c. If M is any intermediate field of a finite normal extension inside $\mathbb{C}$, then $M^{*\dagger} = M$.

d. If M is any intermediate field of a finite normal extension $L : K$ inside $\mathbb{C}$, then the Galois group of $M : K$ is a subgroup of the Galois group of $L : K$.

e. If M is any intermediate field of a finite normal extension $L : K$ inside $\mathbb{C}$, then the Galois group of $L : M$ is a quotient of the Galois group of $L : K$.

Chapter 13

A Worked Example

The Fundamental Theorem of Galois theory is quite a lot to take in at one go, so it is worth spending some time thinking it through. We, therefore, analyse how the Galois correspondence works out on an extended example.

The extension that we discuss is a favourite with writers on Galois theory, because of its archetypal quality. A simpler example would be too small to illustrate the theory adequately, and anything more complicated would be unwieldy. The example is the Galois group of the splitting field of $t^4 - 2$ over $\mathbb{Q}$.

The discussion is cut into small pieces to make it more easily digestible.

1. Let $f(t) = t^4 - 2$ over $\mathbb{Q}$, and let K be a splitting field for f such that $K \subseteq \mathbb{C}$. We can factorize f as follows:

$$f(t) = (t - \xi)(t + \xi)(t - i\xi)(t + i\xi)$$

where $\xi = \sqrt[4]{2}$ is real and positive. Therefore, $K = \mathbb{Q}(\xi, i)$. Since K is a splitting field, $K : \mathbb{Q}$ is finite and normal. We are working in $\mathbb{C}$, so separability is automatic.

2. We find the degree of $K : \mathbb{Q}$. By the tower law,

$$[K : \mathbb{Q}] = [\mathbb{Q}(\xi, i) : \mathbb{Q}(\xi)][\mathbb{Q}(\xi) : \mathbb{Q}]$$

The minimal polynomial of i over $\mathbb{Q}(\xi)$ is $t^2 + 1$, since $i^2 + 1 = 0$ but $i \notin \mathbb{R} \supseteq \mathbb{Q}(\xi)$. So $[\mathbb{Q}(\xi, i) : \mathbb{Q}(\xi)] = 2$.

Now ξ is a zero of f over $\mathbb{Q}$, and f is irreducible by Eisenstein's Criterion, Theorem 3.19. Hence f is the minimal polynomial of ξ over $\mathbb{Q}$, and $[\mathbb{Q}(\xi) : \mathbb{Q}] = 4$. Therefore,

$$[K : \mathbb{Q}] = 2.4 = 8$$

3. We shall find the elements of the Galois group of $K : \mathbb{Q}$. By a direct check, or by Corollary 5.13, there is a $\mathbb{Q}$-automorphism σ of K such that

$$\sigma(i) = i \qquad \sigma(\xi) = i\xi$$

and another, τ, such that

$$\tau(i) = -i \qquad \tau(\xi) = \xi$$

Products of these yield eight distinct $\mathbb{Q}$-automorphisms of K, as follows:

Automorphism	Effect on ξ	Effect on i
1	ξ	i
σ	$i\xi$	i
σ^2	$-\xi$	i
σ^3	$-i\xi$	i
τ	ξ	$-i$
$\sigma\tau$	$i\xi$	$-i$
$\sigma^2\tau$	$-\xi$	$-i$
$\sigma^3\tau$	$-i\xi$	$-i$

Other products do not give new automorphisms, since $\sigma^4 = 1$, $\tau^2 = 1$, $\tau\sigma = \sigma^3\tau$, $\tau\sigma^2 = \sigma^2\tau$, $\tau\sigma^3 = \sigma\tau$. (The last two relations follow from the first three.)

Now any $\mathbb{Q}$-automorphism of K sends i to some zero of $t^2 + 1$, so $i \mapsto \pm i$; similarly, ξ is mapped to ξ, $i\xi$, $-\xi$, or $-i\xi$. All possible combinations of these (eight in number) appear in the above list, so these are precisely the $\mathbb{Q}$-automorphisms of K.

