

**Definition 0.1.** Normal Extensions. Let  $\iota : K \rightarrow L$  be a finite extension. Then the following are equivalent:

1. For all irreducible polynomials  $f \in K[X]$  that have root in  $L$ ,  $L$  splits  $f$ .
2. For all elements  $a \in L$ ,  $L$  splits  $\min(a, K)$ .
3. There exists generators  $a_1, \dots, a_n \in L$  such that for all generators  $a_i$ , there exists a polynomial  $f_i \in K[X]$  where  $a_i$  is a root and  $L$  splits  $f_i$ .
4. There exists some polynomial  $f \in K[X]$  such that  $L$  is the splitting field of  $f$ .
5. For all  $K$ -extension  $\iota_M : K \rightarrow M$  and  $K$ -extension morphisms  $\phi, \psi : L \rightarrow M$ ,  $\phi L = \psi L$ .

If any of the above are true,  $\iota : K \rightarrow L$  is called a **normal extension**. We also sometimes say  $L$  is **normal over  $K$** .

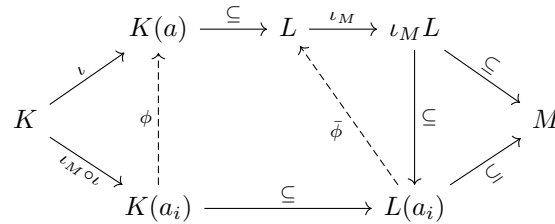
*Proof.* (1  $\Rightarrow$  2) Since finite extensions are algebraic, the second statement is well-defined. By minimal polynomials are irreducible and have a root in  $L$ , we are done.

(2  $\Rightarrow$  3)  $L$  is a finite extension so there exists  $a_0, \dots, a_{n-1} \in L$  such that  $L = K(a_0, \dots, a_{n-1})$ . For each generator  $a_i$ , pick  $f_i = \min(a_i, K)$ .

(3  $\Rightarrow$  4) Let  $f = \prod_{i \in n} f_i$ .  $L$  clearly splits  $f$  and since the roots of  $f$  include the generators  $a_0, \dots, a_{n-1}$ ,  $L$  is generated by the roots of  $f$ .

(4  $\Rightarrow$  1) Let  $g$  be an irreducible polynomial over  $K$  with a root  $a \in L$ . We do not know whether  $g$  splits in  $L$ , but we know there exists a finite extension  $\iota_M : L \rightarrow M$  that splits  $\bar{\iota}g$ , i.e. contains all the roots of  $g$ . We will show in that in this larger field, all the roots of  $g$  are already in  $L$ .

Let  $a_i$  be any root of  $g$  in  $M$ . The proof is contained in the following diagram.



We will show that  $\iota_M L = L(a_i)$ , i.e. the root  $a_i$  is already in  $L$ . Note that by  $\iota_M : L \rightarrow L(a_i)$  being an injective  $K$ -vector space morphism, it suffices to show  $\dim_K L = \dim_K L(a_i)$ .

We already have  $\dim_K L \leq \dim_K L(a_i)$ . For the other inequality, note that by definition,  $L$  splits  $f$  and  $L$  is generated by the roots of  $f$ . This clearly implies  $L(a_i)$  splits  $\overline{\iota_M \circ \iota} f$  and is generated by the roots of  $\overline{\iota_M \circ \iota} f$ , i.e.  $L(a_i)$  is the splitting field of  $\overline{\iota_M \circ \iota} f$ . Since  $a$  and  $a_i$  are galois conjugates, there exists a  $K$ -extension morphism  $\phi : K(a_i) \rightarrow K(a)$ ,  $a_i \mapsto a$ . So then  $\phi : K(a_i) \rightarrow L$  is a  $K(a_i)$ -extension that splits  $\overline{\iota_M \circ \iota} f$ . Hence by the minimal property of splitting fields, there exists a  $K(a_i)$ -extension morphism  $\bar{\phi} : L(a_i) \rightarrow L$ . This

is clearly a  $K$ -extension morphism. In particular,  $\bar{\phi}$  is an injective  $K$ -vector space morphism between finite dimensional  $K$ -vector spaces  $L(a_i)$  and  $L$ . Hence  $\dim_K L(a_i) \leq \dim_K L$ .

(4  $\Rightarrow$  5) This is image invariance of splitting fields.

(5  $\Rightarrow$  1) We require the machinery of *normal closures*, which we will investigate below.  $\square$

For now, we restrict the definition of normality to 1 to 4.

**Example 0.2.** Non-Normal Extensions.

The  $\mathbb{Q}$ -extension  $\iota : \mathbb{Q} \rightarrow \mathbb{Q}(\sqrt[3]{2})$  is *not* normal, since

$$\bar{\iota} \min(\sqrt[3]{2}, \mathbb{Q}) = X^3 - 2 = (X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}X + \sqrt[3]{2}^2)$$

does not factorise further. In a sense, the other roots  $\sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$  are "missing" from the field  $\mathbb{Q}(\sqrt[3]{2})$ .

