Chapter 14

Galois Theory

En un mot les calculs sont impraticables.

Evariste Galois

1. THE MAIN THEOREM OF GALOIS THEORY

In the last chapter we studied algebraic field extensions, using extensions generated by a single element as the basic tool. This amounts to studying the properties of a single root of an irreducible polynomial

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0. \tag{1.1}$$

Galois theory, the topic of this chapter, is the theory of *all* the roots of such a polynomial and of the symmetries among them.

We will restrict our attention to fields of *characteristic zero* in this chapter. It is to be understood that all fields occurring have characteristic zero, and we will not mention this assumption explicitly from now on.

The notation K/F will indicate that K is an extension field of F. This notation is traditional, though there is some danger of confusion with the notation R/I for the quotient of a ring R by an ideal I.

As we have seen, computation in a field $F(\alpha)$ generated by a single root can easily be made by identifying it with the formally constructed field $F[x]/(f)$. But suppose that an irreducible polynomial $f(x)$ factors into linear factors in a field extension K, and that its roots in K are $\alpha_1,\ldots,\alpha_n$. How to compute with all these roots at the same time isn't clear. To do so we have to know how the roots are related, and this depends on the particular case. In principle, the relations can be obtained by expanding the equation $f(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n)$. Doing so, we find that the sum of the roots is $-a_{n-1}$, that their product is $\pm a_0$, and so on. However, it may not be easy to interpret these relations directly.

The fundamental discovery which arose through the work of several people, especially of Lagrange and Galois, is that the relationships between the roots can be understood in terms of symmetry. The original model for this symmetry is complex conjugation, which permutes the two roots $\pm i$ of the irreducible real polynomial $x^2 + 1$, while leaving the real numbers fixed. We will begin by observing that such a symmetry exists for any quadratic field extension.

An extension K/F of degree 2 is generated by any element α of K which is not in F. Moreover, α is a root of an irreducible quadratic polynomial

$$(1.2) \qquad f(x) = x^2 + bx + c$$

with coefficients in F. Then $\alpha' = -b - \alpha$ is also a root of f, so this polynomial splits into linear factors over K: $f(x) = (x - \alpha)(x - \alpha')$.

The fact that α and α' are roots of the same irreducible polynomial provides us with our symmetry. According to Proposition (2.9) of Chapter 13, there is an isomorphism

$$(1.3) \qquad \sigma: F(\alpha) \longrightarrow F(\alpha'),$$

which is the identity on F and which sends $\alpha \rightsquigarrow \alpha'$. But either root generates the extension: $F(\alpha) = K = F(\alpha')$. Therefore σ is an automorphism of K.

This automorphism switches the two roots α, α'. For, since σ is the identity on F, it fixes b, and $\alpha + \alpha' = b$. So if $\sigma(\alpha) = \alpha'$, we must have $\sigma(\alpha') = \alpha$. It follows that σ^2 sends $\alpha \rightsquigarrow \alpha$ and, since α generates K over F, that σ^2 is the identity.

Note also that σ is not the identity automorphism, because the two roots α, α' are distinct. If α were a double root of the quadratic polynomial (1.2), the quadratic formula would give $\alpha = -\frac{1}{2}b$. This would imply $\alpha \in F$, contrary to our hypothesis that f is irreducible.

Since our field F is assumed to have characteristic zero, the quadratic extension K can be obtained by adjoining a square root δ of the discriminant $D = b^2 - 4c$, a root of the irreducible polynomial $x^2 - D$. Its other root is $-\delta$, and σ interchanges the two square roots.

Whenever K is obtained by adjoining a square root δ, there is an automorphism which sends $\delta \rightsquigarrow -\delta$. For example, let $\alpha = 1 + \sqrt{2}$, and let $K = \mathbb{Q}(\alpha)$. The irreducible polynomial for α over $\mathbb{Q}$ is $x^2 - 2x - 1$, and the other root of this polynomial is $\alpha' = 1 - \sqrt{2}$. There is an automorphism σ of K which sends $\sqrt{2} \rightsquigarrow -\sqrt{2}$ and $\alpha \rightsquigarrow \alpha'$. It is important to note right away that such an automorphism will *not* be continuous when K is considered as a subfield of $\mathbb{R}$. It is a symmetry of the algebraic structure of K, but it does not respect the geometry given by the embedding of K into the real line.

By definition, an *F-automorphism* of an extension field K is an automorphism which is the identity on the subfield F [see Chapter 13 (2.10)]. In other words, an automorphism σ of K is an F-automorphism if $\sigma(c) = c$ for all $c \in F$. Thus complex conjugation is an $\mathbb{R}$-automorphism of $\mathbb{C}$, and the symmetry σ we have just found is an F-automorphism of the quadratic extension K. It is not difficult to show that σ is the only F-automorphism of this extension other than the identity.

The group of all F-automorphisms of K is called the *Galois group* of the field extension. We often denote this group by $G(K/F)$. When K/F is a quadratic extension, the Galois group $G(K/F)$ is a group of order 2.

Let us now consider the next simplest example, that of a biquadratic extension. We will call a field extension K/F *biquadratic* if $[K{:}F] = 4$ and if K is generated by the roots of *two* irreducible quadratic polynomials. Every such extension has the form

$$K = F(\alpha,\beta), \tag{1.4}$$

where $\alpha^2 = a$ and $\beta^2 = b$, and where a, b are elements of F. The element β generates an intermediate field—a field $F(\beta)$ between F and K. Since $K = F(\alpha,\beta)$, the requirement that $[K{:}F] = 4$ implies that $F(\beta)$ has degree 2 over F and that α is not in the field $F(\beta)$. So the polynomial $x^2 - a$ is irreducible over $F(\beta)$. Similarly, the polynomial $x^2 - b$ is irreducible over the intermediate field $F(\alpha)$.

Notice that K is an extension of $F(\beta)$ of degree 2, generated by α. Let us apply what we have just learned about quadratic extensions to this extension. Substituting $F(\beta)$ for F, we find that there is an $F(\beta)$-automorphism of K which interchanges the two roots $\pm\alpha$ of $x^2 - a$. Call this automorphism σ. Since it is the identity on $F(\beta)$, σ is also the identity on F, so it is an F-automorphism too. Similarly, there is an $F(\alpha)$-automorphism τ of K which interchanges the roots $\pm\beta$ of $x^2 - b$, and τ is also an F-automorphism.

The two automorphisms we have found operate on the roots α, β as follows:

$$\begin{array}{cc} \alpha \overset{\sigma}{\rightsquigarrow} -\alpha & \alpha \overset{\tau}{\rightsquigarrow} \alpha \\ \beta \overset{\sigma}{\rightsquigarrow} \beta & \beta \overset{\tau}{\rightsquigarrow} -\beta. \end{array} \tag{1.5}$$

Composing these operations, we find that $\sigma\tau$ changes the signs of both roots α, β and that the automorphisms σ^2, τ^2, and $\sigma\tau\sigma\tau$ leave α and β fixed. Since K is generated over F by the roots, these last three automorphisms are all equal to the identity. Therefore the four automorphisms $\{1, \sigma, \tau, \sigma\tau\}$ form a group of order 4, with relations

$$\sigma^2 = 1, \quad \tau^2 = 1, \quad \sigma\tau = \tau\sigma.$$

We have shown that the Galois group $G(K/F)$ contains the Klein four group. In fact it is equal to that group, as we shall see in a moment.

For example, let $F = \mathbb{Q}$, $\alpha = i$, and $\beta = \sqrt{2}$, so that $K = \mathbb{Q}(i, \sqrt{2})$. In this case, the automorphism σ is complex conjugation, while τ sends $\sqrt{2} \rightsquigarrow -\sqrt{2}$, fixing i.

For quadratic or biquadratic extensions, the degree $[K : F]$ is equal to the order of the Galois group $G(K/F)$. We will now state two theorems, Theorems (1.6) and (1.11), which describe the general circumstances under which this happens. These theorems will be proved in later sections of the chapter.

(1.6) **Theorem.** For any finite extension K/F, the order $|G(K/F)|$ of the Galois group divides the degree $[K : F]$ of the extension.

A finite field extension K/F is called a *Galois extension* if the order of the Galois group is equal to the degree:

$$|G(K/F)| = [K : F]. \tag{1.7}$$

Theorem (1.6) shows that the Galois group of a biquadratic extension has order at most 4. Since we already have four automorphisms in hand, there are no others, and the Galois group is the Klein four group, as was asserted. All quadratic and biquadratic extensions are Galois.

If G is a group of automorphisms of a field K, the set of elements of K which are fixed by all the automorphisms in G forms a subfield, called the *fixed field* of G. The fixed field is often denoted by K^G:

$$K^G = \{\alpha \in K \,|\, \varphi(\alpha) = \alpha \text{ for all } \varphi \in G\}. \tag{1.8}$$

One consequence of Theorem (1.6) is that when K/F is a Galois extension, the only elements of K which are fixed by the whole Galois group are the elements of F:

(1.9) **Corollary.** Let K/F be a Galois extension, with Galois group $G = G(K/F)$. The fixed field of G is F.

For let L denote the fixed field. Then $F \subset L$, and this inclusion shows that every L-automorphism of K is also an F-automorphism, that is, that $G(K/L) \subset G$. On the other hand, by definition of the fixed field, every element of G is an L-automorphism. So $G(K/L) = G$. Now $|G| = [K : F]$ because K/F is a Galois extension, and by Theorem (1.6), $|G|$ divides $[K : L]$. Since $F \subset L \subset K$, this shows that $[K : F] = [K : L]$, hence that $F = L$. □

This corollary is important because it provides a method for checking that an element of a Galois extension K is actually in the field F. We will use it frequently.

Being Galois is a strong restriction on a field extension, but nevertheless there are many Galois extensions. This is the key fact which led to Galois' theory. In order to state the theorem which describes the Galois extensions, we need one more definition.

(1.10) **Definition.** Let $f(x) \in F[x]$ be a nonconstant monic polynomial. A *splitting field* for $f(x)$ over F is an extension field K of F such that

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

The second condition just says that K is the smallest extension of F which contains all the roots. The biquadratic extension (1.4) is a splitting field of the polynomial $f(x) = (x^2 - a)(x^2 - b)$.

Every polynomial $f(x) \in F[x]$ has a splitting field. To find one, we choose a field extension L in which f splits into linear factors [Chapter 13 (5.3)] and then take for K the subfield $F(\alpha_1,\ldots,\alpha_n)$ of L generated by the roots.

(1.11) **Theorem.** If K is a splitting field of a polynomial $f(x)$ over F, then K is a Galois extension of F. Conversely, every Galois extension is a splitting field of some polynomial $f(x) \in F[x]$.

(1.12) **Corollary.** Every finite extension is contained in a Galois extension.

To derive this corollary from the theorem, let K/F be a finite extension, let $\alpha_1,\ldots,\alpha_n$ be generators for K over F, and let $f_i(x)$ be the monic irreducible polynomial for α_i over F. We extend K to a splitting field L of the product $f = f_1 \cdots f_n$ over K. Then L will also be a splitting field of f over F. So L is the required Galois extension. □

(1.13) **Corollary.** Let K/F be a Galois extension, and let L be an intermediate field: $F \subset L \subset K$. Then K/L is a Galois extension too.

For, if K is the splitting field of a polynomial $f(x)$ over F, then it is also the splitting field of the same polynomial over the larger field L, so K is a Galois extension of L. □

Let us go back to biquadratic extensions. We can prove that the Galois group of such an extension has order 4 without appealing to Theorem (1.6). All that is needed is the following elementary proposition:

(1.14) **Proposition.**

(a) Let K be an extension of a field F, let $f(x)$ be a polynomial with coefficients in F, and let σ be an F-automorphism of K. If α is a root of $f(x)$ in K, then $\sigma(\alpha)$ is also a root.

(b) Let K be a field extension generated over F by elements $\alpha_1,\ldots,\alpha_r$, and let σ be an F-automorphism of K. If σ fixes each of the generators α_i, then σ is the identity automorphism.

(c) Let K be a splitting field of a polynomial $f(x)$ over F. The Galois group $G(K/F)$ operates faithfully on the set $\{\alpha_1,\ldots,\alpha_n\}$.

Proof. Part (a) was proved in the last chapter [Chapter 13 (2.10)]. To prove part (b), assume that K is generated by $\alpha_1,\ldots,\alpha_n$. Then every element of K can be expressed as a polynomial in $\alpha_1,\ldots,\alpha_n$ with coefficients in F [Chapter 13 (2.6b)]. If σ is an automorphism which is the identity on F and which also fixes each of the elements α_i, then it fixes every polynomial in $\{\alpha_i\}$ with coefficients in F; hence it is the identity. The third assertion (c) follows from the first two: The first tells us that every $\sigma \in G(K/F)$ permutes the set $\{\alpha_1,\ldots,\alpha_n\}$, and the second tells us that the operation on this set is faithful. □

Proposition (1.14) does not address the most interesting question: *Which permutations of the roots of a polynomial extend to automorphisms of the splitting field?* This question is the central theme of Galois theory.

Let us apply Proposition (1.14) to the biquadratic extension (1.4). Part (a), applied to the polynomial $x^2 - a$, shows that any F-automorphism φ of K permutes the roots $\pm\alpha$. Similarly, φ permutes $\pm\beta$. Only four permutations of $\{\pm\alpha, \pm\beta\}$ act in this way. Since the elements α, β generate K, (1.14b) tells us that an F-automorphism which fixes both of them is the identity. So the four automorphisms which we have already found are the only ones. This proves that $G(K/F)$ is the Klein four group.

One of the most important parts of Galois theory is the determination of the *intermediate fields* L, those sandwiched between F and K : $F \subset L \subset K$. The Main Theorem of Galois theory asserts that when K/F is a Galois extension, the intermediate fields are in bijective correspondence with the subgroups of the Galois group. The importance of this correspondence is not immediately clear. We will have to see it used to understand it.

The intermediate field corresponding to a subgroup H of $G(K/F)$ is the fixed field K^H of H, which was defined above. In the other direction, if L is an intermediate field, the Galois group $G(K/L)$ is a subgroup of $G(K/F)$. This is the subgroup which corresponds to L.

(1.15) **Theorem.** *The Main Theorem:* Let K be a Galois extension of a field 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 $F \subset L \subset K$. Its inverse function is

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

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

$$(1.16) \qquad [K:L] = |H|, \quad \text{hence} \quad [L:F] = [G:H].$$

We will prove this theorem in Section 5.

The fields F and K are included among the intermediate fields. The subgroup which corresponds to the field F is the whole group G [see (1.9)], and the one corresponding to K is the trivial subgroup $\{1\}$.

Let us go back to our example of the biquadratic extension $K = \mathbb{Q}(i, \sqrt{2})$, for which σ is complex conjugation, while τ interchanges $\sqrt{2} \rightsquigarrow -\sqrt{2}$. Its Galois group, the Klein four group, has three proper subgroups:

$$H_1 = \{1, \sigma\}, \quad H_2 = \{1, \tau\}, \quad H_3 = \{1, \sigma\tau\}.$$

According to the Main Theorem, there are three proper intermediate fields, namely the fixed fields L_i of these subgroups. They are easily determined:

$$L_1 = \mathbb{Q}(\sqrt{2}), \quad L_2 = \mathbb{Q}(i), \quad \text{and} \quad L_3 = \mathbb{Q}(i\sqrt{2}).$$

A Galois group is finite, so it has finitely many subgroups. But without the Main Theorem, it isn't obvious that there are only finitely many intermediate fields. It might seem natural to expect two randomly chosen elements of a Galois extension K/F to generate different subfields. This tends not to happen, and in fact most elements will generate the whole extension K. The case of the biquadratic extension $K = \mathbb{Q}(i, \sqrt{2})$ will illustrate this point. Let γ be any element of K. The field $\mathbb{Q}(\gamma)$ generated by γ must be one of the intermediate fields we have found. So if γ is not contained in $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, or $\mathbb{Q}(i\sqrt{2})$, then $\mathbb{Q}(\gamma) = K$. Now the set $(1, i, \sqrt{2}, i\sqrt{2})$ is a basis for K over F, so we may write an arbitrary element γ in the form

$$\gamma = c_1 + c_2 i + c_3\sqrt{2} + c_4 i\sqrt{2}, \quad \text{with } c_i \in \mathbb{Q}.$$

This element is not in one of the three proper intermediate fields unless two of the coefficients c_2, c_3, c_4 are zero. The element $i + \sqrt{2}$, for example, generates the whole extension K. We will return to this point in Section 4.

2. CUBIC EQUATIONS

Having examined biquadratic extensions in the last section, we now turn to the next general class of examples, the splitting fields of cubic polynomials. Cubic equations

$$(2.1) \qquad f(x) = x^3 + a_2x^2 + a_1x + a_0 = 0$$

were solved explicitly in terms of square roots and cube roots in the sixteenth century by the mathematicians Tartaglia and Cardano. We will begin by reviewing their remarkable ad hoc solution.

The computation is simpler when the coefficient of degree 2 in $f(x)$ vanishes. The quadratic term in our general equation (2.1) can be eliminated by the substitution

$$(2.2) \qquad x = x_1 - a_2/3.$$

Let us write a cubic whose quadratic term vanishes as

$$(2.3) \qquad f(x) = x^3 + px + q,$$

where the coefficients p, q are elements of the field F. Cardano's solution of the equation $f = 0$ starts with the substitution $x = u - v$. Collecting terms in $f(u - v)$, we find

$$f(u - v) = (u^3-v^3) - (3uv-p)(u-v) + q.$$

The point of replacing the variable x by a sum of variables is that we can now split our equation apart. Clearly, $f(u - v) = 0$ if the two equations

$$3uv - p = 0, \quad u^3 - v^3 + q = 0$$

hold. And since we have two variables, we may hope to obtain solutions to such a pair of equations, though it isn't clear a priori that this will help. We solve the first equation for $v = p/3u$ and substitute into the second. Clearing the denominator gives

$$3^3u^6 - p^3 + 3^3u^3q = 0.$$

Miraculously, this equation is quadratic in u^3. Setting $y = u^3$, it reduces to

$$(2.4) \qquad 3^3y^2 + 3^3qy - p^3 = 0.$$

This equation can be solved by the quadratic formula:

$$(2.5) \qquad y = -\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}.$$

Thus we obtain *Cardano's Formula* $x = u - v$, where

$$(2.6) \qquad u = \sqrt[3]{-\frac{q}{2}+\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}, \quad v = \sqrt[3]{u^3+q} = \sqrt[3]{+\frac{q}{2}+\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}.$$

We will be able to prove the existence of a solution of this general type later, without explicit computation [see (7.6)].

