On Non-archimedean Dynamical Systems

Sheldon T. Joyner

Thesis presented in partial fulfilment of the requirements for the degree of MASTER OF SCIENCE at the UNIVERSITY OF STELLENBOSCH

Supervisor : Professor BW GREEN
December 2000

Declaration

I, the undersigned, hereby declare that the work contained in this thesis is my own original work and that I have not previously in its entirety or in part submitted it at any university for a degree.

Abstract

A discrete dynamical system is a pair (X, ϕ) comprising a non-empty set X and a map $\phi : X \to X$. A study is made of the effect of repeated application of ϕ on X, whereby points and subsets of X are classified according to their behaviour under iteration. These subsets include the JULIA and FATOU sets of the map and the sets of periodic and preperiodic points, and many interesting questions arise in the study of their properties.

Such questions have been extensively studied in the case of complex dynamics, but much recent work has focussed on non-archimedean dynamical systems, when X is projective space over some field equipped with a non-archimedean metric. This work has uncovered many parallels to complex dynamics alongside more striking differences.

In this thesis, various aspects of the theory of non-archimedean dynamics are presented, with particular reference to JULIA and FATOU sets and the relationship between good reduction of a map and the empty JULIA set. We also discuss questions of the finiteness of the sets of periodic points in special contexts.

Opsomming

'n Paar (X, ϕ) bestaande uit 'n nie-leë versameling X tesame met 'n afbeelding $\phi : X \to X$ vorm 'n diskrete dinamiese sisteem. In die bestudering van so 'n sisteem lê die klem op die uitwerking op elemente van X van herhaalde toepassing van ϕ op die versameling. Elemente en subversamelings van X word geklasifiseer volgens dinamiese kriteria en op hierdie wyse ontstaan die JULIA en FATOU versamelings van die afbeelding en die versamelings van periodiese en preperiodiese punte. Interessante vrae oor die eienskappe van hierdie versamelings kom na vore.

In die geval van komplekse dinamika is sulke vrae reeds deeglik bestudeer, maar onlangse werk is op nie-archimediese dinamiese sisteme gedoen, waar X 'n projektiewe ruimte is oor 'n liggaam wat met 'n nie-archimediese norm toegerus is. Hierdie werk het baie ooreenkomste maar ook treffende verskille met die komplekse dinamika uitgewys.

In hierdie tesis word daar ondersoek oor verskeie aspekte van die teorie van nie-archimediese dinamika ingestel, in besonder met betrekking tot die JULIA en FATOU versamelings en die verband tussen goeie reduksie van 'n afbeelding en die leë JULIA versameling. Vrae oor die eindigheid van versamelings van periodiese punte in spesiale kontekste word ook aangebied.

Preface

The ideal page of Mathematics reveals human authorship most subtley: rather than by errors or personal allusions, the perfect Maths text manifests the humanity of the writer by giving a glimpse of the creative intellect which differentiates us from machines and points to our having been created. I hope that my exposition of the Mathematics in this dissertation succeeds in conveying some vision of that creativity.

The thesis contains original material in Sections 4.1 and 4.2, so the Mathematics which it presents is chiefly the work of others. In my discussion of their discoveries, it has been my aim to carefully explain the details at the same time as giving a lucid account of the meaning of the results.

Where appropriate, I have acknowledged my intellectual debt in the body of the thesis, but I would like to extend especial thanks to RL BENEDETTO who has been most helpful. The proofs of Lemma 2.1 and Proposition 3.2 were shown us in an interesting lecture series on p-adic Analysis presented by Professor S BÖGE of Heidelberg University. I would also like to thank Professor APJ VAN DER WALT for his marvellous course on Fractals and his suggestions for possible further avenues of investigation of the non-archimedean MANDELBROT set. I am also indebted to the examiners for their many useful comments and suggestions for improvements to the thesis.

In the preparation of this thesis, the help of Professor BW GREEN has been invaluable: not only were the courses he presented indispensable to my being able to produce the thesis, but I could also not have done without his suggestions, ideas, knowledge, encouragement and enthusiasm.

During 1999 and 2000 I have been financially supported by two NRF grantholder bursaries awarded through Professor GREEN; two HARRY CROSSLEY scholarships; a Professor GGCILLIÉ scholarship and a Stellenbosch 2000 merit bursary. I have been supported in other ways by many inspiring people, whom I would also like to thank; particularly my parents and brothers, and ALEX PEREZ, ALISHA ALMEIDA, RENE POTGIETER, and friends at Stellenbosch Central Methodist Church.

Contents

Chapter 1

Introduction

Given a map ϕ from a non-empty set X to itself, a study of the results of repeated application (or "iteration") of the map often yields interesting and valuable information about ϕ. To emphasize the role of the "dynamics" of the map, we refer to such a pair (X, ϕ) as a *discrete dynamical system*. It is usual to identify points and subsets of X which satisfy certain dynamical criteria with respect to the map ϕ: for example, we ask which are the *fixed points* of ϕ - those points $x \in X$ such that $\phi(x) = x$; and a step further, which are the fixed points of ϕ^n for some $n \in \mathbb{N}\backslash\{0\}$ (the *periodic points* of ϕ). Points and sets of X thus become intrinsics of the map ϕ and can be studied with the aim of learning more about the map.

Endowing the set X of a discrete dynamical system (X, ϕ) with a metric opens up further possibilities for study: we can ask how the distances between points are affected under iteration. In exploring these possibilities when X is the RIEMANN sphere $\mathbb{P}^1(\mathbb{C})$ equipped with the spherical metric arising from the archimedean absolute value on $\mathbb{C}$ and $\phi(z) \in \mathbb{C}(z)$ is a rational map, the subject of complex dynamical systems was born. Complex dynamics is a rich area of study with its origins in the work of JULIA and FATOU early this century. Central to this field are sets named in their respective honour - the JULIA and FATOU sets of a given rational map ϕ. Roughly speaking, the FATOU set of a map ϕ consists of all the points of $\mathbb{P}^1(\mathbb{C})$ for which small errors stay small under iteration: that is, if two points are "close" together and both are in the FATOU set, then their iterates under ϕ will still be "close". The complement of the FATOU set is the JULIA set of ϕ. Comprising as it does those points of X for which small errors can become large under iteration, the JULIA set often turns out to be a complicated fractal set which splits the FATOU set into a large set of connected components, called FATOU *components*.

