Appendix B
Chebyshev Polynomials and Their Inverses

The Chebyshev polynomial of degree n is defined by the formula

$$T_n(x) = \cos n \arccos x.$$

These polynomials were discovered by Pafnuty Chebyshev (1821–1894) when he was considering the problem of the best approximation of a given function by polynomials of degree $\leq n$. They play an important role in approximation theory. Rather surprising is the fact that these polynomials became useful in algebra: the problem from which they originally appeared is far from algebra, and even their definition uses transcendental functions.

Nevertheless, in some algebraic problems, the series T_n of Chebyshev polynomials appears along with the polynomials $P(x) = x^n$. From a "philosophical" point of view, these two classes result from the existence of two families of finite groups of projective transformations of the space $\mathbb{C}P^1$: cyclic groups C_n and dihedral groups D_n.

In complex analysis, the class of polynomials x^n extends to the family of multivalued analytic functions x^α, $\alpha \in \mathbb{R}$, which contains, along with the polynomials x^n, their inverses $x^{1/n}$ and satisfies the composition relation $(x^\alpha)^\beta = x^{\alpha\beta}$.

In a similar manner, we extend the class of Chebyshev polynomials T_n to the family of multivalued analytic functions T_α, $\alpha \in \mathbb{R}$, which contains, along with the polynomials T_n, their inverses $T_{1/n}$ and satisfies the composition relation $T_\beta \circ T_\alpha = T_{\alpha\beta}$.

A multivalued function can be defined without the notion of analytic continuation, just by giving its set of values at each point. This sometimes helps us in carrying over the definition of the multivalued function to an arbitrary field (where the operation of analytic continuation is not defined). For example, for positive

This appendix was published originally as A. Khovanskii [58].

A. Khovanskii, *Topological Galois Theory*, Springer Monographs in Mathematics,
DOI 10.1007/978-3-642-38871-2

integers n, the function $x^{1/n}$ is defined over every field $\mathbf{k}$: it is a multivalued function that assigns to every $x \in \mathbf{k}$, the set of elements z from the algebraic closure of $\mathbf{k}$ such that $z^n = x$.

It is easier to work with a germ of a single-valued function than with a multivalued function. This can be done when all values of a multivalued function come from the analytic continuation of a single-valued germ.

In Sect. B.1.1, the multivalued Chebyshev function T_α, $\alpha \in \mathbb{R}$, is defined as a function of a complex variable x by means of its set of values. In Sect. B.1.2, we define a series at the point $x = 1$ whose analytic continuation is T_α (see Sect. B.1.3).

In Sect. B.2.1, we give an algebraic definition of Chebyshev polynomials and their inverses over an arbitrary field of characteristic not equal to 2. In addition, if the characteristic of the field is not equal to 3, then these functions are used to construct solutions in radicals of equations of degree 3 and 4 over this field (see Sects. B.2.2 and B.2.3).

In Sects. B.3.1–B.3.3, we discuss three classical problems whose solution involves the families of polynomials x^n and T_n. In Sect. B.3.1, we discuss the problem of describing all complex polynomials that can be inverted in radicals. This problem was solved by Joseph Ritt. In Sect. B.3.2, we discuss Schur's problem, which was solved by Michael Fried, of describing all polynomials $P \in \mathbb{Q}[x]$ for which the maps $P : \mathbb{Z}_p \to \mathbb{Z}_p$ are invertible for infinitely many prime numbers p. In Sect. B.3.3, we formulate a result of Julia, Fatou, and Ritt on the affine classification of *integrable* polynomial maps from the complex line to itself.

B.1 Chebyshev Functions over the Complex Numbers

B.1.1 Multivalued Chebyshev Functions

The *Chebyshev function of degree* $\alpha \in \mathbb{R}$ is the multivalued function T_α of a complex variable x that is defined by the relation

$$T_\alpha(x) = \frac{u^\alpha(x) + u^{-\alpha}(x)}{2}, \tag{B.1}$$

where u is the two-valued function defined by relation

$$x = \frac{u(x) + u^{-1}(x)}{2}. \tag{B.2}$$

In formula (B.1), we mean that every value $f(x)$ of the multivalued function $u^\alpha(x)$ is summed with the value $(f(x))^{-1}$ of the function $u^{-\alpha}(x)$ (and not with any other of its values). According to formula (B.2), the function $u(x)$ satisfies the equation $u^2(x) - 2xu(x) + 1 = 0$. Its roots $u_1(x)$, $u_2(x)$ satisfy $u_1(x)u_2(x) = 1$, so it doesn't matter which of the two roots we use in formula (B.1). (Note that these roots can be explicitly calculated: $u_{1,2}(x) = x \pm \sqrt{x^2 - 1}$.) The choice of the other root only permutes the summands $u^{\alpha}(x)$ and $u^{-\alpha}(x)$ and does not change the sum.

