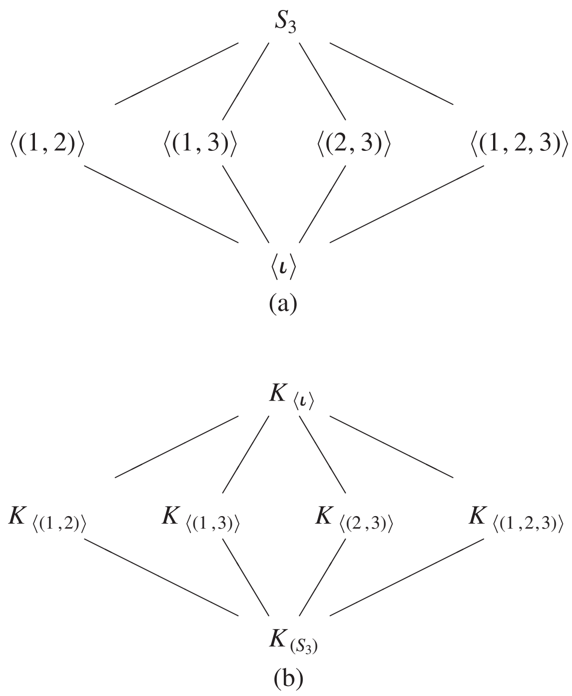


46.12 Figure

$$K_{\langle(1,2)\rangle} = \mathbb{Q}(r_3) = \mathbb{Q}\left(\frac{\sqrt[3]{2}}{2}\left(-1-\sqrt{3}i\right)\right)$$

$$K_{\langle(1,3)\rangle} = \mathbb{Q}(r_2) = \mathbb{Q}\left(\frac{\sqrt[3]{2}}{2}\left(-1+\sqrt{3}i\right)\right)$$

$$K_{\langle(1,2,3)\rangle} = \mathbb{Q}(\sqrt{3}i)$$

Normal subgroups of $G(K/\mathbb{Q})$ correspond to subfields of K that are normal extensions of $\mathbb{Q}$ by Theorem 46.8. Thus the only intermediate fields of K that are normal extensions of $\mathbb{Q}$ are K, $\mathbb{Q}$, and $\mathbb{Q}(\sqrt{3}i)$ corresponding to the normal subgroups of S_3, namely $\{\iota\}$, S_3, and $\langle(1,2,3)\rangle$, respectively. ▲

Not every subgroup diagram of a Galois group looks like its own inversion, as we will see in the next section.

EXERCISES 46

Computations

The field $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ is a finite normal extension of $\mathbb{Q}$. It can be shown that $[K : \mathbb{Q}] = 8$. In Exercises 1 through 8, compute the indicated numerical quantity. The notation is that of Definition 46.1.

1. $[K : \mathbb{Q}\sqrt{2}]$

2. $|G(K/\mathbb{Q})|$

3. $|\lambda(\mathbb{Q})|$

4. $|\lambda(\mathbb{Q}(\sqrt{2}, \sqrt{3}))|$

5. $|\lambda(\mathbb{Q}(\sqrt{6}))|$

6. $|\lambda(\mathbb{Q}(\sqrt{30}))|$

7. $|\lambda(\mathbb{Q}(\sqrt{2} + \sqrt{6}))|$

8. $|\lambda(K)|$

9. Describe the group of the polynomial $(x^4 - 1) \in \mathbb{Q}[x]$ over $\mathbb{Q}$.

10. Let G be the group of the polynomial $x^3 + 2$ over $\mathbb{Q}$. Find the order of G and identify a well-known group that is isomorphic with G.

11. Let K be the splitting field of $x^3 - 5$ over $\mathbb{Q}$.

- **a.** Show that $K = \mathbb{Q}(\sqrt[3]{5}, i\sqrt{3})$.
- **b.** Describe the six elements of $G(K/\mathbb{Q})$ by giving their values on $\sqrt[3]{5}$ and $i\sqrt{3}$.
- **c.** To what group we have seen before is $G(K/\mathbb{Q})$ isomorphic?
- **d.** Using the notation given in the answer to part (b) in the back of the text, give the diagrams for the subfields of K and for the subgroups of $G(K/\mathbb{Q})$, indicating corresponding intermediate fields and subgroups, as we did in Example 46.11.

