14 Symmetric polynomials

In this section, we consider a special type of polynomials in several variables, called *symmetric polynomials.* This is a very classic algebraic subject, which we will encounter later in great generality in Galois theory.

In 12.3, we saw that for an integral domain R, a non-zero polynomial $f \in R[X]$ has no more than $n = \deg(f)$ zeros in R. For $R = \mathbf{Z}$, the *fundamental theorem of algebra* 26.3 tells us that f has *exactly* $n = \deg(f)$ zeros, provided that we count them with multiplicity and are willing to consider zeros in a suitable ring larger than $\mathbf{Z}$ itself, for example $\mathbf{C}$. This is also true for an arbitrary integral domain, and in §21, we will construct the necessary "extension fields."

Even if the zeros of $f \in R[X]$ can only be found in a larger ring $R' \supset R$, it turns out that "symmetric expressions" in the zeros of f lie in R itself. We will see how to calculate them *without* ever venturing outside the ground ring R. The methods we give are used by all computer algebra packages.

▶ General polynomial of degree n

We define a "general" polynomial of degree n by working in the ring $R = \mathbf{Z}[T_1, T_2, \ldots, T_n]$ of polynomials in the n variables $T_1, T_2, \ldots, T_n$. We can also allow other rings than $\mathbf{Z}$ for the ring of coefficients, but for the sake of simplicity, we will not do so. The *(total) degree* of the monomial $T_1^{e_1} T_2^{e_2} \ldots T_n^{e_n}$ is equal to $e_1 + e_2 + e_3 + \ldots + e_n$, and we define the *degree* $\deg(f)$ of a non-zero polynomial $f \in R$ as the maximum of the degrees of the monomials in f. If all monomials in f are of the same degree d, then f is called *homogeneous* of degree d. An arbitrary polynomial $f \in R$ of degree d can be written as $f = f_0 + f_1 + f_2 + \ldots + f_d$ with f_k homogeneous of degree k by combining the monomials of equal degree.

The *general polynomial* F_n of degree n is the monic polynomial in $R[X]$ with zeros the variables $T_1, T_2, \ldots, T_n$:

$$F_n = (X - T_1)(X - T_2) \ldots (X - T_n) = X^n + \sum_{k=1}^{n} (-1)^k s_k X^{n-k} \in R[X].$$

The coefficients $s_k \in R$ are called the *elementary symmetric polynomials* in the zeros T_i of f, and the Frenchman François Viète (1540–1603) already knew that for $k = 1, 2, \ldots n$, the polynomial s_k is equal to

$$s_k = \sum_{1 \le i_1 < i_2 < \ldots i_k \le n} T_{i_1} T_{i_2} \ldots T_{i_k},$$

the sum of all products of exactly k different zeros of F. The polynomial $s_k \in R$ is homogeneous of degree k, and we have

$$s_1 = T_1 + T_2 + \ldots + T_n,$$
$$s_2 = T_1T_2 + T_1T_3 + \ldots + T_1T_n + T_2T_3 + T_2T_4 + \ldots + T_{n-1}T_n,$$

and

$$s_n = T_1 T_2 T_3 \dots T_n \qquad .$$

Note that, by definition, the general polynomial of degree n has coefficients in the integral domain $R_0 = \mathbf{Z}[s_1, s_2, \dots, s_n]$ and that its n zeros are the variables of the extension ring $R = \mathbf{Z}[T_1, T_2, \dots, T_n] \supset R_0$.

► Symmetric polynomials

A polynomial in $R = \mathbf{Z}[T_1, T_2, \dots, T_n]$ (or, more generally, in $A[T_1, T_2, \dots, T_n]$ for a commutative ring A) is called *symmetric* (in the variables T_i) if it is invariant under all permutation of the variables T_i. Somewhat more formally, we can consider the natural action of the symmetric group S_n on R given by

$$(\sigma f)(T_1, T_2, \dots, T_n) = f(T_{\sigma(1)}, T_{\sigma(2)}, \dots, T_{\sigma(n)}) \qquad \text{for } f \in R, \sigma \in S_n.$$

The symmetric polynomials in R are then the polynomials in R that are invariant under the action of S_n. For every $\sigma \in S_n$, the map $f \mapsto \sigma f$ is an *automorphism* of R, so that we have an inclusion $S_n \subset \mathrm{Aut}(R)$. It follows easily that the symmetric polynomials form a *subring* $R_0 \subset R$.