Theorem B.1 *The functions T_α can be defined by the relations*

$$x = \cos z(x), \quad T_\alpha(x) = \cos \alpha z(x).$$

Proof If $x = \cos z_0$, then $z(x) = \pm(z_0 + 2k\pi)$ and

$$\cos(\alpha z(x)) = \frac{\exp(i\alpha z(x)) + \exp(-i\alpha z(x))}{2}.$$

We also have $u_{1,2}(x) = \exp(\pm i z(x))$ and $u_{1,2}^{\pm\alpha}(x) = \exp i\alpha(\pm z(x))$. The theorem follows. □

Proposition B.2 *The function T_n, for positive integers n, is the polynomial of degree n with integer coefficients that satisfies the following formula:*

$$T_n(x) = \sum_{0 \le k \le [n/2]} \binom{n}{2k} x^{n-2k}(x^2 - 1)^k.$$

Proof The relation $T_n(x) = (u^n(x) + u^{-n}(x))/2$ combined with the equalities

$$u^n(x) = \left(x + \sqrt{x^2 - 1}\right)^n \quad \text{and} \quad u^{-n}(x) = \left(x - \sqrt{x^2 - 1}\right)^n$$

and Newton's binomial theorem gives the formula for $T_n(x)$. □

Definition B.3 The function T_n is called the *Chebyshev polynomial of degree n*.

The Chebyshev polynomials satisfy the identity $T_n(\cos z) = \cos nz$ (see Theorem B.1). They can be defined using this identity (and that is how Chebyshev defined them). The polynomial T_n is an even function for even n, and an odd function for odd n. The leading coefficient of the polynomial T_n is equal to 2^n. Later, we will need the formula $T_3(x) = 4x^3 - 3x$.

Corollary B.4 *The equation $T_n(x) = a$ can be explicitly solved by radicals. Its roots are the values $T_{1/n}(a)$ of the multivalued function $T_{1/n}$ at the point a.*

Proof If $\cos z = a$ and $x = \cos(z/n)$, then $x = T_{1/n}(a)$ and $T_n(x) = a$. □

This "trigonometric" computation, when carried over to algebra, gives a solution of the equation $T_n(x) = a$, where a is an element of a field with characteristic not equal to 2 (see Corollary B.9). Note that $T_{1/n}$ is an n-valued function: a choice of a value of the function $u(a)$ does not change the values $T_\alpha(a)$, but the function $u^{1/n}(a)$ assumes n values.

B.1.2 Germs of a Chebyshev Function at the Point $x = 1$

The multivalued function $T_\alpha(x)$, like the function x^α, has a special germ at the point $x = 1$, with value equal to 1. It is easier to work with single-valued germs than with their multivalued analytic continuations. From now on, by x^α we denote the germ

$$1 + \sum_{k=1}^{\infty} \frac{\alpha \cdots (\alpha - k + 1)}{k!} (x - 1)^k.$$

Properties of the Germs of Power Functions at the Point $x = 1$

A power function enjoys the following properties.

1. *Composition property:* if $f = x^\alpha$ and $g = x^\beta$, then $f \circ g = x^{\alpha\beta}$; in other words, $(x^\beta)^\alpha = x^{\alpha\beta}$.
2. *Multiplicative property:* $x^\alpha x^\beta = x^{\alpha+\beta}$.
3. *Algebraicity property:* for $\alpha = 1/n$, where n is a positive integer, the germ $z = x^\alpha$ satisfies the algebraic equation $z^n = x$.

Analytic Germs Invariant Under Involution

The involution τ of the complex line $\tau(u) = u^{-1}$ maps the point $u = 1$ to itself. It is easy to describe all germs f of analytic functions at this point that are invariant under the involution τ, i.e., such that $f = f \circ \tau$.

Proposition B.5 *The equality $f = f \circ \tau$ holds if and only if $f(u) = \varphi(x)$, where $x = (u + u^{-1})/2$ and φ is a germ of an analytic function at the point $x = 1$.*

Proof Let $u(x)$ be one of the two branches of the function defined by the equation

$$\frac{u(x) + u^{-1}(x)}{2} = x.$$

If $f = f(\tau)$, then the function $\varphi(x) = f(u(x))$ does not depend on the choice of branch and is analytic in a punctured neighborhood of the point $x = 1$. By the theorem on removable singularities, it is analytic at this point as well. □

Germs of analytic functions of a variable u that are not invariant under the involution τ give *two-valued Puiseux germs* of the variable x.

