

620-321 Algebra  
Semester 1, 2005  
Additional notes on Galois Theory  
(revised 27 May 2005)

**Assumption:** all fields are assumed to have characteristic 0. Much, but not all, of what follows can be generalized to fields of arbitrary characteristic.

Suppose  $F \subseteq K$  is a field extension. An  $F$ -automorphism of  $K$  (or an automorphism of  $K$  over  $F$ ) is a field isomorphism  $\phi : K \rightarrow K$  which fixes  $F$ , that is,  $\phi(a) = a$  for every  $a \in F$ . The collection of  $F$ -automorphisms of  $K$  forms a group with composition as the group operation. This group is called the *Galois group* of the extension and is denoted  $G(K/F)$  or  $\text{Gal}(K/F)$ .

Let  $H$  be a group of automorphisms of the field  $K$ . The set of elements of  $K$  which are fixed by all the automorphisms of  $H$  forms a subfield, called the *fixed field* of  $H$ . The fixed field is usually denoted  $K^H$ , so

$$K^H = \{a \in K \mid \phi(a) = a \text{ for all } \phi \in H\}.$$

A field extension  $F \subseteq K$  of finite degree is called a *Galois extension* if the order of the Galois group is equal to the degree of the extension, that is,

$$|G(K/F)| = [K : F]$$

We can now state the main result we want to prove.

**Theorem 1 (Main Theorem of Galois Theory)** *Let  $K$  be a Galois extension of  $F$  and let  $G = G(K/F)$  be its Galois group. The function*

$$H \rightsquigarrow K^H$$

*is a bijective map from the set of subgroups of  $G$  to the set of intermediate fields  $F \subseteq L \subseteq K$ . Its inverse is the function*

$$L \rightsquigarrow G(K/L).$$

*This correspondence has the property that if  $H = G(K/L)$  then*

$$[K : L] = |H| \text{ and hence } [L : F] = [G : H].$$

*Moreover  $L$  is a Galois extension of  $F$  if and only if  $H$  is a normal subgroup of  $G$ . When this is so,  $G(K/L)$  is isomorphic to the quotient group  $G/H$ .*

This remarkable correspondence between intermediate field between  $F$  and  $K$  and the subgroups of  $G(K/F)$  is called the *Galois correspondence*. Note that it is order reversing: if  $L_1 \subseteq L_2$  then  $G(K/L_1) \supseteq G(K/L_2)$  and if  $H_1 \subseteq H_2$  then  $K^{H_1} \supseteq K^{H_2}$ . Since the Galois group  $G(K/F)$  is finite, there are only finitely many fields  $L$  with  $F \subseteq L \subseteq K$ . Without the Main Theorem, this isn't obvious.

We next embark on the task of proving this theorem. In particular we will establish some conditions equivalent to being a Galois extension and give some other useful results. First we introduce the notion of a *splitting field* and show that splitting fields are Galois extensions. In particular we then have a source of examples.

**Splitting fields:** We know that a monic irreducible polynomial  $f(x)$  has a root in the field  $E = F[x]/(f(x))$  which is an extension of  $F$  of degree equal to the degree of  $f(x)$ . Thus in  $E[x]$  we have  $f(x) = (x - \alpha_1) \cdot g(x)$  where  $\alpha_1 \in E$ . Inductively by successively adding roots to the irreducible factors of  $g(x)$  we can find an extension  $L$  of  $F$  such that in  $L[x]$  our original polynomial  $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$  with  $\alpha_i \in L$ .

**Definition 1** *Let  $f(x) \in F[x]$  be a non-constant monic polynomial. A field extension  $K$  of  $F$  is a splitting field for  $f(x)$  if*

1.  $f(x)$  factors into linear factors in  $K$ :  $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$  with  $\alpha_i \in K$ ;
2.  $K$  is generated by the roots of  $f(x)$ :  $K = F(\alpha_1, \dots, \alpha_n)$

Every polynomial  $f(x) \in F[x]$  has a splitting field. First write  $f(x)$  as a product of irreducible factors. Then as above add roots to each of the irreducible factors of  $f(x)$  until it splits into linear factors in the field extension  $L$  and then take  $K$  to be the subfield  $F(\alpha_1, \dots, \alpha_n)$  of  $L$  generated by all the roots.

We are going to show that the splitting field  $K$  for a polynomial  $f(x) \in F[x]$  is unique (up to isomorphism) and is a Galois extension of  $F$ . Eventually it will also emerge from the theory that conversely Galois extensions are splitting fields.