Let us now examine the Galois theory of an irreducible cubic polynomial $f(x)$. We may assume that $f(x)$ has the form (2.3). Let K be a splitting field of $f(x)$ over F, and let $\alpha_1, \alpha_2, \alpha_3$ be the three roots of $f(x)$ in K, ordered in an arbitrary way, so that

$$(2.7) \qquad f(x) = x^3+px+q = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3).$$

Expanding the right side of this equation, we obtain the relations

$$(2.8) \qquad \begin{aligned} \alpha_1 + \alpha_2 + \alpha_3 &= 0 \\ \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3 &= p \\ \alpha_1\alpha_2\alpha_3 &= -q. \end{aligned}$$

The first of these relations shows that the third root α_3 is in the field generated by the first two roots. Thus we have a chain of fields

$$F \subset F(\alpha_1) \subset K,$$

and $K = F(\alpha_1, \alpha_2) = F(\alpha_1, \alpha_2, \alpha_3)$. Let us denote $F(\alpha_1)$ by L. There are two fundamentally different cases which may arise, namely either

$$(2.9) \qquad L = K \quad \text{or} \quad L < K.$$

In terms of the roots, the first case occurs when the last two roots α_2 and α_3 can be expressed in terms of α_1 and elements of F, that is, if they can be written as polynomials in α_1 with coefficients in F [see Chapter 13 (2.6)]. The second case occurs when the last two roots can not be expressed in this way.

For example, let $f(x) = x^3 - 2$. The three roots of this polynomial are $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \zeta\sqrt[3]{2}$, $\alpha_3 = \zeta^2\sqrt[3]{2}$, where $\sqrt[3]{2}$ denotes the real cube root of 2 and $\zeta = e^{2\pi i/3}$. Since α_1 is real, the field $\mathbb{Q}(\alpha_1)$ is contained in $\mathbb{R}$. It doesn't contain the other two roots, which are complex. Hence if $F = \mathbb{Q}$ and $L = \mathbb{Q}(\alpha_1)$, we are in the second case. On the other hand, if we let $F = \mathbb{Q}(\zeta)$, then $F(\alpha_1)$ contains α_2, so we are in the first case.

To analyze the dichotomy (2.9), we consider the way the irreducible polynomial $f(x)$ factors in the field L. By assumption, $f(x)$ is irreducible in $F[x]$, and it factors into linear factors in $K[x]$. In the ring $L[x]$, $f(x)$ has the factor $(x - \alpha_1)$:

$$(2.10) \qquad f(x) = (x - \alpha_1)h(x),$$

where $h(x)$ is a quadratic polynomial with coefficients in L. Division by $x - \alpha_1$ gives the same result if it is carried out in the larger field K. Looking at (2.7), we see that $h(x) = (x - \alpha_2)(x - \alpha_3)$ in $K[x]$. Therefore $L < K$ if and only if $h(x)$ is irreducible over L. In this case, the degree of $L(\alpha_2) = K$ over L is 2. Also, since we assume $f(x)$ irreducible over F, $[L : F] = 3$ in either case. So we have

$$(2.11) \qquad [K : F] = \begin{cases} 3 \text{ if } L = K \\ 6 \text{ if } L < K \end{cases}.$$

(2.12) **Example.** The polynomial $f(x) = x^3 + 3x + 1$ is irreducible over $\mathbb{Q}$, and it has only one real root. To see that there is only one real root, we note that the derivative of f does not vanish on the real line. Therefore $f(x)$ defines an increasing function of the real variable x. It takes the value 0 only once. The real root does not generate the splitting field K, which also contains two complex roots. So $[K : \mathbb{Q}] = 6$ in this case.

On the other hand, the splitting field of the polynomial $f(x) = x^3 - 3x + 1$ over $\mathbb{Q}$ has degree 3. One of its roots is $\eta_1 = 2 \cos 2\pi/9 = \zeta + \zeta^8$, where $\zeta = e^{2\pi i/9}$. Having the polynomial in hand, we can check this directly. But actually, we made this example by computing the irreducible polynomial for η_1 over $\mathbb{Q}$. The way to compute this polynomial is to guess its other roots. We note that η_1 is the sum of a ninth root of 1 and its inverse. There are two other sums of this sort: $\eta_2 = \zeta^2 + \zeta^7$ and $\eta_3 = \zeta^4 + \zeta^5$. We guess that these are the other roots and expand $(x - \eta_1)(x - \eta_2)(x - \eta_3)$, obtaining f. In this example, η_2 happens to be equal to ${\eta_1}^2 - 2$, and $\eta_3 = -\eta_1 - \eta_2$. So $K = F(\eta_1)$. □

We go back to a general cubic equation. According to Theorem (1.11), the order of the Galois group $G = G(K/F)$ is the degree of the field extension $[K : F]$. For cubic equations, this degree determines the group G completely. Namely, Proposition (1.14) tells us that G operates faithfully on the set $\{\alpha_1, \alpha_2, \alpha_3\}$ of roots. These roots are distinct [Chapter 13 (5.8)]. So G is a subgroup of the symmetric group S_3, which has order 6. If $[K : F] = 6$, then G is the whole symmetric group. In this case any permutation of the roots is realized by an F-automorphism of K. On the other hand, the only subgroup of S_3 of order 3 is the alternating group A_3, a cyclic group. So if $[K : F] = 3$, then $G = A_3$. In this case the cyclic permutations and the identity are the only ones which extend to F-automorphisms. Thus the roots of an irreducible cubic polynomial may have either dihedral or cyclic symmetry. But these symmetries are algebraic; they will not be symmetries of K when this field is viewed as a set of points in the complex plane.

Let us determine the intermediate fields in the case that the degree $[K : F]$ is 6. (There are no intermediate fields properly between F and K when $[K : F] = 3$.) The symmetric group S_3 has three conjugate subgroups of order 2 and one subgroup, A_3, of order 3. There are three obvious intermediate fields: $F(\alpha_1), F(\alpha_2), F(\alpha_3)$. They are isomorphic but not equal subfields of K, and they correspond to the three subgroups of order 2. But the intermediate field which corresponds to the subgroup A_3 is not obvious. Let us denote this mystery field by L. According to the Main Theorem, $G(K/L) = A_3$. Hence $[K : L] = 3$ and $[L : F] = 2$. So L is a quadratic extension of F, which can be obtained by adjoining a square root. The Main Theorem has told us an interesting fact: K contains the square root δ of an element of F. And since there is only one intermediate extension of degree 2, this square root is essentially unique. The Main Theorem also tells us that L is the fixed field of the subgroup A_3. So an even permutation of the roots leaves δ fixed, while an odd permutation does not. The required element is

$$\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3). \tag{2.13}$$

A permutation of the roots multiplies δ by the sign of the permutation. Hence δ is not fixed by all elements of $G(K/F) = S_3$, so $\delta \not\in F$. But δ^2 is fixed by every permutation. Corollary (1.9) tells us that $\delta^2 \in F$.

For any cubic polynomial $f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$, the element

$$D = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2 \tag{2.14}$$

is called the *discriminant* of the polynomial. It is an element of the field F which is zero if and only if two roots of $f(x)$ are equal. So it is analogous to the discriminant of the quadratic polynomial $x^2 + bx + c = (x - \alpha_1)(x - \alpha_2)$, which is $b^2 - 4c = (\alpha_1 - \alpha_2)^2$. If the cubic f is irreducible, then its roots are distinct, hence $D \neq 0$.

The fact that the discriminant of the cubic polynomial is an element of F follows from Corollary (1.9), but it is not trivial. We will prove it abstractly in the next section, but it can also be checked by direct calculation. Using formulas (2.8), we can compute the discriminant in terms of the coefficients p, q. It is

$$D = -4p^3 - 27q^2. \tag{2.15}$$

(2.16) **Proposition.** The discriminant of an irreducible cubic polynomial $f(x) \in F[x]$ is a square in F if and only if the degree of the splitting field is 3.

If we choose a polynomial with integer coefficients at random, the chances are good that its discriminant will not be a square in $\mathbb{Q}$. For example, the discriminant of $x^3 + 3x + 1$ is -135. On the other hand, the discriminant of $x^3 - 3x + 1$ is 81, a square. This agrees with the fact that $[K : F] = 3$ [see (2.12)].

Proof of the Proposition. If D is not a square, then $\delta \not\in F$, and therefore $[F(\delta) : F] = 2$. Since $\delta \in K$, $[K : F]$ is divisible by 2, hence by (2.11), $[K : F] =$

6. On the other hand, if $\delta \in F$, then every element of the Galois group $G = G(K/F)$ fixes δ. Since odd permutations change the sign of δ, they are not in G, and hence $G \neq S_3$. Therefore $[K : F] = 3$. □

How could such a proposition be true? There must be a formula which expresses the second root α_2 in terms of the elements α_1, δ, and the coefficients p, q. This formula exists, and it is instructive to compute it explicitly.

3. SYMMETRIC FUNCTIONS

Galois theory is concerned with the problem of determining those permutations of the roots of a polynomial which extend to field automorphisms. In this section we examine a simple situation in which every permutation extends, namely when the roots are independent variables.

Let R be any ring, and consider the polynomial ring $R[u_1,\dots,u_n]$ in n variables u_i. A permutation σ of $\{\mathbf{1},\dots,\mathbf{n}\}$ can be made to operate on polynomials, by permuting the variables. We must decide here how we want permutations to operate. Let us keep automorphisms on the left. Then σ operates by the inverse permutation on the indices:

$$(3.1) \qquad f = f(u_1,\dots,u_n) \overset{\sigma}{\rightsquigarrow} f(u_{1\sigma^{-1}},\dots,u_{n\sigma^{-1}}) = \sigma f.$$

This is clearly an automorphism of $R[u]$. Since it acts as the identity on R, σ is called an *R-automorphism*. So the symmetric group S_n operates by R-automorphisms on the polynomial ring $R[u]$. A polynomial is called *symmetric* if it is left fixed by all permutations.

It is easy to describe the symmetric polynomials. In order for g to be symmetric, two monomials in $\{u_1,\dots,u_n\}$ which differ by a permutation of the indices, such as $u_1{}^2u_2$ and $u_2{}^2u_3$, must have the same coefficients in g. A symmetric polynomial which involves a given monomial must include the whole orbit. Thus

$$g(u) = (u_1{}^3+u_2{}^3+u_3{}^3) + 5(u_1{}^2u_2+u_1{}^2u_3+u_2{}^2u_3+u_2{}^2u_1+u_3{}^2u_2+u_3{}^2u_1) - u_1u_2u_3$$

is a symmetric polynomial of degree 3 in three variables.

There are n special symmetric polynomials with integer coefficients, called the *elementary symmetric functions* s_i:

$$(3.2) \qquad \begin{aligned} s_1 &= u_1 + u_2 + \cdots + u_n \\ s_2 &= u_1u_2 + u_1u_3 + \cdots + u_{n-1}u_n = \sum_{i<j} u_iu_j \\ s_3 &= \sum_{i<j<k} u_iu_ju_k \\ &\ \vdots \\ s_n &= u_1u_2\cdots u_n. \end{aligned}$$

They are the coefficients of the polynomial $(x-u_1)(x-u_2)\cdots(x-u_n)$ when it is expanded as a polynomial in x:

(3.3) $p(x) = (x-u_1)(x-u_2)\cdots(x-u_n) = x^n - s_1x^{n-1} + s_2x^{n-2} - \cdots \pm s_n.$

We have reversed the order of the indices and alternated the sign here. The coefficients s_i are symmetric because $p(x)$ is symmetric with respect to permutation of the indices.

The main theorem on symmetric functions asserts that the elementary symmetric functions generate the ring of all symmetric polynomials:

(3.4) **Theorem.** Every symmetric polynomial $g(u_1,\ldots,u_n) \in R[u]$ can be written in a unique way as a polynomial in the elementary symmetric functions $s_1,\ldots,s_n$. In other words, let $z_1,\ldots,z_n$ be variables. For each symmetric polynomial $g(u)$, there is a unique polynomial $\varphi(z_1,\ldots,z_n) \in R[z_1,\ldots,z_n]$ such that

$$g(u_1,\ldots,u_n) = \varphi(s_1,\ldots,s_n).$$

The proof of this theorem is at the end of the section.

For example,

$$u_1^2 + \cdots + u_n^2 = s_1^2 - 2s_2. \tag{3.5}$$

The *discriminant* of the polynomial $p(x)$ (3.3), defined to be

$$\begin{aligned} D &= (u_1-u_2)^2(u_1-u_3)^2\cdots(u_{n-1}-u_n)^2 \\ &= \prod_{i<j}(u_i-u_j)^2 = \pm\prod_{i\neq j}(u_i-u_j), \end{aligned} \tag{3.6}$$

is perhaps the most important symmetric polynomial. Both of the last two expressions for the discriminant are convenient at times, so it is unfortunate that they may differ by a sign. To go from the second expression for D to the last one requires $\frac{1}{2}n(n-1)$ sign changes, so the correct sign to replace the symbol ± is

$$(-1)^{n(n-1)/2}. \tag{3.7}$$

It is clear that D is a symmetric polynomial with integer coefficients. So Theorem (3.4) tells us that it can be written as an integer polynomial in the elementary symmetric functions. In other words, there exists a polynomial

$$\Delta(z_1,\ldots,z_n) \in \mathbb{Z}[z_1,\ldots,z_n] \tag{3.8}$$

so that $D = \Delta(s_1,\ldots,s_n)$. Unfortunately, this expression for D in terms of the elementary symmetric functions is very complicated. I don't know what it is for $n > 3$.

We can compute the discriminant for $n = 2$ easily:

$$(u_1-u_2)^2 = s_1^2 - 4s_2. \tag{3.9}$$

This is the familiar formula for the discriminant of the quadratic polynomial $p(x) = x^2 - s_1x + s_2$. When $n = 3$, the expression for the discriminant is already too complicated to remember:

(3.10)
$$(u_1 - u_2)^2(u_1 - u_3)^2(u_2 - u_3)^2 = s_1^2s_2^2 - 4s_2^3 - 4s_1^3s_3 - 27s_3^2 + 18s_1s_2s_3.$$

It is important to note that such an expression is an *identity* in $\mathbb{Z}[u_1,\ldots,u_n]$. It remains true when substitutions are made for the variables u_i. If we are given particular elements $\{\alpha_1,\ldots,\alpha_n\}$ in a ring R, we can expand the polynomial obtained by substituting α_i for u_i in $p(x)$:

$$(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n) = x^n - b_1x^{n-1} + b_2x^{n-2} - \cdots \pm b_n.$$

The indices and the signs have been adjusted to agree with (3.3). Then

$$b_i = s_i(\alpha_1,\ldots,\alpha_n),$$

and

$$\prod_{i<j}(\alpha_i - \alpha_j)^2 = \Delta(b_1,\ldots,b_n).$$

This follows by substitution of α_i for u_i.

It is also important that the expression of a symmetric polynomial in terms of the elementary symmetric functions is unique:

(3.11) **Corollary.** There are no polynomial relations among the elementary symmetric functions $s_1,\ldots,s_n$. Equivalently, the subring $R[s_1,\ldots,s_n]$ of $R[u]$ generated by $\{s_i\}$ is isomorphic to the polynomial ring $R[z_1,\ldots,z_n]$ in n variables.

This is a restatement of the uniqueness in Theorem (3.4). □

The corollary can be used in the following way: Let

(3.12)
$$f(x) = x^n - a_1x^{n-1} + a_2x^{n-2} - \cdots \pm a_n$$

be a polynomial with coefficients in a ring R. We define the *discriminant* of $f(x)$ to be the element $\Delta(a_1,\ldots,a_n)$ of R, where $\Delta(z_1,\ldots,z_n)$ is the polynomial (3.8). Since this polynomial is unique, the discriminant is defined, whether the polynomial is a product of linear factors in $R[x]$ or not.

For example, let $n = 3$. Then formula (3.10) shows that

(3.13)
$$\Delta(0, p, -q) = -4p^3 - 27q^2,$$

which agrees with the formula (2.15) for the discriminant of the cubic polynomial $x^3 + px + q$.

We can use undetermined coefficients to compute the expression of a symmetric polynomial in terms of the elementary symmetric functions. To apply this method, we notice that the elementary symmetric function s_i has degree i in the variables u. That is why we chose the index i for it. So we assign the *weight* i to the variable z_i, and we define the *weighted degree* of a monomial $z_1^{e_1}z_2^{e_2}\cdots z_n^{e_n}$ to be

$$e_1 + 2e_2 + \cdots + ne_n. \tag{3.14}$$

Substitution of s_i for z_i into a polynomial of weighted degree d in z yields a polynomial of (ordinary) degree d in $u_1,\dots,u_n$.

For example, to compute the discriminant of a cubic polynomial in terms of the elementary symmetric functions, we notice that its degree in u is 6. There are seven monomials in z_1, z_2, z_3 of weighted degree 6:

$$z_1^6,\ z_1^4z_2,\ z_1^3z_3,\ z_1^2z_2^2,\ z_1z_2z_3,\ z_2^3,\ z_3^2. \tag{3.15}$$

So D is a linear combination of these monomials. To compute its coefficients, we evaluate D on some special polynomials: Setting $f(x) = x^2(x-1)$, we get $D = 0$, $s_1 = 1$, and $s_2 = s_3 = 0$. Since the only one of the monomials (3.15) which does not involve z_2 or z_3 is z_1^6, the coefficient of z_1^6 in the discriminant is zero. The coefficients of z_2^3 and z_3^2 can be computed using the special polynomials $x^3 - x$ and $x^3 - 1$, for example.

Proof of Theorem (3.4). Let's warm up by working out the case of the symmetric polynomial

$$f(x) = u_1^2u_2 + u_1^2u_3 + u_2^2u_1 + u_2^2u_3 + u_3^2u_1 + u_3^2u_2$$

as an example. To analyze it, our first step is to set $u_3 = 0$. We obtain a symmetric polynomial $f^0 = u_1^2u_2 + u_2^2u_1$ in the remaining variables u_1, u_2. Let us denote the elementary symmetric functions in u_1, u_2 by $s_1^0 = u_1 + u_2$ and $s_2^0 = u_1u_2$. We notice that $f^0 = s_1^0s_2^0$.

