Recall the *lexicographic monomial order* with $x_1 > x_2 > \cdots > x_n$ defined in Section 9.6, where the nonzero monomial term with exponents $(a_1, a_2, \ldots, a_n)$ comes before the nonzero monomial term with exponents $(b_1, b_2, \ldots, b_n)$ if the initial components of the two n-tuples of exponents are equal and the first component where they differ has $a_i > b_i$. If $f(x_1, \ldots, x_n)$ contains the monomial $Ax_1^{a_1}x_2^{a_2}\ldots x_n^{a_n}$ then since $f(x_1, \ldots, x_n)$ is symmetric it also contains all the permuted monomials. Among these choose the lexicographically largest monomial, which therefore satisfies $a_1 \geq a_2 \geq \cdots \geq a_n \geq 0$.

38. **(a)** Show that the monomial $As_1^{a_1-a_2}s_2^{a_2-a_3}\cdots s_n^{a_n}$ in the elementary symmetric functions has the same lexicographic initial term.

(b) Show that subtracting $As_1^{a_1-a_2}s_2^{a_2-a_3}\cdots s_n^{a_n}$ from $f(x)$ yields either 0 or a symmetric polynomial of the same degree whose terms are lexicographically smaller than the terms in $f(x_1, \ldots, x_n)$.

(c) Show that the iteration of this procedure (lexicographic ordering, choosing the lexicographically largest term, subtracting the associated monomial in the elementary symmetric functions) terminates, expressing $f(x_1, \ldots, x_n)$ as a polynomial in the elementary symmetric functions.

39. Use the algorithm described in Exercise 38 to prove that a polynomial $f(x_1, \ldots, x_n)$ that is symmetric in $x_1, \ldots, x_n$ can be expressed *uniquely* as a polynomial in the elementary symmetric functions.

40. Use the procedure in Exercise 38 to express each of the following symmetric functions as a polynomial in the elementary symmetric functions:

(a) $(x_1 - x_2)^2$

(b) $x_1^2 + x_2^2 + x_3^2$

(c) $x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2$.

41. Use the procedure in Exercise 38 to express $\sum_{i \neq j} x_i^2 x_j$ as a polynomial in the elementary symmetric functions.

We now know that a symmetric polynomial $f(x_1, \ldots, x_n)$ can be written uniquely as a polynomial in the elementary symmetric functions. Using this existence and uniqueness we can describe an alternate and computationally useful method for determining the coefficients of the elementary symmetric functions in this polynomial. As in Exercise 37 we may assume that $f(x_1, \ldots, x_n)$ is homogeneous of degree M. Let N be the maximum degree of any of the variables $x_1, \ldots, x_n$ in $f(x_1, \ldots, x_n)$.

(a) Determine all of the possible monomials $A_i s_1^{a_1}s_2^{a_2}\cdots s_n^{a_n}$ appearing in $f(x_1, \ldots, x_n)$ from the constraints

$$a_1 + 2a_2 + \cdots + na_n = M$$
$$a_1 + a_2 + \cdots + a_n \leq N.$$

(b) Since $f(x_1, \ldots, x_n) = \sum A_i s_1^{a_1}s_2^{a_2}\cdots s_n^{a_n}$ is a polynomial *identity*, it is valid for any substitution of values for $x_1, \ldots, x_n$. Each substitution into this equation gives a linear relation on the coefficients A_i and so a sufficient number of substitutions will determine the A_i.

42. Show that the function $(x_1 + x_2 - x_3 - x_4)(x_1 + x_3 - x_2 - x_4)(x_1 + x_4 - x_2 - x_3)$ is symmetric in x_1, x_2, x_3, x_4 and use the preceding procedure to prove it can be expressed as a polynomial in the elementary symmetric functions as $s_1^3 - 4s_1s_2 + 8s_3$.

43. Express each of the following in terms of the elementary symmetric functions:

(a) $\sum_{i \neq j} x_i^2 x_j$ **(b)** $\sum_{i,j,k \text{ distinct}} x_i^2 x_j x_k$ **(c)** $\sum_{i,j,k \text{ distinct}} x_i^2 x_j^2 x_k^2$.

44. Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be the roots of a quartic polynomial $f(x)$ over $\mathbb{Q}$. Show that the quantities $\alpha_1\alpha_2 + \alpha_3\alpha_4$, $\alpha_1\alpha_3 + \alpha_2\alpha_4$, and $\alpha_1\alpha_4 + \alpha_2\alpha_3$ are permuted by the Galois group of $f(x)$. Conclude that these elements are the roots of a cubic polynomial with coefficients in $\mathbb{Q}$ (also sometimes referred to as the *resolvent cubic* of $f(x)$).