We begin by observing that an isomorphism  $\sigma : F \rightarrow \overline{F}$  of fields extends naturally to an isomorphism of  $F[x]$  with  $\overline{F}[x]$  sending  $x \mapsto x$  and applying  $\sigma$  to the coefficients. If  $f(x) \in F[x]$  we will denote the corresponding polynomial in  $\overline{F}$  by  $\overline{f}(x)$ .

**Lemma 2** *Let  $F \subseteq K$  and  $\overline{F} \subseteq \overline{K}$  be field extensions and let  $\sigma : F \rightarrow \overline{F}$  be an isomorphism. If  $\beta \in K$  is algebraic over  $F$  with minimum polynomial  $g(x)$ , then  $\sigma$  can be extended to a monomorphism  $\phi : F(\beta) \rightarrow \overline{K}$  if and only if  $\overline{g}(x)$  has a root in  $\overline{K}$ . The number of such extensions is the number of distinct roots of  $\overline{g}(x)$  in  $\overline{K}$ .*

*Proof:* If such an extension  $\phi$  exists we can apply it to the relation  $g(\beta) = 0$  to get  $\overline{g}(\phi(\beta)) = 0$ . Thus  $\phi(\beta)$  is a root of  $\overline{g}(x)$  in  $\overline{K}$ . Conversely suppose that  $\overline{\beta}$  is a root of  $\overline{g}(x)$  in  $\overline{K}$ . Observe that  $\overline{g}(x)$  is monic and irreducible in  $\overline{F}[x]$  and hence is the minimum polynomial for  $\overline{\beta}$ . Thus the composition  $\phi$  of the isomorphisms

$$F(\beta) \cong F[x]/(g(x)) \cong \overline{F}[x]/(\overline{g}(x)) \cong \overline{F}(\overline{\beta})$$

is the desired extension. Moreover it is clear the number of choices for  $\overline{\beta}$  is just the number of distinct roots of  $\overline{g}(x)$  in  $\overline{K}$ .  $\square$

**Theorem 3** *Let  $\sigma : F \rightarrow \overline{F}$  be an isomorphism. Let  $F \subseteq K$  be a splitting field for  $f(x) \in F[x]$  and let  $\overline{F} \subseteq \overline{K}$  be a splitting field for the corresponding polynomial  $\overline{f}(x) \in \overline{F}[x]$ . Then  $\sigma$  extends to an isomorphism  $\psi : K \rightarrow \overline{K}$ . The number of such isomorphisms extending  $\sigma$  is precisely  $[K : F]$ .*

*Proof:* If  $f(x)$  factors into linear factors over  $F$ , then  $\bar{f}(x)$  also factors into linear factors. In this case  $F = K$  and  $\bar{F} = \bar{K}$  so  $\psi = \sigma$ . Now assume that  $f(x)$  does not factor completely and choose one of its monic irreducible factors  $g(x)$ . Let  $\beta \in K$  be a root of  $g(x)$  and define  $F_1 = F(\beta)$ . Now  $\bar{g}(x)$  is irreducible over  $\bar{F}$  and so has  $m$  distinct roots in  $\bar{K}$  where  $m = [F_1 : F]$  is the degree of  $g(x)$ . By the previous lemma there are precisely  $m$  choices for an extension of  $\sigma$  to a monomorphism  $\phi_1 : F_1 \rightarrow \bar{K}$ . Moreover any extension of  $\sigma$  to an isomorphism  $\psi : K \rightarrow \bar{K}$  must restrict to one of these choices of  $\phi_1$ .

Now  $[F_1 : F] > 1$  and since  $[K : F] = [K : F_1][F_1 : F]$  we have  $[K : F_1] < [K : F]$  and we can apply induction. Observe that  $K$  is also a splitting field for  $f(x)$  over  $F_1$  and for any choice of  $\phi_1$  the field  $\bar{K}$  is a splitting field for  $\bar{f}(x)$  over  $\phi_1(F_1)$ . So by the induction hypothesis there are exactly  $[K : F_1]$  choices for an isomorphism  $\phi_2 : K \rightarrow \bar{K}$  extending  $\phi_1$ . Hence there are  $[K : F] = [K : F_1][F_1 : F]$  choices altogether for extending  $\sigma$  to an isomorphism  $\psi : K \rightarrow \bar{K}$ .  $\square$