The second step is to compare f with the polynomial s_1s_2 in three variables. We compute the polynomial $f - s_1s_2$, where $s_1 = u_1 + u_2 + u_3$ and $s_2 = u_1u_2 + u_1u_3 + u_2u_3$, finding that

$$f - s_1s_2 = -3u_1u_2u_3.$$

We recognize this polynomial as $-3s_3$. So $f = s_1s_2 - 3s_3$.

The general case is similar. There is nothing to show when $n = 1$, because $u_1 = s_1$ in that case. Proceeding by induction, we assume the theorem proved for $n-1$ variables. Given a symmetric polynomial f in $u_1,\dots,u_n$, we consider the polynomial f^0 obtained by substituting zero for the last variable: $f^0(u_1,\dots,u_{n-1}) = f(u_1,\dots,u_{n-1},0)$. We note that f^0 is a symmetric polynomial in $u_1,\dots,u_{n-1}$. By the induction hypothesis, f^0 may be expressed as a polynomial in the elementary symmetric functions in $\{u_1,\dots,u_{n-1}\}$, which we denote by

$$s_1^0 = u_1 + \cdots + u_{n-1}, \dots, s_{n-1}^0 = u_1\cdots u_{n-1}.$$

So we can write $f^0 = g(s_1^0,\dots,s_{n-1}^0)$. Moreover, it follows from the defintion of the polynomials s_i that

$$s_i^0 = s_i(u_1,\dots,u_{n-1},0), \quad \text{if } i = 1,\dots,n-1.$$

Consider the polynomial

$$p(u_1,\dots,u_n) = f(u_1,\dots,u_n) - g(s_1,\dots,s_{n-1}),$$

as a polynomial in $u_1,\dots,u_n$. Being a difference of symmetric polynomials, this polynomial is symmetric. Also, it has the property that $p(u_1,\dots,u_{n-1},0) = 0$. Therefore every monomial occurring in p is divisible by u_n. By symmetry, p is divisible by u_i for every i, and hence it is divisible by s_n. So

$$(3.16) \qquad f(u_1,\dots,u_n) = g(s_1,\dots,s_{n-1}) + s_n h(u_1,\dots,u_n),$$

for some symmetric polynomial h. We now work on $h(u_1,\dots,u_n)$. By induction on the degree, h is a polynomial in the symmetric functions, and hence so is f.

It remains to prove the uniqueness of $\varphi(s_1,\dots,s_n)$. The uniqueness means that there is only one polynomial $\varphi(z_1,\dots,z_n)$ in the variables z_i, such that $\varphi(s_1,\dots,s_n) = f(u_1,\dots,u_n)$, as polynomials in $u_1,\dots,u_n$. In other words, the kernel of the substitution map

$$\sigma\colon R[z] \longrightarrow R[u]$$

sending $z_i \rightsquigarrow s_i$ is zero. To show this, suppose $\varphi(s_1,\dots,s_n) = 0$ for some $\varphi \in R[z]$. Setting $u_n = 0$ in this expression we still get zero: $\varphi(s_1{}^0,\dots,s_{n-1}{}^0,0) = 0$. By induction on n, this implies that $\varphi(z_1,\dots,z_{n-1},0) = 0$. Therefore z_n divides $\varphi(z)$, and we may write $\varphi(z) = z_n\psi(z)$. Then $0 = \varphi(s) = s_n\psi(s) = u_1\cdots u_n\psi(s)$. Since the product $u_1\cdots u_n$ is not a zero-divisor in the polynomial ring $R[u]$, $\psi(s) = 0$. The polynomial $\psi(z)$ has lower total degree in z than $\varphi(z)$, so we may apply induction on the degree to conclude that $\psi = 0$. Hence $\varphi = 0$ too. □

Now suppose that $R = F$ is a field. Then we may also consider the field of rational functions in the variables u_i, that is, the field of fractions of $F[u_1,\dots,u_n]$. The symmetric group also acts on this field, and the corresponding assertion is true:

(3.17) **Theorem.** Every symmetric rational function is a rational function in $s_1,\dots,s_n$.

Proof. Let $r(u) = f(u)/g(u)$ be a symmetric rational function, where $f, g \in F[u]$. We can build a symmetric function from g by multiplying all the σg together:

$$G = \prod_{\sigma\in S_n} \sigma g$$

is a symmetric polynomial. Then $G(u)r(u)$ is a symmetric rational function, and it is also a polynomial in $\{u_1,\dots,u_r\}$—a symmetric polynomial. By Theorem (3.4), $G(u)$ and $G(u)r(u)$ are polynomials in the elementary symmetric functions $\{s_i\}$. Thus $r(u)$ is a rational function in $\{s_i\}$. □

The pair of fields

$$(3.18) \qquad F(s) = F(s_1,\dots,s_n) \subset F(u_1,\dots,u_n) = F(u)$$

is an example of a Galois extension. This follows from Theorem (1.11), because $F(u)$ is a splitting field of the polynomial $p(x)$ (3.3) and because the roots $u_1, \ldots, u_n$ are distinct. By Proposition (1.14), the Galois group $G = G(F(u)/F(s))$ operates faithfully on the roots. On the other hand, G contains the full symmetric group, by construction. Therefore $G = S_n$. As a corollary, we find that $[F(u) : F(s)] = n!$. Needless to say, this can be proved directly.

4. PRIMITIVE ELEMENTS

At the end of the first section, we saw that generically chosen elements of a biquadratic extension K/F generate K. It is possible to derive a general statement of this type as a corollary of the Main Theorem of Galois theory. But we are going to prove it directly instead, and then use this fact in the proof of the Main Theorem.

(4.1) **Theorem.** *Existence of a primitive element:* Let K be a finite extension of a field F of characteristic zero. There is an element $\gamma \in K$ such that $K = F(\gamma)$.

An element γ which generates a field extension K/F is called a *primitive element* for K over F. So the theorem can be restated by saying that every finite extension K of a field F has a primitive element. We have restated our general hypothesis that F has characteristic zero here because this theorem is not true for fields of characteristic p.

Proof of Theorem (4.1). We use induction on the number of generators of K. Say that $K = F(\alpha_1, \ldots, \alpha_n)$. If $n = 1$, there is nothing to prove. For $n > 1$, the induction principle allows us to assume the theorem true for the intermediate field $K_1 = F(\alpha_1, \ldots, \alpha_{n-1})$. So we may assume that K_1 is generated by a single element β. Then $K = K_1(\alpha_n) = F(\beta, \alpha_n)$. We have to show that this field has a primitive element. We are thereby reduced to the case that $n = 2$, so that K is generated by two elements α, β.

Let $f(x), g(x)$ be the irreducible polynomials for α, β over F, and let K' be an extension of K in which f and g split completely [Chapter 13 (5.3)]. Call their roots $\alpha = \alpha_1, \ldots, \alpha_m$ and $\beta = \beta_1, \ldots, \beta_n$. By Chapter 13 (5.8), the elements α_i are distinct.

We are going to show that for most choices of $c \in F$, the linear combination $\gamma = \beta + c\alpha$ generates K. Let us denote the field $F(\gamma)$ by L. It suffices to show that $\alpha \in L$, because if so, then $\beta = \gamma - c\alpha$ will be in L too, and this will imply that $L = K$. The way we show that α is in L is indirect: We determine its irreducible polynomial over L. As we know, this is the monic polynomial of least degree in $L[x]$ which has α as a root.

To begin with, α is a root of $f(x)$. The trick is to use the polynomial $g(x)$ to cook up a second polynomial with the root α, namely $h(x) = g(\gamma - cx)$. Notice that $h(x)$ has coefficients in L and that $h(\alpha) = 0$. If we show that the greatest common divisor of f and h in $L[x]$ is $x - \alpha$, then it will follow that $-\alpha$, being one of the coefficients of $x - \alpha$, is in L. Now the monic greatest common divisor of f and h is the same, whether computed in $L[x]$ or in $K'[x]$ [Chapter 13 (5.4)]. So we may make our computation in $K'[x]$. In that ring, f is a product of the linear factors $x - \alpha_i$, and it suffices to show that none of them divides h, that is, that none of the elements α_i, except for $\alpha = \alpha_1$ itself, is a root of $h(x)$. Having gotten this far, the rest is just a matter of computing the roots of h.

Since the roots of g are β_j, the roots of $h(x) = g(\gamma - cx)$ are obtained by solving the equations

$$\gamma - cx = \beta_j$$

for x. Since $\gamma = \beta + c\alpha$, the roots are $(\gamma - \beta_j)/c = (\beta - \beta_j)/c + \alpha$. We want these roots to be different from α_i, $i \neq 1$. This will be so provided that c does not take one of the finitely many values

$$-\frac{\beta_j - \beta}{\alpha_i - \alpha}, \tag{4.2}$$

with $i, j \neq 1, 1$. □

(4.3) **Example.** Consider the field $K = \mathbb{Q}[i, \sqrt[3]{2}]$. This field has degree 6 over $\mathbb{Q}$ [see Chapter 13 (3.5d)]. In the notation of the previous proof, we have $\beta_1 = i$, $\beta_2 = -i$, and $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \zeta\sqrt[3]{2}$, $\alpha_3 = \zeta^2\sqrt[3]{2}$, where $\zeta = e^{2\pi i/3}$. Condition (4.2) becomes

$$\sqrt[3]{2}c \neq -\frac{\pm i - i}{\zeta^\nu - \zeta}, \quad \nu = 1, 2.$$

This condition holds for all $c \in \mathbb{Q}$ except $c = 0$. Therefore $\gamma = i + c\sqrt[3]{2}$ generates K over $\mathbb{Q}$ for all rational numbers $c \neq 0$. Of course, many other combinations of the two elements β, α will generate $F(\beta, \alpha)$. In this example, the product $i\sqrt[3]{2}$ also generates K. □

Theorem (4.1) is important for two reasons. First, explicit computation in an extension of the form $F(\gamma)$ is easy if the irreducible equation for γ over F is known. Second, since finite extensions have the form $F(\gamma)$, we can derive their properties from facts about algebraic elements. It is this aspect which is most important for us.

The power of Theorem (4.1) is shown by applying it to the study of automorphisms of fields. Consider a finite group G of automorphisms of the field K, and denote its fixed field K^G by F.

(4.4) **Proposition.** Let G be a finite group of automorphisms of a field K, and let F be its fixed field. Let $\{\beta_1, \ldots, \beta_r\}$ be the orbit of an element $\beta = \beta_1 \in K$ under the action of G. Then β is algebraic over F, its degree over F is r, and its irreducible polynomial over F is $g(x) = (x - \beta_1) \cdots (x - \beta_r)$.

Note that the degree of β, being the order of an orbit, divides the order of the group.

Proof. Let $f(x)$ be the irreducible polynomial for β over F. Since $f(x)$ is fixed by G, each of the elements β_i is a root of f (1.14), and so g divides f. Also, g is fixed by all permutations of $\{\beta_1,\dots,\beta_r\}$, and hence by the operation of G, which permutes the orbit. Therefore $g(x) \in F[x]$. Since f is irreducible, $g = f$. □

This proposition provides a method for determining the irreducible polynomial for an element β of a Galois extension K over F. For example, let K be the biquadratic extension $\mathbb{Q}(i, \sqrt{2})$, and let $\beta = i + \sqrt{2}$. The Galois group of $K/\mathbb{Q}$ is the Klein four group, and the orbit of β consists of the four elements $\pm i \pm \sqrt{2}$. So the irreducible polynomial for β over $\mathbb{Q}$ is

$$(x - i - \sqrt{2})(x - i + \sqrt{2})(x + i - \sqrt{2})(x + i + \sqrt{2})$$
$$= (x^2 - 2ix - 3)(x^2 + 2ix - 3) = x^4 - 2x^2 + 9.$$

We can also determine this polynomial by computing powers of β and finding the linear relation of smallest degree between them (see Chapter 13, Section 3). However, the method given here is preferable because it always produces an irreducible polynomial.

(4.5) **Corollary.** Let K/F be a Galois extension, and let $g(x)$ be an irreducible polynomial in $F[x]$. If g has one root in K, then it factors into linear factors in $K[x]$.

Proof. According to Corollary (1.9), F is the fixed field of the Galois group $G = G(K/F)$. Let β be a root of $g(x)$ in K. By Proposition (4.4), the irreducible polynomial for β over F is $(x - \beta_1)\cdots(x - \beta_r)$, where $\{\beta_1,\dots,\beta_r\}$ is the G-orbit of β. Since $g(x)$ is the irreducible polynomial for β, it is equal to this product, so it factors into linear factors in K, as asserted. □

The corollary tells us in particular that every Galois extension is a splitting field, which is part of Theorem (1.11). For, take any generators $\alpha, \beta, \dots$ for K over F, and let $f(x)$ be the product of their irreducible polynomials. Then f splits completely in K, and hence K is a splitting field for f.

(4.6) **Theorem.** Let G be a group of order n of automorphisms of a field K, and let F be its fixed field. Then $[K : F] = n$.

Proof. Proposition (4.4) shows that every element β 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 field extension K/F is bounded by n too. To see this, we form a chain of extension fields as follows: We choose an element $\alpha_1 \in K$ which is not in F, and we set $F_1 = F(\alpha_1)$. Then $[F_1 : F] \le n$. If $F_1 \ne K$, we choose an element $\alpha_2 \in K$ which is not in F_1, and we set $F_2 = F(\alpha_1, \alpha_2)$. By the theorem of the primitive element, F_2 is generated by a single element γ, and by Corollary (3.6) of

Chapter 13, the degree of γ over F is bounded by n. So $[F_2 : F] \leq n$. Continuing in this way, we obtain a chain $F < F_1 < F_2 \ldots$ in which $[F_i : F] \leq n$ for all i. This chain must be finite. So $F_i = K$ for some i, and $[K : F] \leq n$.

Applying Theorem (4.1) once more, we conclude that K has a primitive element: $K = F(\beta)$. Any element of G which fixes β acts as the identity on $K = F(\beta)$. Since we are assuming that G is a group of automorphisms of K, the identity is the only such element. Therefore the stabilizer of β is $\{1\}$, and the orbit has order n. By Proposition (4.4), β has degree n over F, and $[K : F] = n$. □

Using the theorem we have just proved, we can derive the first theorem, Theorem (1.6), which was stated in Section 1. That theorem says that for any finite extension K/F, the order of its Galois group divides its degree. To prove this, we set $G = G(K/F)$. Then G operates on K, so by Theorem (4.6), $|G| = [K : K^G]$. And since $F \subset K^G \subset K$, $[K : K^G]$ divides $[K : F]$. □

Theorem (4.6) also provides us with a converse to Corollary (1.9):

(4.7) **Corollary.** Let G be a finite group of automorphisms of a field K, and let F be its fixed field. Then K is a Galois extension of F, and its Galois group is G.

Proof. By definition of the fixed field, the elements of G are F-automorphisms of K. Hence $G \subset G(K/F)$. Since $|G(K/F)| \leq [K : F]$ and $[K : F] = |G|$, it follows that $|G(K/F)| = [K : F]$ and that $G = G(K/F)$. □

We can get some interesting examples to illustrate Proposition (4.4) and Theorem (4.6) by considering automorphisms of the field $\mathbb{C}(y) = K$ of rational functions in y. For instance, let σ, τ be the automorphisms of K defined by $y \rightsquigarrow -y$ and $y \rightsquigarrow iy^{-1}$. The automorphisms $\{1, \sigma, \tau, \sigma\tau\}$ form a group G of order 4.

(4.8) **Proposition.** Let K and G be as above. The fixed field $F = K^G$ is the field $\mathbb{C}(w)$ of rational functions in $w = y^2 - y^{-2}$.

In other words, every rational function $f(y)$ which is fixed by σ can be expressed as a rational function in w.

Proof. First of all, G does fix $w = y^2 - y^{-2}$, so w is in the fixed field. Therefore the fixed field F contains the field $\mathbb{C}(w)$. Next, we compute the irreducible polynomial for y over F. The orbit of y is $\{y, iy^{-1}, -y, -iy^{-1}\}$, so Proposition (4.4) tells us that the irreducible equation for y is $(x - y)(x - iy^{-1})(x + y)(x + iy^{-1}) = x^4 - wx^2 - 1$. This polynomial has coefficients in $\mathbb{C}(w)$, so y has degree 4 over that field. It follows that $[K : \mathbb{C}(w)] = 4$. On the other hand, $\mathbb{C}(w) \subset F \subset K$, and since $|G| = 4$, Theorem (4.6) tells us that $[K : F] = 4$. Counting degrees shows that $\mathbb{C}(w) = F$. □

A famous theorem called *Lüroth's theorem* asserts that any subfield of the field $\mathbb{C}(y)$ which properly contains the complex numbers is the field of rational functions in some rational function w of y.

5. PROOF OF THE MAIN THEOREM

Let $f(x)$ be a monic polynomial of degree n with coefficients in a field F. We recall that a splitting field of $f(x) \in F[x]$ is a field of the form $K = F(\alpha_1, \dots, \alpha_n)$, such that $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ in $K[x]$. The existence of a splitting field was proved in Chapter 13 (5.3). We now want to show that any two splitting fields of a given polynomial $f(x)$ are isomorphic. This follows from the fact that a field extension of the form $F(\alpha)$ is determined by the irreducible polynomial for α over F, and from some "bookkeeping." The bookkeeping required for the proof is notationally a little confusing, but not difficult.

Any isomorphism $\varphi: F \longrightarrow \tilde{F}$ of fields extends to an isomorphism $F[x] \longrightarrow \tilde{F}[x]$ between the polynomial rings by

$$a_n x^n + \cdots + a_0 \rightsquigarrow \tilde{a}_n x^n + \cdots + \tilde{a}_0,$$

where $\tilde{a}_i = \varphi(a_i)$. Let us denote the image of $f(x)$ by $\tilde{f}(x)$. Since φ is an isomorphism, $\tilde{f}(x)$ will be an irreducible polynomial if and only if $f(x)$ is irreducible.

The following lemma generalizes Chapter 13 (2.9).

(5.1) **Lemma.** With the above notation, let $f(x)$ be an irreducible polynomial in $F[x]$. Let α be a root of $f(x)$ in an extension field K of F, and let $\tilde{\alpha}$ be a root of $\tilde{f}(x)$ in an extension $\tilde{K}$ of $\tilde{F}$. There is a unique isomorphism

$$\varphi_1 : F(\alpha) \longrightarrow \tilde{F}(\tilde{\alpha})$$

which restricts to φ on the subfield F, and which sends α to $\tilde{\alpha}$.

