Cycles of Polynomial Mappings

by

Michael Ernest Zieve

B.A. (Harvard University) 1992

A dissertation submitted in partial satisfaction of the

requirements for the degree of

Doctor of Philosophy

in

Mathematics

in the

GRADUATE DIVISION
of the

UNIVERSITY of **CALIFORNIA** at **BERKELEY**

Committee in charge:

Professor Hendrik W. Lenstra, Jr., Chair

Professor Robert F. Coleman

Professor David Aldous

1996

The dissertation of Michael Ernest Zieve is approved:

Chair Date

Date

Date

University of California, Berkeley

1996

Abstract

Cycles of Polynomial Mappings

by

Michael Ernest Zieve

Doctor of Philosophy in Mathematics

University of California at Berkeley

Professor Hendrik W. Lenstra, Jr., Chair

Let R be a ring and $f(x) \in R[x]$ a polynomial over R; we study the finite cycles of f in R, namely the m-tuples of distinct elements $x_1, \ldots, x_m \in R$ such that $f(x_1) = x_2$, $f(x_2) = x_3, \ldots, f(x_{m-1}) = x_m$ and $f(x_m) = x_1$. One phenomenon we repeatedly observe is that the possible cycle lengths m are severely restricted. For instance, if $R = \mathbb{Z}$ is the ring of integers, then no polynomial over R has cycles of length greater than two. We give results restricting the cycle lengths for various types of rings. Our most difficult results deal with discrete valuation rings R. For these rings it is not too hard to control the part of the cycle length which is relatively prime to characteristic of the residue field, but the part of the cycle length which is a power of the residue characteristic is much more elusive. We prove various bounds in this last case, and give examples illustrating that are bounds are nearly best possible. We also study numerous other properties of cycles of polynomial mappings.

Contents

Acknowledgements

First and foremost, I would like to thank Hendrik W. Lenstra, Jr. for answering every question I have ever asked him, as well as several I did not think to ask. I would also like to thank Bjorn Poonen and Joseph H. Silverman for their contributions to this work.

Chapter 1

Introduction

This thesis is concerned with cycles of polynomial mappings of rings. Given a ring R and a polynomial $f(x) \in R[x]$, there is an induced mapping $f : R \to R$ sending y to $f(y)$. We are primarily interested in the behavior of this mapping under iteration. In particular, we study those finite subsets of R which are preserved by the mapping f; a *cycle* of f is an m-tuple $(x_1, x_2, \ldots, x_m)$ of distinct elements of R for which f maps $x_1 \to x_2 \to x_3 \cdots \to x_m \to x_1$. In the next chapter we prove various results about cycles of polynomial mappings, some of which we highlight below. We begin Chapter 3 by explaining how these results fit into the general framework of nonarchimedean dynamical systems: essentially, when we put a nonarchimedean valuation on R we can geometrically study the dynamical behavior of the map f under iteration. In the remainder of Chapter 3 we attempt to give a panoramic view of the various studies which from our perspective form pieces of the field we call nonarchimedean dynamics; our goal is to convey our belief that these numerous different studies, some of which are quite far removed from one another in goals and techniques, should in fact be viewed as pieces of a single broad field of mathematics.

We now summarize the results of Chapter 2. The first five results provide various restrictions on the lengths of cycles of polynomial mappings. The thrust of these results is that there are severe arithmetic restrictions on the cycle lengths. The idea behind the proofs of these results is that one can study a cycle in a ring R by studying the relationships between the lengths of the projections of the cycle modulo successive powers of I. Naturally, one can prove more precise results when one considers a restricted class of rings R. Thus, Theorems 7 and 8 give very precise results about the cycle lengths in case R is a discrete valuation ring; Theorem 8 is the deepest result in this thesis, and we postpone its intricate and difficult proof until Section 2.3. All of these results are 'nonexistence' results, in the sense that they show various numbers cannot occur as cycle lengths under appropriate circumstances; we complement these results with three 'existence' results, namely Proposition 10 and the surrounding examples. Proposition 12 treats a different problem: if R is a discrete valuation ring, it discusses the possibilities for the least power of the maximal ideal modulo which the elements of the cycle are all distinct. The next result completely determines which cycle lengths occur over the rings of p-adic integers, and the final result of Section 2.1 shows an 'integrality' result: under certain circumstances, cycles in the fraction field of a domain must actually lie in the domain itself.

The passage from Section 2.1 to Section 2.2 is accompanied by a change in tone. Whereas in Section 2.1 we give deep results relying on intricate hypotheses, in Section 2.2 we include only results of a lighter type, namely charming results which hold in extreme generality. Here R is an integral domain. We begin by showing how a cycle in R leads to several solutions of an equation $u + v = w$ in units u, v of R (with $w \in R$ fixed). Such unit equations have been thoroughly studied, and there are various circumstances in which one has control over the solutions of such equations; we discuss this in the first subsection of this section. The next subsection gives some consequences for cycles; in particular, Corollary 25 shows the surprising result that, if some polynomial over the integral domain R has a cycle in R of length a prime number p, then there are polynomials over R having cycles in R of any prescribed length less than p. An immediate consequence is that the set of prime numbers occurring as cycle lengths of polynomial mappings of an integral domain R is an initial segment of the set of prime numbers. We conclude this section with further general results, including criteria on R for the existence of cycles in R of prescribed lengths.

In Section 2.3 we prove Theorem 8, which bounds the power of p in the cycle length of a polynomial mapping of a discrete valuation ring of characteristic zero and residue characteristic p. The proof relies on a series of combinatorial lemmas, as well as two deep algebraic results, one of which was proven for us by Hendrik W. Lenstra, Jr. We also discuss how one can prove better bounds for polynomials satisfying certain mild hypotheses.

The results mentioned above deal with polynomial mappings of rings. In Section 2.4 we discuss the extent to which the corresponding results remain valid in the setting of power series over complete local rings; and in Section 2.5 we study rational functions over rings and rational mappings of the projective line over a nonarchimedean field. Finally, in Section 2.6 we give various examples illustrating the general theory.

Chapter 2

The main results

Let R be a ring and $f(x) \in R[x]$ a polynomial over R; we will study the finite cycles of f in R, i.e. the m-tuples of distinct elements $x_1, \ldots, x_m \in R$ such that $f(x_1) = x_2, f(x_2) = x_3, \ldots, f(x_{m-1}) = x_m$ and $f(x_m) = x_1$. Here, and throughout this chapter, all rings are assumed to be commutative with a multiplicative identity element 1. We shall prove various results about the cycles of polynomial mappings. We then consider other classes of mappings, including power series over complete local rings and certain rational maps on a ring or on $\mathbb{P}^1$ of a nonarchimedean field. Our proofs of the results for rational maps amount to reducing to the case of polynomials; this is rather different from what we do for power series. Our proofs in the power series case are the same as the proofs in the polynomial case, although there are some technical difficulties that must be addressed; in Section 2.4 we summarize the differences between the proofs in the polynomial and power series cases. Thus, the reader primarily interested in power series should consult Section 2.4 while reading the rest of this chapter.

We now give some notation. For a function f, by f^k we denote the k^{th} iterate of f. Some of our results hold only under the assumption that R is a discrete valuation ring; there is some terminology we will constantly use in this circumstance. Namely, whenever we speak of a discrete valuation ring R, we use the following notation: $\mathfrak{m}$ is the maximal ideal, π is a uniformizer, $\kappa = R/\mathfrak{m}$ is the residue field, $p = \operatorname{char}(\kappa)$ the residue characteristic, $e = \operatorname{ord}_{\mathfrak{m}}(p)$ the ramification index, and K is the fraction field of R. Finally, we use the term nonarchimedean field to refer to a field K together with a nonarchimedean valuation on K.

2.1 Results

We begin with a preliminary description of the possible cycle lengths.

Proposition 1. *Let R be a ring and let I be a proper ideal of R which contains every zero-divisor in R. Let $f(x) \in R[x]$ have a cycle $(x_1, \dots, x_m)$ in R. Then either $m = k$ or $m = ks$ or $m = ksp^n$, where n is a positive integer, k is the length of the projected cycle in R/I (i.e. the size of the image of $\{x_1, \dots, x_m\}$ in R/I), p is the additive order of 1 in R/I, and s is the least positive integer for which $\sum_{i=0}^{s-1}((f^k)'(x_1))^i \in I$.*

It is possible that p or s (or both) might not exist; in those cases the result still holds, but with even fewer possibilities for m. For instance, if s does not exist (which happens e.g. if $(f^k)'(x_1) \in I$) then $m = k$.

Corollary 2. *With notation as above, if $(f^k)'(x_1) \in I$, then $m = k$.*

Borrowing some terminology from complex dynamics, if $(f^k)'(x_1) \in I$ we say the cycle is attracting; thus, this corollary may be interpreted as saying that attracting cycles inject modulo I.

Proof of Proposition 1. To start with, we may assume $x_1 = 0$: for, consider $\hat{f}(x) = f(x + x_1) - x_1$; this polynomial has the cycle $(0, x_2 - x_1, \dots, x_m - x_1)$. Since this cycle is a translate of the original cycle, its projection in R/I has the same length, i.e. the same k as does the original cycle. Moreover, it has the same s, since

$$(\hat{f}^k)'(0) = \prod_{i=1}^{k} \hat{f}'(x_i - x_1) = \prod_{i=1}^{k} f'(x_i) = (f^k)'(x_1);$$

thus, it suffices to prove the result in case $x_1 = 0$.

Clearly k divides m, so we consider $g = f^k$, for which 0 lies in an m/k-cycle in I. Say $g(x) \equiv b + ax \pmod{x^2}$, where $b = g(0) \in I$ and $a = g'(0) = (f^k)'(0)$. If $b = 0$, then $m = k$; now assume $b \neq 0$. By an easy induction,

$$g^j(x) \equiv b(1 + a + \cdots + a^{j-1}) + a^j x \pmod{(bI, Ix, x^2)}.$$

Since 0 is in an m/k-cycle of g, there is a least positive integer t for which $g^t(0) \equiv 0 \pmod{bI}$; clearly t divides m/k. Let $c = 1 + a + \cdots + a^{t-1}$. Then t is the least positive integer for which there is some $\gamma \in I$ such that $b(c-\gamma) = 0$; thus $c - \gamma$ is either zero or a zero-divisor, and in any case must be in I, so $c \in I$. Conversely, if $c \in I$ then clearly $bc \in bI$; thus, t is the least positive integer for which $1 + a + \cdots + a^{t-1} \in I$, so $t = s$. Since $a^t - 1 = (a-1)(1 + a + \cdots + a^{t-1}) \in I$, we have $a^t \equiv 1 \pmod{I}$.

Now consider $h(x) = g^s(x) \equiv \tilde{b} + \tilde{a}x \pmod{x^2}$; this polynomial has an m/ks-cycle in I containing 0. Here $\tilde{b} \equiv 0 \pmod{bI}$ and $\tilde{a} \equiv a^t \equiv 1 \pmod{I}$. If $\tilde{b} = 0$, then $m = ks$; now assume $\tilde{b} \neq 0$. As above, let $\tilde{t}$ be the least positive integer for which $h^{\tilde{t}}(0) \equiv 0 \pmod{\tilde{b}I}$; clearly $\tilde{t}$ divides m/kt. As above, $\tilde{t}$ is the least positive integer for which $\sum_{i=0}^{\tilde{t}-1} \tilde{a}^i$ lies in I; since $\tilde{a} \equiv 1 \pmod{I}$, this says $\tilde{t}$ is the least positive integer in I, so $\tilde{t} = p$.

Next consider $\ell(x) = h^p(x)$; this polynomial has an m/ksp-cycle in I containing 0. As above, either $m = ksp$ or there is another factor p dividing m, i.e. ksp^2 divides m. We can continue in this manner; since at each stage we either find m or introduce another factor p in m, after finitely many steps we will have introduced all factors p in m, hence will have found m, which must have the desired form. ■

In case I is a prime ideal we can restate the Proposition by relating s to the multiplicative order of $(f^k)'(x_1)$ in $(R/I)^*$.

Corollary 3. *With notation as above, suppose in addition that I is a prime ideal. Then either $m = k$ or $m = kr$ or $m = krp^n$, where r is the multiplicative order of $(f^k)'(x_1)$ in $(R/I)^*$. In particular, we have $m = krp^n$ where $k \leq \#R/I$ and $r \mid \#(R/I)^*$.*

Proof. Note that $r = 1$ if and only if $(f^k)'(x_1) \equiv 1 \pmod{I}$, in which case $s = p$; in this case the Proposition implies that either $m = k$ or $m = kp^n$, which is equivalent to the desired conclusion. Now suppose $r > 1$; then $a = (f^k)'(x_1) \not\equiv 1 \pmod{I}$, so, since I is prime, $a^j - 1 = (a-1)(1 + a + \cdots + a^{j-1})$ lies in I precisely when

$1+a+\cdots+a^{j-1}\in I$. Thus r exists precisely when s exists, and if they exist they are equal, which completes the proof. ■

This corollary applies to local rings, such as $\mathbb{Z}/p^t\mathbb{Z}$. It also applies to subrings of number fields. For this chapter we are primarily concerned with the case of discrete valuation rings, so we restate the corollary in this case.

Corollary 4. *Let $f(x)\in R[x]$ have a cycle $(x_1,\ldots,x_m)$ in the discrete valuation ring R. Then either $m=k$ or $m=kr$ or $m=krp^n$, where n is a positive integer, k is the length of the projected cycle in κ (i.e. the size of the image of $\{x_1,\ldots,x_m\}$ in κ), and r is the multiplicative order of $(f^k)'(x_1)$ in κ^* (set $r=\infty$ if $(f^k)'(x_1)\in\mathfrak{m}$).*

This corollary severely restricts the possible cycle lengths, as indicated by our next result.

Corollary 5. *Let $f(x)\in R[x]$ have a cycle of length m in the discrete valuation ring R. Then $m=kb$ where k is the length of the projected cycle in κ (so $k\leq\#\kappa$). Under f^k the cycle splits into k disjoint cycles of length b, each lying in some coset of $\mathfrak{m}$ in R. Then $b=r$ or $b=rp^n$, where r is the order of a cyclic subgroup of κ^* (so $r\mid\#\kappa^*$).*

Our next task is to bound n. This only matters in case the residue characteristic is positive. When the discrete valuation ring R has positive characteristic, any value of n can occur; Poonen provided a proof of this shortly after I posed the question to him [19]. I present his proof below.

Lemma 6 (Poonen). *Let R be a complete discrete valuation ring of characteristic $p>0$. For any $n>0$ there exist polynomials $x^p+cx\in R[x]$ (with $c\in 1+\mathfrak{m}$) having cycles in $\mathfrak{m}$ of length p^n.*

Proof. [Poonen] Let $g(x)=Tx+x^p\in\mathbb{F}_p[[T]][x]$. Let $K=\mathbb{F}_p((T))$, and let v be the valuation of the algebraic closure $\bar{K}$ of K which is normalized by $v(T)=1$. Let x_1 be a nonzero solution to $g(x)=0$, so $v(x_1)=1/(p-1)$. Let x_2 be a nonzero solution to $g(x)=x_1$, so $v(x_2)=1/p(p-1)$, and so on.

Make the $\mathbb{F}_p$-vector space generated by $x_1, ..., x_k$ into an $\mathbb{F}_p[T]$-module by letting T act as the additive polynomial g. This module is generated by x_k and is isomorphic to the module $\mathbb{F}_p[T]/(T^k)$. Now let $F(x) = x + g(x)$, which acts as $1 + T$. Then x_k is a periodic point of F of period equal to the order of $1 + T$ in the multiplicative group $(\mathbb{F}_p[T]/T^k)^*$, which is the least integer no less than $\log_p k$. Choosing $k = p^n$ makes this order be n.

