13. (a) Let $\pm\alpha, \pm\beta$ denote the roots of the polynomial $f(x) = x^4 + ax^2 + b \in \mathbb{Z}[x]$. Prove that $f(x)$ is irreducible if and only if $\alpha^2, \alpha \pm \beta$ are not elements of $\mathbb{Q}$.[3]

(b) Suppose $f(x)$ is irreducible and let G be the Galois group of $f(x)$. Prove that

(i) $G \cong V$, the Klein 4-group, if and only if b is a square in $\mathbb{Q}$ if and only if $\alpha\beta \in \mathbb{Q}$ is rational.

(ii) $G \cong C$, the cyclic group of order 4, if and only if $b(a^2 - 4b)$ is a square in $\mathbb{Q}$ if and only if $\mathbb{Q}(\alpha\beta) = \mathbb{Q}(\alpha^2)$.

(iii) $G \cong D_8$, the dihedral group of order 8, if and only if b and $b(a^2 - 4b)$ are not squares in $\mathbb{Q}$ if and only if $\alpha\beta \notin \mathbb{Q}(\alpha^2)$.

14. Prove the polynomial $x^4 - px^2 + q \in \mathbb{Q}[x]$ is irreducible for any distinct odd primes p and q and has as Galois group the dihedral group of order 8.[4]

15. Prove the polynomial $x^4 + px + p \in \mathbb{Q}[x]$ is irreducible for every prime p and for $p \neq 3, 5$ has Galois group S_4. Prove the Galois group for $p = 3$ is dihedral of order 8 and for $p = 5$ is cyclic of order 4.[5]

16. Determine the Galois group over $\mathbb{Q}$ of the polynomial $x^4 + 8x^2 + 8x + 4$. Determine which of the subfields of this field are Galois over $\mathbb{Q}$ and for those which are Galois determine a polynomial $f(x) \in \mathbb{Q}[x]$ for which they are the splitting field over $\mathbb{Q}$.

17. Find the Galois group of $x^4 - 7$ over $\mathbb{Q}$ explicitly as a permutation group on the roots.

18. Let θ be a root of $x^3 - 3x + 1$. Prove that the splitting field of this polynomial is $\mathbb{Q}(\theta)$ and that the Galois group is cyclic of order 3. In particular the other roots of this polynomial can be written in the form $a + b\theta + c\theta^2$ for some $a, b, c \in \mathbb{Q}$. Determine the other roots explicitly in terms of θ.

19. Let $f(x)$ be an irreducible polynomial of degree 4 in $\mathbb{Q}[x]$ with discriminant D. Let K denote the splitting field of $f(x)$, viewed as a subfield of the complex numbers $\mathbb{C}$.

(a) Prove that $\mathbb{Q}(\sqrt{D}) \subset K$.

(b) Let τ denote complex conjugation and let τ_K denote the restriction of complex conjugation to K. Prove that τ_K is an element of $\mathrm{Gal}(K/\mathbb{Q})$ of order 1 or 2 depending on whether every element of K is real or not.

(c) Prove that if $D < 0$ then K cannot be cyclic of degree 4 over $\mathbb{Q}$ (i.e., $\mathrm{Gal}(K/\mathbb{Q})$ cannot be a cyclic group of order 4).

(d) Prove generally that $\mathbb{Q}(\sqrt{D})$ for squarefree $D < 0$ is not a subfield of a cyclic quartic field (cf. also Exercise 19 of Section 7).

20. Determine the Galois group of $(x^3 - 2)(x^3 - 3)$ over $\mathbb{Q}$. Determine all the subfields which contain $\mathbb{Q}(\rho)$ where ρ is a primitive 3^{rd} root of unity.

21. Let $G \leq S_n$ be a subgroup of the symmetric group and suppose $\sigma_1, \ldots, \sigma_k$ are generators for G. If the function $f(x_1, x_2, \ldots, x_n)$ is fixed by the generators σ_i show it is fixed by G.

22. (*Newton's Formulas*) Let $f(x)$ be a monic polynomial of degree n with roots $\alpha_1, \ldots, \alpha_n$. Let s_i be the elementary symmetric function of degree i in the roots and define $s_i = 0$ for $i > n$. Let $p_i = \alpha_1^i + \cdots + \alpha_n^i$, $i \geq 0$, be the sum of the i^{th} powers of the roots of $f(x)$.

---

[3] cf. the note *An Elementary Test for the Galois Group of a Quartic Polynomial*, Luise-Charlotte Kappe and Bette Warren, Amer. Math. Monthly, 96(1989), pp. 133–137.

[4] Ibid.

[5] Ibid.

