Proof: Let us write f in the form $f = g^n + ph$, where $g(x) = x$, $h(x) = (a_{n-1}x^{n-1} + \cdots + a_1x + a_0)/p$. 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

$f = g \cdot h$, so we speak about factorization of polynomials (or about irreducibility if such factorization does not exist). However, on the set of polynomials, we have another interesting operation which leads to analogous notions and problems, and that is the *composition*. Thus, in this section, we will be interested in "factorizations" (i.e. decompositions) of the form $f = g \circ h$.

Definition 11.5. *We say that a polynomial $f \in \mathbb{C}[x]$ of degree greater than 1 is* indecomposable *(over $\mathbb{C}$) if $f = g \circ h$, $g, h \in \mathbb{C}[x]$, implies that $\deg g = 1$ or $\deg h = 1$.*

Definition 11.6. *We say that two decompositions of f, $f = g_1 \circ g_2$ and $f = h_1 \circ h_2$, are* equivalent *if there is a linear function L such that $h_1 = g_1 \circ L$, $h_2 = L^{-1} \circ g_2$. More generally, for two decompositions $f = g_1 \circ g_2 \circ \cdots \circ g_r$ and $f = h_1 \circ h_2 \circ \cdots \circ h_r$ we say that they are* equivalent *if $r = 1$ or $r \geq 2$ and there are linear functions $L_1, \ldots, L_{r-1}$ such that*

$$h_1 = g_1 \circ L_1, \quad h_j = L_{j-1}^{-1} \circ g_j \circ L_j,\ (1 < j < r), \quad h_r = L_{r-1}^{-1} \circ g_r.$$

We write $(g_1, \ldots, g_r) \sim (h_1, \ldots, h_r)$.

Any polynomial $f(x)$ with $\deg f > 1$ can be expressed as a composition of indecomposable polynomials. This can be easily proved by induction over the degree of f. Such expression is called *a complete decomposition* of $f(x)$. Ritt's theorems talk about properties of decompositions of polynomials with complex coefficients. The first Ritt's theorem describes the connections between two complete decompositions of a polynomial $f(x)$. In particular, they have equal lengths (the number of "factors" in decomposition), while the degrees of the indecomposable polynomials which occur in one decomposition represent a permutation of the degrees which occur in the other decomposition. (This statement generally holds for polynomials over fields of characteristic 0, and even more generally for polynomials over arbitrary fields under the assumption that the characteristic of the field does not divide the degree of the polynomial.)

The second Ritt's theorem characterizes the solutions of the equation $a \circ b = c \circ d$ in indecomposable polynomials $a, b, c, d \in \mathbb{C}[x]$. Up to equivalence, all solutions come from these two identities:

$$x^n \circ x^m p(x^n) = x^m p(x)^n \circ x^n,$$

$$D_n(x, a^m) \circ D_m(x, a) = D_{mn}(x, a) = D_m(x, a^n) \circ D_n(x, a),$$

where $p(x) \in \mathbb{C}[x]$ is an arbitrary polynomial, while $D_m(x,a)$ is the m-th *Dickson polynomial* with parameter a, defined by

$$D_m\Big(z + \frac{a}{z}, a\Big) = z^m + \Big(\frac{a}{z}\Big)^m, \tag{11.14}$$

or by the explicit formula

$$D_m(x,a) = \sum_{i=0}^{\lfloor m/2 \rfloor} \frac{m}{m-i}\binom{m-i}{i}(-a)^i x^{m-2i}. \tag{11.15}$$

The first identity is the generalization of the well-known property of the exponentiation $(x^m)^n = (x^n)^m = x^{mn}$, while the second generalizes the property of the *Chebyshev polynomials of the first kind* T_n, which can be defined by $T_n(\cos(\alpha)) = \cos(n\alpha)$, from where it is easily seen that $T_n \circ T_m = T_m \circ T_n = T_{mn}$. Let us list some other properties of the Dickson polynomials which are easily obtained from definition (11.14) and explicit formula (11.15):

$$D_1(x,a) = x, \quad D_2(x,a) = x^2 - 2a, \tag{11.16}$$

$$D_{mn}(x,a) = D_m(D_n(x,a), a^n), \tag{11.17}$$

$$b^m D_m(x,a) = D_m(bx, b^2 a), \tag{11.18}$$

$$D_{2m}(x,a) - 2a^m = (x^2 - 4a)E_m(x,a)^2, \tag{11.19}$$

where polynomials E_m are defined by

$$\Big(z - \frac{a}{z}\Big)E_m\Big(z + \frac{a}{z}, a\Big) = z^{m+1} - \Big(\frac{a}{z}\Big)^{m+1}. \tag{11.20}$$

