \in \mathbb{F}[t]$ be such that $p = gh$, then it means that over $\mathbb{E}[t]$, both g and h divide $p(t) = (t - u^{1/p})^p$. Thus, there exist e_1 and e_2 such that $g(t) = (t - u^{1/p})^{e_1}$ and $h(t) = (t - u^{1/p})^{e_2}$ where $e_1 + e_2 = p$. But since $g \in \mathbb{F}[t]$, then $(t - u^{1/p})^{e_1} \in \mathbb{F}[t]$. If we expend the product, we obtain

$$g(t) = t^{e_1} - e_1 u^{1/p} t^{e_1 - 1} + \cdots \in \mathbb{F}[t].$$

Hence, $-e_1 u^{1/p} \in \mathbb{F}$. If e_1 is non-zero, then we get that $u^{1/p} \in \mathbb{F}$ which is impossible so e_1 must be zero. Since e_1 is between 0 and p, then it is either equal to 0 or to p. In both cases, we get that the only divisors of p are 1 and itself. Therefore, p is irreducible and so it is the minimal polynomial of $u^{1/p}$. It follows that $[\mathbb{F}(u^{1/p}) : \mathbb{F}] = p$. Consider now the minimal polynomial $m \in \mathbb{F}(u^{1/p})[t]$ of $v^{1/p}$ over $\mathbb{F}(u^{1/p})$. Since $v^{1/p}$ satisfies the polynomial $f(t) = t^p - v$, then m divides f. It follows that $m(t) = (t - v^{1/p})^e$ over $\mathbb{E}[t]$. With a similar argument as for the previous extension, m must be equal to f. Thus, the minimal polynomial has degree p and so by the multiplicativity of the degree, $[\mathbb{E} : \mathbb{F}] = p^2$.

For all $\alpha \in \mathbb{F}$, define $\mathbb{K}_\alpha = \mathbb{F}(u^{1/p} + \alpha v^{1/p})$ which is a subfield of $\mathbb{E}$ containing $\mathbb{F}$. Notice that $\mathbb{K}_\alpha$ is an extension of degree at most p since $(u^{1/p} + \alpha v^{1/p})^p$ is an element of $\mathbb{F}$ and so the minimal polynomial has degree at most p. Suppose that $\mathbb{K}_{\alpha_1} = \mathbb{K}_{\alpha_2}$ for some distinct α_1 and α_2 in $\mathbb{F}$, then the field $\mathbb{K}_{\alpha_1}$ contains both $u^{1/p} + \alpha_1 v^{1/p}$ and $u^{1/p} + \alpha_2 v^{1/p}$ and so it must contain their substraction $(\alpha_1 - \alpha_2)v^{1/p}$. Since $(\alpha_1 - \alpha_2)$ is non-zero, then multiplying by $(\alpha_1 - \alpha_2)^{-1} \in \mathbb{F}$ gives us that $v^{1/p} \in \mathbb{K}_{\alpha_1}$. From that, we easily deduce that $u^{1/p}$ is in $\mathbb{K}_{\alpha_1}$ as well since it can be obtained by substracting $(u^{1/p} + \alpha_1 v^{1/p})$ with $\alpha_1 v^{1/p}$. Thus, since $\mathbb{K}_{\alpha_1} \subset \mathbb{E}$ contains both $u^{1/p}$ and $v^{1/p}$, we must have $\mathbb{K}_{\alpha_1} = \mathbb{E}$ which is impossible since $\mathbb{K}_{\alpha_1}$ has degree at most p and $\mathbb{E}$ has degree p^2. Thus, by contradiction, the $\mathbb{K}_\alpha$'s are distinct and so there are infinitely many of them even though $\mathbb{E}$ is an extension of finite degree.

With Theorem 4.1.2, we have shown the first part of the Galois correspondence. Our goal now is to show the reverse direction of the correspondence.