The images of points of the FATOU set are clearly also in the FATOU set, but more than that, ϕ maps points of any FATOU component into some other FATOU component, thereby inducing a map, say Φ, on the set of FATOU components, to itself. Thus, this set, together with Φ, is a dynamical system. It so happens that in this system, each point is preperiodic - i.e. each FATOU component is ultimately mapped to some repeating sequence of FATOU components, under the induced action of the map ϕ of which we are considering the FATOU set. This is the celebrated "No Wandering Domains Theorem" which stood as a conjecture for a long period before being proved in its full generality by D.SULLIVAN in 1985.

To enter the realm of non-archimedean dynamical systems, we instead consider non-archimedean norms on fields, such as the p-adic metric for a fixed prime p on $\mathbb{Q}$ or its extension to the field Ω_p, which is the (algebraically closed) completion of the algebraic closure of the completion of $\mathbb{Q}$ under this metric. This subject can be seen to be a study of local dynamical information with a view towards better understanding the global picture, paralleling the frequent number theoretic use of local-global principles. For example, given a DEDEKIND domain R, we can consider the quotient field K of R equipped with valuations coming from each of the distinct non-zero prime ideals of R in turn, and study the (local) dynamical properties of a map $\phi : \mathbb{P}^n(K) \to \mathbb{P}^n(K)$ at each such non-zero prime. Piecing together the information thus obtained yields data about the map ϕ. MORTON and SILVERMAN use just such a procedure to produce units in a number field, in [13].

The theory currently being developed in non-archimedean dynamics exhibits parallels to complex dynamics as well as more striking differences: while BENEDETTO has shown in [1] that there is a similar "No Wandering Domains" theorem in p-adic dynamics, (where the notion of "components" had to be modified owing to the total disconnectedness of Ω_p), it is possible for the JULIA set of a map ϕ to be non-compact, or even empty - phenomena which are not possible in the archimedean case. In fact, SILVERMAN and MORTON [13] have shown that for a large class of maps - namely those which have good reduction in some coordinate system - the JULIA set is empty.

The relationship of the good reduction of a map to its JULIA set being empty is one of the principal avenues of exploration undertaken in this thesis. Firstly, though, we set the stage by outlining rudimentary facts in the study of non-archimedean dynamical systems. We then proceed to define the JULIA and FATOU sets and to elucidate some of their

interesting properties for maps of the projective line over a non-archimedean field to itself. Following this we generalize the *good reduction / empty* JULIA *set* result of MORTON and SILVERMAN: they showed that it holds for rational maps $\phi : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$, where K is some non-archimedean valued field, but it is also true for rational maps $\psi : \mathbb{P}^n(K) \to \mathbb{P}^n(K)$ where n is any positive integer.

The question of whether good reduction is equivalent to having empty JULIA set is very difficult for general maps of smooth projective varieties, but for polynomial maps of the projective line over a non-archimedean field to itself, BENEDETTO has managed to settle this question completely. As a prelude to a discussion of his findings, we define a non-archimedean analogue of the MANDELBROT set and show how it catalogues all quadratic maps of the projective line to itself having good reduction in some co-ordinate system (unless the characteristic of the residue field is two). Applying this information, we are able to establish the equivalence of a quadratic polynomial map of $\mathbb{P}^1(K)$ to itself having good reduction to its JULIA set being empty, barring the case where the characteristic of the residue field is two.

A valuable example of a discrete dynamical system is given by a variety X defined over a number field K, together with a morphism $\phi : X \to X$. In Chapter 5 we shall discuss the fascinating result of NORTHCOTT [15], which shows that in this case there exists a finite bound on the number of preperiodic, K-rational points, depending only on the degree $[K : \mathbb{Q}]$. (As the name suggests, *preperiodic points* of a map ϕ are those points $x \in X$ such that there exist $m, n \in \mathbb{N}\backslash\{0\}; m \neq n$ such that $\phi^m(x) = \phi^n(x)$ - i.e. after a finite number of iterates, each preperiodic point is mapped onto a periodic point). Much recent work has focussed on determining such bounds for different classes of maps. (For example, in 1994, MEREL [12] showed that the set of integers n for which the elliptic curve X defined over a number field K has K-rational n-torsion points is bounded above by an expression depending only on the degree $[K : \mathbb{Q}]$. This was the final step, building on work of MANIN, MAZUR, KAMIENNY, FREY and FALTINGS, in proving the "uniform boundedness conjecture" to be true: viewing $\phi_n : X \to X$ as multiplication by some integer n, then (X, ϕ_n) is a dynamical system, and applying NORTHCOTT'S theorem it follows that there exist at most finitely many K-rational n-torsion points. Since this is true for each n, from MEREL'S result we know that the total number of K-rational torsion points of X is finite, and depends only on the degree of the number field over $\mathbb{Q}$.)

Returning to the case where the field of definition of the variety is equipped with a non-

archimedean metric, we present a theorem of MORTON and SILVERMAN which deals both with good reduction and the finiteness of the number of periodic points of a certain kind: in this situation, if the projective line is mapped to itself by some separable morphism which has good reduction and degree at least two, then the morphism has at most finitely many attracting periodic points.

Although beyond the scope of this dissertation, this is an area of active research (see for example [7] or [8]). In more general situations, properties of sets of periodic points of varieties equipped with morphisms are used to obtain important geometric and arithmetic information.

Chapter 2

Preliminaries

2.1 Non-archimedean valued fields and the p-adics

A norm is a special kind of function by means of which a field can be endowed with a metric topology. An example is the absolute value function on $\mathbb{Q}$ (the rational numbers) which gives us the notion of the "size" of rational numbers and the distance between them. The properties by means of which a norm is defined are precisely what is needed so as to induce a metric on the given space, namely non-negativity; zero being precisely what is mapped to the identity of the ordered abelian group which is the image of the space under the norm; multiplicativity; and the triangle inequality.

