

# GALOIS THEORY NOTES

## 1. SPLITTING FIELDS AND NORMAL EXTENSIONS

**Proposition 1.1.** Let  $K \leq L$  be fields. Suppose that  $\alpha \in L$  is algebraic over  $K$  and let  $p(x) \in K[x]$  be a minimal polynomial for  $\alpha$ . Then there is a unique isomorphism  $K[x]/(p(x)) \rightarrow K[\alpha] = K(\alpha)$  mapping  $x$  to  $\alpha$  and fixing  $K$ .

*Proof.* There is a unique map  $K[x] \rightarrow K[\alpha]$  mapping  $x$  to  $\alpha$  and fixing  $K$ . It is surjective and its kernel is the ideal generated by  $p(x)$ . □

If  $\sigma : K \rightarrow L$  is a homomorphism of fields and  $f = a_0 + a_1x + \cdots + a_nx^n \in F[x]$ , then we let  $f^\sigma = \sigma(a_0) + \sigma(a_1)x + \cdots + \sigma(a_n)x^n \in F[x]$ .

**Lemma 1.2.** Suppose that  $\sigma : K \rightarrow L$  is an isomorphism of fields and suppose  $K' = K[\alpha]$  is an extension of  $K$  where  $f \in F[x]$  the minimal polynomial of  $\alpha \in K'$ . Let  $\sigma : K \rightarrow L$  be a field homomorphism.

- If  $\sigma' : K' \rightarrow L$  extends  $\sigma$ , then  $f^\sigma(\sigma(\alpha')) = 0$
- If  $\beta \in L$  satisfies that  $f^\sigma(\beta) = 0$ , then there is precisely one extension of  $\sigma$  mapping  $\alpha$  to  $\beta$ .

*Proof.* The first point is obvious. For the second point, let  $\phi : K[x] \rightarrow L$  be given by  $\phi(P) = P^\sigma(\beta)$ . This is a ring homomorphism. Now observe that  $\phi(f) = f^\sigma(\beta) = 0$ , thus  $\phi$  vanishes on the ideal generated by  $f$  and so there is a well defined field homomorphism  $\phi : K[x]/(f) \rightarrow L$  mapping  $x + (f)$  to  $\beta$ . Finally, we use the isomorphism  $K' \cong K[x]/(f)$  that maps  $\alpha$  to  $x$  and fixes  $K$ , giving the desired extension. The extension is clearly unique as  $K' = K(\alpha)$ . □

**Proposition 1.3.** Let  $K \leq K'$  be an algebraic field extension and suppose that  $\sigma : K \rightarrow L$  is a field homomorphism where  $L$  is algebraically closed. Then there exists an extension  $\sigma' : K' \rightarrow L$ . Moreover,  $\sigma'$  must be an isomorphism if  $K'$  is algebraically closed and  $L$  is algebraic over  $\sigma(K)$ .

*Proof.* Use Zorn's lemma to construct a maximal subfield  $K'' \subset K'$  such that  $\sigma$  extends to  $K''$ . If  $K'' \neq K'$  then choose  $\alpha \in K' \setminus K''$ . Now as  $K'$  is algebraic over  $K$  we can let  $f \in K[x]$  be a minimal polynomial of  $\alpha$  over  $K$ . Now as  $f^\sigma$  has a root in  $L$  as  $L$  is algebraically closed, we can use the previous lemma to extend  $\sigma$  to  $K''[\alpha]$ , contradicting the maximality of  $K''$ . If  $K'$  is algebraically closed, then so is  $\sigma'(K')$  since any element of  $\sigma'(K')[x]$  is of the form  $f^{\sigma'}$  for some  $f \in K'[x]$  and so we can let  $\alpha$  be a root of  $f$ , giving that  $\sigma'(\alpha)$  is a root of  $f^{\sigma'}$ . Now  $\sigma'(K') \geq \sigma(K)$  so if  $L$  is algebraic over  $\sigma(K)$ , then  $L$  is also algebraic over  $\sigma'(K')$ . So if  $L$  is algebraically closed then  $L = \sigma'(K')$ , giving that  $\sigma'$  is surjective and thus an isomorphism (all field isomorphisms are injective). □

**Corollary 1.4.** The algebraic closure of a field  $K$  is unique upto an isomorphism fixing  $K$ .

**Definition 1.5** (Splitting field). Let  $K \leq L$  be fields and let  $\mathcal{F} \subset K[x]$  be a family of polynomials. We say that  $L$  is a splitting field for  $\mathcal{F}$  over  $F$  if each  $f \in \mathcal{F}$  splits into linear factors in  $L[x]$  and  $L$  is the field generated by  $K$  and the roots of all polynomials in  $\mathcal{F}$ .