The *germ of the Chebyshev function T_α at the point $x = 1$* is the germ of the analytic function of the variable x such that the germ of the function $(u^\alpha + u^{-\alpha})/2$ (which is invariant under the involution τ) is equal to $T_\alpha(x(u))$, where $x(u) = (u + u^{-1})/2$. In this section, the germ of the Chebyshev function is denoted by T_α, the same symbol as was used for the multivalued function itself. The germs T_α inherit the properties of germs of power functions.

Properties of the Germs of Chebyshev Functions at the Point $x = 1$

1. *Composition property:* $T_\alpha \circ T_\beta = T_{\beta\alpha}$.
2. *Multiplicative property:* $T_\alpha T_\beta = (T_{\alpha+\beta} + T_{\alpha-\beta})/2$.
3. *Algebraicity property:* for $\alpha = n$, where n is a natural number, the germ T_α is the germ of the Chebyshev polynomial T_n. The germ $T_{1/n}$ satisfies the algebraic equation $T_n(T_{1/n}(x)) = x$.
4. *Trigonometric property:* $T_\alpha(\cos z) = \cos \alpha z$, in the sense that the germs of functions of the variable z at the point $z = 0$ are equal. The composition $T_\alpha(\cos z)$ is well defined, since $\cos 0 = 1$.

Proposition B.6 *The family of germs of Chebyshev functions satisfies properties 1–4 above.*

Proof Property 4 follows from Theorem B.1. This property completely characterizes the germ T_α. Indeed, the function $\cos z$ is even. By the implicit function theorem, the germ of the function z^2 at zero is an analytic function of the germ at $z = 1$ of the function $\cos z$. The function $\cos \alpha z$ is an analytic function of z^2. Properties 1–3 are simple properties of the function cos: to prove property 1, if $\cos v = \cos \beta z = T_\beta(\cos z)$, then $\cos \alpha v = T_\alpha(\cos v)$ and $T_\alpha T_\beta \cos z = \cos \alpha\beta z$. Property 2 follows from the identity $\cos \alpha z \cos \beta z = [\cos((\alpha + \beta)z) + \cos((\alpha - \beta)z)]/2$. Property 3 is proved for $\alpha = n$ in Proposition B.2; for $\alpha = 1/n$, it follows from the composition property. □

B.1.3 Analytic Continuation of Germs

In this section, we show that the set of values of the multivalued function generated by the germ T_α is consistent with the definition from Sect. B.1.1. The compositional inverse of the germ at 0 of the function $\cos z$ is a two-valued Puiseux germ at the point $x = 1$. Its values differ by a sign. Let $\pi^{-1}(x)$ be one of the two inverses (differing by sign) of the function $\cos z = x$ that has this Puiseux germ at the point $x = 1$. Consider the even function $\Phi_\alpha(z) = \cos \alpha z$ of the variable z. By definition, $T_\alpha = \Phi_\alpha \circ \pi^{-1}$.

The function $\cos z$ has simple critical points $z = k\pi$ and two critical values $x = \pm 1$. We say that the curve $x(t)$ that goes from point 1 to point x_0, i.e., $x(0) = 1$, $x(1) = x_0$, is *admissible* if $x(t) \neq \pm 1$ for $0 \leq t \leq 1$. The Puiseux germ of the function π^{-1} at the point $x = 1$ can be continued along the admissible curve $x(t)$ that goes from $x = 1$ to x_0 in the following sense: either of the two branches of the germ can be continued analytically along $x(t)$ up to $t = 1$ if $x_0 \neq \pm 1$, and up to any $t < 1$ if $x_0 = \pm 1$. In the second case, the continuation up to $t = 1$ is a two-valued Puiseux germ at the point $x_0 = \pm 1$ (whose branches at x_0 coincide).

In the same sense, the germ $T_\alpha = \Phi_\alpha \circ \pi^{-1}$ can be continued along any admissible curve $x(t)$. The germ T_α is regular and single-valued (not two-valued, like π^{-1}); therefore, it has a unique continuation along an admissible curve. For some admissible curves that go from $x = 1$ to the point $x = \pm 1$, the result of continuation may also turn out to be an analytic germ (and not a two-valued Puiseux germ).

Let us show that formulas (B.1) and (B.2) describe all values of the multivalued function that is obtained by continuation of the germ T_α. Let x_0 and $a = T_\alpha(x_0)$ be any numbers that satisfy (B.1) and (B.2).