The proofs of Ritt's theorems and other interesting properties of decompositions of polynomials can be found in the book [358]. The book [275] focuses on the Dickson polynomials.

Ritt's results on decompositions have significant applications in various mathematical problems. One such problem is the classification of the polynomials $f, g \in \mathbb{Q}[x]$ for which the Diophantine equation $f(x) = g(y)$ has infinitely many integer solutions. Bilu and Tichy in 2000 provided a complete answer to this question. Namely, they proved that the equation $f(x) = g(y)$ has infinitely many rational solutions with bounded denominators (i.e. there exists a positive integer Δ such that the equation has infinitely many rational solutions (x,y) for which Δx and Δy are integers) if and only if $f(x) = \varphi(f_1(\lambda(x)))$, $g(x) = \varphi(g_1(\mu(x)))$, where $\varphi(x) \in \mathbb{Q}[x]$, polynomials $\lambda(x), \mu(x) \in \mathbb{Q}[x]$ are linear, and $(f_1(x), g_1(x))$ is a standard pair over $\mathbb{Q}$

such that the equation $f_1(x) = g_1(x)$ has infinitely many rational solutions with bounded denominators.

There are five types of standard pairs and in their definitions we encounter powers, the Dickson polynomials and some concrete polynomials of small degree. Let us now list five types of standard pairs:

(i) A standard pair of the first kind is a pair of the form $(x^m, ax^r p(x)^m)$, or switched $(ax^r p(x)^m, x^m)$, where $0 \le r < m$, $\gcd(r, m) = 1$ and $r + \deg p(x) > 0$.

(ii) A standard pair of the second kind is $(x^2, (ax^2+b)p(x)^2)$ (or switched).

(iii) A standard pair of the third kind is $(D_m(x, a^n), D_n(x, a^m))$, where $\gcd(m, n) = 1$.

(iv) A standard pair of the fourth kind is $\left(a^{-\frac{m}{2}} D_m(x, a), -b^{-\frac{n}{2}} D_n(x, b)\right)$, where $\gcd(m, n) = 2$.

(v) A standard pair of the fifth kind is $((ax^2-1)^3, 3x^4-4x^3)$ (or switched).

We will not prove this result (an interested reader can find the proof in the paper [45]), but we will demonstrate that for each of the mentioned five pairs, it is indeed possible that the equation

$$f(x) = g(y) \tag{11.21}$$

has infinitely many integer solutions. We will assume that the polynomial p from the definition of the standard pair of the first kind has integer coefficients.

(i) Since $\gcd(r, m) = 1$, there exist integers q, s such that $qm - sr = 1$. Now, $x = a^q t^r p(a^s t^m)$, $y = a^s t^m$, for $t \in \mathbb{Z}$, is an infinite family of solutions of equation (11.21).

(ii) Let a, b be integers for which the Pellian equation $u^2 - av^2 = b$ has infinitely many solutions. Then for $x = up(v)$, $y = v$, we obtain infinitely many solutions of (11.21).

(iii) Here, we obtain an infinite family of solutions of equation (11.21) for $x = D_n(t, a)$, $y = D_m(t, a)$, $t \in \mathbb{Z}$.