A famous theorem of OSTROWSKI asserts that up to topological equivalence, the only norms which $\mathbb{Q}$ admits are the usual absolute value and the p-adic norms associated to each integer prime p. Unlike the usual absolute value with the Euclidean distance on $\mathbb{R}^n$ to which it gives rise, these p-adic norms are little served by our intuition. This is because p-adic norms are non-archimedean: they satisfy a stronger inequality than the triangle inequality where the addition of elements is concerned:

Definition 2.1 *A norm $|\cdot|$ on a field K is said to be non-archimedean if, for every $x, y \in K$, with $|x| \geq |y|$, then for every $N \in \mathbb{N}$, also $|x| \geq |Ny|$.*
Any other norm is called archimedean.

Definition 2.2 *A norm $|\cdot|$ on a field K is said to satisfy the ultrametric property if, for every $x, y \in K$, $|x + y| \leq \max\{|x|, |y|\}$.*

A norm is non-archimedean if and only if it satisfies the ultrametric property: firstly it is a triviality that all norms which satisfy the ultrametric property are non-archimedean.

On the other hand, if $(K, |\cdot|)$ is a non-archimedean normed field, then $|1| \leq |1| = 1$ implies that $|N| \leq 1$ for every $N \in \mathbb{N}$. But then, if $|z| \leq 1$, also $|z+1| \leq 1$:

$$|z+1|^n = |\sum_{i=0}^{n} \binom{n}{i} z^{n-i}| \leq \sum_{i=0}^{n} |\binom{n}{i}||z^{n-i}|$$

from the triangle inequality. Here, $|\binom{n}{i}| \leq 1$ and $|z^{n-i}| \leq 1$ for all n, i.

Thus, $|z+1|^n \leq n+1$ for every $n \in \mathbb{N}$. However, since for each $\varepsilon > 0$, there exists $M \in \mathbb{N}$ such that $\sqrt[M]{M+1} < 1+\varepsilon$, we know that $|z+1| \leq 1$. Now let x and y be arbitrary elements of K, not both zero, and consider $|x+y|$. Suppose WLOG that $|y| \leq |x| \neq 0$. Then applying what we have just shown, $|x+y| = |x||1+\frac{y}{x}| \leq |x|$ since $|\frac{y}{x}| \leq 1$. i.e. $|x+y| \leq \max\{|x|, |y|\}$.

It is clear that ultrametricity implies the triangle inequality: if $|x+y| \leq \max\{|x|, |y|\}$, then also $|x+y| \leq |x| + |y|$.

A useful consequence of the ultrametric property is the following: whenever $l, m \in K$ and $|l| > |m|$, then $|l+m| = |l|$:
indeed, if $l, m \in K$ with $|l| > |m|$, then $|l| = |l+m-m| \leq \max\{|l+m|, |m|\} = |l+m|$ (since $|l| \not\leq |m|$). Thus $|l+m| \leq \max\{|l|, |m|\} = |l|$ implies $|l+m| = |l| = \max\{|l|, |m|\}$.

Some topological oddities which arise in the metric topology of a non-archimedean norm are the following, (where throughout we let $(K, |\cdot|)$ be any non-archimedean normed field): (0) *Each triangle is isoceles:*
If $w, y, z \in K$, then if $|z-w| \neq |z-y|$, say $|z-y| > |z-w|$, we have that $|w-y| = |w-z+z-y| = |z-y|$ from ultrametricity.
(1) *Each point of a disc is a centre of the disc:*
(By "disc", we mean a set of the form $D_r(x) = \{z \in K : |z-x| < r\}$ or the "closed disc" $\overline{D}_r(x) = \{z \in K : |z-x| \leq r\}$.)
If $D_r(x)$ is a disc in K and $y \in D_r(x)$ is chosen arbitrarily, then for any other z in the disc, $|y-z| = |y-x+x-z| \leq \max\{|y-x|, |x-z|\} < r$, and if $w \in K$ has $|w-y| < r$ then also $|w-x| = |w-y+y-x| < r$ as before, so that $D_r(x) = D_r(y)$ (and similarly for the "closed" disc $\overline{D}_r(x)$).
(2) *If two discs intersect, then they are either equal or one is properly contained in the other:*
Suppose that there exists $w \in D_r(x) \cap D_s(y)$ and that there exists $z \in D_r(x) \backslash D_s(y)$. Then from (1), we know that $D_r(x) = D_r(w)$ and $D_s(y) = D_s(w)$. It is then trivial that either $D_r(x) = D_s(y)$ or one of these discs is properly contained in the other.

We shall often work with *rank one valuations* rather than norms. These provide an alternative (though entirely equivalent) viewpoint to that given by norms, although they fit into the context of more general valuations, for which there is a well developed theory.

Definition 2.3 *A* non-archimedean valuation *on a field K is a function* $v : K \longrightarrow \Gamma \cup \{\infty\}$ *where* $(\Gamma, +, \prec)$ *is an ordered abelian group and* ∞ *represents some object such that for every* $\sigma \in \Gamma$, $\sigma \prec \infty$ *and* $\sigma + \infty = \infty$, *with the following properties:*
(0) $v(f) = \infty \Leftrightarrow f = 0$
(1) $v(gh) = v(g) + v(h)$ *for every* $g, h \in K$
(2) $v(g+h) \geq \min\{v(g), v(h)\}$ *for every* $g, h \in K$
If Γ *is a subgroup of* $(\mathbb{R}, +)$, *then* v *is a* rank one *valuation.*

From any rank one valuation a norm which provides precisely the same information as the valuation itself, may be defined as follows: if $r \in \mathbb{R}; r > 1$ then let $|z|_v = r^{-v(z)}$. It is easily seen that this is a norm. The set of all possible norms of elements of $K\backslash\{0\} = K^*$ forms a subgroup of $(\mathbb{R}^+, .)$ called the *value group* of the valuation, which we denote by $|K^*|$.

