This document is written to summarized the Galois theory as taught by professor S. Baek. as a part of the Modern Algebra 2, MAS312, at KAIST. The author is responsible for all mistakes and error in the document.

# Preliminary

Before continuing reading this, be warned that the following content is aimed as a summary or a recap, not as a tutorial that would helps through the subject. The readers are adviced to have enough basic background on group and field theory as the detail and intuition for those things might not be included in the pages.

The course, MAS312, thought much more than this but details unrelated to achieving the main goal, that polynomial degree exceeding 5 are unsolvable, are omitted.

However, some of the basic prerequisite would also be provided in this section, as a reminder.

**Definition 0.1: Solvable Group**

For a group $G$, denote $G_0 = G$ and $G_i = [G_{i-1}, G_{i-1}]$, the commutator of $G_{i-1}$. Then, the group is called solvable when the chain of subgroup

$$G = G_0 > G_1 > \cdots > G_n > \cdots$$

that terminates.

Equivalently, if there is a chain of subgroup of $G$ of the form

$$\{ e \} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

where each $G_i/G_{i-1}$ is abelian, then $G$ is solvable.

Also, there is an important result for the solvable group, which is that

**Theorem 0.1**

$G$ is solvable if and only $N$ and $G/N$ is solvable for any (some) $N \lhd G$.

**Definition 0.2: Field Composition**

Let $E/F$ be a field extension with intemediate field $L$ and $K$, then $LK$ denotes the composite field, which is the smallest subfield of $E$ containing $L$ and $K$.

Notice that if $K = F(\alpha_1, \ldots, \alpha_n)$, then $LK = L(\alpha_1, \ldots, \alpha_n)$ by the definition. Moreover, The field composition will later be needed in the proof of the galois theorem, so note that if $E/F$ is galois, then $E/KL$ is also galois with the galois group $\mathrm{Gal}(E/F) = \mathrm{Gal}(E/K) \cap \mathrm{Gal}(E/L)$.

# 1 Normal Extensions

To get started, let refresh the defition of a splitting field.

> Note: Splitting field $E$ of $f$ over $F$ is the field $F(\alpha_1, \cdots, \alpha_n)$ where each of the $\alpha_i$ is a root of $f$. This implies that $E$ is the smallest field extension that $f$ factors into linear terms.

And the important properties of field extensions is presented in the following lemma.

**Lemma 1.1**

Let $E = F(\alpha)$ be a finite extension of $F$ and let $L/K$ be an extension with a homomorphism $\phi : F \to K$. Then,

1. For any root $\beta$ of $\phi(f)$ in $L$, there is a homomorphism $\psi : E \to L$ such that $\psi(\alpha) = \beta$ and $\psi|_F = \phi$.
2. If $\psi : E \to L$ is an extension of $\phi$, then $\psi(\alpha)$ is a root of $\phi(f)$.
3. If $G/F$ is a field extension, then there exists an extension $H/K$ with $\psi : G \to H$ extending $\phi$.

***Proof:*** TODO □

Then, it is possible to define the normal field extension, and extension which, will be later related with normal subgroups. As there is multiple equivalent definition of a normal extension, consider first that these few statements are equivalent.

**Theorem 1.2**

The following are equivalent

1. $E$ is a splitting field of some polynomial over $F$
2. For any extension $L/E$ and homomorphism $\phi : E \to L$ with $\phi|_F = \mathrm{id}_F$, $\phi(E) = E$
3. Every irreducible polynomial $f$ over $F$ that has a root in $E$ spilts in $E$

***Proof:*** consider this chain of implication:
$(1 \Rightarrow 2)$:

Assuming that $E$ is a splitting field of $f$ over $F$, then let $\alpha_1, \ldots, \alpha_n$ be all the roots of $f$. This means that $E = F(\alpha_1, \ldots, \alpha_n)$.

Let $\phi$ be any homomorphism sending $E \to L$ such that $\phi|_F = \mathrm{id}_F$, then

$$0 = \phi(0) = \phi(f(\alpha_i)) = \phi(f)\phi(\alpha_i) = f(\phi(\alpha_i))$$

Therefore, $\phi$ sends $\alpha_i \mapsto \alpha_j$ for all $i$ and for some $j$. Thus, $\phi(E) \subset E$ because each of the generators of $\phi(E)$ is present in $E$.

Next, assuming $0 \neq e \in \ker(\phi)$, then, the minimal polynomial of $e$ is $m_e(x) = a_n x^n + \cdots + a_0$ with $a_0 \neq 0$. This is because if $a_0 = 0$, then $m_e$ is reducible, contradicting that it is minimal. So,

$$-a_0 = \phi(0 - a_0) = \phi(m_e(e) - a_0) = \phi(a_n e^n + \cdots + a_1 e) = \phi(e)\phi(a_n e^{n-1} + \cdots + a_1) = 0$$

since $\phi(e) = 0$. This yield a contradiction, thus $\ker(\phi) = \{\, 0 \,\}$.

Then, as $[E : F]$ is finite, it must be the case that $\phi(E) = E$.

$(2 \Rightarrow 3)$:

Let $f$ be an irreducible polynomial over $F$ that has a root in $E$, namely $\alpha$. Then, let $L$ be the splitting field of $f$ over $E$.

Let $\beta$ be any roots of $f$ in $L$, then there is an extension $\phi : F(\alpha) \to L$ such that $\phi(\alpha) = \beta$. Also, there is an extension $K/L$ and $\psi : E \to K$ wit $\psi|_{F(\alpha)} = \phi$. These are due to the Lemma 1.1

By assumption, $\psi(\alpha) = \phi(\alpha) = \beta$ and $\phi(E) = E$, therefore, $\beta \in E$ for any $\beta$. Thus, $f$ splits in $E$.

$(3 \Rightarrow 1)$:

As $E/F$ is finite, then $E = F(\beta_1, \cdots, \beta_n)$ for some $\beta_i \in E$. For each $i$, let $f_i$ be the minimal polynomial of $\beta_i$, so that $f_i$ is irreducible and $f_i(\beta_i) = 0$.