Now, the field $L = K(x_k)$ is a totally ramified extension of K of degree $p^{k-1}(p-1)$, so its field of constants is $\mathbb{F}_p$. In other words, by the classification of local fields of characteristic p, there is an isomorphism $L \cong \mathbb{F}_p((t))$. Under this isomorphism, $F(x)$ becomes a polynomial $f(x) = x^p + cx$ with coefficients in $\mathbb{F}_p[[t]]$ and $c - 1 \in t\mathbb{F}_p[[t]]$, and x_k becomes a periodic point (in $t\mathbb{F}_p[[t]]$) of f of period n. Finally, $\mathbb{F}_p[[t]]$ embeds into R, so the result is proved. ■

Theorem 7. *Let R be a discrete valuation ring of characteristic $p > 0$. For any $n > 0$ there exists $f(x) \in R[x]$, of degree p, having a cycle $(y_1, \ldots, y_{p^n})$ in $\mathfrak{m}$ with $f'(y_1) \equiv 1 \pmod{\mathfrak{m}}$.*

Proof. Let $\tilde{R}$ be the completion of R; the previous result produces a monic polynomial $g(x) \in \tilde{R}[x]$, of degree p, having a cycle $(x_1, \ldots, x_{p^n})$ in $\mathfrak{m}$ (with $g'(x_1) \equiv 1 \pmod{\mathfrak{m}}$). Now choose elements $y_1, \ldots, y_{p^n}$ in R so that each $y_i - x_i$ is in a sufficiently high power of $\mathfrak{m}$; the Lagrange interpolation formula produces a polynomial $f(x)$ over the fraction field of R which has the cycle $(y_1, \ldots, y_{p^n})$, and in fact the polynomial must lie in $R[x]$ and must satisfy $f'(x_1) \equiv 1 \pmod{\mathfrak{m}}$. ■

When the discrete valuation ring R has characteristic zero, the situation is very different (and significantly more difficult). Here there is a bound on n, as indicated by the following result.

Theorem 8. *Suppose R is a discrete valuation ring of characteristic zero, and $p > 0$. Let $h(x) \in R[x]$ have a cycle $(x_1, \ldots, x_m)$ in $\mathfrak{m}$, and suppose that $h'(x_1) \equiv 1 \pmod{\mathfrak{m}}$. Then $m = p^n$, where the integer n satisfies $n \leq 1 + (\log(2e) - \log(p-1))/\log p$. Moreover, if $p = 2$ then $n \leq 1 + (\log e/\log 2)$.*

Our proof of this result is rather complicated, and we postpone it until Section 2.3; there we also discuss possible improvements of this bound. We now briefly summarize the idea of the proof: when $x_1 = 0$ (which we may assume, as above) we show that the first several coefficients of $f^{p^i}(x) - x$ are in rather high powers of $\mathfrak{m}$, for each small i; then, once they are in sufficiently high powers, we show we must in fact have $f^{p^i}(0) = 0$. We now show that this bound on n is nearly best possible, by giving a family of examples for which the value of n is within 1 of our bound.

Example 9. Let R be the valuation ring of $K = \mathbb{Q}_p(\mu_{p^n})$, where μ_{p^n} is the group of p^n-th roots of unity, and let ζ be a primitive p^n-th root of unity, so $\zeta \equiv 1 \pmod{\mathfrak{m}}$. Then $K/\mathbb{Q}_p$ is totally ramified, of degree $e = p^{n-1}(p-1)$. For any nonzero $y \in \mathfrak{m}$, the polynomial $f(x) = \zeta x \in R[x]$ has the p^n-cycle $(y, y\zeta, y\zeta^2, \ldots, y\zeta^{p^n-1})$, and the power of p in the cycle length, namely n, satisfies

$$n = 1 + \frac{\log e - \log{(p-1)}}{\log p}.$$

In fact, if R is the valuation ring of $\mathbb{Q}_p(\mu_{p^n})$, and we have any $a \le \#\kappa$, $b \mid \#\kappa^*$, and $n_0 \le n$, then there is a polynomial in $R[x]$ having an abp^{n_0}-cycle in R, for which a is the length of the projected cycle in κ. We will prove this in Example 11. First we give the following result, which essentially reduces the problem of determining the lengths of cycles in R to the problem of determining the lengths of cycles in $\mathfrak{m}$. We prove it for local rings; in the special case of discrete valuation rings with finite residue fields, a more difficult proof has been given by Pezda [18].

Proposition 10. *Let R be a local ring with maximal ideal $\mathfrak{m}$. Suppose some polynomial $g(x) \in R[x]$ has a cycle in $\mathfrak{m}$ of length m. Then, for any $k \le \#R/\mathfrak{m}$, there is a polynomial in $R[x]$ having a cycle in R of length km. In fact, if the cycle of length m is $(y_1, \ldots, y_m)$, and $a_1, \ldots, a_k$ are any elements of R lying in distinct classes $\pmod{\mathfrak{m}}$, then there is a polynomial in $R[x]$ which has the cycle*

$$\sigma = (a_1 + y_1, a_2 + y_1, \ldots, a_k + y_1, a_1 + y_2, \ldots, a_k + y_2, a_1 + y_3, \ldots, a_k + y_m).$$

Proof. It suffices to construct polynomials $f_j(x) \in R[x]$ (for $1 \le j \le k$) such that, for each i and ℓ,

$$f_j(a_i + y_\ell) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \ne j; \end{cases}$$

for, given such polynomials, the polynomial

$$\Big(g(x - a_k) + a_1\Big) \cdot f_k(x) + \sum_{d=1}^{k-1} (x + a_{d+1} - a_d) \cdot f_d(x)$$

has the desired cycle σ. So now we need only construct f_j. To this end, let $h_j(x) = \prod(x - a_i - y_r)$, where the product is over all i, r with $i \ne j$. Then each $h_j(a_j + y_s) \in R^*$, so

$$f_j(x) = 1 - \prod_{s=1}^{m} \left(1 - \frac{h_j(x)}{h_j(a_j + y_s)}\right)$$

is an element of $R[x]$. This polynomial f_j takes the desired values at the points $a_i + y_\ell$. ■

We can now show that Corollary 5, along with the bound in Theorem 8, is nearly best possible.

Example 11. Let R be the valuation ring of $K = \mathbb{Q}_p(\mu_{p^n})$, where μ_{p^n} is the group of p^n-th roots of unity, and let ζ be a primitive p^n-th root of unity, so $\zeta \equiv 1 \pmod{\mathfrak{m}}$. Then $K/\mathbb{Q}_p$ is totally ramified, of degree $e = p^{n-1}(p-1)$. Let α be a primitive $(p-1)^{\text{th}}$ root of unity in R. Pick any $a \le p$ $(= \#\kappa)$, $b \mid p - 1$ $(= \#\kappa^*)$, and $n_0 \le n$. For any nonzero $y \in \mathfrak{m}$, the polynomial $f(x) = \alpha^{(p-1)/b}\zeta^{p^{n-n_0}} x \in R[x]$ has the bp^{n_0}-cycle $(y, y\zeta, y\zeta^2, \ldots, y\zeta^{bp^{n_0}-1})$ in $\mathfrak{m}$; by the previous proposition, there is a polynomial in $R[x]$ having an abp^{n_0}-cycle in R.

Next we show that, in many cases, all the powers of p in the cycle length must occur already modulo some small power of $\mathfrak{m}$.

Proposition 12. *Suppose R is a discrete valuation ring of characteristic 0 and residue characteristic $p > 0$. Let $f(x) \in R[x]$ have a cycle in R of length yp^n, where y is not divisible by p. Let $q + 1$ be minimal such that the projected cycle $(\mathrm{mod}\ \mathfrak{m}^{q+1})$ has length divisible by p^n—in other words, this is the first power of $\mathfrak{m}$*

modulo which we already see the entire p-power in the cycle length. If the completion of R does not contain the p^{th} roots of unity (which occurs, for instance, if $p-1\nmid e$) then $q \le e$. If the completion of R contains a primitive p^{th} root of unity, then q can be arbitrarily large.

There is an explicit formula for q: namely, if $(x_1,\dots,x_m)$ is the cycle, and $p\mid m$, then (for any i) we have

$$q=\operatorname{ord}_{\mathfrak{m}}(x_{i+m/p}-x_i).$$

Proof. If the completion $\tilde{R}$ of R contains a primitive p^{th} root of unity ω, then $f(x)=\omega x$ has the p-cycle $(x_0,\omega x_0,\dots,\omega^{p-1}x_0)\subset\mathfrak{m}$, for any nonzero $x_0\in\mathfrak{m}$; by choosing x_0 in a sufficiently high power of $\mathfrak{m}$, we can make q arbitrarily large (for polynomials and cycles in $\tilde{R}$). To achieve this with polynomials and cycles in R, simply choose elements $y_0,\dots,y_{p-1}$ in R so that each $y_i-\omega^i x_1$ is in a sufficiently high power of $\mathfrak{m}$; the Lagrange interpolation formula produces a polynomial over the fraction field of R which has the cycle $(y_0,\dots,y_{p-1})$, and in fact the polynomial must lie in $R[x]$.

Conversely we show that, if $q>e$, then the completion of R contains the p^{th} roots of unity; this will finish the proof. By taking the appropriate iterate of our polynomial, we may assume that the cycle in question is a p-cycle; by conjugating by a translation we may assume the cycle contains 0. These operations do not affect q. Say the cycle is $(0,x_1,x_2,\dots,x_{p-1})$; then $\operatorname{ord}_{\mathfrak{m}}(x_1)=q$. Thus $f(x)=x_1+ax+a_2x^2+\dots$; by an easy induction,

$$f^j(x)\equiv x_1(1+a+\dots+a^{j-1}) \pmod{(x_1^2,x)},$$

so from $f^p(0)=0$ we conclude that

$$1+a+\dots+a^{p-1}\equiv 0 \pmod{x_1}.$$

This implies that

$$(a-1)^p\equiv a^p-1\equiv 0 \pmod{\mathfrak{m}},$$

so $a\equiv 1 \pmod{\mathfrak{m}}$. Put $\psi(x)=1+x+\dots+x^{p-1}$, so $\psi(a)\equiv 0 \pmod{\mathfrak{m}^q}$. Thus $\operatorname{ord}_{\mathfrak{m}}(\psi(a))\ge q>e$. Write $b=a-1$; then $\psi(a)=b^{p-1}+p(1+t)\in p\mathfrak{m}$, where

$t \in \mathfrak{m}$. Thus $b^{p-1} = -p(1+s)$ for some $s \in \mathfrak{m}$. Since $1+s$ is a $(p-1)^{\text{th}}$ power in the completion $\tilde{R}$ of R, this implies that $-p$ is a $(p-1)^{\text{th}}$ power in $\tilde{R}$; thus, the fraction field of $\tilde{R}$ contains the field $\mathbb{Q}_p(\sqrt[p-1]{-p})$, which contains the p^{th} roots of unity. ■

Next we determine precisely which cycle lengths occur over the rings $\mathbb{Z}_p$ of p-adic integers. This has also been done by Pezda [18], using a different method.

Theorem 13. *Suppose $f(x) \in \mathbb{Z}_p[x]$ has a cycle of length m in $\mathbb{Z}_p$. Then $m = k$ or $m = kr$ for some integers k, r such that $1 \leq k \leq p$ and r divides $p-1$; except if $p = 2$ or $p = 3$, in which case $m = kp$ is also a possibility. Conversely, all of the above values of m do occur as lengths of cycles in $\mathbb{Z}_p$ for polynomials in $\mathbb{Z}_p[x]$.*

Proof. By Corollary 4 and Theorem 8, the only possible cycle lengths not mentioned in the above theorem are $m = 12$ and $m = 18$, both for $p = 3$. In particular, these two lengths can occur only if the order of $(f^k)'(x)$ in $(\mathbb{Z}_p/p\mathbb{Z}_p)^*$ is $r = 2$ for any x in the cycle, and in addition there is an extra factor of p. But this cannot occur, since, by the above proposition, the factor of p arises in passing from (mod p) to (mod p^2), so in fact we must have $r = 1$.

As for the existence assertion, it follows from Proposition 10, the existence of cycles of length $p-1$ in $p\mathbb{Z}_p$, and the existence of cycles of length p in $p\mathbb{Z}_p$ for $p = 2$ and $p = 3$. The last fact is the easiest to verify, since we simply mention that $f(x) = -x$ has the cycle $(2, -2)$ in $2\mathbb{Z}_2$, and that $f(x) = (6-x)(x+1)/2$ has the 3-cycle $(0, 3, 6)$ in $3\mathbb{Z}_3$. Finally, the existence of cycles of length $p-1$ in $p\mathbb{Z}_p$ is also quite easy to verify: just let $\alpha \in \mathbb{Z}_p$ be a primitive $(p-1)^{\text{th}}$ root of unity, and note that $f(x) = \alpha x$ has the cycle $(p, p\alpha, p\alpha^2, \ldots, p\alpha^{p-2})$. ■

The final result of this section shows that, if the leading coefficient of the polynomial is a unit in R, then any cycle in the fraction field of R must actually be in R.

Proposition 14. *Let R be an integrally closed domain, with fraction field K. Let $f(x) \in R[x]$ be a polynomial with degree $d \geq 2$ whose leading coefficient is a unit. Then any finite cycle of f in K must actually lie in R.*

Proof. Any element in K which lies in an n-cycle of f is a root of the monic polynomial $f^n(x) - x \in R[x]$, hence is in R. ■

2.2 More results

In this section we prove several results about cycle lengths in quite general rings. Throughout this section R denotes an integral domain. We begin with a trivial but useful lemma.