Exercise 1. Verify this.

Since the kth elementary symmetric polynomial $s_k \in R$ is symmetric, we have the inclusion $\mathbf{Z}[s_1, s_2, \dots, s_n] \subset R_0$. The fundamental theorem for symmetric polynomials says that this inclusion is an equality: *every* symmetric polynomial is a polynomial in the elementary symmetric polynomials. This theme is elaborated further in Galois theory: polynomials with “many” symmetries are contained in “small” subrings.

14.1. Fundamental theorem. *Let $P \in R = \mathbf{Z}[T_1, T_2, \dots, T_n]$ be a symmetric polynomial. Then there is a unique way to write P as a polynomial in the elementary symmetric polynomials s_k.*

We give a constructive proof, that is, a proof that gives an *algorithm* to write a P as an element of $\mathbf{Z}[s_1, s_2, \dots, s_n]$.

Proof. We order the monomials in P *lexicographically*, as in a dictionary. In other words, monomials $T_1^{e_1} T_2^{e_2} \dots T_n^{e_n}$ with the highest exponent e_1 are in front, if two monomials have the same e_1, their order is determined by e_2, and so on.

Now, let $c \cdot T_1^{e_1} T_2^{e_2} \dots T_n^{e_n}$ with $c \in \mathbf{Z} \setminus \{0\}$ be the first term in P, lexicographically, and let $d = e_1 + e_2 + e_3 + \dots + e_n$ be its degree. Then we have $e_1 \geq e_2 \geq e_3 \geq \dots \geq e_n$. After all, if this is not the case, then through a suitable permutation of the T_i, we can transform this term into one that comes earlier lexicographically and that must also be in P because of the symmetry of P; this gives a contradiction. Now, form the monomial

$$\Sigma = s_1^{e_1 - e_2} s_2^{e_2 - e_3} s_3^{e_3 - e_4} \dots s_{n-1}^{e_{n-1} - e_n} s_n^{e_n} \in R$$

of degree

$$\begin{aligned} &e_1 - e_2 + 2(e_2 - e_3) + 3(e_3 - e_4) + \ldots + (n-1)(e_{n-1} - e_n) + ne_n \\ &= e_1 + e_2 + e_3 + \ldots + e_n = d \leq \deg(P), \end{aligned}$$

with first term $T_1^{e_1} T_2^{e_2} \ldots T_n^{e_n}$ (lexicographically), and consider $P_1 = P - c\Sigma \in R$. Because $\deg(\Sigma) \leq \deg(P)$, we have $\deg(P_1) \leq \deg(P)$, and all monomials in P_1 come *later*, lexicographically, than $T_1^{e_1} T_2^{e_2} \ldots T_n^{e_n}$. Since only finitely many different monomials are possible when the degree is bounded, we see that by repeatedly subtracting an element of $\mathbf{Z}[s_1, s_2, \ldots, s_n]$, we can reduce the polynomial P to 0. In other words, P is itself contained in $\mathbf{Z}[s_1, s_2, \ldots, s_n]$.

To prove that there are not two ways to write a polynomial in $\mathbf{Z}[T_1, \ldots, T_n]$ as a polynomial in $\mathbf{Z}[s_1, s_2, \ldots, s_n]$, we must show that there is no non-zero polynomial $g \in \mathbf{Z}[X_1, X_2, \ldots, X_n]$ with $g(s_1, s_2, \ldots, s_n) = 0$. To do this, suppose that such a polynomial does exist. Write every monomial in g in the form

$$cX_1^{e_1-e_2} X_2^{e_2-e_3} X_3^{e_3-e_4} \ldots X_{n-1}^{e_{n-1}-e_n} X_n^{e_n},$$

and consider the monomial M in g for which the corresponding n-tuple $(e_1, e_2, \ldots, e_n)$ comes first lexicographically. When expanding $g(s_1, s_2, \ldots, s_n)$ as a polynomial in $\mathbf{Z}[T_1, T_2, \ldots, T_n]$, we see that M leads to a term $cT_1^{e_1} T_2^{e_2} \ldots T_n^{e_n}$ that does not disappear, so we have a contradiction. □

It follows from the uniqueness of representations in terms of the elementary symmetric polynomials s_k that $\mathbf{Z}[s_1, s_2, \ldots, s_n]$ can be viewed as a polynomial ring in the variables s_k: the elementary symmetric polynomials are *algebraically independent*.

