Chapter 6

Galois Groups and the Fundamental Theorem of Galois Theory

We now turn to the key idea of Galois Theory, namely that to every extension K of a field F we can associate a group, the Galois group of K over F, and that properties of the field extension are expressed within the structure of the group. This latter fact is encoded within the Fundamental Theorem of Galois Theory and we prove this theorem, the main result of the course, in this chapter.

Galois groups

The primary object that we are interested in when studying Galois theory is the following:

Definition 6.1 Let K be an extension of the field F. The *Galois group* $\mathrm{Gal}(K/F)$ of K over F is the set of all F-automorphisms of K with binary operation being composition of automorphisms.

Recall that an F-automorphism of K is an isomorphism $\phi\colon K \to K$ such that $a\phi = a$ for all $a \in F$. Certainly the identity map is an F-automorphism, while if ϕ and ψ are F-automorphisms of K then so are the composite $\phi\psi$ and the inverse ϕ^{-1}. Of course, composition of maps is an associative binary operation and we can therefore conclude that the Galois group $\mathrm{Gal}(K/F)$ is indeed a group.

Example 6.2 Recall from Example 3.10 that there are precisely two $\mathbb{Q}$-automorphisms of $\mathbb{Q}(i)$, namely those given, respectively, by

$$a + bi \mapsto a + bi \qquad \text{and} \qquad a + bi \mapsto a - bi$$

for $a, b \in \mathbb{Q}$; that is, a $\mathbb{Q}$-automorphism is determined by to which of the two roots of $X^2 + 1$ it maps i. Hence $|\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})| = 2$; that is, $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \cong C_2$.

We shall observe in our main theorem that it is no coincidence that this group order equals the degree $|\mathbb{Q}(i) : \mathbb{Q}|$ of the extension.

The sets $\mathscr{F}$ and $\mathscr{G}$

Definition 6.3 Let K be an extension of the field F and let $G = \mathrm{Gal}(K/F)$ be the Galois group of K over F.

(i) Define $\mathscr{G}$ to be the set of subgroups of G.

(ii) Define $\mathscr{F}$ to be the set of *intermediate fields*; that is,

$$\mathscr{F} = \{\, L \mid L \text{ is a field with } F \subseteq L \subseteq K \,\}.$$

(iii) If $H \in \mathscr{G}$, define

$$H^* = \{\, x \in K \mid x\phi = x \text{ for all } \phi \in H \,\},$$

the set of points in K fixed by all F-automorphisms in H.

(iv) If $L \in \mathscr{F}$, define

$$L^* = \{\, \phi \in G \mid x\phi = x \text{ for all } x \in L \,\},$$

the set of all F-automorphisms that fix all points in L.

We shall show that (iii) and (iv) in this definition provide us with maps $^*\colon \mathscr{G} \to \mathscr{F}$ and $^*\colon \mathscr{F} \to \mathscr{G}$ and then investigate properties of these maps.

Comment: Stewart's book denotes the above maps by † and * to distinguish between them. I choose to follow the notation in Cohn's chapter on field theory, namely to denote both maps by the same symbol. My reason for this is that it is usually clear which one we are actually using, some of the notation becomes a little more transparent (at least, in my opinion) and it certainly gives me one less thing of which to keep track.

Lemma 6.4 *Let K be an extension of the field F and $G = \mathrm{Gal}(K/F)$.*

(i) *If $H \in \mathscr{G}$, then $H^* \in \mathscr{F}$;*

(ii) *If $L \in \mathscr{F}$, then $L^* \in \mathscr{G}$;*

(iii) *If $H_1, H_2 \in \mathscr{G}$ with $H_1 \leqslant H_2$, then $H_1^* \supseteq H_2^*$;*

(iv) *If $L_1, L_2 \in \mathscr{F}$ with $L_1 \subseteq L_2$, then $L_1^* \geqslant L_2^*$.*

Thus our definitions of * provide us with maps $\mathscr{G} \to \mathscr{F}$ and $\mathscr{F} \to \mathscr{G}$ that *reverse inclusions.*

Proof: (i) All elements of the Galois group, by definition, fix all points in the base field F, so we certainly observe

$$F \subseteq H^* \subseteq K.$$

In particular, H^* is non-empty and contains non-zero elements since it contains the field F. Suppose $x, y \in H^*$. Then, since each $\phi \in H^*$ is a field isomorphism,

$$\begin{aligned}(x+y)\phi &= x\phi + y\phi = x + y\\ (xy)\phi &= (x\phi)(y\phi) = xy\\ (-x)\phi &= -(x\phi) = -x\\ (1/x)\phi &= 1/(x\phi) = 1/x\end{aligned}$$

for all $\phi \in H$ (and where $x \neq 0$ in the fourth equation). This shows that $x + y, xy, -x \in H^*$ and, if $x \neq 0$, $1/x \in H^*$. Hence H^* is closed under the field operations, so we conclude that H^* is indeed an intermediate field.

(ii) First note that the identity map certainly fixes all points in the intermediate field L, so L^* is non-empty. Let $\phi, \psi \in L^*$. Then

$$x(\phi\psi) = (x\phi)\psi = x\psi = x \qquad \text{for all } x \in L,$$

using the fact that $x\phi = x\psi = x$ for all $x \in L$, and hence $\phi\psi \in L^*$. Similarly

$$x = x\phi\phi^{-1} = (x\phi)\phi^{-1} = x\phi^{-1} \qquad \text{for all } x \in L,$$

so $\phi^{-1} \in L^*$. We conclude that L^* is a subgroup of G.