If we let  $F = \bar{F}$  and  $\sigma = \text{identity}$ , we obtain the following corollary:

**Corollary 4** *Any two splitting fields of  $f(x) \in F[x]$  over  $F$  are isomorphic.*  $\square$

If we let  $F = \bar{F}$ ,  $K = \bar{K}$  and  $\sigma = \text{identity}$ , then the extensions the identity to isomorphisms of  $K$  are just  $F$ -automorphisms. So we can conclude the following:

**Corollary 5** *If  $K$  is a splitting field of  $f(x) \in F[x]$  over  $F$ , then  $|G(K/F)| = [K : F]$ , that is,  $K$  is a Galois extension of  $F$ .*  $\square$

**Separated roots and primitive elements:** Two key results we need are the following which rely on our being in a field of characteristic 0. (They are false for certain fields of characteristic  $p > 0$ .)

**Proposition 6** *Let  $F$  be a field of characteristic 0. If  $f(x) \in F[x]$  is an irreducible polynomial, then the roots (in any splitting field) of  $f(x)$  are all distinct.*

*Proof:* Suppose suppose on the contrary that  $K$  is a splitting field for  $f(x)$  and that  $f(x) = (x - \alpha)^2 \cdot g(x)$  in  $K[x]$ . Just as in the usual calculus we can differentiate polynomial formally and the product rule holds. Thus  $f'(x) = 2(x - \alpha)g(x) + (x - \alpha)^2g'(x)$ . Now  $f(x)$  is the minimal polynomial in  $F[x]$  for  $\alpha$ . But  $f'(x) \in F[x]$  also has  $\alpha$  as a root which contradicts the minimality of  $f(x)$ . Hence  $f(x)$  has no repeated roots.  $\square$

**Theorem 7 (Existence of a primitive element)** *Let  $K$  be a finite extension of a field  $F$  of characteristic 0. Then there is an element  $\gamma \in K$  such that  $K = F(\gamma)$*

*Proof:* Since the extension has finite degree, it has a finite set of generators say  $K = F(a_1, \dots, a_n)$ . By induction it suffices to consider the case  $n = 2$  and find a primitive element for  $F(u, v)$ . We may suppose that  $f(x)$  and  $g(x)$  are the minimal polynomials in  $F[x]$  for  $u$  and  $v$  respectively.

Let  $L$  be a splitting field for  $f(x) \cdot g(x)$  containing  $F(u, v)$ . Now in  $L$  the roots of  $f(x)$  are distinct and we can label them  $u = u_1, u_2, \dots, u_n$  where  $n$  is the degree of  $f(x)$

and we have chosen  $u = u_1$  the first labelled root. Similarly  $g(x)$  has distinct roots  $v = v_1, v_2, \dots, v_m$  where  $m$  is the degree of  $g(x)$ .

Since  $F$  is infinite there is an element  $c \in F$  which is different from all the elements

$$\frac{u_i - u_1}{v_1 - v_j} \text{ for all } 1 \leq i \leq n \text{ and } 1 < j \leq m.$$

Define  $\gamma = u + cv = u_1 + cv_1$ .

We now show that  $F(u, v) = F(\gamma)$ . Let  $h(x) = f(\gamma - cx) \in F(\gamma)[x]$ . Note that  $h(v) = f(\gamma - cv) = f(u) = 0$ , so  $v = v_1$  is a root of  $h(x)$ . Consider some other root  $v_j$  ( $j > 1$ ) of  $g(x)$ . If  $f(\gamma - cv_j) = 0$  then for some  $i$  we have  $\gamma - cv_j = u_i$ . Then, since  $\gamma = u_1 + cv_1$  we have  $u_1 + cv_1 - cv_j = u_i$  or  $c = \frac{u_i - u_1}{v_1 - v_j}$  which contradicts the choice of  $c$ . Thus  $v$  is the only common root of  $g(x)$  and  $h(x)$ .

Let  $p(x)$  be the minimal polynomial of  $v$  over  $F(\gamma)$ . Then  $p(x)|g(x)$  so it splits in  $L[x]$  and has distinct roots. Also  $p(x)|h(x)$  so all its roots are roots of  $h(x)$ . Thus  $p(x)$  has a single root  $v$  and the degree of  $p(x)$  is 1. Thus  $v \in F(\gamma)$  and so also  $u = \gamma - cv \in F(\gamma)$ . Hence  $F(u, v) = F(\gamma)$  as desired. This completes the proof.  $\square$

**Groups of automorphisms of a field:** Our approach to the Main Theorem is based on Artin's theorem which depends on the above theorem on primitive elements and the following very useful proposition on orbits of roots.