By assumption, $f_i$ splits in $E$. Therefore, $E$ is a splitting field of $f_1 \cdot f_2 \cdots f_n$

□

From the previous theorem, the defintion of a normal extension is as follow:

**Definition 1.1: Normal Extensions**

Let $E/F$ be a finite extension. $E/F$ is called normal if and only if $E$ satisfied any of the condition in theorem 1.2

In fact, normal Extensions can be defined not only on finite extensions but any algebraic extensions. This was not included in the course and thus, will not be included in this summary.

**Corollary 1.3**

Let $E = F(\alpha_1, \ldots, \alpha_n)$ be a field extension over $F$, Then, $E/F$ is normal if and only if every minimal polynomial $m_{\alpha_i}$ of $\alpha_i$ splits in $E$.

***Proof:***
$(\Longrightarrow)$:

follow from theorem 1.2

$(\Longleftarrow)$:

Let $f = \prod_{i=1}^{n} m_{\alpha_i}$. Then, $f$ splits over $E$ as every $m_{\alpha_i}$ splits over $E$ by assumption. As all generators of $E$ is a root of $f$, then $E$ is the splitting field of $f$ over $F$. Therefore, $E$ is normal.

□

One would expect the normal extension to be transitive, but it is not. One of the many counterexamples of transitivity is the tower $\mathbb{Q}(\sqrt[4]{5})/\mathbb{Q}(\sqrt{5})/\mathbb{Q}$, in which each consecutive pair of extension is normal, but $\mathbb{Q}(\sqrt[4]{5})/\mathbb{Q}$ is not normal.

However, there is a weak sense of normal that is left to the smaller, restricted subfield.

**Corollary 1.4**

Let $L/E/F$ be a tower of field extensions, then if $L/F$ is normal, $L/E$ is also normal.

***Proof:*** Let $L$ be a splitting field of $f \in F[x]$, then $L$ is also a splitting field of $f \in E[x]$. Thus, normal by definition. □

Lastly, the normal closure of a field extension is just the smallest field extensions that is normal. The following are formalization of said idea.

**Definition 1.2: Normal Closure**

Let $E/F$ be a field extension, then $K$ is a normal closure of $E$ if $K/F$ is a normal extension and $[K : F]$ is minimal. ie. There is no intermediate field $K/L/F$ such that $L/F$ is normal.

**Theorem 1.5: Uniqueness of Normal Closure**

Let $E/F$ be an extension, then there exists a unique normal closure $L$ of $E/F$ up to an isomorphism fixing $E$.

***Proof:*** Let $E = F(\alpha_1, \cdots, \alpha_n)$ and $m_{\alpha_i}$ be the minimal polynomials. Let $L$ be the splitting field of $f = \prod_{i=1}^{n} m_{\alpha_i}$ over $E$. Then, $L$ is the splitting field of $f$ over $F$.

Then there be intermediate field $L/K/E$ such that $K/F$ is normal, then $K/E$ must be normal. So, $f$ must splits in $K$. Thus, $L = K$. So, $L$ is a normal closure.

For the uniqueness, assume that there is $L'$, another closure of $E/F$. Then $L'$ must also be a splitting field of $f$. By the uniqueness of splitting field, $L' \simeq L$. □

## 2 Separable Extensions

Separable extensions are easier for the intuition than normal extensions. It captures the notion of duplicated roots, similar to the two equal roots of the polynomial $x^2 - 2x + 1$, which is $x = 1$.

Although the definition of separable is not yet formally defined, a rough explanation can be given. If a polynomial is divisible by some square of linear factor, then there is a multiple (duplicated) root, and otherwise, there is none. However, checking all the divisor is a lot more difficult than checking the derivative, especially the derivative of a polynomial, hence the following useful lemma.

**Lemma 2.1**

a root $\alpha$ of a polynomial $f$ is with multiplicity 1 (ie. simple, no multiple roots) if and only if $f'(\alpha) = 0$.

***Proof:***
($\Longrightarrow$):

If $f(x) = (x - \alpha)g(x)$, then $f'(x) = g(x) + (x - \alpha)g'(x)$. As $g(\alpha)$ is non-zero, then $f'(\alpha) = g(\alpha) \neq 0$

($\Longleftarrow$):

If $f(x) = (x - \alpha)^2 g(x)$, then $f'(x) = 2(x - \alpha)g(x) + (x - \alpha)^2 g'(x)$ So, $f'(\alpha) = 0$.

□

**Theorem 2.2**

Let $f \in F[x]$ be a polynomial, then the following are equivalent.

1. $f$ and $f'$ are relatively prime.
2. $f$ has no multiple roots in any field extension of $F$.
3. There is a field extension $E/F$ such that $f$ splits over $E$ and $f$ has no multiple roots in $E$.

***Proof:***
($1 \Rightarrow 2$):

Follow from lemma 2.1

($2 \Rightarrow 3$):

Take $E$ to be the splitting field of $f$ over $F$, then $E$ is an extension of $F$.

($3 \Rightarrow 1$):

Assume that $f$ and $f'$ has a common factor $d$. Then $d \mid \gcd(f, f')$ implying that $d^2 \mid f$. This can be checked using standard arithmetic. Thus, if $d \neq 1$, then $(x - \alpha) \mid d$, so $f$ has a multiple root.

□

From above theorem, one could define the word separable for polynomial, and moreover, for an element over some base field.

**Definition 2.1: Separable Polynomial, Element**

A polynomial $f$ is called separable if it satisfies theorem 2.2. An element $\alpha \in E$ that is algebraic over $F$ is called separable over $F$ if the minimal polynomial of $\alpha$ over $F$ is separable.

**Corollary 2.3**

If $f \in F[x]$ is an irreducible polynomial such that $f' \neq 0$, $f$ is separable.

***Proof:*** Assume that $f$ has multiple roots, then $f$ and $f'$ is not coprime. Then, $f \mid f'$ as $f$ is irreducible. However, $\deg f' \leq \deg f$ which implies $f = f' = 0$ □

**Lemma 2.4**

Let $E/F$ be any finite field extension, and $\sigma : F \to K$ be a field homomorphism. Then there exists at most $[E : F]$ extension $\tau : E \to K$ of $\sigma$.

***Proof:*** Let $E = F(\alpha_1, \ldots, \alpha_n)$, then the proof proceed by induction. If $n = 1$, then $E = F(\alpha)$. Let $m_\alpha$ be the minimal polynomial of $\alpha$. This implies

$$0 = \tau(0) = \tau(m_\alpha(\alpha)) = \sigma(m_\alpha)(\tau(\alpha))$$

Therefore, $\tau(\alpha)$ is a root of $\sigma(m_\alpha)$.