(iii) Suppose $H_1 \leqslant H_2$. If $x \in H_2^*$, then $x\phi = x$ for all $\phi \in H_2$, so $x\phi = x$ for all $\phi \in H_1$. Hence $x \in H_1^*$.

(iv) Suppose $L_1 \subseteq L_2$. If $\phi \in L_2^*$, then $x\phi = x$ for all $x \in L_2$, so $x\phi = x$ for all $x \in L_1$. Hence $\phi \in L_1^*$. □

The Fundamental Theorem of Galois Theory

In the Fundamental Theorem of Galois Theory, we shall actually observe that $^*\colon \mathscr{G} \to \mathscr{F}$ and $^*\colon \mathscr{F} \to \mathscr{G}$ are inverses of each other under sufficient assumptions concerning the field extension K of F. We shall define the term that encodes these conditions.

Definition 6.5 A finite extension of fields is called a *Galois extension* if it is normal and separable.

Lemma 6.6 *Let K be a finite Galois extension of a field F and L be an intermediate field ($F \subseteq L \subseteq K$). Then K is a Galois extension of L.*

PROOF: First K is a finite normal extension of F, so by Theorem 3.13, it is the splitting field of some polynomial $g(X) \in F[X]$. Now $g(X)$ can also be viewed as a polynomial over L and K is still the splitting field for $g(X)$ over L (it is obtained by adjoining the roots of $g(X)$ to the subfield L). Hence K is a finite normal extension of L.

Second K is a separable extension of F. If $\gamma \in K$, then the minimum polynomial $m(X)$ of γ over F has distinct roots in a splitting field (that is, distinct roots in K). Now the minimum polynomial $m'(X)$ of γ over L must divide $m(X)$ (by Lemma 2.11(iv)) and so $m'(X)$ also has distinct roots in K where it splits. It follows that K is also a separable extension of L.

Thus the extension K of L satisfies the two required conditions so is a Galois extension. □

Theorem 6.7 (Fundamental Theorem of Galois Theory) *Let K be a finite Galois extension of a field F and $G = \mathrm{Gal}(K/F)$. Then:*

(i) $|G| = |K : F|$.

(ii) *The maps $H \mapsto H^*$ and $L \mapsto L^*$ are mutual inverses and give a one-one inclusion-reversing correspondence between $\mathscr{G}$ and $\mathscr{F}$.*

(iii) *If L is an intermediate field, then*

$$|K : L| = |L^*| \qquad \text{and} \qquad |L : F| = |G|/|L^*|.$$

(iv) *An intermediate field L is a normal extension of F if and only if L^* is a normal subgroup of G. Moreover, in this situation,*

$$\mathrm{Gal}(L/F) \cong G/L^*.$$

PROOF: (i) Let $n = |K : F|$. Since K is a finite separable extension of F, use the Theorem of the Primitive Element (Theorem 4.11), or Corollary 5.9 when F is a finite field, to write

$$K = F(\alpha)$$

for some $\alpha \in K$. Let $f(X)$ be the minimum polynomial of α over F. Then

$$\deg f(X) = |F(\alpha) : F| = n.$$

Note that the elements of $F(\alpha)$ are linear combinations of powers of α,

$$x = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1},$$

with $a_0, a_1, \ldots, a_{n-1} \in F$, and the effect of applying any F-automorphism $\phi \in G$ is then determined by the value of $\alpha\phi$:

$$\begin{aligned} x\phi &= (a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1})\phi \\ &= a_0 + a_1(\alpha\phi) + a_2(\alpha\phi)^2 + \cdots + a_{n-1}(\alpha\phi)^{n-1}. \end{aligned}$$

Furthermore, if we apply ϕ to the equation $f(\alpha) = 0$ we obtain

$$f(\alpha\phi) = 0,$$

so $\alpha\phi$ must be one of the roots of $f(X)$. Since $f(X)$ has degree n, we conclude that there are at most n F-automorphisms of K; that is,

$$|G| \leqslant n.$$

Finally, recall that since K is a separable extension of F, the minimum polynomial $f(X)$ of α has distinct roots in its splitting field. It splits over K, because $f(X)$ is irreducible over F, has at least one root in K and K is a normal extension of F. We conclude that $f(X)$ has n distinct roots in K. Let β be any root of $f(X)$ in K. Now

$$|F(\beta) : F| = \deg f(X) = |F(\alpha) : F| = |K : F|,$$

by Theorem 2.14, so $F(\beta) = K = F(\alpha)$. We now apply Lemma 3.5 to conclude there is an isomorphism $\psi\colon F(\alpha) \to F(\beta)$ such that ψ extends the identity map $F \to F$ and satisfies $\alpha\psi = \beta$. Hence there is an F-automorphism $\psi \in G$ which maps α to β. This establishes the reverse inequality, there are at least n F-automorphisms in G, and we have established part (i) of the Fundamental Theorem:

$$|G| = n = |K : F|.$$

(iii) We can deduce the third part of the Fundamental Theorem from (i). Let L be an intermediate field: $F \subseteq L \subseteq K$. Then, by definition,

$$\begin{aligned} L^* &= \{\, \phi \in G \mid x\phi = x \text{ for all } x \in L \,\} \\ &= \mathrm{Gal}(K/L), \end{aligned}$$

since L^* consists of all automorphisms of K that fix all points of L. By Lemma 6.6, K is a finite Galois extension of L, so we can apply part (i) to conclude

$$|L^*| = |\mathrm{Gal}(K/L)| = |K : L|.$$

Finally, we complete the proof of (iii) by use of the Tower Law (Theorem 2.4):