12. Describe the group of the polynomial $(x^4 - 5x^2 + 6) \in \mathbb{Q}[x]$ over $\mathbb{Q}$.

13. Describe the group of the polynomial $(x^3 - 1) \in \mathbb{Q}[x]$ over $\mathbb{Q}$.

Concepts

14. Give an example of two normal extensions K_1 and K_2 of the same field F such that K_1 and K_2 are not isomorphic fields but $G(K_1/F) \simeq G(K_2/F)$.

15. Determine whether each of the following is true or false.

- **a.** Two different subgroups of a Galois group may have the same fixed field.
- **b.** If $F \leq E < L \leq K$ are field extensions and K is a normal extension of F, then $\lambda(E) < \lambda(L)$.
- **c.** If K is a normal extension of F, then K is a normal extension of E, where $F \leq E \leq K$.
- **d.** If two normal extensions E and L of a field F have isomorphic Galois groups, then $[E : F] = [L : F]$.
- **e.** If E is a normal extension of F and H is a normal subgroup of $G(E/F)$, then E_H is a normal extension of F.
- **f.** If E is any normal simple extension of a field F, then the Galois group $G(E/F)$ is a simple group.
- **g.** No Galois group is simple.
- **h.** If two intermediate fields E_1 and E_2 of a normal extension K over F have isomorphic groups, $\lambda(E_1)$ and $\lambda(E_2)$, then $K_{\lambda(E_1)}$ is isomorphic with $K_{\lambda(E_2)}$.
- **i.** An extension E of degree 2 over a field F is always a normal extension of F.
- **j.** An extension E of degree 2 over a field F is always a normal extension of F if the characteristic of F is zero.

Theory

16. A normal extension K of a field F is **abelian over** F if $G(K/F)$ is an abelian group. Show that if K is abelian over F and $F \leq E \leq K$, then K is abelian over E and E is abelian over F.

17. Let K be a normal extension of a field F. Prove that for every $\alpha \in K$, the **norm of** α **over** F, given by

$$N_{K/F}(\alpha) = \prod_{\sigma \in G(K/F)} \sigma(\alpha),$$

and the **trace of** α **over** F, given by

$$Tr_{K/F}(\alpha) = \sum_{\sigma \in G(K/F)} \sigma(\alpha),$$

are elements of F.

18. Consider $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Referring to Exercise 17, compute each of the following (see Table 43.5).

- **a.** $N_{K/\mathbb{Q}}(\sqrt{2})$
- **b.** $N_{K/\mathbb{Q}}(\sqrt{2} + \sqrt{3})$
- **c.** $N_{K/\mathbb{Q}}(\sqrt{6})$
- **d.** $N_{K/\mathbb{Q}}(2)$
- **e.** $Tr_{K/\mathbb{Q}}(\sqrt{2})$
- **f.** $Tr_{K/\mathbb{Q}}(\sqrt{2} + \sqrt{3})$
- **g.** $Tr_{K/\mathbb{Q}}(\sqrt{6})$
- **h.** $Tr_{K/\mathbb{Q}}(2)$

19. Let $K = F(\alpha)$ be a normal extension of F. Let

$$\operatorname{irr}(\alpha, F) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0.$$

Referring to Exercise 17, show that

a. $N_{K/F}(\alpha) = (-1)^n a_0$,

b. $Tr_{K/F}(\alpha) = -a_{n-1}$.

20. Let $f(x) \in F[x]$ be a polynomial of degree n such that each irreducible factor is separable over F. Show that the order of the group of $f(x)$ over F divides $n!$.