Proof. We know that $F(\alpha)$ is isomorphic to the quotient $F[x]/(f)$, and similarly $\tilde{F}(\tilde{\alpha})$ is isomorphic to $\tilde{F}[x]/(\tilde{f})$. The rings $F[x]$ and $\tilde{F}[x]$ are isomorphic, as we just saw, and since f and $\tilde{f}$ correspond under this isomorphism, so do the ideals (f) and $(\tilde{f})$ which they generate. Therefore the residue rings $F[x]/(f)$ and $\tilde{F}[x]/(\tilde{f})$ are also isomorphic. Combining these isomorphisms yields the required isomorphism φ_1. This extension of φ is unique because α generates $F(\alpha)$ over F. □

(5.2) **Proposition.** Let $\varphi: F \longrightarrow \tilde{F}$ be an isomorphism of fields. Let $f(x)$ be a nonconstant polynomial in $F[x]$, and let $\tilde{f}(x)$ be the corresponding polynomial in $\tilde{F}[x]$. Let K and $\tilde{K}$ be splitting fields for $f(x)$ and $\tilde{f}(x)$. There is an isomorphism $\psi: K \longrightarrow \tilde{K}$ which restricts to φ on the subfield F of K.

If we let $F = \tilde{F}$ and $\varphi =$ identity, we obtain the following corollary:

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

The corollary is the result we are really after. The auxiliary isomorphism φ is introduced into the proposition to make the induction step of the proof work.

Proof of Proposition (5.2). If $f(x)$ factors into linear factors over F, then $\tilde{f}(x)$ also factors into linear factors. In this case $K = F$ and $\tilde{K} = \tilde{F}$, so $\varphi = \psi$. Assume that f does not split completely. Choose an irreducible factor $g(x)$ of $f(x)$ of degree >1. The corresponding polynomial $\tilde{g}(x)$ will be an irreducible factor of $\tilde{f}(x)$. Let α be a root of g in K and write $F_1 = F(\alpha)$. Make a similar choice of $\tilde{\alpha}$ and $\tilde{F}_1 = \tilde{F}(\tilde{\alpha})$ in $\tilde{K}$. Then by Lemma (5.1), we can extend φ to an isomorphism $\varphi_1: F_1 \longrightarrow \tilde{F}_1$ which sends $\alpha \rightsquigarrow \tilde{\alpha}$. Being a splitting field for f over F, K is also a splitting field of f over the larger field F_1, and similarly $\tilde{K}$ is a splitting field for $\tilde{f}$ over $\tilde{F}_1$. Therefore we may replace $F, \tilde{F}, \varphi$ by $F_1, \tilde{F}_1, \varphi_1$ and proceed by induction on the degree of K over F. □

We are now in a position to prove the second of the theorems, Theorem (1.11), which was announced in Section 1. One part of this theorem was proved in the last section, using Corollary (4.5). For convenience, we restate the other part here.

Theorem. Let K be the splitting field of a polynomial $f(x) \in F[x]$. Then K is a Galois extension of F; that is, $|G(K/F)| = [K : F]$.

We will prove the theorem by going back over the proof of Proposition (5.2), keeping careful track of the number of choices.

(5.4) **Lemma.** With the notation of (5.2), the number of isomorphisms $\psi: K \longrightarrow \tilde{K}$ extending φ is equal to the degree $[K : F]$.

The theorem follows from this lemma if we set $\tilde{F} = F, \tilde{K} = K$, and $\varphi =$ identity. □

Proof of Lemma (5.4). We proceed as in the proof of Proposition (5.2), choosing an irreducible factor $g(x)$ of $f(x)$ and one of the roots α of $g(x)$ in K. Let $F_1 = F(\alpha)$. Any isomorphism $\psi: K \longrightarrow \tilde{K}$ extending φ will send F_1 to some subfield $\tilde{F}_1$ of $\tilde{K}$. This field $\tilde{K}$ will have the form $\tilde{F}(\tilde{\alpha})$, where $\tilde{\alpha} = \psi(\alpha)$ is a root of $\tilde{g}(x)$ in $\tilde{K}$.

Conversely, to extend φ to ψ, we may start by choosing any root $\tilde{\alpha}$ of $\tilde{g}(x)$ in $\tilde{K}$. We then extend φ to a map $\varphi_1: F_1 \longrightarrow \tilde{F}_1 = \tilde{F}(\tilde{\alpha})$ by setting $\varphi_1(\alpha) = \tilde{\alpha}$. We use induction on $[K : F]$. Since $[K : F_1] < [K : F]$, the induction hypothesis tells us that for this particular choice of φ_1, there are $[K : F_1]$ extensions of φ_1 to an isomorphism $\psi: K \longrightarrow \tilde{K}$. On the other hand, $\tilde{g}$ has distinct roots in $\tilde{K}$ because g and $\tilde{g}$ are irreducible [Chapter 13 (5.8)]. So the number of choices for $\tilde{\alpha}$ is the degree of g, which is $[F_1 : F]$. There are $[F_1 : F]$ choices for the isomorphism φ_1. This gives us a total of $[K : F_1][F_1 : F] = [K : F]$ extensions of φ to $\psi: K \longrightarrow \tilde{K}$. □

Since any two splitting fields K of a polynomial $f(x) \in F[x]$ are isomorphic, the Galois group $G(K/F)$ depends, up to isomorphism, only on f. It is often referred to as the *Galois group of the polynomial* over F.

The following corollary collects together several criteria for an extension to be Galois. Most of them have already been proved, and we leave the remaining proofs as exercises.

(5.5) **Corollary.** Let K/F be a finite field extension. The following are equivalent:

(i) K is a Galois extension of F;
(ii) K is the splitting field of an irreducible polynomial $f(x) \in F[x]$;
(ii′) K is the splitting field of a polynomial $f(x) \in F[x]$;
(iii) F is the fixed field for the action of the Galois group $G(K/F)$ on K;
(iii′) F is the fixed field for an action of a finite group of automorphisms of K. □

We now have enough information to prove the Main Theorem of Galois theory, which relates intermediate fields to subgroups of the Galois group.

Proof of Theorem (1.15). Let K/F be a Galois extension. We have to show that the maps

$$L \rightsquigarrow G(K/L) \quad \text{and} \quad H \rightsquigarrow K^H$$

are inverse functions between the set of intermediate fields and the set of subgroups of $G = G(K/F)$. To do so, we verify that the composition of these two maps in either direction is the identity.

Let L be an intermediate field. The corresponding subgroup of G is $H = G(K/L)$. By definition, H acts trivially on L, so $L \subset K^H$. On the other hand, K is a Galois extension of L by (1.13); hence $[K : L] = |H|$. By Theorem (4.6), $|H| = [K : K^H]$, so $L = K^H$.

In the other direction, suppose that we start with a subgroup $H \subset G$, and let $L = K^H$. Then $H \subset G(K/L)$. But $|H| = [K : K^H] = [K : L] = |G(K/L)|$. Therefore $H = G(K/L)$. This shows that the two maps are inverses, as required. Since K is a Galois extension of $L = K^H$, $[K : L] = |H|$, and $[L : F] = [G : H]$. □

The correspondence given by the Main Theorem has some surrounding details which we will now discuss. First of all, the correspondence between fields and subgroups is *order reversing*, that is, if L, L' are two intermediate fields and if $H = G(K/L)$, $H' = G(K/L')$ are the corresponding subgroups, then $L \subset L'$ if and only if $H \supset H'$. This is clear from the definitions of the maps and is consistent with the relations (1.16).

To complete the picture, we will show that the immediate fields L which are *Galois extensions* of F correspond to the *normal subgroups* of G. Let L be an intermediate field. An F-automorphism σ of K will carry L to some intermediate field σL which may or may not be the same as L. We call σL a *conjugate subfield*.

(5.6) **Theorem.** Let K/F be a Galois extension, and let L be an intermediate field. Let $H = G(K/L)$ be the corresponding subgroup of $G = G(K/F)$.

(a) Let σ be an element of G. The subgroup of G which corresponds to the conjugate subfield σL is the conjugate subgroup $\sigma H \sigma^{-1}$. In other words, $G(K/\sigma L) = \sigma H \sigma^{-1}$.

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

(5.7) **Diagram.**

$$\begin{array}{l} G = G(K/F) \\ \textit{operates on } K \\ \textit{fixing } F \end{array} \left\{ \begin{array}{c} K \\ \\ L \\ \\ F \end{array} \right. \begin{array}{l} \left.\begin{array}{c} \\ \\ \\ \end{array}\right\} \begin{array}{l} H = G(K/L) \\ \textit{operates on } K, \\ \textit{fixing } L \end{array} \\ \left.\begin{array}{c} \\ \\ \\ \end{array}\right\} \begin{array}{l} \textit{If } H \textit{ is normal,} \\ \textit{then } G/H = G(L/F) \\ \textit{operates here} \end{array} \end{array}$$

(5.8) **Example.** *In the case of the cubic equation (2.1) whose splitting field has de*gree 6, the only intermediate extension which is Galois, other than F and K, is $F(\delta)$, which corresponds to the alternating group $H = A_3 \subset S_3$. The Galois group $G(F(\delta)/F)$ is cyclic of order 2, as is the quotient group S_3/A_3. The three fields $F(\alpha_i)$ are conjugate. This agrees with the fact that the three subgroups of S_3 of order 2 are conjugate.

Proof of Theorem (5.7). (a) Let $\sigma L = L'$. If τ is an element of $H = G(K/L)$, then $\sigma\tau\sigma^{-1}$ is in $H' = G(K/L')$. To check this, we must show that $\sigma\tau\sigma^{-1}$ fixes any element $\alpha' \in L'$. By definition of σL, $\alpha' = \sigma(\alpha)$ for some $\alpha \in L$. Then $\sigma\tau\sigma^{-1}(\alpha') = \sigma\tau(\alpha) = \sigma(\alpha) = \alpha'$, as required. It follows that $H' \supset \sigma H \sigma^{-1}$ and by symmetry, or by counting elements, that $H' = \sigma H \sigma^{-1}$. The fact which we have just checked is actually a general property of group actions on sets [Chapter 5 (6.4)].

(b) Now suppose that H is normal. Then $H = \sigma H \sigma^{-1}$ for all $\sigma \in G$; hence $G(K/L) = G(K/\sigma L)$. This implies that $L = \sigma L$ for all σ [see (1.9)]. Thus every F-automorphism of K carries L to itself and hence defines an F-automorphism of L by restriction. This restriction defines a homomorphism

(5.9) $$\pi\colon G \longrightarrow G(L/F).$$

Its kernel is the set of $\sigma \in G$ which induces the identity on L, which is H. Therefore G/H is isomorphic to a subgroup of $G(L/F)$. Counting degrees and orders, we find

$$[L : F] = |G/H| \leq |G(L/F)|.$$

It follows that L is a Galois extension and that $G/H \approx G(L/F)$.

Conversely, suppose that L/F is Galois. Then L is a splitting field of some polynomial $g(x) \in F[x]$; that is, $L = F(\beta_1,\ldots,\beta_k)$, where β_i are the roots of $g(x)$

in K. An F-automorphism σ of K permutes these roots and therefore carries L to itself: $L = \sigma L$. By (a), $H = \sigma H \sigma^{-1}$; thus H is a normal subgroup. □

6. QUARTIC EQUATIONS

Let K/F be a Galois extension. We have seen that if β is an element of K whose monic irreducible polynomial over F is $g(x)$, then g splits completely in K, and the G-orbit of β is the set of roots of g (4.4). So G operates *transitively* on the roots of an irreducible polynomial $g \in F[x]$, provided that this polynomial has at least one root in K. Combining this observation with Proposition (1.14), we find:

(6.1) **Proposition.** Let K/F be a splitting field of a polynomial $f(x) \in F[x]$. The Galois group G of K/F operates faithfully on the set $\{\alpha_1,\dots,\alpha_n\}$ of roots of f. Hence this operation represents G as a subgroup of the symmetric group S_n. The roots form a single orbit if and only if f is irreducible over F. □

When the Galois extension K is exhibited as the splitting field of a polynomial of degree n, it is customary to view the Galois group G as a subgroup of the symmetric group S_n. If the polynomial f is irreducible, then it is a *transitive* subgroup, which means that it acts transitively on the indices $\{\mathbf{1},\dots,\mathbf{n}\}$. However, the same Galois extension K/F can be exhibited as a splitting field of many polynomials, so this representation of G as a subgroup of S_n is not unique.

For instance, let K/F be the splitting field of an irreducible cubic equation such that $[K:F] = 6$. Then the Galois group is represented as the whole symmetric group S_3. However, the theorem of the primitive element tells us that K can also be generated by a single element γ. Since $[K:F] = 6$, γ has degree 6 over F. This means that its orbit has order 6 and that its irreducible polynomial has degree 6. So if we think of K as the splitting field of this sextic polynomial, the Galois group is represented as a subgroup of S_6. This isn't a very economical way to represent S_3.

Let us suppose that our Galois extension K is the splitting field of a polynomial $f(x)$ and that its roots in K are $\alpha_1,\dots,\alpha_n$. Then, viewing G as a subgroup of S_n, we may pose the following two problems:

(6.2) (i) Given a subgroup $\mathcal{H}$ of S_n, decide if $G \subset \mathcal{H}$.
(ii) Determine G.

If we could solve (i) for every subgroup $\mathcal{H}$, then (ii) would also be solved.

Lagrange's approach to these problems is to look for functions of the roots which are *partially symmetric*. A partially symmetric polynomial is a polynomial $p(u_1,\dots,u_n)$ in the variables $\{u_1,\dots,u_n\}$ which is left fixed by the permutations in a given subgroup $\mathcal{H}$ of S_n but not by any other permutations. For example, we saw in (2.13) that

$$(u_1 - u_2)(u_1 - u_3)(u_2 - u_3)$$

is a partially symmetric function for the alternating group, when $n = 3$. There is no difficulty in generalizing this construction to arbitrary n by defining

$$(6.3) \qquad \delta(u) = (u_1 - u_2)(u_1 - u_3)\cdots(u_{n-1} - u_n) = \prod_{i<j}(u_i - u_j).$$

This element is a square root of the discriminant (3.6). The effect of a permutation of the indices is to multiply δ by the sign of the permutation. Having this partially symmetric function in hand, we substitute the roots $\alpha_1,\ldots,\alpha_n$ of our polynomial into it, to obtain an element $\delta(\alpha) = \delta$ of K which is fixed by even permutations of the roots. We can decide whether or not δ is in F by determining whether or not the discriminant D is a square. This will provide information about the Galois group.

(6.4) **Proposition.** Let K/F be a Galois extension which is the splitting field of an irreducible polynomial $f(x) \in F[x]$ of degree n. Let $\alpha_1,\ldots,\alpha_n$ be the roots of $f(x)$ in K, and let $\delta = \delta(\alpha)$. Then $\delta \neq 0$. Moreover:

(a) *$\delta \in F$ if and only if the Galois group G is a subgroup of the alternating group A_n.*

(b) In any case, the subgroup $G(K/F(\delta))$ of G is contained in the alternating group.

Proof. The case $\delta = 0$ occurs only if two of the roots are equal, and this can not happen if f is irreducible [Chapter 13 (5.8)]. Next, assume that δ is in F. Since odd permutations send $\delta \rightsquigarrow -\delta$ and since $\delta \neq 0$, odd permutations don't fix δ. On the other hand, the elements of F are fixed by every automorphism in G. It follows that G does not contain any odd permutations, hence that $G \subset A_n$. Conversely, if $\delta \notin F$, we use the fact that $K^G = F$. There must be an element of G which doesn't fix δ. This element will be an odd permutation, so $G \not\subset A_n$. This proves (a). Part (b) follows from (a) when we replace F by $F(\delta)$. □

We will now discuss quartic equations, beginning with an interesting special case which is controlled by the discriminant. We consider a complex number which is presented as a nested square root, say $\alpha = \sqrt{r+s\sqrt{t}}$, where r, s, t are in a field F. The numbers

$$(6.5) \qquad \sqrt{3+2\sqrt{2}},\quad \sqrt{5+\sqrt{21}},\quad \sqrt{7+2\sqrt{5}},\quad \sqrt{5+2\sqrt{5}}$$

are a few samples. We ask the following question: Is there an expression for α in terms of two square roots which are not nested?

Since $\alpha^2 = r + s\sqrt{t}$, it is easy to write down a quartic polynomial which has α as a root, namely

$$(6.6) \qquad f(x) = (x^2 - (r + s\sqrt{t}))(x^2 - (r - s\sqrt{t})) = x^4 + bx^2 + c,$$

where $b = -2r$and $c = r^2 - s^2t$. If α' denotes one of the two square roots of $r - s\sqrt{t}$, then the roots of this quartic are

$$(6.7) \qquad \alpha, \alpha', -\alpha, -\alpha'.$$

The splitting field $K = F(\alpha,\alpha')$ of f can be reached by the sequence $\sqrt{t},\alpha,\alpha'$ of three square root adjunctions, so the degree $[K : F]$ divides 8. The degree will be less than 8 if one of the square root adjunctions is unnecessary.

We must decide whether or not f is irreducible. To do so, we first check the irreducibility of the quadratic polynomial $q(y) = y^2 + by + c$ whose roots are α^2,α'^2. If q is irreducible, then f doesn't have a root in F. In that case f, if reducible, will be the product of two quadratic polynomials. Computing with undetermined coefficients, we find that the product must have the form

$$(6.8) \qquad x^4 + bx^2 + c = (x^2 + ux + v)(x^2 - ux + v).$$

We will be able to determine whether or not such a factorization exists, at least when $F = \mathbb{Q}$.

If $f(x)$ is reducible, then α is a root of a quadratic polynomial, so it can be written using only one square root. This happens with $\sqrt{3+2\sqrt{2}}$ for example, which is equal to $1 + \sqrt{2}$, as you will check by squaring both expressions. The quartics derived from the other examples (6.5) are irreducible over $\mathbb{Q}$.

We now return to our question. Let's suppose that f is irreducible. Notice that to write α in terms of unnested square roots $\sqrt{p},\sqrt{q}$ amounts to finding a biquadratic extension $K = F(\sqrt{p},\sqrt{q})$ of F which contains α. Suppose that a biquadratic extension K which contains α can be found. Then K is a Galois extension of F, so $f(x)$ factors into linear factors in K. This means that K contains a splitting field of f. In fact, K will be the splitting field, because f is irreducible and of degree 4. So the Galois group G of f will be the Klein four group. If G is not the Klein four group, then α can not be written in terms of unnested square roots.