$$|L : F| = \frac{|K : F|}{|K : L|} = \frac{|G|}{|L^*|}.$$

(ii) We have observed that for an intermediate field $L \in \mathscr{F}$,

$$L^* = \{\, \phi \in G \mid x\phi = x \text{ for all } x \in L \,\} = \mathrm{Gal}(K/L),$$

while, by definition, for a subgroup $H \in \mathscr{G}$,

$$H^* = \{\, x \in K \mid x\phi = x \text{ for all } \phi \in H \,\} = \mathrm{Fix}_K(H),$$

the set of points of K fixed by the maps in H. Lemma 6.4 tells us that

$$L^* \in \mathscr{G}, \qquad H^* \in \mathscr{F}$$

and that the $*$-operations reverse inclusions. To complete the proof of (ii), namely to show these operations are each other's inverses, we must prove that

$$\begin{aligned} H^{**} &= H && \text{for all } H \in \mathscr{G} \\ L^{**} &= L && \text{for all } L \in \mathscr{F}. \end{aligned}$$

This will require us to make use of two further lemmas.

Lemma 6.8 *Let K be a finite Galois extension of a field F and $G = \mathrm{Gal}(K/F)$. The fixed field of G,*

$$G^* = \mathrm{Fix}_K(G) = \{\, x \in K \mid x\phi = x \text{ for all } \phi \in G \,\},$$

is precisely the base field of F.

PROOF: Let us write $F_1 = G^*$. It follows from Lemma 6.4(i) that F_1 is some intermediate field: $F \subseteq F_1 \subseteq K$.

Let us apply the Theorem of the Primitive Element (Theorem 4.11, or use Corollary 5.9 if F is finite) to observe $K = F(\alpha)$ for some $\alpha \in K$. Let $f(X)$ be the minimum polynomial of α over F and let $g(X)$ be the minimum polynomial of α over F_1. Since $f(X)$ is a polynomial with coefficients from F_1 (as $F \subseteq F_1$) with $f(\alpha) = 0$, we conclude that $g(X)$ divides $f(X)$.

Now $f(X)$ is an irreducible polynomial over F with the root α in the normal separable extension K. Hence $f(X)$ splits over K and the roots of $f(X)$ in K are distinct. Let β be one of these roots of $f(X)$ in K. In the proof of part (i) of the Fundamental Theorem of Galois Theory, we observed there is an element $\psi \in G$ mapping α to β. Apply ψ to the equation

$$g(\alpha) = 0.$$

The coefficients of $g(X)$ are elements of F_1, so they are fixed by ψ (by definition of F_1). Hence, upon applying ψ, we conclude

$$g(\beta) = g(\alpha\psi) = \big(g(\alpha)\big)\psi = 0.$$

Hence each of the roots of $f(X)$ are also roots of $g(X)$. As these roots are distinct, we conclude that $g(X)$ is not a proper divisor of $f(X)$ but must satisfy

$$g(X) = f(X).$$

In particular, these polynomials have the same degree. Thus

$$\begin{aligned} |K : F_1| = |F_1(\alpha) : F_1| &= \deg g(X) \\ &= \deg f(X) = |F(\alpha) : F| = |K : F| = |K : F_1| \cdot |F_1 : F| \end{aligned}$$

Hence $|F_1 : F| = 1$ and $F_1 = F$, as required. □

Lemma 6.9 *Let K be a finite separable extension of a field F and let H be a finite group of F-automorphisms of K (that is, H is some subgroup of $\mathrm{Gal}(K/F)$). Then*

$$|K : H^*| = |H|$$

(where $H^* = \mathrm{Fix}_K(H)$).

PROOF: Write $L = H^*$. By the Theorem of the Primitive Element (Theorem 4.11, or Corollary 5.9 if F is finite), write $K = F(\alpha)$ for some $\alpha \in K$. Put

$$g(X) = \prod_{\phi \in H} (X - \alpha\phi),$$

which is some polynomial with coefficients from K; that is, $g(X) \in K[X]$. If $\psi \in H$, write $\bar{\psi}$ for the automorphism of the ring $K[X]$ obtained by applying ψ to the coefficients of polynomials. If we apply $\bar{\psi}$ to one of the linear factors $X - \alpha\phi$ of $g(X)$, we produce $X - \alpha\phi\psi$, which is again one of the linear factors of $g(X)$ since the product $\phi\psi$ is again an element of the group H. Indeed, the map $\phi \mapsto \phi\psi$ is a bijection $H \to H$ and so $\bar{\psi}$ permutes the linear factors of $g(X)$; that is,

$$g(X)\bar{\psi} = \prod_{\phi \in H} (X - \alpha\phi\psi) = g(X)$$

for all $\psi \in H$. Thus the coefficients appearing in $h(X)$ are fixed by all elements of H; that is, these coefficients belong to $\mathrm{Fix}_K(H) = H^* = L$ and we conclude that

$$g(X) \in L[X].$$

The definition of $g(X)$ says that it splits in K and, since $K = F(\alpha)$, we certainly build K by adjoining the roots of K to the subfield L. Thus K is the splitting field of $g(X)$ over L and hence, by Theorem 3.13, K is a normal extension of L.

The field K is also a separable extension of L, since K is a separable extension of F. (This is essentially observed in the second half of the proof of Lemma 6.6; also see Question 3(b) on Problem Sheet IV.) In conclusion, K is a finite Galois extension of L and we can apply part (i) of the Fundamental Theorem of Galois Theory to conclude

$$|K : L| = |\mathrm{Gal}(K/L)| \geqslant |H|.$$

(Note every element of H is an L-automorphism of K, so H is a subgroup of $\mathrm{Gal}(K/L)$.)