Lemma 15. *If there is a polynomial in $R[x]$ having an m-cycle in R, then there is a polynomial in $R[x]$ having an m-cycle $(x_1, \ldots, x_m)$ in R with $x_1 = 0$ and $x_2 = 1$.*

Proof. Say $f(x) \in R[x]$ has the cycle $(y_1, \ldots, y_m)$ in R. Then $g(x) = f(x + y_1) - y_1 \in R[x]$ has the cycle $(0, y_2 - y_1, \ldots, y_m - y_1)$ in R; that is, by conjugating by the translation $x \mapsto x + y_1$ we may assume $y_1 = 0$. Let the cycle of g be $(0, z_2, \ldots, z_m)$. Then $h(x) = g(z_2 x)/z_2$ has the cycle $(0, 1, z_3/z_2, \ldots, z_m/z_2)$. Since $g(x)$ is in the ideal (z_2, x) of $R[x]$, if w is any multiple of z_2 then also $g(w)$ is a multiple of z_2; thus, each $z_i = g(z_{i-1})$ is a multiple of z_2, so the above cycle is in R. Since $f(x) = z_2 + \sum_{i=1}^{d} a_i x^i$, $f(z_2 x/z_2) = 1 + \sum_{i=1}^{d} a_i z_2^{i-1} x^i \in R[x]$. This completes the proof. ■

Lemma 16. *If $f(x) \in R[x]$ has a cycle $(x_1, x_2, \ldots, x_m)$ in R, then each $(x_{i+j} - x_i)/(x_{j+1} - x_1)$ is a unit in R.*

Proof. For any positive integer r, $x_k - x_\ell$ divides $f(x_k) - f(x_\ell) = x_{k+1} - x_{\ell+1}$; thus,

$$(x_k - x_\ell) \mid (x_{k+1} - x_{\ell+1}) \mid \cdots \mid (x_k - x_\ell),$$

so the numbers $x_{k+i} - x_{\ell+i}$, for variable i, are all associates. ■

Corollary 17. *If $f(x) \in R[x]$ has a cycle $(x_1, \ldots, x_m)$ in R, then $x_{i+j} - x_i$ divides $x_{i+jr} - x_i$.*

Proof. Since $x_{i+j} - x_i$ divides each of $x_{i+jr} - x_{i+j(r-1)}$, $x_{i+j(r-1)} - x_{i+j(r-2)}$, ... ,$x_{i+j} - x_i$, it also divides their sum $x_{i+jr} - x_i$. ■

Corollary 18. *If $f(x) \in R[x]$ has a cycle $(x_1, \ldots, x_m)$ in R, and j is coprime to m, then each $(x_{i+j} - x_i)/(x_2 - x_1)$ is a unit in R.*

Proof. Let r be a positive integer with $jr \equiv 1 \pmod{m}$; the previous corollary implies that $x_{i+j} - x_i$ divides $x_{i+1} - x_i$. The previous corollary also implies that $x_{i+1} - x_i$ divides $x_{i+j} - x_i$, so $x_{i+j} - x_i$ is an associate of $x_{i+1} - x_i$, which is an associate of $x_2 - x_1$ by Lemma 16. ■

Corollary 19. *If $f(x) \in R[x]$ has a cycle $(x_1, \ldots, x_m)$ in R and m is not squarefree, let q be the product of the distinct prime divisors of m. Then the equation $u + v = (x_{q+1} - x_1)/(x_2 - x_1)$ has at least $\varphi(m)$ solutions in units u, v of R.*

Proof. For each j, $1 \leq j \leq m$, which is coprime to m, also $q - j$ is coprime with m; we have

$$\frac{x_{j+1} - x_1}{x_2 - x_1} + \frac{x_{q+1} - x_{j+1}}{x_2 - x_1} = \frac{x_{q+1} - x_1}{x_2 - x_1},$$

where the previous corollary implies that each of the addends is in R^*. ■

In the next subsection we will explain that there are quite general circumstances under which an equation $u + v = w$ in units u, v of R (with $w \in R$ fixed) can have only finitely many solutions; thus, in such circumstances any sufficiently large cycle length must be squarefree. But in fact squarefree cycle lengths cannot be too large either, as our next result indicates. Here we use the simplest unit equation, namely $u + v = 1$. An *exceptional unit* of a ring is a unit u for which $u - 1$ is also a unit. This terminology is due to Nagell [16].

Corollary 20. *If $f(x) \in R[x]$ has a cycle $(x_1, \ldots, x_m)$ in R, and $j(j-1)$ is coprime to m, then $(x_j - x_1)/(x_2 - x_1)$ is an exceptional unit in R.*

Proof. By Corollary 18, $y = (x_j - x_1)/(x_2 - x_1)$ is a unit. Corollary 18 also implies that $y - 1 = (x_j - x_2)/(x_2 - x_1)$ is a unit. ■

As above, under quite general circumstances, there are only finitely many exceptional units in a given ring R. Thus, if there are too many integers j, with $1 \leq j \leq m$, for which $j(j-1)$ is coprime to m, then there cannot be an m-cycle in R. We now investigate the number of such j.

Define $\psi(m) = \#\{j \in \mathbb{Z}/m\mathbb{Z} : j(j-1) \in (\mathbb{Z}/m\mathbb{Z})^*$. This function is similar to the Euler totient $\varphi(m)$. In particular, it is multiplicative: if a and b are coprime, then in the bijection $\mathbb{Z}/ab \leftrightarrow \mathbb{Z}/a \times \mathbb{Z}/b$ sending j to (j, j), the set of $j \in \mathbb{Z}/m\mathbb{Z}$ for which $j(j-1) \in (\mathbb{Z}/m\mathbb{Z})^*$ maps to the product of the corresponding subsets of $\mathbb{Z}/a\mathbb{Z}$ and $\mathbb{Z}/b\mathbb{Z}$. At the prime power p^i, we have $\psi(p^\alpha) = p^{\alpha-1}(p-2)$. Thus, we have the following formula for $\psi(m)$: if the prime factorization of m is $m = \prod_{i=1}^k p_i^{\alpha_i}$, then $\psi(m) = \prod_{i=1}^k p_i^{\alpha_i - 1}(p-2)$. Note that $\psi(m) = 0$ if and only if m is even. Also, for any positive integer n there are only finitely many m with $\psi(m) = n$; thus, $\psi(m) \to \infty$ as the odd number $m \to \infty$. In particular, if R has only finitely many exceptional units, then there cannot be any long cycles of odd length in R.

2.2.1 Exceptional units and the Lenstra constant

As above, an exceptional unit of a ring is a unit u for which $u - 1$ is also a unit. Exceptional units were originally studied in case R is the ring of integers of an algebraic number field. In that case both Chowla [1] and Nagell [15] proved that R has only finitely many exceptional units. In fact, the set of exceptional units can be effectively determined by Baker's methods [4, Lemme 4]. Furthermore, when R is a ring of S-integers in a number field, there are bounds on the number of exceptional units [2, 3] and on the height of any exceptional unit. Unfortunately, the bound on the height is quite large, thus prohibiting explicit determination of all exceptional units in R by this method. However, de Weger has worked on reducing the bounds. For a few rings classical diophantine techniques have been used to determine the exceptional units. For instance, see the papers of Nagell [16, 17] and Wasén[25]. Various examples of exceptional units are given by Lenstra [6]. Nagell [17] determined the exceptional units in the ring of integers of the real subfield of the seventh cyclotomic field. He also determined all exceptional units in the ring of integers of every number field whose unit group has rank at most one, see [16] for references. He also shows that exceptional units in quartic CM fields are scarce; this was done for general CM fields by Györy [5].

Nagell [15] noted that, when u is an exceptional unit, also $1/u$ and $1-u$ are exceptional units. Lenstra [6] mentioned that, if u, v and u/v are exceptional units, then also $(1-u)/(1-v)$ is an exceptional unit; he also noted that any automorphism of the ring maps the exceptional units of the ring to themselves.

Recently Schlickewei [21] has shown that, in any finitely generated subgroup of $\mathbb{C}^*$, there are only finitely many solutions to the equation $x+y=1$; moreover he gives an explicit bound for the number of solutions, which depends only on the rank of the group. This result applies to unit equations $u+v=w$.

One application of exceptional units is in the determination of the Lenstra constant of a ring. The Lenstra constant of a ring R was defined (but not christened) in [6] to be

$$\begin{aligned} (2.1) \qquad L(R) \;&=\; \sup\{k : \text{ there exist } x_1, \ldots, x_m \in R \text{ such that } x_i - x_j \in R^* \\ &\qquad \text{for all } i, j \text{ for which } 1 \leq i < j \leq m\}. \end{aligned}$$

Lenstra combined an idea of Hurwitz with an argument from the geometry of packings to show that, in the ring of integers R of an algebraic number field, if $L(R)$ is sufficiently large then the usual norm is a Euclidean algorithm on R. Given a sequence $x_1, \ldots, x_m \in R$ as in (2.1), each $(x_i - x_1)/(x_2 - x_1)$ with $3 \leq i \leq m$ is an exceptional unit; thus, to determine the Lenstra constant of a ring one could attempt to list all exceptional units, then check every sequence $0, 1, x_3, \ldots, x_m$ where $x_3, \ldots, x_m$ are exceptional units. Unfortunately, as mentioned above it is not so easy to determine the exceptional units in a general ring, and even once they are known, the determination of the Lenstra constant is still 'hard' (NP-complete).

In practice the Lenstra constant of a ring is determined by giving identical upper and lower bounds for it. Define M to be the smallest norm of a (proper) ideal of R:

$$M(R) = \min\{\#(R/I) : I \subset R \text{ is an ideal}, I \neq R\}.$$

Clearly M is a prime power whenever it is finite.

Lemma 21 (Lenstra). *We have* $2 \leq L \leq M$.

Proof. First, the sequence $(0,1)$ shows that $L \geq 2$. To prove $L \leq M$, let $x_1, \ldots, x_m$ as in (2.1), and let I be a proper ideal of R; since I does not contain any of the units $x_i - x_j$, the elements $x_1, \ldots, x_m$ have distinct images in R/I, so $\#(R/I) \geq m$. ■

When R is the ring of integers of a number field of degree n, the ideal $I = 2R$ yields $M \leq 2^n$; thus, $L \leq 2^n$. It is not known whether there is a better upper bound on L, in terms of n alone; there exist number fields of arbitrarily large degree for which $L > n$, but this is a long ways off. To give a lower bound for the Lenstra constant, it of course suffices to write down a suitable sequence $x_1, \ldots, x_m$.

We now give some examples from [6]. Let R be the valuation ring of the field $K = \mathbb{Q}(\mu_{p^k})$, where μ_m denotes the group of m^{th} roots of unity (and ζ_m is a generator of μ_m). Then $L(R) \leq M(R) = p$, and the sequence $(\zeta_p^i - 1)/(\zeta_p - 1)$ $(1 \leq i \leq p)$ shows that $L(R) \geq p$, so $L(R) = p$. Now let R be the valuation ring of $\mathbb{Q}(\mu_m)$; then $L(R) \geq p$ for any prime divisor p of m; further, $L \geq 1 + m/q$, where q is the largest prime power dividing m, because of the sequence $0, 1, \zeta_m, \zeta_m^2, \ldots, \zeta_m^{(m/q)-1}$. Let R be the valuation ring of $\mathbb{Q}(\zeta_p) \cap \mathbb{R} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, where p is an odd prime; then $m = p$ unless p is a Fermat prime, in which case $M = p - 1$. Moreover, Leutbecher and Niklasch [9] used p-torsion on the unit circle to construct a sequence demonstrating that $L \geq p - 1$ in this case. For $p = 7, 11,$ and 13 it is known that $L = p$ [9, 6, 8, 7]. Various rings of integers of number fields have been shown to be norm-Euclidean by means of Lenstra's method, and in each case a lower bound on the Lenstra constant is computed; see [6, 8, 12, 7, 9].

2.2.2 Connection with cycle lengths

We now apply the results of the previous two subsections to give results about the possible cycle lengths. First, if R is any integral domain of characteristic zero whose unit group is a finitely generated subgroup of $\mathbb{C}^*$, then Schlickewei's result implies, by Corollary 20, that there is no m-cycle in R if $\psi(m)$ exceeds the number of exceptional units plus two. In particular, there is a bound on the odd numbers which occur as cycle lengths. Likewise, there is no m-cycle in R if m is not squarefree and $\phi(m)$ exceeds the number of solutions to any unit equation in R, so there is a bound on the non-squarefree numbers which occur as cycle lengths. Combining these two bounds gives a bound on the possible cycle lengths. When R is a ring of S-integers in a number field, one gets a better bound on m by using Evertse's result [2], which gives a sharper bound on the number of solutions to a unit equation in this case.

We can give an especially good bound on the prime numbers which occur as cycle lengths.

Lemma 22. *If a polynomial over R has a p-cycle in R, where p is prime, then $p \leq L(R)$.*

Proof. This follows at once from Corollary 18. ■

Next we show that this bound is sharp.

Lemma 23. *If $m \leq L(R)$, then there exists a polynomial over R having an m-cycle in R.*

Proof. Since $m \leq L(R)$, there are $x_1, \ldots, x_m \in R$ for which each $x_j - x_i \in R^*$. Let K be the fraction field of R. There is a unique polynomial over K, of degree less than m, which has the cycle $(x_1, \ldots, x_m)$. This is given explicitly by the Lagrange interpolation formula, as

$$f(x) = \sum_{i=1}^{n} \frac{x_{i+1}(x-x_1)(x-x_2)\ldots\widehat{(x-x_i)}\ldots(x-x_m)}{(x_i-x_1)(x_i-x_2)\ldots\widehat{(x_i-x_i)}\ldots(x_i-x_m)}.$$

Since the denominator of each summand is a unit in R, in fact $f(x) \in R[x]$. ■

Corollary 24. *The set of prime numbers which occur as lengths of cycles of polynomials over R is the set of prime numbers $\leq L(R)$.*

Corollary 25. *If there exists a polynomial over R having a p-cycle in R, where p is prime, then for any $m \leq p$ there exists a polynomial over R having an m-cycle in R.*

In fact, for any number m (not just primes), one can write down algebraic conditions which are necessary and sufficient for the existence of a polynomial over R which has an m-cycle in R. This follows from the following general result.

Lemma 26. *Let R be an integral domain. Let $\alpha_1, \dots, \alpha_m$ be distinct elements of R, and let $\beta_1, \dots, \beta_m$ be arbitrary elements of R. Then there exists a polynomial $f(x) \in R[x]$ such that (for each $1 \leq i \leq m$) $f(\alpha_i) = \beta_i$, if and only if, for each $2 \leq k \leq m$,*

$$\prod_{1 \leq i < j \leq k} (\alpha_i - \alpha_j)$$

divides the determinant of the matrix

$$\begin{bmatrix} \beta_1 & \beta_2 & \dots & \beta_k \\ 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_k \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_k^2 \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{k-2} & \alpha_2^{k-2} & \dots & \alpha_k^{k-2} \end{bmatrix}$$

Proof. If there exists such a polynomial $f(x) \in R[x]$, then, by considering the remainder of f upon division by $(x - \alpha_1) \dots (x - \alpha_m)$ we see we may assume f has degree less than m. Let K be the fraction field of R. There is a unique polynomial in $K[x]$ of degree less than m which maps every $\alpha_i \to \beta_i$. Thus, this polynomial has coefficients in R if and only if there is a polynomial over R with the desired property. Say this specific polynomial in $K[x]$ is $\sum_{i=0}^{m-1} a_i x^i$. The condition that each $f(\alpha_i) = \beta_i$ may be stated as

$$\begin{bmatrix} 1 & \alpha_1 & \dots & \alpha_1^{m-1} \\ 1 & \alpha_2 & \dots & \alpha_2^{m-1} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_m & \dots & \alpha_m^{m-1} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{m-1} \end{bmatrix} = \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_m \end{bmatrix}.$$

Note that the square matrix is Vandermonde, and has determinant

$$V_m = \prod_{1 \leq i < j \leq m} (\alpha_j - \alpha_i),$$

which is nonzero. Thus, by Cramer's rule,

$$a_i = \frac{1}{c} \cdot \begin{vmatrix} 1 & \alpha_1 & \dots & \beta_1 & \dots & \alpha_1^{m-1} \\ 1 & \alpha_2 & \dots & \beta_2 & \dots & \alpha_2^{m-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_m & \dots & \beta_m & \dots & \alpha_m^{m-1} \end{vmatrix},$$

where the column of β's replaces the column α^{i-1}. Thus, $f(x) \in R[x]$ if and only if V_m divides each of these determinants.

Now we induct on m. First, if there is some polynomial over R having an m-cycle in R, then each of these determinants is divisible by V_m In particular, the last of these determinants is the one we need. Conversely, suppose that V_m divides each of the determinants, and that there is a polynomial $g(x) \in R[x]$ mapping α_i to β_i for each $i < m$. Again we may assume g has degree less than $m-1$; thus, adding some R-linear combination of lower rows to the first row, we can replace the matrix we have by the same one in which each β_i is replaced by 0 except β_m, which is replaced by $\beta_m - g(\alpha_m)$. The resulting matrix has the same determinant, so this determinant is still divisible by V_m. But this determinant is just the product of $\beta_m - g(\alpha_m)$ with the Vandermonde determinant V_{m-1}; thus, $\prod_{i=1}^{m-1}(\alpha_m - \alpha_i)$ divides $\beta_m - g(\alpha_m)$. Hence

$$h(x) = \frac{\beta_m - g(\alpha_m)}{\prod_{i=1}^{m-1}(\alpha_m - \alpha_i)} \prod_{i=1}^{m-1}(x - x_i) \in R[x],$$

so also $g(x) + h(x) \in R[x]$ and $g + h$ maps α_i to β_i whenever $1 \leq i \leq m$. This completes the proof. ■

In the case of 4-cycles this provides the following nice criterion:

Corollary 27. *Let R be an integral domain. There exists a polynomial in $R[x]$ having a 4-cycle in R, if and only if there exist units $u, v \in R^*$ for which $u+v$ and $u+1$ are associates, and for which $1+u+v \in R^*$.*

We conclude with a result about cycle lengths in rings with just a few units. For a ring R, let $C(R)$ denote the set of lengths of cycles in R; in other words, $C(R)$ is the set of m for which there exists a polynomial in $R[x]$ having an m-cycle in R.

