Hence, we proved the following connection between the resultant and the discriminant

$$a_0 \operatorname{Disc}(f) = (-1)^{n(n-1)/2} \operatorname{Res}(f, f'), \tag{11.7}$$

which can serve as the definition of the discriminant of a polynomial in an arbitrary commutative ring with unity. The elements different from zero in the first row of the matrix from the definition of $\operatorname{Res}(f, f')$ are a_0 and na_0. Therefore, $\operatorname{Res}(f, f')$ is a multiple of a_0 and $\operatorname{Disc}(f)$ is a polynomial with integer coefficients in variables $a_0, \dots, a_n$. From

$$\operatorname{Disc}(f) = (-1)^{n(n-1)/2} a_0^{n-2} \prod_{i=1}^{n} f'(\alpha_i)$$

and Corollary 11.11, it follows that for $f \in A[x]$, where A is an integral domain of characteristic 0, f has multiple roots (i.e. it is not square-free) if and only if $\operatorname{Disc}(f) = 0$.

11.3 Irreducibility of polynomials

Definition 11.4. *Let A be an integral domain. We say that a polynomial $f \in A[x]$ is* reducible *(in $A[x]$, or over A) if it can be written in the form $f = gh$, where $g, h \in A[x] \setminus A$. If a non-constant polynomial is not reducible, then we say that it is* irreducible *(over A).*

We are first interested in the irreducibility of polynomials over $\mathbb{Z}$. The following result is a direct consequence of Gauss' lemma for polynomials (Lemma 11.4).

Corollary 11.12. *A polynomial with integer coefficients is irreducible over $\mathbb{Z}$ if and only if it is irreducible over $\mathbb{Q}$.*

Proof: It is clear that the irreducibility over $\mathbb{Q}$ implies the irreducibility over $\mathbb{Z}$. We will prove the converse. Let $f \in \mathbb{Z}[x]$ and $f = gh$, where $g, h \in \mathbb{Q}[x]$. We can assume that $\operatorname{cont}(f) = 1$. Let us choose a positive integer m such that $mg \in \mathbb{Z}[x]$. Let $\operatorname{cont}(mg) = n$. Then for $r = m/n \in \mathbb{Q}$, we have $rg \in \mathbb{Z}[x]$ and $\operatorname{cont}(rg) = 1$. Analogously, we choose $s \in \mathbb{Q}$ such that $sh \in \mathbb{Z}[x]$ and $\operatorname{cont}(sh) = 1$. Now, by Gauss' lemma 11.4, $\operatorname{cont}(rg)\operatorname{cont}(sh) = \operatorname{cont}(rsgh)$. From $\operatorname{cont}(rsf) = 1$ and $\operatorname{cont}(f) = 1$, we conclude that $rs = 1$, so

$$f = (rg)(sh)$$

is a factorization of f over $\mathbb{Z}$. □

When examining the (ir)reducibility of a polynomial over $\mathbb{Q}$, it is useful to first examine whether the polynomial has rational roots, i.e. linear factors. In doing so, the following theorem may be useful.

Theorem 11.13. *Let* $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$*, and let* $\alpha = r/s \in \mathbb{Q}$*, where* $\gcd(r,s) = 1$*, be a rational root of* f*. Then* $r \mid a_0$ *and* $s \mid a_n$*.*

Proof: If $f(r/s) = 0$, then also $s^n f(r/s) = 0$, so we have

$$\begin{aligned} 0 &= a_n r^n + a_{n-1} r^{n-1} s + \cdots + a_1 r s^{n-1} + a_0 s^n \\ &= a_n r^n + s(a_{n-1} r^{n-1} + \cdots + a_1 r s^{n-2} + a_0 s^{n-1}) \qquad (11.8) \\ &= r(a_n r^{n-1} + a_{n-1} r^{n-2} s + \cdots + a_1 s^{n-1}) + a_0 s^n. \qquad (11.9) \end{aligned}$$

Now, from (11.8), it follows that $s \mid a_n r^n$, and since $\gcd(r,s) = 1$, we obtain $s \mid a_n$. Analogously, from (11.9), it follows that $r \mid a_0 s^n$ and $r \mid a_0$. $\square$

The statement of Theorem 11.13 holds (with an analogous proof) for polynomials $f \in A[x]$, where A is a unique factorization domain, and roots $\alpha = r/s \in \mathbb{Q}(A)$, where $\mathbb{Q}(A)$ is the *fraction field* of A, i.e. the smallest field which contains A. For example, the fraction field of $\mathbb{Z}$ is $\mathbb{Q}$, whilst the fraction field of $K[x]$ is the field of rational functions $K(x)$ on K.

If the polynomial $f \in \mathbb{Z}[x]$ is reducible, then we may ask how to factorize it into the product of irreducible factors. Here, we will present *Kronecker's algorithm* for factorization. If $f(x)$ is reducible and $\deg f = n$, then it has a factor $g(x)$ of degree $\le r = \lfloor n/2 \rfloor$. In order to find $g(x)$, let us consider numbers $c_j = f(j)$ for $j = 0, 1, \ldots, r$. If $c_j = 0$, then $x - j$ divides $f(x)$. And if $c_j \ne 0$, then $g(j)$ divides c_j. For any choice of divisors $d_i \mid c_i$, $i = 0, 1, \ldots, r$, there is precisely one polynomial $g(x)$ such that $\deg g \le r$ and $g(j) = d_j$ for $j = 0, 1, \ldots, r$. This is the polynomial

$$g(x) = \sum_{j=0}^{r} d_j g_j(x), \quad \text{where} \quad g_j(x) = \prod_{\substack{0 \le k \le r \\ k \ne j}} \left(\frac{x-k}{j-k} \right)$$

(Lagrange's interpolation polynomial). Now, for each polynomial obtained in this manner, we need to check whether the coefficients of the polynomial g are integers and whether $g(x)$ divides the polynomial $f(x)$.