On the other hand, $\deg g(X) = |H|$, so the degree of the minimum polynomial of α over L is at most $|H|$. Hence

$$|K : L| = |L(\alpha) : L| \leqslant |H|.$$

We have therefore shown

$$|K : H^*| = |K : L| = |H|,$$

as required. □

We now return to the proof of part (ii) of the Fundamental Theorem of Galois Theory. Let $L \in \mathscr{F}$. It follows from Lemma 6.6 that K is also a Galois extension of L. We have observed $L^* = \mathrm{Gal}(K/L)$ in part (iii). Now

$$L^{**} = \mathrm{Fix}_K(L^*) = L,$$

by Lemma 6.8 applied to the extension K of L.

Now let $H \in \mathscr{G}$. Let $H_1 = H^{**}$. Certainly H fixes all the points in H^* (by definition of H^*), so $H \leqslant H_1$. Take $L = H^*$ in the previous step to conclude

$$H_1^* = H^{***} = (H^*)^{**} = H^*.$$

Now by Lemma 6.9 applied twice to the subgroups H and H_1,

$$|K : H^*| = |H| \qquad \text{and} \qquad |K : H_1^*| = |H_1|,$$

so we conclude $|H| = |H_1|$. It follows that

$$H = H_1 = H^{**},$$

as required. The completes the proof of part (ii) of the Fundamental Theorem of Galois Theory.

(iv) We turn to the last part of the Fundamental Theorem. Let $L \in \mathscr{F}$ and consider what it means for L^* to be a normal subgroup of G. Observe

$$\begin{aligned}
L^* \trianglelefteqslant G \quad & \text{if and only if} \quad \phi\theta\phi^{-1} \in L^* \quad \text{for } \theta \in L^*,\ \phi \in G \\
& \text{if and only if} \quad x(\phi\theta\phi^{-1}) = x \quad \text{for } x \in L,\ \theta \in L^*,\ \phi \in G \\
& \text{if and only if} \quad x\phi\theta = x\phi \quad \text{for } x \in L,\ \theta \in L^*,\ \phi \in G \\
& \text{if and only if} \quad x\phi \in L^{**} \quad \text{for } x \in L,\ \phi \in G \\
& \text{if and only if} \quad x\phi \in L \quad \text{for } x \in L,\ \phi \in G,
\end{aligned}$$

using part (ii). Hence

$$L^* \trianglelefteqslant G \qquad \text{if and only if} \qquad L\phi \subseteq L \quad \text{for all } \phi \in G.$$

Now suppose $L\phi \subseteq L$ for all $\phi \in G$. Let $g(X)$ be an irreducible polynomial over F and suppose that $g(X)$ has some root β which lies in L. Put

$$h(X) = \prod_{\phi \in G} (X - \beta\phi).$$

If $\psi \in G$, the induced automorphism $\bar{\psi}$ of $K[X]$ permutes the linear factors of $h(X)$ when we apply it, so $\bar{\psi}$ fixes the coefficients of $h(X)$; that is, $h(X)$ is actually a polynomial with coefficients in $G^* = \mathrm{Fix}_K(G) = F$ (using Lemma 6.8). Since β is a root of $h(X)$ by construction, the minimum polynomial of β (that is, a scalar multiple of our irreducible polynomial $g(X)$) divides $h(X)$, so we conclude $g(X)$ divides $h(X)$. By assumption, $L\phi \subseteq L$ for all $\phi \in G$, and hence all the roots of $h(X)$ belong to L. Since $g(X)$ divides $h(X)$, we conclude that $g(X)$ splits in L. We have shown that if $L\phi \subseteq L$ for all $\phi \in G$, then L is a normal extension of F.

Conversely, suppose L is a normal extension of F. Let $\alpha \in L$ and $\phi \in G$. Let $f(X)$ be the minimum polynomial of α over F. Now $f(\alpha) = 0$, so applying ϕ, we conclude $f(\alpha\phi) = 0$. Thus $\alpha\phi$ is a root of $f(X)$. However, since L is a normal extension of F, all the roots of $f(X)$ belong to L. We thus conclude $\alpha\phi \in L$. It follows that if L is a normal extension of F then $L\phi \subseteq L$ for all $\phi \in G$.

We have then proved the following lemma which will be key in establishing part (iv) of the Fundamental Theorem:

Lemma 6.10 *Let K be a finite Galois extension of a field F and $G = \mathrm{Gal}(K/F)$. The following conditions on an intermediate field L are equivalent:*

(i) *L^* is a normal subgroup of G;*

(ii) *$L\phi \subseteq L$ for all $\phi \in G$;*

(iii) *L is a normal extension of F.* □

The equivalence of (i) and (iii) in the lemma establish the first step of part (iv) of the Fundamental Theorem. Finally, let us assume L is a normal extension of F. First this means that L is a Galois extenson of F (since L inherits separability from the bigger field K). The lemma also tells us that $L^* \trianglelefteqslant G$ and $L\phi \subseteq L$ for all $\phi \in G$. Hence each F-automorphism ϕ of K induces a F-automorphism $\phi|_L$ of L. (The restriction is certainly a map $\phi|_L \colon L \to L$ that preserves the field operations, while it is an automorphism since $\phi^{-1}|_L$ is the inverse.) Hence we can define a map $\Phi \colon G \to \mathrm{Gal}(L/F)$ by

$$\phi \mapsto \phi|_L.$$

Now

$$\ker \Phi = \{\, \phi \in G \mid x\phi = x \text{ for all } x \in L \,\} = L^*,$$

by definition, so

$$\begin{aligned}
|\mathrm{im}\,\Phi| &= \frac{|G|}{|L^*|} && \text{(by the First Isomorphism Theorem)} \\
&= \frac{|K:F|}{|K:L|} && \text{(by parts (i) and (iii))} \\
&= |L:F| && \text{(by the Tower Law)} \\
&= |\mathrm{Gal}(L/F)| && \text{(by (i) applied to the Galois extension } L \text{ of } F).
\end{aligned}$$

Hence Φ is surjective and so, by the First Isomorphism Theorem,

$$\mathrm{Gal}(L/F) \cong G/L^*.$$

This completes the proof of the Fundamental Theorem of Galois Theory. □

In light of the fact that we have established part (ii) of the Fundamental Theorem, we can make the following definition.