21. Let $f(x) \in F[x]$ be a polynomial such that every irreducible factor of $f(x)$ is a separable polynomial over F. Show that the group of $f(x)$ over F can be viewed in a natural way as a group of permutations of the zeros of $f(x)$ in $\bar{F}$.

22. Let F be a field and let ζ be a primitive nth root of unity in $\bar{F}$, where the characteristic of F is 0.

a. Show that $F(\zeta)$ is a normal extension of F.

b. Show that $G(F(\zeta)/F)$ is abelian. [*Hint:* Every $\sigma \in G(F(\zeta)/F)$ maps ζ onto some ζ^r and is completely determined by this value r.]

23. A normal extension K of a field F is **cyclic over** F if $G(K/F)$ is a cyclic group.

a. Show that if K is cyclic over F and $F \leq E \leq K$, then E is cyclic over F and K is cyclic over E.

b. Show that if K is cyclic over F, then there exists exactly one field $E, F \leq E \leq K$, of degree d over F for each divisor d of $[K : F]$.

24. Let K be a normal extension of F.

a. For $\alpha \in K$, show that

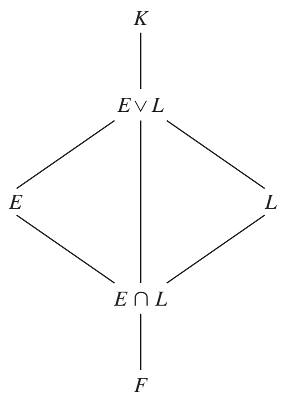
$$f(x) = \prod_{\sigma \in G(K/F)} (x - \sigma(\alpha))$$

is in $F[x]$.

b. Referring to part (a), show that $f(x)$ is a power of $\operatorname{irr}(\alpha, F)$, and $f(x) = \operatorname{irr}(\alpha, F)$ if and only if $K = F(\alpha)$.

25. Let K be a normal extension of the field F. If E and L are both intermediate fields of the extension, the **join**, $E \vee L$, is the intersection of all intermediate fields of the extension that contain both E and L. See Figure 46.13. Describe $G(K/(E \vee L))$ in terms of $G(K/E)$ and $G(K/L)$.

26. With reference to the situation in Exercise 25, describe $G(K/(E \cap L))$ in terms of $G(K/E)$ and $G(K/L)$.



46.13 Figure

SECTION 47 ILLUSTRATIONS OF GALOIS THEORY

Symmetric Functions

Let F be a field of characteristic zero, and let $y_1, \cdots, y_n$ be indeterminates. There are some natural automorphisms of $F(y_1, \cdots, y_n)$ leaving F fixed, namely, those defined by permutations of $\{y_1, \cdots, y_n\}$. To be more explicit, let σ be a permutation of $\{1, \cdots, n\}$, that is, $\sigma \in S_n$. Then σ gives rise to a natural map $\overline{\sigma} : F(y_1, \cdots, y_n) \to F(y_1, \cdots, y_n)$ given by

$$\overline{\sigma}\left(\frac{f(y_1, \cdots, y_n)}{g(y_1, \cdots, y_n)}\right) = \frac{f(y_{\sigma(1)}, \cdots, y_{\sigma(n)})}{g(y_{\sigma(1)}, \cdots, y_{\sigma(n)})}$$

for $f(y_1, \cdots, y_n), g(y_1, \cdots, y_n) \in F[y_1, \cdots, y_n]$, with $g(y_1, \cdots, y_n) \neq 0$. It is immediate that $\overline{\sigma}$ is an automorphism of $F(y_1, \cdots, y_n)$ leaving F fixed. The elements of $F(y_1, \cdots, y_n)$ left fixed by *all* $\overline{\sigma}$, for all $\sigma \in S_n$, are those rational functions that are *symmetric* in the indeterminates $y_1, \cdots, y_n$.

