Galois Theory - Week 7 - Normality, Separability and Fixed Fields

Antonio León Villares

April 2023

Contents

Based on the notes by Tom Leinster, Chapter 7

1 Normality

1.1 Definition: Normality

*An **algebraic field extension** $M : K$ is **normal** if $\forall \alpha \in M$, the **minimal polynomial** of α splits in M.*
(Definition 7.1.1)

1.2 Lemma: Normality from Irreducible Polynomials

*Let $M : K$ be an **algebraic extension**. Then, $M : K$ is **normal if and only if** every **irreducible polynomial** over K either:*

- *has **no roots** in M*
- ***splits** in M*

---

*In other words, $M : K$ is normal if any **irreducible polynomial** over K which has **at least** one root in M has **all** its roots in M.*
(Lemma 7.1.2)

Proof. Assume that $M : K$ is normal, and let f be an irreducible polynomial over K. Moreover, say that f has a root $\alpha \in M$. Then, since f is irreducible, the minimal polynomial of α is f/c, where $c \in K$ is the leading coefficient of f. But now, $M : K$ is normal, so f/c must split in M, so f must split too. Hence, if $M : K$ is normal, any irreducible polynomial over K with a root in M splits in M.

On the other hand, assume that every irreducible polynomial over K either has no roots in M or splits in M, and let $\alpha \in M$. Since $M : K$ is algebraic, α has a minimal polynomial over K. This minimal polynomial is irreducible, and since it has at least one root (namely α), by assumption it must split in M. But then, we have shown that any $\alpha \in M$ has a minimal polynomial which splits in M, which is precisely the definition of a normal extension, so $M : K$ is normal.

□

1.2.1 Examples

- the prototypical example of a **non-normal** extension is:

$$\mathbb{Q}(\xi) : \mathbb{Q}$$

where ξ is the real root of $t^3 - 2$. Namely, take ξ itself, which has minimal polynomial $t^3 - 2$. The roots of $t^3 - 2$ are:

$$\xi, \omega\xi, \omega^2\xi$$

where $\omega = e^{2\pi i/3}$. Clearly, $t^3 - 2$ won't split in $\mathbb{Q}(\xi)$, since $\omega \notin \mathbb{Q}(\xi) \subseteq \mathbb{R}$. Alternatively, notice that $t^3 - 2$ only has one root in $\mathbb{Q}(\xi)$, so even if it has a root, it doesn't split, so by the Lemma, it can't be normal.

- we will see that the **splitting field** of a (non-zero) polynomial is always normal

1.2.2 Exercises

1. **Prove that every extension of degree 2 is normal. This should remind you of the fact that every subgroup of index 2 is normal.**
2. *[Exercise 7.1.4]* **What happens if we drop the word "irreducible" from Lemma 7.1.2? Does it still hold?**

1.3 Normality and Splitting Fields

1.3.1 Theorem: Finite, Normal Fields are Splitting Fields

> *Let $M : K$ be a* ***field extension****. Then, for some non-zero $f \in K[t]$:*
>
> $$M = SF_K(f) \iff M : K \text{ is } \textbf{\textit{finite}} \text{ and } \textbf{\textit{normal}}$$
>
> *(Theorem 7.1.5)*

Proof.

- ($\Longleftarrow$) Assume that $M : K$ is finite and normal. We need to show that M is the splitting field of some non-zero polynomial $f \in K[t]$.

  Since $M : K$ is finite, then there exists a basis:

  $$\alpha_1, \ldots, \alpha_n$$

  of M over K, such that:

  $$M = K(\alpha_1, \ldots, \alpha_n)$$

  By finiteness, each α_i is algebraic over K, since:

> *Let $M : K$ be a* ***field extension****. Then, the following are equivalent:*
>
> 1. *$M : K$ is* ***finite***
> 2. *$M : K$ is* ***finitely generated*** ***and*** ***algebraic***
> 3. *for some* ***finite*** *set $\{\alpha_1, \dots, \alpha_n\}$ of algebraic elements of M over K:*
>
> $$M = K(\alpha_1, \dots, \alpha_n)$$
>
> *(Proposition 5.2.4)*

Define m_i to be the minimal polynomial of α_i over K. Since $M : K$ is normal, each m_i splits over M, so in particular

$$f = m_1 m_2 \dots m_n \in K[t]$$

also splits in M. But then, the set of roots of f in M contains $\{\alpha_1, \dots, \alpha_n\}$, and we have that $M = K(\alpha_1, \dots, \alpha_n)$, so M is generated over K by the set of roots of f, so by definition M must be the splitting field of f, as required.

- ($\implies$) Now, assume that $M : K$ is a field extension, and that $\exists f \in K[t]$, such that $M = SF_K(f)$. We first show that $M : K$ is finite, and then that it is normal.

  (1) **M is finite**

  Since $M = SF_K(f)$, f splits over M, so let $\alpha_1, \dots, \alpha_n$ be the roots of f in M. Then, by definition of splitting field, $M = K(\alpha_1, \dots, \alpha_n)$. Moreover, each α_i is algebraic, since they are roots of a non-zero polynomial f, so by Proposition 5.2.4, $M : K$ is finite.

  (2) **K is normal**

  Let $\delta \in M$ have minimal polynomial $m \in K[t]$. m splits in its splitting field over M, $SF_M(m)$. We need to show that if $\varepsilon \in SF_M(m)$ is a root of m, then $\varepsilon \in M$. Then, we will have shown that any polynomial in $K[t]$ splits in M.

  Hence, let $\varepsilon \in SF_M(m)$ be a root of m. m is the minimal polynomial of δ over K, so it is a monic, irreducible polynomial over K. Since it is an annihilating polynomial for ε, it must also be its minimal polynomial. Now recall:

*Let K be a **field**.*

1. *Let $m \in K[t]$ be a **monic, irreducible** polynomial. Then:*

$$\exists M : K,\ \exists \alpha \in M \ : \ M = K(\alpha)$$

   *where α is **algebraic**, and has a **minimal polynomial** m over K. Moreover, if (M_1, α_1) and (M_2, α_2) are 2 such pairs, there is **exactly one isomorphism**:*

$$\varphi : M_1 \to M_2$$

   over K, such that $\varphi(\alpha_1) = \alpha_2$.

2. *There exists an **extension** $M : K$ and a **transcendental** $\alpha \in M$, such that:*

$$M = K(\alpha)$$

   *Moreover, if (M_1, α_1) and (M_2, α_2) are 2 such pairs, there is **exactly one isomorphism**:*

$$\varphi : M_1 \to M_2$$

   over K, such that $\varphi(\alpha_1) = \alpha_2$.