Theorem 4.1.3 (Primitive Element Theorem)**.** *If $\mathbb{E}/\mathbb{F}$ is finite and separable, then $\mathbb{E}$ contains an α such that $\mathbb{E} = \mathbb{F}(\alpha)$.*

Proof. We can assume that $\mathbb{F}$ is infinite because otherwise, $\mathbb{E}$ is a finite field and so by Theorem 0.1.2, $\mathbb{E}$ can be generated by a single element. Since $\mathbb{E}$ is a finite extension, then there exist $\alpha_1, ..., \alpha_n$ such that $\mathbb{E} = \mathbb{F}(\alpha_1, ..., \alpha_n)$. Let's prove the claim by induction on the number of generators. If $n = 1$, then $\mathbb{E} = \mathbb{F}(\alpha_1)$ and so we are done. Assume now that it holds for a natural number n and suppose that $\mathbb{E} = \mathbb{F}(\alpha_1, ..., \alpha_{n+1})$, then we can write $\mathbb{E} = \mathbb{F}(\alpha_1, ..., \alpha_n)(\alpha_{n+1})$. Since $\mathbb{E}$ is separable, then $\mathbb{F}(\alpha_1, ..., \alpha_n)$ is separable as well, so by the inductive hypothesis, there is a α_0 such that $\mathbb{F}(\alpha_1, ..., \alpha_n) = \mathbb{F}(\alpha_0)$. It follows that $\mathbb{E} = \mathbb{F}(\alpha_0, \alpha_{n+1})$. For all $t \in \mathbb{F}$, consider the subfield $\mathbb{E}_t = \mathbb{F}(\alpha_0 + t\alpha_{n+1}) \subset \mathbb{E}$ which contains $\mathbb{F}$, then by the previous Corollary, they cannot be all distinct since otherwise, there would be infinitely many subfields of $\mathbb{E}$ containing $\mathbb{F}$. It follows that $\mathbb{E}_{t_1} = \mathbb{E}_{t_2}$ for some distinct $t_1, t_2 \in \mathbb{F}$. Let $\mathbb{E}_0 = \mathbb{F}(\alpha_0 + t_1\alpha_{n+1}) = \mathbb{F}(\alpha_0 + t_2\alpha_{n+1})$ and notice that $\mathbb{E}_0$ is a field containing both $\alpha_0 + t_1\alpha_{n+1}$ and $\alpha_0 + t_2\alpha_{n+1}$, so by subtracting the two elements, $\mathbb{E}_0$ also contains $(t_2 - t_1)\alpha_{n+1}$. Since $t_2 - t_1$ is a non-zero, then $\alpha_{n+1} \in \mathbb{E}_0$. It follows that $\mathbb{E}_0 = \mathbb{E}$ which means that if we let $\alpha = \alpha_0 + t_1\alpha_{n+1}$, we obtain $\mathbb{E} = \mathbb{F}(\alpha)$. Therefore, the theorem holds by induction. ∎

The separability assumption is key in the statement. Again, consider $\mathbb{F} = \mathbb{F}_p(u, v)$ and $\mathbb{E} = \mathbb{F}_p(u^{1/p}, v^{1/p})$ for some prime p. Let's prove that $\mathbb{E}$ has no primitive element, i.e., there is no $\alpha \in \mathbb{E}$ such that $\mathbb{E} = \mathbb{F}(\alpha)$. Let $\alpha \in \mathbb{E}$, then there exist polynomials $f, g \in \mathbb{F}_p[x, y]$ such that $\alpha = f(u^{1/p}, v^{1/p})/g(u^{1/p}, v^{1/p})$. It follows that $\alpha^p = f/g \in \mathbb{F}$ which implies that $[\mathbb{F}(\alpha) : \mathbb{F}] \leq p$. Hence, the primitive element theorem fails in this particular example since we don't have separability.

To prove the converse of the Galois correspondence, recall that in the proof of Theorem 4.1.2, to show the injectivity, we used the fact that we can recover a subfield of the Galois extension containing the ground field by looking at the fixed points of a subgroup of the Galois group. It follows that the mapping $H \mapsto \mathbb{E}^H$ maps subgroups of the Galois group to subfields of $\mathbb{E}$ containing $\mathbb{F}$.