Lemma 28. *Let R be a domain for which $R^* \subseteq \{1, -1\}$.*

- *If char$(R) = 0$ or 2 then $C(R) = \{1, 2\}$.*
- *If char$(R) = 3$ then $C(R) = \{1, 2, 3\}$.*

Note that these are all the cases, since if $p = \mathrm{char}(R) > 0$ then R^* contains ${\mathbb{F}_p}^*$, so $|R^*| \geq p - 1 > 2$ if $p > 3$.

Proof. Let $(x_1, \ldots, x_m)$ be a cycle of f in R. Put $y_i = x_{i+1} - x_i$. By Lemma 16, the y_i's are associates of each other; hence every $y_j = \pm y_1$. The sum of the y_j's is zero; if the y_j's are not all equal, there is a minimal j for which $y_j = -y_1$, but then $x_{j+1} = x_{j-1}$, so $m = 2$. If all the y_i's are the same, then m must equal the characteristic of R. Note that $f(x) = -x$ has the cycles (0) and $(1, -1)$, so the lengths $m = 1$ and $m = 2$ always occur. Finally, $f(x) = x + 1$ has the cycle $(0, 1, 2)$. This completes the proof. ■

This result applies, for instance, to $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{Z}$, $\mathbb{Z}[\sqrt{-5}]$, and polynomial rings over these rings. Note that $L(R)$ is at most two more than the number of exceptional units of R, so certainly if R^* is finite then there is a bound on the prime numbers occurring as cycle lengths.

2.3 Bounding the p-power in the cycle length

In this section we prove the following result.

Theorem 8. *Let R be a discrete valuation ring of characteristic zero. Let $h(x) \in R[x]$ have a cycle $(x_1, \ldots, x_m)$ in $\mathfrak{m}$, and suppose that $h'(x_1) \equiv 1 \pmod{\mathfrak{m}}$. Then $m = p^n$, where the integer n satisfies*

$$0 \leq n \leq 1 + \frac{\log(2e) - \log(p-1)}{\log p};$$

if $p = 2$ we have the stronger inequality $n \leq 1 + (\log e)/\log 2$.

Everything besides the bound on n follows from Proposition 1; further, by conjugating by the translation $L(x) = x - x_1$, we may assume our cycle contains 0. Henceforth we will make this assumption. In the first subsection we state some preliminary lemmas; in Section 2.3.2 we complete the proof of this theorem, by proving Theorem 33; in the next subsection we discuss how close our bound on n is to being optimal, and mention various other results which follow from (slight modifications of) our arguments; and in Section 2.3.4 we finally prove the preliminary lemmas.

There is one special piece of notation which we use in this section, but not in the rest of this thesis. Namely, here we denote the k^{th} iterate of a function f by $f^{\circ k}$, rather than just f^k.

Finally, we mention that our proof holds in somewhat greater generality—one need only assume that R is a ring, $\mathfrak{m}$ is an ideal of R which contains every zero-divisor in R, the additive order of 1 in $R/\mathfrak{m}$ is a prime number p, there is some $i > 0$ for which $p \notin \mathfrak{m}^i$, the only number $f^{p^j}(0)$ lying in every $\mathfrak{m}^i$ is 0 itself, and: for e satisfying $p \in \mathfrak{m}^e$ but $p \notin \mathfrak{m}^{e+1}$, and for each ℓ such that $2e/(p-1) < p^\ell$, if $f^{p^\ell}(0) \notin \mathfrak{m}^j$ then $p \cdot f^{p^\ell}(0) \notin \mathfrak{m}^{e+j}$.

2.3.1 Some combinatorial lemmas

Let $f(x) = x + \sum_{i=0}^{d} b_i x^i \in \mathbb{Z}[b_0, b_1, \dots, b_d][x]$ be a generic polynomial of degree d; let $f^{\circ p}$ be the p^{th} iterate of f. The coefficient of x^β in $f^{\circ p}(x) - x$ is a polynomial in $b_0, b_1, \dots, b_d$; thus, it is a sum of terms $c \cdot \prod_{i=0}^{d} b_i^{\alpha_i}$, where $\alpha_0, \alpha_1, \dots, \alpha_d \geq 0$ and c is a nonzero integer. It is convenient to put $\alpha_i = 0$ for $i > d$.

Lemma 29. *We have*

(1) $\sum_{i=0}^{d} (i-1)\alpha_i = \beta - 1$

(2) If $\beta \leq p - 1$*, then* $\alpha_0 + \sum_{i=2}^{p-1} \alpha_i \geq 1$ *except for the monomials* $\binom{p}{\ell} b_1^\ell x$ *(for* $1 \leq \ell \leq p$*).*

(3) If $\beta = 0$*, then* $\alpha_0 \geq 1$*; in fact,* $\alpha_0 \geq 2$ *except for the monomials* $\binom{p}{\ell+1} b_0 b_1^\ell$ *(for* $0 \leq \ell \leq p-1$*).*

(4) If $\beta = 1$, then $\alpha_0 + \alpha_1 \geq 1$.

Now assume p is prime, and let $g(x) \in \mathbb{F}_p[b_0, b_1, \ldots, b_d][x]$ be the reduction of $f^{\circ p}$ modulo p. Then the coefficient of x^β in $g(x) - x$ is a sum of terms $c \cdot \prod_{i=0}^d b_i^{\alpha_i}$, where $\alpha_0, \alpha_1, \ldots, \alpha_d \geq 0$ and $c \in \mathbb{F}_p$ is nonzero. Then the results of the previous lemma apply to g; moreover, we have the following result for g.

Lemma 30. *For $0 \leq \beta \leq p-1$,*

(1) $\sum_{i=0}^{p-1} \alpha_i \geq p$

(2) $2\alpha_0 + \alpha_1 \geq p - 1$.

We postpone the proofs of these lemmas until Section 2.3.4.

2.3.2 The main result

Let R be a discrete valuation ring having characteristic zero, residue characteristic $p > 0$, and ramification index $e < \infty$. Let $f(x) \in R[x]$ be a polynomial such that $f(0)$ and $f'(0) - 1$ are in $\mathfrak{m}$, and such that 0 is in a finite cycle of f. Then the length of this cycle is a power of p, say p^n; we will give a bound for n.

Let c_i^k be the coefficient of x^i in the polynomial $f^{\circ p^k} - x$, and let $C_i^k = \operatorname{ord}_{\mathfrak{m}}(c_i^k)$. We know that $C_0^0, C_1^0 \geq 1$, and every C_i^k is a nonnegative integer. We will use the lemmas of the previous section to show that, for each k, the C_i^k must be reasonably large; but we will then show that, once the C_i^k are large enough (for some k), we must in fact have $C_0^k = \infty$, whence $c_0^k = 0$ and $n \leq k$. The lemmas of the previous section are applicable because $f^{\circ p^{k+1}}$ is the p^{th} iterate of $f^{\circ p^k}$; thus, c_j^{k+1} is a sum of terms $c \cdot \prod_{i=0}^d (c_i^k)^{\alpha_i}$, where $\alpha_0, \ldots, \alpha_d \geq 0$ and c is a nonzero integer. Note that $\operatorname{ord}_{\mathfrak{m}}$ of such a term is given by $\operatorname{ord}_{\mathfrak{m}}(c) + \sum_{i=0}^d \alpha_i C_i^k$. We consider separately the terms for which $p \nmid c$ and the terms for which $p \mid c$. For terms of the first type we know the α_i must satisfy the criteria of both lemmas from the previous section; thus, for any such term $\operatorname{ord}_{\mathfrak{m}}$ is at least as big as

$$D_j^{k+1} = \min \left\{ \sum_{i=0}^{p-1} \alpha_i C_i^k : \sum_{i=0}^{p-1} \alpha_i \geq p,\ 2\alpha_0 + \alpha_1 \geq p - 1,\ \sum_{i=0}^{p-1} (i-1)\alpha_i \leq j - 1 \right\}.$$

For terms with $p \mid c$ we know the α_i must satisfy Lemma 29, so any such term has $\operatorname{ord}_{\mathfrak{m}} \geq E_j^{k+1}$, where E_j^{k+1} is defined as follows: for $j \geq 2$, put

$$E_j^{k+1} = \min\left\{e + C_\ell^k : 0 \leq \ell \leq p-1,\ \ell \neq 1\right\};$$

and for $j < 2$ put $E_0^{k+1} = e + C_0^k$ and $E_1^{k+1} = \min\{e + C_0^k,\ e + C_1^k\}$. In summary,

$$C_j^{k+1} \geq \min\left\{D_j^{k+1},\ E_j^{k+1}\right\}.$$

Proposition 31. *If $p > 2$, then for every nonnegative integer k such that $2e/(p-1) \geq p^{k-1}$, we have $C_0^k, C_1^k \geq (p^k+1)/2$ and $C_2^k, \ldots, C_{p-1}^k \geq (p^k-1)/2$.*

Proof. The proof is a straightforward induction on k. The result is clear for $k = 0$. Assuming the bounds hold for k, we have $D_j^{k+1} \geq \sum_{i=0}^{p-1} \alpha_i C_i^k$; by (2) of Lemma 30, $\alpha_0 + \alpha_1 \geq (p-1)/2$, so, also applying (1) of Lemma 30, we have

$$D_j^{k+1} \geq p \cdot \frac{p^k - 1}{2} + \frac{p-1}{2} = \frac{p^{k+1}-1}{2}.$$

Next, from $\sum_{i=0}^{p-1}(i-1)\alpha_i \leq j-1$, we have

$$\alpha_0 \geq 1 - j + \sum_{i=2}^{p-1}(i-1)\alpha_i \geq 1 - j + \sum_{i=2}^{p-1}\alpha_i \geq 1 - j + p - \alpha_0 - \alpha_1,$$

so $2\alpha_0 + \alpha_1 \geq p + 1 - j$. Thus, for $j \leq 1$, we have $\alpha_0 + \alpha_1 \geq (p+1)/2$, so the same argument as above gives $D_j^{k+1} \geq (p^{k+1}+1)/2$. Now we make use of the inductive hypothesis (for $k+1$), namely that $2e/(p-1) \geq p^k$, or equivalently $e \geq (p^{k+1} - p^k)/2$. We have $E_j^{k+1} \geq e + (p^k - 1)/2 \geq (p^{k+1}-1)/2$; and for $j \leq 1$, the same steps give $E_j^{k+1} \geq (p^{k+1}+1)/2$. ■

We have now shown that the C_i^k are large when k is large; in our next result we will show that $C_0^k = \infty$ whenever the C_i^k are sufficiently large. To show this we need the following observation: if $D_0^{k+1} > e + C_0^k$ and C_0^k, $C_1^k > 0$, then $C_0^{k+1} = e + C_0^k$; this follows from (3) of Lemma 29, which implies that c_0^{k+1} is a sum of terms which are all in $\mathfrak{m}^{1+e+C_0^k}$ except for the single term pc_0^k.

Proposition 32. *If $p > 2$ and $2e/(p-1) < p^k$ and we have (for some $w \geq 0$) $C_0^w, C_1^w \geq (p^k+1)/2$ and $C_2^w, \ldots, C_{p-1}^w \geq (p^k-1)/2$, then $C_0^{w+1} = e + C_0^w$ and $C_1^{w+1} \geq (p^k+1)/2$ and $C_2^{w+1}, \ldots, C_{p-1}^{w+1} \geq (p^k-1)/2$; thus, $C_0^{w+r} = er + C_0^w$.*

Proof. This follows in an elementary manner from the above observation and the lemmas of the previous section. ■

Theorem 33. *For p odd, we have the bound $n \leq 1 + \dfrac{\log(2e) - \log(p-1)}{\log p}$.*

Proof. Let ℓ be the least integer such that $2e/(p-1) < p^\ell$; by Proposition 31 we have $C_0^\ell, C_1^\ell \geq (p^\ell + 1)/2$ and $C_2^\ell, \ldots, C_{p-1}^\ell \geq (p^\ell - 1)/2$. By Proposition 32 we have $C_0^{\ell+r} = er + C_0^\ell$. Since 0 is in a cycle of f of length p^n, for any $m \geq n$ we have $c_0^m = f^{\circ p^m}(0) = 0$, so $C_0^m = \infty$; thus $C_0^\ell = \infty$, so $n \leq \ell$. But

$$\ell = 1 + \left\lfloor \frac{\log(2e) - \log(p-1)}{\log p} \right\rfloor,$$

so the proof is complete. ■

For $p = 2$, the above arguments must be modified slightly, and when this is done they yield the bound $n - 1 \leq \log e / \log 2$.

2.3.3 Improving the main result

The bound in Theorem 8 is nearly best possible, in light of Example 11. That example demonstrates that for every odd p there are infinitely many fields K for which the bound in Theorem 8 is achieved; and for $p = 2$, there are infinitely many fields K for which a number one less than the bound is achieved. In this subsection we discuss how one can improve the bound in Theorem 8 under certain additional hypotheses. Throughout this section R denotes a discrete valuation ring.

Hua-Chieh Li [10] used rather different methods to prove the following result.

Theorem 34 (Li). *If $f(x) \in R[[x]]$ satisfies*

(1) $f(0) \in \mathfrak{m}$ and $f'(0) \equiv 1 \pmod{\mathfrak{m}}$;

(2) for each $r > 0$, we have $f^{\circ r}(x) \neq x$; and

(3) f has a fixed point in $\mathfrak{m}$,

and 0 *is in a finite cycle of* f *of length* p^n*, then*

$$n \leq 1 + \frac{\log e - \log{(p-1)}}{\log p}.$$

However, without the fixed point hypothesis this bound on n is not generally true.

Example 35. The polynomial $f(x) = 3 + (5x - x^2)/2 \in \mathbb{Z}_3[x]$ has the 3-cycle $(0, 3, 6)$ in $3\mathbb{Z}_3$. Here

$$1 + \frac{\log e - \log{(p-1)}}{\log p} = 1 - \frac{\log 2}{\log 3} < 1 = n.$$

The argument we used to prove Theorem 33 gives more information about n when we know more about certain of the C_i^k. For instance, we now prove a result which implies Li's result.

Theorem 36. *Under the hypotheses of Theorem 8, if the cycle lies in* $\mathfrak{m}^2$ *then*

$$n \leq 1 + \frac{\log e - \log{(p-1)}}{\log p}.$$

It is easy to see that this result implies Theorem 34 (at least for polynomials; but the same proof works for power series, as will be explained in Section 2.4). To see the implication for polynomials, note that, if $a \in \mathfrak{m}$ is a fixed point of f, then a is a root of $f(x) - x = \sum_{i=0}^{\infty} c_i x^i$; but $\mathrm{ord}_{\mathfrak{m}}(c_1 a) > \mathrm{ord}_{\mathfrak{m}}(c_1) \geq 1$ and, for $i \geq 2$, $\mathrm{ord}_{\mathfrak{m}}(c_i a^i) \geq i \cdot \mathrm{ord}_{\mathfrak{m}}(a) \geq i \geq 2$, so the nonarchimedean nature of K implies that $\mathrm{ord}_{\mathfrak{m}}(c_0) \geq 2$. The same argument shows that the power series analogue of Theorem 36 implies Theorem 34.