Hence, the number of extension $\tau$ of $\sigma$ is equal to the number of distinct root of $\sigma(m_\alpha)$, which is equal to the number of distinct root of $m_\alpha$, which is bounded by $[E : F]$.

Now, for $n > 1$, assume for induction that the statement holds for $E = F(\alpha_1, \ldots, \alpha_{n-1})$. As $E = F(\alpha_1, \ldots, \alpha_n) = F(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)$. The number of extensions of $\sigma$ is then bounded by $[E : F(\alpha_1, \ldots, \alpha_{n-1})][F(\alpha_1, \ldots, \alpha_{n-1}) : F]$ where the first term is from the case of $n = 1$, and the latter term is from the induction hypothesis. □

Notice also that any irreducible polynomial $f$ over $\mathbb{Q}$ is separable, since $f' = 0$ if and only if $f$ is of degree 0. That means $f$ must be a constant function. As $f$ is irreducible, $f$ cannot be constant, so $f' \neq 0$, which implies that $f$ is separable.

This kind of extensions that have similar property as $\mathbb{Q}$ are called perfect fields. The detail of perfect field was given in the class, but would be too irrelevant for this paper, so the author excluded it.

One might expect that the definition of separable field extension is close to the definition for polynomial or elements, but, it was defined in a different way.

**Definition 2.2: Separable Field Extension**

A field extension $E/F$ is called separable if there is a field homomorphism $\sigma : F \to K$ that has exactly $[E : F]$ extensions.

However, the definition below also is related to the sense of separability introduced earlier. This will be proven in the next theorem.

**Theorem 2.5**

A finite extension $F(\alpha)/F$ is separable if and only if $\alpha$ is separable over $F$.

***Proof:***
($\Longrightarrow$):

Let $m_\alpha$ be the minimal polynomial of $\alpha$. By definition, there is a mapping $\sigma : F \to K$ such that there is $\deg(m_\alpha) = [F(\alpha) : F]$ extensions. Since each extension $\tau$ map $\alpha$ to a root of $\sigma(m_\alpha)$, then $\sigma(m_\alpha)$ must have $[F(\alpha) : F]$ distinct roots, so $m_\alpha$ must have $\deg(m_\alpha)$ distinct roots, thus it is separable.

($\Longleftarrow$):

Let $E$ be a splitting field of $m_\alpha$, the minimal polynomial of $\alpha$. Then let $\sigma : F \to E$. As $m_\alpha$ is separable, then $m_\alpha$ has exactly $\deg(m_\alpha) = [F(\alpha) : F]$ distinct roots. Therefore, there is $[F(\alpha) : F]$ extensions which are $\tau$ that sends $\alpha$ to each of the roots of $m_\alpha$.

□

This tie the definition of separable field extension and the definition of separable element loosely, then the next theorem, another important result of a separable extension is that it is the extension is generated by a single element. These two theorems together show that all separable extension $E/F$ is, in fact, $F(\alpha)/F$ where $\alpha$ is separable.

**Theorem 2.6**

Let $E/F$ be a finite separable extension, then $E = F(\alpha)$ for some $\alpha \in E$.

***Proof:*** TODO □

# 3 Galois Group and Extensions

For any field extension or polynomial, one can define the Galois group.

**Definition 3.1: Galois Group**

Let $E/F$ be a field extension, then

$$\mathrm{Gal}(E/F) = \mathrm{Aut}_F(E) = \{\, \sigma : E \to E \mid \sigma|_F = \mathrm{id}_F \,\}$$

and for a polynomial $f \in F[x]$ $\mathrm{Gal}(f) = \mathrm{Gal}(K/F)$ where $K$ is the splitting field of $f$ over $F$.

**Remark 1**

For a polynomial $f$ over $F$, an automorphism $\sigma$ that fixes $F$, and $E = F(\alpha_1, \ldots, \alpha_n)$ being the splitting field of $f$ over $F$ where $\alpha_i$ are roots of $f$. For any $i$, the following holds:

$$0 = \sigma(0) = \sigma(f(\alpha_i)) = f(\sigma(\alpha_i))$$

Therefore, $\sigma$ maps $\alpha_i$ to $\alpha_j$ for all $i$ and some $j$. Thus, $\mathrm{Gal}(f)$ acts on the set $\{\, \alpha_1, \ldots, \alpha_n \,\}$. So there is an embedding $\mathrm{Gal}(f) \hookrightarrow S_{\deg f}$

**Definition 3.2: Galois Extension**

A finite extension $E/F$ is called Galois if $|\mathrm{Gal}(E/F)| = [E : F]$

Notice that for any finite field extension, $E/F$, it must follow that $|\mathrm{Aut}(E/F)| \leq |\mathrm{Emb}_F(E, \cdot)|$, because one might have a embedding of $E$ fixing $F$ to certain field, apart of $E$. In fact, the equality follows if $E/F$ is normal. If $E/F$ is normal, then by the definition, the homomorphism fixing $F$ must have image $E$, therefore, every embedding of $E$ fixing $F$ must be an isomorphism.

Moreover, generally, $|\mathrm{Emb}_F(E, \cdot)| \leq [E : F]$ as shown in the section of separable extension. If $E/F$ is separable, then by definition, the number of embedding of $E$ fixing $F$ must equal to $[E : F]$.

This lead to the next theorem proving that a galois extension is normal and separable. In fact, the converse also hold.

**Theorem 3.1: Galois is Normal and Separable**

An extension $E/F$ is Galois if and only if it is a normal and separable extension.

***Proof:***

($\Longrightarrow$):

Since there are $\mathrm{Gal}(E/F) = [E : F]$ automorphisms fixing $F$, then $\mathrm{id} : F \hookrightarrow E$ has exactly $[E : F]$ extensions, so $E/F$ is separable. Let $K \supset E$ be a field extension with any $\tau : E \to K$ that extends identity on $F$, then consider

$$A = \{\, \sigma : E \to E \hookrightarrow K \mid \sigma \in \mathrm{Gal}(E/F) \,\}$$

Then, $\tau \in A$ and $|A| = [E : F]$. This means that $\tau(E) = E$. Therefore, $E/F$ is normal.