Proposition 4.1.4. *If $\mathbb{E}/\mathbb{F}$ is a finite Galois extension and H is a subgroup of the Galois group, then $[\mathbb{E} : \mathbb{E}^H] = \#H$.*

Proof. The proof that $\mathbb{E}^H$ is a subfield of $\mathbb{E}$ containing $\mathbb{F}$ is precisely the same as in Lemma 2.2.1. Hence, we can apply Theorem 4.1.1 and get that $\mathbb{E}$ is a Galois extension of $\mathbb{E}^H$, and thus, by Theorem 3.3.4, a separable extension of $\mathbb{E}^H$. Thus, by the Primitive Element Theorem, there is a $\alpha \in \mathbb{E}$ such that $\mathbb{E} = \mathbb{E}^H(\alpha)$. Define $\alpha_1, ..., \alpha_n$ as the orbit of α under the action of H on $\mathbb{E}$. By the Orbit-Stabilizer Theorem on α, we have that $n \cdot \#\text{Stab}_H(\alpha) = \#H$. Since each element of H is uniquely determined by where it maps α, then the unique element in the stabilizer is the identity map. It follows that $n = \#H$.

Define $p(x) = \prod(x - \alpha_i) \in \mathbb{E}[x]$ and let's show that it is the minimal polynomial of α. We already observed in some previous proofs that the coefficients of p are fixed by every element of H, so by definition, they are all contained in $\mathbb{E}^H$. Thus, p is a polynomial in $\mathbb{E}^H[x]$ of degree $\#H$ for which α is a root. To prove that p is irreducible over $\mathbb{E}^H[x]$, let $q \in \mathbb{E}^H[x]$ be a monic divisor of p. If q is non-trivial, then it has a root α_i in $\mathbb{E}$. By properties of automorphisms, the elements of H must map α_i to another root og q. Moreover, since H acts transitively on the α_j's, then all the α_j's are roots of q. It follows that $q = p$ and hence, the only monic divisors of p are 1 and p. Therefore, p must be the minimal polynomial of α since it is an irreducible polynomial over $\mathbb{E}^H[x]$ for which α is a root. It follows that

$$[\mathbb{E} : \mathbb{E}^H] = [\mathbb{E}^H[x]/(p) : \mathbb{E}^H] = \deg p = \#H$$

which proves our claim. ■

Corollary. *If $\mathbb{E}/\mathbb{F}$ is a finite Galois extension and H is a subgroup of the Galois group, then $H = \text{Gal}(\mathbb{E}/\mathbb{E}^H)$.*

Proof. First, since $\mathbb{E}/\mathbb{E}^H$ is Galois, then $\#\,\text{Gal}(\mathbb{E}/\mathbb{E}^H) = [\mathbb{E} : \mathbb{E}^H] = \#H$. Next, let $\varphi \in H$, then φ is a homomorphism from $\mathbb{E}$ to $\mathbb{E}$ which fixes $\mathbb{E}^H$ by definition. Thus, $\varphi \in \text{Gal}(\mathbb{E}/\mathbb{E}^H)$ and so $H \subset \text{Gal}(\mathbb{E}/\mathbb{E}^H)$. Since both are finite and have the same cardinality, then we obtain $H = \text{Gal}(\mathbb{E}/\mathbb{E}^H)$. ■

We can summarize the previous propositions into the following fundamental theorem of Galois Theory. This correspondence will let us understand the structure of Galois extensions in a deeper way.

Theorem 4.1.5 (Galois Correspondence)**.** *Given a field $\mathbb{F}$ and a finite Galois extension $\mathbb{E}$, the functions $\mathbb{K} \mapsto \text{Gal}(\mathbb{E}/\mathbb{K})$ 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* $\text{Gal}(\mathbb{E}/\mathbb{F})$.