This can be fixed by adding elements to the extension until the extension is normal. The "smallest" such extension will be the *normal closure*.

**Lemma 0.3.** *Normality Lifts up.*

Let  $K \xrightarrow{\iota_L} L \xrightarrow{\iota_M} M$  be extensions and  $f$  a polynomial over  $K$ . Then  $\iota_M \circ \iota_L : K \rightarrow M$  is the splitting field of  $f$  implies  $\iota_M : L \rightarrow M$  is the splitting field of  $\bar{\iota}_L f$ . Consequently,  $\iota_M \circ \iota_L : K \rightarrow M$  normal implies  $\iota_M : L \rightarrow M$  normal.

*Proof.* Suppose  $\iota_M \circ \iota_L : K \rightarrow M$  is the splitting field of  $f$ . Clearly,  $M$  splits  $\bar{\iota}_L f$ . Let  $S_f$  be the roots of  $f$  in  $M$ .  $S_f$  is also the roots of  $\bar{\iota}_L f$  in  $M$ . Then the smallest subfield of  $M$  containing  $\iota_M L$  and  $S_f$  also contains  $\iota_M(\iota_L K)$ , i.e.  $M = K(S_f) \subseteq L(S_f) \subseteq M$ . Hence  $M$  is generated by  $S_f$  as an  $L$ -extension.  $\square$

**Definition 0.4.** Normal Closure.

Let  $K \xrightarrow{\iota_L} L \xrightarrow{\iota_N} N$  be extensions. Then  $(N, \iota_N)$  is called a **normal closure of  $(L, \iota_L)$**  when it is a *smallest* normal  $K$ -extension containing  $\iota_L : K \rightarrow L$  in the sense that  $\iota_N \circ \iota_L : K \rightarrow N$  is normal and for any  $\iota_M : L \rightarrow M$  such that  $\iota_M \circ \iota_L : K \rightarrow M$  is normal, there exists a  $L$ -extension morphism  $\bar{\iota}_M : N \rightarrow M$ . Diagrammatically,

$$\begin{array}{ccc} & & N \\ & \nearrow \iota_N & \downarrow \bar{\iota}_M \\ K & \xrightarrow{\iota_L} & L \\ & \searrow \iota_M & \downarrow \\ & & M \end{array}$$

Note that we have not proved normal closures to be unique yet, hence the emphasis on "a normal closure" not "the normal closure".

**Theorem 0.5.** *Existence and Uniqueness of Normal Closure of Finite Extensions.*

Let  $\iota_L : K \rightarrow L$  be a finite  $K$ -extension. Then there exists an  $L$ -extension  $\iota_N : L \rightarrow N$  such that  $(N, \iota_N)$  is a normal closure of  $(L, \iota_L)$ . Furthermore,  $N$  is a finite extension and unique up to isomorphism, i.e. any other normal closure of  $\iota_L : K \rightarrow L$  is isomorphic to  $N$  as a  $K$ -extension. Thus we denote  $N$  as  $N(L/K)$  and refer to anything isomorphic to it as the normal closure of  $(L, \iota)$ .

*Proof.* Since  $L$  is a finite dimensional  $K$ -vector space, by existence of a basis, let  $a_0, \dots, a_{n-1}$  be a finite set of generators of  $L$ , i.e.  $L = K(a_0, \dots, a_{n-1})$ . Let  $f = \prod_{i \in n} \min(a_i, K)$ . There exists a  $K$ -extension  $\iota_{\tilde{N}} : K \rightarrow \tilde{N}$  that splits  $f$ . Let  $N$  be the  $K$ -subextension of  $\tilde{N}$  generated by the roots of  $f$ , i.e. the splitting field of  $f$ . Since for all generators  $a_i$  of  $L$ ,  $N$  splits  $\min(a_i, K)$ , we have a  $K$ -extension  $\iota_N : L \rightarrow N$  by embedding via conjugates. Clearly,  $\iota_N \circ \iota_L : K \rightarrow N$  is normal. We will now show that it has the minimal property of normal closures.

Let  $\iota_M : L \rightarrow M$  be an  $L$ -extension such that  $\iota_M \circ \iota_L : K \rightarrow M$  is normal. By lifting normality of  $N$ ,  $\iota_N : L \rightarrow N$  is the splitting field of  $\bar{\iota}_L f$ . For a generator  $a_i$  of  $L$ ,  $\min(a_i, K) = \min(\iota_M(a_i), K)$ . So normality of  $M$  over  $K$  implies  $M$  splits  $f$ , consequently splitting  $\bar{\iota}_L f$ . Hence by the minimal property of splitting fields, there exists an  $L$ -extension morphism  $\bar{\iota}_M : N \rightarrow M$  such that  $\bar{\iota}_M \circ \iota_N = \iota_M$ . Thus,  $(N, \iota_N)$  is a normal closure of  $\iota_L : K \rightarrow L$ .