Prove *Newton's Formulas*:

$$\begin{aligned}
&p_1 - s_1 = 0\\
&p_2 - s_1 p_1 + 2s_2 = 0\\
&p_3 - s_1 p_2 + s_2 p_1 - 3s_3 = 0\\
&\quad\vdots\\
&p_i - s_1 p_{i-1} + s_2 p_{i-2} - \cdots + (-1)^{i-1} s_{i-1} p_1 + (-1)^i i s_i = 0
\end{aligned}$$

23. **(a)** If $x + y + z = 1$, $x^2 + y^2 + z^2 = 2$ and $x^3 + y^3 + z^3 = 3$, determine $x^4 + y^4 + z^4$.
(b) Prove generally that x, y, z are not rational but that $x^n + y^n + z^n$ is rational for every positive integer n.

24. Prove that an $n \times n$ matrix A over a field of characteristic 0 is nilpotent if and only if the trace of A^k is 0 for all $k \geq 0$.

25. Prove that two $n \times n$ matrices A and B over a field of characteristic 0 have the same characteristic polynomial if and only if the trace of A^k equals the trace of B^k for all $k \geq 0$.

26. Use the fact that the trace of AB is the same as the trace of BA for any two $n \times n$ matrices A and B to show that AB and BA have the same characteristic polynomial over a field of characteristic 0 (the same result is true over a field of arbitrary characteristic).

27. Let $f(x)$ be a monic polynomial of degree n with roots $\alpha_1, \alpha_2, \ldots, \alpha_n$.
(a) Show that the discriminant D of $f(x)$ is the square of the Vandermonde determinant

$$\begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \ldots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \ldots & \alpha_n^{n-1} \end{vmatrix} = \prod_{i>j}(\alpha_i - \alpha_j).$$

(b) Taking the Vandermonde matrix above, multiplying on the left by its transpose and taking the determinant show that one obtains

$$D = \begin{vmatrix} p_0 & p_1 & p_2 & \cdots & p_{n-1} \\ p_1 & p_2 & p_3 & \cdots & p_n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p_{n-1} & p_n & p_{n+1} & \cdots & p_{2n-2} \end{vmatrix}$$

where $p_i = \alpha_1^i + \cdots + \alpha_n^i$ is the sum of the i^{th} powers of the roots of $f(x)$, which can be computed in terms of the coefficients of $f(x)$ using Newton's formulas above. This gives an efficient procedure for calculating the discriminant of a polynomial.

28. Let α be a root of the irreducible polynomial $f(x) \in F[x]$ and let $K = F(\alpha)$. Let D be the discriminant of $f(x)$. Prove that $D = (-1)^{n(n-1)/2} \mathrm{N}_{K/F}(f'(\alpha))$, where $f'(x) = D_x f(x)$ is the derivative of $f(x)$.

The following exercises describe the *resultant* of two polynomials and in particular provide another efficient method for calculating the discriminant of a polynomial.

29. Let F be a field and let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ and $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$ be two polynomials in $F[x]$.
(a) Prove that a necessary and sufficient condition for $f(x)$ and $g(x)$ to have a common root (or, equivalently, a common divisor in $F[x]$) is the existence of a polynomial

$a(x) \in F[x]$ of degree at most $m-1$ and a polynomial $b(x) \in F[x]$ of degree at most $n-1$ with $a(x)f(x) = b(x)g(x)$.

(b) Writing $a(x)$ and $b(x)$ explicitly as polynomials show that equating coefficients in the equation $a(x)f(x) = b(x)g(x)$ gives a system of $n+m$ linear equations for the coefficients of $a(x)$ and $b(x)$. Prove that this system has a nontrivial solution (hence $f(x)$ and $g(x)$ have a common zero) if and only if the determinant

$$R(f,g) = \begin{vmatrix} a_n & a_{n-1} & \cdots & a_0 & & & & \\ & a_n & a_{n-1} & \cdots & a_0 & & & \\ & & a_n & a_{n-1} & \cdots & a_0 & & \\ & & & \ddots & & & & \\ & & & & a_n & a_{n-1} & \cdots & a_0 \\ b_m & b_{m-1} & \cdots & b_0 & & & & \\ & b_m & b_{m-1} & \cdots & b_0 & & & \\ & & b_m & b_{m-1} & \cdots & b_0 & & \\ & & & \ddots & & & & \\ & & & & b_m & b_{m-1} & \cdots & b_0 \end{vmatrix}$$

is zero. Here $R(f,g)$, called the *resultant* of the two polynomials, is the determinant of an $(n+m) \times (n+m)$ matrix R with m rows involving the coefficients of $f(x)$ and n rows involving the coefficients of $g(x)$.