Proof. Let A be the set of subfields of $\mathbb{E}$ containing $\mathbb{F}$ and B be the set of subgroups of the Galois group. Define the functions $\varphi_1 : A \to B$ and $\varphi_2 : B \to A$ by $\varphi_1(\mathbb{K}) = \text{Gal}(\mathbb{E}/\mathbb{K})$ and $\varphi_2(H) = \mathbb{E}^H$. Let's show that both functions are mutually inverse bijections. By Theorem 4.1.2, φ_1 is injective. To show that it is surjective, let H be a subgroup of the Galois group, then $\varphi_1(\varphi_2(H)) = \text{Gal}(\mathbb{E}/\mathbb{E}^H) = H$ by the previous corollary. Thus, φ_1 is a bijection with inverse φ_2. It follows that φ_2 must be a bijection as well. ■

4.2 Properties of the Galois Correspondence

TODO

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**$\mathrm{Gal}(\mathbb{E}/\mathbb{Q}) = D_8$.

Complements: Let $\sigma \in \mathrm{Gal}(\mathbb{E}/\mathbb{F})$ and $\mathbb{F} \subset \mathbb{K} \subset \mathbb{E}$, then $\sigma\mathbb{K}\{\sigma x : x \in \mathbb{K}\}$ is also a subfield of $\mathbb{E}/\mathbb{F}$. If H corresponds to $\mathbb{K}$ under Galois correspondence, $\sigma H \sigma^{-1}$ corresponds to $\sigma\mathbb{K}$. (it is not hard to prove why, prove it Samy **TODO**). (Lemma)

Theorem 4.2.1. *Given $\mathbb{F} \subset \mathbb{K} \subset \mathbb{E}$, then TFAE:*

1. $\sigma\mathbb{K} = \mathbb{K}$ *for all* $\sigma \in \mathrm{Gal}(\mathbb{E}/\mathbb{F})$.
2. $\mathbb{K}$ *is Galois over* $\mathbb{F}$.
3. $\mathrm{Gal}(\mathbb{E}/\mathbb{K})$ *is a normal subgroup of* $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$.

Proof. Proposition 1 is equivalent to Proposition 3 by the previous lemma. Proposition 1 implies 3 since $\sigma\mathbb{K} = \mathbb{K}$ is equivalent to $\sigma\,\mathrm{Gal}(\mathbb{E}/\mathbb{K})\sigma^{-1}$ for all $\sigma \in \mathrm{Gal}(\mathbb{E}/\mathbb{F})$, which by definition, implies that $\mathrm{Gal}(\mathbb{E}/\mathbb{K}) \trianglelefteq \mathrm{Gal}(\mathbb{E}/\mathbb{F})$. Proposition 1 implies 2 because if we consider the homomorphism $\mathrm{Gal}(\mathbb{E}/\mathbb{F}) \to \mathrm{Aut}(\mathbb{K}/\mathbb{F}) : \varphi \mapsto \varphi|_{\mathbb{K}}$ (which is well defined by Proposition 1), we get that its kernel is simply $\mathrm{Gal}(\mathbb{E}/\mathbb{K})$ which gives us (Isomorohism Theorem **TODO**). The rest of the proof is left as an exercise. **TODO** ■

5 Solvability by Radicals

Let's go back to the historical origini of Galois Theory.

Definition (Radical Extensions)**.** An extension $\mathbb{E}/\mathbb{F}$ is called a radical extension if there exists a positive integer n and $a \in \mathbb{F}$ such that $\mathbb{E} = \mathbb{F}[x]/(g)$ where g is an irreducible factor of $x^n - a \in \mathbb{F}[x]$. We could also write $\mathbb{E} = \mathbb{F}(\sqrt[n]{a})$ but since $x^n - a$ might have different irreducible factors, this notation is ambiguous.

Definition. A tower of radical extensions $\mathbb{E}/\mathbb{F}$ is a sequence

$$\mathbb{F} = \mathbb{E}_0 \subset \mathbb{E}_1 \subset \mathbb{E}_2 \subset \cdots \subset \mathbb{E}_n = \mathbb{E}$$

where $\mathbb{E}_i/\mathbb{E}_{i-1}$ is a radical extension for all $i = 1, ..., n$.