**Proposition 1.6.** A splitting field is unique upto an isomorphism fixing  $F$ .

*Proof.* Let  $L \geq K$  and  $L' \geq K$  be two splitting fields for a family  $\mathcal{F} \subset K[x]$ . We note that  $L'$  and  $L$  are both algebraic over  $K$  (as they are generated by roots). This means that we may use Proposition 1.3 to extend the identity map  $K \rightarrow K$  to a field homomorphism  $\sigma : L \rightarrow \widehat{L}'$  where  $\widehat{L}' \geq L'$  is algebraically closed. However, note that  $\sigma(L) \subset L'$  since  $\sigma$  maps each root of some  $f \in \mathcal{F}$  to a root of  $f$  (as  $\sigma$  fixes  $K$ ). So  $\sigma : L \rightarrow L'$  is a homomorphism. It remains to show that  $\sigma$  is surjective. To see this, let  $f \in \mathcal{F}$  and write  $f(x) = \prod_i (x - \alpha_i)$  where  $\alpha_i \in L$ . Then  $f = f^\sigma = \prod_i (x - \sigma(\alpha_i))$ . This shows that any root in  $L'$  of any  $f \in \mathcal{F}$  is in the image of  $\sigma$  (using the unique factorization property). Thus as  $L'$  is generated by these roots, the surjectivity of  $\sigma$  follows.  $\square$

If  $K_1$  and  $K_2$  are two fields with a common subfield  $K$ , we say that a homomorphism  $K_1 \rightarrow K_2$  is a  $K$ -homomorphism if it restricts to the identity on  $K$ .

**Theorem 1.7.** Let  $L$  be an algebraic extension of a field  $K$ . Then the following are equivalent.

- (1)  $L$  is a splitting field for some family of polynomials in  $K[x]$ .
- (2) Any  $K$ -homomorphism  $L \rightarrow \overline{L}$ , where  $\overline{L} \geq L$  is an algebraic closure, restricts to an automorphism of  $L$ .
- (3) Any irreducible polynomial in  $K[x]$  that has a root in  $L$  must decompose into linear factors in  $L[x]$ .

*Proof.* (i)  $\implies$  (ii): If  $L$  is a splitting field for some polynomials in  $K[x]$  and  $\sigma : L \rightarrow \overline{L}$  is a  $K$ -homomorphism, then as in the proof of the uniqueness of splitting fields above, we see that  $\sigma$  maps into  $L$ . We also saw that it permutes the roots of a polynomial in  $K[x]$  in  $L$  and thus the image of  $\sigma$  is  $L$ , thus  $\sigma$  is surjective and hence an automorphism.

(ii)  $\implies$  (iii): Suppose  $f \in K[x]$  is irreducible and has a root  $\alpha \in L$ . Now if  $\alpha' \in \overline{L}$  is another root of  $f$ , then since  $f$  is irreducible we have an isomorphism  $K[\alpha] \rightarrow K[\alpha']$  mapping  $\alpha$  to  $\alpha'$ , which we may extend to an  $K$ -homomorphism  $\sigma : L \rightarrow \overline{L}$  by a previous Lemma. By condition (ii), we see that  $\sigma$  maps  $L$  to  $L$  and thus  $\alpha' = \sigma(\alpha) \in L$ . Hence  $L$  contains all the roots of  $f$ .

(iii)  $\implies$  (ii): As  $L$  is algebraic, every element  $\alpha \in L$  is the root of some irreducible polynomial  $f \in K[x]$ . We thus let  $\mathcal{F} \subset K[x]$  be those irreducible polynomials with at least one root in  $L$ , which split into linear factors by assumption. Thus  $L$  is the splitting field of  $\mathcal{F}$  over  $K$ .  $\square$

**Definition 1.8.** We say that an extension  $K \leq L$  is normal if it is the splitting field of some family of polynomials.

**Example 1.9.** The extension  $\mathbb{Q} \leq \mathbb{Q}[2^{1/3}]$  is not normal. To see this we use the characterization (iii) in the Theorem as follows: The polynomial  $x^3 - 2$  is irreducible, has one root  $2^{1/3}$  in our extension but not any other. Alternatively, we can use (ii) by noting that although there is  $\mathbb{Q}$ -homomorphism  $\mathbb{Q}[2^{1/3}] \rightarrow \overline{\mathbb{Q}}$  mapping  $2^{1/3}$  to  $2^{1/3}e^{2\pi i/3}$ , it does not restrict to an automorphism of  $\mathbb{Q}[2^{1/3}]$ .

**Example 1.10.** Normal is not transitive. As an example, consider the field extensions  $\mathbb{Q} \leq \mathbb{Q}[\sqrt{2}] \leq \mathbb{Q}[2^{1/4}]$ . The intermediate field extensions are normal (as they are of degree 2) but the extension  $\mathbb{Q} \leq \mathbb{Q}[2^{1/4}]$  is not.

**Definition 1.11.** If  $L \geq K$  is an algebraic extension, then we say that  $L' \leq L \leq K$  is a normal closure of  $L \geq K$  if  $L' \geq K$  is a normal extension and any  $L' \geq L'' \geq K$  such that  $L'' \geq K$  is normal must satisfy  $L'' = L'$ . That is, the normal closure if a minimal normal extension.

**Proposition 1.12.** Every algebraic extension  $L \geq K$  has a normal closure. More precisely, let  $\mathcal{F}$  be the set of all irreducible polynomials in  $K[x]$  such that each element of  $L \setminus K$  is the root of some  $f \in \mathcal{F}$ . Then the splitting field of  $\mathcal{F}$  is the normal closure of  $L \geq K$ .