The p-adic valuation on $\mathbb{Q}$ for a fixed prime p is a mapping to $(\mathbb{Z}, +) \cup \{\infty\}$ defined by $v_p(\frac{a}{b}) = v_p(p^n \frac{g}{h}) = n$, where $p \nmid g; p \nmid h$, and we pick $r = p$ to define the associated norm:

$$|\frac{a}{b}| = |p^n \frac{g}{h}| = p^{-v_p(\frac{a}{b})} = p^{-n} = |p^n|.$$

Because of the information which they give about the divisibility of numbers by fixed primes, the p-adic valuations have important applications in Number Theory, where they are used to piece together local algebraic information (at each prime) in order to establish facts which are pertinent to the overall or global understanding of some number theoretical question.

It is often convenient in dynamical systems for the valued field with which we work to be complete, algebraically closed, or both. In the p-adic context, we make use of the smallest algebraically closed field extending $\mathbb{Q}$ which is complete under the norm arising from the p-adic valuation. Unlike its counterpart $\mathbb{C}$, the algebraic closure of the completion of $\mathbb{Q}$ under the p-adic metric is not complete. It is thus necessary to take the completion of this extension of $\mathbb{Q}$ (which *is* algebraically closed) as the analogue of $\mathbb{C}$ in the non-archimedean setting. For more details on this field, (Ω_p, v_p), we refer the reader to KOBLITZ, [9].

Given a normed field, the polynomial ring with coefficients in the field is equipped with a norm which arises in a very natural way and which we shall find particularly useful:

Definition 2.4 *If $(K, |\cdot|)$ is a normed field, then the* GAUSS *norm of a polynomial $f \in K[x_0, \ldots, x_n]$ for some $r \geq 0$, is defined to be*

$$|f|_G := \max\{|a| : a \text{ is a coefficient of } f\}.$$

It is not difficult to show that this is in fact a norm, and that should the norm on K be non-archimedean it inherits this non-archimedeanity. (See BOSCH *et al.*, [3] for the details.) Given the ring of formal power series in one variable with coefficients in a normed field $(K, |\cdot|)$, we can analogously define a GAUSS norm on the algebra

$$K\{z\} := \{f(z) = \sum_{i=0}^{\infty} a_i z^i \in K[[z]] : |a_i| \to 0 \text{ as } i \to \infty\}$$

but here this norm is not multiplicative: given power series f and g, $|f|_G|g|_G$ may strictly exceed $|fg|_G$, although this cannot occur in the case of polynomials.

2.2 Elementary facts from non-archimedean analysis

We develop certain facts here which will prove useful in our later discussion.
Let a rank one non-archimedean valued field (K, v) (i.e. a field equipped with a non-archimedean valuation) be fixed throughout the subsequent discussion.

Definition 2.5 *The* ring of integers $\mathcal{O}_K$ *of (K, v) is defined by:*

$$\mathcal{O}_K = \{z \in K : v(z) \geq 0\}.$$

Remarks

- For any non-archimedean valued field (K, v), $\mathcal{O}_K$ is a valuation ring (i.e. it is a local ring in which the ideals are linearly ordered by inclusion) with valuation ideal $\mathcal{M}_K = \{z \in K : v(z) > 0\}$.
- If $a \in \mathcal{O}_K$, we use the following notation for reduction modulo $\mathcal{M}_K$: $\overline{a} = a + \mathcal{M}_K$.
- We denote the *residue field* $\mathcal{O}_K/\mathcal{M}_K$ by $\overline{K}$.

Definition 2.6 *The valued field (K, v) is called* henselian *if it satisfies the following condition: Whenever $f(x) = a_0 + \cdots + a_n x^n \in \mathcal{O}_K[x]$ and there exists $\alpha_0 \in \mathcal{O}_K$ such that $f(\alpha_0) \equiv 0 \ (mod \mathcal{M}_K)$ but $f'(\alpha_0) \not\equiv 0 \ (mod \mathcal{M}_K)$ (that is, $\overline{\alpha_0} \in \overline{K}$ is a simple root of $\overline{f}(x) = \overline{a_0} + \cdots + \overline{a_n} x^n \in \overline{K}[x]$), then there exists a unique $\alpha \in \mathcal{O}_K$ such that $\alpha - \alpha_0 \in \mathcal{M}_K$ and $f(\alpha) = 0$.*

The unique lifting of simple roots criterion used to define henselian fields is usually referred to as "HENSEL'S Lemma," since it was first shown to be valid for $\mathbb{Q}_p$ (the completion of $\mathbb{Q}$ under the p-adic metric, sometimes called "HENSEL'S field of p-adics") by HENSEL. HENSEL'S Lemma turns out to be analogous to the classical method of numerical approximation of roots due to NEWTON. (See KOBLITZ [9].)

Each algebraically closed valued field is henselian, since any polynomial can be expressed as a product of linear factors over such a field, so any simple root of a reduced polynomial clearly corresponds to a unique root of the polynomial in the ring of integers. (Observe that each root must be in the valuation ring, since if

$$f(x) = (x - \alpha_0) \ldots (x - \alpha_n) = c_0 + \cdots + c_{n+1} x^{n+1},$$

then $c_{n+1-k} = \sum_{i_1 < i_2 < \ldots < i_k} \alpha_{i_1} \ldots \alpha_{i_k}$ so from ultrametricity, if precisely k roots of f are not in $\mathcal{O}_K$, then $v(c_{n+1-k}) < 0$.)

For subsequent use, we now state a similar condition to that given by HENSEL'S Lemma, and show that it is true for any non-archimedean valued field which is complete. It is formulated for power series, as follows:

Lemma 2.1 (HENSEL'S Lemma for Power Series) *Let (K, v) be a complete non-archimedean valued field, and $f(x) = \sum_{i \geq 0} a_i x^i \in \mathcal{O}_K\{x\}$. Suppose that there are polynomials g_0 and h_0 in $\mathcal{O}_K[x]$ such that*
(a) g_0 is monic of degree l;
(b) $\overline{h_0}$ and $\overline{g_0}$ (the coefficient-wise reduced polynomials in $\overline{K}[x]$) are relatively prime; and
(c) $f \equiv g_0 h_0 (mod \mathcal{M}_K)$ (so that $\overline{f}$, the reduced series, is a polynomial - i.e. almost all of the coefficients of f are in $\mathcal{M}_K$).
Then there exists a monic polynomial $g \in \mathcal{O}_K[x]$ of degree l and a power series $h(x) \in \mathcal{O}_K[[x]]$ such that $g \equiv g_0 \pmod{\mathcal{M}_K}$, $h \equiv h_0 \pmod{\mathcal{M}_K}$ and $f = gh$.