We say that a monomial $s_1^{a_1} s_2^{a_2} \ldots s_n^{a_n}$ has *weight* $a_1 + 2a_2 + 3a_3 + \ldots + na_n$; more generally, the weight of $g \in \mathbf{Z}[s_1, s_2, \ldots, s_n]$ is the maximum of the weights of the monomials in g. If all monomials in g have the same weight d, then g is said to be *isobaric* of weight d. Note that the weight of $g \in \mathbf{Z}[s_1, s_2, \ldots, s_n]$ is nothing but the *degree* of g as an element of $R = \mathbf{Z}[T_1, T_2, \ldots, T_n]$. The proof of 14.1 shows the following.

14.2. Corollary. *A homogeneous symmetric polynomial in $\mathbf{Z}[T_1, T_2, \ldots, T_n]$ of degree d can be written in a unique way as an isobaric polynomial of weight d in $\mathbf{Z}[s_1, s_2, \ldots, s_n]$.* □

An arbitrary symmetric polynomial P can be written as a sum of homogeneous polynomials P_k of degree k; the polynomials P_k are symmetric because the action of S_n on $\mathbf{Z}[T_1, T_2, \ldots, T_n]$ leaves the degree invariant. By 14.2, the polynomial P_k can be written as an isobaric polynomial of weight k in the elementary symmetric polynomials s_k.

▶ Calculations with symmetric polynomials

There is a shortened notation for *symmetric polynomials* P, defined as follows: for every S_n-orbit in P, we write a single representative preceded by the symbol $\sum_n$ to indicate that we take the sum over the monomials in the S_n-orbit of the representative. In this notation, the kth elementary symmetric polynomial $s_k \in R$ is equal to

$$s_k = \sum_n T_1T_2T_3 \ldots T_k.$$

More generally, $\sum_n f$ with $f \in \mathbf{Z}[T_1, T_2, \ldots, T_n]$ is the notation for the sum of the polynomials in the S_n-orbit of f. Examples:

$$\sum_3 T_1^2T_2 = T_1^2T_2 + T_1^2T_3 + T_2^2T_3 + T_1T_2^2 + T_1T_3^2 + T_2T_3^2$$

$$\sum_4 T_1T_2T_3 = T_1T_2T_3 + T_1T_2T_4 + T_1T_3T_4 + T_2T_3T_4$$

$$\sum_4 T_1T_2 = T_1T_2 + T_1T_3 + T_1T_4 + T_2T_3 + T_2T_4 + T_3T_4$$

If we want to use the method from the proof of 14.1 to write a given symmetric polynomial as a polynomial in the s_k, then the short notation is often useful. After all, if a monomial $rT_1^{e_1}T_2^{e_2}\ldots T_n^{e_n}$ occurs in a symmetric polynomial $f \in \mathbf{Z}[T_1, T_2, \ldots, T_n]$, then $\sum_n rT_1^{e_1}T_2^{e_2}\ldots T_n^{e_n}$ also occurs in that polynomial.

14.3. Examples. 1. Take $n \geq 2$ and $P = T_1^2 + T_2^2 + \ldots + T_n^2 = \sum_n T_1^2$. Then T_1^2 is lexicographically the highest term in P, so we form

$$s_1^2 = (T_1 + T_2 + \ldots + T_n)^2 = \sum_n T_1^2 + 2\sum_n T_1T_2$$

and calculate $P_1 = P - s_1^2 = -2\sum_n T_1T_2 = -2s_2$. In this case, we are done after one step, and we find $P = s_1^2 - 2s_2$. Note that P is homogeneous of degree 2 and $s_1^2 - 2s_2$ is isobaric of weight 2.