The proof of Theorem 36 is completely analogous to the proof of Theorem 33, and we will not give the details. We only mention the versions one needs of Propositions 31 and 32. The version of Proposition 31 is: for every $k \geq 0$ such that $e/(p-1) \geq p^{k-1}$, we have $C_0^k \geq p^k + 1$, $C_1^k \geq p^k$, and $C_2^k, \ldots, C_{p-1}^k \geq p^k - 1$. And the version of Proposition 32 is: if $e/(p-1) < p^k$, $C_0^w \geq p^k + 1$, $C_1^w \geq p^k$, and $C_2^w, \ldots, C_{p-1}^w \geq p^k - 1$, then $C_0^{w+r} = er + C_0^w$. The proofs of these two results are similar to those of Propositions 31 and 32, and Theorem 36 follows from these results just as Theorem 33 follows from Propositions 31 and 32.

We mention one more result, about the nonexistence of cycles satisfying certain conditions.

Theorem 37. *Given $f(x) \in R[x]$ satisfying $f(0) \in \mathfrak{m}$. Suppose that $p \geq 5$ and 0 is in a cycle of length m (a power of p); if $r = \operatorname{ord}_{\mathfrak{m}}(f(0))$ satisfies $r \geq e$, and $p-1 \nmid e$, then $m = 1$.*

Proof. Suppose to the contrary that $m = p^n$, where $n \geq 1$. Write $g(x) = f^{p^{n-1}}(x)$ as $x + \sum_{i \geq 0} a_i x^i$, and put $A_i = \operatorname{ord}_{\mathfrak{m}}(a_i)$; thus, $a_i = c_i^{n-1}$ and $A_i = C_i^{n-1}$. Since $\#(R/\mathfrak{m})^*$ is coprime to p, Corollary 4 implies that $f'(0) \equiv 1 \pmod{\mathfrak{m}}$. Now, note that $A_0 \geq C_0^0 = r \geq e$ (by (3) of Lemma 29) and that $A_1 \geq 1$ (by (4) of Lemma 29). Also, since $f^{p^{n-1}}(0) \neq 0$, we have $A_0 < \infty$.

Now, $0 = g^p(0)$ is a sum of many terms, most of which are in $\mathfrak{m}^{e+A_0+1}$. Precisely, if the term is divisible by p, then (3) of Lemma 29 implies, since $A_0, A_1 > 0$, that the term is in $\mathfrak{m}^{e+A_0+1}$ unless the term is pa_0. Further, except for the term $a_0 a_1^{p-1}$, every term which is not divisible by p has $\alpha_0 \geq 2$. If $\alpha_0 \geq 3$ or $\alpha_1 \geq 1$, then the term is in $\mathfrak{m}^{e+A_0+1}$; the only remaining possibility is if $\alpha_0 = 2$ and $\alpha_1 = 0$. By (1) of Lemma 29, we must have $\alpha_2 = 1$ and $\alpha_i = 0$ for $i > 2$, which contradicts (1) of Lemma 30. Thus, all terms involved in $0 = g^p(0)$ are in $\mathfrak{m}^{e+A_0+1}$, except possibly the terms pa_0 and $a_0 a_1^{p-1}$. Since $p-1 \nmid e$, these two terms have different valuations; since $\operatorname{ord}_{\mathfrak{m}}(pa_0) = e + A_0 < e + A_0 + 1$, this implies that the sum of all these terms is not in $\mathfrak{m}^{e+A_0+1}$, which is absurd, since the sum is 0. ■

Corollary 38. *If $p \geq 5$ and $p-1 \nmid e$, then there is no polynomial $f(x) \in R[x]$ having a cycle in pR of length p^n with $n > 0$.*

For, if there were such a cycle, we could conjugate by $x - a$ (for any element a of the cycle), after which we could apply the above result.

2.3.4 Proofs of the combinatorial lemmas

In this section we prove the two lemmas of Section 2.3.1. We begin with the second lemma, which is more interesting. Our proofs make use of the following trivial result:

Lemma 39. *Given $f(x) = x + \sum_{i=0}^{d} b_i x^i \in \mathbb{Z}[b_0, b_1, \ldots, b_d][x]$. For any $k \geq 0$, any term $cx^{\beta} \prod_{i=0}^{d} b_i^{\alpha_i}$ in $f^{\circ k}(x) - x$ in which $\sum_{i \geq p} \alpha_i > 0$, $\beta \leq p-1$, and $\alpha_0 \leq p-1$, must have c divisible by p.*

Proof. The result is clear for $k = 0$; now induct on k. Each relevant term of $f^{\circ k} = f(f^{\circ(k-1)})$ arises from some monomials of $f^{\circ(k-1)}$ by using some (nonconstant) term of f, namely either $b_s x^s$ for some $s \geq 2$ or $(1 + b_1)x$. In either case, each of our inductive hypotheses applies to the involved monomials of $f^{\circ(k-1)}$, except for the hypothesis that $\sum_{i \geq p} \alpha_i > 0$; let us refer to this last hypothesis as Hypothesis S. If we use the term $(1 + b_1)x$, or a term $b_s x^s$ with $s < p$, then one of these involved monomials must satisfy Hypothesis S, and consequently must vanish modulo p, so also does the resulting term of $f^{\circ k}$. If we use a term $b_s x^s$ with $s \geq p$, then the resulting term of $f^{\circ k}$ is divisible by a multinomial coefficient $\binom{s}{*,\ldots,*}$; any such coefficient vanishes (mod p) unless one of the $*$'s is at least p, in which case our term is divisible by the p^{th} power of some monomial in $f^{\circ(k-1)}$. But any such monomial is divisible by either b_0 or x, so either $\alpha_0 \geq p$ or $\beta \geq p$, a contradiction. This completes the proof. ■

Now we give the proofs for the two parts of Lemma 30. We will use the following notation: $g(x) \in \mathbb{F}_p[b_0, b_1, \ldots, b_d][x]$ is the reduction of $f^{\circ p}$ modulo p. Then the coefficient of x^{β} in $g(x) - x$ is a sum of terms $c \cdot \prod_{i=0}^{d} b_i^{\alpha_i}$, where $\alpha_0, \alpha_1, \ldots, \alpha_d \geq 0$ and $c \in \mathbb{F}_p$ is nonzero. It is convenient to set $\alpha_i = 0$ for $i > d$.

Lemma 40. *For $0 \leq \beta \leq p-1$, we have $\sum_{i=0}^{p-1} \alpha_i \geq p$.*

Proof. By Lemma 39, we only need to consider monomials in which $\sum_{i \geq p} \alpha_i = 0$. In the ring $S = \mathbb{F}_p[b_0, b_1, \ldots, b_{p-1}]$, let $\mathfrak{m}$ be the ideal $(b_0, b_1, \ldots, b_{p-1})$, and let R be the ring $S/\mathfrak{m}^p$. Let $A = R[x]/(x^p)$. Then A contains the element $y = x + \sum_{i=0}^{p-1} b_i x^i$, and (in A) we have $y^p = 0$. Define an R-module homomorphism $\sigma : A \to A$ by $\sigma : x \mapsto y$. Since A is a free R-module of rank p, we may view σ as a matrix over R, i.e. $\sigma \in M_{p \times p}(R)$ (here we choose the basis $\{1, x, x^2, \ldots, x^{p-1}\}$ for A). Write $\sigma = 1 + \epsilon$, where 1 denotes the identity matrix and $\epsilon \in M_{p \times p}(R)$. Since $y - x \in \mathfrak{m}[x]$, we have $\epsilon \in M_{p \times p}(\mathfrak{m})$. Thus, $\sigma^p - 1 = \epsilon^p \in M_{p \times p}(\mathfrak{m}^p)$, which is what we are trying to prove. ■

Lemma 41. *For $0 \leq \beta \leq p-1$ and p odd, we have $2\alpha_0 + \alpha_1 \geq p-1$.*

Proof. (due to Lenstra) Here we let $R = \mathbb{F}_p[b_0, b_1, \dots, b_d]/\mathfrak{m}^{(p-1)/2}$, where $\mathfrak{m} = (b_0, b_1^2)$. Let $\sigma : R[x] \to R[x]$ be the R-algebra homomorphism defined by $\sigma : x \mapsto x + \sum_{i=0}^{d} b_i x^i$. Then $\sigma^p(x) = x + \sum_{i\geq 0} c_i x^i$, where the $c_i \in R$ are almost all zero. The lemma is equivalent to the assertion that $c_i = 0$ for $0 \leq i \leq p-1$. Now, since $b_0^p = 0$, we have

$$\sigma(x^p) = (x + \sum b_i x^i)^p = x^p + b_0^p + \sum_{i\geq 1} b_i^p x^{ip} \in (x^p),$$

so σ induces a map $\tilde{\sigma} : R[x]/(x^p) \to R[x]/(x^p)$. The lemma is equivalent to the assertion that $\tilde{\sigma}^p$ is the identity.

Consider the homomorphism $\mathbb{F}_p[b_0, b_1] \to \mathbb{F}_p[u, b_1]/(b_1^{p-1})$ defined by $b_0 \mapsto ub_1^2$ and $b_1 \mapsto b_1$; its kernel is $(b_0, b_1^2)^{(p-1)/2}$. Thus,

$$R = \left(\mathbb{F}_p[b_0, b_1]/(b_0, b_1^2)^{(p-1)/2}\right)[b_2, b_3, \dots, b_d] \hookrightarrow R' = \left(\mathbb{F}_p[u, b_1]/(b_1^{p-1})\right)[b_2, b_3, \dots, b_d].$$

Next, since b_2 is not a zero divisor in R', we may adjoin b_2^{-1} to R', to make $S = R'[b_2^{-1}]$. As above, we have a map $\sigma : S[x] \to S[x]$ which induces $\tilde{\sigma} : S[x]/(x^p) \to S[x]/(x^p)$, and it suffices to show that $\tilde{\sigma}^p$ is the identity.

Consider the polynomial $g(T) = b_0 + b_1 T + \cdots + b_{p-1}T^{p-1} \in S[T]$. Since b_1 is nilpotent, $b_0 = ub_1^2$, and b_2 is a unit, we conclude from the theory of Newton polygons that there is a factor $b_0' + b_1'T + T^2$ of g in $S[T]$ for which $b_0' \in (b_1^2)$ and $b_1' \in (b_1)$. Say $b_0' = b_1^2 c_0$ and $b_1' = b_1 c_1$; since $T^2 + c_1 T + c_0$ is monic, we may adjoin to S a root γ of this polynomial, to get $S' = S[\gamma]$. Then $\delta = b_1\gamma$ is a root of $b_0' + b_1'T + T^2$, and hence of g. Now put $y = x - \delta$, so $y^p = x^p - b_1^p\gamma^p = 0$. Then $S'[x^p]/(x^p)$ has an S'-basis $1, y, \dots, y^{p-1}$. We have

$$\begin{aligned} \sigma y = \sigma x - \delta &= y + \sum_{i=0}^{p-1} b_i (y+\delta)^i \\ &= \sum_{i=0}^{p-1} b_i\delta^i + y \cdot (1 + \sum_{i=1}^{p-1} i b_i \delta^{i-1}) + y^2 \cdot (\dots) \\ &= y \cdot (1+\epsilon) + y^2 \cdot (\dots), \end{aligned}$$

where we have used the fact that $g(\delta) = 0$ and we define $\epsilon = \sum_{i=1}^{p-1} i b_i \delta^{i-1} \in S'$. Thus, $\tilde{\sigma}$ acts on our S'-basis as a triangular matrix with diagonal entries $1, (1+\epsilon), (1+$

$\epsilon)^2, \ldots, (1+\epsilon)^{p-1}$. Since $\epsilon \in (b_1, \delta) = (b_1)$, we know $\epsilon^{p-1} = 0$. Now, in the ring $\mathbb{F}_p[v]$, we have

$$\sum_{i=0}^{p-1} (1+v)^i = \frac{(1+v)^p - 1}{v} = v^{p-1},$$

so, upon substituting $v = \epsilon$, we find that $\sum_{i=0}^{p-1}(1+\epsilon)^i = 0$. Thus, we have a ring homomorphism $Z = \mathbb{Z}[c]/(1 + c + \cdots + c^{p-1}) \to S'$ defined by $c \mapsto 1 + \epsilon$. Since $Z \cong \mathbb{Z}[e^{2\pi i/p}]$ by the map $c \mapsto e^{2\pi i/p}$, in $Z[z]$ we have $\prod_{i=0}^{p-1}(z - c^i) = z^p - 1$. Hence, in $S'[z]$ we have $\prod_{i=0}^{p-1}(z - (1+\epsilon)^i) = z^p - 1$, so the characteristic polynomial of the matrix corresponding to $\tilde{\sigma}$ is just $z^p - 1$, whence (by the Cayley-Hamilton theorem) $\tilde{\sigma}^p$ is the identity. This completes the proof. ∎

Finally, we prove a result of which Lemma 29 is a special case.

Lemma 42. *Let $f(x) = x + \sum_{i=0}^{d} b_i x^i \in \mathbb{Z}[b_0, b_1, \ldots, b_d][x]$ be a generic polynomial; let $f^{\circ k}(x)$ be the k^{th} iterate of f, for $k \geq 0$. The coefficient of x^β in $f^{\circ k}(x) - x$ is a polynomial in $b_0, b_1, \ldots, b_d$; thus, it is a sum of terms $c \cdot \prod_{i=0}^{d} b_i^{\alpha_i}$, where $\alpha_0, \alpha_1, \ldots, \alpha_d \geq 0$ and c is a nonzero integer. Then*

(1) $\sum_{i=0}^{d}(i-1)\alpha_i = \beta - 1$

(2) If $\beta \leq k-1$, then $\alpha_0 + \sum_{i=2}^{k-1} \alpha_i \geq 1$ except for the monomials $\binom{k}{\ell} b_1^\ell x$ (for $1 \leq \ell \leq k$).

(3) If $\beta = 0$, then $\alpha_0 \geq 1$; in fact, $\alpha_0 \geq 2$ except for the monomials $\binom{k}{\ell+1} b_0 b_1^\ell$ (for $0 \leq \ell \leq k-1$).

(4) If $\beta = 1$, then $\alpha_0 + \alpha_1 \geq 1$.

Proof. For any sequence $\alpha = (\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_d)$ of nonnegative integers, let $S(\alpha) = \alpha_0 + 2\sum_{r=2}^{d} \alpha_r$. We associate to α the monomial $b_0^{\alpha_0} \ldots b_d^{\alpha_d}$. Then the only nonzero monomials in $f^{\circ k}(x) - x$ having $S = 0$ are those arising from

$$(1 + b_1)^k x - x = \sum_{\ell=1}^{k} \binom{k}{\ell} b_1^\ell x;$$

for all other monomials we have $S \geq 1$. We now show that much of the lemma follows from part (1). If $\alpha_0 = \alpha_2 = \alpha_3 = \cdots = \alpha_{k-1} = 0$ and $S \geq 1$, then by (1) we have

$$\beta - 1 = \sum_{i=0}^{d}(i-1)\alpha_i = \sum_{i=k}^{d}(k-1)\alpha_i \geq k-1,$$

so $\beta \geq k$; thus, (2) follows from (1). Similarly, the first part of (3) follows from (1), and (4) follows from (1). So we have only to prove (1) and the second part of (3).