(Theorem 4.3.16)

Thus, it follows that there exists a unique isomorphism over K:

$$\theta : K(\delta) \to K(\varepsilon)$$

such that:

$$\theta(\delta) = \varepsilon$$

Moreover, recall:

1. *Let:*
   - $M : S : K$ *be a* ***field extension***
   - $$0_K \neq f \in K[t]$$
   - $Y \subseteq M$

   Let S be the ***splitting field*** *of f over K. Then, $S(Y)$ is the* ***splitting field*** *of f over $K(Y)$:*

   $$S = SF_K(f) \implies S(Y) = SF_{K(Y)}(f)$$

2. *Let:*
   - $$0_K \neq f \in K[t]$$
   - *L be a* ***subfield*** *of $SF_K(f)$ containing K, such that:*

     $$SF_K(f) : L : K$$

   Then, $SF_K(f)$ is the ***splitting field*** *of f over L:*

   $$SF_K(f) = SF_L(f)$$

(Lemma 6.2.14)

Since $M = SF_K(f)$, by part 2 we have that:

$$M = SF_K(f) : K(\delta) : K \implies M = SF_K(f) = SF_{K(\delta)}(f)$$

Moreover, since $SF_K(f) = K(\alpha_1, \ldots, \alpha_n)$, we can use part 1 with $Y = \{\varepsilon\} \subseteq M$, which results in:

$$K(\alpha_1, \ldots, \alpha_n, \varepsilon) = SF_{K(\varepsilon)}(f)$$

Lastly, since θ is a homomorphism over K, and $f \in K[t]$, then:

$$\theta_* f = f$$

where recall θ_* is the canonical homomorphism of the form $\theta_* : K(\delta)[t] \to K(\varepsilon)[t]$.

The last step is to use:

Let:

- *ψ be an **isomorphism of fields**:*

$$\psi : K_1 \to K_2$$

-

$$0_K \neq f \in K_1[t]$$

- *M_1 be a **splitting field** of f over K_1*
- *M_2 be a **splitting field** of $\psi_* f$ over K_2*

Then:

1. *there exists an **isomorphism**:*

$$\varphi : M_1 \to M_2$$

   *which **extends** ψ*

2. *there are **at most** $[M : K]$ such **extensions** φ*

(Proposition 6.2.11)

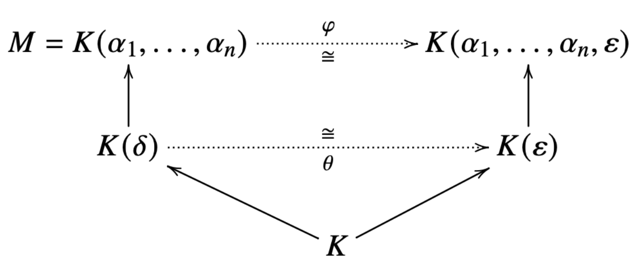
Indeed:

- θ is an isomorphism from $K(\delta)$ to $K(\varepsilon)$
- $f \in K[t]$ is non-zero, so certainly $f \in K(\delta)[t]$ is non-zero
- we have that $M_1 = M = SF_{K(\delta)}(f)$
- we have that $M_2 = K(\alpha_1, \dots, \alpha_n, \varepsilon) = SF_{K(\varepsilon)}(f)$, since $\theta_* f = f$

so the theorem applies, and there exists an isomorphism:

$$\varphi : M \to K(\alpha_1, \dots, \alpha_n, \varepsilon)$$

extending θ. Moreover, since θ is an isomorphism over K, and φ extends θ, then φ is also an isomorphism over K. Diagrammatically, we have:



But now, notice that:

$$\delta \in M = K(\alpha_1, \dots, \alpha_n)$$

Since φ is an isomorphism over K, then:

$$\varphi(\delta) \in K(\varphi(\alpha_1), \dots, \varphi(\alpha_n))$$

φ extends θ, so by definition:

$$\varphi(\delta) = \theta(\delta) = \varepsilon \implies \varepsilon \in K(\varphi(\alpha_1), \dots, \varphi(\alpha_n))$$

Moreover, we have that:

> *Let M_1, M_2 be* ***extensions*** *of a* ***field*** *K. Let:*
>
> $$\varphi : M_1 \to M_2$$
>
> *be a* ***homomorphism over*** *K:*
>
> $$\forall a \in K, \quad \varphi(a) = a$$
>
> *Then, the* ***annihilating polynomials*** *of $\alpha \in M_1$ are the* ***same*** *as the* ***annihilating polynomials*** *of $\varphi(\alpha)$.*
> *(Example 6.1.4)*

Since α_i has annihilating polynomial f, it thus follows that $\varphi(\alpha_i)$ also has f as annihilating polynomial, so:

$$f(\varphi(\alpha_i)) = 0 \implies \varphi(\alpha_i) \in \{\alpha_1, \dots, \alpha_n\}$$

But then we have shown that:

$$\varepsilon \in K(\alpha_1, \dots, \alpha_n) = M$$

so any root ε of f is also in M, so $M : K$ is a normal extension as required.

□

1.3.2 Corollary: Normality of Intermediate Fields

> *Let $M : L : K$ be* ***field extensions****. If $M : K$ is* ***finite*** *and* ***normal****, then so is $M : L$.*
> *(Corollary 7.1.6)*

Proof. From the theorem above, if $M : K$ is finite and normal, then M is a splitting field of some non-zero polynomial $f \in K[t]$, so $M = SF_K(f)$. Then, using part 2 of:

> 1. *Let:*
>
>   - $M : S : K$ *be a* ***field extension***
>   - $$0_K \neq f \in K[t]$$
>   - $Y \subseteq M$
>
>   *Let S be the* ***splitting field*** *of f over K. Then, $S(Y)$ is the* ***splitting field*** *of f over $K(Y)$:*
>
> $$S = SF_K(f) \implies S(Y) = SF_{K(Y)}(f)$$
>
> 2. *Let:*
>
>   - $$0_K \neq f \in K[t]$$
>   - *L be a* ***subfield*** *of $SF_K(f)$ containing K, such that:*
>
> $$SF_K(f) : L : K$$
>
>   *Then, $SF_K(f)$ is the* ***splitting field*** *of f over L:*
>
> $$SF_K(f) = SF_L(f)$$
>
> *(Lemma 6.2.14)*

we must have that $SF_K(f) = SF_L(f)$ is the splitting field of f over L; in other words, $M : L$ must also be normal.

□

- **If $M : L : K$ is an extension, and $M : K$ is normal, can $L : K$ be normal too?**
  - yes, since for exmple we can consider trivial extensions:

    $$\mathbb{Q}(\sqrt{2}) : \mathbb{Q}(\sqrt{2}) : \mathbb{Q}$$

  - $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ is a normal extension, since $\mathbb{Q}(\sqrt{2})$ is the splitting field of $t^3 - 2$
- **What is an example of a field extension where $M : K$ is normal, but $L : K$ isn't?**
  - let ξ be the real root of $t^3 - 2$
  - we already saw that $\mathbb{Q}(\xi) : \mathbb{Q}$ is **not** normal ($t^3 - 2$ doesn't split in $\mathbb{Q}(\xi)$, as it is missing $\omega\xi$ and $\omega^2\xi$, where $\omega = e^{2\pi i/3}$)
  - now consider the extension:

    $$\mathbb{Q}(\xi, \omega) : \mathbb{Q}(\xi) : \mathbb{Q}$$

- it is clear that $\mathbb{Q}(\xi, \omega)$ is the splitting field of $t^3 - 2$, and so, normal (over $\mathbb{Q}$ and $\mathbb{Q}(\xi)$)
- however, we know that $\mathbb{Q}(\xi)$ isn't normal over $\mathbb{Q}$

1.4 Galois Action on Normal Extensions

1.4.1 Proposition: Galois Maps Between Conjugates

*Let $M : K$ be a **finite normal** extension, and $\alpha_1, \alpha_2 \in M$. Then:*

$$\alpha_1, \alpha_2 \textit{ are } \textbf{\textit{conjugate}} \textit{ over } K \iff \exists \varphi \in Gal(M : K) \ : \ \alpha_2 = \varphi(\alpha_1)$$

*In other words, 2 elements are conjugate over K if there is an element of the **Galois Group** which maps between them.*
(Proposition 7.1.9)

Proof.