2. Now, take $n \geq 3$ and $P = T_1^3 + T_2^3 + \ldots + T_n^3 = \sum_n T_1^3$. Then T_1^3 is lexicographically the highest term in P, so we form

$$s_1^3 = (T_1 + T_2 + \ldots + T_n)^3 = \sum_n T_1^3 + 3\sum_n T_1^2T_2 + 6\sum_n T_1T_2T_3.$$

The coefficients 3 and 6 indicate how often a term occurs when we expand s_1^3. We find $P_1 = P - s_1^3 = -3\sum_n T_1^2T_2 - 6\sum_n T_1T_2T_3$. The lexicographically highest term in P_1 is $-3T_1^2T_2$, so we subtract -3 times

$$s_1s_2 = \sum_n T_1 \cdot \sum_n T_1T_2 = \sum_n T_1^2T_2 + 3\sum_n T_1T_2T_3$$

and obtain

$$P_2 = P_1 + 3s_1s_2 = P - s_1^3 + 3s_1s_2 = 3\sum_n T_1T_2T_3 = 3s_3.$$

Conclusion: $P = T_1^3 + T_2^3 + \ldots + T_n^3 = s_1^3 - 3s_1s_2 + 3s_3$. Again, note that P is homogeneous of degree 3 and $s_1^3 - 3s_1s_2 + 3s_3$ is isobaric of weight 3.

Exercise 2. What happens in the cases $n < 2$ (in Example 1) and $n < 3$ (in Example 2)?

See Exercise 24 for the representation of the *sum of powers* $\sigma_k = T_1^k + T_2^k + \ldots + T_n^k$ in terms of the elementary symmetric polynomials using *Newton's identities*.

▶ Discriminant

A common symmetric polynomial in $\mathbf{Z}[T_1, T_2, \ldots, T_n]$ is the *discriminant*

$$\Delta_n = \prod_{1\le i<j\le n} (T_i - T_j)^2 \tag{14.4}$$

of the general polynomial F_n of degree n. The polynomial Δ_n is homogeneous of degree $n(n-1)$, so by 14.2, it is a universal isobaric expression of weight $n(n-1)$ in $\mathbf{Z}[s_1, s_2, \ldots, s_n]$. In other words, the discriminant of the general polynomial F_n of degree n is a polynomial in the coefficients $(-1)^{n-k}s_k$ of F_n.

After the uninteresting case $\Delta_1 = 1$, we have

$$\Delta_2 = (T_1 - T_2)^2 = (T_1 + T_2)^2 - 4T_1T_2 = s_1^2 - 4s_2,$$

a result that is also written as $\Delta(X^2 + AX + B) = A^2 - 4B$. Using the method of 14.1, we can express Δ_n in the elementary symmetric polynomials, and with some effort, we obtain

$$\Delta_3 = s_1^2s_2^2 - 4s_2^3 - 4s_1^3s_3 - 27s_3^2 + 18s_1s_2s_3$$
$$\Delta_4 = \frac{1}{27}\left(4(s_2^2 - 3s_1s_3 + 12s_4)^3 - (2s_2^3 - 72s_2s_4 + 27s_1^2s_4 - 9s_1s_2s_3 + 27s_3^2)^2\right),$$

formulas that are too unpleasant to remember. For large values of n, the formulas for the Δ_n are, moreover, too unpleasant to write down.

Exercise 3. Verify that Δ_4 is in $\mathbf{Z}[s_1, s_2, s_3, s_4]$.

Next, let A be an arbitrary integral domain and $f \in A[X]$ a monic polynomial of degree n. Then by 12.3, the polynomial f has at most n zeros in A; in 21.13, we will prove that the number of zeros of f in a sufficiently large integral domain $A' \supset A$ is *exactly* n is the sense that

$$f = \prod_{i=1}^{n}(X - \alpha_i)$$

holds with $\alpha_i \in A'$. If A is a subring of $\mathbf{C}$ such as $\mathbf{Z}$, $\mathbf{Q}$, or $\mathbf{R}$, then by the fundamental theorem of algebra 26.3, we can always take $A' = \mathbf{C}$. The discriminant of f is now defined as

$$\Delta(f) = \prod_{1\le i<j\le n} (\alpha_i - \alpha_j)^2. \tag{14.5}$$

Since A' is an integral domain, we have $\Delta(f) = 0$ if and only if f has a double zero in A'.

The homomorphism $\mathbf{Z}[T_1, T_2, \ldots, T_n] \to A'$ that sends T_i to α_i maps Δ_n onto $\Delta(f)$. Since the images of the elementary symmetric polynomials s_k, which are sent to (plus or minus) the coefficients of f, are contained in A, we see that $\Delta(f)$ is also an element of A. In other words, the discriminant of a polynomial $f \in A[X]$ is an element of A, and it is given by a universal polynomial in the coefficients of f.

