18. Notation as in the previous exercises.

(a) Prove that ℓ_1 intersects the x-axis in the point $(\eta_1/2, 0)$ and that ℓ_2 intersects the x-axis in the point $(\eta_2/2, 0)$.

(b) Prove that C_1 is the circle having the points $(\eta_1, -1)$ and $(0, 1)$ as diameter. Prove that $s = \eta_1'$. Similarly prove that C_2 is the circle having the points $(\eta_2, -1)$ and $(0, 1)$ as diameter and that $t = \eta_4'$.

(c) Prove that P has coordinates $(\eta_1'', 0)$ and hence that the construction in the previous problem constructs the regular 17-gon by straightedge and compass.

14.6 GALOIS GROUPS OF POLYNOMIALS

Recall that the Galois group of a separable polynomial $f(x) \in F[x]$ is defined to be the Galois group of the splitting field of $f(x)$ over F.

If K is a Galois extension of F then K is the splitting field for some separable polynomial $f(x)$ over F. Any automorphism $\sigma \in \text{Gal}(K/F)$ maps a root of an irreducible factor of $f(x)$ to another root of the irreducible factor and σ is uniquely determined by its action on these roots (since they generate K over F). If we fix a labelling of the roots $\alpha_1, \dots, \alpha_n$ of $f(x)$ we see that any $\sigma \in \text{Gal}(K/F)$ defines a unique permutation of $\alpha_1, \dots, \alpha_n$, hence defines a unique permutation of the subscripts $\{1, 2, \dots, n\}$ (which depends on the fixed labelling of the roots). This gives an injection

$$\text{Gal}(K/F) \hookrightarrow S_n$$

of the Galois group into the symmetric group on n letters which is clearly a homomorphism (both group operations are composition). We may therefore think of Galois groups as subgroups of symmetric groups. Since the degree of the splitting field is the same as the order of the Galois group by the Fundamental Theorem, this explains from the group-theoretic side why the splitting field for a polynomial of degree n over F is of degree at most $n!$ over F (Proposition 13.26).

In general, if the factorization of $f(x)$ into irreducibles is $f(x) = f_1(x) \cdots f_k(x)$ where $f_i(x)$ has degree n_i, $i = 1, 2, \dots, k$, then since the Galois group permutes the roots of the irreducible factors among themselves we have $\text{Gal}(K/F) \le S_{n_1} \times \cdots \times S_{n_k}$.

If $f(x)$ is irreducible, then given any two roots of $f(x)$ there is an automorphism in the Galois group G of $f(x)$ which maps the first root to the second (this follows from our extension Theorem 13.27). Such a group is said to be *transitive* on the roots, i.e., you can get from any given root to any other root by applying some element of G. The fact that the Galois group must be transitive on blocks of roots (namely, the roots of the irreducible factors) can often be helpful in reducing the number of possibilities for the structure of G (cf. the discussion of Galois groups of polynomials of degree 4 below).

Examples

(1) Consider the biquadratic extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$, which is the splitting field of $(x^2-2)(x^2-3)$. Label the roots as $\alpha_1 = \sqrt{2}$, $\alpha_2 = -\sqrt{2}$, $\alpha_3 = \sqrt{3}$ and $\alpha_4 = -\sqrt{3}$. The elements of the Galois group are $\{1, \sigma, \tau, \sigma\tau\}$ where σ maps $\sqrt{2}$ to $-\sqrt{2}$ and fixes $\sqrt{3}$ and τ fixes $\sqrt{2}$ and maps $\sqrt{3}$ to $-\sqrt{3}$. As permutations of the roots for this labelling we see that σ interchanges the first two and fixes the second two and τ fixes the first two and interchanges the second two, i.e.,

$$\sigma = (12) \qquad \text{and} \qquad \tau = (34)$$

as elements of S_4. Similarly, or by taking the product of these two elements, we see that

$$\sigma\tau = (12)(34) \in S_4.$$

Hence

$$\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \cong \{1, (12), (34), (12)(34)\} \subset S_4$$

identifying this Galois group with the Klein-4 subgroup of S_4. Note that if we had changed the labelling of the roots above we would have obtained a different (isomorphic) representation of the Galois group as a subgroup of S_4 (for example, interchanging the second and third roots would have given the subgroup $\{1, (13), (24), (13)(24)\}$).