45. If $f(x) = x^3 + px + q \in \mathbb{Z}[x]$ is irreducible, prove that its discriminant $D = -4p^3 - 27q^2$ is an integer not equal to $0, \pm 1$.

46. Prove that every finite group occurs as the Galois group of a field extension of the form $F(x_1, x_2, \ldots, x_n)/E$.

47. Let F be a field of characteristic 0 in which every cubic polynomial has a root. Let $f(x)$ be an irreducible quartic polynomial over F whose discriminant is a square in F. Determine the Galois group of $f(x)$.

48. This exercise determines the splitting field K for the polynomial $f(x) = x^6 - 2x^3 - 2$ over $\mathbb{Q}$ (cf. also Exercise 2 of Section 8).

(a) Prove that $f(x)$ is irreducible over $\mathbb{Q}$ with roots the three cube roots of $1 \pm \sqrt{3}$.

(b) Prove that K contains the field $\mathbb{Q}(\sqrt{-3})$ of 3rd roots of unity and contains $\mathbb{Q}(\sqrt{3})$, hence contains the biquadratic field $F = \mathbb{Q}(i, \sqrt{3})$. Take the product of two of the roots in (a) to prove that K contains $\sqrt[3]{2}$ and conclude that K is an extension of the field $L = \mathbb{Q}(\sqrt[3]{2}, i, \sqrt{3})$.

(c) Prove that $[L : \mathbb{Q}] = 12$ and that K is obtained from L by adjoining the cube root of an element in L, so that $[K : \mathbb{Q}] = 12$ or 36.

(d) Prove that if $[K : \mathbb{Q}] = 12$ then $K = \mathbb{Q}(\sqrt[3]{2}, i, \sqrt{3})$ and that $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to the direct product of the cyclic group of order 2 and S_3. Prove that if $[K : \mathbb{Q}] = 12$ then there is a unique real cubic subfield in K, namely $\mathbb{Q}(\sqrt[3]{2})$.

(e) Take the quotient of the two real roots in (a) to show that $\sqrt[3]{2 + \sqrt{3}}$ and $\sqrt[3]{2 - \sqrt{3}}$ (real roots) are both elements of K. Show that $\alpha = \sqrt[3]{2 + \sqrt{3}} + \sqrt[3]{2 - \sqrt{3}}$ is a real root of the irreducible cubic equation $x^3 - 3x - 4$ whose discriminant is $-2^2 3^4$. Conclude that the Galois closure of $\mathbb{Q}(\alpha)$ contains $\mathbb{Q}(i)$ so in particular $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\sqrt[3]{2})$.

(f) Conclude from (e) that $G = \mathrm{Gal}(K/\mathbb{Q})$ is of order 36. Determine all the elements of G explicitly and in particular show that G is isomorphic to $S_3 \times S_3$.

49. Prove that the Galois group over $\mathbb{Q}$ of $x^6 - 4x^3 + 1$ is isomorphic to the dihedral group of order 12. [Observe that the two real roots are inverses of each other.]

50. *(Criterion for the Galois Group of an Irreducible Cubic over an Arbitrary Field)* Suppose K is a field and $f(x) = x^3 + ax^2 + bx + c \in K[x]$ is irreducible, so the Galois group of $f(x)$ over K is either S_3 or A_3.

(a) Show that the Galois group of $f(x)$ is A_3 if and only if the resultant quadratic polynomial $g(x) = x^2 + (ab - 3c)x + (b^3 + a^3c - 6abc + 9c^2)$ has a root in K. [If α, β, γ are the roots of $f(x)$ show that the Galois group is A_3 if and only if the element $\theta = \alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2$ is an element of K and that θ is a root of $g(x)$.] Show that the discriminant of $g(x)$ is the same as the discriminant of $f(x)$.

(b) $(\mathrm{ch}(K) \neq 2)$ If K has characteristic different from 2 show either from (a) or directly from the definition of the discriminant that the Galois group of $f(x)$ is A_3 if and only if the discriminant of $f(x)$ is a square in K.

(c) $(\mathrm{ch}(K) = 2)$ If K has characteristic 2 show that the discriminant of $f(x)$ is always a square. Show that $f(x)$ can be taken to be of the form $x^3 + px + q$ and that the Galois group of $f(x)$ is A_3 if and only if the quadratic $x^2 + qx + (p^3 + q^2)$ has a root in K (equivalently, if $(p^3 + q^2)/q^2 \in K$ is in the image of the *Artin–Schreier map* $x \mapsto x^2 - x$ mapping K to K).

(d) If $K = \mathbb{F}_2(t)$ where t is transcendental over $\mathbb{F}_2$. Prove that the polynomials $x^3 + t^2x + t^3$, $x^3 + (t^2 + t + 1)x + (t^2 + t + 1)$, and $x^3 + (t^2 + t + 1)x + (t^3 + t^2 + t)$ have A_3 as Galois group while $x^3 + t^2x + t$ and $x^3 = x + t$ have S_3 as Galois group.