14.6. Example. The general formula for the discriminant of a cubic polynomial is difficult to remember, but the well-known formula

$$\Delta(X^3 + pX + q) = -4p^3 - 27q^2 \tag{14.7}$$

that arises by substituting $(s_1, s_2, s_3) = (0, p, -q)$ in the general expression for Δ_3 is both easy to remember and easy to deduce. After all, by taking $A = \mathbf{Z}[p, q]$, we know that the discriminant is a universal polynomial in p and q. Since there are only two monomials in $\mathbf{Z}[s_2, s_3]$ of weight $3(3-1) = 6$, namely s_2^3 and s_3^2, there in fact exist constants $c_1, c_2 \in \mathbf{Z}$ such that we have $\Delta(X^3 + pX + q) = c_1p^3 + c_2q^2$. We can easily calculate c_1 and c_2 by choosing a few suitable values for p and q. Namely, we have $c_1 = -\Delta(X^3 - X) = -4$ and $c_2 = \Delta(X^3 - 1) = -27$.

Exercise 4. Verify this.

▶ Resultant

Usually, discriminants of polynomials of higher degree in $A[X]$ are not calculated using the general formula for Δ_n; instead, the *resultant* is used. To avoid restrictions on division, if necessary, we replace the integral domain A with its field of fractions; from now on, we assume that $A = K$ is a *field*. For polynomials

$$f = a\prod_{i=1}^{n}(X - \alpha_i) \qquad \text{and} \qquad g = b\prod_{j=1}^{m}(X - \beta_j)$$

in $K[X]$ of degree n and m, respectively, the resultant $R(f, g)$ is defined by

$$R(f, g) = a^m b^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j). \tag{14.8}$$

The following properties are immediate from this definition:

(R1) $R(f, g) = (-1)^{mn}R(g, f)$.
(R2) $R(f, g) = a^m \prod_{i=1}^{n} g(\alpha_i)$.
(R3) If $g_1 \in K[X]$ is of degree m_1 with $g \equiv g_1 \bmod (f)$, then we have $R(f, g) = a^{m-m_1}R(f, g_1)$.

Using these properties and division with rest in $K[X]$, we can calculate resultants *without* ever needing any explicit knowledge of the zeros α_i and β_j that occur in the definition. Using (R1), if necessary, we may assume that we have $\deg(g) \geq \deg(f)$. We then use (R3) to replace g with the remainder $g_1 \in A[X]$ of the division of g by f. We can lower the degree of the polynomials by repeating these steps, and as soon as f has degree 0 or 1 and we know the zeros $\alpha_i \in A$, property (R2) gives the value of the resultant.

For a monic polynomial $f = \prod_{i=1}^{n}(X - \alpha_i)$, the derivative in a zero α_i is equal to

$$f'(\alpha_i) = (\alpha_i - \alpha_1)(\alpha_i - \alpha_2)\ldots(\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1})\ldots(\alpha_i - \alpha_n).$$

If we take the product of these expressions for $i = 1, 2, \ldots, n$, then after counting the number of factors -1, we see that

$$\Delta(f) = (-1)^{n(n-1)/2} R(f, f'). \tag{14.9}$$

This is how we can use the resultant to calculate discriminants of polynomials in $K[X]$.

14.10. Example. **1**. Take $K = \mathbf{Q}(p, q)$ and $f = X^3 + pX + q$. Then we have

$$\Delta(X^3 + pX + q) = -R(X^3 + pX + q, 3X^2 + p).$$

If we apply (R1) and then (R3) for $f = 3X^2 + p$, $g = X^3 + pX + q$, and $g_1 = g - (X/3)f = (2p/3)X + q$, then this becomes $-3^2 \cdot R(3X^2 + p, (2p/3)X + q)$. If we apply (R1) once more and recall that g_1 has a single zero $\alpha = -3q/(2p)$, then property (R2) gives

$$\Delta(X^3 + pX + q) = -3^2 \cdot \left(\frac{2p}{3}\right)^2 \left[3\left(\frac{-3q}{2p}\right)^2 + p\right] = -4p^3 - 27q^2,$$

in accordance with (14.7).