Proof: Assuming that f, g_0 and h_0 are as above, we construct two sequences of polynomials with limits g and h respectively, which yield the desired factorization of f :

the GAUSS norm on $K\{x\}$ can also be expressed additively by setting

$$v_G(\sum_{i\geq 0} a_i x^i) := \min_{i\geq 0}\{v(a_i)\}.$$

(We refer to the function v_G as the Gaussian valuation on $K\{x\}$.)

From (c), $v_G(f - g_0h_0) > 0$. Applying BEZOUT'S identity in $\overline{K}[x]$, by (b) there exist $u, w \in \mathcal{O}_K[x]$ such that $v_G(ug_0 + wh_0 - 1) > 0$. Now there also exists $\pi \in \mathcal{M}_K$ such that $v_G(ug_0 + wh_0 - 1) \geq v(\pi) > 0$ and $v_G(f - g_0h_0) \geq v(\pi) > 0$. (Indeed, any $\pi \in \mathcal{M}_K$ such that $v(\pi) = \min\{v_G(f - g_0h_0), v_G(ug_0 + wh_0 - 1)\}$ could be chosen.) We proceed to inductively construct polynomials g_n and $h_n \in \mathcal{O}_K[x]$ such that

(i) g_n is monic of degree l;

(ii) $v_G(g_n - g_{n-1}) \geq nv(\pi)$ and $v_G(h_n - h_{n-1}) \geq nv(\pi)$; and

(iii) $v_G(f - g_nh_n) \geq (n+1)v(\pi)$.

Setting $g_{-1} = g_0$ and $h_{-1} = h_0$, these conditions are satisfied for $n = 0$. Now suppose that such polynomials have been constructed for $n = 1, \ldots, m$. Because of (d), there exists M such that $v(a_i) > (m+2)v(\pi)$ for every $i > M$. But then

$$\begin{aligned} v_G(\sum_{i=M+1}^{\infty} a_i x^i) &= \min_{i\geq M+1}\{v(a_i)\} \\ &> (m+2)v(\pi), \end{aligned}$$

so since v_G is non-archimedean,

$$v_G(\sum_{i=0}^{\infty} a_i x^i - g_m h_m) \geq \min\{v_G(\sum_{i=0}^{M} a_i x^i - g_m h_m), v_G(\sum_{i=M+1}^{\infty} a_i x^i)\}.$$

The induction hypothesis ensures that $v_G(\sum_{i=0}^{\infty} a_i x^i - g_m h_m) \geq (m+1)v(\pi)$, and hence

$$v_G(\sum_{i=0}^{M} a_i x^i - g_m h_m) \geq (m+1)v(\pi).$$

Thus we can define $y \in \mathcal{O}_K[x]$ by:

$$\pi^{m+1} y = \sum_{i=0}^{M} a_i x^i - g_m h_m. \tag{2.1}$$

Now in $\mathcal{O}_K[x]$, we can divide yw by g_m, obtaining: $yw = qg_m + r$ where $\deg r < \deg g_m = l$ or $r = 0$. Then

$$\begin{aligned} yug_m + ywh_m &= yug_m + (qg_m + r)h_m \\ &= (yu + qh_m)g_m + rh_m \end{aligned}$$

Define $u^* := yu + qh_m$ and $w^* := r$, and now set $g_{m+1} = g_m + \pi^{m+1}w^*$ and $h_{m+1} = h_m + \pi^{m+1}u^*$. Observe that $u^*, w^* \in \mathcal{O}_K[x]$.

Furthermore, since deg w^* < deg $g_m = l$, g_{m+1} is also monic of degree l. (In general though, deg u^* could exceed deg h_m.) Now

$$\begin{aligned}
& f - g_{m+1}h_{m+1} \\
= & \sum_{i=M+1}^{\infty} a_i x^i + \sum_{i=0}^{M} a_i x^i - g_m h_m + g_m h_m - (g_m + \pi^{m+1}w^*)(h_m + \pi^{m+1}u^*) \\
= & \sum_{i=M+1}^{\infty} a_i x^i + \pi^{m+1}y - \pi^{m+1}w^*h_m - \pi^{m+1}u^*g_m - \pi^{m+1}\pi^{m+1}u^*w^* \quad \text{from (2.1)} \\
= & \sum_{i=M+1}^{\infty} a_i x^i + \pi^{m+1}y - \pi^{m+1}(yug_m + ywh_m) - \pi^{2m+2}u^*w^*,
\end{aligned}$$

where the last equality holds from the definition of u^* and of w^*.

Now

$$\begin{aligned}
& v_G(ug_1 + wh_1 - 1) \\
= \; & v_G(u(g_1 - g_0) + w(h_1 - h_0) + ug_0 + wh_0 - 1) \\
\geq \; & \min\{v_G(u) + v_G(g_1 - g_0); v_G(w) + v_G(h_1 - h_0); v_G(ug_0 + wh_0 - 1)\} \\
\geq \; & \min\{v_G(u) + v(\pi); v_G(w) + v(\pi); v(\pi)\} \\
& \text{from assumption (ii) and the choice of } \pi; \\
= \; & v(\pi) \qquad \text{since } u, w \in \mathcal{O}_K[x],
\end{aligned}$$

so that continuing inductively yields $v_G(ug_m + wh_m - 1) \geq v(\pi)$.
But then $v_G(yug_m + ywh_m - y) \geq v(\pi) + v_G(y)$. Thus

$$\begin{aligned}
& v_G(f - g_{m+1}h_{m+1}) \\
& = v_G(\sum_{i=M+1}^{\infty} a_i x^i + \pi^{m+1}y - \pi^{m+1}(yug_m + ywh_m) - \pi^{2m+2}u^*w^*) \\
& \geq \min\{v_G(\sum_{i=M+1}^{\infty} a_i x^i), v(\pi^{m+1}) + v_G(yug_m + ywh_m - y), v(\pi^{2m+2}) + v_G(u^*w^*)\} \\
& \geq \min\{(m+2)v(\pi), (m+1)v(\pi) + v(\pi) + v_G(y), (2m+2)v(\pi) + v_G(u^*w^*)\} \\
& = (m+2)v(\pi) \quad \text{as required.}
\end{aligned}$$