Definition 6.11 When K is a finite Galois extension of the field F, the maps $H \mapsto H^*$ and $L \mapsto L^*$ are called the *Galois correspondence* between the set $\mathscr{G}$ of subgroups of the Galois group and the set $\mathscr{F}$ of intermediate fields.

Examples of Galois groups

Let us now turn to illustrating the use of the Fundamental Theorem of Galois Theory and the calculation of Galois groups. We make a further definition of what we mean by a Galois group.

Definition 6.12 Let $f(X)$ be a polynomial over a field F. The *Galois group* $\mathrm{Gal}(f(X))$ of $f(X)$ is the Galois group $\mathrm{Gal}(K/F)$ of the splitting field K of $f(X)$ over F.

If F is a field of characteristic zero, then the splitting field K of a polynomial $f(X)$ over F is a normal extension, by Theorem 3.13, and is separable by Corollary 4.9. Hence we may apply the Fundamental Theorem of Galois Theory in such a situation.

Example 6.13 Let $f(X) = X^4 - 2$ over $\mathbb{Q}$. The roots of this polynomial in $\mathbb{C}$ are

$$\sqrt[4]{2}, \quad -\sqrt[4]{2}, \quad i\sqrt[4]{2}, \quad -i\sqrt[4]{2}.$$

Hence the splitting field of $f(X)$ over $\mathbb{Q}$ is

$$K = \mathbb{Q}(\sqrt[4]{2}, i).$$

Now $f(X)$ is the minimum polynomial of $\sqrt[4]{2}$ over $\mathbb{Q}$ (since it is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion), so

$$|\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}| = \deg f(X) = 4.$$

As $\mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$, the minimum polynomial of i over $\mathbb{Q}(\sqrt[4]{2})$ is $X^2 + 1$ (the latter cannot factorize into linear polynomials over a subfield of $\mathbb{R}$). Hence

$$|\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})| = 2.$$

Hence, by the Tower Law,

$$|K : \mathbb{Q}| = |K : \mathbb{Q}(\sqrt[4]{2})| \cdot |\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}| = 8.$$

Part (i) of the Fundamental Theorem of Galois Theory tells us that

$$|\mathrm{Gal}(K/\mathbb{Q})| = 8.$$

On the other hand, any $\mathbb{Q}$-automorphism of K is determined by its effect on $\sqrt[4]{2}$ and i, but must map $\sqrt[4]{2}$ to one of the four roots of $f(X)$ and must map i to $\pm i$. These choices would

give us at most eight $\mathbb{Q}$-automorphisms, so they must all *be* $\mathbb{Q}$-automorphisms of K. Hence the members of $\mathrm{Gal}(K/\mathbb{Q})$ are as follows:

$$\begin{array}{rll}
\sigma\colon & \sqrt[4]{2} \mapsto i\sqrt[4]{2}, & i \mapsto i \\
\sigma^2\colon & \sqrt[4]{2} \mapsto -\sqrt[4]{2}, & i \mapsto i \\
\sigma^3\colon & \sqrt[4]{2} \mapsto -i\sqrt[4]{2}, & i \mapsto i \\
\mathrm{id}\colon & \sqrt[4]{2} \mapsto \sqrt[4]{2}, & i \mapsto i \\
\tau\colon & \sqrt[4]{2} \mapsto \sqrt[4]{2}, & i \mapsto -i \\
\sigma\tau\colon & \sqrt[4]{2} \mapsto -i\sqrt[4]{2}, & i \mapsto -i \\
\sigma^2\tau\colon & \sqrt[4]{2} \mapsto -\sqrt[4]{2}, & i \mapsto -i \\
\sigma^3\tau\colon & \sqrt[4]{2} \mapsto i\sqrt[4]{2}, & i \mapsto -i
\end{array}$$

The formulae for these automorphisms are calculated as follows. Write σ and τ for the maps labelled as such above. Then

$$(\sqrt[4]{2})\sigma^2 = (i\sqrt[4]{2})\sigma = (i\sigma)(\sqrt[4]{2}\sigma) = i \cdot i\sqrt[4]{2} = -\sqrt[4]{2}$$

and

$$i\sigma^2 = i$$

since $i\sigma = i$. Hence, if the first map is σ, the second map is indeed σ^2. Similar calculations apply for the other $\mathbb{Q}$-automorphisms.

Our conclusion is that $\mathrm{Gal}(K/\mathbb{Q})$ is a group of order 8 possessing an element σ of order 4 and an element τ of order 2. We also calculate that

$$\tau^{-1}\sigma\tau\colon \sqrt[4]{2} \mapsto -i\sqrt[4]{2}, \quad i \mapsto i,$$

so

$$\tau^{-1}\sigma\tau = \sigma^3 = \sigma^{-1}.$$

Hence

$$\mathrm{Gal}(K/\mathbb{Q}) \cong D_8,$$

the dihedral group of order 8.