51. This exercise proves *Sturm's Theorem* determining the number of real roots of a polynomial $f(x) \in \mathbb{R}[x]$ in an interval $[a, b]$. The multiple roots of $f(x)$ are zeros of the g.c.d. of $f(x)$ and its derivative $f'(x)$, and it follows that to determine the real roots of $f(x)$ in $[a, b]$ we may assume that the roots of $f(x)$ are *simple*.

Apply the Euclidean algorithm to $f_0(x) = f(x)$ and its derivative $f_1(x) = f'(x)$ using the *negative* of the remainder at each stage to find a sequence of polynomials $f(x), f'(x), f_2(x), \ldots, f_n(x)$ with

$$f_{i-1}(x) = q_i(x)f_i(x) - f_{i+1}(x) \qquad i = 0, 1, \ldots, n-1$$

where $f_n(x) \in \mathbb{R}$ is a nonzero constant.

(a) Prove that consecutive polynomials $f_i(x)$, $f_{i+1}(x)$ for $i = 0, 1, \ldots, n-1$ have no common zeros. [Show that otherwise $f_{i+2}(c) = f_{i+3}(c) = \cdots = 0$, and derive a contradiction.]

(b) If $f_i(c) = 0$ for some $i = 0, 1, \ldots, n-1$, prove that one of the two values $f_{i-1}(c)$, $f_{i+1}(c)$ is strictly negative and the other is strictly positive.

For any real number α, let $V(\alpha)$ denote the number of sign changes in the *Sturm sequence* of real numbers

$$f(\alpha), f'(\alpha), f_2(\alpha), \ldots, f_n(\alpha),$$

ignoring any 0's that appear (for example $-1, -2, 0, +3, -4$ has signs $--+-$ disregarding the 0, so there are 2 sign changes, the first from -2 to $+3$, the second from $+3$ to -4).

(c) Suppose $\alpha < \beta$ and that all the elements in the Sturm sequences for α and for β are nonzero. Prove that unless $f_i(c) = 0$ for some $\alpha < c < \beta$ and some $i = 0, 1, \ldots, n-1$, then the signs of all the elements in these two Sturm sequences are the same, so in particular $V(\alpha) = V(\beta)$.

(d) If $f_j(c) = 0$ prove that there is a sufficiently small interval (α, β) containing c so that $f_j(x)$ has no zero other than c for $\alpha < x < \beta$.

(e) If $j \geq 1$ in (d), prove that the number of sign changes in $f_{j-1}(\alpha)$, $f_j(\alpha)$, $f_{j+1}(\alpha)$ and in $f_{j-1}(\beta)$, $f_j(\beta)$, $f_{j+1}(\beta)$ are the same. [Observe that $f_{j-1}(c)$ and $f_{j+1}(c)$ have opposite signs by (b) and $f_{j-1}(x)$ and $f_{j+1}(x)$ do not change sign in (α, β).]

(f) If $j = 0$ in (d) show that the number of sign changes in $f(\alpha)$, $f'(\alpha)$ is one more than the number of sign changes in $f(\beta)$, $f'(\beta)$. [If $f'(c) > 0$ then $f(x)$ is increasing at c, so that $f(\alpha) < 0$, $f(\beta) > 0$, and $f'(x)$ does not change sign in (α, β), so the signs change from $-+$ to $++$. Similarly if $f'(c) < 0$.]

(g) Prove *Sturm's Theorem*: if $f(x)$ is a polynomial with real coefficients all of whose real roots are simple then the number of real zeros of $f(x)$ in an interval $[a, b]$ where $f(a)$ and $f(b)$ are both nonzero is given by $V(a) - V(b)$. [Use (c), (e) and (f) to see that as α runs from a to b the number $V(\alpha)$ of sign changes is constant unless α passes through a zero of $f(x)$, in which case it decreases by precisely 1.]

(h) Suppose $f(x) = x^5 + px + q \in \mathbb{R}[x]$ has simple roots. Show that the sequence of polynomials above is given by $f(x)$, $5x^4 + p$, $(-4p/5)x + q$, and $-D/(256p^4)$ where $D = 256p^5 + 3125q^4$ is the discriminant of $f(x)$. Conclude for $p > 0$ that $f(x)$ has precisely one real root and for $p < 0$ that $f(x)$ has precisely 1 or 3 real roots depending on whether $D > 0$ or $D < 0$, respectively. [E.g., if $p < 0$ and $D < 0$ then at $-\infty$ the signs are $- + -+$ with 3 sign changes and at $+\infty$ the signs are $+ + ++$ with no sign changes.]