The original question of Galois theory is the following: Is every finite extensions of $\mathbb{Q}$ contained in a tower of radical extensions ? More classicaly, given a polynomial $f \in \mathbb{Q}[x]$ can its roots be expressed in terms of radicals. Notice the similarity with the problem of constructibility discussed in one of the previous sections. Recall that we solved the problem of constructibility by showing that any tower of extension must have a degree equal to a power of 2. This observation gave us a strong tool to show that some elements are not constructible. However, this is harder with towers of radical extensions since we don't have such restrictions. The goal now is to find a structural invariant of $\mathbb{Q}(\alpha)/\mathbb{Q}$ when α is a constructible by radicals. Instead of the degree, we will focus on the Galois group of the extension to find this invariant.

5.1 Automorphism Group of Radical Extensions

Let $\mathbb{F}$ be a field and $\mathbb{E}$ be a radical extension of $\mathbb{F}$ generated by the nth root of $a \in \mathbb{F}$. Notice that $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$ might only contain the identity and hence, the extension would not be Galois. Take for example $\mathbb{F} = \mathbb{Q}$ and $\mathbb{E} = \mathbb{Q}(\sqrt[3]{2})$, then we already showed that $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{1\}$.

Theorem 5.1.1. *Suppose that $\mathbb{F}$ contains n distinct nth roots of 1, and let*

$$\mu_n(\mathbb{F}) = \{x \in \mathbb{F}^\times : x^n = 1\} \cong \mathbb{Z}/n\mathbb{Z},$$

then any radical extension of $\mathbb{F}$ is Galois with an abelian Galois group.

Proof. For simplicity, write $\mathbb{E} = \mathbb{F}(a^{1/n})$. Consider the map $\eta : \mathrm{Aut}(\mathbb{E}/\mathbb{F}) \to \mu_n(\mathbb{F})$ that maps $\sigma \in \mathrm{Aut}(\mathbb{E}/\mathbb{F})$ to $\sigma(a^{1/n})a^{-1/n} \in \mu_n(\mathbb{F})$. Check that it is a homomorphism (**TODO**). Moreover, η is injective (**TODO**). ■

5.2 Some Group Theory

Definition. A finite group G is solvable if there is a sequence of subgroups $G_0, ..., G_n$ such that

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

where G_{i+1}/G_i is abelian for all $i \in \{0, ..., n-1\}$.

Example:

- Every abelian group is solvable.
- S_3 is solvable since $A_3 \cong \mathbb{Z}/3\mathbb{Z}$ is a normal subgroup of S_3 and so we get the sequence $1 \trianglelefteq A_3 \trianglelefteq S_3$ where both $A_3/1 \cong \mathbb{Z}/3\mathbb{Z}$ and $S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$ are abelian.
- Take S_4 and recall that K_4 is a normal subgroup of S_4 which is abelian. However, the sequence $1 \trianglelefteq K_4 \triangle S_3$ doens't prove that **TODO**
- The only normal subgroup of S_5 is A_5 and A_5 is simple so both S_5 and A_5 cannot be simple since they are not abelian. **TODO**

For what follows, we assume that fields all have characteristic 0.

Lemma 5.2.1. *If G is a solvable group, then any quotient $\overline{G}$ of G is solvable.*

Proof. Since G is solvable, then there exists a sequence

$$1 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

where G_{i+1}/G_i is abelian for all $i \in \{0, ..., n-1\}$. Since $\overline{G}$ is a quotient G, then there exists a surjective homomorphism $\eta : G \to \overline{G}$. For each i, we can restrict η to G_i and define $\overline{G_i}$ as $\eta(G_i)$. We can prove **TODO**that

$$1 \trianglelefteq \overline{G_2} \trianglelefteq \cdots \trianglelefteq \overline{G}$$

Moreover, the map $G_{i+1}/G_i \to \overline{G_{i+1}}/\overline{G_i} : aG_i \mapsto \eta(a)\overline{G_i}$ is surjective. It follows that $\overline{G_{i+1}}/\overline{G_i}$ is abelian. Therefore, $\overline{G}$ is solvable **TODO**. ■

Theorem 5.2.2. *If $\mathbb{E}/\mathbb{F}$ is a tower of radical extensions, then it is contained in a Galois extension with solvable Galois group.*