- ($\Longleftarrow$) Assume that:
$$\exists \varphi \in Gal(M : K) \ : \ \alpha_2 = \varphi(\alpha_1)$$
Since φ is an automorphism over K, by

  *Let M_1, M_2 be **extensions** of a **field** K. Let:*
  $$\varphi : M_1 \to M_2$$
  *be a **homomorphism over** K:*
  $$\forall a \in K, \quad \varphi(a) = a$$
  *Then, the **annihilating polynomials** of $\alpha \in M_1$ are the **same** as the **annihilating polynomials** of $\varphi(\alpha)$.*
  (Example 6.1.4)

  it follows that α_1 and $\varphi(\alpha_1)$ have the same annihilating polynomial. But $\varphi(\alpha_1) = \alpha_2$, so by definition of conjugacy, α_1, α_2 are conjugate over K.
- ($\Longrightarrow$) Now, assume that α_1, α_2 are conjugate over K. By assumption, $M : K$ is a finite and normal extension, so in particular, it is algebraic. In particular, α_1, α_2 are algebraic over K, and since they are conjugate, they must both have the same minimal polynomial $m \in K[t]$.

  Using:

Let K be a ***field****.*

1. *Let $m \in K[t]$ be a* ***monic, irreducible*** *polynomial. Then:*

$$\exists M : K,\ \exists \alpha \in M\ :\ M = K(\alpha)$$

   where α is ***algebraic****, and has a* ***minimal polynomial*** *m over K. Moreover, if (M_1, α_1) and (M_2, α_2) are 2 such pairs, there is* ***exactly one isomorphism****:*

$$\varphi : M_1 \to M_2$$

   over K, such that $\varphi(\alpha_1) = \alpha_2$.

2. *There exists an* ***extension*** *$M : K$ and a* ***transcendental*** *$\alpha \in M$, such that:*

$$M = K(\alpha)$$

   Moreover, if (M_1, α_1) and (M_2, α_2) are 2 such pairs, there is ***exactly one isomorphism****:*

$$\varphi : M_1 \to M_2$$

   over K, such that $\varphi(\alpha_1) = \alpha_2$.

(Theorem 4.3.16)

we have that there exists a unique isomorphism over K:

$$\theta : K(\alpha_1) \to K(\alpha_2)$$

such that:

$$\theta(\alpha_1) = \alpha_2$$

Since $M : K$ is normal, it is the splitting field of some non-zero polynomial $f \in K[t]$. We once again use:

1. *Let:*

   - $M : S : K$ *be a* ***field extension***
   - $$0_K \neq f \in K[t]$$
   - $Y \subseteq M$

   Let S *be the* ***splitting field*** *of* f *over* K*. Then,* $S(Y)$ *is the* ***splitting field*** *of* f *over* $K(Y)$*:*

   $$S = SF_K(f) \implies S(Y) = SF_{K(Y)}(f)$$

2. *Let:*

   - $$0_K \neq f \in K[t]$$
   - L *be a* ***subfield*** *of* $SF_K(f)$ *containing* K*, such that:*

   $$SF_K(f) : L : K$$

   Then, $SF_K(f)$ *is the* ***splitting field*** *of* f *over* L*:*

   $$SF_K(f) = SF_L(f)$$

(Lemma 6.2.14)

which implies that $M = SF_K(f)$ is also the splitting field of $K(\alpha_1), K(\alpha_2)$. Moreover, θ is a homomorphism over K, so in particular $\theta_* f = f$. Thus, by:

Let:

- ψ *be an* ***isomorphism of fields****:*

$$\psi : K_1 \to K_2$$

-

$$0_K \neq f \in K_1[t]$$

- M_1 *be a* ***splitting field*** *of* f *over* K_1
- M_2 *be a* ***splitting field*** *of* $\psi_* f$ *over* K_2

Then:

1. *there exists an* ***isomorphism****:*

$$\varphi : M_1 \to M_2$$

   which ***extends*** ψ

2. *there are* ***at most*** $[M : K]$ *such* ***extensions*** φ

(Proposition 6.2.11)

there exists an automorphim φ of M extending θ. Since θ is an isomorphism over K, so is φ. Thus, φ is an automorphism of M over K, so by definition $\varphi \in Gal(M : K)$, and we have that:

$$\varphi(\alpha_1) = \theta(\alpha_1) = \alpha_2$$

as required.

□

1.4.2 Corollary: Galois Acts Transitively on Roots

As a corollary to the above theorem, we can consider how the Galois Group acts upon the set of roots of a polynomial.

Let f *be an* ***irreducible polynomial*** *over a field* K*. Then, the action of* $Gal_K(f)$ *on the* ***roots*** *of* f *is* ***transitive****.*
In other words, the action of the Galois Group on the set of roots generates ***one orbit****, so from one root, we can always reach all other roots through an element of the Galois Group; thus, if* X *denotes the set of roots of* f*:*

$$\forall \alpha_1, \alpha_2 \in X, \exists \varphi \in Gal_K(f) \; : \; \varphi(\alpha_1) = \alpha_2$$

(Corollary 7.1.11)

Proof. This follows immediately from Proposition 7.1.9 above, since f is irreducible, so all of its roots in $SF_K(f)$ have the same minimal polynomial (f/c where $c \in K$ is the leading coefficient of f), and so, are conjugate over K. Lastly, we have that $SF_K(f) : K$ is finite and normal by Theorem 7.1.5 above, so Proposition 7.1.9 applies.

□

1.4.3 Example: Mapping Between Roots of Unity

- consider the pth roots of unity for prime p:

$$\omega = e^{2\pi i/p}, \omega^2, \dots, \omega^{p-1}$$

- their minimal polynomial is the pth cyclotomic polynomial:

$$f(t) = 1 + t + \dots t^{p-1} \in \mathbb{Q}[t]$$

- by Corollary 7.1.11 above, since f is irreducible over $\mathbb{Q}$ (as we showed), then for each $i \in \{1, \dots, p-1\}$:

$$\exists \varphi \in Gal_{\mathbb{Q}}(f) \ : \ \varphi(\omega) = \omega^i$$

- this is **highly non-trivial**: before, we first had to manually find such a φ, and then arduously check root by root that it worked
- in fact, for each $i \in \{1, \dots, p-1\}$, there is exactly **one** element $\varphi_i \in Gal_{\mathbb{Q}}(f)$ such that:

$$\varphi_i(\omega) = \omega^i$$

  Assume this isn't the case, and that $\exists \varphi, \phi \in Gal_{\mathbb{Q}}(f)$ such that $\varphi \neq \phi$ but:

$$\varphi(\omega) = \omega^i = \phi(\omega)^i$$

  φ is an automorphism, so it is invertible, so:

$$\omega = (\varphi^{-1} \circ \phi)(\omega)$$

  But now, the Galois Group acts faithfully on the roots, so:

$$\varphi^{-1} \circ \phi = \iota$$

  By uniqueness of inverses, $\phi = \varphi$.