(iv) This case is the most involved. In order to simplify it, let us take that $a = 1$. According to the assumption $\gcd(m, n) = 2$, the numbers

$m/2$ and $n/2$ are not both even, so let $n/2$ be odd. Let b be a negative integer such that $|b|$ is not a square and let (u, v) be a solution of Pell's equation $v^2 + bu^2 = 4$. We claim that for $x = D_{n/2}(v, 1)$, equation (11.21) has a solution, i.e. that there exists $y \in \mathbb{Z}$ such that $-b^{-n/2} D_n(y, b) = D_{mn/2}(v, 1)$. By using properties (11.16) – (11.20), we have

$$\begin{aligned} -b^{-n/2} D_n(y, b) &= -D_n\Big(\frac{y}{\sqrt{-b}}, -1\Big) = D_{n/2}\Big(- D_2\Big(\frac{y}{\sqrt{-b}}, -1\Big), 1\Big) \\ &= D_{n/2}\Big(- \frac{1}{b} y^2 + 2, 1\Big). \end{aligned}$$

If we compare this with $D_{mn/2}(v, 1) = D_m(D_{n/2}(v, 1), 1)$, we obtain $y^2 = -b(D_m(v, 1) - 2)$. If we also use (11.19), we get

$$y^2 = -b(v^2 - 4) E_{m/2}(v, 1)^2 = b^2 u^2 E_{m/2}(v, 1)^2$$

and we see that we can take $y = buE_{m/2}(v, 1)$.

(v) Let us take a positive integer a such that the Pellian equation $v^2 - 3au^2 = -2$ has a solution. Let us choose the sign of v such that $v \equiv 1 \pmod 3$. Then for $x = u(v + 2)$, $y = ((v + 1)^3 + 4)/3$, we obtain infinitely many solutions of (11.21).

Theorem 11.16. *If a polynomial $f \in \mathbb{Q}[x]$ is indecomposable over $\mathbb{Q}$, then f is indecomposable over $\mathbb{C}$.*

Proof: Assume the contrary, and let $f = g \circ h$ be a decomposition of f, where $g, h \in \mathbb{C}[x]$, $\deg g = r$, $\deg h = n$. If $h(x) = a_n x^n + \cdots + a_0$, then we can write $f = g_1 \circ h_1$, where

$$g_1(x) = g(a_n x + h(0)), \quad h_1(x) = \frac{1}{a_n}(h(x) - h(0)),$$

so that the polynomial h_1 is monic and $h_1(0) = 0$. Let $g_1(x) = b_r x^r + \cdots + b_0$, $h_1(x) = x^n + c_{n-1} x^{n-1} + \cdots + c_1 x$, $f(x) = d_k x^k + d_{k-1} x^{k-1} + \cdots + d_0$. Then

$$f(x) = b_r (h_1(x))^r + b_{r-1} (h_1(x))^{r-1} + \cdots + b_0. \qquad (11.22)$$

Notice that $\deg b_{r-1}(h_1(x))^{r-1} = k - n$. Therefore, from (11.22), by comparing the coefficients with $x^k, x^{k-1}, \ldots, x^{k-n+1}$ of $f(x)$ and $b_r(h(x))^r$, we obtain: $d_k = b_r$, $d_{k-1} = rb_r c_{n-1}$, $d_{k-2} = rb_r c_{n-2} + b_r \binom{r}{2} c_{n-1}^2, \ldots$, $d_{k-n+1} = rb_r c_1 +$members which contain powers of $c_2, \ldots, c_{n-1}$. From this, we obtain $c_{n-1}, c_{n-2}, \ldots, c_2, c_1 \in \mathbb{Q}$. Since $c_0 = 0 \in \mathbb{Q}$, we see that $h_1(x) \in \mathbb{Q}[x]$. Now, from (11.22), it follows that $g_1(x) \in \mathbb{Q}[x]$, so we obtained a contradiction with the assumption that f is indecomposable over $\mathbb{Q}$. □

The proof of Theorem 11.16 that is presented here follows those proofs given in the paper [259] and a manuscript by I. Gusić. An alternative proof can be found in [358, Chapter 1.3]. That proof uses the following result ("lemma on taking roots with a remainder") which is also an independent interest (we will use it in Chapter 15.5 for the construction of elliptic curves with large rank).