Moreover,

$$v_G(g_{m+1} - g_m) = v_G(\pi^{m+1}u^*) \geq (m+1)v(\pi)$$

and

$$v_G(h_{m+1} - h_m) = v_G(\pi^{m+1}w^*) \geq (m+1)v(\pi),$$

so that g_{m+1} and h_{m+1} satisfy (i), (ii), and (iii). By induction, then, we have constructed sequences of functions of which it is now possible to take the limits under v_G. These limits

will exist owing to the completeness of K under the valuation v. (It is possible to show that $K\{x\}$ is complete with respect to v_G whenever K is complete with respect to v.) We denote these limits respectively by g and h and observe that g is a monic polynomial of degree l, with $g \equiv g_0 \pmod{\mathcal{M}_K}$ and h is a power series satisfying $h \equiv h_0 \pmod{\mathcal{M}_K}$, with $f = gh$. □

In passing we mention an easy consequence of HENSEL'S Lemma for Power Series, namely:

Corollary 2.1 *Every complete, non-archimedean valued field is henselian.*

Proof: Since each complete, non-archimeadean valued field satisfies HENSEL'S Lemma for Power Series, we need only show that this implies that HENSEL'S Lemma also holds. Now if $f(x) \in \mathcal{O}_K[x]$ has $f(\alpha) \equiv 0 \pmod{\mathcal{M}_K}$ and $f'(\alpha) \not\equiv 0 \pmod{\mathcal{M}_K}$ for some $\alpha \in \mathcal{O}_K$, then $(x-\alpha)$ is a polynomial in $\mathcal{O}_K[x]$, for which $(x-\overline{\alpha})$ and $\frac{\overline{f}(x)}{(x-\overline{\alpha})}$ are relatively prime in $\overline{K}[x]$, so that from the above lemma, there exists $a \in \mathcal{O}_K$ and $h(x) \in \mathcal{O}_K[x]$ such that $f(x) = (x-a)h(x)$, with $\overline{h}(x) = \frac{\overline{f}(x)}{(x-\overline{\alpha})}$. It follows that no root of h reduces to $\overline{\alpha}$. But then a is unique such that $a - \alpha \in \mathcal{M}_K$ and $f(a) = 0$. □

In particular, $\mathbb{Q}_p$, the completion of $\mathbb{Q}$ under the p-adic metric, is henselian, as is (Ω_p, v_p).

Remarks

- An interesting characterization of henselian fields is the following:
  A non-archimedean valued field (K, v) (where the valuation is non-trivial) is henselian if and only if the valuation v has a unique prolongation (i.e. an extension as of functions) to a valuation on any given algebraic closure of K.
- We have already mentioned a fact which follows as a trivial consequence of this characterization, namely that each algebraically closed, non-archimedean valued field is henselian.
- The above corollary also follows from this result, since it is possible to show that the valuation on any complete non-archimedean valued field admits a unique prolongation to a valuation on any given algebraic closure.
- (For the details, we refer the reader to MCCARTHY'S text [11].)

For the remainder of the chapter, we assume that K is algebraically closed and complete with respect to a valuation of rank one. In this context, we have a marvellous tool for

investigating the roots of a given polynomial $f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$, which goes by the name of the NEWTON polygon of f. This is defined to be the lower convex hull of $\{(i, v(a_i)) : i = 0, 1, \ldots, n\}$ on an XY-axis system. Although it does not enable us to find the roots explicitly, it is easily shown that if $-\lambda$ is a slope of some segment of the NEWTON polygon which has a projection on the X-axis of total length l, then f has precisely l roots of value λ.

The NEWTON polygon of a given power series $g(z) = \sum_{i=0}^{\infty} b_iz^i \in K[[z]]$ is defined to be the limit of the NEWTON polygons of the nth partial sums $g_n(z) = \sum_{i=0}^{n} b_iz^i$ of g, and it encodes similar information about the values of roots of g. For our discussion we require

Definition 2.7 *A power series $f(x) = \sum_{i=0}^{\infty} a_ix^i$ with coefficients in K is said to converge on $\overline{D}_r(0) = \{z \in K : |z| \leq r\}$ if $\lim_{N\to\infty} \sum_{i=0}^{N} a_iz^i$ exists for all $z \in \overline{D}_r(0)$.*

Observe that the condition $\lim_{i\to\infty} |a_i|r^i = 0$ is then both necessary and sufficient for the convergence of the power series $f(x) = \sum_{i=0}^{\infty} a_ix^i$ on $\overline{D}_r(0)$ in the non-archimedean situation. This is clearly in contrast to the archimedean case, where the above condition is not sufficient for convergence of power series.

Now if μ is a value which is assumed by some z within the radius of convergence of g, (i.e. there exists z such that g converges at z and $v(z) = \mu$), then if no side of the NEWTON polygon has gradient $-\mu$, no roots of g have value μ; while if a segment of the NEWTON polygon has slope $-\mu$ and this segment has finite projection on the X-axis (say the projection has length m), then there exist precisely m roots of g with value μ.

A very useful application of NEWTON polygons is the following "Roots Theorem" which gives a simple condition for the existence and number of roots of a given norm, of a power series with coefficients in an algebraically closed, non-archimedean valued field. Firstly though, we define some terminology:

Definition 2.8 *If $r \in |K^*|$ and $x \in K$, then $\overline{D}_r(x)$ is called a* rational *closed disc.* (This term originates from the p-adic setting, where $|\Omega_p|$ is a subset of $\mathbb{Q}$.)