*Proof.* Let  $\bar{L} \geq L$  be the algebraic closure of  $L$ . Define  $\bar{L} \geq L' \geq L$  to be the splitting field for the family  $\mathcal{F} \subset K[x]$  of minimal polynomials for elements of  $L$ . We claim that  $L'$  is the normal closure. Thus suppose that  $L \leq L'' \leq L'$  is such that  $K \leq L''$  is normal. We must show that  $L'' = L'$ , and since  $L'$  is generated by the roots of elements of  $\mathcal{F}$ , we must show that any root  $\alpha \in L'$  of a polynomial  $f \in \mathcal{F}$  is in  $L''$ . To see this, note that by definition  $f$  is a minimal polynomial of some  $\alpha' \in L$ . There is a  $K$ -homomorphism  $\sigma : K[\alpha'] \rightarrow \bar{L}$  mapping  $\alpha'$  to  $\alpha \in L$ . As  $L'' \geq L \geq K[\alpha']$ , we may extend this  $K$ -homomorphism to  $\sigma : L'' \rightarrow \bar{L}$ . But by characterization (ii) of the normality of  $K \leq L''$ , we see that  $\sigma$  is an automorphism of  $L''$ . This means that  $\alpha = \sigma(\alpha') \in L''$  as  $\alpha' \in L \subset L''$ . Thus this shows that  $L' \subset L''$ , and so  $L' = L''$  as required.  $\square$

**Proposition 1.13.** If  $K \leq L$  is an algebraic extension and  $L \leq L_1, L_2 \leq \bar{L}$  are two normal extensions of  $K$ , then  $L_1 \cap L_2$  is a normal extension of  $K$ . In particular, if  $L_1$  and  $L_2$  are both normal closures of  $L \geq K$ , then  $L_1 = L_2$ .

*Proof.* This follows from characterization (iii): If  $f \in K[x]$  is irreducible and has a root in  $\alpha \in L_1 \cap L_2$ , then  $f$  decomposes to linear factors in  $L_i[x]$  for  $i = 1, 2$ . By uniqueness of factorizations, this means that these linear factors are in  $(L_1 \cap L_2)[x]$ .  $\square$

**Proposition 1.14.** A normal closure of an algebraic extension  $L \geq K$  is unique upto an  $L$ -automorphism.

*Proof.* By the previous construction, we have one such normal closure given by  $L[\mathcal{R}]$  where

$$\mathcal{R} = \{r \in \bar{L} \mid f(r) = 0 \text{ for some } f \in \mathcal{F}\}$$

where  $\mathcal{F} \subset K[x]$  is the set of all irreducible polynomials such that each element of  $L$  is the root of some  $f \in \mathcal{F}$ . We now let  $L' \geq L$  be another field such that  $L' \geq K$  is the normal closure of  $L \geq K$ . We now construct an isomorphism  $L[\mathcal{R}] \rightarrow L'$  which fixes  $L$ . We extend the inclusion  $L \rightarrow \bar{L}$  to an  $L$ -homomorphism  $\sigma : L[\mathcal{R}] \rightarrow \bar{L}$ . Note that  $L'' = \sigma(L[\mathcal{R}]) = L[\sigma(\mathcal{R})]$  contains  $L$  and is the splitting field of  $\mathcal{F}$  in  $\bar{L}$  over  $K$ . Thus  $L'$  and  $L''$  are subfields of  $\bar{L}$  that are normal extensions of  $K$  and both contain  $L$ . Moreover,  $L''$  is also a normal closure of  $L \geq K$  as it follows the construction given in Proposition 1.12 (i.e., it is a splitting field of minimal polynomials over  $K[x]$  of elements in  $L$ ). By the previous proposition, it follows that  $L' = L''$ , thus  $\sigma$  is an isomorphism.  $\square$

## 2. SEPERABLE EXTENSIONS

**Lemma 2.1.** An irreducible polynomial  $f \in K[x]$  splits into distinct linear factors in some algebraic closure if and only if  $f' = 0$ .

*Proof.* By the product rule it follows that if  $f(\alpha) = 0$  then  $\alpha$  is a repeated root if and only if  $f'(\alpha) = 0$ . If  $f$  is irreducible, has a repeated root  $\alpha$  and  $f' \neq 0$  then  $(X - \alpha) | \gcd(f, f') | f$ , which contradicts the irreducibility of  $f$ .  $\square$

As a consequence, if  $\text{char} K = 0$  then an irreducible polynomial must split into distinct linear factors.

**Definition 2.2.** We say that  $f \in K[x]$  is separable if  $f$  splits into distinct linear factors in some (hence any) algebraic closure of  $K$ .

**Theorem 2.3.** If  $\text{char} K = p$  and  $f \in K[x]$  is irreducible, then each root of  $f$  has multiplicity  $p^r$  where  $r$  is minimal non-negative integer such that  $f(x) = g(x^{p^r})$  for some  $g \in K[x]$ .