Lemma 11.17. *Let K be a field of characteristic 0. If $A \in K[x]$ is a monic polynomial and $\deg A = rn$, where $r, n \geq 1$, then there exists a monic polynomial $B \in K[x]$ such that $\deg B = n$ and $\deg(A - B^r) < n(r-1)$.*

Proof: We will prove by induction over i that for each $i \leq n$ there exists $B_i \in K[x]$ such that $\deg B_i = n$ and $\deg(A - B_i^r) < nr - i$. For $i = 0$, we can take $B_0 = x^n$. Let us assume that the statement is true for $i - 1$, where $0 < i \leq n$. Hence, there is a polynomial B_{i-1} of degree n such that $\deg(A - B_{i-1}^r) < nr - i + 1$. We search for the polynomial B_i in the form $B_i = B_{i-1} + cx^{n-i}$. We have

$$B_i^r = B_{i-1}^r + rcB_{i-1}^{r-1}x^{n-i} + \binom{r}{2}c^2B_{i-1}^{r-2}x^{2(n-i)} + \cdots ,$$

where the degrees of all summands, starting from the second onwards are $\leq n(r-2) + 2(n-i) = nr - 2i < nr - i$. The degree of $B_{i-1}^{r-1}x^{n-i}$ is $nr - i$, so we can choose c such that terms with x^{nr-i} are cancelled, and we obtain $\deg(A - B_i^r) = \deg(A - B_{i-1}^r - rcB_{i-1}^{r-1}x^{n-i}) < nr - i$. Since the polynomial B_0 is monic, from the construction it follows that all polynomials B_i are monic. □

By using basic properties of algebraic numbers, in Chapter 12.3, we will show that in the case of polynomials in $\mathbb{Z}[x]$, already the indecomposability over $\mathbb{Z}$ implies the indecomposability over $\mathbb{C}$. We will present here the result from [165], where all possible decompositions of Fibonacci and related polynomials are described by analytic methods.

For $f \in \mathbb{C}[x]$ and $\gamma \in \mathbb{C}$, we define

$$\delta(f, \gamma) = \deg\gcd(f - \gamma, f').$$

Lemma 11.18. *Let $f \in \mathbb{C}[x]$ and $f = g \circ h$ be a decomposition of f over $\mathbb{C}$, where $\deg g \geq 2$. Then there exists $\gamma \in \mathbb{C}$ such that $\delta(f, \gamma) \geq \deg h$.*

Proof: Let α be a root of $g'(x)$ (which exists due to $\deg g \geq 2$). Let us take $\gamma = g(\alpha)$. Then the polynomials $f(x) - \gamma = g(h(x)) - g(\alpha)$ and $f'(x) = g'(h(x))h'(x) - g'(\alpha)h'(x)$ are both divisible by $h(x) - \alpha$, so $\deg \gcd(f - \gamma, f') \geq \deg(h - \alpha) = \deg h$. □

Let U_n be the n-th *Chebyshev polynomial of the second kind,* defined as

$$U_{n-1}(\cos x) = \frac{\sin nx}{\sin x}. \tag{11.23}$$

From the addition formulas for the sine function, it follows that these polynomials satisfy the following recurrence

$$U_0(x) = 1,\ U_1(x) = 2x,\ U_{n+1}(x) = 2xU_n(x) - U_{n-1}(x).$$

In this book, there was already a lot of discussions of Fibonacci numbers F_n. Let us now define the *Fibonacci polynomials* by the following recurrence

$$F_0(x) = 0,\ F_1(x) = 1,\ F_{n+1}(x) = xF_n(x) + F_{n-1}(x).$$

Notice that we have $F_n(1) = F_n$, for any $n \geq 0$. For n even, the polynomial $F_n(x)$ is odd, i.e. $F_n(-x) = -F_n(x)$, while for n odd, the polynomial $F_n(x)$ is even, i.e. $F_n(-x) = F_n(x)$. We consider the question of what can be said concerning the decomposability of these two families of polynomials. Since they are connected by the formula $F_n(x) = U_{n-1}(\frac{ix}{2})(-i)^{n-1}$, it is sufficient to give an answer (over $\mathbb{C}$) for one of them.

Theorem 11.19. *The polynomial U_n is indecomposable for n odd, while for n even, all its decompositions are equivalent to the decomposition of the form $U_n(x) = V_{n/2}(x^2)$, where $V_{n/2}$ is a polynomial of degree $n/2$.*

The polynomial F_n is indecomposable for n even, while for n odd, all its decompositions are equivalent to the decomposition of the form $F_n(x) = H_{(n-1)/2}(x^2)$, where $H_{(n-1)/2}$ is a polynomial of degree $(n-1)/2$.