Conversely, if K/F is a Galois extension whose Galois group is the Klein four group, then K contains three intermediate fields of degree 2 over F. Any two of these fields taken together generate K. So K is a biquadratic extension of F, and any element of K can be written in terms of two unnested square roots.

We compute the discriminant of $f(x)$, using the list (6.7) of roots.

$$D = \prod_{i<j}(\alpha_i - \alpha_j)^2 = (4\alpha\alpha')^2(\alpha - \alpha')^4(\alpha + \alpha')^4 = 2^4(b^2 - 4c)^2c$$
$$= 2^8s^4t^2(r^2 - s^2t).$$

If D is a square in F, then G is a transitive subgroup of the alternating group A_4 whose order divides 8. The Klein four group is the only such group. It consists of the even permutations of order 2:

$$(6.9) \qquad V = \{(1), (12)(34), (13)(24), (14)(23)\}.$$

There is no other transitive operation of V on $\{1,2,3,4\}$. So we find:

(6.10) **Proposition.** Let $\alpha = \sqrt{r+s\sqrt{t}}$, with $r,s,t \in F$, and assume that $f(x) = x^4 - 2rx^2 + (r^2 - s^2t)$ is irreducible over F. Then α can be written in terms of two unnested square roots if and only if $r^2 - s^2t$ is a square in F. □

If $\alpha = \sqrt{5+\sqrt{21}}$, then $r^2 - s^2t = 25 - 21 = 4$, which is a square. In the last two examples (6.5), $r^2 - s^2t$ is not a square in $\mathbb{Q}$.

Let us determine the unnested expression for $\alpha = \sqrt{5+\sqrt{21}}$ explicitly. Galois theory provides the clue; namely it suggests determining the intermediate fields. They are quadratic extensions of $\mathbb{Q}$, so they are generated by square roots. These square roots are the ones we need to express α. One intermediate quadratic extension is obvious, namely $\mathbb{Q}(\sqrt{21})$. But this isn't the one we need. To find another intermediate extension, we determine the fixed field of the subgroup H of order 2 which is generated by $\sigma = (\mathbf{1}\,\mathbf{2})(\mathbf{3}\,\mathbf{4})$. If the roots of f are listed in the order (6.7), the H-orbit of α is $\{\alpha, \alpha'\}$, (where $\alpha' = \sqrt{5-\sqrt{21}}$, and the irreducible polynomial for α over K^H is $(x-\alpha)(x-\alpha') = x^2 - (\alpha+\alpha')x + \alpha\alpha'$. So K has degree 2 over the field $L = F(\alpha+\alpha', \alpha\alpha')$, and this field is contained in K^H. A consideration of degrees shows that $L = K^H$. With this clue, we compute, finding $\alpha\alpha' = 2$, $(\alpha+\alpha')^2 = 14$, and $\alpha + \alpha' = \sqrt{14}$. Similarly, $\alpha - \alpha' = \sqrt{6}$. We solve for α, obtaining $\alpha = \frac{1}{2}(\sqrt{6} + \sqrt{14})$. □

It is harder to analyze a general quartic equation, and the roots can usually not be written explicitly in a useful way. However, there is another partially symmetric function which helps to determine the Galois group. Let $f(x)$ be an irreducible quartic polynomial with roots $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ in a splitting field K. Then by Proposition (6.1), its Galois group is a subgroup of S_4, and the roots form one orbit. The transitive subgroups of S_4 are

$$S_4,\ A_4,\ D_4,\ C_4,\ V, \tag{6.11}$$

where V is the group (6.9). Actually, there are three conjugate subgroups isomorphic to D_4 and three conjugate subgroups isomorphic to C_4. The other subgroups are uniquely determined. There are some other subgroups of S_4 which are isomorphic to the Klein four group, but they are not transitive.

Let us ask for partially symmetric functions of the roots to distinguish these groups. As we have seen, the element δ determines whether or not $G \subset A_4$. The subgroups of A_4 in our list are A_4 and V. So $\delta \in F$ if and only if G is one of these two groups.

Next, we consider the partially symmetric polynomial

$$\beta_1(u) = u_1u_3 + u_2u_4. \tag{6.12}$$

A permutation of the indices carries $\beta_1(u)$ to one of the three polynomials $\beta_i(u)$, $i = 1, 2, 3$, where

$$\beta_2(u) = u_1u_2 + u_3u_4 \quad \text{and} \quad \beta_3(u) = u_1u_4 + u_2u_3.$$

Since S_4 has order 24, the stabilizer of $\beta_1(u)$ is of order 8; it is one of the three dihedral groups D_4. The polynomial $(x - \beta_1(u))(x - \beta_2(u))(x - \beta_3(u))$ is left fixed by all permutations of the variables u_i, so its coefficients are symmetric functions. They can be computed explicitly in terms of the elementary symmetric functions.

Going back to our quartic polynomial, we substitute the roots α_i into $\beta_j(u)$, to obtain three elements $\beta_j(\alpha) = \beta_j \in K$. They form one orbit under the action of the symmetric group on the roots. If they are distinct elements of K, then the stabilizer of β_1 in S_4 will have order 8, so it will be the dihedral group D_4. We are lucky: The β_j are distinct. For example,

$$\beta_1 - \beta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4 - \alpha_1\alpha_2 - \alpha_3\alpha_4 = (\alpha_1 - \alpha_4)(\alpha_3 - \alpha_2).$$

Since we have assumed that f is irreducible, its roots α_i are distinct. The right side of this equation shows that $\beta_1 - \beta_2 \neq 0$.

Since the Galois group G permutes the elements β_i, the polynomial $g(x) = (x-\beta_1)(x-\beta_2)(x-\beta_3)$ has coefficients in F. It is called the *resolvent cubic* of the quartic polynomial $f(x)$.

Though the symmetric group acts transitively on $\{\beta_1, \beta_2, \beta_3\}$, the Galois group G, which is a subgroup of S_4, may not act transitively. Whether or not it does provides information about G. If G fixes β_1 for example, then G is contained in the stabilizer D_4 of β_1. In this case β_1 will be in the field F (1.9), so the resolvent cubic will have a root in F. Proceeding as in the proof of Proposition (6.4), we find the following:

(6.13) **Proposition.** Let $g(x)$ be the resolvent cubic of an irreducible quartic polynomial $f(x)$, and let K be a splitting field of f. Then $g(x)$ has a root in F if and only if the Galois group $G = G(K/F)$ is a subgroup of one of the dihedral groups D_4. In any case, if β is a root of $g(x)$ in K, then the Galois group $G(K/F(\beta))$ is a subgroup of a dihedral group D_4. □

Thus the polynomials $x^2 - D$, where D is the discriminant, and the resolvent cubic $g(x)$ nearly suffice to describe the Galois group. The results are summed up in this table:

(6.14) **Table.**

	D a square in F	D not a square
g reducible	$G = V$	$G = D_4$ or C_4
g irreducible	$G = A_4$	$G = S_4$

Explicit computation for arbitrary quartic equations becomes unpleasant, but we can easily calculate the discriminant of a quartic which has the form

$$x^4 + rx + s. \tag{6.15}$$

The discriminant is a symmetric polynomial of degree 12 and therefore has weighted degree 12 in the elementary symmetric functions $s_1, \ldots, s_4$. Substituting $(0, 0, -r, s)$ for (s_1, s_2, s_3, s_4) into the unknown formula for the discriminant will kill any monomial involving s_1 or s_2. And the only monomials of weighted degree 12 which do not involve s_1 and s_2 are $s_3{}^4$ and $s_4{}^3$. Thus the discriminant of (6.15) has the form

$$D = \Delta(0,0,-r,s) = cr^4 + c's^3.$$

We can determine the coefficients c, c' by computing the discriminant of two particular polynomials. The answer is

$$D = -27r^4 + 256s^3. \tag{6.16}$$

For example, the discriminant of

$$f(x) = x^4 + 8x + 12 \tag{6.17}$$

is $3^4 \cdot 2^{12}$. This is a square in $\mathbb{Q}$. The Galois group of the splitting field of (6.17) over $\mathbb{Q}$ is therefore a subgroup of A_4.

To calculate the resolvent cubic $g(x)$ of the polynomial (6.15), we write the resolvent cubic for the general polynomial whose roots are $u_1,\ldots,u_4$ as

$$g(x) = x^3 - b_1x^2 + b_2x - b_3;$$

then since β_i is a quadratic function in $\{u_j\}$, b_i has degree $2i$ in $\{u_j\}$ and weighted degree $2i$ in the symmetric functions. Proceeding as above, one finds

$$g(x) = x^3 - 4sx - r^2. \tag{6.18}$$

The resolvent cubic of the particular quartic polynomial (6.17) is $x^3 - 48x - 64$. The quartic (6.17) and its resolvent cubic are both irreducible over $\mathbb{Q}$. It follows that $G = A_4$ for the polynomial (6.17).

7. KUMMER EXTENSIONS

Let us now consider the splitting field over a field F of a polynomial of the form

$$f(x) = x^p - a, \tag{7.1}$$

where p is a prime. We will assume that the base field F is a subfield of $\mathbb{C}$ which contains the primitive pth root of unity $\zeta_p = e^{2\pi i/p}$. The complex roots of $f(x)$ are the pth roots of a, and if α denotes a particular pth root, then the roots of $f(x)$ are

$$\alpha,\ \zeta\alpha,\ \zeta^2\alpha,\ldots,\zeta^{p-1}\alpha, \tag{7.2}$$

where $\zeta = \zeta_p$. Therefore the splitting field is generated by a single root: $K = F(\alpha)$.

(7.3) **Proposition.** Let F be a subfield of $\mathbb{C}$ which contains the pth root of unity ζ_p, and let a be an element of F which is not a pth power in F. Then the splitting field of $f(x) = x^p - a$ has degree p over F, and its Galois group is a cyclic group of order p.

Proof. Let K be a splitting field of f, and let α be one of its roots in K. Assume that α is not in F. Then there is an automorphism σ of K/F which does not fix

α. Since the roots of f are $\zeta^i\alpha$, $i = 0,\dots,p-1$, $\sigma(\alpha) = \zeta^\nu\alpha$ for some $\nu \neq 0$. We now compute the powers of σ. Remembering that σ is an automorphism and that $\sigma(\zeta) = \zeta$ because $\zeta \in F$, we find $\sigma^2(\alpha) = \sigma(\zeta^\nu\alpha) = \zeta^\nu\sigma(\alpha) = \zeta^{2\nu}\alpha$. Similarly, $\sigma^i(\alpha) = \zeta^{i\nu}\alpha$ for each i. Since ζ is a pth root of unity, the smallest positive power of σ which fixes α is σ^p. Hence the order of σ in the Galois group is at least p. On the other hand, α generates K over F, and α is a root of the polynomial $x^p - a$ of degree p, so $[K : F] \leq p$. This shows at the same time that $[K : F] = p$, that $x^p - a$ is irreducible over F, and that $G(K/F)$ is cyclic of order p. □

Here is a striking converse to Proposition (7.3):

(7.4) **Theorem.** Let F be a subfield of $\mathbb{C}$ which contains the pth root of unity ζ, and let K/F be a Galois extension of degree p. Then K is obtained by adjoining a pth root to F.

Extensions of this type are often called *Kummer extensions*. For $p = 2$, the theorem reduces to a familiar assertion: Every extension of degree 2 can be obtained by adjoining a square root. But suppose that $p = 3$ and that F contains ζ_3. If the discriminant of the irreducible cubic polynomial (2.3) is a square in F, then the splitting field of f has degree 3 [see (2.16)], so its Galois group is a cyclic group. Therefore the splitting field of such a polynomial has the form $F(\sqrt[3]{a})$, for some $a \in F$. This isn't obvious.

Proof of Theorem (7.4). The Galois group G has prime order $p = [K : F]$, so it is a cyclic group. Any element σ, not the identity, will generate it. Let us view K as an F-vector space. Then σ is a *linear operator* on K. For, since σ is an F-automorphism,

$$\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta) \quad \text{and} \quad \sigma(c\alpha) = \sigma(c)\sigma(\alpha) = c\sigma(\alpha),$$

for all $c \in F$ and $\alpha, \beta \in K$. Since G is a cyclic group of order p, $\sigma^p = 1$. An eigenvalue λ for this operator must satisfy the relation $\lambda^p = 1$, which means that λ is a power of ζ. By hypothesis, these eigenvalues are in the field F. Moreover, there is at least one eigenvalue different from 1. This is a fact about any linear operator T such that some power of T is the identity, because such a linear operator can be diagonalized [Chapter 9 (2.3)]. Its eigenvalues are the entries of the diagonal matrix A which represents it. If T is not the identity, as is the case here, then $A \neq I$, so some diagonal entry is different from 1.

We choose an eigenvector α with an eigenvalue $\zeta^i \neq 1$. Then $\sigma(\alpha) = \zeta^i\alpha$, and hence $\sigma(\alpha^p) = \sigma(\alpha)^p = (\zeta^i\alpha)^p = \zeta^{ip}\alpha^p = \alpha^p$. So σ fixes α^p. Since σ generates G, the element α^p is in the fixed field K^G, which is F (1.9). We have therefore found an element $\alpha \in K$ whose pth power is in F. Since $\sigma(\alpha) \neq \alpha$, the element α is not in F itself. Since $[K : F]$ is prime, α generates K. □

(7.5) **Example.** Consider the cyclic cubic polynomial (2.12) $x^3 - 3x + 1$. Let $\{\eta_i, \eta_2, \eta_3\}$ denote its roots. There is an element $\sigma \in G(K/F)$ acting as a cyclic permutation. We choose the basis $(1, \eta_1, \eta_2)$ for K over $F = \mathbb{Q}(\zeta_3)$. (Why is it a basis?) With respect to this basis, the matrix of the linear operator σ is

$$\sigma = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & -1 \end{bmatrix},$$

because $\sigma(1) = 1$, $\sigma(\eta_1) = \eta_2$, $\sigma(\eta_2) = \eta_3 = -\eta_1 - \eta_2$. The vector $(0, 1, -\zeta_3)^t$ is an eigenvector with eigenvalue ζ_3. Thus if $\alpha = \eta_1 - \zeta_3\eta_2$, then α^3 is an element of F, and α generates the splitting field of $x^3 - 3x + 1$ over F. We can compute α^3 explicitly, using the fact that $\eta_1 = \zeta_9 + \zeta_9{}^8$ and $\eta_2 = \zeta_9{}^2 + \zeta_9{}^7$. Noting that $\zeta_3 = \zeta_9{}^3$, we find $\alpha = \zeta_9{}^8 - \zeta_9{}^5$ and $\alpha^3 = 3(1 - \zeta_3)$. □

(7.6) **Example.** Let $f(x)$ be an arbitrary irreducible cubic polynomial over a field F, and let K be a splitting field of $f(x)(x^3 - 1)$ over F. Let $L \subset K$ be the intermediate field generated by ζ and $\delta = \sqrt{D}$, where D is the discriminant of f. Then $[L : F]$ divides 4, and $[K : L] = 3$, by (2.16). The four elements $\{1, \sqrt{D}, \sqrt{-3}, \sqrt{(-3D)}\}$ span L as F-vector space in any case. By Theorem (7.4), $K = L(\sqrt[3]{b})$, for some $b \in L$. Therefore the roots of $f(x)$ admit some expression in terms of a cube root of the form

$$\sqrt[3]{c_1 + c_2\sqrt{D} + c_3\sqrt{-3} + c_4\sqrt{-3D}}, \quad \text{with } c_i \in F. \ \square$$

8. CYCLOTOMIC EXTENSIONS

The subfield K of the complex numbers which is generated over $\mathbb{Q}$ by $\zeta_n = e^{2\pi i/n}$ is called a *cyclotomic field*. Also, for any subfield F of $\mathbb{C}$, the field $F(\zeta_n)$ is called a *cyclotomic extension* of F. It is the splitting field over F of the polynomial

$$(8.1) \qquad x^n - 1.$$

If we denote ζ_n by ζ, the roots of this polynomial are the powers of ζ, the nth roots of unity $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$. We will concentrate on the case that n is a prime integer p different from 2 in this section.

The polynomial $x^{p-1} + \cdots + x + 1$ is irreducible over $\mathbb{Q}$, and $\zeta = \zeta_p$ is one of its roots [Chapter 11 (4.6)]. So it is the irreducible polynomial for ζ over $\mathbb{Q}$. Its roots are the powers $\zeta, \zeta^2, \ldots, \zeta^{p-1}$. Hence the Galois group of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$ has order $p - 1$.

(8.2) **Proposition.** Let p be a prime integer, and let $\zeta = \zeta_p$.

(a) The Galois group of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$ is isomorphic to the multiplicative group $\mathbb{F}_p{}^\times$ of nonzero elements of the prime field $\mathbb{F}_p$. It is a cyclic group of order $p - 1$.

(b) For any subfield F of $\mathbb{C}$, the Galois group of $F(\zeta)$ over F is a cyclic group.

Proof. Let G be the Galois group of $F(\zeta)$ over F. We define a map $v\colon G \longrightarrow \mathbb{F}_p{}^\times$ as follows: Let $\sigma \in G$ be an automorphism. It will carry ζ to another root of the polynomial $x^p + \cdots + x + 1$, say to ζ^i. The exponent i is determined as an integer modulo p, because ζ has multiplicative order p. We set $v(\sigma) = i$. Let us verify that v is multiplicative: If τ is another element of G such that $v(\tau) = j$, that is, $\tau(\zeta) = \zeta^i$, then

$$\sigma\tau(\zeta) = \sigma(\zeta^j) = \sigma(\zeta)^j = \zeta^{ij}. \tag{8.3}$$

Also, the identity automorphism sends ζ to ζ, and hence $v(1) = 1$. Since v is compatible with multiplication and $v(\sigma) \neq 0$, v is a homomorphism to $\mathbb{F}_p{}^\times$. The homomorphism is injective because, since ζ generates K, the action of an automorphism is determined when we know its action on ζ. Thus G is isomorphic to its image in $\mathbb{F}_p{}^\times$. Since $\mathbb{F}_p{}^\times$ is a cyclic group, so is every subgroup. Therefore G is cyclic. If $F = \mathbb{Q}$, then $|G| = |\mathbb{F}_p{}^\times| = p - 1$, so these two groups are isomorphic. □

Suppose that $F = \mathbb{Q}$. Then being cyclic and of order $p - 1$, the Galois group G of $K = \mathbb{Q}(\zeta_p)$ has exactly one subgroup of order k for each integer k which divides $p - 1$. If $(p - 1)/k = r$ and if σ is a generator for G, then the subgroup of order k is generated by σ^r. So by the Main Theorem of Galois theory, there will be exactly one intermediate field L with $[L:\mathbb{Q}] = r$. These fields are generated by certain sums of powers of $\zeta = \zeta_p$. We will illustrate this by some simple examples.