*Proof.* Write  $g(x) = \sum_j c_j x^j$ . Since

$$g'(x) = \sum_j j c_j x^{j-1}$$

we observe that  $g'(x)$  is not the zero polynomial as follows: If  $g'(x) = 0$  then  $c_j = 0$  whenever  $j$  is not divisible by  $p$ . From this it follows that  $g(x) = \sum_k c_{kp} x^{kp} = h(x^p)$ . It now follows that

$$f(x) = g(x^{p^r}) = h((x^{p^r})^p) = h(x^{p^{r+1}}),$$

which contradicts the maximality of  $r$ . Thus  $g'(x) \neq 0$ . This means that  $g(x) = \prod_i (x - \alpha_i)$  where  $\alpha_i$  are distinct. Write  $\alpha_i = \beta_i^{p^r}$ , which exists in an algebraic closure. Note that the  $\beta_i$  must also be distinct. Thus

$$f(x) = \prod_i (x^{p^r} - \beta_i^{p^r}) = \prod_i (x - \beta_i)^{p^r},$$

where the last equality follows from Freshman's dream in characteristic  $p$ . As the  $\beta_i$  are distinct, the proof is complete.  $\square$

**Definition 2.4.** If  $K \leq L$  is an algebraic field extension then  $\alpha \in L$  is called separable over  $K$  if the minimal polynomial is separable (splits over linear factors in some, hence any, algebraic closure). We say that the extension  $K \leq L$  is separable if all elements of  $L$  are separable over  $K$ .

Thus from above, in characteristic zero all algebraic extensions are separable, as all irreducible polynomials are separable.

**Example 2.5.** Consider the field  $K = \mathbb{F}_p(t)$ . The polynomial  $f(x) = x^p - t$  is irreducible by Eisenstein's criterion in  $\mathbb{F}_p[t]$  as  $t$  is prime in this UFD, and hence  $f(x)$  is irreducible also over its field of fractions  $K$  by Gauss's Lemma. Now,  $f(\alpha) = 0$  in for some  $\alpha \in \overline{K}$ , that is  $\alpha^p = t$ . But by Freshman's dream we have that

$$x^p - t = x^p - \alpha^p = (x - \alpha)^p,$$

thus  $\alpha$  is a root of multiplicity  $p$  for  $f(x)$ . Thus  $f(x)$  is irreducible but not separable.

**Definition 2.6.** If  $K \leq L$  is an algebraic extension, then we let

$$\text{Hom}_K(L, \overline{K})$$

denote the set of all  $K$ -homomorphisms  $L \rightarrow \overline{K}$ . We let

$$|L : K|_s = |\text{Hom}_K(L, \overline{K})|$$

be the separable degree of  $K \leq L$ , which does not depend on the choice of  $\overline{K}$ .

**Proposition 2.7.** If  $K \leq L \leq M$  are algebraic extensions then there is a bijection

$$\text{Hom}_K(L, \overline{K}) \times \text{Hom}_L(M, \overline{K}) \rightarrow \text{Hom}_K(M, \overline{K}).$$

In particular

$$|M : K|_s = |L : K|_s |M : L|_s.$$

*Proof.* For each  $\sigma \in \text{Hom}_K(L, \overline{K})$  we choose an arbitrary (there are many choices)  $\phi(\sigma) : \overline{K} \rightarrow \overline{K}$  automorphism that extends  $\sigma$ , where we have used Proposition???. Now we define a mapping

$$\text{Hom}_K(L, \overline{K}) \times \text{Hom}_L(M, \overline{K}) \rightarrow \text{Hom}_K(M, \overline{K})$$

by

$$(\sigma, \tau) \mapsto \phi(\sigma) \circ \tau.$$

Let us first check that it is well defined. If  $k \in K$  then

$$(\phi(\sigma) \circ \tau)(k) = \phi(\sigma)(\tau(k)) = \phi(\sigma)(k) = \sigma(k) = k,$$

so indeed  $\phi(\sigma) \circ \tau$  is a  $K$ -homomorphism. To show injectivity, suppose that

$$\phi(\sigma) \circ \tau = \phi(\sigma') \circ \tau'.$$

Then for any  $\ell \in L$  we have that

$$\phi(\sigma)(\tau(\ell)) = \phi(\sigma)(\ell) = \sigma(\ell)$$

and by the same argument  $\phi(\sigma')(\tau'(\ell)) = \sigma'(\ell)$ . Thus  $\sigma = \sigma'$ . This means that  $\phi(\sigma) = \phi(\sigma')$  and so by injectivity of field automorphisms, we must have that  $\tau'(m) = \tau(m)$  for all  $m \in M$ . So  $\tau = \tau'$ . It now remains to show injectivity. Thus suppose that  $\gamma \in \text{Hom}_K(M, \overline{K})$ . Let  $\sigma$  be the restriction of  $\gamma$  to  $L$  and observe that  $\sigma \in \text{Hom}_K(L, \overline{K})$ . Now let

$$\tau = \phi(\sigma)^{-1} \circ \gamma : M \rightarrow \overline{K}.$$

If  $\ell \in L$  then

$$\tau(\ell) = \phi(\sigma)^{-1}(\gamma(\ell)) = \phi(\sigma)^{-1}(\sigma(\ell)) = \phi(\sigma)^{-1}\phi(\sigma)(\ell) = \ell,$$

thus indeed  $\tau \in \text{Hom}_L(M, \overline{K})$ . This shows that  $\gamma = \phi(\sigma) \circ \tau$  is in the image of our map, thus our map is surjective.  $\square$

**Proposition 2.8.** If  $K \leq L$  is a finite extension then

- (1) If  $K$  has characteristic zero then  $|L : K| = |L : K|_s$
- (2) If  $K$  has characteristic  $p$  then  $|L : K| = p^r |L : K|_s$  for some integer  $r \geq 0$ .