2. Take $K = \mathbf{Q}$ and $f = X^5 + X + 1$. Then we have

$$\begin{aligned}
\Delta(X^5 + X + 1) &= R(X^5 + X + 1, 5X^4 + 1) = R(5X^4 + 1, X^5 + X + 1) \\
&= 5^4 \cdot R(5X^4 + 1, \frac{4}{5}X + 1) \\
&= 5^4 \cdot \left(\frac{4}{5}\right)^4 \cdot \left[5 \cdot \left(\frac{-5}{4}\right)^4 + 1\right] = 5^5 + 4^4 = 3381.
\end{aligned}$$

Since f is irreducible in $\mathbf{Z}[X]$, the complex zeros of f do not lie in $\mathbf{Z}$ or $\mathbf{Q}$, and it is therefore not easy to give them "explicitly." However, this is not at all necessary to calculate the discriminant.

EXERCISES.

5. Suppose that $f \in \mathbf{Z}[T_1, T_2, \ldots, T_n]$ is invariant under every exchange $T_i \leftrightarrow T_j$ of two variables. Is f necessarily symmetric?

6. Let α_1, α_2, and α_3 be the zeros of $X^3 - X - 1$ in $\mathbf{C}$, and set $p_k = \alpha_1^k + \alpha_2^k + \alpha_3^k$ for all $k \in \mathbf{Z}$. Prove: the sequence $\{p_k\}_{k \in \mathbf{Z}}$ consists of integers that satisfy $p_{-1} = -1$, $p_0 = 3$, $p_1 = 0$, and the recurrence relation $p_k = p_{k-2} + p_{k-3}$ for $k \in \mathbf{Z}$.

7. Show: for $f \in \mathbf{Z}[T_1, T_2, \ldots, T_n]$ homogeneous of degree d and $r \in \mathbf{Z}$, we have

$$f(rT_1, rT_2, \ldots, rT_n) = r^d f(T_1, T_2, \ldots, T_n).$$

Conversely, is f homogeneous of degree d if this identity holds for all $r \in \mathbf{Z}$?

8. Give an example of a ring A and a non-homogeneous polynomial $f \in A[T_1, T_2, \ldots, T_n]$ that satisfies $f(rT_1, rT_2, \ldots, rT_n) = r^d f(T_1, T_2, \ldots, T_n)$ for all $r \in A$ for some $d \geq 1$.

9. Show that there are exactly $\binom{n+d-1}{n-1}$ distinct monomials $T_1^{e_1} T_2^{e_2} \ldots T_n^{e_n}$ of degree d.

10. Express the symmetric polynomials $\sum_n T_1^2 T_2$ and $\sum_n T_1^3 T_2$ in the elementary symmetric polynomials.

11. Show that the orbit of the polynomial $B = T_1T_2 + T_3T_4 \in \mathbf{Z}[T_1, T_2, T_3, T_4]$ under the action of S_4 consists of three elements B, B', and B'', and determine the cubic polynomial in $\mathbf{Z}[s_1, s_2, s_3, s_4][X]$ with these three zeros.

12. Show that the discriminant of the cubic polynomial from the previous exercise is equal to the discriminant Δ_4 of the general polynomial of degree 4, and use this to determine $\Delta_4 \in \mathbf{Z}[s_1, s_2, s_3, s_4]$.

13. Show that the resultant of the polynomials $f = \sum_{i=0}^n a_i X^i$ and $g = \sum_{j=0}^m b_j X^j$ of degree n and m in $K[X]$ is equal to the $(m+n) \times (m+n)$ determinant

$$\begin{array}{c} m \left\{ \begin{array}{c} \\ \\ \\ \\ \end{array} \right. \\ n \left\{ \begin{array}{c} \\ \\ \\ \\ \end{array} \right. \end{array}
\underbrace{\begin{vmatrix}
a_n & a_{n-1} & \cdots & a_0 & & \\
 & a_n & a_{n-1} & \cdots & a_0 & \\
 & & & \ddots & & \\
 & & a_n & a_{n-1} & \cdots & a_0 \\
b_m & b_{m-1} & \cdots & b_0 & & \\
 & b_m & b_{m-1} & \cdots & b_0 & \\
 & & & \ddots & & \\
 & & b_m & b_{m-1} & \cdots & b_0
\end{vmatrix}}_{m+n}$$

in terms of the coefficients of f and g. (Take all coefficients left blank equal to 0.) [Hint: show that this determinant also has properties (R1) and (R3).]