30. **(a)** With notations as in the previous problem, show that we have the matrix equation

$$R \begin{pmatrix} x^{n+m-1} \\ x^{n+m-2} \\ \vdots \\ x \\ 1 \end{pmatrix} = \begin{pmatrix} x^{m-1}f(x) \\ x^{m-2}f(x) \\ \vdots \\ f(x) \\ x^{n-1}g(x) \\ x^{n-2}g(x) \\ \vdots \\ g(x) \end{pmatrix}.$$

(b) Let R' denote the matrix of cofactors of R as in Theorem 30 of Section 11.4, so $R'R = R(f,g)I$, where I is the identity matrix. Multiply both sides of the matrix equation above by R' and equate the bottom entry of the resulting column matrices to prove that there are polynomials $r(x), s(x) \in F[x]$ such that $R(f,g)$ is equal to $r(x)f(x) + s(x)g(x)$, i.e., the resultant of two polynomials is a linear combination (in $F[x]$) of the polynomials.

31. Consider $f(x)$ and $g(x)$ as general polynomials and suppose the roots of $f(x)$ are $x_1, \ldots, x_n$ and the roots of $g(x)$ are $y_1, \ldots, y_m$. The coefficients of $f(x)$ are powers of a_n times the elementary symmetric functions in $x_1, x_2, \ldots, x_n$ and the coefficients of $g(x)$ are powers of b_m times the elementary symmetric functions in $y_1, y_2, \ldots, y_m$.

(a) By expanding the determinant show that $R(f,g)$ is homogeneous of degree m in the coefficients a_i and homogeneous of degree n in the coefficients b_j.

(b) Show that $R(f,g)$ is $a_n^m b_m^n$ times a symmetric function in $x_1, \ldots, x_n$ and $y_1, \ldots, y_m$.

(c) Since $R(f,g)$ is 0 if $f(x)$ and $g(x)$ have a common root, say $x_i = y_j$, show that $R(f,g)$ is divisible by $x_i - y_j$ for $i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, m$. Conclude by degree considerations that

$$R = a_n^m b_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} (x_i - y_j).$$

(d) Show that the product in (c) can be also be written

$$R(f, g) = a_n^m \prod_{i=1}^{n} g(x_i) = (-1)^{nm} b_m^n \prod_{j=1}^{m} f(y_j).$$

This gives an interesting *reciprocity* between the product of g evaluated at the roots of f and the product of f evaluated at the roots of g.

32. Consider now the special case where $g(x) = f'(x)$ is the derivative of the polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ and suppose the roots of $f(x)$ are $\alpha_1, \alpha_2, \ldots, \alpha_n$. Using the formula

$$R(f, f') = \prod_{i=1}^{n} f'(\alpha_i)$$

of the previous exercise, prove that

$$D = (-1)^{n(n-1)/2} R(f, f')$$

where D is the discriminant of $f(x)$.

33. **(a)** Prove that the discriminant of the cyclotomic polynomial $\Phi_p(x)$ of the p^{th} roots of unity for an odd prime p is $(-1)^{(p-1)/2} p^{p-2}$ [One approach: use Exercise 5 of the previous section together with the determinant form for the discriminant in terms of the power sums p_i.]

(b) Prove that $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2} p}) \subset \mathbb{Q}(\zeta_p)$ for p an odd prime. (Cf. also Exercise 11 of Section 7.)

34. Use the previous exercise to prove that every quadratic extension of $\mathbb{Q}$ is contained in a cyclotomic extension (a special case of the Kronecker–Weber Theorem).

35. Prove that the discriminant D of the polynomial $x^n + px + q$ is given by the formula $(-1)^{n(n-1)/2} n^n q^{n-1} + (-1)^{(n-1)(n-2)/2} (n-1)^{n-1} p^n$.

36. Prove that the discriminant of $x^n + nx^{n-1} + n(n-1)x^{n-2} + \cdots + n(n-1)\ldots(3)(2)x + n!$ is $(-1)^{n(n-1)/2} (n!)^n$.

The following exercises 37 to 43 outline two procedures for writing a symmetric function in terms of the elementary symmetric functions. Let $f(x_1, \ldots, x_n)$ be a polynomial which is symmetric in $x_1, \ldots, x_n$. Recall that the degree (sometimes called the *weight*) of the monomial $Ax_1^{a_1} x_2^{a_2} \ldots x_n^{a_n}$ ($a_i \geq 0$) is $a_1 + a_2 + \cdots + a_n$ and that a polynomial is *homogeneous (of degree m)* if every monomial has the same degree (m).

37. **(a)** Show that every polynomial $f(x_1, \ldots, x_n)$ can be written as a sum of homogeneous polynomials. Show that if $f(x_1, \ldots, x_n)$ is symmetric then each of these homogeneous polynomials is also symmetric.

(b) Show that the monomial $Bs_1^{a_1} s_2^{a_2} \ldots s_n^{a_n}$ in the elementary symmetric functions is a homogeneous polynomial in $x_1, x_2, \ldots, x_n$ of degree $a_1 + 2a_2 + \cdots + na_n$.

In writing $f(x_1, \ldots, x_n)$ as a polynomial in the symmetric functions it therefore suffices to assume that $f(x_1, \ldots, x_n)$ is homogeneous.