*Proof.* By finiteness of this extension  $L$  can be obtained from  $K$  by finitely many simple extensions, so we only need to prove this when  $L = K(\alpha)$  is a simple extension and then use the previous proposition to give the general case by induction. If  $\text{Char} K = 0$  then we know that  $|L : K| = \deg f = |L : K|_s$  where  $f \in K[x]$  is the minimal polynomial of  $\alpha$ , where we have used the fact that  $f$  is separable and there is a unique  $K$ -homomorphism mapping  $\alpha$  to any given root of  $f$ . If  $\text{Char} K = p$  then  $|L : K| = \deg f = p^r |L : K|_s$  where  $r$  is maximal integer such that  $f(x) = g(x^{p^r})$  for some polynomial  $g(x) \in K[x]$ , as seen in a previously proven result. Thus completing the proof.  $\square$

**Theorem 2.9.** Let  $K \geq L$  be a finite extension. The following are equivalent.

- (1)  $K \geq L$  is separable.

- (2)  $L = K(a_1, \dots, a_n)$  for some  $a_1, \dots, a_n \in L$  that are separable over  $K$   
 (3)  $|L : K|_s = |L : K|$

*Proof.* (i)  $\implies$  (ii) is trivial. (ii)  $\implies$  (iii): Letting  $K_i = K_{i-1}(a_i)$  we see that  $a_i$  is separable over  $K_{i-1} \geq K$  and thus  $|K_i : K_{i-1}| = \deg(f_i) = |K_i : K_{i-1}|_s$  where  $f_i$  is the minimal polynomial of  $a_i$  over  $K_{i-1}$ . We are now done by the multiplicativity formula. (iii)  $\implies$  (i): We only need to focus on  $\text{Char} K = p > 0$ . If  $a \in L$  is not separable over  $K$  then

$$|K(a) : K|_s < |K(a) : K|$$

, but then

$$|L : K|_s = |L : K(a)|_s |K(a) : L|_s < |L : K(a)| |K(a) : K| = |L : K|.$$

□

**Corollary 2.10.** If  $K \leq L \leq M$  are algebraic extensions then  $K \leq M$  is separable if and only if  $K \leq L$  and  $L \leq M$  are separable.

*Proof.* First suppose  $K \leq M$  is separable. Then clearly  $K \leq L$  is separable. Now for  $a \in M$  we have that the minimal polynomial  $f(x) \in K[x]$  of  $a$  over  $K$  splits into linear factors. If  $g(x) \in L[x]$  is the minimal polynomial of  $a$  over  $L$ , then clearly  $g(x) | f(x)$  as  $f(x) \in L[x]$ . Thus  $g(x)$  also splits into linear factors.

Conversely, assume now that  $K \leq L$  and  $L \leq M$  are separable. Fix  $a \in M$ . Then  $|L(a) : L| = |L(a) : L|_s$  as  $L \leq M$  is separable. Now let  $L' \leq L$  be the field generated by  $K$  and the coefficients of the minimal polynomial  $f(x) \in L[x]$  of  $a$  over  $L$ . Thus  $f(x) \in L'[x]$  which means that  $a$  is separable over  $L'$  as well (as  $f(x)$  splits into linear factors and  $f(a) = 0$ ). Thus  $|L'(a) : L'|_s = |L(a) : L|$ . It now follows that

$$|L'(a) : K|_s = |L'(a) : L'|_s |L' : K|_s = |L'(a) : L| |L' : K| = |L'(a) : K|,$$

hence by the previous theorem we have that  $L'(a)$  is separable over  $K$ , and thus  $a$  is separable over  $K$ . □

**Theorem 2.11** (Primitive element theorem). If  $K \leq L$  is a finite separable extension, then  $L = K(a)$  for some  $a \in L$ .

*Proof.* If  $L$  is finite, then this follows from the fact that the multiplicative group of a field is cyclic. Suppose thus that  $K$  and  $L$  are infinite. We may reduce to the case where  $L = K(\alpha, \beta)$ , as the general case then follows by induction (If  $L = K(a_1, \dots, a_n)$  then  $L = K'(a_1, a_2)$  where  $K' = K(a_3, \dots, a_n)$  and certainly  $L$  is separable over  $K'$ ). For  $c \in K$ , we let  $\gamma_c = \alpha + c\beta$ . We will show that  $L = K(\gamma_c)$  for infinitely many  $c \in K$  as follows. If  $L \neq K(\gamma_c)$  then definitely  $\beta \notin K(\gamma_c)$ . As  $L$  is separable over  $K(\gamma_c)$ , this means that the minimal polynomial of  $\beta$  over  $K(\gamma_c)$  has another root  $\beta' \in \overline{K}$ . Thus there exists a  $K(\gamma_c)$ -homomorphism  $\sigma : L \rightarrow \overline{K}$  with  $\sigma(\beta) = \beta' \neq \beta$ . We thus get that

$$\sigma(\alpha) + c\sigma(\beta) = \alpha + c\beta$$

and thus

$$c = \frac{\sigma(\alpha) - \alpha}{\beta - \sigma(\beta)}.$$

But the right hand side has only finitely many choices (as there are only finitely many choices of  $\sigma$ ) and so if we choose a  $c$  not of this form (as  $K$  is infinite) we see that  $L = K(\gamma_c)$  as desired. □