($\Longleftarrow$):

Since $E/F$ is separable, then there is a homomorphism $\sigma : F \to K$ that have $[E : F]$ extensions. Notice that field homomorphism is injective, thus $F \simeq \sigma(F)$. Let those extensions be $\tau_1, \ldots, \tau_m$, and let $\tau_i' = \tau_i \circ \tau_1^{-1}$ so that $\tau_i'$ fixes $\sigma(F)$. Then, $\tau_1(E) \simeq E$ as $\tau_1$ is injective.

As $E/F$ is normal, $\tau_i'(\tau_1(E)) = \tau_1(E)$ for all $1 \leq i \leq m$. Therefore, there are exactly $m = [E : F]$ automorphisms $\tau_1(E) \to \tau_1(E)$ fixing $\sigma(F)$. This translates to that $|\mathrm{Gal}(\tau_1(E)/\sigma(F))| = |\mathrm{Gal}(E/F)| = m = [E : F]$.

□

### Lemma 3.2

Let $f$ be a non-constant separable polynomial over $F$, then if $\alpha$ is a root of $f$, $\deg(\alpha) = |\mathrm{Gal}(f)\alpha|$, the orbit of $\alpha$.

***Proof:*** Notice that $\mathrm{Gal}(f)\alpha = \{\, \sigma(\alpha) \mid \sigma \in \mathrm{Gal}(f) \,\}$. Let $E/F$ be the splitting field of $f$. Now,

$$\deg(\alpha) = [F(\alpha) : F] = \frac{[E : F]}{[E : F(\alpha)]}$$

As $E/F$ is Galois, the extension $E/F(\alpha)$ is also Galois as from corollary 1.4 and theorem 3.1. Since $[E : F(\alpha)] = |\mathrm{Gal}(E : F(\alpha))| = \left|\mathrm{Aut}_{F(\alpha)}(E)\right|$ is the automorphism fixing $F(\alpha)$, then the result follows by the orbit stabilizer theorem. □

From this lemma, it is obtained that for a polynomial of degree $n$, there is at most $n$ roots, and the galois group $G$ acts on the set of roots, thus there must be a map $G \hookrightarrow S_n$.

Moreover, if $f$ is irreducible, then the there is only one orbit of $\alpha$, a root of $f$. This means that the galois group of $f$ must be a transitive subgroup of $S_n$. This observations can help when determining the galois group for given polynomials.

As separable extensions are transitive, and normal extensions are halfly transitive, in the sense of corollary 1.4. Then a Galois extension is also halfly transitive in the same sense.

Next, the galois correspondence theorem connects the field theory with the group theory. Here, the notion of normal field extension and normal subgroup starts to be related. The galois correspondence theorem connects the notion of subfield, ie. intermediate field extensions with subgroup of the galois group by using group action.

The path begins with the fixed point theorem.

### Theorem 3.3: Galois and Fixed Point

Let $G < \mathrm{Aut}(E)$ be a finite subgroup of the group of automorphisms of $E$, and let

$$F = E^G = \{\, \alpha \in E \mid \sigma(\alpha) = \alpha \forall \sigma \in G \,\}$$

be the fixed point of $E$ regarding the action of $G$.
Then $E/F$ is Galois with the corresponding group $\mathrm{Gal}(E/F) = G$.

***Proof:*** For any extensions, $[E : F] \geq |\mathrm{Gal}(E/F)| \geq |G|$, therefore, it suffices to show that $|G| \geq [E : F]$.

#### Claim 1

Let $\alpha \in E$ and $G\alpha = \{\, \sigma(\alpha) \mid \sigma \in G \,\}$ denotes the orbit of $\alpha$. Let $f = \prod_{\beta \in G\alpha}(x - \beta)$ so that $f(\alpha) = 0$ and $f$ has no multiple roots.

Choose any $\tau \in G$, then $\tau$ fixes $G\alpha$ as $G\alpha = \{\, \tau(\beta) \mid \beta \in G\alpha \,\}$. Thus, $\tau(f) = f$. As $f$ is separable over $F$ and $f(\alpha) = 0$, then $m_\alpha$ is separable over $F$. Thus, $F(\alpha)/F$ is separable, and $[F(\alpha) : F] = \deg(m_\alpha) \leq \deg(f) = |G\alpha| \leq |G|$

Now, assume for contradiction that $[E : F] > |G|$, then there exists $K = F(\alpha_1, \ldots, \alpha_n)$ such that $[K : F] > |G|$. Also, as $K/F$ is seperable, then $K = F(\beta)$ by theorem 2.6. However, $[F(\beta) : F]$ corresponds to the claim (1), and thus $[F(\beta) : F] \leq |G|$. This is a contradiction, thus $[E : F] \leq |G|$, which means $[E : F] = |G|$ □

The theorem describes that the extension by restricting a field to its subfield fixed by certain group, the degree of the restriction, corresponds to the index of the group.

### Theorem 3.4: Correspondence

Let $E/F$ be a galois extension with $G = \mathrm{Gal}(E/F)$, then there is a 1-1 correspondence between the set of subgroup of $G$ and the subfields of $E$ containing $F$. The correspondence is given by

$$\phi : K \mapsto \mathrm{Gal}(E/K)$$

and

$$\phi^{-1} : E^H \nleftarrow H$$

***Proof:*** The proof will show that $\mathrm{Gal}(E/E^H) = H$ and $E^{\mathrm{Gal}(E/K)} = K$. The former one follows from the previous theorem 3.3.

For the latter one, let $H = \mathrm{Gal}(E/K)$, then $K \subset E^H$ as $K$ is fixed by all actions in $H$. Then, $|H| = [E : E^H]$ by the previous theorem 3.3. As $E/F$ is galois, then $E/K$ must also be galois by the "half" transitivity mentioned earlier, so $[E : K] = |H|$.

As $|H| = [E : E^H] = [E : K]$, with $K \subset E^H$ then $[E^H : K] = 1$ by the tower rule, which means $E^H = K$. □

Moreover, if $K/E/F$ is an extension such that $K/E$, $K/F$, $E/F$ are galois, then the result also extends to that $\mathrm{Gal}(K/E) \lhd \mathrm{Gal}(K/F)$ and $\mathrm{Gal}(E/F) \simeq \mathrm{Gal}(K/F)/\mathrm{Gal}(K/E)$. This can be proven as a corollary to the theorem.