- this in fact tells us that:

$$Gal_{\mathbb{Q}}(f) = \{\varphi_1, \dots, \varphi_{p-1}\} \cong C_{p-1}$$

1.4.4 Example: Galois Group of $t^3 - 2$

- consider $t^3 - 2$, which has 3 distinct roots in its splitting field
- this tells us that $G = Gal_{\mathbb{Q}}(t^3 - 2)$ is isomorphic to a subgroup of S_3 (so it must be one of $\iota, C_2, C_3 \cong A_3, S_3$)
- G acts transitively on the 3 roots, so it must have *at least* 3 elements (if ξ is a root, we need that there are enough elements which map ξ to each of the roots)
- thus, we have:

$$G \cong C_3 \quad or \quad G \cong S_3$$

- 2 of the roots are complex conjugates, so one of the elements of G must be complex conjugation, which is an element of order 2
- C_3 has no elements of order 2 by Lagrange's Theorem
- hence:

$$Gal(t^3 - 2) \cong S_3$$

1.4.5 Exercises

1. *[Exercise 7.1.12]* **Show by example that Corollary 7.1.11 becomes false if you drop the word "irreducible".**

1.5 Theorem: Normal Extensions and Normal Subgroups

Let $M : L : K$ be a ***field extension****, with $M : K$* ***finite*** *and* ***normal****. Then:*

1. *let*

$$\varphi L = \{\varphi(\alpha) \mid \alpha \in L\}$$

then

$$L : K \text{ is a } \textbf{normal} \text{ extension} \iff \forall \varphi \in Gal(M : K),\ \varphi L = L$$

2. *if $L : K$ is a* ***normal*** *extension, then:*
   - *$Gal(M : L)$ is a* ***normal subgroup*** *of $Gal(M : K)$*
   - $$\frac{Gal(M : K)}{Gal(M : L)} \cong Gal(L : K)$$

(Theorem 7.1.15)

- **What does the first statement of this Theorem say?**
  - an **element** of the **Galois Group** simply **permutes** the elements of a **normal extension**
  - it **fixes** the extension as a set
- **What is the significance of the second statement of the Theorem**
  - we know that $Gal(M : L) \subseteq Gal(M : K)$ since the automorphism over L (which fix L) are surely automorphisms over K (since $K \subseteq L$, so they fix K)
  - we also know that $Gal(M : L) \leq Gal(M : K)$, since both are subgroups of S_n, and $Gal(M : K)$ contains all elements of $Gal(M : L)$ (by the argument above)
  - this theorem tells us that, in fact, $Gal(M : L)$ is a **normal subgroup** whenever $M : K$ is finite and normal

---

Proof.

(1)

- ($\Longrightarrow$) Let $\varphi \in Gal(M : K)$, and assume that $L : K$ is normal. We claim that $\varphi L = L$.

  Notice, $L : K$ is finite and normal (as $M : K$ is finite). If we take any $\alpha \in L$ so by Proposition 7.1.9:

  > *Let $M : K$ be a **finite normal** extension, and $\alpha_1, \alpha_2 \in M$. Then:*
  >
  > $$\alpha_1, \alpha_2 \text{ are } \textbf{conjugate} \text{ over } K \iff \exists \varphi \in Gal(M : K) \ : \ \alpha_2 = \varphi(\alpha_1)$$
  >
  > *In other words, 2 elements are conjugate over K if there is an element of the **Galois Group** which maps between them.*
  > *(Proposition 7.1.9)*

  α and $\varphi(\alpha)$ must be conjugate over K. But then, they have the same minimal polynomial. By normality, this polynomial splits in L, which means that $\varphi(\alpha) \in L$, so we have that $\varphi L \subseteq L$. Similarly, we can take $\alpha \in L$, and since φ^{-1} is in the Galois Group, by Proposition 7.1.9 we have that $\alpha, \varphi^{-1}(\alpha)$ are conjugate, have the same minimal polynomial, and this minimal polynomial splits in L, so $\varphi^{-1}(\alpha) \in L \implies \alpha \in \varphi L$, so $L \subseteq \varphi L$, which completes the proof.

- ($\Longleftarrow$) Now, assume that $\forall \varphi \in Gal(M : K)$, we have that $\varphi L = L$. We need to show that $L : K$ is normal.

  Let $\alpha \in L$ have minimal polynomial $m \in K[t]$. By assumption, $M : K$ is finite and normal, so m splits in M. Now, by definition, α is conjugate to every other root α' of m over K. Then, using Proposition 7.1.9 again, we must have that $\exists \varphi \in Gal(M : K) \ : \ \varphi(\alpha) = \alpha'$. But then, $\alpha' \in \varphi L = L$ by assumption. Thus, m must split in L aswell, and since it was an arbitrary polynomial, $L : K$ must be normal

(2)

Now, assume that $L : K$ is normal. We need to show that $Gal(M : L)$ is a normal subgroup of $Gal(M : K)$. Define:

$$\varphi \in Gal(M : K) \qquad \theta \in Gal(M : L)$$

To show that $Gal(M : L) \triangleleft Gal(M : K)$, it is sufficient to show that:

$$\varphi^{-1}\theta\varphi \in Gal(M : L)$$

An element of $Gal(M : L)$ is an automorphism over L, so this is equivalent to:

$$\forall \alpha \in L, \quad \varphi^{-1}\theta\varphi(\alpha) = \alpha \implies \theta\varphi(\alpha) = \varphi(\alpha)$$

But using (1), since $L : K$ is normal, $\varphi L = L$, so $\varphi(\alpha) \in L$. Since $\theta \in Gal(M : L)$, it fixes any element of L, so clearly:

$$\theta\varphi(\alpha) = \varphi(\alpha)$$

as required.

To prove the second part, we make use of the First Isomorphism Theorem:

Let:

$$\theta : G \to H$$

be a ***group homomorphism****.*
Let:

$$N := ker(\theta)$$

so that $N \triangleleft G$*; and,* $im(\theta) \leq H$*.*
There is an ***isomorphism****:*

$$\psi : G/ker(\theta) \to im(\theta)$$

defined by:

$$\psi(gN) = \theta(g)$$

If θ *is* ***surjective****, then* $im(\theta) = H$*, and so:*

$$G/ker(\theta) \cong H$$

To prove the claim, it is thus sufficient to find a group homomorphism:

$$\nu : Gal(M : K) \to Gal(L : K)$$

such that $\ker(\nu) = Gal(M : L)$.

To this end, since $L : K$ is normal, we know that any $\varphi \in Gal(M : K)$ is such that $\varphi L = L$. In other words, φ permutes the elements of L, and thus, restricts to an automorphism $\hat{\varphi}$ of L. Since φ is an automorphism of M over K, then $\hat{\varphi}$ is an automorphism of L over K, so $\hat{\varphi} \in Gal(L : K)$. This indicates that we should define:

$$\nu(\varphi) = \hat{\varphi}$$

ν will ba group homomorphism, as it preserves function composition. What is its kernel? Well, this is the set of all automorphisms of M which act as the identity on elements of L; that is, all automorphisms of M which fix each element of L. This is precisely the definition of $Gal(M : L)$, so:

$$\ker(\nu) = Gal(M : L)$$

Hence, all we have left to show is that ν is surjective.