Theorem 2.1 (Roots Theorem) *If $f = \sum_{i=0}^{\infty} c_ix^i \in K[[x]]$ is a non-zero power series which converges on some rational closed disc $\overline{D}_r(0)$, then there exists $\alpha \in K$ with $f(\alpha) = 0$*

and $|\alpha| = r$ *if and only if there exist* $m, n \in \mathbb{N}, m > n$ *with*

$$|c_m|r^m = |c_n|r^n = \max_{i\geq 0}\{|c_i|r^i\}.$$

If we choose m *and* n *such that for every* $t > m, |c_t|r^t < |c_m|r^m$ *and for every* $s < n$, $|c_s|r^s < |c_n|r^n$, *then there exist precisely* $m - n$ *roots of* f *on* $C_r(0) := \{z \in K : |z| = r\}$.

Proof:

Suppose that there exists a root α of f with $|\alpha| = r$. Then

$$|f(\alpha)| = |\sum_{i=0}^{\infty} c_i\alpha^i| = 0 < \max_{i\geq 0}\{|c_i|r^i\}.$$

If $|c_j|r^j = \max_{i\geq 0}\{|c_i|r^i\}$ for a unique j, then from ultrametricity, $|f(\alpha)| = |c_j|r^j$. Indeed, $\lim_{i\to\infty} |c_i|r^i = 0$ from the convergence of f on $\overline{D}_r(0)$ so that the ultrametric property is applicable even though the sum is infinite:

$$|\sum_{i=0}^{\infty} c_i\alpha^i| = \max\{|\sum_{i=0}^{j-1} c_i\alpha^i|, |c_j|r^j, |\sum_{i=j+1}^{\infty} c_i\alpha^i|\},$$

because $|\sum_{i=j+1}^{N} c_i\alpha^i| < |c_j|r^j$ for each $N > j$. But then $|c_j|r^j = 0$, contradicting the fact that f is non-zero. Hence, there exist $m, n \in \mathbb{N}$ with $m > n$, such that

$$|c_m|r^m = |c_n|r^n = \max_{i\geq 0}\{|c_i|r^i\}$$

and for which $|c_t|r^t < |c_m|r^m$, for every $t > m$, and $|c_s|r^s < |c_n|r^n$, for every $s < n$.

Now if $t > m$, then since $|\alpha| = r$, also $v(c_t) + tv(\alpha) > v(c_m) + mv(\alpha)$, which implies that

$$-v(\alpha) < \frac{v(c_t) - v(c_m)}{t - m}. \tag{2.2}$$

Similarly for $s < n$, we have $v(c_s) + sv(\alpha) > v(c_n) + nv(\alpha)$, so that

$$-v(\alpha) > \frac{v(c_n) - v(c_s)}{n - s}. \tag{2.3}$$

This implies that each point $(s, v(c_s))$ with $s < n$ lies above the line through $(n, v(c_n))$ of gradient $-v(\alpha)$. Since the line segment between $(n, v(c_n))$ and $(m, v(c_m))$ has slope $-v(\alpha)$ (clearly $|c_m|r^m = |c_n|r^n$ implies that $v(c_m) + mv(\alpha) = v(c_n) + nv(\alpha)$), we see that $(n, v(c_n))$ is in fact a vertex of the NEWTON polygon, from the definition. Moreover, if $s < n$, then no point $(s, v(c_s))$ can be a vertex of the NEWTON polygon which begins a segment of slope $-v(\alpha)$.

Each point $(j, v(c_j))$ for $j > n$ is on or above the line through $(n, v(c_n))$ of gradient $-v(\alpha)$, since otherwise, there exists some point $(i, v(c_i))$ for $i > n$, such that

$$\frac{v(c_i) - v(c_n)}{i - n} < -v(\alpha),$$

from which it would follow, reversing the calculations performed to obtain (2.2) and (2.3), that $|c_i|r^i > |c_n|r^n$.

Again because the line segment between $(n, v(c_n))$ and $(m, v(c_m))$ has slope $-v(\alpha)$, $(m, v(c_m))$ is also on the NEWTON polygon. Because of condition (2.2), in order to see that $(m, v(c_m))$ is also a *vertex* of the NEWTON polygon it only remains to show that the polygon does not have a final infinite segment of slope $-v(\alpha)$. Suppose that this were the case. Then f is not a polynomial, and for every $i > m$, there exists $j > i$ such that the vertical distance from $(j, v(c_j))$ to this line is less than or equal to the vertical distance from $(i, v(c_i))$ to the line. That is,

$$\begin{array}{rcc} v(c_j) - [-v(\alpha)(j-m) + v(c_m)] & \leq & v(c_i) - [-v(\alpha)(i-m) + v(c_m)] \\ \Leftrightarrow \quad v(c_j) + jv(\alpha) - mv(\alpha) & \leq & v(c_i) + iv(\alpha) - mv(\alpha) \\ \Leftrightarrow \quad v(c_j\alpha^j) & \leq & v(c_i\alpha^i) \\ \Leftrightarrow \quad |c_j|r^j & \geq & |c_i|r^i, \end{array}$$

which is not possible since for arbitrarily large $i > m$, we have that $|c_i|r^i \neq 0$ (since f is not a polynomial in the case under study) and $\lim_{t\to\infty} |c_t|r^t = 0$.

We conclude that $(n, v(c_n))$ and $(m, v(c_m))$ are in fact vertices of the NEWTON polygon of f, so that precisely $(m - n)$ roots of f have norm r.

Conversely, supposing the existence of a greatest m and a least n such that

$$|c_m|r^m = |c_n|r^n = \max_{i\geq 0}\{|c_i|r^i\},$$

where $m > n$, then since there exists $\gamma \in K$ such that $|\gamma| = r$ (as the disc $\overline{D}_r(0)$ is rational) the above discussion with $v(\alpha)$ replaced by $v(\gamma)$ suffices to show that $(n, v(c_n))$ and $(m, v(c_m))$ are vertices of the NEWTON polygon of f, and there thus exist $m-n$ roots of f with norm r. □

Observation: Suppose that $f = \sum_{i=0}^{\infty} c_i(z-a)^i$ is a non-zero power series with coefficients in K which converges in some closed rational disc $\overline{D}_r(a)$ about some $a \in K$. Then it is clear from the roots theorem that there exists $\alpha \in K$ with $f(\alpha) = 0$ and $|\alpha - a| = r$ if and only if there exist $m, n \in \mathbb{N}, m > n$ with

$$|c_m|r^m = |c_n|r^n = \max_{i\geq 0}\{|c_i|r^i\}.$$

The number of such roots on $C_r(a) := \{z \in K : |z-a| = r\}$ can be calculated as in the theorem.

