Discrete Mathematics 315–316 (2014) 83–94

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Chebyshev action on finite fields

T. Alden Gassert

Department of Mathematics and Statistics, University of Massachusetts, Amherst, 710 N. Pleasant Street, Amherst, MA, 01003, USA

ARTICLE INFO

Article history:
Received 19 September 2012
Received in revised form 12 October 2013
Accepted 15 October 2013
Available online 5 November 2013

Keywords:
Chebyshev polynomial
Iterated polynomial
Post-critically finite map
Finite field
Prime decomposition

ABSTRACT

Given a polynomial $\phi(x)$ and a finite field $\mathbb{F}_q$ one can construct a directed graph where the vertices are the values in the finite field, and emanating from each vertex is an edge joining the vertex to its image under ϕ. When ϕ is a Chebyshev polynomial of prime degree, the graphs display an unusual degree of symmetry. In this paper we provide a complete description of these graphs, and then use these graphs to determine the decomposition of primes in the Chebyshev radical extensions.

1. Introduction

Let K be a number field and ϕ be a monic polynomial of degree at least 2 with coefficients in $\mathcal{O}_K$, the ring of integers of K. We denote the n-fold iterate of ϕ by $\phi^n(x) = \phi(\phi^{n-1}(x))$, where $\phi^0(x) := x$. For a fixed $t \in \mathcal{O}_K$, if $\phi^n(x) - t$ is irreducible for $n \geq 1$, one can obtain, very naturally, a tower of fields over K in the following way. Let $\{\theta_0 = t, \theta_1, \theta_2, \ldots\}$ be a compatible sequence of preimages of t satisfying $\phi(\theta_n) = \theta_{n-1}$ (and hence $\phi^n(\theta_n) - t = 0$), then we obtain a nested sequence of fields

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots,$$

where $K_n := K(\theta_n)$ and $[K_n : K] = (\deg \phi)^n$.

In this paper, we give the decomposition of prime ideals in the towers obtained when $K = \mathbb{Q}$ and $\phi = T_\ell$ is a Chebyshev polynomial of the first kind of prime degree ℓ. The number fields arising from this construction are the *Chebyshev radical extensions*, and from now on, we use K_n to refer to such an extension of degree ℓ^n over $\mathbb{Q}$.

In general, for each $d \geq 0$, $T_d \in \mathbb{Z}[x]$ is the monic, degree-d polynomial defined by

$$T_d(z + z^{-1}) = z^d + z^{-d},$$

or equivalently, $T_d(2\cos\theta) = 2\cos(d\theta)$. These polynomials satisfy a multitude of relations (see [4, Chapter 2], or [6, Chapter 1]), but from a dynamical standpoint, the most significant property is that these polynomials commute under composition:

$$T_d \circ T_e = T_e \circ T_d = T_{de}.$$

In particular, $T_\ell^n = T_{\ell^n}$, which provides an intimate access to each number field in the tower described above. We note that there are many values of $t \in \mathbb{Z}$ for which $T_\ell^n(x) - t$ is irreducible for each $n \geq 1$. For example, if ℓ is an odd prime and t is divisible by ℓ exactly once, then it can easily be shown that every iterate is Eisenstein at ℓ. A broader result is stated in Theorem 1.2(1) below.

We determine the decomposition of primes by studying the dynamics of a Chebyshev polynomial over a finite field, an approach proposed by Aitken, Hajir, and Maire [1]. For a general polynomial ϕ, the dynamics of ϕ over $\mathbb{F}_q$, where q is a prime

E-mail address: gassert@math.umass.edu.

0012-365X/$ – see front matter
http://dx.doi.org/10.1016/j.disc.2013.10.014

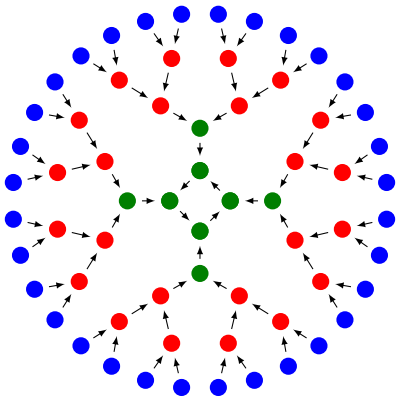

Fig. 1. A component of the graph of T_2 over the finite field of order 29^4. The color of the vertex corresponds to the smallest field containing the element associated to the vertex: green—$\mathbb{F}_{29}$; red—$\mathbb{F}_{29^2}$; blue—$\mathbb{F}_{29^4}$. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

power, can be captured in a directed graph. The graph is constructed as follows: each element $a \in \mathbb{F}_q$ corresponds to a vertex in the graph – which by abuse of notation we also call a – and the graph contains the directed edge (a, b) if $\phi(a) = b$. In the case of the Chebyshev polynomials, the components of the graph are radially symmetric. (See Fig. 1.) Moreover, the number of components and their structure can be determined completely. We use the standard definitions from arithmetic dynamics to describe this structure.