## 3. GALOIS EXTENSIONS

**Definition 3.1.** A field extension  $K \leq L$  is called *Galois* if it is normal and separable. We also say  $L$  is *Galois* over  $K$ . We define  $\text{Gal}(L/K) := \text{Aut}_K(L)$  to be the set of  $K$ -automorphisms  $L \rightarrow L$ .

**Proposition 3.2.** Suppose that  $K \leq L$  is Galois and  $K \leq E \leq L$  is an intermediate field.

- (1) Then  $L$  is also Galois over  $E$  and  $\text{Gal}(L/E) \subset \text{Gal}(L/K)$ .
- (2) If  $E$  is also Galois over  $K$ , then every  $\sigma \in \text{Gal}(L/K)$  restricts to an automorphism  $\sigma|_E \in \text{Gal}(E/K)$ . Moreover, this restriction homomorphism is surjective.

*Proof.* It is clear from the definition that  $K \leq L$  normal (resp. separable) implies that  $E \leq L$  is normal (resp. separable). Any  $E$ -automorphism fixes each element of  $E$  and hence each element of  $K \leq E$ , thus the inclusion in (i). For (ii): We already know that as  $E$  is normal over  $K$  then any  $K$ -automorphism of  $L$  must map  $E$  into  $E$  surjectively as  $E$  is the splitting field of some polynomials over  $K$  and thus any automorphism permutes these roots (which are the generators for  $E$  over  $K$ ). By Proposition??? any  $K$ -automorphism  $\sigma : E \rightarrow E$  can be extended to some  $K$ -homomorphism  $\bar{\sigma} : \bar{K} \rightarrow \bar{K}$ . But  $\bar{\sigma}$  must permute the roots of any polynomial in  $K[x]$  and in particular those for which  $L$  is the splitting field for, thus  $\bar{\sigma}$  restricts to an automorphism of  $L$ .  $\square$

**Proposition 3.3.** Let  $L$  be a field and let  $G$  be a subgroup of  $\text{Aut}(L)$ . Let

$$K = L^G := \{a \in L \mid ga = a \text{ for all } g \in G\}$$

be the fixed field of  $G$ .

- (1) If  $G$  is finite then  $K \leq L$  is a finite Galois extension and  $\text{Gal}(L/K) = G$  and  $[L : K] = |G|$
- (2) If  $K \leq L$  is algebraic and  $G$  is not necessarily finite, then  $K \leq L$  is a Galois Extension with  $G \leq \text{Gal}(L/K)$ .

*Proof.* We first show that in both case (i) or (ii), the orbit  $Ga$  is finite for all  $a \in L$ . This is obvious in (i). In (ii), since  $a$  is algebraic over  $K$  then there is a non-zero polynomial  $f \in K[x]$  such that  $f(a) = 0$ . But now  $f(g(a)) = 0$  for all  $g \in G$  as  $g$  fixes  $K$  and hence  $f$ . Thus the orbit  $Ga$  is contained in the roots of  $f$ , which is a finite set. So now we just assume that  $Ga$  is finite for all  $a \in L$ . Consider the polynomial

$$f_a(x) = \prod_{\alpha \in Ga} (x - \alpha).$$

Note that  $g$  permutes these linear factors, thus  $f_a(x) \in L^G[x] = K[x]$ . Thus  $a$  is algebraic over  $K$ . Moreover, it now follows that  $L$  is the splitting field of  $\{f_a \mid a \in L\}$ , thus  $L$  is normal over  $K$  and also separable as these factors are distinct. Thus  $K \leq L$  is indeed a Galois extension. We now complete the proof of (i), thus assume from now that  $G$  is finite. To show that  $K \leq L$  is a finite extension, it will be enough to find a uniform bound on intermediate fields  $K \leq L' \leq L$  such that  $K \leq L'$  is a finite normal extension (because we know  $K \leq L$  is algebraic and thus if it is infinite then we choose finitely many elements in  $L$  such that the field they generate is arbitrarily large. The normal closure of this field is also finitely generated hence a finite extension). Now as such an  $L'$  is finite, the primitive root theorem says that  $L' = K(a)$  for some  $a \in L$ . But then we know that the minimal polynomial of  $a$  is a divisor of  $f_a(x) \in K[x]$  above, which is of degree at most  $|G|$ , thus  $[L' : K] \leq |G|$ . It follows that  $[L : K] \leq |G|$ , so  $L$  is indeed a finite extension. Now we use the primitive root theorem to write  $L = K(\alpha)$  for some  $\alpha \in L$ . Observe that if  $g\alpha = \alpha$  then  $g = \text{Id}_L = 1_G$ , thus  $|G| \leq [L : K]_s = [L : K]$ . This completes the proof that  $[L : K] = |G|$ .  $\square$