**Proposition 8** *Let  $G$  be a finite group of automorphisms of a field  $K$  and let  $F = K^G$  be its fixed field. Let  $\{\beta_1, \dots, \beta_m\}$  be the orbit of an element  $\beta = \beta_1 \in K$  under the action of  $G$ . Then  $\beta$  is algebraic over  $F$ , its degree over  $F$  is  $m$ , and its irreducible polynomial over  $F$  is  $g(x) = (x - \beta_1) \cdots (x - \beta_m)$ . Note that  $m$  divides the order of  $G$  (since it is the size of an orbit).*

*Proof:* Observe that the polynomial  $g(x)$  is fixed by all the permutations of  $\{\beta_1, \dots, \beta_m\}$  and hence by the action of  $G$  which permutes the orbit. Therefore  $g(x) \in F[x]$  and  $\beta$  is algebraic over  $F$ . Let  $f(x)$  be the monic irreducible polynomial for  $\beta$  over  $F$ . Since  $f(x)$  is fixed by  $G$ , each of the elements  $\beta_i$  is a root of  $f(x)$  and so  $g(x)$  divides  $f(x)$ . But  $f(x)$  is the minimal polynomial for  $\beta$ , so  $g(x) = f(x)$ .  $\square$

We combine the above proposition with the existence of primitive elements to prove the following:

**Theorem 9 (E. Artin)** *Let  $G$  be a finite group of automorphisms of a field  $K$  and let  $F = K^G$  be its fixed field. Then the order of  $G$  is equal to the degree of  $K$  over  $F$ , that is,  $|G| = [K : K^G]$ .*

*Proof:* The above proposition shows that every element  $\beta$  of  $K$  is algebraic over  $F$  and that its degree divides  $n = |G|$ . The theorem of the primitive element implies that the degree of the whole extension is bounded by  $n$  too.

To see this choose an element  $\alpha_1 \in K$  which is not in  $F$  and set  $F_1 = F(\alpha_1)$ . Then  $[F_1 : F] \leq n$ . If  $F_1 \neq K$  choose  $\alpha_2 \in K$  which is not in  $F_1$  and set  $F_2 = F(\alpha_1, \alpha_2)$ . By the theorem of the primitive element  $F_2$  is generated by a single element  $\gamma$  and again

$[F_2 : F] \leq n$ . Continuing in this way we obtain a chain  $F < F_1 < F_2 \dots$  in which  $[F_i : F] \leq n$  for all  $i$ . Such a chain must be finite and thus  $F_i = K$  for some  $i$  and  $[K : F] \leq n$ .

Again by the theorem of the primitive element  $K = F(\beta)$  for some element  $\beta \in K$ . Any element which fixes  $\beta$  is the identity on all of  $K$  and hence is  $1 \in G$ . Therefore the stabilizer of  $\beta$  in  $G$  is 1 and the orbit has size  $n = |G|$ . So by the above proposition,  $\beta$  has degree  $n$  over  $F$  and  $[K : F] = n$ .  $\square$

We can now deduce several corollaries which imply parts of the Main Theorem.

**Corollary 10** *If  $F \subseteq K$  is a finite extension field, then the order of the Galois group  $G(K/F)$  divides the degree of the extension  $[K : F]$ .*

*Proof:* Put  $G = G(K/F)$ . The  $G$  acts on  $K$  as a group of automorphisms so by the above theorem  $|G| = [K : K^G]$ . Since  $F \subseteq K^G \subseteq K$ , it follows that  $[K : K^G]$  divides  $[K : F]$  which proves the result.  $\square$

**Corollary 11** *Let  $G$  be a finite group of automorphisms of a field  $K$  and let  $F = K^G$  be its fixed field. Then  $K$  is a Galois extension of  $F$  and  $G = G(K/F)$ , that is,*

$$G = G(K/K^G).$$

*Proof:* By definition of the fixed field the elements of  $G$  are  $F$ -automorphisms of  $K$  and so  $G \subseteq G(K/F)$ . Now by the previous corollary  $|G(K/F)| \leq [K : F]$  and by the above theorem  $[K : F] = |G|$ . It follows that  $|G(K/F)| = [K : F]$  and  $G = G(K/F)$ .  $\square$