To do this, we need to show that we can "reach" any automorphism ψ of L over K by applying ν to some automorphism φ of M over K. Notice, this is equivalent to showing that φ extends ψ, since by definition of homomorphism extension, we'd require that:

$$\forall a \in K, \quad \varphi(a) = \psi(a)$$

and we will just set $\psi = \nu(\varphi)$. In other words, we just need to show that ψ extends to some φ.

To do this, we can proceed as in the proof of Proposition 7.1.9. To this end, since $M : K$ is a normal extension, it is the splitting field of some $f \in K[t]$. Then, from Lemma 6.2.14, M will also be the splitting field of f over L. We also have that $\psi_* f = f$, as ψ is a homomorphism over K, and $f \in K[t]$. Thus, applying Proposition 6.2.11, there exists an automorphism φ of M which extends ψ, so ν is surjective, and so: by the First Isomorphism Theorem:

$$\frac{Gal(M : K)}{Gal(M : L)} \cong Gal(L : K)$$

□

1.5.1 Example: Normal Extensions and Normal Subgroups

Consider the extensions:

$$\mathbb{Q}(\xi, \omega) : \mathbb{Q}(\omega) : \mathbb{Q}$$

where ξ is the real root of $t^3 - 2$, and $\omega = e^{2\pi i/3}$. $\mathbb{Q}(\xi, \omega)$ is the splitting field of $t^3 - 2$ over $\mathbb{Q}$, so in particular it is a finite, normal extension of $\mathbb{Q}$. Similarly, $\mathbb{Q}(\omega)$ is the splitting field of the cyclotomic polynomial $1 + t + t^2$ over $\mathbb{Q}$, so it too is a finite, normal extesnion of $\mathbb{Q}$.

Using

> *Let $M : L : K$ be a* ***field extension****, with $M : K$* ***finite*** *and* ***normal****. Then:*
>
> 1. *let*
>
> $$\varphi L = \{\varphi(\alpha) \mid \alpha \in L\}$$
>
> *then*
>
> $$L : K \text{ is a } \textbf{normal} \text{ extension} \iff \forall \varphi \in Gal(M : K),\ \varphi L = L$$
>
> 2. *if $L : K$ is a* ***normal*** *extension, then:*
>   - *$Gal(M : L)$ is a* ***normal subgroup*** *of $Gal(M : K)$*
>   - $$\frac{Gal(M : K)}{Gal(M : L)} \cong Gal(L : K)$$
>
> *(Theorem 7.1.15)*

since $\mathbb{Q}(\omega) : \mathbb{Q}$ is normal, any $\varphi \in Gal(\mathbb{Q}(\xi, \omega) : \mathbb{Q})$ restricts to an automorphism of $\mathbb{Q}(\omega)$. Since:

$$Gal(\mathbb{Q}(\xi, \omega) : \mathbb{Q}) = Gal_{\mathbb{Q}}(t^3 - 2)$$

it follows that the element of $Gal_{\mathbb{Q}}(t^3 - 2)$ fix $\mathbb{Q}(\omega)$ as a set.

Moreover, by normality, we also have that:

$$\frac{Gal(\mathbb{Q}(\xi, \omega) : \mathbb{Q})}{Gal(\mathbb{Q}(\xi, \omega) : \mathbb{Q}(\omega))} \cong Gal(\mathbb{Q}(\omega) : \mathbb{Q})$$

Now, we showed above that:

$$Gal_{\mathbb{Q}}(t^3 - 2) \cong S_3$$

so the elements of $Gal_{\mathbb{Q}}(t^3 - 2)$ are 6 permutations, which operate over all the roots $\xi, \omega\xi, \omega^2\xi$. Now, consider the elements of $Gal(\mathbb{Q}(\xi, \omega) : \mathbb{Q}(\omega))$. This group contains a subset of these 6 permutations which fix ω. In particular, this means that its elements are fully determined by where they map ξ (since then we can figure out where all the other roots get mapped to). There are 3 such options, so we must have that:

$$Gal(\mathbb{Q}(\xi, \omega) : \mathbb{Q}(\omega)) \cong A_3 \cong C_3$$

Finally, we know that $Gal(\mathbb{Q}(\omega) : \mathbb{Q}) \cong C_2$ (this just contains the identity and complex conjugation). Thus, what the isomorphism above says is that:

$$\frac{S_3}{A_3} \cong C_2$$

which is what we'd expect.

2 Separability

2.1 Motivating Separability

- **How can the degree of an extension be used to bound the order of its Galois group?**
  - we have that:

> *Let f be a* ***non-zero polynomial*** *over a* ***field*** *K. Then:*
>
> 1. *there exists a* ***splitting field*** *of f over K*
> 2. *any 2* ***splitting fields*** *of f are* ***isomorphic*** *over K*
> 3. *if M is a* ***splitting field*** *of f over K:*
>
> $$\text{\# of } \textbf{automorphisms} \text{ of } M \text{ over } K \leq [M:K] \leq \deg(f)!$$
>
> *(Theorem 6.2.13)*

  - this implies that if $M : K$ is a splitting field extension, then:

$$|Gal(M:K)| \leq [M:K]$$

- **Why is this a bound? That is, why is it an inequality?**
  - this comes from the fact that in deriving the above Theorem, we made a distinction between the the **degree** of a polynomial and the number of **distinct** roots
  - after all, if there's **repeated roots**, the degree will be larger than the number of distinct roots
- **What is the purpose of separability?**
  - with **separable extensions**, we can guarantee that a polynomial has **no repeated roots** in its **splitting field**
  - this will then allow us to have that:

$$|Gal(M:K)| = [M:K]$$

2.2 Definition: Separable Polynomials

> *An* ***irreducible polynomial*** *over a* ***field*** *is* ***separable*** *if it has* ***no repeated roots*** *in its* ***splitting field****.*
> *Alternatively:*
>
> - *$f \in K[t]$ is* ***separable*** *if it splits into* ***distinct linear factors*** *in $SF_K(f)$:*
>
> $$f(t) = a(t - \alpha_1) \dots (t - \alpha_n)$$
>
> - *f is* ***separable*** *if and only if it has $\deg(f)$* ***distinct*** *roots in its* ***splitting field***
>
> *(Definition 7.2.2)*

2.2.1 Example: Non-Separable Polynomial

- generally, most polynomials are **separable** (for isntance, $t^3 - 2$ is separable, since it has 3 distinct roots in its splitting field $\mathbb{C}$)
- to come up with an **irreducible polynomial** that is **inseparable** is a bit complicated
- the simplest example is:

$$f(t) = t^p - u \in K[t]$$

  where $K = \mathbb{F}_p(u)$: the field of **rational expressions** over $\mathbb{F}_p$ (p is prime) with an indeterminate variable symbol u
- so $f(t)$ is a polynomial, whose coefficients are rational expressions over a symbol u (in this case, the non-zero coefficients are $1, u \in \mathbb{F}_p(u)$)
- notice, the roots of f in $SF_K(f)$ will be the pth roots of u, and:

> *Let p be a **prime**:*
>
> 1. *In a **field** of **characteristic** p, every element has **at most one** pth root*
> 2. *In a **finite field** of **characteristic** p, every element has **exactly one** pth root*
>
> *(Corollary 2.3.22)*

- thus, there is a **single** root of f in its splitting field, but $\deg(f) > 1$,
- alternatively, one can argue by using the **Frobenius Map**:

> *Let p be a **prime**, and R a **ring** of **characteristic** p. Then:*
>
> 1. *The **Frobenius map**:*
>
> $$\theta : R \to R$$
> $$\theta(r) = r^p$$
>
>   *is a **homomorphism**.*
> 2. *If R is a **field**, then θ is **injective.***
> 3. *If R is a **finite field**, then θ is an **automorphism** of R.*
>
> *(Proposition 2.3.20)*

  from which we get that if α is a root of f in $SF_K(f)$:

$$f(t) = t^p - u = t^p - \alpha^p = (t - \alpha)^p$$

  so α is a repeated root

- to show that it is irreducible, we can use contradiction, and assume it is reducible
- if this is the case, then it can be factorised into 2 non-trivial factors:

$$f(t) = (t-\alpha)^p = (t-\alpha)^i (t-\alpha)^{p-i}$$

  where both factors are in $K[t]$ and $i \in (0, p)$
- the coefficient of t^{i-1} in $(t-\alpha)^i$ is $-i\alpha$, so $-i\alpha \in K$
- since $i \in \mathbb{F}_p$, it is invertible in K, so $\alpha \in K$
- this would imply that u has a pth root in $K = \mathbb{F}_p(u)$, but this is impossible (we saw this in W3): assume that u has a pth root in $\mathbb{F}_p(u)$. In particular, this means that there exist $f, g \in \mathbb{F}_p[u]$ such that:

$$\left(\frac{f}{g}\right)^p = u \implies f^p = ug^p$$

  Considering degree:

$$\deg(f^p) = \deg(ug^p) \implies p\deg(f) = 1 + p\deg(g)$$

  But this is impossible: p divides the LHS, but won't divide the RHS. Hence, u can't have a root in $K = \mathbb{F}_p(u)$.

2.3 Formal Derivatives

2.3.1 Motivation

- **In real analysis, how can one check if a root is repeated?**
  - say $f(x)$ is some polynomial over $\mathbb{R}$
  - to check if $\alpha \in \mathbb{R}$ is a repeated root of f, we can **differentiate** f, and evaluate $f'(x)$ at $x = \alpha$
  - if $f'(\alpha) = 0$, then $f(x)$ and $f'(x)$ must share a linear factor $x - \alpha$, which implies that α is a repeated root of f

2.3.2 Definition: The Formal Derivative

*Let K be a **field**, and let:*

$$f(t) = \sum_{i=0}^{n} a_i t^i \in K[t]$$

*The **formal derivative** of f is:*

$$(Df)(t) = \sum_{i=1}^{n} i a_i t^{i-1} \in K[t]$$

(Definition 7.2.6)

2.3.3 Lemma: Rules for the Formal Derivative

> *Let K be a **field**. Then:*
>
> $$\forall f, g \in K[t], D(f+g) = Df + Dg$$
> $$\forall f, g \in K[t], D(fg) = f \cdot Dg + Df \cdot g$$
> $$\forall a \in K, Da = 0_K$$
>
> *(Lemma 7.2.7)*

2.3.4 Lemma: Number of Roots and the Formal Derivative

This is the algebraic analogue to the real analysis test for root repetition. In fact, it gives us a way of checking for repeated roots in the splitting field, without having to know what the splitting field is!

> *Let f be a non-zero polynomial over a **field** K. The following are **equivalent**:*
>
> 1. *f has a **repeated root** in $SF_K(f)$*
> 2. *f and Df have a **common root** in $SF_K(f)$*
> 3. *f and Df have a **non-constant common factor** in $K[t]$*
>
> *(Lemma 7.2.9)*

Proof.

① $\implies$ ②

Assume that f has a repeated root $\alpha \in SF_K(f)$. Then, we have that:

$$\exists g(t) \in SF_K(f)[t], \ : \ f(t) = (t-\alpha)^2 g(t)$$

Computing the formal derivative:

$$\begin{aligned} Df &= D((t-\alpha)^2 g) \\ &= 2(t-\alpha)g + (t-\alpha)^2(Dg) \\ &= (t-\alpha)(2g + (t-\alpha) \cdot Dg) \end{aligned}$$

Thus, $\alpha \in SF_K(f)$ is a common root between f and Df.

② $\implies$ ③

Assume that f and Df have a common root in $SF_K(f)$, say α. Then, α will be algebraic over K (as $f \neq 0$), and thus has a minimal polynomial g over K. But then, g will be a non-constant common factor shared by both f and Df, as required.

③ $\implies$ ②

Assume that f and Df have a non-constant common factor in $K[t]$. g will split in $SF_K(f)$, and any root of g in $SF_K(f)$ will be a common root of f and Df.

② $\implies$ ①

Assume that f and Df have a common root $\alpha \in SF_K(f)$. Then, there exists some $g \in SF_K(f)[t]$, such that:

$$f(t) = (t - \alpha)g(t)$$

Computing the formal derivative:

$$Df = g + (t - \alpha) \cdot Dg$$

Since f and Df have α as a common root, then:

$$(Df)(\alpha) = 0 \implies g(\alpha) = 0$$

so there exists some $h \in SF_K(f)[t]$ such that:

$$g(t) = (t - \alpha)h(t)$$

But then:

$$f(t) = (t - \alpha)^2 h(t)$$

and f has a repeated root in $SF_K(f)$.

□

2.3.5 Proposition: Separability from Formal Derivative

*Let f be an **irreducible** polynomial over a **field**. Then, f is **inseparable** if and only if:*

$$Df = 0$$

(Proposition 7.2.10)

Proof. Assume that f is irreducible. f is inseparable if and only if it has repeated roots in its splitting field. By Proposition 7.2.9 above, this is true if and only if f and Df have a non.-constant common factor, so f divides Df. But then:

$$\deg(Df) < \deg(f) \implies f \mid Df \iff Df = 0$$

□

2.3.6 Corollary: Separability from Field Characteristic

*Let K be a **field**. Then:*

1. *If $char(K) = 0$, then every **irreducible** polynomial over K is **separable**.*
2. *If $char(K) = p > 0$, then for an **irreducible** polynomial $f \in K[t]$:*

$$f \text{ is } \textbf{inseparable} \iff f(t) = \sum_{i=0}^{r} b_i t^{ip}$$

where $b_0, \ldots, b_r \in K$.

(Corollary 7.2.11)

---

*Notice, this says that the **only** irreducible polynomials which are inseparable are those polynomials in t^p over fields of characteristic p.*

Proof. Let f be an irreducible polynomial given by:

$$f(t) = \sum a_i t^i$$

f is inseparable if and only if $Df = 0$. Thus, f is inseparable if and only if:

$$\forall i \geq 1, ia_i = 0$$

When $char(K) = 0$, by definition, this can only be the case if $\forall i \geq 1, a_i = 0$, so f will be a constant polynomial, which contradicts the fact that f is irreducible. Thus, in fields of characteristic 0, no irreducible polynomial can be inseparable.