47.1 Definition An element of the field $F(y_1, \cdots, y_n)$ is a **symmetric function in** $y_1, \cdots, y_n$ **over** F, if it is fixed by all permutations of $y_1, \cdots, y_n$, in the sense just explained. ■

Let $\overline{S_n}$ be the group of all the automorphisms $\overline{\sigma}$ for $\sigma \in S_n$. Observe that $\overline{S_n}$ is naturally isomorphic to S_n. Let K be the subfield of $F(y_1, \cdots, y_n)$, which is the fixed field of $\overline{S_n}$. Consider the polynomial

$$f(x) = \prod_{i=1}^{n}(x - y_i);$$

this polynomial $f(x) \in (F(y_1, \cdots, y_n))[x]$ is a **general polynomial of degree** n. Let $\overline{\sigma_x}$ be the polynomial extension of $\overline{\sigma}$, as defined in Definition 44.4, to $(F(y_1, \cdots, y_n))[x]$, where $\overline{\sigma_x}(x) = x$. Now $f(x)$ is fixed by each map $\overline{\sigma_x}$ for $\sigma \in S_n$; that is,

$$\prod_{i=1}^{n}(x - y_i) = \prod_{i=1}^{n}(x - y_{\sigma(i)}).$$

Thus the coefficients of $f(x)$ are in K; they are, except for sign, the *elementary symmetric functions* in $y_1, \cdots, y_n$. As illustration, note that the constant term of $f(x)$ is

$$(-1)^n y_1 y_2 \cdots y_n,$$

the coefficient of x^{n-1} is $-(y_1 + y_2 + \cdots + y_n)$, and so on. These are symmetric functions in $y_1, \cdots, y_n$.

The first elementary symmetric function in $y_1, \cdots, y_n$ is

$$s_1 = y_1 + y_2 + \cdots + y_n,$$

the second is $s_2 = y_1y_2 + y_1y_3 + \cdots + y_{n-1}y_n$, and so on, and the nth is $s_n = y_1y_2 \cdots y_n$.

Consider the field $E = F(s_1, \cdots, s_n)$. Of course, $E \leq K$, where K is the field of all symmetric functions in $y_1, \cdots, y_n$ over F. Since the characteristic of E is zero, the extension K over E is a separable extension. Thus $F(y_1, \cdots, y_n)$ is a finite normal extension of E, namely, the splitting field of

$$f(x) = \prod_{i=1}^{n}(x - y_i)$$

over E. Since the degree of $f(x)$ is n, we have at once that

$$[F(y_1, \cdots, y_n) : E] \leq n!$$

(see Exercise 19, Section 44). However, since K is the fixed field of $\overline{S_n}$ and

$$|\overline{S_n}| = |S_n| = n!,$$

we have also

$$n! = [F(y_1, \cdots, y_n) : K].$$

Therefore,

$$n! = [F(y_1, \cdots, y_n) : K] \leq [F(y_1, \cdots, y_n) : E] \leq n!,$$

so

$$K = E.$$

The full Galois group of $F(y_1, \cdots, y_n)$ over E is therefore $\overline{S_n}$. The fact that $K = E$ shows that every symmetric function can be expressed as a rational function of the elementary symmetric functions $s_1, \cdots, s_n$. We summarize these results in a theorem.

47.2 Theorem Let F be a field with characteristic zero. Let $s_1, \cdots, s_n$ be the elementary symmetric functions in the indeterminates $y_1, \cdots, y_n$. Then every symmetric function of $y_1, \cdots, y_n$ over F is a rational function of the elementary symmetric functions. Also, $F(y_1, \cdots, y_n)$ is a finite normal extension of degree $n!$ of $F(s_1, \cdots, s_n)$, and the Galois group of this extension is naturally isomorphic to S_n.

In view of Cayley's Theorem 8.11, it can be deduced from Theorem 47.2 that any finite group can occur as a Galois group (up to isomorphism). (See Exercise 11.)

The proof of Theorem 47.2 only uses the fact that the characteristic of F is zero to conclude that the extension $F(y_1, y_2, \ldots, y_n)$ over E is a separable extension. With a bit more work, the proof can be modified to allow F to be an arbitrary field.