The simplest case is $p = 5$. Then $[K:\mathbb{Q}] = 4$, and there is an intermediate field of degree 2 over $\mathbb{Q}$. It is generated by $\eta = \zeta + \zeta^4 = 2\cos 2\pi/5$. Since $2\cos 2\pi/5 = \frac{1}{2}(-1 + \sqrt{5})$, the intermediate field is the quadratic number field $\mathbb{Q}(\sqrt{5})$.

(8.4) **Proposition.** The subfield L of $K = \mathbb{Q}(\zeta_p)$ whose degree over $\mathbb{Q}$ is $\frac{1}{2}(p - 1)$ is generated over $\mathbb{Q}$ by the element $\eta = \zeta + \zeta^{p-1} = 2\cos 2\pi/p$. Moreover, $L = K \cap \mathbb{R}$.

Since $L = K \cap \mathbb{R}$, L is also called the *real subfield* of K.

Proof. Notice that ζ is a root of the quadratic equation $x^2 - \eta x + 1$, which has coefficients in $\mathbb{Q}(\eta)$. Therefore $[K:\mathbb{Q}(\eta)] \leq 2$. On the other hand, η is a real number, while ζ is not real, so $\mathbb{Q}(\eta) < K$. It follows that $[K : \mathbb{Q}(\eta)] = 2$, that $\mathbb{Q}(\eta) = K \cap \mathbb{R}$, and that $[\mathbb{Q}(\eta) : \mathbb{Q}] = \frac{1}{2}(p - 1)$. □

When $p = 7$, $\eta = \zeta + \zeta^6$ has degree 3 over $\mathbb{Q}$. Its irreducible polynomial over $\mathbb{Q}$ can be computed by a method which we have used before (2.12). We guess that the other roots are $\eta_2 = \zeta^2 + \zeta^5$ and $\eta_3 = \zeta^3 + \zeta^4$. These are the other sums of a pth root and its inverse. It is not hard to show that $\{\eta_1, \eta_2, \eta_3\}$ is the G-orbit of $\eta = \eta_1$, so this guess can be justified formally. We expand $(x - \eta_1)(x - \eta_2)(x - \eta_3)$ and use the relation $\zeta^6 + \cdots + \zeta + 1 = 0$, obtaining the irreducible equation $x^3 + x^2 - 2x - 1$ for η over $\mathbb{Q}$.

The cyclotomic field $\mathbb{Q}(\zeta_7)$ also contains a quadratic extension of $\mathbb{Q}$. It is generated by $\epsilon = \zeta + \zeta^2 + \zeta^4$. If we set $\epsilon' = \zeta^3 + \zeta^5 + \zeta^6$, then $(x - \epsilon)(x - \epsilon') = x^2 + x + 2$ is its irreducible equation. The discriminant of this polynomial is -7, so $\mathbb{Q}(\epsilon) = \mathbb{Q}(\sqrt{-7})$. It follows that $\mathbb{Q}(\zeta_7)$ contains $\sqrt{-7}$.

Suppose that $p = 17$. Then $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 16$. A cyclic group of order 16 contains a chain of subgroups $C_{16} \supset C_8 \supset C_4 \supset C_2 \supset C_1$. By the Main Theorem of Galois theory, there is a corresponding chain of intermediate fields $\mathbb{Q} \subset F_1 \subset F_2 \subset F_3 \subset \mathbb{Q}(\zeta)$, of degrees $1, 2, 4, 8, 16$ over $\mathbb{Q}$. The field F_3 of degree 8 is the real subfield generated by $\eta = 2\cos 2\pi/17$, as in Proposition (8.4). Since each extension in this chain has degree 2, F_3 can be reached by a succession of three square root adjunctions. This proves that $2\cos 2\pi/17$, and hence the regular 17-gon, can be constructed by ruler and compass [Chapter 13 (4.9)].

The other field extension which we will describe for all primes is the one of degree 2 over $\mathbb{Q}$. The Main Theorem of Galois theory tells us that there is a unique intermediate field L of $\mathbb{Q}$ of degree 2, corresponding to the subgroup H of G of order $\frac{1}{2}(p - 1)$. If σ generates G, then H is generated by σ^2.

(8.5) **Theorem.** Let p be an odd prime, and let L be the unique quadratic extension of $\mathbb{Q}$ contained in the cyclotomic field $\mathbb{Q}(\zeta_p)$. Then

$$L = \mathbb{Q}(\sqrt{\pm p}),$$

where the sign is $(-1)^{1/2(p-1)}$.

Proof. We need to select a generator of L whose equation is easy to determine. Gauss's method is to take the sum of half of the powers of ζ, suitably chosen.

There is another choice of generator for L which is a little simpler to work with. Let D be the discriminant of the polynomial

$$(8.6) \qquad x^p - 1.$$

This discriminant can be computed directly in terms of the roots $\{1, \zeta, \zeta^2, \ldots, \zeta^{p-1}\}$, but it is easier to determine D using the following nice formula:

(8.7) **Lemma.** Let $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$. The discriminant of f is

$$D = \pm f'(\alpha_1) \cdots f'(\alpha_n) = \pm \prod_i f'(\alpha_i),$$

where f' is the derivative.

Proof. By the product rule for differentiation,

$$f'(x) = \sum_{i=1}^{n} (x - \alpha_1) \cdots (x - \alpha_{i-1})(x - \alpha_{i+1}) \cdots (x - \alpha_n).$$

Therefore

$$f'(\alpha_i) = (\alpha_i - \alpha_1) \cdots (\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1}) \cdots (\alpha_i - \alpha_n).$$

This is the product of the differences $(\alpha_i - \alpha_j)$, with the given i and with $j \neq i$.

Thus

$$\prod_i f'(\alpha_i) = \prod_{i \neq j} (\alpha_i - \alpha_j) = \pm D. \ \square$$

We apply this lemma to our polynomial $x^p - 1$. Its derivative is px^{p-1}, so the discriminant is

$$D = \pm \prod_i p\zeta^{i(p-1)} = \pm \zeta^N p^p,$$

where the exponent N is some integer. To determine ζ^N, we note that D is a rational number, because the coefficients of $x^p - 1$ are rational. The only power of ζ which is rational is 1. Therefore $\zeta^N = 1$ and

$$D = \pm p^p. \tag{8.8}$$

The square root of this discriminant is $\delta = \sqrt{\pm p^p}$. It is in the field $\mathbb{Q}(\zeta)$. Since p is odd and since square factors can be pulled out of a square root,

$$\mathbb{Q}(\delta) = \mathbb{Q}(\sqrt{\pm p}). \tag{8.9}$$

Therefore this field is a quadratic subfield of $\mathbb{Q}(\zeta)$, and since L is the only quadratic subfield, it is L. We leave the determination of the sign as an exercise. □

The following theorem, first stated by Kronecker, is one of the most beautiful theorems of algebraic number theory. Unfortunately, it would take too long to prove it here.

(8.10) **Theorem.** Every Galois extension K of $\mathbb{Q}$ whose Galois group is abelian is contained in one of the cyclotomic fields $\mathbb{Q}(\zeta_n)$. □

9. QUINTIC EQUATIONS

The main motivation behind Galois' work was the problem of solving fifth-degree equations. We are going to study his solution in this section. A short time earlier, Abel had shown that the quintic

$$x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1 + a_0 \tag{9.1}$$

with variable coefficients a_i could not be solved in terms of radicals, but it remained to find an explicit polynomial with rational coefficients which couldn't be solved. Anyhow, because the problem was over 200 years old, interest in it continued. In the meantime, Galois' ideas have turned out to be much more important than the question which motivated them.

An expression in terms of radicals may become very complicated, and I don't know a good notation for a general one. However, it is easy to give a precise recursive definition. Let F be an arbitrary subfield of the complex numbers. We say that a complex number α is *expressible by radicals over* F if there is a tower of subfields $F = F_0 \subset F_1 \subset \ldots \subset F_r$ of $\mathbb{C}$ such that

(9.2)

(i) $\alpha \in F_r$, and

(ii) for every $j = 1,\ldots, r$, F_j is generated over F_{j-1} by a radical β_j. In other words, $F_j = F_{j-1}(\beta_j)$, and for some integer n_j, $\beta_j^{n_j} \in F_{j-1}$.

This definition is formally similar to the description [Chapter 13 (4.9)] of the real numbers which can be constructed by ruler and compass. In that description, only square roots of positive real numbers are allowed.

(9.3) **Proposition.** Let α be a root of a polynomial $f(x) \in F[x]$ of degree ≤ 4. Then α is expressible by radicals over F.

Proof. For quadratic polynomials, this is the quadratic formula. For cubics, Cardano's formula gives the solution. Suppose that $f(x)$ is quartic. If f is reducible, then α is a root of a polynomial of lower degree, and the problem is solved. If not, then f has distinct roots in a splitting field K, so its discriminant D is not zero. Let $g(x)$ be the resolvent cubic of f. We proceed by adjoining the square root δ of D, obtaining a field F_1 (possibly equal to F). Next, we use Cardano's formula to solve the resolvent cubic. This will require a square root extension F_2 followed by a cube root extension F_3. At this point, Table (6.14) shows that the Galois group of K/F_3 is a subgroup of the Klein four group. Therefore K can be reached by a sequence of at most two more square root extensions $F_3 \subset F_4 \subset F_5 = K$. □

The nth roots of unity $\zeta_n = e^{2\pi i/n}$ are allowable in an expression by radicals. Also, if $n = rs$, then $\sqrt[n]{b} = \sqrt[r]{\sqrt[s]{b}}$. So at the cost of adding more steps to the chain of fields, we may assume that all the roots are pth roots, for various prime integers p.

Note that there is a great deal of ambiguity in an expression by radicals, because there are n choices for each $\sqrt[n]{b}$. The notation $(-3 + \sqrt[5]{2})^{1/4}$ may stand for any one of 20 complex numbers, so the tower of fields $\mathbb{Q} \subset \mathbb{Q}(\sqrt[5]{2}) \subset \mathbb{Q}((-3 + \sqrt[5]{2})^{1/4})$ is not uniquely defined. This ambiguity is inherent in the notation. Since the notation is cumbersome anyhow, we won't bother trying to make it more precise. We won't use it very much.

(9.4) **Proposition.** Let $f(x)$ be an irreducible polynomial over a field F. If one root of f in K can be expressed by radicals, so can any other root.

Proof. Suppose that one root α can be expressed by radicals, say using the tower $F = F_0 \subset \ldots \subset F_r$. Choose a field L which contains F_r and which is a splitting field of some polynomial of the form $f(x)g(x)$ over F. Then L is also the splitting field of fg over $F(\alpha)$. Let α' be a root of f in another field K', and let L' be a splitting field of fg over $F(\alpha')$. Then we can extend the isomorphism $F(\alpha) \longrightarrow F(\alpha')$ to an isomorphism $\varphi : L \longrightarrow L'$ (5.2). The tower of fields $F = \varphi(F_0) \subset \ldots \subset \varphi(F_r)$ shows that α' is expressible by radicals. □

(9.5) **Proposition.** Let α be a complex number which can be expressed by radicals over F. Then a tower of fields $F = F_0 \subset \ldots \subset F_r = K$ can be found so that the conditions (i) and (ii) of (9.2) hold and, in addition,

(iii) for each j, F_j is a Galois extension of F_{j-1} and the Galois group $G(F_j/F_{j-1})$ is a cyclic group.

Proof. Consider the tower given in the definition (9.2), in which $F_r = F(\beta_1,\ldots,\beta_r)$. As we have remarked, we may assume that $\beta_j^{p_j} \in F_{j-1}$ for some prime integer p_j. Let $\zeta_{p_j} = e^{2\pi i/p_j}$ be the p_j-th root of 1. We form a new chain of fields by adjoining the elements $(\zeta_{p_1},\ldots,\zeta_{p_r};\beta_1,\ldots,\beta_r)$ in that order. Theorem (7.4) and Proposition (8.2) show that each of these extensions is Galois, with cyclic Galois group. Some of the extensions in this tower may be trivial because of redundancy. If so, we shorten the chain. Since the last field $F(\{\zeta_{p_j}\},\{\beta_j\})$ in this chain contains F_r, it contains α. □

Let us consider the Galois group of a product of polynomials $f(x)g(x)$ over F. Let K' be a splitting field of fg. Then K' contains a splitting field K of f, because f factors into linear factors in K'. Similarly, K' contains a splitting field F' of g. So we have a diagram of fields

(9.6)
$$\begin{tikzcd}
 & K' & \\
K \arrow[ur, phantom, sloped, "\subset"] & & F' \arrow[ul, phantom, sloped, "\supset"] \\
 & F \arrow[ul, phantom, sloped, "\supset"] \arrow[ur, phantom, sloped, "\subset"] &
\end{tikzcd}$$

(9.7) **Proposition.** With the above notation, let $G = G(K/F)$, $H = G(F'/F)$, and $\mathcal{G} = G(K'/F)$.

(a) G and H are quotients of $\mathcal{G}$.

(b) $\mathcal{G}$ is isomorphic to a subgroup of the product group $G \times H$.

Proof. The first assertion follows from the fact that K and F' are intermediate fields which are Galois extensions of F (5.7b). Let us denote the canonical homomorphisms $\mathcal{G} \longrightarrow G$, $\mathcal{G} \longrightarrow H$ by subscripts: $\sigma \rightsquigarrow \sigma_f$ and $\sigma \rightsquigarrow \sigma_g$. Then σ_f describes the way that σ operates on the roots of f, and σ_g describes the way it operates on the roots of g. We map $\mathcal{G}$ to $G \times H$ by $\sigma \rightsquigarrow (\sigma_f, \sigma_g)$. If σ_f and σ_g are both the identity, then σ operates trivially on the roots of fg, and hence $\sigma = 1$. This shows that the map $\mathcal{G} \longrightarrow G \times H$ is injective and that $\mathcal{G}$ is isomorphic to a subgroup of $G \times H$. □

(9.8) **Proposition.** Let f be a polynomial over F whose Galois group G is a simple nonabelian group. Let F' be a Galois extension of F, with abelian Galois group. Let K' be a splitting field of f over F'. Then the Galois group $G(K'/F')$ is isomorphic to G.

This proposition is a key point. It tells us that if the Galois group of f is a simple nonabelian group, then we will not make any progress toward solving for its roots if we replace F by an abelian extension F'.

Proof of Proposition (9.8). We first reduce ourselves to the case that $[F' : F]$ is a prime number. To do this, we suppose that the lemma has been proved in that case, and we choose a cyclic quotient group H of $G(F'/F)$ of prime order. Such a quotient exists because $G(F'/F)$ is abelian. This quotient determines an intermediate field $F_1 \subset F'$ which is a Galois extension of F, and such that $G(F_1/F) = H$ (5.7). Let K_1 be the splitting field of f over F_1. Then since $[F_1 : F]$ is a prime, $G(K_1/F_1) = G$. So we may replace F by F_1 and K by K_1. Induction on $[F' : F]$ will complete the proof.

So we may assume that $[F' : F] = p$ and that $H = G(F'/F)$ is a cyclic group of order p. The splitting field K' will contain a splitting field of f over F, call it K. We are then in the situation of Proposition (9.7). So the Galois group $\mathcal{G}$ of K' over F is a subgroup of $G \times H$, and it maps surjectively to G. It follows that $|G|$ divides $|\mathcal{G}|$, and $|\mathcal{G}|$ divides $|G \times H| = p|G|$. If $|G| = |\mathcal{G}|$, then counting degrees shows that $K' = K$. In this case, K contains the Galois extension F', and hence H is a quotient of G (5.7b). Since G is a nonabelian simple group, this is impossible. The only remaining possibility is that $\mathcal{G} = G \times H$. Applying the Main Theorem to the chain of fields $F \subset F' \subset K'$, we conclude that $G(K'/F') = G$, as required. □

(9.9) **Theorem.** The roots of a quintic polynomial $f(x)$ whose Galois group is S_5 or A_5 can not be expressed by radicals over F.

Proof. Let K be a splitting field of f. If $G = S_5$, then the discriminant of f is not a square in F. In that case, we replace F by $F(\delta)$, where δ is a square root of the discriminant in K. The Galois group $G(K/F(\delta))$ is A_5. Obviously, it is enough to show that the roots of f can not be expressed by radicals over the larger field $F(\delta)$. This reduces the case that the group is S_5 to the case that it is A_5.

Suppose that the Galois group of f is A_5 but that some root α of f is expressible by radicals over F. Say that $\alpha \in F_r$, where F_r is the end of a chain of field extensions $F = F_0 \subset \ldots \subset F_r$, each extension in the chain being Galois, with a cyclic Galois group. Now since the Galois group of f over F is a simple group, Proposition (9.8) shows inductively that for each i, the Galois group of f over F_i is A_5 too. On the other hand, since it has a root α in F_r, the polynomial f will not remain irreducible over that field. Therefore the Galois group of f over F_r will not operate transitively on the five roots of f in a splitting field. In particular, the Galois group can not be the alternating group. This is a contradiction, which shows that the roots of f are not expressible by radicals. □

We will now exhibit a specific quintic polynomial over $\mathbb{Q}$ whose Galois group is S_5. The facts that 5 is prime and that the Galois group G acts transitively on the roots $\{\alpha_1, \ldots \alpha_5\}$ limit the possible Galois groups greatly. For, since the action is transitive, $|G|$ is divisible by 5. Thus G contains an element of order 5. The only elements of order 5 in S_5 are cyclic permutations such as $\sigma = (\mathbf{12345})$.

(9.10) **Lemma.** If G contains a transposition, then $G = S_5$.