We prove each of these assertions by induction on S. They are both true for $S = 0$. For $S = 1$ the only term is

$$\begin{aligned} b_0 \sum_{\ell=0}^{k-1}(1+b_1)^{k-1-\ell} &= \sum_{\ell=0}^{k-1}(a+b_1)^{\ell} \\ &= b_0 \sum_{\ell=0}^{k-1}\sum_{r=0}^{\ell}\binom{\ell}{r} b_1^r \\ &= b_0 \sum_{r=0}^{k-1} b_1^r \sum_{\ell=r}^{k-1}\binom{\ell}{r} \\ &= b_0 \sum_{r=0}^{k-1}\binom{k}{r+1} b_1^r, \end{aligned}$$

for which the assertions hold. For $S > 1$, both statements are vacuously true for $k = 0$; now induct on k. Each term of $f^{\circ k} = f(f^{\circ(k-1)})$ arises from some monomials of $f^{\circ(k-1)}$ by using some (nonconstant) term of f, namely either $b_s x^s$ for some $s \geq 2$ or $(1+b_1)x$ (the term b_0 is irrelevant, since $S > 1$). In either case, our inductive hypotheses apply to the involved monomials of $f^{\circ(k-1)}$, since their S values are no larger than the present S. For $b_s x^s$ we have

$$\begin{aligned} \sum(i-1)\alpha_i &= (s-1) + \sum_{\substack{\text{involved}\\ \text{monomials}}} \sum(i-1)\alpha_i \\ &= (s-1) + \sum_{\substack{\text{involved}\\ \text{monomials}}} (\text{degree} - 1) \\ &= (s-1) + (\beta - s) = \beta - 1. \end{aligned}$$

And if $\beta = 0$, every involved monomial has $\alpha_0 \geq 1$, so we have $\alpha_0 \geq s \geq 2$. Next for $(1+b_1)x$, there is a unique involved monomial of $f^{\circ(k-1)}$, which has the same value of S, so each of our assertions follows from the corresponding assertion for this monomial. This completes the proof. ■

2.4 Power series over complete local rings

We will now show that the results above for polynomials over a local ring remain true for power series over a complete (Noetherian) local ring. The above arguments basically work for power series as well as polynomials, but one must use extreme care when composing power series to make sure that the formal composite of two power series is actually the same function as the composition of the two functions involved.

The possible difficulties are illustrated by the following example, which I learned from Lenstra.

Example. Let R be a complete valuation ring. Put $f(x) = x^2 - x$ and let $g(x) \in R[[x]]$ be the formal inverse (under composition) of $f(x)$. Thus, $g \circ f(x) = x$ as formal power series. But

$$(g \circ f)(1) = 1 \neq 0 = g(0) = g(f(1)).$$

Here one can successively solve for the coefficients of g from the relation $g(x^2 - x) = x$; alternatively, one can write down an explicit formula for them involving binomial coefficients, if one uses the relation $g(x)^2 - g(x) = x$. Finally, g will always have positive radius of convergence.

To deal with the composition of power series, we cite the following result from [20, page 120].

Fact. *Let K be a complete nonarchimedean field, and let $f(x) = \sum a_n x^n$ and $g(x) = \sum b_n x^n$ be formal power series over K. Suppose that $\sum b_n y^n$ converges for a specific $y \in K$. Put $\tau = \max_{n \geq 0} |b_n||y|^n$, and assume $\lim_{n\to\infty} |a_n|\tau^n = 0$. Define $c_m = \sum_{n=0}^{\infty} a_n b_m^{(n)}$, where $b_m^{(n)} = \sum_{j_1+\cdots+j_n=m} b_{j_1} \ldots b_{j_n}$ and $b_0^{(0)} = 1$. Then $h(x) = \sum_{m=0}^{\infty} c_m x^m$ (the formal composition of f and g) converges at y, and satisfies*

$$h(y) = f(g(y)).$$

Using this fact, one can indeed verify that the arguments for polynomials also apply to power series; there are a few extra points which must be checked. The setup is as follows: $f(x) \in R[[x]]$ has a cycle $(x_1, \ldots, x_n)$ in R, where R is a complete

Noetherian local ring with maximal ideal $\mathfrak{m}$ and residue characteristic p. Now, first we must verify that f defines a mapping $\mathfrak{m}/\mathfrak{m}^j \to \mathfrak{m}/\mathfrak{m}^j$ for any positive integer j (or even, if f converges on all of R, a mapping $R/\mathfrak{m}^j \to R/\mathfrak{m}^j$). And next we must verify that the *formal* iterates of the power series f define the same function as the iterates of the function f. Other than these two points, there is no trouble in replacing the word 'polynomial' by the phrase 'power series' in the results and proofs of section 2.1, with the sole exception of Proposition 14 whose proof depends crucially on the fact that f is a polynomial. For the proof of Theorem 8, and the proofs of the other results of section 2.3, observe the following: given any $f(x) = x + \sum_{i=0}^{\infty} b_i x^i \in R[[x]]$, the coefficient of x^β in $f^p(x) - x$ is a sum of terms $c \cdot \prod_{i=0}^{\infty} b_i^{\alpha_i}$, where $c \neq 0$ and the α_i are nonnegative integers almost all of which are zero. If $\alpha_i = 0$ for $i > d$, then this term also occurs in the coefficient of x^β in $g^p(x) - x$, where $g(x) = x + \sum_{i=0}^{d} b_i x^i$; since g is a polynomial, Lemmas 29 and 30 apply. Thus, the results of these two lemmas apply to power series as well as to polynomials; since all the arguments of Sections 2.3.2 and 2.3.3 rely only on these lemmas, all the results of those sections are valid for power series as well as for polynomials.

We now verify the two technical points mentioned above.

Claim. *Let $D \subseteq R$ be the domain of convergence of f, so either $D = \mathfrak{m}$ or $D = R$. Then f defines a mapping $D/\mathfrak{m}^j \to D/\mathfrak{m}^j$, for any $j \geq 1$, and also f defines a mapping $D \to D$.*

Proof. First note that if $D = \mathfrak{m}$, then $f(0) \in \mathfrak{m}$, for otherwise f would map any element of $\mathfrak{m}$ outside $\mathfrak{m}$, so f could not have a cycle. Now, say $f(x) = \sum_{i=0}^{\infty} f_i x^i$; then $f : D \to D$, and for any j there is some r such that $f(y) \equiv \sum_{i=0}^{r} f_i y^i \pmod{\mathfrak{m}^j}$ for all $y \in D$. Thus, for any j, since the polynomial $\sum_{i=0}^{r} f_i x_i$ defines a mapping $D/\mathfrak{m}^j \to D/\mathfrak{m}^j$, also f defines a mapping $D/\mathfrak{m}^j \to D/\mathfrak{m}^j$. ■

Claim. *Let D be the domain of convergence of f. For any positive integer j, the j^{th} formal iterate of f and the j^{th} iterate of the function $f : D \to D$ agree as functions on D.*

Proof. This follows by induction from the above fact, since if f^{j-1} has this property then also does $f^j = f^{j-1} \circ f$. ■

From the above, we get (for instance) the following translation of Corollary 4 and Theorem 8.

Theorem 43. *Let R be a complete Noetherian local ring with maximal ideal $\mathfrak{m}$ and residue characteristic p, let $f(x) \in R[[x]]$, and suppose there is a cycle $(x_1, \ldots, x_m)$ of f in R. Let k be the length of the projected cycle in $R/\mathfrak{m}$ and let r be the order of $(f^k)'(x_1)$ in $(R/\mathfrak{m})^*$ (put $r = 0$ if $(f^k)'(x_1) \in \mathfrak{m}$). Then we have either $m = k$, $m = kr$, or, if $p > 0$, $m = krp^n$, where (if R has characteristic zero) the positive integer n satisfies $n \leq 1 + \log(2e/(p-1))/\log p$, and moreover $n \leq 1 + \log e/\log 2$ if $p = 2$.*

2.5 Rational functions and rational maps

In this section we generalize the idea of Proposition 14 to show that our results apply to a more general class of rational functions than just polynomials. We begin with a straightforward generalization.

Proposition 44. *Let $h(x) = f(x)/g(x)$ be a rational function over a ring R, where $f, g \in R[x]$. Let $\sigma = (x_1, \ldots, x_m)$ be a cycle of h in R, and assume that every $g(x_i)$ is a unit in R. Then there is a polynomial over R having the cycle σ.*

Our proof relies on the following lemma.

Lemma 45. *If S is a finite set of units in a ring R, then there is a polynomial $\psi_S(x) \in R[x]$ such that $\psi_S(\alpha) = 1/\alpha$ for each $\alpha \in S$.*

Proof. Define ψ_S to be the polynomial for which $\prod_{\alpha \in S}(1 - x/\alpha) = 1 - x\psi_S(x)$. Then $\psi_S(\alpha) = 1/\alpha$ for each $\alpha \in S$. ■

Proof of Proposition 44. For $S = \{g(x_1), \ldots, g(x_m)\}$, note that $f(x) \cdot \psi_S(g(x))$ has the cycle σ. ■

Thus, any cycle which occurs for a rational function with the special property of the proposition, also occurs for a polynomial; so our results which depend only on the particular cycle (and not on the corresonding polynomial) apply in the setting of the proposition. Thus, Propositions 10 and 12, Theorems 13 and 37, and Corollary 38 remain valid when we generalize their hypotheses from polynomials to rational functions satisfying the condition of the above proposition. In fact, we will see that most of our other results apply as well to rational functions as in the above proposition.

Lemma 46. *Let θ be a polynomial satisfying the conclusion of Proposition 44, let I be a proper ideal of R containing all the zero-divisors, and let k be the length of the projected cycle in R/I. If $m > k$, then $(h^k)'(x_1) \equiv (\theta^k)'(x_1) \pmod{I}$.*

This lemma implies that Proposition 1, its corollaries, and Theorems 8 and 36 remain valid when their hypotheses are generalized from polynomials to rational functions satisfying the condition of the above proposition, since the conclusions of those results depend only on the cycle and on the image of $(f^k)'(x_1)$ in R/I (and all of these results certainly hold in the more general context in case $m = k$).

Proof of Lemma 46. We first show that, for any two polynomials $\delta, \gamma \in R[x]$ having the same cycle $(y_1, \ldots, y_\ell)$ (with $\ell > 1$) which lies in the coset $x_1 + I$ of R, we have $\delta'(y_1) \equiv \gamma'(y_1) \pmod{I}$. Here $y_3 - y_2 = \delta(y_2) - \delta(y_1) \equiv (y_2 - y_1)\delta'(y_1) \pmod{(y_2-y_1)^2}$; the same holds for γ, so $(y_2-y_1)(\delta'(y_1) - \gamma'(y_1)) \in (y_2-y_1)^2$, whence $(y_2-y_1)(\delta'(y_1) - \gamma'(y_1) - (y_2-y_1)d) = 0$ for some $d \in R$. Since I contains all the zero-divisors of R, we have $(\delta'(y_1) - \gamma'(y_1) - (y_2-y_1)d) \in I$, so also $(\delta'(y_1) - \gamma'(y_1)) \in I$, as desired.

We apply this to the polynomials δ, γ where $\delta = \theta^k$ and γ is a polynomial which has the same cycle $(x_1, x_{k+1}, x_{2k+1}, \ldots, x_{m-k+1})$ as does h^k. Thus, it suffices to show that $(h^k)'(x_1) \equiv \gamma'(x_1) \pmod{I}$. Note that $h^k = r/s$, where $r, s \in R[x]$ and each $s'(x_{kt+1}) \in R^*$. Here $\gamma(x) = r(x) \cdot \psi_S(s(x))$, where $S = \{s(x_1), s(x_{k+1}), \ldots, s(x_{m-k+1})\}$. Since $\prod_{\alpha \in S}(1 - x/\alpha) = 1 - x\psi_S(x)$, we have

$$-s(x_1)\psi_S'(s(x_1)) - \psi_S(s(x_1)) = \frac{-1}{s(x_1)} \cdot \prod_{\alpha \neq s(x_1)} \left(1 - \frac{s(x_1)}{\alpha}\right),$$

so, from $s(x_1) \equiv s(x_{kt+1}) \pmod{I}$ we conclude that $\psi_S'(s(x_1)) \equiv -1/s(x_1)^2 \pmod{I}$. Thus $\gamma'(x_1) \equiv r'(x_1)/s(x_1) - r(x_1)/s(x_1)^2 \pmod{I}$, and this last expression is just $(h^k)'(x_1)$, completing the proof. ■

We now extend the above results to a broader class of rational functions. The verification itself is easy, the main difficulty lies in finding the right definition; we thank Silverman [23] for his help in discovering this definition. In [14] Morton and Silverman gave a related definition, and thus studied a somewhat smaller class of rational functions; in this section we follow the development of that paper when possible. It is interesting to note that the methods Morton and Silverman use to derive results similar to ours, namely methods of algebraic geometry, seem quite unrelated to our methods.

For the remainder of this section, R is a domain, K its fraction field, $\mathfrak{p}$ is a prime ideal of R, and κ is the fraction field of the domain $R/\mathfrak{p}$. By $R_\mathfrak{p}$ we mean the localization of R at the prime $\mathfrak{p}$: so $\kappa = R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$. Finally, ϕ denotes a rational function $\phi : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ of degree $d \geq 1$ defined over K; that is, a pair of coprime homogeneous polynomials in $K[X, Y]$ of degree d.

Definition. The rational map $\phi : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ has *good reduction* with respect to $\mathfrak{p}$ at the element $[x_0 : y_0]$ of $\mathbb{P}^1(K)$ (where we assume $x_0, y_0 \in R_\mathfrak{p}$ are not both in $\mathfrak{p}R_\mathfrak{p}$) if there exist homogeneous polynomials $\phi_1, \phi_2 \in R_\mathfrak{p}[x, y]$, of the same degree, such that the map ϕ is given by

$$\phi([x : y]) = [\phi_1(x, y) : \phi_2(x, y)],$$

and the maps $\tilde{\phi}_1, \tilde{\phi}_2 : \mathbb{A}^2(\kappa) \to \mathbb{A}^1(\kappa)$, gotten by reducing the coefficients of ϕ_1 and ϕ_2 modulo $\mathfrak{p}R_\mathfrak{p}$, do not have $(\tilde{x}_0, \tilde{y}_0)$ as a common root (for $a \in R_\mathfrak{p}$, we let $\tilde{a}$ denote the image of a in $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$).

In [14] rational maps were considered which have good reduction with respect to $\mathfrak{p}$ at all points of $\mathbb{P}^1(K)$; we will see that one only needs good reduction at all points of whatever cycle is under consideration.

Lemma 47. *If ϕ has good reduction with respect to $\mathfrak{p}$ at $[x_0 : y_0]$ and ψ has good reduction with respect to $\mathfrak{p}$ at $[x_1 : y_1] = \phi([x_0 : y_0])$, then $\psi \circ \phi$ has good reduction with respect to $\mathfrak{p}$ at $[x_0 : y_0]$.*

Proof of Lemma 46. We have $\phi_1, \phi_2, \psi_1, \psi_2$ as in the definition. Put $X = \phi_1(x_0, y_0)$ and $Y = \phi_2(x_0, y_0)$; by hypothesis, at most one of X and Y is in the ideal $\mathfrak{p}R_\mathfrak{p}$. Similarly, $Z = \psi_1(x_1, y_1)$ and $W = \psi_2(x_1, y_1)$ are not *both* in $\mathfrak{p}R_\mathfrak{p}$, so x_1 and y_1 are not both in $\mathfrak{p}R_\mathfrak{p}$. Since $[x_1 : y_1] = \phi([x_0 : y_0]) = [X : Y]$, we have $X = ux_1$ and $Y = uy_1$ for some nonzero $u \in K$; but since each of (x_1, y_1) and (X, Y) is in $R_\mathfrak{p} \times R_\mathfrak{p}$ but not in $\mathfrak{p}R_\mathfrak{p} \times \mathfrak{p}R_\mathfrak{p}$, we must have $u \in R_\mathfrak{p}^*$.

