for our Galois group G, are the groups

$S_4, \quad A_4$

$D_8 = \{1, (1324), (12)(34), (1423), (13)(24), (14)(23), (12), (34)\}$ and its conjugates

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

$C = \{1, (1234), (13)(24), (1432)\}$ and its conjugates.

(D_8 is the dihedral group, a Sylow 2-subgroup of S_4, with 3 (isomorphic) conjugate subgroups in S_4, V is the Klein 4-subgroup of S_4, normal in S_4, and C is a cyclic group, with 3 (isomorphic) conjugates in S_4).

Consider the elements

$$\theta_1 = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4)$$
$$\theta_2 = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4)$$
$$\theta_3 = (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3)$$

in the splitting field for $g(y)$. These elements are permuted amongst themselves by the permutations in S_4. The stabilizer of θ_1 in S_4 is the dihedral group D_8. The stabilizers in S_4 of θ_2 and θ_3 are the conjugate dihedral subgroups of order 8. The subgroup of S_4 which stabilizes all three of these elements is the intersection of these subgroups, namely the Klein 4-group V.

Since S_4 merely permutes $\theta_1, \theta_2, \theta_3$ it follows that the elementary symmetric functions in the θ's are fixed by all the elements of S_4, hence are in F. An elementary computation in symmetric functions shows that these elementary symmetric functions are $2p$, $p^2 - 4r$, and $-q^2$, which shows that $\theta_1, \theta_2, \theta_3$ are the roots of

$$h(x) = x^3 - 2px^2 + (p^2 - 4r)x + q^2$$

called the *resolvent cubic* for the quartic $g(y)$. Since

$$\begin{aligned}\theta_1 - \theta_2 &= \alpha_1\alpha_3 + \alpha_2\alpha_4 - \alpha_1\alpha_2 - \alpha_3\alpha_4 \\ &= -(\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3)\end{aligned}$$

and similarly

$$\begin{aligned}\theta_1 - \theta_3 &= -(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_4) \\ \theta_2 - \theta_3 &= -(\alpha_1 - \alpha_2)(\alpha_3 - \alpha_4)\end{aligned}$$

we see that the discriminant of the resolvent cubic is the *same* as the discriminant of the quartic $g(y)$, hence also as the discriminant of the quartic $f(x)$. Using our formula for the discriminant of the cubic, we can easily compute the discriminant in terms of p, q, r:

$$D = 16p^4r - 4p^3q^2 - 128p^2r^2 + 144pq^2r - 27q^4 + 256r^3$$

from which one can give the formula for D in terms of a, b, c, d:

$$\begin{aligned}D = &- 128b^2d^2 - 4a^3c^3 + 16b^4d - 4b^3c^2 - 27a^4d^2 + 18abc^3 \\ &+ 144a^2bd^2 - 192acd^2 + a^2b^2c^2 - 4a^2b^3d - 6a^2c^2d \\ &+ 144bc^2d + 256d^3 - 27c^4 - 80ab^2cd + 18a^3bcd.\end{aligned}$$

The splitting field for the resolvent cubic is a subfield of the splitting field of the quartic, so the Galois group of the resolvent cubic is a quotient of G. Hence knowing the action of the Galois group on the roots of the resolvent cubic $h(x)$ gives information about the Galois group of $g(y)$, as follows:

(Galois group of a quartic)

a. Suppose first that the resolvent cubic is irreducible. If D is not a square, then G is not contained in A_4 and the Galois group of the resolvent cubic is S_3, which implies that the degree of the splitting field for $g(y)$ is divisible by 6. The only possibility is then $G = S_4$.

b. If the resolvent cubic is irreducible and D is a square, then G is a subgroup of A_4 and 3 divides the order of G (the Galois group of the resolvent cubic is A_3). The only possibility is $G = A_4$.

c1. We are left with the case where the resolvent cubic is reducible. The first possibility is that $h(x)$ has 3 roots in F (i.e., splits completely). Since each of the elements $\theta_1, \theta_2, \theta_3$ is in F, every element of G fixes all three of these elements, which means $G \subseteq V$. The only possibility is $G = V$.