Proof. By transposition τ we mean, as always, a permutation which interchanges two indices. We may assume that G contains the cyclic permutation σ above. Renumbering if necessary, we may assume that τ acts as $(\mathbf{1\,i})$. We replace σ by σ^{i-1} and renumber again, to reduce to the case that τ is the transposition $(\mathbf{1\,2})$. It remains only to verify that σ and τ generate S_5, which is left as an exercise. □

(9.11) **Corollary.** Suppose that the irreducible polynomial (9.1) has roots $\{\alpha_1, \ldots, \alpha_5\}$, and let K be its splitting field. If $F(\alpha_1, \alpha_2, \alpha_3) < K$, then $G(K/F)$ is the symmetric group S_5.

For let $F' = F(\alpha_1, \alpha_2, \alpha_3)$. The only nontrivial permutation fixing $\alpha_1, \alpha_2, \alpha_3$ is the transposition $(\mathbf{4\,5})$. If $F' \neq K$, this permutation must be in $G(K/F')$. Thus $G(K/F)$ contains a transposition. □

(9.12) **Corollary.** Let $f(x)$ be an irreducible quintic polynomial over $\mathbb{Q}$ with exactly three real roots. Then its Galois group is the symmetric group, and hence its roots can not be expressed by radicals.

For, call the real roots $\alpha_1, \alpha_2, \alpha_3$. Then $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) \subset \mathbb{R}$, but since α_4, α_5 are not real, K is not a subfield of $\mathbb{R}$. So we can apply Corollary (9.11) to conclude that the Galois group of f is S_5. By Theorem (9.9), the roots of f can not be expressed by radicals. □

(9.13) **Example.** The polynomial $x^5 - 16x = x(x^2 - 4)(x^2 + 4)$ has three real roots, but of course it is not irreducible. But we can add a small constant without changing the number of real roots. This is seen by looking at the graph of the polynomial. For instance,

$$x^5 - 16x + 2$$

still has three real roots, and it is irreducible by the Eisenstein Criterion [Chapter 10 (4.9)]. So its roots can not be expressed by radicals over $\mathbb{Q}$.

Il parait après cela qu'il n'y a aucun fruit à tirer
de la solution que nous proposons.

Evariste Galois

EXERCISES

1. The Main Theorem of Galois Theory

1. Determine the irreducible polynomial for $i + \sqrt{2}$ over $\mathbb{Q}$.
2. Prove that the set $(1, i, \sqrt{2}, i\sqrt{2})$ is a basis for $\mathbb{Q}(i, \sqrt{2})$ over $\mathbb{Q}$.
3. Determine the intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.
4. Determine the intermediate fields of an arbitrary biquadratic extension without appealing to the Main Theorem.
5. Prove that the automorphism $\mathbb{Q}(\sqrt{2})$ sending $\sqrt{2}$ to $-\sqrt{2}$ is discontinuous.
6. Determine the degree of the splitting field of the following polynomials over $\mathbb{Q}$.
   (a) $x^4 - 1$ (b) $x^3 - 2$ (c) $x^4 + 1$
7. Let α denote the positive real fourth root of 2. Factor the polynomial $x^4 - 2$ into irreducible factors over each of the fields $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2}, i)$, $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\alpha, i)$.
8. Let $\zeta = e^{2\pi i/5}$.
   (a) Prove that $K = \mathbb{Q}(\zeta)$ is a splitting field for the polynomial $x^5 - 1$ over $\mathbb{Q}$, and determine the degree $[K : \mathbb{Q}]$.
   (b) Without using Theorem (1.11), prove that K is a Galois extension of $\mathbb{Q}$, and determine its Galois group.
9. Let K be a quadratic extension of the form $F(\alpha)$, where $\alpha^2 = a \in F$. Determine all elements of K whose squares are in F.
10. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. Determine $[K : \mathbb{Q}]$, prove that K is a Galois extension of $\mathbb{Q}$, and determine its Galois group.
11. Let K be the splitting field over $\mathbb{Q}$ of the polynomial $f(x) = (x^2 - 2x - 1)(x^2 - 2x - 7)$. Determine $G(K/\mathbb{Q})$, and determine all intermediate fields explicitly.
12. Determine all automorphisms of the field $\mathbb{Q}(\sqrt[3]{2})$.
13. Let K/F be a finite extension. Prove that the Galois group $G(K/F)$ is a finite group.
14. Determine all the quadratic number fields $\mathbb{Q}[\sqrt{d}]$ which contain a primitive pth root of unity, for some prime $p \neq 2$.
15. Prove that every Galois extension K/F whose Galois group is the Klein four group is biquadratic.
16. Prove or disprove: Let $f(x)$ be an irreducible cubic polynomial in $\mathbb{Q}[x]$ with one real root α. The other roots form a complex conjugate pair $\beta, \overline{\beta}$, so the field $L = \mathbb{Q}(\beta)$ has an automorphism σ which interchanges $\beta, \overline{\beta}$.
17. Let K be a Galois extension of a field F such that $G(K/F) \approx C_2 \times C_{12}$. How many intermediate fields L are there such that (a) $[L : F] = 4$, (b) $[L : F] = 9$, (c) $G(K/L) \approx C_4$?
18. Let $f(x) = x^4 + bx^2 + c \in F[x]$, and let K be the splitting field of f. Prove that $G(K/F)$ is contained in a dihedral group D_4.
19. Let $F = \mathbb{F}_2(u)$ be the rational function field over the field of two elements. Prove that the polynomial $x^2 - u$ is irreducible in $F[x]$ and that it has two equal roots in a splitting field.

20. Let F be a field of characteristic 2, and let K be an extension of F of degree 2.

(a) Prove that K has the form $F(\alpha)$, where α is the root of an irreducible polynomial over F of the form $x^2 + x + a$, and that the other root of this equation is $\alpha + 1$.

(b) Is it true that there is an automorphism of K sending $\alpha \rightsquigarrow \alpha + 1$?

2. Cubic Equations

1. Prove that the discriminant of a real cubic is positive if all the roots are real, and negative if not.

2. Determine the Galois groups of the following polynomials.
(a) $x^3 - 2$ (b) $x^3 + 27x - 4$ (c) $x^3 + x + 1$ (d) $x^3 + 3x + 14$
(e) $x^3 - 3x^2 + 1$ (f) $x^3 - 21x + 7$ (g) $x^3 + x^2 - 2x - 1$
(h) $x^3 + x^2 - 2x + 1$

3. Let f be an irreducible cubic polynomial over F, and let δ be the square root of the discriminant of f. Prove that f remains irreducible over the field $F(\delta)$.

4. Let α be a complex root of the polynomial $x^3 + x + 1$ over $\mathbb{Q}$, and let K be a splitting field of this polynomial over $\mathbb{Q}$.

(a) Is $\sqrt{-3}$ in the field $\mathbb{Q}(\alpha)$? Is it in K?

(b) Prove that the field $\mathbb{Q}(\alpha)$ has no automorphism except the identity.

***5.** Prove Proposition (2.16) directly for a cubic of the form (2.3), by determining the formula which expresses α_2 in terms of α_1, δ, p, q explicitly.

6. Let $f \in \mathbb{Q}[x]$ be an irreducible cubic polynomial which has exactly one real root, and let K be its splitting field over $\mathbb{Q}$. Prove that $[K : \mathbb{Q}] = 6$.

7. When does the polynomial $x^3 + px + q$ have a multiple root?

8. Determine the coefficients p, q which are obtained from the general cubic (2.1) by the substitution (2.2).

9. Prove that the discriminant of the cubic $x^3 + px + q$ is $-4p^3 - 27q^2$.

3. Symmetric Functions

1. Derive the expression (3.10) for the discriminant of a cubic by the method of undetermined coefficients.

2. Let $f(u)$ be a symmetric polynomial of degree d in $u_1, \ldots, u_n$, and let $f^0(u_1, \ldots, u_{n-1}) = f(u_1, \ldots, u_{n-1}, 0)$. Say that $f^0(u) = g(s^0)$, where s_i^0 are the elementary symmetric functions in $u_1, \ldots, u_{n-1}$. Prove that if $n > d$, then $f(u) = g(s)$.

3. Compute the discriminant of a quintic polynomial of the form $x^5 + ax + b$.

4. With each of the following polynomials, determine whether or not it is a symmetric function, and if so, write it in terms of the elementary symmetric functions.
(a) $u_1^2u_2 + u_2^2u_1$ $(n = 2)$
(b) $u_1^2u_2 + u_2^2u_3 + u_3^2u_1$ $(n = 3)$
(c) $(u_1 + u_2)(u_2 + u_3)(u_1 + u_3)$ $(n = 3)$
(d) $u_1^3u_2 + u_2^3u_3 + u_3^3u_1 - u_1u_2^3 - u_2u_3^3 - u_3u_1^3$ $(n = 3)$
(e) $u_1^3 + u_2^3 + \cdots + u_n^3$

5. Find two natural bases for the ring of symmetric functions, as free module over the ring R.

***6.** Define the polynomials $w_1,\dots,w_n$ in variables $u_1,\dots,u_n$ by $w_k = u_1{}^k + \cdots + u_n{}^k$.

(a) Prove *Newton's identities:* $w_k - s_1w_{k-1} + s_2w_{k-2} - \cdots \pm s_{k-1}w_1 \mp ks_k = 0$.

(b) Do $w_1,\dots,w_n$ generate the ring of symmetric functions?

7. Let $f(x) = x^3 + a_2x^2 + a_1x + a_0$. Prove that the substitution $x = x_1 - (a_2/3)$ does not change the discriminant of a cubic polynomial.

8. Prove that $[F(u) : F(s)] = n!$ by induction, directly from the definitions.

9. Let $u_1,\dots,u_n$ be variables and let D_1 denote the discriminant. Define

$$D_2 = \sum_k \prod_{\substack{i<j \\ i,j\neq k}} (u_i - u_j)^2.$$

(a) Prove that D_2 is a symmetric polynomial, and compute its expression in terms of the elementary symmetric polynomials for the cases $n = 2, 3$.

(b) Let $a_1,\dots,a_n$ be elements of a field of characteristic zero. Prove that $D_1(a_1,\dots,a_n) = D_2(a_1,\dots,a_n) = 0$ if and only if the number of distinct elements in the set $\{a_1,\dots,a_n\}$ is $\leq n - 2$.

10. Compute the discriminants of the polynomials given in Section 2, exercise 2.

***11.** (*Vandermonde* determinant) (a) Prove that the determinant of the matrix

$$\begin{bmatrix} 1 & u_1 & u_1{}^2 & \cdots & u_1{}^{n-1} \\ 1 & u_2 & & & u_2{}^{n-1} \\ \vdots & & & & \\ 1 & u_n & u_n{}^2 & \cdots & u_n{}^{n-1} \end{bmatrix}$$

is a constant multiple of $\delta(u)$.

(b) Determine the constant.

4. *Primitive Elements*

1. Let G be a group of automorphisms of a field K. Prove that the fixed elements K^G form a subfield of K.

2. Let $\alpha = \sqrt[3]{2}$, $\zeta = \frac{1}{2}(-1 + \sqrt{-3})$, $\beta = \alpha\zeta$.

(a) Prove that for all $c \in \mathbb{Q}$, $\gamma = \alpha + c\beta$ is the root of a sixth-degree polynomial of the form $x^6 + ax^3 + b$.

(b) Prove that the irreducible polynomial for $\alpha + \beta$ is cubic.

(c) Prove that $\alpha - \beta$ has degree 6 over $\mathbb{Q}$.

3. For each of the following sets of automorphisms of the field of rational functions $\mathbb{C}(y)$, determine the group of automorphisms which they generate, and determine the fixed field explicitly.

(a) $\sigma(y) = y^{-1}$ (b) $\sigma(y) = iy$ (c) $\sigma(y) = -y$, $\tau(y) = y^{-1}$ (d) $\sigma(y) = \zeta y$, $\tau(y) = y^{-1}$, where $\zeta = e^{2\pi i/3}$ (e) $\sigma(y) = iy$, $\tau(y) = y^{-1}$

4. (a) Show that the automorphisms $\sigma(y) = (y + i)/(y - i)$, $\tau(y) = i(y - 1)/(y + 1)$ of $\mathbb{C}(y)$ generate a group isomorphic to the alternating group A_4.

*(b) Determine the fixed field of this group.

***5.** Let F be a finite field, and let $f(x)$ be a nonconstant polynomial whose derivative is the zero polynomial. Prove that f is not irreducible over F.

5. Proof of the Main Theorem

1. Let $K = \mathbb{Q}(\alpha)$, where α is a root of the polynomial $x^3 + 2x + 1$, and let $g(x) = x^3 + x + 1$. Does $g(x)$ have a root in K?
2. Let $f \in F[x]$ be a polynomial of degree n, and let K be a splitting field for f. Prove that $[K : F]$ divides $n!$.
3. Let G be a finite group. Prove that there exists a field F and a Galois extension K of F whose Galois group is G.
4. Assume it known that π and e are transcendental numbers. Let K be the splitting field of the polynomial $x^3 + \pi x + 6$ over the field $F = \mathbb{Q}(\pi)$.
   (a) Prove that $[K : F] = 6$.
   (b) Prove that K is isomorphic to the splitting field of $x^3 + ex + 6$ over $\mathbb{Q}(e)$.
5. Prove the isomorphism $F[x]/(f(x)) \approx \tilde{F}[x]/(\tilde{f}(x))$ used in the proof of Lemma (5.1) formally, using the universal property of the quotient construction.
6. Prove Corollary (5.5).
7. Let $f(x)$ be an irreducible cubic polynomial over $\mathbb{Q}$ whose Galois group is S_3. Determine the possible Galois groups of the polynomial $(x^3 - 1) \cdot f(x)$.
8. Consider the diagram of fields

$$\begin{tikzcd} & K' & \\ K \arrow[ur, phantom, sloped, "\subset"] & & F' \arrow[ul, phantom, sloped, "\supset"] \\ & F \arrow[ul, phantom, sloped, "\subset"] \arrow[ur, phantom, sloped, "\subset"] & \end{tikzcd}$$

   in which K is a Galois extension of F, and K' is generated over F by K and F'. Prove that K' is a Galois extension of F' and that its Galois group is isomorphic to a subgroup of $G(K/F)$.
9. Let $K \supset L \supset F$ be fields. Prove or disprove:
   (a) If K/F is Galois, then K/L is Galois.
   (b) If K/F is Galois, then L/F is Galois.
   (c) If L/F and K/L are Galois, then K/F is Galois.
10. Let K be a splitting field of an irreducible cubic polynomial $f(x)$ over a field F whose Galois group is S_3. Determine the group $G(F(\alpha)/F)$ of automorphisms of the extension $F(\alpha)$.
11. Let K/F be a Galois extension whose Galois group is the symmetric group S_3. Is it true that K is the splitting field of an irreducible cubic polynomial over F?
12. Let K/F be a field extension of characteristic $p \neq 0$, and let α be a root in K of an irreducible polynomial $f(x) = x^p - x - a$ over F.
    (a) Prove that $\alpha + 1$ is also a root of $f(x)$.
    (b) Prove that the Galois group of f over F is cyclic of order p.

6. Quartic Equations

1. Compute the discriminant of the quartic polynomial $x^4 + 1$, and determine its Galois group over $\mathbb{Q}$.
2. Let K be the splitting field of an irreducible quartic polynomial $f(x)$ over F, and let the roots of $f(x)$ in K be $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. Also assume that the resolvent cubic $g(x)$ has a root,

say $\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4$. Express the root α_1 explicitly in terms of a succession of square roots.

3. What can you say about the Galois group of an irreducible quartic polynomial over $\mathbb{Q}$ which has exactly two real roots?

4. Suppose that a real quartic polynomial has a positive discriminant. What can you say about the number of real roots?

5. Let K be the splitting field of a reducible quartic polynomial with distinct roots over a field F. What are the possible Galois groups of K/F?

6. What are the possible Galois groups over $\mathbb{Q}$ of an irreducible quartic polynomial $f(x)$ whose discriminant is negative?

7. Let g be the resolvent cubic of an irreducible quartic polynomial $f \in F[x]$. Determine the possible Galois groups of g over F, and in each case, say what you can about the Galois group of f.

8. Let K be the splitting field of a polynomial $f \in F[x]$ with distinct roots $\alpha_1,\ldots,\alpha_n$, and let $G = G(K/F)$. Then G may be regarded as a subgroup of the symmetric group S_n. Prove that a change of numbering of the roots changes G to a conjugate subgroup.

9. Let $\alpha_1,\ldots,\alpha_4$ be the roots of a quartic polynomial. Discuss the symmetry of the elements $\alpha_1\alpha_2$ and $\alpha_1 + \alpha_2$ along the lines of the discussion in the text.

10. Find a quartic polynomial over $\mathbb{Q}$ whose Galois group is **(a)** S_4, **(b)** D_4, **(c)** C_4.

11. Let α be the real root of a quartic polynomial f over $\mathbb{Q}$. Assume that the resolvent cubic is irreducible. Prove that α can't be constructed by ruler and compass.

12. Determine the Galois groups of the following polynomials over $\mathbb{Q}$.
(a) $x^4 + 4x^2 + 2$ **(b)** $x^4 + 2x^2 + 4$ **(c)** $x^4 + 4x^2 - 5$ **(d)** $x^4 - 2$ **(e)** $x^4 + 2$
(f) $x^4 + 1$ **(g)** $x^4 + x + 1$ **(h)** $x^4 + x^3 + x^2 + x + 1$ **(i)** $x^4 + x^2 + 4$

13. Compute the discriminant of the quartic polynomial $x^4 + ax + b$, using the formula in Lemma (8.7).

***14.** Let f be an irreducible quartic polynomial over F of the form $x^4 + rx + s$, and let $\alpha_1,\alpha_2,\alpha_3,\alpha_4$ be the roots of f in a splitting field K. Let $\eta = \alpha_1\alpha_2$.

(a) Prove that η is the root of a sextic polynomial $h(x)$ with coefficients in F.

(b) Assume that the six products $\alpha_i\alpha_j$ are distinct. Prove that $h(x)$ is irreducible, or else it has an irreducible quadratic factor.

(c) Describe the possibilities for the Galois group $G = G(K/F)$ in the following three cases: h is irreducible, h is a product of an irreducible quadratic and an irreducible quartic, and h is the product of three irreducible quadratics.

(d) Describe the situation when some of the products are equal.

15. Let K be the splitting field of the polynomial $x^4 - 3$ over $\mathbb{Q}$.

(a) Prove that $[K : \mathbb{Q}] = 8$ and that K is generated by i and a single root α of the polynomial.