**Corollary 3.5**

$K/E/F$ is an extension such that $K/E$, $K/F$ are galois, then $E/F$ is normal if and only if $\mathrm{Gal}(K/E) \lhd \mathrm{Gal}(K/F)$. In that case, $\mathrm{Gal}(E/F) \simeq \mathrm{Gal}(K/F)/\mathrm{Gal}(K/E)$.

***Proof:***

$$\begin{aligned}
\mathrm{Gal}(K/E) \lhd \mathrm{Gal}(K/F) &\iff \sigma\,\mathrm{Gal}(K/E)\sigma^{-1} = \mathrm{Gal}(K/E) && \forall \sigma \in \mathrm{Gal}(K/F) \\
&\iff \sigma(E) = E && \forall \sigma \in \mathrm{Gal}(K/F) \\
&\iff E \text{ is normal over } F
\end{aligned}$$

where the first line to second can be observed by the correspondence of $\sigma(E)$ and $\sigma H \sigma^{-1}$ where $H = \mathrm{Gal}(K/E)$.

Moreover, when the galois subgroup is normal, $\mathrm{Gal}(K/F)/\mathrm{Gal}(K/E) \simeq \mathrm{Gal}(E/F)$ is given by a homomorphism $\phi : \sigma \mapsto \sigma|_E$ and the first isomorphism theorem. □

# 4 Cyclotomic Extensions

Cyclotomic extensions literally means the extensions that splits (tomic) a circle (cyclo). This extensions are the extension adjoining the roots of unity, as the roots of unity splits the unit circle into equal sections.

Firstly, the $n$th roots of unity are those number that equal 1 when raised to the $n$th power. Equivalently, the $n$th roots of unity are the roots of the polynomial $f(x) = x^n - 1$. This polynomial exists over all field as the only coefficient is 1. Notice that $f$ is separable over all field with characteristic coprime to $n$.

Let $\mu_n$ be a group of the roots of unity,

$$\mu_n = \{\, \eta \mid \eta^n = 1 \,\}$$

then $\mu_n$ is cyclic.

**Definition 4.1: primitive $n$th root of unity**

Since $\mu_n$ is cyclic, define the generators of $\mu_n$ as the primitive $n$th root of unity.

The course did also provide more information regarding the cyclotomic polynomial, such as the cyclotomic extension on other field of characteristic $p$. However, the detail will be omitted.

It is enough to realize that for a primitive $n$th root $\eta$, $\mathbb{Q}(\eta)/\mathbb{Q}$ is the splitting field of the polynomial $x^n - 1$, which is a galois extension. Moreover, $\mathrm{Gal}(\mathbb{Q}(\eta)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ is abelian.

Cyclotomic extensions study the adjoint of a primitive root to a field, kummer extensions, based on cyclotomic, study the adjoint of certain elements on to a field already containing a primitive root.

# 5 Kummer Extension

Kummer extensions can be thought of as extensions of cyclotomic extensions. This is because the base field of a kummer extension is assumed to contain the group $\mu_n$ of roots of unity.

**Definition 5.1: exponent**

An exponent of a group $G$, denoted $\exp(G)$ is the least number $n$ such that $g^n = 1$ for any element $g \in G$. Equivalently, it is the least common multiple of the order of each element in $G$.

Starting with a lemma that assure every distinct group homomorphism to non-zero element of a field are linearly independent.

**Lemma 5.1**

Let $G$ be any group and $F$ be a field. A set $\{ \sigma_1, \dots, \sigma_n \}$ of homomorphism from $G \to F^\times$ is linearly independent. Formally,

$$\exists a_i \in F \sum_{i=1}^{n} a_i \sigma_i = 0 \implies \forall i \; a_i = 0$$

***Proof:*** At $n = 1$, $a_1\sigma_1 = 0$ implies $a_1 = 0$ if $\sigma_1$ is non-zero. Then, the proof proceed by induction.

Assuming the induction hypothesis, and consider that there exists $y$ such that $\sigma_1(y) \neq \sigma_n(y)$ as $\sigma_1 \neq \sigma_y$.

If $\sum_{i=1}^{n} a_i\sigma_i = 0$, then for any $x \in G$,

$$\sum_{i=1}^{n} a_i\sigma_i(x) = \sum_{i=1}^{n} a_i\sigma_i(yx) = 0$$

From that,

$$0 = \sum_{i=1}^{n} a_i\sigma_i(yx) - \sigma_n(y)\sum_{i=1}^{n} a_i\sigma_i(x) = \sum_{i=1}^{n-1} a_i\sigma_i(x)(\sigma_i(y) - \sigma_n(y))$$

As $\sigma_1(y) \neq \sigma_n(y)$, then $a_1 = 0$. Then $\sum_{i=1}^{n} a_i\sigma_i = \sum_{i=2}^{n} a_i\sigma_i = 0$ implying $a_i = 0$ for all $i$ by the induction hypothesis. □

Again, kummer extensions assume the presence of the group of root of unity in the base field. Moreover, a galois field extension $E/F$ is said to be cyclic or abelian, if $\mathrm{Gal}(E/F)$ has that property. Note also that the degree of the extension must corresponds to the order of the group assuming that $E/F$ is galois.

**Theorem 5.2**

Let $\mu_n \subset F$.
$E/F$ is cyclic of degree $n$ if and only if $E$ is a splitting field of some irreducible $x^n - a$.

***Proof:***
($\implies$):

Notice that $E/F$ is galios with $\mathrm{Gal}(E/F)$ cyclic, so $\mathrm{Gal}(E/F) = \{ \mathrm{id}, \sigma, \sigma^2, \cdots, \sigma^{n-1} \}$ By the previous lemma 5.1, the element in $\mathrm{Gal}(E/F)$ is linearly independent. So,

$$\sum_{i=1}^{n} \eta^i\sigma_i \neq 0$$

Choosing $\alpha$ making the sum $\beta = \sum_{i=1}^{n} \eta^i\sigma_i(\alpha)$ being non-zero, it follows that

$$\sigma(\beta) = \eta\sigma^2(\alpha) + \cdots + \eta^{n-2}\sigma^{n-1}(\alpha) + \eta^{n-1}\mathrm{id}(\alpha)$$

which means that $\eta\sigma(\beta) = \beta$, or $\sigma(\beta) = \eta^{-1}\beta$.