We also have the following converse:

**Corollary 12** *Suppose that  $F \subseteq K$  is a Galois extension with Galois group  $G(K/F)$ . Then the fixed field of  $G$  is  $F$ , that is,*

$$F = K^{G(K/F)}.$$

*Proof:* Let  $L$  be the fixed field of  $G = G(K/F)$ . Since every  $L$ -automorphism is also an  $F$ -automorphism we have  $F \subseteq L$  and  $G(K/L) \subseteq G$ . But by definition of fixed field, every element of  $G$  is an  $L$ -automorphism and so  $G = G(K/L)$ . Now  $|G| = [K : F]$  since  $K$  is a Galois extension of  $F$ . Now by the first of the above corollaries  $|G|$  divides  $[K : L]$ . Since  $F \subseteq L \subseteq K$  this implies  $[K : F] = [K : L]$  and so  $F = L$ .  $\square$

**Characterizing Galois extensions:** Next we combine this last corollary with the earlier proposition on orbits, but first a definition. An extension field  $F \subseteq K$  is a *normal extension* if every irreducible polynomial  $g(x) \in F[x]$  which has at least one root in  $K$  splits into linear factors in  $K[x]$ .

**Corollary 13** *Let  $F \subseteq K$  be a Galois extension and let  $g(x)$  be a monic irreducible polynomial in  $F[x]$ . If  $g(x)$  has one root in  $K$  then it factors into linear factors in  $K[x]$ . That is, Galois extensions are normal.*

*Proof:* By the previous corollary,  $F$  is the fixed field of  $G = G(K/F)$ . Let  $\beta$  be a root of  $g(x)$  in  $K$ . By the proposition on orbits the irreducible polynomial for  $\beta$  over  $F$  is  $(x - \beta_1) \cdots (x - \beta_m)$  where  $\{\beta_1, \dots, \beta_m\}$  is the  $G$ -orbit of  $\beta$ . Since  $g(x)$  is the monic irreducible polynomial for  $\beta$  it is equal to this product and so splits into linear factors in  $K$  as required.  $\square$

**Proposition 14** *A finite normal extension  $F \subseteq K$  is the splitting field of some suitable polynomial  $f(x) \in F[x]$ .*

*Proof:* Take any finite set of generators for  $K$  over  $F$  and let  $f(x)$  be the product of their monic irreducible polynomials. Then, by definition of a normal extension,  $f(x)$  splits completely into linear factors in  $K$  and so  $K$  is a splitting field for  $f(x)$ .  $\square$

In view of the following important result the Galois group  $G(K/F)$  of an extension is often referred to as the *Galois group of the polynomial  $f(x)$*  for which  $K$  is the splitting field over  $F$ .

**Theorem 15 (Characterization of Galois extensions)** *Let  $F \subseteq K$  be a finite extension field. Then the following are equivalent.*

1.  $K$  is a Galois extension of  $F$ .
2.  $K$  is a normal extension of  $F$ .
3.  $K$  is the splitting field of some polynomial  $f(x) \in F[x]$ .

*Proof:* The previous corollary asserts that (1) implies (2), and the previous proposition says that (2) implies (3). That (3) implies (1) is our earlier Corollary 5  $\square$

**Corollary 16** *If  $K$  is a Galois extension of  $F$  and if  $L$  is an intermediate field  $F \subseteq L \subseteq K$ , then  $K$  is also a Galois extension of  $L$ .*

*Proof:* Since  $K$  is a Galois extension, by the characterization theorem it is a splitting field for a polynomial  $f(x) \in F[x]$ . But then  $K$  is also a splitting field for the polynomial  $f(x) \in L[x]$ . Hence  $K$  is a Galois extension of  $L$ .  $\square$

The following collects together a number of results we have proved.

**Corollary 17** *Let  $F \subseteq K$  be a finite extension field. Then the following are equivalent:*

1.  $K$  is a Galois extension of  $F$ .
2.  $K$  is the splitting field of an irreducible polynomial  $f(x) \in F[x]$ .
3.  $K$  is the splitting field of a polynomial  $f(x) \in F[x]$ .
4.  $F$  is the fixed field for the action of the Galois group  $G(K/F)$  on  $K$ .
5.  $F$  is the fixed field for the action of a finite group of automorphisms on  $K$ .  $\square$

Finally we are in a position to finish our task.