Proof: According to the above-mentioned arguments, it is sufficient to prove the statement of the theorem for polynomials U_n. We want to apply Lemma 11.18. From (11.23), we conclude that U_n has n real roots $\alpha_k = \cos(\frac{\pi k}{n+1})$, $k = 1, \dots, n$. According to Rolle's theorem (see [262, Chapter 3.1], [426, Chapter 5.3.1]), the derivative U_n' has $n-1$ real roots $\beta_1, \dots, \beta_{n-1}$, which satisfy $\alpha_k > \beta_k > \alpha_{k+1}$.

Let us take $\gamma_k = U_n(\beta_k)$. We claim that for n odd, the numbers γ_k are all distinct, and if n is even, then $\gamma_k = \gamma_l$ if and only if $k = l$ or $k + l = n$.

The polynomial U_n' is odd if n is even, and even if n is odd. Therefore, its roots are symmetric with respect to the origin

$$\beta_k = -\beta_{n-k}, \quad (k = 1, \dots, n-1). \tag{11.24}$$

Furthermore, from (11.23), we conclude that $|\gamma_k|$ is the maximum of the function $|\frac{\sin(n+1)x}{\sin x}|$ on the interval $[k\pi/(n+1), (k+1)\pi/(n+1)]$. Therefore, for $1 \le k \le (n-1)/2$, we have

$$\frac{1}{\sin\left(\frac{(k+1)\pi}{n+1}\right)} < |\gamma_k| < \frac{1}{\sin\left(\frac{k\pi}{n+1}\right)},$$

which implies that

$$|\gamma_k| > |\gamma_{k+1}| > 1, \quad (1 \le k \le (n-3)/2). \tag{11.25}$$

Let us now assume that n is odd. Then

$$|\gamma_1| > |\gamma_2| > \cdots > |\gamma_{(n-1)/2}|\,. \tag{11.26}$$

Since the polynomial U_n is odd, we have

$$\gamma_k = -\gamma_{n-k}, \quad (1 \le k \le n-1). \tag{11.27}$$

From (11.26) and (11.27), it now follows that the numbers γ_k are indeed all distinct. If $\delta(U_n, \gamma) > 0$, then γ is equal to one of the numbers γ_k. Since those numbers are all distinct, we conclude that $\delta(U_n, \gamma) \le 1$, for any $\gamma \in \mathbb{C}$. From Lemma 11.18, it now follows that the polynomial U_n is indecomposable.

In the case when n is even, we have

$$|\gamma_1| > |\gamma_2| > \cdots > |\gamma_{(n-2)/2}| > 1 = |\gamma_{n/2}|,$$

$$\gamma_k = \gamma_{n-k}, \quad (1 \le k \le n-1),$$

which shows that $\gamma_k = \gamma_l$ if and only if $k = l$ or $k + l = n$. Hence, in this case, we have $\delta(U_n, \gamma) \le 2$, for any $\gamma \in \mathbb{C}$.

From Lemma 11.18, it now follows that in any decomposition $U_n = g \circ h$ we have $\deg h = 2$, i.e. $h(x) = ax^2 + bx + c$ for $a, b, c \in \mathbb{C}$. Furthermore, $g(h(-x)) = U_n(-x) = U_n(x) = g(h(x))$, so from $g(ax^2 + bx + c) = g(ax^2 - bx + c)$ we conclude that $b = 0$, i.e. $h(x) = ax^2 + c$, so indeed the decomposition $U_n = g \circ h$ is equivalent to the decomposition $U_n(x) = V_{n/2}(x^2)$. □

Let us mention that, using Theorem 11.19 and Bilu-Tichy criterion, it was proved in [165] that for $m, n \ge 3$, $m \ne n$, the Diophantine equation $F_m(x) = F_n(y)$ has only finitely many integer solutions. Similar results on decomposability of families of polynomials and applications to solvability of Diophantine equations can be found in [42, 132, 133, 258, 391].