Let d' be the degree of ψ. Then $\gamma_1 = \psi_1(\phi_1(x, y), \phi_2(x, y))$ and $\gamma_2 = \psi_2(\phi_1(x, y), \phi_2(x, y))$ are homogeneous polynomials in $R_\mathfrak{p}[x, y]$ of degree dd', and $\psi \circ \phi([x : y]) = [\gamma_1(x, y) : \gamma_2(x, y)]$. Since $\gamma_1(x_0, y_0) = \psi_1(X, Y) = u^{d'}\psi_1(x_1, y_1) = u^{d'}Z$ and similarly $\gamma_2(x_0, y_0) = u^{d'}W$, either $\gamma_1(x_0, y_0)$ or $\gamma_2(x_0, y_0)$ is in $R_\mathfrak{p}^*$, so (x_0, y_0) is not a common root of $\tilde{\gamma}_1$ and $\tilde{\gamma}_2$. This completes the proof. ■

Corollary 48. *If ϕ has good reduction with respect to $\mathfrak{p}$ at all points of a finite cycle of ϕ in $\mathbb{P}^1(K)$, then the same is true for any iterate of ϕ.*

Corollary 49. *If ϕ has good reduction with respect to $\mathfrak{p}$ at $[x_0 : y_0]$, then $\imath \circ \phi \circ \imath$ has good reduction with respect to $\mathfrak{p}$ at $[y_0 : x_0]$. Here $\imath = y/x$.*

We give one more definition before stating the main result of this section: if $\psi : \mathbb{P}^1 \to \mathbb{P}^1$ is a rational map which fixes the point P, then ψ induces a linear map on the cotangent space of $\mathbb{P}^1$ at P,

$$\psi_P^* : \Omega_P(\mathbb{P}^1) \to \Omega_P(\mathbb{P}^1).$$

This cotangent space is one dimensional, so the map is multiplication by a scalar. We denote this scalar by $\psi'(P)$ and call it the *derivative of ψ at P*. Note that this definition agrees with the usual definition of derivative of a rational function $\psi(z) \in K(z)$ whenever $P \neq \infty$.

Now we give the main result of this section.

Theorem 50. *Let K be a nonarchimedean field and let $\mathfrak{p}$ be the maximal ideal of the valuation ring of K; suppose that the residue class field κ has characteristic p, and that e is the ramification index. Let $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ be a rational map of degree at least two defined over K, and suppose there is a cycle of ϕ in $\mathbb{P}^1(K)$, of length m, consisting of points at which ϕ has good reduction with respect to $\mathfrak{p}$. Let k be the length of the projected cycle in $\mathbb{P}^1(\kappa)$, and let r be the order of $(\widetilde{\phi^k})'(\tilde{P})$ in κ^*, for any point P in the cycle (if $(\widetilde{\phi^k})'(\tilde{P}) = 0$ then $r = 0$.) Then either $m = k$, $m = kr$, or, if $p > 0$, $m = krp^n$, where, if K has characteristic zero, the positive integer n satisfies $n \leq 1 + \log(2e/(p-1))/\log p$ and moreover $n \leq 1 + \log e/\log 2$ if $p = 2$.*

Proof of Lemma 46. We may assume that some point P in the cycle lies in the valuation ring R of K: for, otherwise we simply conjugate ϕ by the reciprocal map $\imath : [x, y] \to [y, x]$; the new map has a cycle consisting of the reciprocals of the elements of the original cycle, and the new map has good reduction at all points of the new cycle by Corollary 49. Thus, the k^{th} iterate of ϕ has P as a fixed point mod $\mathfrak{p}$; we will consider the cycle of length m/k consisting of all points of the original cycle which are congruent mod $\mathfrak{p}$ to the point P. This cycle of length m/k lies in R; since ϕ^k has good reduction with respect to $\mathfrak{p}$ at all points of this cycle, the denominator of ϕ^k, evaluated at any point of the cycle, must be a unit in R. Thus, we are in the situation described in Proposition 44. This completes the proof. ■

A weaker result has been shown by Morton and Silverman [14, Thm.1.1]; their result differs from ours in that they do not bound n, and they require the additional hypothesis that ϕ has good reduction everywhere. Their proof relies on the calculation of multiplicities in certain divisors in [13], and is entirely different from ours.

The proof of the theorem amounts to reducing to the simpler setting of Proposition 44; previously we noted that several of our results for polynomials hold as well for rational functions satisfying the conditions of that proposition. Thus the same is true for rational functions with good reduction. Namely, Propositions 10 and 12, Theorems 13, 36 and 37, and Corollary 38 remain valid if we extend their hypotheses to cover not just polynomials but rational functions with good reduction on the relevant cycle.

2.6 Examples

We conclude this chapter by giving several examples. We begin by discussing p-cycles in the maximal ideal. Here R is a discrete valuation ring of residue characteristic p, and $\mathfrak{m}$ is the maximal ideal of R. One simple type of p-cycle is $(0, b, 2b, \dots, (p-1)b)$, where $b \in \mathfrak{m}$ $(b \neq 0)$. This is a cycle for the polynomial

$$x + b - \frac{p}{b^{p-2}(p-1)!} \prod_{i=0}^{p-2} (x - ib),$$

which has coefficients in R whenever $(p-2)\mathrm{ord}_{\mathfrak{m}}(b) \leq e = \mathrm{ord}_{\mathfrak{m}}(p)$. Thus, there exists some such b precisely when $p \leq e + 2$.

We now give several examples demonstrating that Theorem 8 is best possible, at least when p or e is small. Suppose R is a discrete valuation ring of mixed characteristic, and let π be a uniformizer. If $e = 1$, Theorem 8 implies there is no p-cycle in $\mathfrak{m}$ unless $p \leq 3$, in which case there is no p^2-cycle in $\mathfrak{m}$. If $e = 1$ and $p \leq 3$ then the previous example provides polynomials over R having p-cycles in R. If $e = 2$, Theorem 8 implies there is no p-cycle in $\mathfrak{m}$ unless $p \leq 5$, in which case there is no p^2-cycle unless $p = 2$, in which case there is no p^3-cycle. Again, each of the remaining possibilities does occur. For instance,

$$f(x) = \frac{-\pi^3 + \pi^5 - \pi^2 x - 4\pi^3 x + \pi^5 x + 4\pi x^2 + 3\pi^2 x^2 - \pi^3 x^2 - 2x^3}{(-1+\pi)\,\pi^2\,(1+\pi)}$$

is in R when $p = 2$ and $e = 2$, and has the cycle $(0, \pi, \pi^2, \pi + \pi^2)$. And, if $\pi^2 = 5$, then the polynomial

$$f(x) = \frac{(6x^4 + 400x^3 + 781x^2 + 2737x - 50) + \pi(-9x^4 - 64x^3 - 890x^2 - 501x + 62)}{62 - 10\pi}$$

has the cycle $(0, \pi, 2\pi, 5 + 3\pi, -5 + 4\pi)$. Moreover, the following is true, although our proof is not too pleasant: if $p = 5$ and $e = 2$ and $5/\pi^2$ is a square in $R/\mathfrak{m}$, then there is a polynomial over R having a 5-cycle in $\mathfrak{m}$. Further, if $p = 5$ and $e = 2$ and $\#(R/\mathfrak{m}) = 5$, then there only exists a polynomial with a 5-cycle if $5/\pi^2$ is a square in $R/\mathfrak{m}$, and in this case, if the cycle is $(0, \pi, a\pi, b\pi, c\pi)$, then $\mathfrak{m}$ contains $a-2$, $b-3$, and $c-4$. It would be nice to have an intuitive explanation for these strange facts. We give our (non-intuitive) proof below.

If there exists a polynomial over R having a 5-cycle in $\mathfrak{m}$, then there exists a polynomial over R, of degree at most 4, having a 5-cycle in $\mathfrak{m}$ of the form $\sigma = (0, \pi, a\pi, b\pi, c\pi)$. It is also necessary that $0, 1, a, b, c$ all be distinct (mod $\mathfrak{m}$); we will assume that, in some order, a, b, c are congruent to $2, 3, 4$ (mod $\mathfrak{m}$). The Lagrange interpolation formula is a formula for the unique polynomial over K (the fraction field of R) which has the cycle σ. When we write out this formula we find that the constant term and the coefficient of x are already in R. The coefficient of x^2 is in R if and only if the ordered triple (a, b, c) (mod $\mathfrak{m}$) is either $(2, 3, 4)$ or $(4, 3, 2)$. If the coefficient of x^3 is in R, then $(a, b, c) = (4, 3, 2)$ (mod $\mathfrak{m}$); and if $a = 2 + A\pi$, $b = 3 + B\pi$, and $c = 4 + C\pi$, then the coefficient of x^3 is in R if and only if $A + B + C \in \mathfrak{m}$. Finally, if the previous coefficients are in R, then the coefficient of x^4 is in R if and only if $(A - 2B)^2 \equiv -5/\pi^2 \equiv 5/\pi^2 \pmod{\mathfrak{m}}$, which has a solution (A, B) if and only if $5/\pi^2$ is a square in $R/\mathfrak{m}$.

Russo and Walde in [24, Theorems 7,8] describe the 2-adic periodic points of a polynomial $x^2 + c \in \mathbb{Z}_2[x]$. We give a generalization of their results, along the lines of [14, Corollary 1.2].

Proposition 51. *Let R be a discrete valuation ring having finite residue field κ of size q and characteristic p, and let $f(x) = \sum \alpha_i x^{q^i} \in R[x]$. Put $a = f(0)$ and $b = f(1) - f(0)$, and let r be the multiplicative order of a in κ^* (put $r = 0$ if $a \in \mathfrak{m}$). Let $\alpha \in R$ be a periodic point for f of period m. Then*

$$m = \begin{cases} 1 & \text{if } a - 1 \in \mathfrak{m} \text{ and } b \in \mathfrak{m} \\ p & \text{if } a - 1 \in \mathfrak{m} \text{ and } b \notin \mathfrak{m} \\ 1 & \text{if } a - 1 \notin \mathfrak{m} \text{ and } \alpha + b/(a-1) \in \mathfrak{m} \\ r & \text{if } a - 1 \notin \mathfrak{m} \text{ and } \alpha + b/(a-1) \notin \mathfrak{m}. \end{cases}$$

Proof of Lemma 46. Let k be the length of the projected cycle modulo the maximal ideal $\mathfrak{m}$ of R; then $f^k(x)$ is a polynomial in x^q, so $(f^k)'(\alpha) \in \mathfrak{m}$. By Proposition 4, this implies that $m = k$.

Since $x^q = x$ for any x in the residue field $\kappa = R/\mathfrak{m}$, we see that f acts as a linear map on κ, mapping $x \mapsto f(0) + (f(1) - f(0))\,x$. Put $b = f(0)$ and

$a = f(1) - f(0)$; then the ℓ^{th} iterate of $f|_\kappa$ is given by

$$f^\ell(x) = a^\ell x + b\left(1 + a + \cdots + a^{\ell-1}\right);$$

thus,

$$f^\ell(x) - x = \begin{cases} \ell b & \text{if } a = 1 \\ (a^\ell - 1)\left(x + \frac{b}{a-1}\right) & \text{if } a \neq 1. \end{cases}$$

Now we simply consider each of the various cases. If $a \equiv 1 \pmod{\mathfrak{m}}$ then $f^\ell(\alpha) - \alpha \in \mathfrak{m}$ if and only if $\ell b \in \mathfrak{m}$, so k, the least such ℓ, is either 1 (if $b \in \mathfrak{m}$) or p. If $a \not\equiv 1 \pmod{\mathfrak{m}}$ then k is the least positive integer for which $(a^k - 1)\left(\alpha + \frac{b}{a-1}\right) \in \mathfrak{m}$; thus, k is either 1 (if $\alpha + b/(a-1) \in \mathfrak{m}$) or r. ■

We remark that the reason one can get such a precise result is that the polynomials considered in this proposition have the property that all of their p-adic cycles are attracting. Of course, this is not generally true for polynomials over a discrete valuation ring; moreover, this is in marked contrast to the situation over $\mathbb{C}$.

Chapter 3

Non-archimedean dynamical systems

In its most general incarnation, a dynamical system is a function f from a set to itself. One is interested in the behavior of points of the set under repeated application of f. In particular, the basic object of study is the orbit $\{f^n(x) : n \geq 0\}$, where x is a point in the set and f^n denotes the n^{th} iterate of f. In this generality, one of the only ways to distinguish different orbits is to compare their sizes; so it is natural to pay special attention to the finite orbits. This is what we have done in the previous chapter, in case the dynamical system is a polynomial mapping of a ring, or a power series over a complete nonarchimedean ring, or a rational function over a ring or a rational map on the projective line over a nonarchimedean field (in some of these cases we are considering dynamical systems in which the function f is only defined on some subset of the underlying set).

When the underlying set of a dynamical system is endowed with the structure of a metric space, one can ask various topological questions about an orbit. For instance, does the orbit have limit points? Is it closed? What does it 'look like'? The classical dynamical systems were rational functions on the Riemann sphere; these have been extensively studied. It is natural to ask whether the phenomena which occur in these classical systems will also occur in other dynamical systems. We concentrate on the case when the underlying set of the dynamical system is endowed with the structure of an ultrametric space; examples of this are polynomial mappings (or rational maps) of a ring with a prescribed ideal, power series over a complete nonarchimedean ring, and rational maps on the projective line over a nonarchimedean field. In the past few years various aspects of these 'nonarchimedean' dynamical systems have been studied. In this chapter we summarize the present state of this theory, incorporating the results of several unpublished investigations. One common theme in the classical theory is that the finite orbits determine the dynamical behavior to a surprisingly large extent; to date this seems to be true to an even greater extent in the nonarchimedean case, but it could be that this perception will change as the field of nonarchimedean dynamics matures.

3.1 Local dynamics

Let K be a complete nonarchimedean field, and let $f(x) = \sum_{i=1}^{\infty} a_i x^i$ be a power series over K having no constant term. Supposing that f has nonzero radius of convergence, f defines a mapping from its domain of convergence into K. We would like to understand the dynamics of this mapping "near" the fixed point 0. To do this, we attempt to find simple maps with especially transparent dynamics, such as linear polynomials, which have the same behavior in some small neighborhood of 0 as does f. We also attempt to make this neighborhood as large as possible. It is not hard to show that these results imply corresponding results for the dynamics of an analytic mapping sufficiently close to any finite orbit.

3.1.1 Background

This problem has long been studied when K is a field complete with respect an archimedean (rather than nonarchimedean) valuation. In the nonarchimedean case it turns out that, if the linear coefficient a_1 is neither 0 nor a root of unity, and K has characteristic zero, then f is locally conjugate (near 0) to its derivative $\psi(x) = a_1 x$. This is not generally true in the archimedean case, and the difficulty there has become known as the problem of "small divisors". We now briefly review the situation in the archimedean case. First, it is a simple matter to show that, when a_1 is neither 0 nor a root of unity, there is a unique formal power series $L(x) = x + \sum_{i=2}^{\infty} u_i x^i$ for which $f(L(x)) = L(a_1 x)$. This equation is known as the Schröder functional equation . Since the formal solution is unique, the question of the existence of a local conjugacy amounts to asking whether L has a positive radius of convergence. If $|a_1| < 1$, the convergence is easily established. Likewise, if $|a_1| > 1$ we can linearize on the other side by considering the inverse map. But the set of a_1 with $|a_1| = 1$ and a_1 not a root of unity, for which there is a holomorphic function $f(x) = \sum_{i=1}^{\infty} a_i x^i$ whose series L diverges, forms a dense subset of the unit circle $|x| = 1$. Siegel became the first to overcome a small divisors problem, when he showed that if a_1 on the unit circle satisfies a certain diophantine condition, then L converges. His delicate estimation technique of the series L (Cauchy majorants) did not apply to many other instances of a small divisors problem. Subsequently, much more powerful estimation techniques were developed; Zehnder applied one of these powerful iteration techniques to recover Siegel's result. Herman and Yoccoz noted that Zehnder's proof essentially worked for nonarchimedean fields as well; they also noticed that the diophantine condition is satisfied when K is a nonarchimedean field of characteristic zero. However, Zehnder's proof, as generalized by Herman and Yoccoz, is quite difficult; also, it does not produce an explicit lower bound on the radius of convergence of L. We have discovered a drastically simpler proof of the result of Herman and Yoccoz; moreover, our proof gives an explicit lower bound on the radius of convergence of L. Finally, one should consider the case when L does not converge (for instance, when a_1 is 0 or a root of unity), and attempt to produce some simple map (with easily describable dynamics) other than $a_1 x$ to which f is conjugate in this case. This has not yet been done.