**Proof of the Main Theorem:** We observe that, in view of Corollary 16, the earlier Corollaries 11 and 12 show that the functions  $H \rightsquigarrow K^H$  and  $L \rightsquigarrow G(K/L)$  in the Main Theorem are mutually inverse and hence bijective. Also by Corollary 16 we have  $[K : L] = |G(K/L)|$  and thus  $[L : F] = [G : H]$ . So only the assertions in the Main Theorem concerning normal subgroups remain to be proved.

Now let  $L$  be an intermediate field and let  $H = G(K/L)$  be the corresponding subgroup of  $G = G(K/F)$ . Let  $\sigma$  be an element of  $G$ . Then  $\sigma L$  is another intermediate field and if  $\tau \in H = G(K/L)$  then  $\sigma\tau\sigma^{-1}$  fixes  $\sigma L$  and so  $\sigma\tau\sigma^{-1} \in G(K/\sigma L)$ . By symmetry it follows that  $G(K/\sigma L) = \sigma H\sigma^{-1}$ . (This is actually a general property of groups acting on sets.)

Suppose that  $H$  is normal in  $G$ . Then  $H = \sigma H\sigma^{-1}$  for all  $\sigma \in G$ . Thus  $G(K/L) = G(K/\sigma L)$  and so  $L = \sigma L$ . Thus every  $F$ -automorphism of  $K$  carries  $L$  into itself and hence by restriction defines an  $F$ -automorphism of  $L$ . Thus restriction defines a homomorphism  $\psi : G \rightarrow G(L/F)$ . Its kernel is the set of  $\sigma \in G$  which restrict to the identity on  $L$  and so  $\ker \psi = H$ . So  $G/H$  is isomorphic to a subgroup of  $G(L/F)$ . But  $[L : F] = [G : H] = |G/H| \leq |G(L/F)|$ . It follows that  $F \subseteq L$  is a Galois extension and that  $G/H \cong G(L/F)$ .

Conversely suppose that  $F \subseteq L$  is a Galois extension. Then  $L$  is the splitting field of some polynomial  $f(x) \in F[x]$ . An  $F$ -automorphism  $\sigma$  of  $K$  permutes the roots of  $f(x)$  and therefore carries  $L$  into itself, that is,  $L = \sigma L$ . Hence  $H = \sigma H\sigma^{-1}$  by the above property of actions. Thus  $H$  is normal in  $G$ . This completes the proof of the Main Theorem.  $\square$

**Example 1:** Let  $K$  be the splitting field of the polynomial  $f(x) = x^3 - 5$  which is irreducible over  $\mathbb{Q}$ . Over  $K$  the polynomial  $f(x)$  splits as

$$f(x) = (x - \sqrt[3]{5})(x - \omega\sqrt[3]{5})(x - \omega^2\sqrt[3]{5})$$

where  $\omega = e^{2\pi i/3}$ . The subfield  $L = \mathbb{Q}(\sqrt[3]{5})$  is contained in the reals  $\mathbb{R}$  and so  $\omega \notin L$  and  $\mathbb{Q} \subset L \subset K$  is a tower of proper extensions with  $K = \mathbb{Q}(\sqrt[3]{5}, \omega) = L(\omega)$ . A basis for  $L$  over  $\mathbb{Q}$  is  $\{1, \sqrt[3]{5}, \sqrt[3]{5}^2\}$ . A basis for  $K$  over  $L$  is  $\{1, \omega\}$  and so a basis for  $k$  over  $\mathbb{Q}$  is

$$\{1, \sqrt[3]{5}, \sqrt[3]{5}^2, \omega, \omega\sqrt[3]{5}, \omega\sqrt[3]{5}^2\}.$$

The Galois group is the full symmetric group  $S_3$  on the three roots. It is generated by the two automorphisms  $\sigma$  and  $\tau$  having orders 2 and 3 respectively defined by

$$\sigma(\sqrt[3]{5}) = \sqrt[3]{5}, \quad \sigma(\omega\sqrt[3]{5}) = \omega^2\sqrt[3]{5}, \quad \sigma(\omega^2\sqrt[3]{5}) = \omega\sqrt[3]{5}$$

and

$$\tau(\sqrt[3]{5}) = \omega\sqrt[3]{5}, \quad \tau(\omega\sqrt[3]{5}) = \omega^2\sqrt[3]{5}, \quad \tau(\omega^2\sqrt[3]{5}) = \sqrt[3]{5}.$$

Note that  $\sigma(\omega) = \omega^2 = \bar{\omega}$ ,  $\sigma(\sqrt[3]{5}) = \sqrt[3]{5}$  and  $\tau(\omega) = \omega$ .