Now let  $(M, \iota_M)$  be another normal closure of  $(L, \iota_L)$ . Then by applying minimal property of normal closure twice, we have  $L$ -extension morphisms  $\bar{\iota}_M : N \rightarrow M$  and  $\bar{\iota}_N : M \rightarrow N$ . These are also  $K$ -extension morphisms. Since  $N$  is a finite  $K$ -extension and  $\bar{\iota}_N$  is an injective morphism of  $K$ -vector spaces from  $M$  to  $N$ , we have the dimension of  $M$  as finite and less than equal to that of  $N$ . Similarly, the dimension of  $N$  is less than equal to that of  $M$ . So  $\dim_K N = \dim_K M$  and hence  $\bar{\iota}_M : N \rightarrow M$  is actually a bijection. Thus  $N$  and  $M$  are isomorphic as  $L$ -extensions.  $\square$

**Remark.** The following is the main property of normal extensions

**Theorem 0.6.** Let  $K \xrightarrow{\iota_L} L \xrightarrow{\iota_N} N$  be extensions where  $(N, \iota_N \circ \iota_L)$  is normal. Then for all  $K$ -extension morphisms  $f : (L, \iota_L) \rightarrow (N, \iota_N \circ \iota_L)$ , there exists a  $L$ -extension morphism  $\bar{f} : (N, \iota_N) \rightarrow (N, f)$ .

We are now ready to prove  $5 \Rightarrow 1$ .

**Theorem 0.7.** *Image Invariance gives Splitting Irreducible Polynomials with Roots.*

Let  $\iota_L : K \rightarrow L$  be a  $K$ -extension such that for all  $K$ -extensions  $\iota_M : K \rightarrow M$  and  $K$ -extension morphisms  $\phi, \psi : L \rightarrow M$ ,  $\phi L = \psi L$ . Then for all irreducible polynomials  $f \in K[X]$  that have a root  $a \in L$ ,  $L$  splits  $f$ .

*Proof.* Let  $f$  be an irreducible polynomial over  $K$  with a root  $a \in L$ . We do not know whether  $L$  contains all the roots of  $f$ , but we do know that  $L$ 's normal closure definitely does. So let  $\iota_N : L \rightarrow N(L/K)$  be the normal closure of  $L$ . Then  $f$  is an irreducible polynomial with  $\iota_N(a)$  as a root. So by normality,  $N$  splits  $f$ .

Let  $a_i$  be an arbitrary root of  $f$  in  $N$ . We seek to show that the root  $a_i$  is already in  $\iota_N L$ . The following diagram is the situation.

$$\begin{array}{ccccccc}
 K & \xrightarrow{\iota_L} & K(a) & \xrightarrow{\subseteq} & L & \xrightarrow{\iota_N} & N \xleftrightarrow{\bar{\phi}} \\
 & \searrow \iota_N \circ \iota_L & \downarrow \phi & & \nearrow \subseteq & & \\
 & & K(a_i) & & & & 
 \end{array}$$

Since  $a_i$  is a galois conjugate of  $a$ , there exists a  $K$ -extension morphism  $\phi : (K(a), \iota_L) \rightarrow (K(a_i), \iota_N \circ \iota_L)$  mapping  $a \mapsto a_i$ . This implies  $\phi \circ \iota_L = \iota_N \circ \iota_L$ , i.e.  $(N, \phi \circ \iota_L) = (N, \iota_N \circ \iota_L)$  as  $K$ -extensions. By lifting normality,  $(N, \iota_N)$  and  $(N, \phi)$  are both normal  $K(a)$ -extensions. Thus, there exists a  $K(a)$ -extension morphism  $\bar{\phi} : (N, \iota_N) \rightarrow (N, \phi)$  via finite normal extensions differing by automorphisms. It follows that  $\bar{\phi} \circ \iota_N : (L, \iota_L) \rightarrow (N, \iota_N \circ \iota_L)$  is a  $K$ -extension morphism. Since  $\iota_N$  and  $\bar{\phi} \circ \iota_N$  are both  $K$ -extension morphisms from  $L$  to  $N$ ,  $\iota_N L = \bar{\phi}(\iota_N L)$ . But of course,

$$a_i = \phi(a) = \bar{\phi}(\iota_N(a)) \in \iota_N L$$

Thus, the root  $a_i$  is actually already in  $\iota_N L$ . This completes the proof.  $\square$

test