Proof. Let's prove it by induction on n where n denotes the length of the tower of extension. When $n = 1$, $\mathbb{E} = \mathbb{F}(\alpha)$ with $\alpha^n - a = 0$. Let $\tilde{\mathbb{E}}$ be the splitting field of $x^n - a$, then $\tilde{\mathbb{E}} = \mathbb{F}(\zeta, \alpha)$ where ζ is a primitive nth root of unity. **TODO**$\mathrm{Gal}(\mathbb{F}(\zeta)/\mathbb{F})$ is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ since any automorphism in $\mathrm{Gal}(\mathbb{F}(\zeta)/\mathbb{F})$ must map ζ to another primitive root of unity. Thus, $\mathbb{F}(\zeta)/\mathbb{F}$ is an abelian extension. Similarly, $\mathrm{Gal}(\mathbb{F}(\zeta, \alpha)/\mathbb{F}(\zeta))$ is abelian **TODO**. ■

TODO

If f is solvable by radicals, then $\mathrm{Gal}(f)$ is a solvable group.

TODO

Let's prove the converse by showing that every solvable extension of a field $\mathbb{F}$ is constructible by radicals.

Theorem 5.2.3. *Every solvable extension of a field $\mathbb{F}$ is constructible by radicals.*

Proof. $\mathbb{F}$ has characteristic 0. Two observations: It is enough to show this for abelian extensions $\mathbb{E}/\mathbb{F}$ (meaning the Galois extension is an abelian group) **TODO**. We can also assume that $\mathbb{F}$ contains the nth roots of unity.

Think of $\mathbb{E}/\mathbb{F}$ as an $\mathbb{F}$-linear representation of $G = \mathrm{Gal}(\mathbb{E}/\mathbb{F})$. Decompose $\mathbb{E}$ as $\bigoplus_{\chi \in \hat{G}} \mathbb{E}[\chi]$ where $\hat{G} = \mathrm{Hom}(G, \mathbb{F}^\times)$ **TODO**. .$\mathbb{E}[\chi] = \{v \in \mathbb{E} : \delta \cdot v = \chi(\delta) \cdot v\}$.**TODO**

Suppose $v \in \mathbb{E}[\chi]$, $v \neq 0$ and take an other vector $w \in \mathbb{E}[\chi]$. Consider the ratio w/v and let's show that it is in $\mathbb{F}$ by showing that it is fixed by every $\sigma \in G$. Let $\sigma \in G$, then $\sigma(w/v) = \sigma(w)/\sigma(v) = \chi(\sigma)w/\chi(\sigma)v = w/v$. Thus, v generates $\mathbb{E}[\chi]$ as a vector space of $\mathbb{F}$ so $\dim_{\mathbb{F}} \mathbb{E}[\chi] \leq 1$. $\dim_{\mathbb{F}} \mathbb{E} = [\mathbb{E} : \mathbb{F}] = \#G = n$ and $\dim_{\mathbb{F}} \bigoplus_{\chi \in \hat{G}} \mathbb{E}[x] \leq \#\hat{G} = \#G$. Since they are equal, then we get that $\dim_{\mathbb{F}} \mathbb{E}[\chi] = 1$ for all $\chi \in \hat{G}$.**TODO**It follows that $\mathbb{E}$ is isomorphic to $\mathbb{F}[G]$ as a G-representation (regular representation **TODO**). (Fact: this is also true for G non-abelian). For each $\chi \in \hat{G}$, let $y_\chi \in \mathbb{E}[\chi]$ be a basis, then $\mathbb{E} = \mathbb{F}(y_\chi : \chi \in \hat{G})$. Moreover, for all $\sigma \in G$, $\sigma y_\chi^n = (\sigma y_\chi)^n = \chi(\sigma)^n y_\chi^n = y_\chi^n$ so $y_\chi = a_\chi^{1/n}$ with $a_\chi \in \mathbb{F}$. Thus, $\mathbb{E} = \mathbb{F}(a_\chi^{1/n} : \chi \in \hat{G})$. ■

5.3 Cardano's solution revisited

Consider the reduced cubic $x^3 + px + q = (x - r_1)(x - r_2)(x - r_3)$. The galois group G is a subgroup of S_3. $\mathbb{E} = \mathbb{Q}(r_1, r_2, r_3)$