4. The abstract structure of the Galois group G can be found. The generator-relation presentation

$$G = \langle \sigma, \tau : \sigma^4 = \tau^2 = 1,\ \tau\sigma = \sigma^3\tau \rangle$$

shows that G is the dihedral group of order 8, which we write as $\mathbb{D}_8$.

The group $\mathbb{D}_8$ has a geometric interpretation as the symmetry group of a square. In fact, we can label the four vertices of a square with the zeros of $t^4 - 2$, in such a way that the geometric symmetries are precisely the permutations of the zeros that occur in the Galois group (Figure 13.1).

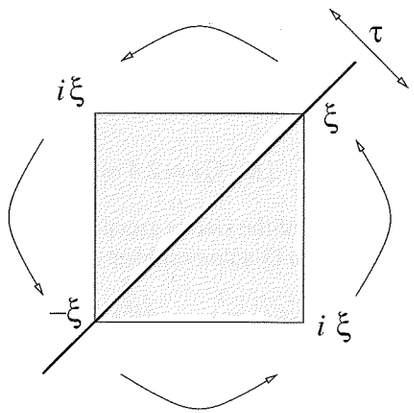

Figure 13.1: The Galois group $\mathbb{D}_8$ interpreted as the symmetry group of a square.

5. It is an easy exercise to find the subgroups of G. If as usual we let $\mathbb{Z}_n$ denote the cyclic group of order n and $\times$ the direct product, then the subgroups are as follows:

Order 8:	G	$G \cong \mathbb{D}_8$
Order 4:	$\{1, \sigma, \sigma^2, \sigma^3\}$	$S \cong \mathbb{Z}_4$
	$\{1, \sigma^2, \tau, \sigma^2, \tau\}$	$T \cong \mathbb{Z}_2 \times \mathbb{Z}_2$
	$\{1, \sigma^2, \sigma\tau, \sigma^3, \tau\}$	$U \cong \mathbb{Z}_2 \times \mathbb{Z}_2$
Order 2:	$\{1, \sigma^2\}$	$A \cong \mathbb{Z}_2$
	$\{1, \tau\}$	$B \cong \mathbb{Z}_2$
	$\{1, \sigma\tau\}$	$C \cong \mathbb{Z}_2$
	$\{1, \sigma^2\tau\}$	$D \cong \mathbb{Z}_2$
	$\{1, \sigma^3\tau\}$	$E \cong \mathbb{Z}_2$
Order 1:	$\{1\}$	$I \cong 1$

6. The inclusion relations between the subgroups of G can be summed up by the *lattice diagram* of Figure 13.2. In such diagrams, $X \subseteq Y$ if there is a sequence of upward-sloping lines from X to Y.

7. Under the Galois correspondence we obtain the intermediate fields. Since the correspondence reverses inclusions, we obtain the lattice diagram in Figure 13.3.

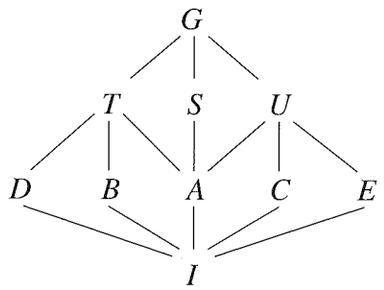

Figure 13.2: Lattice of subgroups.

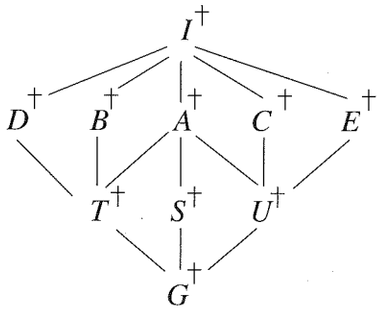

Figure 13.3: Lattice of subfields.