The Galois correspondence is a one-one inclusion-reversing correspondence between the subgroups of D_8 and the intermediate fields between $\mathbb{Q}$ and K.

For example, $\langle\sigma\rangle$ is a subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ of order 4, so $\langle\sigma\rangle^*$ is an intermediate field such that $|K : \langle\sigma\rangle^*| = 4$ (take $L = \langle\sigma\rangle^*$ in part (iii) of the Fundamental Theorem of Galois Theory); that is,

$$|\langle\sigma\rangle^* : \mathbb{Q}| = 2.$$

Note that i is certainly fixed by σ, so $i \in \langle\sigma\rangle^*$ and we conclude

$$\langle\sigma\rangle^* = \mathbb{Q}(i).$$

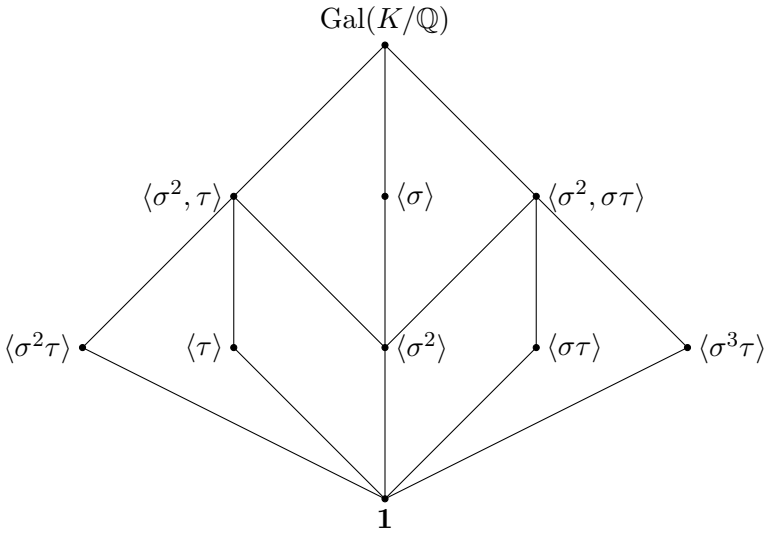
Furthermore, $\langle\sigma\rangle \trianglelefteq \mathrm{Gal}(K/\mathbb{Q})$, while $\mathbb{Q}(i)$ is the splitting field of $X^2 + 1$ over $\mathbb{Q}$, so is a normal extension of $\mathbb{Q}$ (consistent with part (iv) of the Fundamental Theorem of Galois Theory).

Similarly, $\langle\tau\rangle$ is a subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ of order 2, so $|\langle\tau\rangle^* : \mathbb{Q}| = 4$. Note that $\sqrt[4]{2} \in \langle\tau\rangle^*$, so

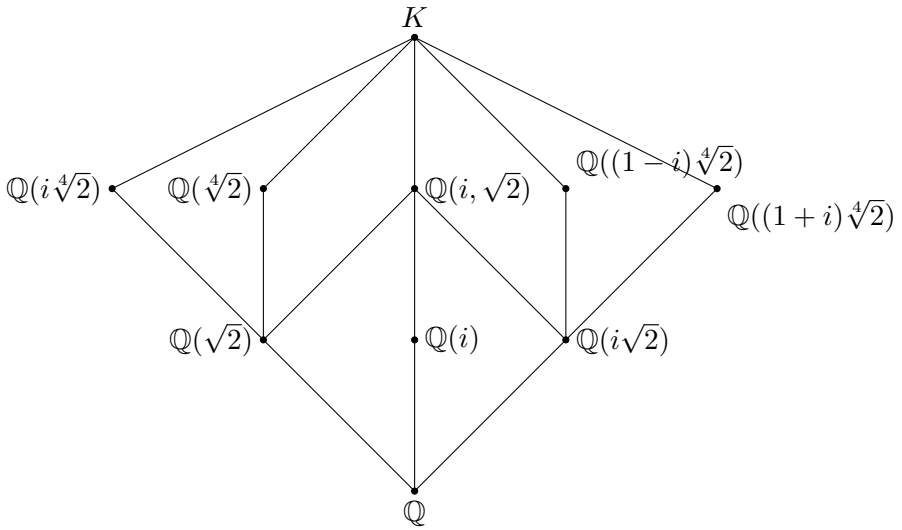
$$\langle\tau\rangle^* = \mathbb{Q}(\sqrt[4]{2}).$$

In this case, $\langle\tau\rangle$ is not a normal subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ and neither is $\mathbb{Q}(\sqrt[4]{2})$ a normal extension of $\mathbb{Q}$ (since the irreducible polynomial $X^4 - 2$ has a root in the field but does not split over $\mathbb{Q}(\sqrt[4]{2})$).

With further analysis, we can work out the subgroup lattice of $D_8 \cong \mathrm{Gal}(K/\mathbb{Q})$:



The corresponding lattice of intermediate fields is obtained by inverting the above diagram:



A general result which will help us calculate Galois groups is the following:

Lemma 6.14 *Let $f(X)$ be a polynomial over the field F, let K be the splitting field of $f(X)$ over F and let Ω be the set of roots of $f(X)$ in K. Then* Gal(K/F) *is isomorphic to the group of permutations that it induces on Ω.*

Since a polynomial of degree n has at most n roots in a splitting field, the above lemma has the following consequence as an immediate corollary.