Now, assume that $char(K) = p$. Then $ia_i = 0$ whenever i divides p, from definition of characteristic. Hence, for the remaining cases, we must have that $a_i = 0$. Thus, in fields of characteristic 0, the irreducible polynomials which are inseparable are those polynomials in terms of t^p. ☐

---

*In fact, it can be shown that every **irreducible** polynomial over a **finite field** is **separable**. Thus, inseparability only arises in **infinite fields of characteristic** p!*

2.4 Definition: Separable Field Elements

Let $M : K$ be an ***algebraic extension****. $\alpha \in M$ is* ***separable*** *over K if its* ***minimal polynomial*** *over K is* ***separable****.*
(Definition 7.2.13)

2.5 Definition: Separable Field Extension

Let $M : K$ be an ***algebraic extension****. $M : K$ is* ***separable*** *if every element of M is* ***separable*** *over K.*
(Definition 7.2.13)

2.5.1 Examples: Separable and Inseparable Extensions

- since in fields of characteristic 0 all polynomials are separable, any algebraic extension $M : K$ where $char(K) = 0$ will be separable
- furthermore, any algebraic extension of a finite field will be a separable extension
- we saw that $t^p - u \in \mathbb{F}_p(u)$ was an inseparable polynomial, so its splitting field will be inseparable (since the root of $t^p - u$ has an inseparable minimal polynomial, and the root is in the splitting field)

2.6 The Order of the Galois Group

2.6.1 Lemma: Algebraicity of Intermediate Fields

Let $M : L : K$ be ***field extensions****. Then*

$$M : K \text{ is } \textbf{algebraic} \implies M : L,\ L : K \text{ are } \textbf{algebraic}$$

(Exercise 7.2.15)

Proof. Assume that $M : K$ is algebraic. Then, if $\alpha \in M$ it has a minimal polynomial $f \in K[t]$. Thus, $L : K$ must be algebraic, since $L \subseteq M$. Moreover, $M : L$ must be algebraic, since $K \subseteq L$, so if α has annihilating polynomial $f \in K[t]$, then $f \in L[t]$ annihilates α aswell. ☐

2.6.2 Lemma: Separability of Intermediate Fields

*Let $M : L : K$ be **field extensions**, and let $M : K$ be **algebraic**. Then:*

$$M : K \text{ is } \textbf{separable} \implies M : L,\ L : K \text{ are } \textbf{separable}$$

(Lemma 7.2.16)

Proof. By Exercise 7.2.15 above, since $M : K$ is algebraic, so are $M : L$ and $L : K$. It is immediate that $L : K$ is separable: if every element of M is separable over K, and $L \subseteq M$, then every element of L must be separable over K too.

To see why $M : L$ must be separable, let $\alpha \in M$. Let m_L, m_K be the minimal polynomials of α over L, K respectively. m_K is an annihilating polynomial of α over L (since $K \subseteq L$), so $m_L \mid m_K$ in $L[t]$. Moreover, $M : K$ is separable, so m_k splits into distinct linear factors in $SF_K(m_K)$. But m_L divides m_K, so m_L must also split into distinct linear factors, so $m_L \in L[t]$ is separable, so α is separable over L.

□

2.6.3 Proposition: Counting Isomorphisms Extensions

Let:

$$\psi : K_1 \to K_2$$

*be an **isomorphism of fields**, and let:*

- *$f \in K[t]$ be a non-zero polynomial*
- *M_1 be the **splitting field** of f over K_1*
- *M_2 be the **splitting field** of $\psi_* f$ over K_2*

*If $M_2 : K_2$ is **separable**, then there are **exactly** $[M_1 : K_1]$ isomorphisms:*

$$\varphi : M_1 \to M_2$$

extending ψ.
(Proposition 7.2.17)

Proof. This is an adaptation of the proof for:

Let:

- ψ *be an* ***isomorphism of fields****:*

$$\psi : K_1 \to K_2$$

- $$0_K \neq f \in K_1[t]$$

- M_1 *be a* ***splitting field*** *of* f *over* K_1
- M_2 *be a* ***splitting field*** *of* $\psi_* f$ *over* K_2

Then:

1. *there exists an* ***isomorphism****:*

$$\varphi : M_1 \to M_2$$

   which ***extends*** ψ

2. *there are* ***at most*** $[M : K]$ *such* ***extensions*** φ

(Proposition 6.2.11)

but since we have a separable field extension, we have $s = \deg(\psi_* m)$. For the inductive hypothesis, we have that $M_2 : K_2(\alpha_j^2)$ is also separable, since $M_2 : K_2$ is. □

2.6.4 Theorem: Order of Galois Group for Normal and Separable Extensions

For every ***finite****,* ***normal****,* ***separable*** *extension* $M : K$*:*

$$|Gal(M : K)| = [M : K]$$

(Theorem 7.2.18)

Proof. Since $M : K$ is finite and normal, then:

$$\exists f \in K[t] \ : \ M = SF_K(f)$$

(Theorem 7.1.5). Since $M : K$ is separable, we can apply Theorem 7.2.17 above, using $M = M_1 = M_2$, $K = K_1 = K_2$ and $\psi = \text{id}_K$, which shows that there are exactly $[M : K]$ automorphisms of M over K, as required. □

2.6.5 Examples: Computing Orders of Galois Groups

- if K is a field of characteristic 0, then for any $f \in K[t]$, $SF_K(f)$ also has characteristic 0 (we have a homomorphism between K and $SF_K(f)$, and this can only be the case if they have the same characteristic). But then, this means that:

$$|Gal_K(f)| = [SF_K(f) : K]$$

  since $SF_K(f)$ will be separable (and trivially normal and finite).

- for instance, with $f = t^3 - 2$, we have that:

$$SF_{\mathbb{Q}}(f) = \mathbb{Q}(\xi, \omega)$$

  and so:

$$[\mathbb{Q}(\xi, \omega) : \mathbb{Q}] = [\mathbb{Q}(\xi, \omega) : \mathbb{Q}(\xi)][\mathbb{Q}(\xi) : \mathbb{Q}] = 2 \times 3 = 6$$

  Hence, $|Gal_{\mathbb{Q}}(t^3 - 2)| = 6$. But also $Gal_{\mathbb{Q}}(t^3 - 2) \leq S_3$, so the only possibility is that $Gal_{\mathbb{Q}}(t^3 - 2) = S_3$, as we showed above.

- we can see that without separability, the above Theorem won't work. Let:

$$K = \mathbb{F}_p(u) \qquad M = SF_K(t^p - u)$$

  If α is **the** root of $t^p - u$, then:

$$M = K(\alpha) \implies [M : K] = \deg_K(\alpha) = p$$

  On the other hand, since $t^p - u$ has a single (non-repeated) root, it follows by:

  > *Let f be a* ***non-zero polynomial*** *over a* ***field*** *K, with k* ***distinct*** *roots in $SF_K(f)$. Then:*
  >
  > $$|Gal_K(f)| \mid k!$$
  >
  > *(Corollary 6.3.14)*

  that $|Gal_K(t^p - u)| = 1 \neq p$. So without separability, we can't use this convenient equality!

3 Fixed Fields

3.1 Recap: Fixed Set

We recall the definition of a fixed set from Week 2.