8. We now describe the elements of these intermediate fields. There are three obvious subfields of K of degree 2 over $\mathbb{Q}$, namely, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i\sqrt{2})$. These are clearly the fixed fields $S^\dagger$, $T^\dagger$, and $U^\dagger$, respectively. The other fixed fields are less obvious. To illustrate a possible approach we shall find $C^\dagger$. Any element of K can be expressed uniquely in the form

$$x = a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3 + a_4 i + a_5 i\xi + a_6 i\xi^2 + a_7 i\xi^3$$

where $a_0, \ldots, a_7 \in \mathbb{Q}$. Then

$$\begin{aligned}\sigma\tau(x) &= a_0 + a_1 i\xi - a_2\xi^2 - a_3 i\xi^3 - a_4 i + a_5(-i)i\xi - a_6 i(i\xi)^2 - a_7 i(i\xi)^3 \\ &= a_0 + a_5\xi - a_2\xi^2 - a_7\xi^3 - a_4 i + a_1 i\xi + a_6 i\xi^2 - a_3 i\xi^3\end{aligned}$$

The element x is fixed by $\sigma\tau$ (and hence by C) if and only if

$$\begin{array}{llll} a_0 = a_0 & a_1 = a_5 & a_2 = -a_2 & a_3 = -a_7 \\ a_4 = -a_4 & a_5 = a_1 & a_6 = a_6 & a_7 = -a_3 \end{array}$$

Therefore, a_0 and a_6 are arbitrary, while

$$a_2 = 0 = a_4 \qquad a_1 = a_5 \qquad a_3 = -a_7$$

It follows that

$$\begin{aligned}x &= a_0 + a_1(1+i)\xi + a_6 i\xi^2 + a_3(1-i)\xi^3 \\ &= a_0 + a_1[(1+i)\xi] + \frac{a_6}{2}[(1+i)\xi]^2 - \frac{a_3}{2}[(1+i)\xi]^3\end{aligned}$$

which shows that

$$C^\dagger = \mathbb{Q}((1+i)\xi)$$

Similarly,

$$A^\dagger = \mathbb{Q}(i, \sqrt{2}) \qquad B^\dagger = \mathbb{Q}(\xi) \qquad D^\dagger = \mathbb{Q}(i\xi) \qquad E^\dagger = \mathbb{Q}((1-i)\xi)$$

It is now easy to verify the inclusion relations specified by the lattice diagram in Figure 13.3.

9. It is possible, but tedious, to check by hand that these are the only intermediate fields.

10. The normal subgroups of G are G, S, T, U, A, I. By the Fundamental Theorem of Galois theory, $G^\dagger$, $S^\dagger$, $T^\dagger$, $U^\dagger$, $A^\dagger$, $I^\dagger$ should be the only normal extensions of $\mathbb{Q}$ that are contained in K. Since these are all splitting fields over $\mathbb{Q}$, for the polynomials t, t^2+1, t^2-2, t^2+2, t^4-t^2-2, t^4-2 (respectively), they are normal extensions of $\mathbb{Q}$. On the other hand, $B^\dagger : \mathbb{Q}$ is not normal, since t^4-2 has a zero, namely, ξ, in $B^\dagger$ but does not split in $B^\dagger$. Similarly, $C^\dagger$, $D^\dagger$, $E^\dagger$ are not normal extensions of $\mathbb{Q}$.

11. According to the Fundamental Theorem of Galois theory, the Galois group of $A^\dagger : \mathbb{Q}$ is isomorphic to G/A. Now G/A is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. We calculate directly the Galois group of $A^\dagger : \mathbb{Q}$. Since $A^\dagger = \mathbb{Q}(i, \sqrt{2})$ there are four $\mathbb{Q}$-automorphisms:

Automorphism	Effect on i	Effect on $\sqrt{2}$
1	i	$\sqrt{2}$
α	i	$-\sqrt{2}$
β	$-i$	$\sqrt{2}$
$\alpha\beta$	$-i$	$-\sqrt{2}$

and since $\alpha^2 = \beta^2 = 1$ and $\alpha\beta = \beta\alpha$, this group is $\mathbb{Z}_2 \times \mathbb{Z}_2$ as expected.