Examples

Let us give our promised example of a finite normal extension having a Galois group whose subgroup diagram does not look like its own inversion.

47.3 Example Consider the splitting field in $\mathbb{C}$ of $x^4 - 2$ over $\mathbb{Q}$. Now $x^4 - 2$ is irreducible over $\mathbb{Q}$, by Eisenstein's criterion, with $p = 2$. Let $\alpha = \sqrt[4]{2}$ be the real positive zero of $x^4 - 2$. Then the four zeros of $x^4 - 2$ in $\mathbb{C}$ are $\alpha, -\alpha, i\alpha$, and $-i\alpha$, where i is the usual zero of $x^2 + 1$ in $\mathbb{C}$. The splitting field K of $x^4 - 2$ over $\mathbb{Q}$ thus contains $(i\alpha)/\alpha = i$. Since α is a real number, $\mathbb{Q}(\alpha) < \mathbb{R}$, so $\mathbb{Q}(\alpha) \neq K$. However, since $\mathbb{Q}(\alpha, i)$ contains all zeros of $x^4 - 2$, we see that $\mathbb{Q}(\alpha, i) = K$. Letting $E = \mathbb{Q}(\alpha)$, we have the diagram in Fig. 47.4.

$$\begin{array}{l} K = \mathbb{Q}(\alpha, i) \\ \quad | \\ E = \mathbb{Q}(\alpha) \\ \quad | \\ \mathbb{Q} \end{array}$$

47.4 Figure

Now $\{1, \alpha, \alpha^2, \alpha^3\}$ is a basis for E over $\mathbb{Q}$, and $\{1, i\}$ is a basis for K over E. Thus

$$\{1, \alpha, \alpha^2, \alpha^3, i, i\alpha, i\alpha^2, i\alpha^3\}$$

is a basis for K over $\mathbb{Q}$. Since $[K : \mathbb{Q}] = 8$, we must have $|G(K/\mathbb{Q})| = 8$, so we need to find eight automorphisms of K leaving $\mathbb{Q}$ fixed. We know that any such automorphism σ is completely determined by its values on elements of the basis $\{1, \alpha, \alpha^2, \alpha^3, i, i\alpha, i\alpha^2, i\alpha^3\}$, and these values are in turn determined by $\sigma(\alpha)$ and $\sigma(i)$. But $\sigma(\alpha)$ must always be a conjugate of α over $\mathbb{Q}$, that is, one of the four zeros of $\text{irr}(\alpha, \mathbb{Q}) = x^4 - 2$. Likewise, $\sigma(i)$ must be a zero of $\text{irr}(i, \mathbb{Q}) = x^2 + 1$. Thus the four possibilities for $\sigma(\alpha)$, combined with the two possibilities for $\sigma(i)$, must give all eight automorphisms. We let $\rho \in G(K/\mathbb{Q})$ be the automorphism with $\rho(\alpha) = i\alpha$ and $\rho(i) = i$; and we let $\mu \in G(K/\mathbb{Q})$ be the automorphism with $\mu(\alpha) = \alpha$ and $\mu(i) = -i$. We have

$$\rho^2(\alpha) = \rho(\rho(\alpha)) = \rho(i\alpha) = i(i\alpha) = -\alpha,$$
$$\rho^2(i) = \rho(\rho(i)) = \rho(i) = i.$$

47.5 Table

	ι	ρ	ρ^2	ρ^3	μ	$\mu\rho$	$\mu\rho^2$	$\mu\rho^3$
$\alpha \rightarrow$	α	$i\alpha$	$-\alpha$	$-i\alpha$	α	$-i\alpha$	$-\alpha$	$i\alpha$
$i \rightarrow$	i	i	i	i	$-i$	$-i$	$-i$	$-i$

Similarly, we have

$$\mu\rho(\alpha) = \mu(\rho(\alpha)) = \mu(i\alpha) = -i\alpha,$$
$$\mu\rho(i) = \mu(\rho(i)) = \mu(i) = -i.$$