14. Prove: for $n \in \mathbf{Z}_{>0}$, we have $\Delta(X^n + a) = (-1)^{\frac{1}{2}n(n-1)} n^n a^{n-1}$.

15. Calculate the discriminant of the polynomial $X^4 + pX + q \in \mathbf{Q}(p, q)[X]$.

16. For every $n > 1$, determine an expression for the discriminant of the polynomial $X^n + pX + q \in \mathbf{Q}(p, q)[X]$.

17. Let $f \in \mathbf{Z}[X]$ be a monic polynomial. Prove that the following are equivalent:
    a. $\Delta(f) \neq 0$.
    b. The polynomial f has no double zeros in $\mathbf{C}$.
    c. The decomposition of f in $\mathbf{Q}[X]$ has no multiple prime factors.
    d. The polynomial f and its derivative f' are relatively prime in $\mathbf{Q}[X]$.
    e. The polynomials $f \bmod p$ and $f' \bmod p$ are relatively prime in $\mathbf{F}_p[X]$ for almost all prime numbers p.

18. Determine the "exceptional primes" in part (e) of the previous exercise for $f = X^3 + X + 1$ and for the polynomial $X^7 + 7X + 1$ from Exercise 12.23.

19. Let $f \in \mathbf{Q}[X]$ be a monic polynomial with $n = \deg(f)$ distinct complex zeros. Prove: the *sign* of $\Delta(f)$ is equal to $(-1)^s$, where $2s$ is the number of non-real zeros of f.

20. Prove: $X^3 + pX + q \in \mathbf{R}[X]$ has three (counted with multiplicity) real zeros $\Longleftrightarrow$ $4p^3 + 27q^2 \leq 0$.

21. Express the sum of powers $\sum_n T_1^4$ in the elementary symmetric polynomials. Does the value of n matter?

22. A rational function $f \in \mathbf{Q}(T_1, T_2, \ldots, T_n)$ is called symmetric if it is invariant under all permutations of the variables T_i. Prove that every symmetric rational function is a rational function in the elementary symmetric functions.

23. Write $\sum_n T_1^{-1}$ and $\sum_n T_1^{-2}$ as rational functions in $\mathbf{Q}(s_1, s_2, \ldots, s_n)$.

24. *(Newton's identities)* Show that the sums of powers $\sigma_k = \sum_n T_1^k$ satisfy

$$\sigma_k - s_1\sigma_{k-1} + s_2\sigma_{k-2} - \ldots + (-1)^{k-1}s_{k-1}\sigma_1 + (-1)^k k s_k = 0 \quad \text{for } 1 \leq k \leq n$$

and that we can use this to, inductively, write the sums of powers σ_k for $1 \leq k \leq n$ as polynomials in $\mathbf{Z}[s_1, s_2, \ldots, s_n]$. Also show that for $k > n$, the sum of powers σ_k can be written as a polynomial in $\mathbf{Z}[s_1, s_2, \ldots, s_n]$ from the relation

$$\sigma_k - s_1\sigma_{k-1} + s_2\sigma_{k-2} - \ldots + (-1)^n s_n\sigma_{k-n} = 0.$$

[Hint: determine the logarithmic derivative $f'/f \in R[[X]]$ of $f = \prod_{i=1}^n (1 - T_i X) \in R[X]$.]

25. Can the method in the previous exercise also be used to write the sums of powers σ_k for $k < 0$ as elements of $\mathbf{Q}(s_1, s_2, \ldots, s_n)$?

26. Show that in terms of the sums of powers σ_k, the discriminant Δ_n can be written as

$$\Delta_n = \det\bigl(\sigma_{i+j-2}\bigr)_{i,j=1}^n.$$

Use this relation to calculate $\Delta_3 \in \mathbf{Z}[s_1, s_2, s_3]$.
[Hint: start with the Vandermonde-determinant $\det(T_i^{j-1})_{i,j=1}^n$.]

27. Show that the discriminant $\Delta_n \in \mathbf{Z}[s_1, s_2, \ldots, s_n]$ of the general polynomial of degree n is an irreducible polynomial in $\mathbf{Z}[s_1, s_2, \ldots, s_n]$. Is Δ_n also irreducible in the ring $\mathbf{C}[s_1, s_2, \ldots, s_n]$?