12. Note that the lattice diagrams for $\mathcal{F}$ and $\mathcal{G}$ do *not* look the same unless one is turned upside-down. Hence there does not exist a correspondence like the Galois correspondence but preserving inclusion relations. It may seem a little odd at first that the Galois correspondence reverses inclusions, but in fact it is entirely natural, and quite as useful a property as preservation of inclusions.

It is in general a difficult problem to compute the Galois group of a given field extension, particularly when there is no explicit representation for the elements of the large field (see Chapter 22).

Exercises

13.1 Find the Galois groups of the following extensions:

a. $\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}$

b. $\mathbb{Q}(\alpha) : \mathbb{Q}$ where $\alpha = \exp(2\pi i/3)$

c. $K : \mathbb{Q}$ where K is the splitting field over $\mathbb{Q}$ for $t^4 - 3t^2 + 4$.

13.2 Find all subgroups of these Galois groups.

13.3 Find the corresponding fixed fields.

13.4 Find all normal subgroups of the above Galois groups.

13.5 Check that the corresponding extensions are normal.

13.6 Verify that the Galois groups of these normal extensions are the relevant quotient groups.

13.7* Consider the Galois group of $t^6 - 7$ over $\mathbb{Q}$ found in Exercise 12.4. Use the Galois correspondence to find all intermediate fields.

13.8* Consider the Galois group of $t^6 - 2t^3 - 1$ over $\mathbb{Q}$ found in Exercise 12.5. Use the Galois correspondence to find all intermediate fields.

13.9 Find the Galois group of $t^8 - i$ over $\mathbb{Q}(i)$.

13.10 Find the Galois group of $t^8 + t^4 + 1$ over $\mathbb{Q}(i)$.

3.11 Use the Galois group $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ of $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}$ to find all intermediate fields. Which of these are normal over $\mathbb{Q}$?

13.12 Mark the following true or false.

a. A 3×3 square has exactly 9 distinct symmetries.
b. The symmetry group of a square is isomorphic to $\mathbb{Z}_8$.
c. The symmetry group of a square is isomorphic to $\mathbb{S}_8$.
d. The symmetry group of a square is isomorphic to a subgroup of $\mathbb{S}_8$.
e. The group $\mathbb{D}_8$ has 10 distinct subgroups.
f. The Galois correspondence preserves inclusion relations.
g. The Galois correspondence reverses inclusion relations.

Chapter 14

Solubility and Simplicity

In order to apply the Galois correspondence, we need to have at our fingertips a number of group-theoretical concepts and theorems. We have already assumed familiarity with elementary group theory: subgroups, normal subgroups, quotient groups, conjugates, permutations (up to cycle decomposition); to these we now add the standard isomorphism theorems. The relevant theory, along with most of the material in this chapter, can be found in any good textbook of group theory, for example, Fraleigh (1989), Humphreys (1996), or Neumann, Stoy, and Thompson (1994).

We start by defining soluble groups and proving some basic properties. These groups are of cardinal importance for the theory of the solution of equations by radicals. Next, we discuss simple groups, the main target being a proof of the simplicity of the alternating group of degree 5 or more. We end by proving Cauchy's Theorem: if a prime p divides the order of a finite group, then the group has an element of order p.

14.1 Soluble Groups

Soluble groups were first defined and studied (though not in the current abstract way) by Galois in his work on the solution of equations by radicals. They have since proved extremely important in many branches of mathematics.

In the following definition and thereafter, the notation $H \lhd G$ will mean that H is a normal subgroup of the group G. Recall that an *abelian* (or *commutative*) group is one in which $gh = hg$ for all elements g, h.

DEFINITION 14.1 *A group G is* soluble *(in the U.S.:* solvable*) if it has a finite series of subgroups*

$$1 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G \tag{14.1}$$

such that

1. $G_i \lhd G_{i+1}$ *for* $i = 0, \ldots, n-1$.
2. G_{i+1}/G_i *is abelian for* $i = 0, \ldots, n-1$.

Condition (1) does not imply that $G_i \lhd G$, since $G_i \lhd G_{i+1} \lhd G_{i+2}$ does not imply $G_i \lhd G_{i+2}$ (see Exercise 14.11).