TODO

Every quartic polynomial is solvable since its galois group is a subgroup of S_4 which is solvable. **TODO**

Constructible Numbers. Recall that a constructible number is a number that is contained in a tower of quadratic extensions. We proved that if α is constructible, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^t$. However, the converse is not true. Let f be any irreducible polynomial of degree 8 over $\mathbb{Q}$ and assume that its Galois group is equal to S_8. **TODO**For $n \geq 4$, S_{n-1} is a maximal subgroup of S_n, i.e., no proper subgroup of S_n contains S_{n-1} properly. **TODO**Improved theorem:

Theorem 5.3.1. *α is constructible by ruler and compass if and only if $\mathbb{Q}(\alpha)$ is contained in a Galois extension $\mathbb{E}/\mathbb{Q}$ with $\mathrm{Gal}(\mathbb{E}/\mathbb{Q}) = 2^t$.*

Proof. Think about it. ■

Every group of cardinality p^t is solvable when p is a prime. By looking at the class equation of a group of cardinality p^t, we obtain that the center of G is always a non trivial normal subgroup of G. If we consider $\tilde{G_1} = Z(G/Z(G))$, then the inverse image G_1 is a normal subgroup of G that contains $Z(G)$. **TODO**

5.4 Fundamental Theorem of Algebra

Some facts:

1. Every polynomial of odd degree in $\mathbb{R}[x]$ has a root in $\mathbb{R}$ by the Intermediate Value Theorem. Thus, $\mathbb{R}$ cannot have an extension of odd degree.

2. Every quadratic equation in $\mathbb{C}[x]$ has a root.

Theorem 5.4.1. *The field of complex numbers $\mathbb{C}$ is algebraically closed.*

Proof. Let $\mathbb{K}$ be a finite extension of $\mathbb{C}$, then it is also a finite extension of $\mathbb{R}$. Let $\mathbb{K}'$ be the Galois closure of $\mathbb{K}$ over $\mathbb{R}$ and G be the Galois group of $\mathbb{K}'$ over $\mathbb{R}$. If we write **TODO** ■

How does one compute the Galois group of a polynomial ? If f is irreducible with degree n, then the Galois group is a subgroup of S_n since it acts on the n roots of f. Define the resolvent of f as the polynomial in n variables defined by

$$R(x_1, ..., x_n) = \prod_{\sigma \in S_n} (r_1 x_{\sigma(1)} + \cdots + r_n x_{\sigma(n)})$$

Since R is fixed under the action of G, then R is a polynomial in $\mathbb{F}[x_1, ..., x_n]$. Now, factor R as $R_1 \cdot \cdots \cdot R_t$.

Proposition 5.4.2. *G is the stabilizer of one of the R_i.*

Proof. We can rewrite R as $\prod_{\epsilon \in S_n/G} \prod_{\sigma \in \epsilon} (\dots)$. Each factor inside is irreducible over $\mathbb{F}$ and the stabilizer of R is G. **TODO** ■

The question of calculating G given f is connected to the problem of factoring polynomials over fields. If $f \in \mathbb{F}_p[x]$, then it is easy to factor. To find the roots of f, we can take the gcd of f and $x^p - x$.

The converse problem: Given a finite group G, is there an extension $\mathbb{E}/\mathbb{Q}$ with $\mathrm{Gal}(\mathbb{E}/\mathbb{Q}) = G$. This is very much open. However, there is an easier result. There exist $\mathbb{E}/\mathbb{F}$ with $[\mathbb{F} : \mathbb{Q}] < \infty$ with $\mathrm{Gal}(\mathbb{E}/\mathbb{F}) = G$. By Cayley, we know that $G \subset S_n$ for some n. Assume without loss of generality that n is prime. Let $\mathbb{E}/\mathbb{Q}$ be an extension with Galois group S_p. Hence, if we define $\mathbb{F} = \mathbb{E}^G$ (can be visualized by the Galois correspondence), we obtain that $\mathrm{Gal}(\mathbb{E}/\mathbb{F}) = G$.