c2. If $h(x)$ splits into a linear and a quadratic, then precisely one of $\theta_1, \theta_2, \theta_3$ is in F, say θ_1. Then G stabilizes θ_1 but not θ_2 and θ_3, so we have $G \subseteq D_8$ and $G \not\subseteq V$. This leaves two possibilities: $G = D_8$ or $G = C$. One way to distinguish between these is to observe that $F(\sqrt{D})$ is the fixed field of the elements of G in A_4. For the two cases being considered, we have $D_8 \cap A_4 = V$, $C \cap A_4 = \{1, (13)(24)\}$. The first group is transitive on the roots of $g(y)$, the second is not. It follows that the first case occurs if and only if $g(y)$ is irreducible over $F(\sqrt{D})$. We may therefore determine G completely by factoring $g(y)$ in $F(\sqrt{D})$, and so completely determine the Galois group in all cases. (cf. the exercises following and in the next section, where it is shown that over $\mathbb{Q}$ the Galois group cannot be cyclic of degree 4 if D is not the sum of two squares — so in particular if $D < 0$.)

We shall give explicit formulas for the roots of a quartic polynomial at the end of the next section.

The Fundamental Theorem of Algebra

We end this section with two proofs of the Fundamental Theorem of Algebra. We need two facts regarding the field $\mathbb{C}$:

(a) Every polynomial with real coefficients of odd degree has a root in the reals. Equivalently, there are no nontrivial finite extensions of $\mathbb{R}$ of odd degree.

(b) Quadratic polynomials with coefficients in $\mathbb{C}$ have roots in $\mathbb{C}$. Equivalently, there are no quadratic extensions of $\mathbb{C}$.

The first result follows from the Intermediate Value Theorem in calculus, since the graph of a monic polynomial $f(x) \in \mathbb{R}[x]$ of odd degree is negative for large negative values of x and positive for large positive values of x, hence crosses the axis somewhere. The equivalence with the second statement follows since a finite extension of $\mathbb{R}$ is a simple extension and the minimal polynomial of a primitive element would have odd degree, hence would be both irreducible over $\mathbb{R}$ and have a root in $\mathbb{R}$, hence must be of degree 1.

The second result follows by a direct computation. By the quadratic formula it suffices to show that every complex number $\alpha = a + bi$, $a, b \in \mathbb{R}$, has a square root in $\mathbb{C}$. Write $\alpha = re^{i\theta}$ for some $r \geq 0$ and some $\theta \in [0, 2\pi)$. Then $\sqrt{r}e^{i\theta/2}$ is a square root of α. (Explicitly, let $c \in \mathbb{R}$ be a square root of the real number $\dfrac{a + \sqrt{a^2+b^2}}{2}$ and let $d \in \mathbb{R}$ be a square root of the real number $\dfrac{-a + \sqrt{a^2+b^2}}{2}$ where the signs of the two square roots are chosen so that cd has the same sign as b. Then multiplying out we see that $(c + di)^2 = a + bi$.)

Theorem 35. *(Fundamental Theorem of Algebra)* Every polynomial $f(x) \in \mathbb{C}[x]$ of degree n has precisely n roots in $\mathbb{C}$ (counted with multiplicity). Equivalently, $\mathbb{C}$ is algebraically closed.

Proof: I. It suffices to prove that every polynomial $f(x) \in \mathbb{C}[x]$ has a root in $\mathbb{C}$. Let τ denote the automorphism complex conjugation. If $f(x)$ has no root in $\mathbb{C}$ then neither does the conjugate polynomial $\bar{f}(x) = \tau f(x)$ obtained by applying τ to the coefficients of $f(x)$ (since its roots are the conjugates of the roots of $f(x)$). The product $f(x)\bar{f}(x)$ has coefficients which are invariant under complex conjugation, hence has real coefficients. It suffices then to prove that a polynomial with real coefficients has a root in $\mathbb{C}$.

Suppose that $f(x)$ is a polynomial of degree n with real coefficients and write $n = 2^k m$ where m is odd. We prove that $f(x)$ has a root in $\mathbb{C}$ by induction on k. For $k = 0$, $f(x)$ has odd degree and by (a) above $f(x)$ has a root in $\mathbb{R}$ so we are done. Suppose now that $k \geq 1$. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the roots of $f(x)$ and set $K = \mathbb{R}(\alpha_1, \alpha_2, \ldots, \alpha_n, i)$. Then K is a Galois extension of $\mathbb{R}$ containing $\mathbb{C}$ and the roots of $f(x)$. For any $t \in \mathbb{R}$ consider the polynomial

$$L_t = \prod_{1 \leq i < j \leq n} [x - (\alpha_i + \alpha_j + t\alpha_i\alpha_j)].$$