> *Let G be a* ***group*** *acting on X, and consider a subset $S \subseteq G$.*
> *The* ***fixed set*** *of S is:*
>
> $$Fix(S) = \{x \mid x \in X, \; \forall s \in S \; : \; sx = x\}$$
>
> *(Definition 2.1.14)*

3.2 Lemma: Elements Fixed by Automorphisms form Subfields

> *Let M be a **field**. Denote with $Aut(M)$ the **group** of **automorphisms** of M. Then:*
>
> $$\forall S \subseteq Aut(M),\ Fix(S) \text{ is a } \textbf{subfield} \text{ of } M$$
>
> *We call $Fix(S)$ the **fixed field** of S.*
> *(Lemma 7.3.1)*

Proof. Recall the following Lemma:

> *Let K, L be **fields**, and let S be a subset of all **homomorphisms** of the form $K \to L$.*
> *Then, the **equalizer** $Eq(S)$ is a **subfield** of K.*
> *(Lemma 2.3.8)*

where the equalizer is:

> *Let X, Y be sets, and let S be a subset of all functions of the form $X \to Y$.*
> *The **equalizer** of S is:*
>
> $$Eq(S) = \{x \mid x \in X, \forall f, g \in S : f(x) = g(x)\}$$
>
> *That is, the **equalizer** is the set of all $x \in X$ which are equal under all functions in S.*
> *(Definition 2.3.7)*

But then, notice that:

$$Fix(S) = Eq(S \cup \{id_M\})$$

Thus, $Fix(S)$ is a subfield of M.

□

3.3 Theorem: Bounding Extension Degree with Subgroup Order

This result requires the most ingenious proof of the whole course.

*Let M be a **field** and H a **finite subgroup** of $Aut(M)$. Then:*

$$[M : Fix(H)] \leq |H|$$

(Theorem 7.3.3)

It must be noted that, in fact, this is an **equality**, and:

$$[M : Fix(H)] = |H|$$

Proof. Let $|H| = n$. It is sufficient to show that if we take $n+1$ elements of M, they are linearly dependent over $Fix(H)$, since then a set of linearly independent elements in M will have at most n elements, and so:

$$[M : Fix(H)] \leq |H|$$

To this end, define:

$$W = \left\{ (x_0, \ldots, x_n) \in M^{n+1} \;\middle|\; \forall \theta \in H, \sum_{i=0}^{n} x_i \theta(\alpha_i) = 0_M \right\}$$

where $\alpha_0, \ldots, \alpha_n$ are an arbitrary set of $n+1$ elements of M. W contains $n+1$-tuples in M^{n+1}. Since there are n elements in H, W is defined by the solutions to a system of n homogeneous equations in $n+1$ variables, so it is a non-trivial M-linear subspace of M^{n+1}.

Now, we claim that that if $(x_0, \ldots, x_n) \in W$ and $\varphi \in H$, then:

$$(\varphi(x_0), \ldots, \varphi(x_n)) \in W$$

Since $(x_0, \ldots, x_n) \in W$ and $\varphi^{-1} \circ \theta \in H$ (for any $\theta \in H$), it follows by definition of W that:

$$\sum_{i=0}^{n} x_i (\varphi^{-1} \circ \theta)(\alpha_i) = 0$$

Applying φ to both sides implies that for all $\theta \in H$:

$$\sum_{i=0}^{n} \varphi(x_i) \theta(\alpha_i) = 0$$

so:

$$(\varphi(x_0), \ldots, \varphi(x_n)) \in W$$

as required.

Now, let $\underline{x} = (x_0, \ldots, x_n)$ be some non-zero vector. Define its length as the unique number $\ell \in [0, n]$ such that:

- $x_\ell \neq 0$
- $\forall j \in (\ell, n], x_j = 0$

W is a non-trivial subspace, so there always exists an element of minimum length ℓ. Moreover, by properties of a subspace, W is closed under scalar multiplication by elements of M, so without loss of generality, we may assume that $x_\ell = 1$. This element of minimum length will be of the form:

$$\underline{x} = (x_0, \dots, x_{\ell-1}, 1, 0, \dots, 0)$$

Moreover, since $\underline{x}$ has minimal length, the only element of W of the form $(y_0, \dots, y_{\ell-1}, 0, 0, \dots, 0)$ must be $\underline{0}$.

We now show that:

$$\forall i \in [0, n], x_i \in Fix(H)$$

Let $\varphi \in H$. We showed that:

$$(x_0, \dots, x_n) \in W \implies (\varphi(x_0), \dots, \varphi(x_n)) \in W$$

Define:

$$\underline{y} = (\varphi(x_0) - x_0, \dots, \varphi(x_n) - x_n)$$

By closure of subspaces $\underline{y} \in W$. Since φ is a field homomorphism, in particular:

$$\forall i \in (\ell, n], x_i = 0 \implies \varphi(x_i) = 0$$

Moreover, again by properties of field homomorphisms, φ preserves the multiplicative identity:

$$\varphi(x_\ell) = 1 \implies \varphi(x_\ell) - x_\ell = 0$$

Hence,

$$\underline{y} = (\varphi(x_0) - x_0, \dots, \varphi(x_{\ell-1}) - x_{\ell-1}, 0, \dots, 0)$$

so by the previous argument, $\underline{y} = 0$, which implies that:

$$\forall i \in [0, n], \varphi(x_i) = x_i \implies x_i \in Fix(H)$$

Overall, this shows that there is a non-zero vector $\underline{x} \in Fix(H)^{n+1}$. Moreover, if we now take $\theta = id$ in the definition of W, and use $\underline{x}$, we get that we have found coefficients in $Fix(H)$, not all of which are 0, such that:

$$\sum_{i=0}^{n} x_i \theta(\alpha_i) = \sum_{i=0}^{n} x_i \alpha_i = 0$$

Hence, the set of $n+1$ elements in M $\{\alpha_0, \dots, \alpha_n\}$ is linearly dependent over $Fix(H)$, which implies that:

$$[M : Fix(H)] \leq n = |H|$$

□

3.4 Proposition: Fixed Field Yields a Normal Extension

Let $M : K$ be a ***finite normal extension****, and let H be a* ***normal subgroup*** *of $Gal(M : K)$. Then, $Fix(H) : K$ is* ***normal****.*
(Proposition 7.3.7)

Proof. H is a group containing automorphisms of M over K, so $K \subseteq Fix(H)$. Now, recall:

> *Let G be a **group** acting on X, and consider a subset $S \subseteq G$. Then:*
>
> $$\forall g \in G \ : \ Fix(gSg^{-1}) = gFix(S)$$
>
> *(Lemma 2.1.15)*

Taking $G = Gal(M : K)$ and $S = H$, we get that for any $\varphi \in Gal(M : K)$:

$$\varphi Fix(H) = Fix(\varphi H \varphi^{-1})$$

But then, since H is a normal subgroup of $Gal(M : K)$:

$$Fix(\varphi H \varphi^{-1}) = Fix(H)$$

Hence, we have shown that for any $\varphi \in Gal(M : K)$, we have:

$$\varphi Fix(H) = Fix(H)$$

so $Fix(H) : K$ is a normal extension by

> *Let $M : L : K$ be a **field extension**, with $M : K$ **finite** and **normal**. Then:*
>
> 1. *let*
>
> $$\varphi L = \{\varphi(\alpha) \mid \alpha \in L\}$$
>
>   *then*
>
> $$L : K \text{ is a } \textbf{normal} \text{ extension} \iff \forall \varphi \in Gal(M : K), \ \varphi L = L$$
>
> 2. *if $L : K$ is a **normal** extension, then:*
>   - *$Gal(M : L)$ is a **normal subgroup** of $Gal(M : K)$*
>   - $$\frac{Gal(M : K)}{Gal(M : L)} \cong Gal(L : K)$$
>
> *(Theorem 7.1.15)*

□