Corollary 6.15 *Let $f(X)$ be a polynomial of degree n over a field F. The Galois group of $f(X)$ over F is isomorphic to a subgroup of the symmetric group S_n of degree n.* □

Proof of Lemma 6.14: Let $\Omega = \{\omega_1, \omega_2, \ldots, \omega_n\}$. Any F-automorphism ϕ of K fixes the coefficients of $f(X)$ and hence, upon applying ϕ to the equation $f(\omega_i) = 0$, we conclude that ϕ must map a root of $f(X)$ to another root. Since ϕ is bijective, we conclude that ϕ induces a permutation of Ω. Hence we have a map

$$\begin{aligned}\rho\colon G &\to \mathrm{Sym}(\Omega)\\ \phi &\mapsto \phi|_\Omega.\end{aligned}$$

Since the group operation in both groups is composition, it follows that ρ is a group homomomorphism. Let $\phi \in \ker \rho$. Then $\omega_i \phi = \omega_i$ for $i = 1, 2, \ldots, n$. However, $K = F(\omega_1, \omega_2, \ldots, \omega_n)$; that is, every element of K is a sum of products involving elements from F and powers of the ω^i, so ϕ must then act as the identity on K; that is, $\phi = 1$. Thus $\ker \rho = \mathbf{1}$, ρ is injective and

$$G \cong \operatorname{im} \rho,$$

which is a subgroup of the symmetric group $\mathrm{Sym}(\Omega)$. □

Example 6.16 (Cubic polynomials) If $f(X)$ is a polynomial of degree 3 over $\mathbb{Q}$, then the Galois group of $f(X)$ over $\mathbb{Q}$ is isomorphic to a subgroup of the symmetric group S_3 of degree 3. We shall show that all possibilities can occur.

(i) Take $f(X) = X^3$. Then $f(X)$ splits over $\mathbb{Q}$, so the splitting field is $K = \mathbb{Q}$ and the Galois group is trivial:

$$\mathrm{Gal}(K/\mathbb{Q}) = \mathbf{1}.$$

(ii) Take $f(X) = X^3 + X = X(X^2 + 1)$. The splitting field of $f(X)$ over $\mathbb{Q}$ is $K = \mathbb{Q}(i)$. The Fundamental Theorem of Galois Theory tells us that

$$|\mathrm{Gal}(K/\mathbb{Q})| = |\mathbb{Q}(i) : \mathbb{Q}| = 2,$$

so

$$\mathrm{Gal}(K/\mathbb{Q}) \cong C_2,$$

a cyclic group of order 2.

(iii) Take $f(X) = X^3 - 3X - 1$. Note

$$\begin{aligned} f(X+1) &= (X+1)^3 - 3(X+1) - 1 \\ &= X^3 + 3X^2 - 3, \end{aligned}$$

which is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion. Hence $f(X)$ is irreducible over $\mathbb{Q}$. To find the roots of the polynomial, recall the trigonometric formula

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta.$$

Now if $\alpha = 2\cos\theta$ for some θ, then

$$\alpha^3 - 3\alpha = 8\cos^3\theta - 6\cos\theta = 2\cos 3\theta.$$

Hence

$$f(\alpha) = 0 \qquad \text{if and only if} \qquad \cos 3\theta = \tfrac{1}{2}.$$

It follows that the three roots of $f(X)$ in $\mathbb{C}$ are

$$\alpha = 2\cos\tfrac{\pi}{9}, \qquad \beta = 2\cos\tfrac{7\pi}{9}, \qquad \gamma = 2\cos\tfrac{13\pi}{9}.$$

Now

$$\begin{aligned} \beta = 2\cos\tfrac{7\pi}{9} &= -2\cos\tfrac{2\pi}{9} \\ &= -2\left(2\cos^2\tfrac{\pi}{9} - 1\right) \\ &= 2 - \alpha^2, \end{aligned}$$

while $\alpha+\beta+\gamma=0$ (from the X^2 coefficient in $f(X)$). Hence $\gamma=\alpha^2-\alpha-2$. We conclude that the splitting field of X^3-3X-1 over $\mathbb{Q}$ is $K=\mathbb{Q}(\alpha)$. Then, by the Fundamental Theorem of Galois Theory,

$$|\mathrm{Gal}(K/\mathbb{Q})| = |K:\mathbb{Q}| = 3,$$

so

$$\mathrm{Gal}(K/\mathbb{Q}) \cong C_3,$$

a cyclic group of order 3.

(iv) Take $f(X)=X^3-2$. The splitting field of $f(X)$ over $\mathbb{Q}$ is $K=\mathbb{Q}(\sqrt[3]{2},\omega)$ where $\omega=\mathrm{e}^{2\pi i/3}$. Then

$$|K:\mathbb{Q}| = |\mathbb{Q}(\sqrt[3]{2},\omega):\mathbb{Q}(\sqrt[3]{2})|\cdot|\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}| = 6,$$

since the minimum polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $f(X)$ and the minimum polynomial of ω over $\mathbb{Q}(\sqrt[3]{2})$ is X^2+X+1. Hence, combining the Fundamental Theorem of Galois Theory with Corollary 6.15, we conclude that $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to a subgroup of order 6 inside the symmetric group S_3 of degree 3; that is,

$$\mathrm{Gal}(K/\mathbb{Q}) \cong S_3.$$

Galois groups of finite fields

We finish this chapter by considering the Galois group of a finite field $\mathbb{F}_{p^n}$ over its prime subfield $\mathbb{F}_p$. Recall that $\mathbb{F}_{p^n}$ occurs as the splitting field of the polynomial $f(X)=X^{p^n}-X$ over $\mathbb{F}_p$, so $\mathbb{F}_{p^n}$ is a normal extension of $\mathbb{F}_p$. Also if $\alpha\in\mathbb{F}_{p^n}$, then α is a root of $f(X)$, so the minimum polynomial of α divides $X^{p^n}-X$ and hence has distinct roots. Consequently, $\mathbb{F}_{p^n}$ is also a separable extension of $\mathbb{F}_p$. We conclude that $\mathbb{F}_{p^n}$ is a finite Galois extension of $\mathbb{F}_p$ and the Fundamental Theorem of Galois Theory applies. In particular, it tells us

$$|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = |\mathbb{F}_{p^n}:\mathbb{F}_p| = n.$$