$L$  is the fixed field of the subgroup  $\{1, \sigma\}$  of  $G$  which is not normal in  $G$ , and so  $L/\mathbb{Q}$  is not a Galois extension. Indeed  $G(L/\mathbb{Q}) \cong 1$ . It follows that  $L$  is not the splitting field of any polynomial over  $\mathbb{Q}$ .

The correspondence between subgroups and fixed field (Galois correspondence) is as follows:

subgroup	fixed field
$\{1\}$	$K$
$\{1, \sigma\}$	$\mathbb{Q}(5^{\frac{1}{3}})$
$\{1, \sigma\tau\}$	$\mathbb{Q}(\omega^2 5^{\frac{1}{3}})$
$\{1, \sigma\tau^2\}$	$\mathbb{Q}(\omega 5^{\frac{1}{3}})$
$\{1, \tau, \tau^2\}$	$\mathbb{Q}(\omega)$
$G$	$\mathbb{Q}$

Observe that the subgroup  $\{1, \tau, \tau^2\}$  is normal in  $G$  and that  $\mathbb{Q}(\omega)$  is a Galois extension of  $\mathbb{Q}$ . Also note that  $G(\mathbb{Q}(\omega)/\mathbb{Q})$  is cyclic of order 2 and is generated by the restriction of  $\sigma$ .

Let  $\gamma = \omega + 5^{\frac{1}{3}}$ . We claim that  $\gamma$  is a primitive element for  $K$  over  $\mathbb{Q}$ , that is,  $K = \mathbb{Q}(\gamma)$ . To see this we apply each of the elements of  $G$  to  $\gamma$  to compute its orbit under the action of  $G$ :

$$\begin{aligned}
1(\gamma) &= \gamma = \omega + 5^{\frac{1}{3}} \\
\tau(\gamma) &= \omega + \omega 5^{\frac{1}{3}} \\
\tau^2(\gamma) &= \omega + \omega^2 5^{\frac{1}{3}} \\
\sigma(\gamma) &= \omega^2 + 5^{\frac{1}{3}} \\
\sigma\tau(\gamma) &= \omega^2 + \omega^2 5^{\frac{1}{3}} \\
\sigma\tau^2(\gamma) &= \omega^2 + \omega 5^{\frac{1}{3}}
\end{aligned}$$

The results are 6 distinct elements of  $K$  and hence the orbit has size 6 which is the degree of the minimum polynomial for  $\gamma$ . Since  $K$  has dimension 6 over  $\mathbb{Q}$  it follows that  $K = \mathbb{Q}(\gamma)$  and  $\gamma$  is primitive.

**Example 2:** Let  $K$  be the splitting field over  $\mathbb{Q}$  of the polynomial  $x^4 - x^2 - 2$ . Over the field  $\mathbb{C}$ ,

$$\begin{aligned}
f(x) &= x^4 - x^2 - 2 = (x^2 + 1)(x^2 - 2) \\
&= (x - i)(x + i)(x - \sqrt{2})(x + \sqrt{2}).
\end{aligned}$$

Thus  $K = \mathbb{Q}(i, \sqrt{2})$  which is a biquadratic extension of  $\mathbb{Q}$ . The Galois group  $G = G(K/\mathbb{Q})$  is the Klein four group, generated by two elements  $\sigma, \tau$  of order 2 defined by  $\sigma(i) = -i, \sigma(\sqrt{2}) = \sqrt{2}$  and  $\tau(i) = i, \tau(\sqrt{2}) = -\sqrt{2}$ . The correspondence between subgroups and fixed field (Galois correspondence) is as follows:

subgroup	fixed field
$\{1\}$	$K$
$\{1, \sigma\}$	$\mathbb{Q}(\sqrt{2})$
$\{1, \tau\}$	$\mathbb{Q}(i)$
$\{1, \sigma\tau\}$	$\mathbb{Q}(i\sqrt{2})$
$G$	$\mathbb{Q}$

One can easily check that  $i + \sqrt{2}$  is a primitive element for  $K$  over  $\mathbb{Q}$ .