As $\beta^n$ is fixed by $\sigma$, and thus by $\sigma^i$, then it must be an element in $F$. So, let $a = \beta^n$. Now, since

$$x^n - a = (x - \beta)(x - \beta\eta)\cdots(x - \beta\eta^{n-1})$$

is split in $F(\beta)$, $F(\beta)$ is the splitting field of $x^n - a$. However, for all $1 \leq i < n$, $\sigma^i$ moves $\beta$. So the galois group $\mathrm{Gal}(E/F(\beta))$ can only contain id, which by theorem 3.4, means $E = F(\beta)$ is the splitting field of $x^n - a$.

($\Longleftarrow$):

Let $E$ be a splitting field of $f(x) = x^n - a$. Since $\mu_n \in F$, then $x^n - 1$ has exactly $n$ roots in $F$, therefore $x^n - 1$ is separable, so $\mathrm{char}\, F = 0$ or $\mathrm{char}\, F$ is coprime to $n$.

As $(x^n - a)' = nx^{n-1} \neq 0$, then $x^n - a$ is also separable, thus $E/F$ is galois. Now, let $\alpha$ be a root of $x^n - a$, Since any homomorphism $\sigma \in \mathrm{Gal}(E/F)$ maps a root of $f$ to a root of $f$, then $\sigma(\alpha)/\alpha \in \mu_n$. So there is a homomorphism $\phi : \mathrm{Gal}(E/F) \to \mu_n$ given by $\sigma \mapsto \sigma(\alpha)/\alpha$

Now, $\phi$ is injective as the kernel is $\sigma$ such that $\sigma(\alpha) = \alpha$, which can only be the identity as $E = F(\alpha)$.

As $|\mathrm{Gal}(E/F)| = n = |\mu_n|$, then $\mathrm{Gal}(E/F) \simeq \mu_n$ by the first isomorphism theorem. So $\mathrm{Gal}(f)$ is cyclic of order $n$.

□

Next, moving from a cyclic extension to an abelian extension.

**Theorem 5.3**

Let $\mu_n \subset F$ and $E/F$ be galois.
$E/F$ is galios and abelian with $\exp(\mathrm{Gal}(E/F)) \mid n$ if and only if $E$ is a splitting field of $(x^n - a_1) \cdots (x^n - a_m)$

***Proof:***
($\Longrightarrow$):

Let $G = \mathrm{Gal}(E/F)$. Then as $G$ is abelian, $G \simeq C_1 \times \cdots \times C_m$. Let $d_i = |C_i|$, then $d_i \mid n$ by the definition of exponent.

Let $H_i = \prod_{j \neq i} C_j$ so that $G/H_i \simeq C_i$. Then the field $E^{H_i}$ is galois over $F$ as $H_i \lhd G$. This is due to corollary 3.5. Thus, $\mathrm{Gal}(E^{H_i}/F) \simeq C_i$ making $E^{H_i} = F(\alpha_i)$ a splitting field of $x^{d_i} - a_i$ where $\alpha_i^{d_i} = a_i$ by theorem 5.2.

Then, $H_1 \cap H_2 \cap \cdots \cap H_m = \{ e \}$, so $E = E^{H_1} E^{H_2} \cdots E^{H_m}$ because the composite fields are the field fixed by the intersection. So

$$E = F(\alpha_1, \cdots, \alpha_m)$$

which means that $E$ splits $(x^{d_1} - a_1) \cdots (x^{d_m} - a_m)$

($\Longleftarrow$):

Let $E$ be the splitting field of $f(x) = (x^n - a_1) \cdots (x^n - a_m)$, then, $E = F(\alpha_1, \cdots, \alpha_n)$ where $\alpha_i$ is the root of $x^n - a_i$. As $F(\alpha_1, \cdots, \alpha_{n-1})(\alpha_n)$ is normal, thus galois, and cyclic over $F(\alpha_1, \cdots, \alpha_{n-1})$ by corollary 3.5.

Then $\mathrm{Gal}(E/F)$ is a product of cyclic groups, thus abelian. Also, $\sigma \in \mathrm{Gal}(E/F)$ maps a root $\alpha$ to $\eta^i \alpha$, then it has degree dividing $n$.

□

Now, when considering a radical extension, it is possible to use the cyclotomic and kummer extensions as an intermediate field. As it was shown that these intermediate field gives that the extension is radical, and galois, and the galois group is abelian, it will be a lot easier to show the galois group using these proved theorem.

# 6 Radical Extensions

As the main goal of the pages is to show the impossibility to formulate an expression solving a general polynomial, it is necessary to take a detour and study the radical operations.

It should we well-known that a field is closed under addition, subtraction, multiplication, division, and exponentiation. However, in expressing the formula for the roots, it is expected that a square root, cubic root, and generally $n$th root are needed.

In this section, radical extensions will be defined as a way to capture the notion of taking the $n$-th root in a field.

**Definition 6.1: Radical Extension**

A finite extension $E/F$ is radical if there exists a chain

$$F \subset F(\alpha_1) \subset F(\alpha_1, \alpha_2) \subset \cdots \subset F(\alpha_1, \ldots, \alpha_m) = E$$

where $\alpha_1^{n_1} \in F$ and $\alpha_i^{n_i} \in F(\alpha_1, \ldots, \alpha_{i-1})$ for all $i \geq 2$.
Moreover, a radical extension is called an $n$-radical extension if $n_1 = \cdots = n_m = n$.

Firstly, notice that the notion of a radical and an $n$-radical extension is similar and in fact, replacable. An $n$-radical looks stronger than a radical extension, but given an arbitrary radical extension, one can find $n = n_1 \cdots n_m$ such that the extension is $n$-radical.

**Theorem 6.1**

If $K/E$ and $E/F$ are radical extensions then $K/F$ is a radical extension.

***Proof:*** By the definition, there is a chain

$$E \subset E(\alpha_1) \subset \cdots \subset E(\alpha_1, \ldots, \alpha_n) = K$$

such that $\alpha_i^p \in E(\alpha_1, \ldots, \alpha_{i-1})$ and a chain

$$F \subset F(\beta_1) \subset \cdots \subset F(\beta_1, \ldots, \beta_m) = E$$

such that $\beta_i^q \in F(\beta_1, \ldots, \beta_{i-1})$.