Proposition B.7 *There exists an admissible curve $x(t)$ that goes from the point $x = 1$ to the point x_0 such that the analytic germ (or the Puiseux germ) that is obtained by continuation of the germ T_α along $x(t)$ takes the value a at the point x_0, where a, x_0 are as defined above.*

Proof Choose z_0 such that $\exp iz_0 = u(x_0)$, $\exp(\alpha i z_0) = u^\alpha(x_0)$. Let $z(t)$ be a curve with $z(0) = 0$, $z(1) = z_0$ such that $z(t)$ does not pass through the points $z = k\pi$ for $0 < t < 1$. Then the curve $x(t) = \cos z(t)$ is admissible; it goes from the point $x = 1$ to the point x_0, and the analytic continuation along this curve of the germ $T_\alpha = \cos\alpha(\cos^{-1})$ gives the germs that take the value a at the point x_0. □

Of special importance to us are the Chebyshev polynomials T_n and their inverses $T_{(1/n)}$. Proposition B.7 provides a description of the set of values of the function $T_{1/n}$ at a point a. Let u_1, u_2 be the roots of the equation $\left(u + u^{-1}\right)/2 = a$ (it is enough to take one of these roots). Let $\{v_{i,j}\}$ be the roots of the equation $v^n = u_i$, where $i = 1, 2$, $1 \le j \le n$. The set $T_{1/n}(a)$ of all values of the function at the point a is equal to the set

$$\left\{ \frac{v_{1,j} + v_{i,j}^{-1}}{2} \right\}$$

and to the set

$$\left\{ \frac{v_{2,j} + v_{2,j}^{-1}}{2} \right\}.$$

B.2 Chebyshev Functions over Fields

B.2.1 Algebraic Definition

The Chebyshev polynomials $T_n \in \mathbb{Z}[x]$ are defined over every field $\mathbf{k}$. If the characteristic of the field is zero, then $\mathbb{Z} \subset \mathbf{k}$ and $T_n \in \mathbf{k}[x]$. If the field has characteristic $p > 0$, then $\mathbb{Z}_p \subset \mathbf{k}$, and the polynomial obtained from T_n by reduction of the coefficients modulo p (which we denote by the same symbol T_n) lies in $\mathbf{k}[x]$. If $p \neq 2$, then $\deg T_n = n$, since the leading coefficient of the polynomial T_n is equal to 2^{n-1}.

Proposition B.8 *If the characteristic of the field* $\mathbf{k}$ *is not equal to* 2*, then the following identity holds in the field of rational functions* $\mathbf{k}(x)$*:*

$$T_n\left(\frac{x+x^{-1}}{2}\right)=\frac{x^n+x^{-n}}{2}. \tag{B.3}$$

Proof The result follows from the formulas (B.1) and (B.2). □

Corollary B.9 *If the characteristic* p *of the field* $\mathbf{k}$ *is not equal to* 2*, then the equation* $T_n(x)=a$ *with* $a\in\mathbf{k}$ *is explicitly solvable in radicals over the field* $\mathbf{k}$.

Proof Plugging $x=(v+v^{-1})/2$ into the identity (B.3), we obtain $(v^n+v^{-n})/2=a$. Then we solve the quadratic equation $u^2-2au+1=0$ for $u=v^n$. Let u_1,u_2 be its roots and $\{v_{1,j}\}$ the set of all roots of u_1 of degree n. Then the elements $v_{2,j}=v_{1,j}^{-1}$ form the set of all roots of degree n of u_2, since $u_1u_2=1$. All roots of the equation $T_n(x)=a$ can be expressed in the form

$$x=\frac{\left(v_{1,j}+v_{1,j}^{-1}\right)}{2}\quad\text{or}\quad x=\frac{\left(v_{2,j}+v_{2,j}^{-1}\right)}{2}.$$

□

The proof of Corollary B.9 shows that the equation $T_n(x)=a$ over a field $\mathbf{k}$ of characteristic not equal to 2 is solvable explicitly using the formula $x=T_{1/n}(a)$, which makes sense over $\mathbf{k}$.

B.2.2 Equations of Degree Three

Let F be a polynomial of degree n over a field $\mathbf{k}$ with characteristic equal to zero or greater than n. Define $Q(y)=aF(\lambda y+x_0)$, where $a,\lambda\neq 0$, and x_0 is an element of the field $\mathbf{k}$ or some finite extension. Under the assumptions about the characteristic of $\mathbf{k}$, we have

$$Q(y)=\sum\frac{a\lambda^kF^{(k)}(x_0)}{k!}y^k.$$

The linear function $Q^{(n-1)}$ takes the value 0 at some point q. Assume that when $x_0=q$, the coefficient of Q at y^{n-1} vanishes. By varying a and λ, we can make any two nonzero coefficients of Q equal to any two given nonzero numbers.