3.1.2 Local conjugacy

We would like to state our result on convergence of L. First we need some background on power series over a complete nonarchimedean field. For any complete nonarchimedean field K, by $|\cdot|$ we denote the valuation on K; by $\mathrm{B}(r)$ we denote the 'open' ball around 0 of radius r, namely $\{x : |x| < r\}$. Let $f(x) = \sum_{i=1}^{\infty} a_i x^i \in K[[x]]$

be a power series over K having no constant term. The radius of convergence of f is

$$r = \frac{1}{\limsup \sqrt[i]{|a_i|}}.$$

Define

$$\begin{aligned} C = C(f) &= \sup_{i \geq 2} \sqrt[i-1]{|a_i|} \\ D = D(f) &= \sup_{i \geq 2} \sqrt[i-1]{|a_i/a_1|} \qquad \text{if } a_1 \neq 0. \end{aligned}$$

If $r > 0$, it follows at once that $C < \infty$ and $D < \infty$. The quantities C and D play a key role in our study of the local conjugacy problem. Our next result, and the discussion which follows, illustrates the geometric significance of C. Before stating this result we observe that the set of formal power series without constant term over a field K is a group under composition; we call the inverse of an element of this group its 'formal inverse'.

Claim. *If $|a_1| = 1$, then the formal inverse $g(x) = \sum_{i=1}^{\infty} b_i x^i$ of f satisfies $|b_1| = 1$ and $C(g) = C(f)$.*

Again suppose $|a_1| = 1$. Then for $|x| < 1/C$ we have $|a_i x^i| \leq C^{i-1}|x|^i = |x|(C|x|)^{i-1} \to 0$ as $i \to \infty$, so f converges on $\mathrm{B}(1/C)$; moreover, $f : \mathrm{B}(1/C) \to \mathrm{B}(1/C)$. The above Claim implies that the formal inverse g of f also maps $\mathrm{B}(1/C)$ to itself. Our hypotheses ensure that $f(g(x)) = g(f(x)) = x$ whenever $x \in \mathrm{B}(1/C)$, so f and g are inverse bijections on $\mathrm{B}(1/C)$. Moreover, it is easy to see that they are isometries of this ball.

We now turn to the problem of local conjugacy, first solving it formally.

Proposition 52. *For any $f(x) = \sum_{i=1}^{\infty} a_i x^i \in K[[x]]$, where K is a field, if a_1 is neither 0 nor a root of unity then there is a unique $L(x) = \sum_{i=1}^{\infty} b_i x^i \in K[[x]]$ with $b_1 = 1$ such that $\psi \circ L = L \circ f$ formally, where $\psi(x) = a_1 x$.*

The proof amounts to simply writing out the functional equation and successively solving for the various coefficients b_i.

We study the convergence of L by estimating $C(L)$. We now present our explicit result.

Theorem 53. *Keep the notation and hypotheses from the previous result, adding the assumption that K is complete with respect to a nonarchimedean valuation. Then*

(1) If $0 < |a_1| < 1$ then $C(L) \leq C(f)/|a_1|$.

(2) If $|a_1| > 1$ then $C(L) \leq D(f)/|a_1|$.

(3) If $|a_1| = 1$ but a_1 is not a root of unity in the residue field then $C(L) \leq C(f)$.

(4) Now suppose a_1 is a primitive ℓ^{th} root of unity in the residue field, and let p denote the residue characteristic. Put $\theta = |a_1^\ell - 1|$.

(4a) If $p = 0$ then $C(L) \leq C(f)/\theta^{1/\ell}$.

(4b) Now suppose that $p > 0$ and K has characteristic zero.

(4b1) If $\theta^{p^I} < |p|^{1/p-1} < \theta^{p^{I-1}}$ for some $I \geq 1$, or if the leftmost inequality holds for $I = 0$, then

$$C(L) \leq C(f)/\left(\theta^{1+I\frac{p-1}{p}}|p|^{\frac{1}{p^I(p-1)}}\right)^{1/\ell}.$$

(4b2) If $\theta^{p^{I-1}} = |p|^{1/p-1}$ for some $I \geq 1$ then for $\psi = |a_1^{\ell p^I} - 1|$ we have

$$C(L) \leq C(f)/\left(\theta^{I\frac{p-1}{p}}\psi^{1/p^I}|p|^{\frac{1}{p^I(p-1)}}\right)^{1/\ell}.$$

Our proof is quite straightforward. We merely use the recursive formulas for the b_i derived in the proof of Proposition 52 to inductively bound $|b_i|$.

3.1.3 Dynamics near a periodic point

The above results show that, if $f(x) = \sum_{i=1}^{\infty} a_i x^i \in K[[x]]$ has a_1 being neither zero nor a root of unity, then in a certain explicit neighborhood of the fixed point 0 the dynamics of the map f are the same (*isometrically*) as the dynamics of the map $a_1 x$. Thus to understand the dynamics near the fixed point 0 one need only understand the corresponding dynamics for the simple map $a_1 x$. These dynamics are completely transparent; the upshot is that the local dynamics in the nonarchimedean case are very rigid.

3.2 Global dynamics

Further away from a periodic point the dynamics are more difficult to describe. Little successful work has been done on this problem. An approach which seems fruitful is based on our technique for controlling cycle lengths in Chapter 2. For simplicity we describe this in the case of polynomial mappings of a ring R together with an ideal I of R. The approach is based on considering the relationships between the images of an orbit in the various rings R/I^n. Again the situation is quite rigid. For example, consider the simple case $R = \mathbb{Z}_p$ and $I = p\mathbb{Z}_p$: let T be the projection in R/I^n of some orbit in R of a polynomial $f(x) \in R[x]$. Then the projection of this orbit in R/I^{n+1} is contained in the preimage of T in this ring; if these two sets are equal, then the projection of the orbit in R/I^{n+2} equals the preimage of T in this ring, and so on. It follows that the closure of the orbit is a closed ball in the metric space R; thus, from a fairly innocuous condition one can conclude precise global information about the orbit. The situation for general discrete valuation rings is similar, though quite a bit more complicated due to the presence of wild ramification. Still, using arguments like those in Chapter 2, one can prove various results in this setting.

The situation is vastly more complicated when one considers polynomial mappings of a nonarchimedean field. Here one can even get behavior which would technically be called 'chaotic'. This brings to mind an analogy with archimedean dynamics, namely the Fatou and Julia sets. For a given rational mapping of the Riemann sphere, the sphere can be written as the disjoint union of two subsets, on one of which the dynamics is not too complicated (the Fatou set) and on the other of which the dynamics is often very complicated and even chaotic. Perhaps for polynomial mappings of the valuation ring of a nonarchimedean field, the ring should be viewed as a subset of a sort of Fatou set. In the classical case the Julia set is the closure of the set of repelling periodic points (a repelling periodic point of a map f is a point x lying in a cycle of length n and satisfying $|(f^n)'(x)| > 1$). In our nonarchimedean setting it is in fact true that a polynomial over the valuation ring of a nonarchimedean field has no repelling periodic points in the valuation ring (since $|y| \leq 1$ for all points y in the valuation ring), so perhaps this is evidence supporting our speculative analogy.

3.3 Further work and ruminations

In this section we very briefly describe the other work that has been done on nonarchimedean dynamics. First there is Lubin's approach to nonarchimedean dynamical systems, based on his paper [11] which lays out the basic tools to be used in future investigations. This approach has the flavor of formal group theory. Lubin carefully studies the linearizing map L as in Proposition 52, which may also be viewed as the logarithm of the formal group $F(x,y) = L^{-1}(L(x)+L(y))$ (the original map f is an automorphism of this formal group). He shows how one can learn much about the dynamics of f by considering properties of the logarithm L and of a related object which he calls the 'Lie logarithm'. As an easy consequence of this approach, one can produce a simple proof of Sen's theorem on ramification in local fields [10].

One can also study a sort of 'arithmetic dynamics', namely dynamical systems on a number field (especially those coming from polynomials or rational functions). By passing to the completion at a nonarchimedean valuation, one can apply the various results from the nonarchimedean case to the arithmetic case. There are new phenomena in the arithmetic case, though, so a global approach is required. Preliminary work in this direction has been done by Call, Morton, and Silverman among others. Here there are various conjectures which seem to be quite far out of reach. Foremost among these is the Uniform Boundedness Conjecture of Morton and Silverman [13], which is a quite general conjecture motivated by the corresponding conjecture for torsion on abelian varieties. In the simplest case this conjecture asserts the existence of a number N such that no quadratic polynomial over $\mathbb{Q}$ has a cycle in $\mathbb{Q}$ of length exceeding N (the existing evidence suggests that one can even take $N = 3$.) But even in this simple case, a proof of the conjecture would be an outstanding achievement: Morton has shown that no quadratic polynomial over $\mathbb{Q}$ has a 4-cycle in $\mathbb{Q}$, and now Flynn, Poonen and Schaefer have found an excellent but difficult proof that there are no 5-cycles either. Even the nonexistence of 6-cycles seems beyond the reach of known methods.

An exciting feature of these arithmetic dynamical systems is their connection with units in a number field. Narkiewicz noticed that from a cycle of a polynomial in a ring, one can produce several units (a special case of our results in Section 2.2). This observation was generalized to rational maps by Morton and Silverman [13], who also gave a method for using two cycles of coprime lengths to produce many more units. Morton and Silverman call these units 'dynamical units'. Given a number field K, by adjoining the elements of a cycle (of a rational map) we construct a field extension containing various dynamical units. Since the Galois action on the units is simple to describe, this provides useful information about the field extension. It is unfortunate that the dynamical units do not in general span a subgroup of finite index in the full unit group, but even so the partial information provided by the dynamical units is far more than one knows for arbitrary field extensions.

Finally, one can generalize to higher-dimensional maps, such as n-tuples of polynomials (or power series) in n variables or rational maps of higher-dimensional varieties (instead of merely the projective line). The results to date in this case are rather preliminary. For instance, Pezda has shown that, as in the one-dimensional case, there are various restrictions on the possible cycle lengths; but it seems there should be many further restrictions, perhaps of a qualitatively different sort, beyond what Pezda gives. Also one can approach the local and global dynamics using methods similar to the ones described above; the partial results known so far suggest only that many interesting phenomena await discovery and explanation. On a different note, Silverman has done a bit of work on higher-dimensional arithmetic dynamics. Here it seems one can prove precise results only for very special types of mappings. The main example studied so far are the Hénon maps; in the classical case of complex dynamics, these maps have been extensively studied since they have the unusual dynamical behavior called strange attractors. Silverman [22] has derived various arithmetic information about the cycles of the Hénon map defined over a number field. By first studying the nonarchimedean dynamical behavior of these maps, we have discovered a different type of arithmetic information about the cycle lengths which, among other things, yields a bound on the cycle lengths of any specific Hénon map. Thus, in this one case the global and local approaches provide complementary results.

I conclude this thesis with an invitation. Today only a handful of mathematicians study nonarchimedean dynamical systems. To my mind this area is quite broad, amenable to techniques of various different flavors, and has important applications to algebraic number theory. There is a vast supply of questions and conjectures awaiting resolution. I hope that more mathematicians will join in the study of this young exciting area of mathematics.

Bibliography

[1] S. Chowla. Proof of a conjecture of Julia Robinson. *Norske Vid. Selsk. Forh. (Trondheim)*, 34:100–101, 1961.

[2] J. Evertse. Upper bounds for the number of solutions of diophantine equations, 1983. Mathematical Centre Tract 168, Mathematisch Centrum, Amsterdam.

[3] J. Evertse and K.Győry. On unit equations and decomposable form equations. *J. Reine Angew. Math.*, 358:6–19, 1985.

[4] K. Győry. Sur les polynômes à coefficients entiers et de discriminant donné, ii. *Publ. Math. Debrecen*, 21:125–144, 1974.

[5] K. Győry. Sur une classe de corps de nombres algébriques et ses applications. *Publ. Math. Debrecen*, 22:151–175, 1975.

[6] H. W. Lenstra, Jr. Euclidean number fields of large degree. *Invent. Math.*, 38:237–254, 1977.

[7] A. Leutbecher. Euclidean fields having a large Lenstra constant. *Ann. Inst. Fourier (Grenoble)*, 35:83–106, 1985.

[8] A. Leutbecher and J. Martinet. Lenstra's constant and Euclidean number fields. *Astérisque*, 94:87–131, 1982.

[9] A. Leutbecher and G. Niklasch. On cliques of exceptional units and Lenstra's construction of Euclidean fields. In H. Schlickewei and E. Wirsing, editors, *Number Theory, Ulm 1987*, number 1380 in Lecture notes in mathematics, pages 150–178. Springer-Verlag, New York.

[10] H.-C. Li. p-adic periodic points and Sen's theorem. *J. Number Theory*, 56:309–318, 1996.

[11] J. Lubin. Nonarchimedean dynamical systems. *Compositio Math.*, 94:321–346, 1994.

[12] J.-F. Mestre. Corps euclidiens, unités exceptionnelles et courbes elliptiques. *J. Number Theory*, 13:123–137, 1981.

[13] P. Morton and J. H. Silverman. Periodic points, multiplicities, and dynamical units. *J. Reine Angew. Math.*, 461:81–122, 1995.

[14] P. Morton and J. H. Silverman. Rational periodic points of rational functions. *Internat. Math. Res. Notices* 1994:97–110, 1994.

[15] T. Nagell. Sur une propriété des unités d'un corps algébrique. *Ark. Mat.*, 5:343–356, 1964.

[16] T. Nagell. Quelques problèmes relatifs aux unités algébriques. *Ark. Mat.*, 8:115–127, 1969.

[17] T. Nagell. Sur un type particulier d'unités algébriques. *Ark. Mat.*, 8:163–184, 1969.

[18] T. Pezda. Polynomial cycles in certain local domains. *Acta Arith.*, 66:11–22, 1994.

[19] B. Poonen. Personal correspondence, April 1995.

[20] W. H. Schikhof. *Ultrametric Calculus: an Introduction to p-adic Analysis.* Number 4 in Cambridge studies in advanced mathematics. Cambridge University Press, New York, 1984.

[21] H. Schlickewei. Unpublished result.

[22] J. H. Silverman. Geometric and arithmetic properties of the Hénon map. *Math. Z., 215:237–250, 1994.*

[23] *J. H. Silverman. Personal correspondence, October 1993.*

[24] *R. Walde and P. Russo. Rational periodic points of the quadratic function* $Q_c(x) = x^2 + c$. Amer. Math. Monthly*, 101:318–331, 1994.*

[25] *R. Wasén. On sequences of algebraic integers in pure extensions of prime degree.* Colloq. Math.*, 30:89–104, 1974.*