Definition 1.1. Let S be a set and $\phi: S \to S$ a map. An element $a \in S$ is *preperiodic* with respect to ϕ, and we write $\mathrm{pper}_{\phi,S}(a) = \rho$, if there exist minimal integers $\rho \geq 0$ and $\pi \geq 1$ such that $\phi^{\rho+\pi}(a) = \phi^{\rho}(a)$. Moreover, if $\rho > 0$, then a is *strictly preperiodic*. If $\rho = 0$, then a is *periodic* with respect to ϕ, and we write $\mathrm{per}_{\phi,S}(a) = \pi$.

The predictable nature of the graph allows us to deduce reducibility results for $T_\ell^n(x) - t$. For the benefit of the reader, we provide a special case of the main result (Theorem 3.1). For a prime p, let

$$v_p = \max_{a \in \mathbb{F}_p} \{\mathrm{pper}_{T_\ell, \mathbb{F}_p}(a)\},$$

and let $\bar{t}$ denote the reduction of t modulo p.

Theorem 1.2. (1) *If $v_p > 0$ and $\mathrm{pper}_{T_\ell,\mathbb{F}_p}(\bar{t}) = v_p$, then every iterate $T_\ell^n(x) - t$ is irreducible modulo p, and thus irreducible in $\mathbb{Z}[x]$.*
(2) *If $v_p > 0$ and $n \leq v_p - \mathrm{pper}_{T_\ell,\mathbb{F}_p}(\bar{t})$, then $T_\ell^n(x) - t$ splits in $\mathbb{F}_p$.*

By a classical result of Dedekind, for all but finitely many primes, the factorization of the polynomial modulo p and the decomposition of the ideal $p\mathbb{Z}$ are linked. In particular, the factorization results define the following behavior.

Corollary 1.3. *Suppose p does not divide the discriminant of $T_\ell^n(x) - t$. Then*

(1) *p is inert in K_n (that is, $p\mathbb{Z}$ is a prime ideal in $\mathcal{O}_{K_n}$) if $v_p > 0$ and $\mathrm{pper}_{T_\ell,\mathbb{F}_p}(\bar{t}) = v_p$;*
(2) *p splits in K_n (that is, $p\mathbb{Z} = \mathfrak{p}_1 \cdots \mathfrak{p}_{\ell^n}$) if $v_p > 0$ and $n \leq v_p - \mathrm{pper}_{T_\ell,\mathbb{F}_p}(\bar{t})$.*

There are two cases that deserve special mention: the case ℓ is an odd prime and $t = 2$, and the case $\ell = 2$ and $t = 0$. For a generic choice of t, the extension K_n is not Galois. Passing to the Galois closure K_n^{Gal}, the Galois group $\mathrm{Gal}(K_n^{\mathrm{Gal}}, \mathbb{Q})$ is non-abelian and is isomorphic to a (possibly very large) subgroup of the wreath product $\mathrm{Wr}(\mathbb{Z}/n\mathbb{Z}, S_\ell)$ [7, Theorem 3.56]. In the first of the two cases listed above, the splitting field of $T_\ell^n(x) - 2$ is an abelian extension of $\mathbb{Q}$. In fact, the splitting field is $\mathbb{Q}(\zeta_{\ell^n})^+$, the maximal totally real subfield of the cyclotomic field $\mathbb{Q}(\zeta_{\ell^n})$, where ζ_{ℓ^n} is a primitive ℓ^n-th root of unity. In the latter case, the Chebyshev radical extension generated by $T_2^n(x)$ is $\mathbb{Q}(\zeta_{2^{n+2}})^+$. In both cases, the decomposition of primes in the towers are known by consequence of the cyclotomic reciprocity law [11, Theorem 2.13]. Namely, for any prime ℓ, the prime p splits completely in $\mathbb{Q}(\zeta_{\ell^n})^+$ if and only if p is congruent to ± 1 modulo ℓ^n. Our decomposition result provides an alternative proof of cyclotomic reciprocity in the totally real case, and more generally may be viewed as an extension of cyclotomic reciprocity to non-abelian extensions of $\mathbb{Q}$.

The structure of the paper is the following. In Section 2, we give a complete description of the graph of T_ℓ over $\mathbb{F}_q$. We combine our knowledge of the graphs with a result by Aitken, Hajir, and Maire to prove our main theorem in Section 3. The connection to cyclotomic reciprocity is also presented in this section. In Section 4, we answer a question posed by Jones regarding the density of periodic points as the order of the field goes to infinity.