(b) Prove that the Galois group of $K/\mathbb{Q}$ is dihedral, and describe the operation of the elements of G on the generators of K explicitly.

16. Let K be the splitting field over $\mathbb{Q}$ of the polynomial $x^4 - 2x^2 - 1$. Determine the Galois group G of $K/\mathbb{Q}$, find all intermediate fields, and match them up with the subgroups of G.

17. Let $f(x)$ be a quartic polynomial. Prove that the discriminants of f and of its resolvent cubic are equal.

18. Prove the irreducibility of the polynomial (6.17) and of its resolvent cubic.

19. Let K be the splitting field of the reducible polynomial $(x-1)^2(x^2+1)$ over $\mathbb{Q}$. Prove that $\delta \in \mathbb{Q}$, but that $G(K/\mathbb{Q})$ is not contained in the alternating group.

20. Let $f(x)$ be a quartic polynomial with distinct roots, whose resolvent cubic $g(x)$ splits completely in the field F. What are the possible Galois groups of $f(x)$?

21. Let $\zeta = e^{2\pi i/3}$ be the cube root of 1, let $\alpha = \sqrt[3]{a+b\sqrt{2}}$, and let K be the splitting field of the irreducible polynomial for α over $\mathbb{Q}(\zeta)$. Determine the possible Galois groups of K over $\mathbb{Q}(\zeta)$.

22. Let $\mathcal{H}$ be a subgroup of the symmetric group S_n. Given any monomial m, we can form the polynomial $p(u) = \Sigma_{\sigma \in \mathcal{H}}\, \sigma m$. Show that if $m = u_1 u_2{}^2 u_3{}^3 \cdots u_{n-1}{}^{n-1}$, then $p(u)$ is partially symmetric for $\mathcal{H}$; that is, it is fixed by the permutations in $\mathcal{H}$ but not by any other permutations.

23. Let $p(u)$ be the polynomial formed as in the last problem, with $\mathcal{H} = A_n$. Then the orbit of $p(u)$ contains two elements, say $p(u), q(u)$. Prove that $p(u) - q(u) = \pm\delta(u)$.

24. Determine the possible Galois groups of a reducible quartic equation of the form $x^4 + bx^2 + c$, assuming that the quadratic $y^2 + by + c$ is irreducible.

25. Compute the discriminant of the polynomial $x^4 + rx + s$ by evaluating the discriminants of $x^4 - x$ and $x^4 - 1$.

26. Use the substitution $x \rightsquigarrow y^{-1}$ to determine the discriminant of the polynomial $x^4 + ax^3 + b$.

27. Determine the resolvent cubic of the polynomials **(a)** $x^4 + rx + s$ and **(b)** $x^4 + a_1x^3 + a_2x^2 + a_3x + a_4$.

28. Let $f(x) = x^4 - 2rx^2 + (r^2 - s^2v)$, with $r, s, v \in F$. Assume that f is irreducible, and let G denote its Galois group. Let $L = F(\sqrt{v}, \delta)$, where $\delta^2 = D$. Prove each statement.
(a) $L(\alpha) = K$
(b) If $[L : F] = 4$, then $G = D_4$.
(c) If $[L : F] = 2$ and $\delta \notin F$, then $G = C_4$.

29. Determine the Galois groups of the last two examples of (6.5).

30. Determine the action of the Galois group G on the roots $\{\alpha, \alpha', -\alpha, -\alpha'\}$ (6.7) explicitly, assuming that **(a)** $G = C_4$, **(b)** $G = D_4$.

31. Determine whether or not the following nested radicals can be written in terms of unnested ones, and if so, find an expression.
(a) $\sqrt{2+\sqrt{11}}$ **(b)** $\sqrt{6+\sqrt{11}}$ **(c)** $\sqrt{11+6\sqrt{2}}$ **(d)** $\sqrt{11+\sqrt{6}}$

***32.** Let K be the splitting field of a quartic polynomial $f(x)$ over $\mathbb{Q}$, whose Galois group is D_4, and let α be a real root of $f(x)$ in K. Decide whether or not α can be constructed by ruler and compass if (a) all four roots of f are real, (b) f has two real roots.

33. Can the roots of the polynomial $x^4 + x - 5$ be constructed by ruler and compass?

7. *Kummer Extensions*

1. Suppose that a Galois extension K/F has the form $K = F(\alpha)$ and that for some integer n, $\alpha^n \in F$. What can you say about the Galois group of K/F?

***2.** Let a be an element of a field F, and let p be a prime. Suppose that the polynomial $x^p - a$ is reducible in $F[x]$. Prove that it has a root in f.

3. Let F be a subfield of $\mathbb{C}$ which contains i, and let K be a Galois extension of F whose group is C_4. Is it true that K has the form $F(\alpha)$, where $\alpha^4 \in F$?
4. Let $f(x) = x^3 + px + q$ be an irreducible polynomial over a field F, with roots $\alpha_1, \alpha_2, \alpha_3$. Let $\beta = \alpha_1 + \zeta\alpha_2 + \zeta^2\alpha_3$, where $\zeta = e^{2\pi i/3}$. Show that β is an eigenvector of σ for the cyclic permutation of the roots unless $\beta = 0$, and compute β^3 explicitly in terms of p, q, δ, ζ.
5. Let K be a splitting field of an irreducible polynomial $f(x) \in F[x]$ of degree p whose Galois group is a cyclic group of order p generated by σ, and suppose that F contains the pth root of unity $\zeta = \zeta_p$. Let $\alpha_1, \alpha_2, \ldots, \alpha_p$ be the roots of f in K. Show that $\beta = \alpha_1 + \zeta^\nu\alpha_2 + \zeta^{2\nu}\alpha_3 + \cdots + \zeta^{(p-1)\nu}\alpha_p$ is an eigenvector of σ, with eigenvalue $\zeta^{-\nu}$, unless it is zero.
6. Let $f(x) = x^3 + px + q$ be an irreducible polynomial over a subfield F of the complex numbers, with complex roots $\alpha = \alpha_1, \alpha_2, \alpha_3$. Let $K = F(\alpha)$.
   (a) Express $(6\alpha^2 + 2p)^{-1}$ explicitly, as a polynomial of degree 2 in α.
   (b) Assume that $\delta = \sqrt{D}$ is in F, so that K contains the other roots of f. Express α_2 as a polynomial in $\alpha = \alpha_1$ and δ.
   (c) Prove that $(1, \alpha_1, \alpha_2)$ is a basis of K, as F-vector space.
   (d) Let σ be the automorphism of K which permutes the three roots cyclically. Write the matrix of φ with respect to the above basis, and find its eigenvalues and eigenvectors.
   (e) Let v be an eigenvector with eigenvalue $\zeta = e^{2\pi i/3}$. Prove that if $\sqrt{-3} \in F$ then $v^3 \in F$. Compute v^3 explicitly, in terms of $p, q, \delta, \sqrt{-3}$.
   (f) Dropping the assumptions that δ and $\sqrt{-3}$ are in F, express v in terms of radicals.
   (g) Without calculation, determine the element v' which is obtained from v by interchanging the roles of α_1, α_2.
   (h) Express the root α_1 in terms of radicals.

8. Cyclotomic Extensions

1. Determine the degree of ζ_7 over the field $\mathbb{Q}(\zeta_3)$.
2. Let $\zeta = \zeta_{13}$, and let $K = \mathbb{Q}(\zeta)$. Determine the intermediate field of degree 3 over $\mathbb{Q}$ explicitly.
3. Let $\zeta = \zeta_{17}$. Determine the succession of square roots which generate the field $\mathbb{Q}(\zeta + \zeta^{16})$ explicitly.
4. Let $\zeta = \zeta_7$. Determine the degree of the following elements over $\mathbb{Q}$.
   (a) $\zeta + \zeta^5$ (b) $\zeta^3 + \zeta^4$ (c) $\zeta^3 + \zeta^5 + \zeta^6$
5. Let $\zeta = \zeta_{13}$. Determine the degree of the following elements over $\mathbb{Q}$.
   (a) $\zeta + \zeta^{12}$ (b) $\zeta + \zeta^2$ (c) $\zeta + \zeta^5 + \zeta^8$ (d) $\zeta^2 + \zeta^5 + \zeta^6$
   (e) $\zeta + \zeta^5 + \zeta^8 + \zeta^{12}$ (f) $\zeta + \zeta^2 + \zeta^5 + \zeta^{12}$ (g) $\zeta + \zeta^3 + \zeta^4 + \zeta^9 + \zeta^{10} + \zeta^{12}$
6. Let $\zeta = \zeta_{11}$.
   (a) Prove that $\alpha = \zeta + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^9$ generates a field of degree 2 over $\mathbb{Q}$, and find its equation.
   (b) Find an element which generates a subfield of degree 5 over $\mathbb{Q}$, and find its equation.
7. Prove that every quadratic extension of $\mathbb{Q}$ is contained in a cyclotomic extension.
8. Let $K = \mathbb{Q}(\zeta_n)$.
   (a) Prove that K is a Galois extension of $\mathbb{Q}$.

(b) Define an injective homomorphism $v\colon G(K/\mathbb{Q}) \longrightarrow U$ to the group U of units in the ring $\mathbb{Z}/(n)$.

(c) Prove that this homormophism is bijective when $n = 6, 8, 12$. (Actually, this map is always bijective.)

***9.** Let p be a prime, and let a be a rational number which is not a pth power. Let K be a splitting field of the polynomial $x^p - a$ over $\mathbb{Q}$.

(a) Prove that K is generated over $\mathbb{Q}$ by a pth root α of a and a primitive pth root ζ of unity.

(b) Prove that $[K : \mathbb{Q}] = p(p - 1)$.

(c) Prove that the Galois groups of $K/\mathbb{Q}$ is isomorphic to the group of invertible 2×2 matrices with entries in $\mathbb{F}_p$ of the form $\begin{bmatrix} a & b \\ & 1 \end{bmatrix}$, and describe the actions of the elements $\begin{bmatrix} a & \\ & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & b \\ & 1 \end{bmatrix}$ on the generators explicitly.

10. Determine the Galois group of the polynomials $x^8 - 1, x^{12} - 1, x^9 - 1$.

11. (a) Characterize the primes p such that the regular p-gon can be constructed by ruler and compass.

(b) Extend the characterization to the case of an n-gon, where n is not necessarily prime.

***12.** Let ν be a primitive element modulo a prime p, and let d be a divisor of $p - 1$. Show how to determine a sum of powers of $\zeta = \zeta_p$ which generates the subfield L of $\mathbb{Q}(\zeta)$ of degree d over $\mathbb{Q}$, using the list of roots of unity $\{\zeta, \zeta^{\nu}, \zeta^{\nu^2}, \dots, \zeta^{\nu^{p-2}}\}$.

9. Quintic Equations

1. Determine the transitive subgroups of S_5.

2. Let G be the Galois group of an irreducible quintic polynomial. Show that if G contains an element of order 3, then $G = S_5$ or A_5.

***3.** Let p be a prime integer, and let G be a p-group. Let H be a proper normal subgroup of G.

(a) Prove that the normalizer $N(H)$ of H is strictly larger than H.

(b) Prove that H is contained in a subgroup of index p and thát that subgroup is normal in G.

(c) Let K be a Galois extension of $\mathbb{Q}$ whose degree is a power of 2, and such that $K \subset \mathbb{R}$. Prove that the elements of K can be constructed by ruler and compass.

4. Let $K \supset L \supset F$ be a tower of field extensions of degree 2. Show that K can be generated over F by the root of an irreducible quartic polynomial of the form $x^4 + bx^2 + c$.

***5.** Cardano's Formula has a peculiar feature: Suppose that the coefficients p, q of the cubic are real numbers. A real cubic always has at least one real root. However, the square root appearing in the formula (2.6) will be imaginary if $(q/2)^2 + (p/3)^3 < 0$. In that case, the real root is displayed in terms of an auxiliary complex number u. This was considered to be an improper solution in Cardano's time. Let $f(x)$ be an irreducible cubic over a subfield F of $\mathbb{R}$, which has three real roots. Prove that no root of f is expressible by real radicals, that is, that there is no tower $F = F_0 \subset \dots \subset F_r$ as in (9.2), in which all the fields are subfields of $\mathbb{R}$.

6. Let $f(x) \in F[x]$ be an irreducible quintic polynomial, and let K be a splitting field for $f(x)$ over F.

(a) What are the possible Galois groups $G(K/F)$, assuming that the discriminant D is a square in F?

*(b) What are the possible Galois groups if D is not a square in F?

7. Determine which real numbers α of degree 4 over $\mathbb{Q}$ can be constructed with ruler and compass in terms of the Galois group of the corresponding polynomial.

8. Is every Galois extension of degree 10 solvable by radicals?

*9. Find a polynomial of degree 7 over $\mathbb{Q}$ whose Galois group is S_7.

Miscellaneous Problems

1. Let K be a Galois extension of F whose Galois group is the symmetric group S_4. What numbers occur as degrees of elements of K over F?

2. Show without computation that the side length of a regular pentagon inscribed in the unit circle has degree 2 over $\mathbb{Q}$.

3. (a) The nonnegative real numbers are those having a real square root. Use this fact to prove that the field $\mathbb{R}$ has no automorphism except the identity.

   (b) Prove that $\mathbb{C}$ has no *continuous* automorphisms except for complex conjugation and the identity.

4. Let K/F be a Galois extension with Galois group G, and let H be a subgroup of G. Prove that there exists an element $\beta \in K$ whose stabilizer is H.

*5. (a) Let K be a field of characteristic p. Prove that the *Frobenius* map φ defined by $\varphi(x) = x^p$ is a homomorphism from K to itself.

   (b) Prove that φ is an isomorphism if K is a finite field.

   (c) Give an example of an infinite field of characteristic p such that φ is not an isomorphism.

   (d) Let $K = \mathbb{F}_q$, where $q = p^r$, and let $F = \mathbb{F}_p$. Prove that $G(K/F)$ is a cyclic group of order r, generated by the Frobenius map φ.

   (e) Prove that the Main Theorem of Galois theory holds for the field extension K/F.

6. Let K be a subfield of $\mathbb{C}$, and let G be its group of automorphisms. We can view G as acting on the point set K in the complex plane. The action will probably be discontinuous, but nevertheless, we can define an action on line segments $[\alpha,\beta]$ whose endpoints are in K, by defining $g[\alpha,\beta] = [g\alpha, g\beta]$. Then G also acts on polygons whose vertices are in K.

   (a) Let $K = \mathbb{Q}(\zeta)$, where ζ is a primitive fifth root of 1. Find the G-orbit of the regular pentagon whose vertices are $1, \zeta, \zeta^2, \zeta^3, \zeta^4$.

   (b) Let α be the side length of the pentagon of (a). Show that $a = \alpha^2 \in K$, and find the irreducible equation for α over $\mathbb{Q}$. Is $\alpha \in K$?

7. A polynomial $f \in F[x_1,\dots,x_n]$ is called $\frac{1}{2}$-symmetric if $f(u_{\sigma 1},\dots,u_{\sigma n}) = f(u_1,\dots,u_n)$ for every even permutation σ of the indices, and skew-symmetric if $f(u_{\sigma 1},\dots,u_{\sigma n}) = (\text{sign}\ \sigma) f(u_1,\dots,u_n)$ for every permutation σ.

   (a) Prove that the square root of the discriminant $\delta = \Pi_{i<j}(u_i - u_j)$ is skew-symmetric.

   (b) Prove that every $\frac{1}{2}$-symmetric polynomial has the form $f + g\delta$, where f, g are symmetric polynomials.

*8. Let $f(x,y) \in \mathbb{C}[x,y]$ be an irreducible polynomial, which we regard as a polynomial $f(y)$ in y. Assume that f is cubic as a polynomial in y. Its discriminant D, computed with regard to the variable y, will be a polynomial in x. Assume that there is a root x_0 of $D(x)$ which is not a multiple root.

(a) Prove that the polynomial $f(x_0, y)$ in y has one simple root and one double root.

(b) Prove that the splitting field K of $f(y)$ over $\mathbb{C}(x)$ has degree 6.

9. Let K be a subfield of $\mathbb{C}$ which is a Galois extension of $\mathbb{Q}$. Prove or disprove: Complex conjugation carries K to itself, and therefore it defines an automorphism of K.

***10.** Let K be a finite extension of a field F, and let $f(x) \in K[x]$. Prove that there is a nonzero polynomial $g(x) \in K[x]$ such that $f(x)g(x) \in F[x]$.

***11.** Let $f(x)$ be an irreducible quartic polynomial in $F[x]$. Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be its roots in a splitting field K. Assume that the resolvent cubic has a root $\beta = \alpha_1\alpha_2 + \alpha_3\alpha_4$ in F, but that the discriminant D is not a square in F. According to the text, the Galois group of K/F is either C_4 or D_4.

(a) Determine the subgroup H of the group S_4 of permutations of the roots α_i which stabilizes β explicitly. Don't forget to prove that no permutations other than those you list fix β.

(b) Let $\gamma = \alpha_1\alpha_2 - \alpha_3\alpha_4$ and $\epsilon = \alpha_1 + \alpha_2 - \alpha_3 - \alpha_4$. Describe the action of H on these elements.

(c) Prove that γ^2 and ϵ^2 are in F.

(d) Let δ be the square root of the discriminant. Prove that if $\gamma \neq 0$, then $\delta\gamma$ is a square in F if and only if $G = C_4$. Similarly, prove that if $\epsilon \neq 0$, then $\delta\epsilon$ is a square in F if and only if $G = C_4$.

(e) Prove that γ and ϵ can't both be zero.

***12.** Let $F = \mathbb{F}_p(u, v)$ be a rational function field in two variables over the field $\mathbb{F}_p$ with p elements, and let $K = F(\alpha, \beta)$, where α, β are roots of the polynomials $x^p - u$ and $x^p - v$ respectively. Prove the following.

(a) The extension K/F has no primitive element.

(b) The elements $\gamma = \beta + c\alpha$, where $c \in F$, generate infinitely many different intermediate fields L.

***13.** Let K be a field with p^r elements. Prove that the Frobenius map defined by $\varphi(x) = x^p$ is a linear transformation of K, when K is viewed as a vector space the prime field $F = \mathbb{F}_p$, and determine its eigenvectors and eigenvalues.

Wie weit diese Methoden reichen werden, muss erst die Zukunft zeigen.

Emmy Noether