**Theorem 3.4** (Fundamental theorem of Galois Theory). Suppose that  $K \leq L$  is a Galois extension. Let  $\text{Fields}(L/K)$  denote the set of intermediate fields  $K \leq E \leq L$ . For a group  $G$  we let  $\text{SubGrps}(G)$  denote the set of subgroups  $H \leq G$ . Define the maps

$$\phi : \text{SubGrps}(\text{Gal}(L/K)) \rightarrow \text{Fields}(L/K)$$

that maps

$$H \leq \text{Gal}(L/K)$$

to the fixed field  $L^H$  and

$$\psi : \text{Fields}(L/K) \rightarrow \text{SubGrps}(\text{Gal}(L/K))$$

which maps an intermediate field  $K \leq E \leq L$  to the Galois group  $\text{Gal}(L/E) = \text{Aut}_E(L)$ . Then

$$\phi \circ \psi = \text{Id}_{\text{Fields}(L/K)}.$$

Moreover, if the extension  $K \leq L$  is finite, then

$$\psi \circ \phi = \text{Id}_{\text{SubGrps}(\text{Gal}(L/E))}$$

and thus these maps bijective and inverses of each other. Moreover, if  $K \leq L$  is finite then a subgroup  $H \leq \text{Gal}(L/K)$  is normal if and only if  $L^H$  is normal over  $K$  (and thus  $K \leq L^H$  is Galois), in which case there is a surjective group homomorphism  $\text{Gal}(L/K) \rightarrow \text{Gal}(L^H/K)$  which maps  $\sigma$  to  $\sigma|_{L^H}$  and  $H$  is the kernel of this map, so

$$\text{Gal}(L/K)/H \cong \text{Gal}(L^H/K).$$

*Proof.* Let  $K \leq E \leq L$  be an intermediate field, then we know that  $E \leq L$  is Galois. Now let  $H = \text{Gal}(L/E)$  and  $E' = L^H$ . Clearly  $E \leq E'$  (if  $a \in E$  then  $h(a) = a$  for all  $h \in H$  and so  $a \in L^H = E'$ ). Now suppose for contradiction that  $a \in E'$  but  $a \notin E$ . Hence as  $L/E$  is separable, the minimal polynomial of  $a$  over  $E$  has another root  $b \neq a$  and thus there is a  $h \in \text{Aut}_E(L) = H$  that maps  $a$  to  $b$ . Thus  $a \notin L^H = E'$ , a contradiction. This means that  $E' = E$ , thus showing that  $\psi \circ \phi$  is the identity as claimed.

Now we assume that  $K \leq L$  is finite, thus  $L = K(\alpha)$  for some  $\alpha \in L$  by the primitive root theorem. Clearly  $G = |\text{Gal}(L/K)|$  is finite since  $g \in G$  is uniquely determined by the image of  $\alpha$ , which must be a root of the minimal polynomial of  $\alpha$ . Choose a subgroup  $H \leq \text{Gal}(L/K)$ . Thus  $H$  is finite and we may apply the Proposition ?? to deduce that  $\psi(\phi(H)) = \text{Gal}(L/L^H) = H$ . Thus  $\phi$  and  $\psi$  are inverses in when  $K \leq L$  is a finite extension.

Finally, suppose that  $K \leq E \leq L$  is such that  $E$  is a normal extension of  $K$ . We now wish to show that  $H = \text{Gal}(L/E)$  is normal in  $\text{Gal}(L/K)$ . To see this, we know from Proposition ??? that there is a surjective homomorphism  $\text{Gal}(L/K) \rightarrow \text{Gal}(E/K)$  mapping  $\sigma \in \text{Gal}(L/K)$  to  $\sigma|_E$ . Observe that  $g \in \text{Gal}(L/K)$  is in the kernel of this homomorphism if and only if  $g|_E = 1$  which happens if and only if  $g(e) = e$  for all  $e \in E$  which happens if and only if  $g \in \text{Gal}(L/E) = H$ . Thus  $H$  is the kernel of a homomorphism, thus a normal subgroup as desired.

Conversely, suppose that  $H$  is a normal subgroup of  $\text{Gal}(L/K)$  and let  $E = L^H$ . We wish to show that  $L^H$  is normal over  $K$ . Thus we wish to show that if  $\sigma : L^H \rightarrow \overline{K}$  is a  $K$ -homomorphism then  $\sigma(L^H) = L^H$ . To show this, let  $a \in L^H$  be arbitrary and let  $b = \sigma(a)$ . To show  $b \in L^H$  we have to show that  $hb = b$  for all  $h \in H$ . Now extend  $\sigma$  to an automorphism  $\sigma : L \rightarrow L$  (as  $L$  is normal over  $K$ ). Then  $\sigma H = H\sigma$  as  $H$  is normal in  $\text{Gal}(L/K)$ . Thus  $h\sigma = \sigma h'$  for some  $h' \in H$  and thus

$$hb = h\sigma a = \sigma h'a = \sigma a = b.$$



Thus  $b \in L^H$ . So  $\sigma(L^H) \subset L^H$ . It now remains to show the opposite inclusion. Thus suppose  $a \in L^H$ , then  $\sigma^{-1}H = H\sigma^{-1}$  (note that  $\sigma^{-1} : L \rightarrow L$  is defined as  $\sigma$  is an automorphism of  $L$ ). Now the same argument shows that  $\sigma^{-1}(a) \in L^H$  and thus  $\sigma^{-1}(L^H) \subset L^H$ , i.e.,  $L^H \subset \sigma(L^H)$ .  $\square$