(2) The Galois group of $x^3 - 2$ acts as permutations on the three roots $\sqrt[3]{2}$, $\rho\sqrt[3]{2}$ and $\rho^2\sqrt[3]{2}$ where ρ is a primitive 3rd root of unity. With this ordering, the generators σ and τ we have defined earlier give the permutations

$$\sigma = (123) \qquad \tau = (23)$$

which gives

$$\{1, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\} = \{1, (123), (132), (23), (13), (12)\} = S_3,$$

in this case the full symmetric group on 3 letters.

Recall that every finite group is isomorphic to a subgroup of some symmetric group S_n. It is an open problem to determine whether every finite group appears as the Galois group for some polynomial over $\mathbb{Q}$. We have seen in the last section that every abelian group is a Galois group over $\mathbb{Q}$ (for some subfield of a cyclotomic field). We shall explicitly determine the Galois groups for polynomials of small degree (≤ 4) below which will in particular show that every subgroup of S_4 arises as a Galois group.

We first introduce some definitions and show that the "general" polynomial of degree n has S_n as Galois group (so the second example above should be viewed as "typical").

Definition. Let $x_1, x_2, \ldots, x_n$ be indeterminates. The *elementary symmetric functions* $s_1, s_2, \ldots, s_n$ are defined by

$$\begin{aligned} s_1 &= x_1 + x_2 + \cdots + x_n \\ s_2 &= x_1x_2 + x_1x_3 + \cdots + x_2x_3 + x_2x_4 + \cdots + x_{n-1}x_n \\ &\vdots \\ s_n &= x_1x_2 \cdots x_n \end{aligned}$$

i.e., the i^{th} symmetric function s_i of $x_1, x_2, \ldots, x_n$ is the sum of all products of the x_j's taken i at a time.

Definition. The *general polynomial of degree n* is the polynomial

$$(x - x_1)(x - x_2) \cdots (x - x_n)$$

whose roots are the indeterminates $x_1, x_2, \ldots, x_n$.

It is easy to see by induction that the coefficients of the general polynomial of degree n are given by the elementary symmetric functions in the roots:

$$(x - x_1)(x - x_2) \cdots (x - x_n) = x^n - s_1 x^{n-1} + s_2 x^{n-2} + \cdots + (-1)^n s_n. \quad (14.13)$$

For any field F, the extension $F(x_1, x_2, \ldots, x_n)$ is then a Galois extension of the field $F(s_1, s_2, \ldots, s_n)$ since it is the splitting field of the general polynomial of degree n .

If $\sigma \in S_n$ is any permutation of $\{1, 2, \ldots, n\}$, then σ acts on the rational functions in $F(x_1, x_2, \ldots, x_n)$ by permuting the subscripts of the variables $x_1, x_2, \ldots, x_n$. It is clear that this gives an automorphism of $F(x_1, x_2, \ldots, x_n)$. Identifying $\sigma \in S_n$ with this automorphism of $F(x_1, x_2, \ldots, x_n)$ identifies S_n as a subgroup of $\mathrm{Aut}(F(x_1, x_2, \ldots, x_n))$.

The elementary symmetric functions $s_1, s_2, \ldots, s_n$ are fixed under any permutation of their subscripts (this is the reason they are called *symmetric*), which shows that the subfield $F(s_1, s_2, \ldots, s_n)$ is contained in the fixed field of S_n. By the Fundamental Theorem of Galois Theory, the fixed field of S_n has index precisely $n!$ in $F(x_1, x_2, \ldots, x_n)$. Since $F(x_1, x_2, \ldots, x_n)$ is the splitting field over $F(s_1, s_2, \ldots, s_n)$ of the polynomial of degree n in (13), we have

$$[F(x_1, x_2, \ldots, x_n) : F(s_1, s_2, \ldots, s_n)] \leq n! . \quad (14.14)$$

It follows that we actually have equality and that $F(s_1, s_2, \ldots, s_n)$ is precisely the fixed field of S_n. This proves the following result.

Proposition 30. The fixed field of the symmetric group S_n acting on the field of rational functions in n variables $F(x_1, x_2, \ldots, x_n)$ is the field of rational functions in the elementary symmetric functions $F(s_1, s_2, \ldots, s_n)$.