Using this transformation, we can reduce the polynomial $F(x)=a_3x^3+a_2x^2+a_1x+a_0$ to the form y^3+c or to the form $4y^3-3y+c$. Indeed, the polynomial F'' vanishes at the point $x_0=-a_2/3a_3$. There are two possible cases:

1. $F'(x_0)=0$. In this case, the polynomial F reduces to the form y^3+c via the transformation $aF(y+x_0)$, where $a=a_3^{-1}$, and we obtain $c=F(x_0)a$.

2. $F'(x_0) \neq 0$. In this case, the polynomial F reduces to the form $4y^3 - 3y + c$ via the transformation $aF(\lambda y + x_0)$ with $\lambda = (-4F'(x_0)/3a_3)^{1/2}$, $a = -3(\lambda F'(x_0))^{-1}$. Here $c = F(x_0)a$. (We choose any sign of λ, since we are looking for one transformation that has the properties we need rather than a description of all such transformations.)

Corollary B.10 *A cubic equation $F(x) = a_3x^3 + a_2x^2 + a_1x + a_0$ over a field* $\mathbf{k}$ *of characteristic not equal to* 2 *or* 3 *is solvable in radicals in the following way. Let $x_0 = -a_2/3a_3$ be the root of the polynomial F''.*

1. *If $F'(x_0) = 0$, then $x = x_0 + (-F(x_0)/a_3)^{1/3}$.*
2. *If $F'(x_0) \neq 0$, then $x = x_0 + \lambda T_{1/3}(-c)$, where λ and c are as defined above.*

B.2.3 Equations of Degree Four

An equation of degree four can be reduced to an equation of degree three (which is solvable using the function $T_{1/3}$) by considering a pencil of planar quadrics [12].

Let $Q : V \to \mathbf{k}$ be a quadratic form and $\dim_{\mathbf{k}} V = n$. A quadratic form in the plane or on the line can be decomposed as a product of linear factors (possibly not over the original field $\mathbf{k}$, but over a quadratic extension K). Let K be an extension of the field $\mathbf{k}$. Let V_K and Q_K denote the space and the form that correspond to V and Q under the extension $\mathbf{k} \subset K$.

Lemma B.11 *If Q_K can be factored, then* $\dim_{\mathbf{k}} \ker Q \geq n - 2$. *If this inequality holds, then we can explicitly find a factorization $Q_K = L_1L_2$ over a quadratic extension K of* $\mathbf{k}$.

Proof If $Q_K = L_1L_2$, then $\ker Q_K \supset \cap_{i=1,2}\{L_i = 0\}$ and $\dim_K \ker Q_K \geq n - 2$. The form Q is defined over k, and therefore, $\dim_{\mathbf{k}} \ker Q \geq n - 2$. If the inequality holds, then V can be expressed in the form $V = \ker Q \oplus W$, where $\dim_{\mathbf{k}} W \leq 2$. Let $\pi : V \to W$ be the projection along $\ker Q$, and $\tilde{Q}$ the restriction of the form Q to W. On W, we have the factorization $\tilde{Q} = \tilde{L}_1\tilde{L}_2$, and therefore $Q = (\pi^*\tilde{L}_1)(\pi^*\tilde{L}_1)$. □

Proposition B.12 *Let P, Q be quadratic polynomials of two variables. The coordinates x, y of the points of intersection of two planar quadrics $\mathscr{P} = 0$ and $\mathscr{R} = 0$ can be found by solving one cubic equation and a number of quadratic and linear equations.*

Proof All quadrics of the pencil $0 = \mathscr{Q}_\lambda = \mathscr{P} + \lambda\mathscr{R}$, where λ is a parameter, pass through the desired points. For some λ, some quadric $\mathscr{Q}_\lambda = 0$ splits into a union of two lines, i.e., $\mathscr{Q}_\lambda = \mathscr{L}_1\mathscr{L}_2$, where $\mathscr{L}_1$, $\mathscr{L}_2$ are polynomials of degree 1. These λ satisfy the cubic equation $\det(Q_\lambda) = 0$, where $Q_\lambda = P + \lambda Q$ is the 3×3 matrix of quadratic forms that corresponds to the equation of the quadric in homogeneous coordinates. Indeed, for this λ, the form Q_λ has nontrivial kernel, and therefore, $Q_\lambda = L_1L_2$, where L_1, L_2 can be found by solving one quadratic equation and a