We will construct the $\mathbb{F}_p$-automorphisms of $\mathbb{F}_{p^n}$ using the following:

Definition 6.17 The *Frobenius automorphism* γ of the finite field $\mathbb{F}_{p^n}$ of order p^n is the map $\gamma\colon\mathbb{F}_{p^n}\to\mathbb{F}_{p^n}$ given by

$$\gamma\colon a\mapsto a^p$$

for all $a\in\mathbb{F}_{p^n}$.

First note that

$$(ab)\gamma = (ab)^p = a^p\,b^p = (a\gamma)(b\gamma)$$

and, by "Freshman's Exponentiation",

$$(a+b)\gamma = (a+b)^p = a^p+b^p = a\gamma+b\gamma$$

for all $a,b\in\mathbb{F}_{p^n}$. Hence γ is a homomorphism $\mathbb{F}_{p^n}\to\mathbb{F}_{p^n}$. Note

$$a\in\ker\gamma \qquad \text{if and only if} \qquad a^p=0 \qquad \text{if and only if} \qquad a=0,$$

using the fact that a field has no zero divisors. This tells us $\ker\gamma=\mathbf{0}$ and therefore γ is an injective map. The fact that $\mathbb{F}_{p^n}$ is finite then tells us that γ is necessarily also surjective. In conclusion, γ is an automorphism of the finite field $\mathbb{F}_{p^n}$.

Furthermore, the multiplicative group $\mathbb{F}_p^*$ of the prime subfield $\mathbb{F}_p$ is cyclic of order $p-1$, so

$$a^{p-1} = 1 \qquad \text{for all } a \in \mathbb{F}_p \setminus \{0\}$$

and hence

$$a^p = a \qquad \text{for all } a \in \mathbb{F}_p;$$

that is,

$$a\gamma = a \qquad \text{for all } a \in \mathbb{F}_p.$$

In summary, we have established the following fact about the Frobenius automorphism:

Lemma 6.18 *The Frobenius automorphism γ of $\mathbb{F}_{p^n}$, given by $a\gamma = a^p$ for all $a \in \mathbb{F}_{p^n}$, is an $\mathbb{F}_p$-automorphism of $\mathbb{F}_{p^n}$ (that is, an element of the Galois group $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$).* □

Note further that, for any positive integer k,

$$a\gamma^k = a^{p^k} \qquad \text{for each } a \in \mathbb{F}_{p^n}.$$

We know that every element of $\mathbb{F}_{p^n}$ satisfies $a^{p^n} = a$; that is, $a\gamma^n = a$. Hence $\gamma^n = 1$, the identity element of the Galois group. Now suppose $\gamma^k = 1$ for some positive integer k; that is,

$$a^{p^k} = a \qquad \text{for all } a \in \mathbb{F}_{p^n}.$$

Thus every element of $\mathbb{F}_{p^n}$ is a root of the polynomial $X^{p^k} - X$. Since a polynomial cannot have more roots than its degree, we conclude that $k \geqslant n$.

Hence the smallest positive integer k such that $\gamma^k = 1$ is $k = n$; that is, the order of γ, as an element of the Galois group, is precisely n. It follows that $\langle\gamma\rangle$ is a subgroup of $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ of order n and since the Galois group has order n, we conclude

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle\gamma\rangle.$$

Thus we have established:

Theorem 6.19 *Let p be a prime number and n a positive integer. Then the Galois group $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ of the Galois field of order p^n over its prime subfield is cyclic of order n generated by the Frobenius automorphism γ.* □

Example 6.20 *Let α be a root of the irreducible polynomial $f(X) = X^3 + X + 1$ in some extension of the field $\mathbb{F}_2$. Express the roots of $f(X)$ in $\mathbb{F}_2(\alpha)$ in terms of the basis $\{1, \alpha, \alpha^2\}$.*

Solution: Note that $f(X)$ is indeed irreducible over $\mathbb{F}_2$, since $f(0) = f(1) = 1$, so $f(X)$ has no roots and hence no linear factors over $\mathbb{F}_2$. The simple extension $\mathbb{F}_2(\alpha)$ then has degree 3 over $\mathbb{F}_2$ and consequently $\{1, \alpha, \alpha^2\}$ is a basis for $\mathbb{F}_2(\alpha)$ over $\mathbb{F}_2$.

The field $\mathbb{F}_2(\alpha) \cong \mathbb{F}_8$, so the Galois group $\mathrm{Gal}(()\mathbb{F}_2(\alpha)/\mathbb{F}_2)$ is cyclic of order 3 generated by the Frobenius automorphism $\gamma\colon a \mapsto a^2$. The Galois group permutes the roots of the polynomial $f(X)$ and hence the roots of $f(X)$ are α, $\alpha^2 = \alpha\gamma$ and $\alpha^4 = \alpha\gamma^2$. Observe

$$\alpha^4 = \alpha \cdot \alpha^3 = \alpha(\alpha + 1) = \alpha^2 + \alpha.$$

Hence the roots of $X^3 + X + 1$ in $\mathbb{F}_2(\alpha)$ are α, α^2 and $\alpha^2 + \alpha$. □