Definition. A rational function $f(x_1, x_2, \ldots, x_n)$ is called *symmetric* if it is not changed by any permutation of the variables $x_1, x_2, \ldots, x_n$.

Corollary 31. *(Fundamental Theorem on Symmetric Functions)* Any symmetric function in the variables $x_1, x_2, \ldots, x_n$ is a rational function in the elementary symmetric functions $s_1, s_2, \ldots, s_n$.

Proof: A symmetric function lies in the fixed field of S_n above, hence is a rational function in $s_1, \ldots, s_n$.

This corollary explains why these are called the *elementary* symmetric functions.

Remark: If $f(x_1, \ldots, x_n)$ is a *polynomial* in $x_1, x_2, \ldots, x_n$ which is symmetric then it can be seen that f is actually a polynomial in $s_1, s_2, \ldots, s_n$, which strengthens the statement of the corollary. It is in fact true that a symmetric polynomial whose coefficients lie in R, where R is any commutative ring with identity, is a polynomial in the elementary symmetric functions with coefficients in R. A proof of this fact is implicit in the algorithm outlined in the exercises for writing a symmetric polynomial as a polynomial in the elementary symmetric functions.

Examples

(1) The expression $(x_1 - x_2)^2$ is symmetric in x_1, x_2. We have

$$(x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = s_1^2 - 4s_2,$$

a polynomial in the elementary symmetric functions.

(2) The polynomial $x_1^2 + x_2^2 + x_3^2$ is symmetric in x_1, x_2, x_3, and in this case we have

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 &= (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_1x_3 + x_2x_3) \\ &= s_1^2 - 2s_2. \end{aligned}$$

(3) The polynomial $x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2$ is symmetric. Since

$$\begin{aligned} (x_1x_2 + x_1x_3 + x_2x_3)^2 &= x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2 + 2(x_1^2x_2x_3 + x_2^2x_1x_3 + x_3^2x_1x_2) \\ &= x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2 + 2x_1x_2x_3(x_1 + x_2 + x_3) \end{aligned}$$

we have

$$x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2 = s_2^2 - 2s_1s_3.$$

Suppose now we *start* with the general polynomial

$$x^n - s_1x^{n-1} + s_2x^{n-2} + \cdots + (-1)^n s_n$$

over the field $F(s_1, s_2, \ldots, s_n)$ where we view the $s_i, i = 1, 2, \ldots, n$ as indeterminates. If we define the roots of this polynomial to be $x_1, x_2, \ldots, x_n$ then the s_i are precisely the elementary symmetric functions in the roots $x_1, \ldots, x_n$. Moreover, these roots are indeterminates as well in the sense that there are no polynomial relations over F between them. For suppose $p(t_1, \ldots, t_n)$ is a nonzero polynomial in n variables with coefficients in F such that $p(x_1, \ldots, x_n) = 0$. Then the product, $\widetilde{p}$, over all σ in S_n of $p(t_{\sigma(1)}, \ldots, t_{\sigma(n)})$ is a nonzero symmetric polynomial with $\widetilde{p}(x_1, \ldots, x_n) = 0$. This gives a nonzero polynomial relation over F among $s_1, \ldots, s_n$, a contradiction. Conversely, if the roots of a polynomial $f(x)$ are independent indeterminates over F, then so are the coefficients of $f(x)$ — cf. the beginning of Section 9. Thus defining the general polynomial over F as having indeterminate roots or indeterminate coefficients is equivalent. From this point of view our result can be stated in the following form.

Theorem 32. The general polynomial

$$x^n - s_1x^{n-1} + s_2x^{n-2} + \cdots + (-1)^n s_n$$

over the field $F(s_1, s_2, \ldots, s_n)$ is separable with Galois group S_n.

This result says that if there are no relations among the coefficients of a polynomial of degree n (which is what we mean when we say the s_i are indeterminates above) then the Galois group of this polynomial over the field generated by its coefficients is the full symmetric group S_n. Loosely speaking, this means that the "generic" polynomial of degree n will have S_n as Galois group. Note, however, that over finite fields every polynomial has a *cyclic* Galois group (all extensions of finite fields are cyclic), so that "generic" polynomials in this sense do not exist. Over $\mathbb{Q}$ one can make precise the