By combining the chains,

$$F \subset F(\beta_1) \subset \cdots \subset F(\beta_1, \ldots, \beta_m) \subset \cdots \subset F(\beta_1, \ldots, \beta_m, \alpha_1, \ldots, \alpha_n) = K$$

where each of the consecutive field have the property of a radical field extension. □

Radical extensions capture the notion of taking root as required. If an extension $E/F$ is radical, then any element of $E/F$ can be expressed using algebraic expressions.

It is now the time to define solvability by radicals.

**Definition 6.2: solvability by radical**

A polynomial $f$ is solvable by radical if the splitting field $E$ of $f$ over $F$ is radical over $F$.

This means that a polynomial $f$ is solvable by radical if and only if all the roots of $f$ can be expressed using algebraic expressions.

**Remark 2**

The cyclotomic extensions and kummer extensions are radical extensions.

Before continuing to the next section, there is a lemma for the property of normal closure that preserves being a radical extension. This fact will be used later on in the section of galois theorem.

**Lemma 6.2**

Let $E/F$ be an $n$-radical extension, and $L/E$ be a normal closure of $E/F$. Then $L/F$ is also $n$-radical.

***Proof:*** The proof is done by induction on $m$, the number of generators of $E/F$.

If $m = 1$, which is $E = F(\alpha)$, then $\alpha^n \in F$ and $L = E(\beta_1, \ldots, \beta_k)$ means that each $\beta_i$ is also a root of $x^n - \alpha^n$ as a polynomial over $F$. Thus, $\beta_i^n \in F$ for all $i$.

By induction, assuming that the statement holds for extension with $m - 1$ generators. Then, let $E_0$ be the field satisfying

$$E = F(\alpha_1, \ldots, \alpha_m) = F(\alpha_1, \ldots, \alpha_{m-1})(\alpha_m) = E_0(\alpha_m)$$

and let the normal closure of $E/F$ is $L$ and the normal closure of $E_0/F$ be $L_0$. By induction hypothesis, $L_0/F$ is $n$-radical.

Next, let $L = L_0(\beta_1, \ldots, \beta_l)$ in which $\beta_i$ is a root of the minimal polynomial of $\alpha_m$, then an $F$-automorphism, $\sigma$, of $L$ must permutes the roots so that $\sigma(\alpha_m^n) = \beta_i^n$. Lastly, as $\alpha_m^n \in L_0$ and $L_0/F$ is normal, then $\sigma$ that fixes $F$ gives $\sigma(\alpha_m^n) \in L_0$ by the definition of normal extension. Thus, $L/L_0$ is $n$-radical.

When $L/L_0$ and $L_0/F$ is $n$-radical, it follow by theorem 6.1 that $L/F$ is also $n$-radical. □

# 7 Galois Main Theorem

The next struggle is to explicitly calculate the root of the polynomials. For the case of a quadratic polynomial, say $ax^2 + bx + 2$, there is a formula

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

However, the general formula is impossible to formulate. The following theorems show that result.

**Lemma 7.1**

Let $E/F$ be an extension with intermediate fields $L$ and $K$. If $K/F$ is galois, then $LK/L$ is galois. Moreover, $\mathrm{Gal}(LK/L) \simeq \mathrm{Gal}(K/L \cap K)$ by the restriction map $\psi : \sigma \mapsto \sigma|_K$

***Proof:*** Since $K/F$ is normal, then $K$ is a splitting field of $f$ over $F$, this means that $LK$ is a splitting field of $f$ over $L$. Therefore, $LK/L$ is normal by the definition. Moreover, as $K/F$ is separable, then $K = F(\alpha)$ by theorem 2.6, and $\alpha$ is separable. Therefore, $LK = L(\alpha)$ must be separable over $L$.

As $K/F$ is normal, then any embedding $\sigma : K \to E$ that fixes $F$ must give $\sigma(K) = K$, this includes all $\sigma \in \mathrm{Gal}(LK/L)$ as $L \supset F$ was fixed by definition. Let $\psi : \mathrm{Gal}(LK/L) \to \mathrm{Gal}(K/F)$ such that $\psi : \sigma \mapsto \sigma|_K$ is then well defined.

Next, $\psi$ is injective because if $\sigma|_K = \mathrm{id}_K$, and $\sigma|_L = \mathrm{id}_L$, then $\sigma|_{LK} = \mathrm{id}_{LK}$.

Now, consider the image $\mathrm{im}\,\psi = \{\, \sigma|_K \mid \sigma \in \mathrm{Gal}(LK/L) \,\}$. Then, $K^{\mathrm{im}\,\psi} \subset K$ is trivial, and $K^{\mathrm{im}\,\psi} \subset L$ since all of the $\sigma \in \mathrm{Gal}(LK/L)$ fixes $L$. This means that $\mathrm{Gal}(K/L \cap K) \subset \mathrm{im}\,\psi$

As $\mathrm{im}\,\psi = \mathrm{Gal}(K/L \cap K)$, then by the first isomorphism theorem $\mathrm{Gal}(LK/L) \simeq \mathrm{Gal}(K/L \cap K)$ □

Next, when there are two galois extension sharing the base field, the next lemma applies.

**Lemma 7.2**

If both $K/F$ and $L/F$ is galois, then $LK/F$ is also galois. This is by the injective map $\mathrm{Gal}(LK/F) \to \mathrm{Gal}(L/F) \times \mathrm{Gal}(K/F)$ given by $\sigma \mapsto (\sigma|_L, \sigma|_K)$. Moreover, if $K \cap L = F$, then the said map is an isomorphism.

***Proof:*** If $K/F$ and $L/F$ is galois, then let $K/F$ be the splitting field of $f$ with roots $\alpha_1, \ldots, \alpha_n$ $L/F$ be a splitting field of $g$ with $\beta_1, \ldots, \beta_m$ being the roots of $g$. This gives that $LK = L(\alpha_1, \ldots, \alpha_n) = F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m)$ is a splitting field of $\mathrm{lcm}(f, g)$. And $LK$ is separable because $f$ and $g$ is separable over $F$. Thus, $LK/F$ is galois.