Let us mention that there are more efficient algorithms for factorization of integer polynomials which use a version of Hensel's lemma for polynomials (Berlekamp's algorithm) and LLL reduction (see [302, Chapters 4.2 and 4.3], [342, Chapter 8] and [345, Chapters 2.5 and 8.1]).

Let p be a prime number and $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ the field of residues modulo p with the operations of addition and multiplication modulo p. For $a \in \mathbb{Z}$, we denote by $\bar{a}$ the element of $\mathbb{F}_p$ such that $a \equiv \bar{a} \pmod{p}$. Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$. Then we denote by $\bar{f}$ the reduction of f modulo p, i.e. the polynomial

$$\bar{f}(x) = \bar{a}_0 + \bar{a}_1x + \cdots + \bar{a}_nx^n \in \mathbb{F}_p[x].$$

Theorem 11.14 (Schönemann, 1846). *Let $f = g^n + ph \in \mathbb{Z}[x]$ be a monic polynomial, where n is a positive integer, p is a prime number and $g, h \in \mathbb{Z}[x]$. Assume that $\bar{g}$ is irreducible in $\mathbb{F}_p[x]$ and that $\bar{g}$ does not divide $\bar{h}$ in $\mathbb{F}_p[x]$. Then the polynomial f is irreducible in $\mathbb{Z}[x]$.*

Proof: Assume that $f = f_1f_2$ is a non-trivial factorization of f in $\mathbb{Z}[x]$. We can assume that the polynomials f_1, f_2 are monic. Then $\bar{f} = \bar{f}_1 \cdot \bar{f}_2$ in $\mathbb{F}_p[x]$. Since $\bar{f} = \bar{g}^n$ and $\bar{g}$ is irreducible in $\mathbb{F}_p[x]$, it follows that there exist positive integers u and v such that $u + v = n$ and polynomials $h_1, h_2 \in \mathbb{Z}[x]$, such that

$$f_1 = g^u + ph_1, \quad f_2 = g^v + ph_2.$$

From $f = g^n + ph = (g^u + ph_1)(g^v + ph_2)$, it follows that

$$h = g^uh_2 + g^vh_1 + ph_1h_2. \tag{11.10}$$

We can assume that $u \le v$. Then (11.10) becomes

$$h = g^uh_3 + ph_1h_2, \tag{11.11}$$

where $h_3 = h_2 + g^{v-u}h_1 \in \mathbb{Z}[x]$. Consider the reduction of (11.11) modulo p. We have

$$\bar{h} = \bar{g}^u \cdot \bar{h}_3 \tag{11.12}$$

and we conclude that $\bar{g}$ divides $\bar{h}$ in $\mathbb{F}_p[x]$, which is a contradiction with the assumption of the theorem. □

Theorem 11.15 (Eisenstein, 1850). *Let*

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

be a monic polynomial with integer coefficients and let p be a prime number such that p divides $a_0, a_1, \ldots, a_{n-1}$, but p^2 does not divide a_0. Then f is irreducible in $\mathbb{Z}[x]$.

Proof: Let us write f in the form $f = g^n + ph$, where $g(x) = x$, $h(x) = (a_{n-1}x^{n-1} + \cdots + a_1 x + a_0)/p$. Then all assumptions of Theorem 11.14 are satisfied ($a_0/p \not\equiv 0 \pmod p$ and $\bar{g}(x) = x$ does not divide $\bar{h}(x)$), so f is irreducible in $\mathbb{Z}[x]$. □

Example 11.1. *Let p be a prime number. Then the polynomial*

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

is irreducible in $\mathbb{Z}[x]$.

Solution: We will apply Eisenstein's criterion to the polynomial

$$f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = x^{p-1} + \binom{p}{1} x^{p-2} + \cdots + \binom{p}{p-1}.$$

Each of the binomial coefficients $\binom{p}{i} = \frac{p(p-1)\cdot\ldots\cdot(p-i+1)}{1\cdot 2\cdot\ldots\cdot i}$, for $i = 1, \ldots, p-1$, is divisible by p, while $\binom{p}{p-1} = p$ is not divisible by p^2, so the statement follows from Theorem 11.15. ♢

Example 11.2. *Let $a_1, \ldots, a_n$, $n \geq 2$, be distinct integers. Prove that the polynomial*

$$f(x) = (x - a_1) \cdot \ldots \cdot (x - a_n) - 1$$

is irreducible in $\mathbb{Z}[x]$.

Solution: Assume that $f(x) = f_1(x) f_2(x)$ is a non-trivial factorization of f in $\mathbb{Z}[x]$. From $f(a_i) = -1 = f_1(a_i) f_2(a_i)$, it follows that

$$f_1(a_i) + f_2(a_i) = 0, \text{ for } i = 1, \ldots, n.$$

Since the polynomial $f_1 + f_2$ has at least n roots and degree $\leq n-1$, we conclude that $f_1 + f_2 = 0$. Now, from $f(x) = f_1(x) f_2(x)$, we obtain

$$(x - a_1) \cdot \ldots \cdot (x - a_n) - 1 = -(f_1(x))^2. \tag{11.13}$$

The leading coefficient on the left-hand side of (11.13) is equal to 1, while the one on the right-hand side is equal to -1, which is a contradiction. ♢

11.4 Polynomial decomposition

When we ask whether a polynomial can be factorized, we usually mean whether it can be written as a *product* of two (or more) non-trivial factors