**Example 3.5.** Let  $\alpha = 2^{1/4}$  and let  $L = \mathbb{Q}[\alpha, i]$  which is the splitting field of the polynomial  $X^4 - 2$ . Let us compute the Galois group  $G = \text{Gal}(L/\mathbb{Q})$ . Observe that for  $g \in G$  we have that

$$g(\alpha) \in \{\alpha, i\alpha, -\alpha, -i\alpha\}$$

and

$$g(i) \in \{\pm i\}$$

. Thus  $|G| \leq 8$ . Let us show that all 8 combinations are possible (realised by some  $g \in G$ ). Let  $\sigma : L \rightarrow L$  be the complex conjugation map, so  $\sigma \in G$ . Now we know that for each  $k \in \{0, 1, 2, 3\}$  there exists a  $g_k \in G$  such that  $g_k(\alpha) = i^k \alpha$  (as  $X^4 - 2$  is irreducible over  $\mathbb{Q}$  there is a  $\mathbb{Q}$ -automorphism mapping any root to any other root). Now notice that  $g_k \circ \sigma(\alpha) = g_k(\alpha) = i^k \alpha$  and yet  $g_k \circ \sigma(i) = g_k(-i) = -g_k(i)$ . Thus the elements  $g_k \circ \sigma^e \in \text{Gal}(L/K)$  are all distinct for distinct  $(k, e) \in \{0, 1, 2, 3\} \times \{0, 1\}$  and so all 8 combinations are possible. Let  $r \in G$  be the map given by  $g(\alpha) = i\alpha$  and  $g(i) = i$ . Thus  $g(i^k \alpha) = i^{k+1} \alpha$ . So  $r$  rotates the elements  $\alpha, i\alpha, i^2 \alpha, i^3 \alpha$  cyclically. While  $\sigma$  is an involution that swaps  $i\alpha$  with  $i^3 \alpha$  and fixes  $\alpha, i^2 \alpha$ . Every element of  $G$  is of the form  $r^k \sigma^e$  where  $(k, e) \in \{0, 1, 2, 3\} \times \{0, 1\}$ . Thus  $G$  is isomorphic to  $D_8$  since if consider the elements  $\alpha, i\alpha, i^2 \alpha, i^3 \alpha$  as successive corners of a square, then  $r$  is a rotation and  $\sigma$  is a reflection. Note that  $[L : \mathbb{Q}] = 8$  and a  $\mathbb{Q}$ -basis is given by

$$\{\alpha^k i^e \mid i \in \{0, 1, 2, 3\}, e \in \{0, 1\}\}.$$

Let us consider some intermediate fields and corresponding subgroups. First, consider the reflection group  $\{1, \sigma\}$ . The only elements of  $L$  fixed by this group are  $L \cap \mathbb{R} = \mathbb{Q}[2^{1/4}]$ . This subgroup is not normal and indeed  $\mathbb{Q}[2^{1/4}]$  is not a normal extension of  $\mathbb{Q}$ . On the other hand, the rotation subgroup  $\langle r \rangle$  is normal, and so the fixed field should be normal. To compute the fixed field, note that we may write each  $x \in L$  as

$$x = \sum_{k=0}^3 \lambda_k \alpha^k,$$

for some unique  $\lambda_k \in \mathbb{Q}[i]$ . Thus if  $rx = x$  then  $\lambda_k = i^k \lambda_0$ , thus we must have that  $x = \lambda_0 \in \mathbb{Q}[i]$ . This shows that the fixed field for this rotation subgroup is  $\mathbb{Q}[i]$ , which indeed is normal (the splitting field of  $x^2 + 1$ ). Observe now that each  $g \in G$  restricts to an automorphism of this fixed field  $\mathbb{Q}[i]$  and it restricts to the identity on  $\mathbb{Q}[i]$  if and only if  $g$  is in this rotation group, giving the isomorphism

$$G/\langle r \rangle \cong \text{Gal}(\mathbb{Q}[i]/\mathbb{Q}).$$

Now consider the group of order 4 generated by the reflections  $\sigma$  (complex conjugation) and the map  $\tau \in G$  given by  $\tau(\alpha) = -\alpha$  and  $\tau(i) = i$ . The subgroup is abelian of order 4 as  $\sigma$  and  $\tau$  commute. The fixed field is  $\mathbb{Q}[\alpha^2] = \mathbb{Q}[\sqrt{2}]$ , which is also normal over  $\mathbb{Q}$  (splitting field of  $X^2 - 2$ ).