Now, let $\psi$ be the map

$$\begin{aligned} \psi : \quad \mathrm{Gal}(LK/F) &\to \mathrm{Gal}(L/F) \times \mathrm{Gal}(K/F) \\ \sigma &\mapsto (\sigma|_L, \sigma|_K) \end{aligned}$$

The kernel of the map is $\ker\psi = \{\, \sigma \mid \sigma|_L = \mathrm{id}_L \text{ and } \sigma|_K = \mathrm{id}_K \,\}$, which is that $\ker\psi = \{\, \mathrm{id}_{LK} \,\}$

Next, if $K \cap L = F$, then by the previous lemma (lemma 7.1), $\mathrm{Gal}(LK/L) \simeq \mathrm{Gal}(K/F)$ and $\mathrm{Gal}(LK/K) \simeq \mathrm{Gal}(L/F)$.

Let $(\tau, \rho) \in \mathrm{Gal}(L/F) \times \mathrm{Gal}(K/F)$, then there exists $\tau' \in \mathrm{Gal}(LK/K)$ and $\rho' \in \mathrm{Gal}(LK/L)$ such that their restriction satisfies $\tau'|_L = \tau$ and $\rho'|_K = \rho$. Then, it can be checked that $\psi(\tau'\rho') = (\tau, \rho)$. Therefore, $\psi$ is surjective, thus an isomorphism. □

This lemma agrees on the intuition that if two extensions are disjoint, then the groups are disjoint, then their composite is, loosely speaking in term of galois, the product of those disjoint groups.

**Theorem 7.3: Main Galois Theorem**

Let $f$ be a field of characteristic 0, and let $f \in F[x]$, then $f$ is solvable by radical if and only if $\mathrm{Gal}(f)$ is a solvable group.

***Proof:***
($\Longrightarrow$):

Let $E$ be a splitting field of $f$ over $F$. As $f$ is solvable by radical, then there must be some $n$ and some $L$ such that $L/F$ is an $n$-radical extensions, also, $L$ should contain $E$.

Let $\eta$ be a primitive $n$th root of unity, then, $L(\eta)/L$ is an $n$-radical extension. By transitivity shown in theorem 6.1, $L(\eta)/F$ is $n$-radical.

Let $K$ be a normal closure of $L(\eta)/F$, then $K/F$ is $n$-radical by lemma 6.2 Also, $K/F(\eta)$ is also $n$-radical because one can adjoin $\eta$ to each intermediate field of the chain $F \subset \cdots \subset K$ to have

$$F \subset F(\eta) \subset \cdots \subset K(\eta) = K$$

which shows that $K/F(\eta)$ is $n$-radical.

Now, let

$$F = F_0 \subset F_0(\eta) = F_1 \subset \cdots \subset F_m = K$$

where $F_{i+1} = F_i(\alpha_i)$ and $\alpha_i^n \in F_i$. As $K$ is normal over a field of characteristic 0, then $K$ is galois.

Notice that each successive field in the chain is either a kummer extension or a cyclotomic extension.

Then by the corresponding theorem (3.4)

$$\mathrm{Gal}(K/F) \supset \mathrm{Gal}(K/F_1) \supset \cdots \supset \mathrm{Gal}(K/F_m) = \{\, e \,\}$$

As $F_{i+1} = F_i(\alpha_i)$ where $\alpha_i^n \in F_i$, then $F_{i+1}/F_i$ is cyclic of degree $n$ by theorem (5.2) of kummer extensions. Thus, $\mathrm{Gal}(F_{i+1}/F_i)$ is abelian.

Therefore, as $\mathrm{Gal}(F_{i+1}/F_i) \simeq \mathrm{Gal}(K/F_i)/\mathrm{Gal}(K/F_{i+1})$ by corollary 3.5, $\mathrm{Gal}(K/F)$ is a solvable group by definition.

($\Longleftarrow$):

Let $G = \mathrm{Gal}(f)$ be a solvable group, then there exists a chain

$$\{\, e \,\} = G_m \lhd G_{m-1} \lhd \cdots \lhd G_0 = G$$

such that $G_i/G_{i+1}$ are all abelian.

Let $E$ be the splitting field of $f$ over $F$ and let $K_i = E^{G_i}$ be the field fixed by $G_i$. Then by the correspondence (theorem 3.4)

$$F = K_0 \subset K_1 \subset \cdots \subset K_m = E$$

Let $n$ be the lcm of the degree of all elements in $G_i$ for all $i$. And $\eta$ be the primitive $n$th root of unity. By adjoining $\eta$

$$F = K_0 \subset K_0(\eta) \subset \cdots \subset K_m(\eta) = E(\eta)$$

Now, by corollary 3.5 notice that $K_{i+1}/K_i$ is normal, thus galois, and $K_i(\eta)/K_i$ is an extension. So, by lemma 7.1, $K_{i+1}(\eta)$, the composite of two fields, is galois over $K_i(\eta)$. The lemma also provide that $\mathrm{Gal}(K_{i+1}(\eta)/K_i(\eta)) \subset \mathrm{Gal}(K_{i+1}/K_i) = \frac{G_i}{G_{i+1}}$ which means that $\mathrm{Gal}(K_{i+1}(\eta)/K_i(\eta))$ is an abelian group.

As the degree of $\exp(\mathrm{Gal}(K_{i+1}(\eta)/K_i(\eta)))$ divides $n$, by the construction of $n$, then, as a kummer extension, $K_{i+1}(\eta)/K_i(\eta)$ is the splitting field of $(x^n - a_1)(x^n - a_2)\cdots(x^n - a_m)$ as mentioned in theoerm 5.3. Therefore, $K_{i+1}(\eta)/K_i(\eta)$ is $n$-radical.

As $F(\eta)/F$ is also radical, then this means that $E(\eta)$ is also radical over $F$ by the theorem 6.1. Hence, $E/F$ must also be radical, thus $f$ is solvable by radical.

□

This is the main achievement in this course, to prove that a polynomial is solvable by radical if and only if the galois group is solvable. As for all polynomial of degree less than 5, the galois group is a subset of $S_4$, then there are always solvable. This is the reason why there exist a formula for finding the roots of any polynomial of degree 2, 3, and 4. However, it is known that $S_5$ is not solvable, and there is a polynomial $f$ such that $\mathrm{Gal}(f) \simeq S_5$, therefore, some polynomial of degree 5 cannot be solvable using radicals.