Table 47.5 shows the results of similar computations for $\iota, \rho, \rho^2, \rho^3, \mu, \mu\rho, \mu\rho^2$, and $\mu\rho^3$. These automorphisms account for all eight of the elements of $G(K/\mathbb{Q})$. The table looks remarkably like the dihedral group D_4. To verify that $G(K/\mathbb{Q})$ is isomorphic with D_4 we check the relations $\mu^2 = \iota$, $\rho^4 = \iota$, and $\rho\mu = \mu\rho^3$ by evaluating each at α and i.

$$\mu^2(\alpha) = \mu(\alpha) = \alpha,$$
$$\mu^2(i) = \mu(-i) = i,$$

$$\rho^4(\alpha) = \rho(\rho^3(\alpha)) = \rho(-i\alpha) = -i^2\alpha = \alpha,$$
$$\rho^4(i) = \rho(\rho^3(i)) = \rho(i) = i,$$

$$\rho\mu(\alpha) = \rho(\alpha) = i\alpha = \mu\rho^3(\alpha),$$
$$\rho\mu(i) = \rho(-i) = -i = \mu\rho^3(i).$$

The subgroup diagram for the dihedral group is given in Figure 47.6 (a) with the corresponding subfield diagram in Figure 47.6 (b). This provides a good illustration of how one diagram is the inversion of the other.

The determination of the fixed fields K_{H_i} sometimes requires a bit of ingenuity. Let's illustrate. To find K_{H_2}, we merely have to find an extension of $\mathbb{Q}$ of degree 2 fixed by $\{\iota, \rho, \rho^2, \rho^3\}$. Since all ρ^j leave i fixed, $\mathbb{Q}(i)$ is the field we are after. To find K_{H_4}, we have to find an extension of $\mathbb{Q}$ of degree 4 fixed by ι and μ. Since μ leaves α fixed and α is a zero of $\mathrm{irr}(\alpha, \mathbb{Q}) = x^4 - 2$, we see that $\mathbb{Q}(\alpha)$ is of degree 4 over $\mathbb{Q}$ and is fixed by $\{\iota, \mu\}$. By *Galois theory, it is the only such field*. Here we are using strongly the one-to-one correspondence given by the Galois theory. If we find one field that fits the bill, it is the one we are after. Finding K_{H_7} requires more ingenuity. Since H_7 is a group, for any $\beta \in K$, $\iota(\beta) + \mu\rho^3(\beta)$ is fixed by ι and $\mu\rho^3$, the elements of H_7. Letting $\beta = \alpha$ we see that $\iota(\alpha) + \mu\rho^3(\alpha) = \alpha + i\alpha$ is fixed by H_7. By checking all eight automorphisms in Table 47.5, we see that only ι and $\mu\rho^3$ fix $\alpha + i\alpha$. Thus by the one-to-one correspondence, we must have

$$\mathbb{Q}(\alpha + i\alpha) = \mathbb{Q}(\sqrt[4]{2} + i\sqrt[4]{2}) = K_{H_7}.$$

Suppose we wish to find $\mathrm{irr}(\alpha + i\alpha, \mathbb{Q})$. If $\gamma = \alpha + i\alpha$, then for every conjugate of γ over $\mathbb{Q}$, there exists an automorphism of K mapping γ into that conjugate. Thus we need only compute the various different values $\sigma(\gamma)$ for $\sigma \in G(K/\mathbb{Q})$ to find the other zeros of $\mathrm{irr}(\gamma, \mathbb{Q})$. Every element in D_4 can be written in the form $\rho^i(\mu\rho^3)^j$ where $0 \leq i \leq 3$ and j is either 0 or 1. But $\mu\rho^3(\alpha + i\alpha) = \alpha + i\alpha$, so to compute the conjugates of $\alpha + i\alpha$ we only need to compute $\iota(\alpha + i\alpha)$, $\rho(\alpha + i\alpha)$, $\rho^2(\alpha + i\alpha)$, and $\rho^3(\alpha + i\alpha)$.