Any automorphism of $K/\mathbb{R}$ permutes the terms in this product so the coefficients of L_t are invariant under all the elements of $\mathrm{Gal}(K/\mathbb{R})$. Hence L_t is a polynomial with real coefficients. The degree of L_t is

$$\frac{n(n-1)}{2} = 2^{k-1}m(2^k m - 1) = 2^{k-1}m'$$

where m' is odd (since $k \geq 1$). The power of 2 in this degree is therefore less than k, so by induction the polynomial L_t has a root in $\mathbb{C}$. Hence for each $t \in \mathbb{R}$ one of the elements $\alpha_i + \alpha_j + t\alpha_i\alpha_j$ for some i, j $(1 \leq i < j \leq n)$ is an element of $\mathbb{C}$. Since there are infinitely many choices for t and only finitely many values of i and j we see that for some i and j (say, $i = 1$ and $j = 2$) there are distinct real numbers s and t with

$$\alpha_1 + \alpha_2 + s\alpha_1\alpha_2 \in \mathbb{C} \qquad \alpha_1 + \alpha_2 + t\alpha_1\alpha_2 \in \mathbb{C}.$$

Since $s \neq t$ it follows that $a = \alpha_1 + \alpha_2 \in \mathbb{C}$ and $b = \alpha_1\alpha_2 \in \mathbb{C}$. But then α_1 and α_2 are the roots of the quadratic $x^2 - ax + b$ with coefficients in $\mathbb{C}$, hence are elements of $\mathbb{C}$ by (b) above, completing the proof.

II. The second proof again uses (a) and (b) above, but replaces the computations with the polynomials L_t above with a simple group-theoretic argument involving the nilpotency of a Sylow 2-subgroup of the Galois group:

Let $f(x)$ be a polynomial of degree n with real coefficients and let K be the splitting field of $f(x)$ over $\mathbb{R}$. Then $K(i)$ is a Galois extension of $\mathbb{R}$. Let G denote its Galois group and let P_2 denote a Sylow 2-subgroup of G. The fixed field of P_2 is an extension of $\mathbb{R}$ of odd degree, hence by (a) is trivial.

It follows that $\mathrm{Gal}(K(i)/\mathbb{C})$ is a 2-group. Since 2-groups have subgroups of all orders (recall this is true of a finite p-group for any prime p, cf. Theorem 6.1), if this group is nontrivial, there would exist a quadratic extension of $\mathbb{C}$, impossible by (b), completing the proof.

The Fundamental Theorem of Algebra was first rigorously proved by Gauss in 1816 (his doctoral dissertation in 1798 provides a proof using geometric considerations requiring some topological justification). The first proof above is essentially due to Laplace in 1795 (hence the reason for naming the polynomials L_t). The reason Laplace's proof was deemed unacceptable was that he assumed the existence of a splitting field for polynomials (i.e., that the roots existed *somewhere* in *some* field), which had not been established at that time. The elegant second proof is a simplification due to Artin.

EXERCISES

1. Show that a cubic with a multiple root has a linear factor. Is the same true for quartics?

2. Determine the Galois groups of the following polynomials:
 (a) $x^3 - x^2 - 4$
 (b) $x^3 - 2x + 4$
 (c) $x^3 - x + 1$
 (d) $x^3 + x^2 - 2x - 1$.

3. Prove for any $a, b \in \mathbb{F}_{p^n}$ that if $x^3 + ax + b$ is irreducible then $-4a^3 - 27b^2$ is a square in $\mathbb{F}_{p^n}$.

4. Determine the Galois group of $x^4 - 25$.

5. Determine the Galois group of $x^4 + 4$.

6. Determine the Galois group of $x^4 + 3x^3 - 3x - 2$.

7. Determine the Galois group of $x^4 + 2x^2 + x + 3$.

8. Determine the Galois group of $x^4 + 8x + 12$.

9. Determine the Galois group of $x^4 + 4x - 1$ (cf. Exercise 19).

10. Determine the Galois group of $x^5 + x - 1$.

11. Let F be an extension of $\mathbb{Q}$ of degree 4 that is not Galois over $\mathbb{Q}$. Prove that the Galois closure of F has Galois group either S_4, A_4 or the dihedral group D_8 of order 8. Prove that the Galois group is dihedral if and only if F contains a quadratic extension of $\mathbb{Q}$.

12. Prove that an extension F of $\mathbb{Q}$ of degree 4 can be generated by the root of an irreducible biquadratic $x^4 + ax^2 + b$ over $\mathbb{Q}$ if and only if F contains a quadratic extension of $\mathbb{Q}$.