Corollary 2.2 *If* $f = \sum_{i=0}^{\infty} c_i(z-a)^i \in K[[z]]$ *is a power series converging in some disc* $D_w(a)$ *and* $r \in |K^*|$ *has* $0 < r < w$, *then*
(a) $r' = \max_{i\geq 1}\{|c_i|r^i\}$ *exists and is attained by* f *on* $\overline{D}_r(a)$ *(i.e. there is some* $\alpha \in \overline{D}_r(a)$ *such that* $|f(\alpha) - c_0| = r'$*);* $d = \max\{i \geq 1 : |c_i|r^i = r'\}$ *also exists, and*
(b) f *is a* d*-to-one mapping of* $\overline{D}_r(a)$ *onto* $\overline{D}_{r'}(c_0)$.

Proof:
(a) From the convergence of f on $\overline{D}_r(a)$, we know that r' and d are finite. Now suppose that $\gamma \in K$ has $|\gamma| = r'$.
Then let $g(z) = f(z) - c_0 - \gamma = \sum_{i=1}^{\infty} c_i(z-a)^i - \gamma$. We can write $g(z) = \sum_{i=0}^{\infty} b_i(z-a)^i$ where we let $c_i = b_i$ for each $i > 0$, and $-\gamma = b_0$. But then $\max_{i\geq 0}\{|b_i|r^i\} = \max_{i\geq 1}\{r', |c_i|r^i\}$ is attained for indices 0 and d : indeed, $|\gamma| = |b_0|r^0 = |b_d|r^d = r'$. From the roots theorem we thus know that there exists $\alpha \in K$ for which $|\alpha - a| = r$ and $g(\alpha) = 0$. But then $f(\alpha) - c_0 = \gamma$. i.e. $|f(\alpha) - c_0| = r'$, so that r' is attained.

(b)For any $z \in \overline{D}_r(a)$, then

$$\begin{aligned} |f(z) - c_0| &= |\sum_{i=1}^{\infty} c_i(z-a)^i| \\ &\leq \max_{i\geq 1}\{|c_i||z-a|^i\} \\ &\leq \max_{i\geq 1}\{|c_i|r^i\} = r', \end{aligned}$$

so that $f(\overline{D}_r(a)) \subseteq \overline{D}_{r'}(c_0)$.

Now pick any $y \in \overline{D}_{r'}(c_0)$. If $|y - c_0| = r'$, then we have seen in (a) that precisely d points of $C_r(a) = \{z \in K : |z-a| = r\}$ map to y.

Thus let $|y - c_0| < r'$, and define

$$g_y(z) := f(z) - y = \sum_{i=1}^{\infty} c_i(z-a)^i + c_0 - y.$$

Define $t := |y - c_0|$. WLOG we can suppose that $t > 0$, since otherwise we pick $b \in \overline{D}_r(a)$ such that $f(b) \neq c_0$, express f as a power series about b, and then consider $|y - f(b)|$ instead. (Recall that $\overline{D}_r(a) = \overline{D}_r(b)$.) Now as s ranges over all real numbers between r and 0, from the continuity of the functions $|c_i|s^i$, we know that $\max_{i\geq 1}\{|c_i|s^i\}$ ranges from

r' to 0. Thus, there exists $s_t \in (0,r)$ such that $t = \max_{i\geq 1}\{|c_i|s_t^i\}$. Let $d(t) = \max\{i \geq 1 : |c_i|s_t^i = t\}$. Clearly, $d(t) \leq d$, (since otherwise, if $|c_{d+i}|s_t^{d+i} \geq |c_d|s_t^d$ for some $i > 0$, then $|c_{d+i}| \geq |c_d|s_t^{-i}$ so that because $s_t < r$,

$$|c_{d+i}|r^{d+i} \geq |c_d|s_t^{-i}r^{d+i} = |c_d|r^d\left(\frac{r}{s_t}\right)^i > |c_d|r^d;$$

a contradiction).

Now observe that $s_t \in |K^*|$, since for some i, $|c_i|s_t^i = |y - c_0|$, so s_t is the norm of a root of $x^i - \frac{y-c_0}{c_i}$, which exists in K as it is algebraically closed. Then $\max_{j\geq 1}\{|y-c_0|, |c_j|s_t^j\} = t = |y-c_0| = |c_{d(t)}|s_t^{d(t)}$, so from the roots theorem, g_y has precisely $d(t)$ roots on $C_{s_t}(a)$. i.e. at least $d(t)$ points of $\overline{D}_r(a)$ are mapped to y, so that if $d(t) = d$, then we are done.

Otherwise (for $d(t) < d$), consider the expression $\max_{j\geq 1}\{|c_j|s^j\}$ for s decreasing from r to 0. From the continuity of each function $|c_j|s^j$, for d (which corresponds to the radius r) to drop to $d(t)$, if $d(t) \leq d - m_0$ then there must exist some $s_0 \in (0,r)$ such that $|c_{d-m_0}|s_0^{d-m_0} = |c_d|s_0^d$ for some maximal m_0 in $\{1,2,\ldots,d-1\}$, and for each $s < s_0$, and $0 \leq i < m_0$, then $|c_{d-m_0}|s^{d-m_0} > |c_{d-i}|s^{d-i}$.

Continuing inductively, we find $s_1 \in (0,s_0)$ such that $|c_{d-m_1}|s_1^{d-m_1} = |c_{d-m_0}|s_1^{d-m_0}$ for maximal m_1 in $m_0+1,\ldots,d-1$ and $|c_{d-m_1}|s^{d-m_1} > |c_{d-i}|s^{d-i}$ for $s < s_1$ and $0 \leq i < m_1$; and so on, until we have identified $s_0, s_1, \ldots, s_k$ in $\mathbb{R}$ and $m_0, m_1, \ldots, m_k$ in $\mathbb{N}$ such that $k \leq d-1$; $r > s_0 > s_1 > \ldots > s_k > 0$; $0 < m_0 < m_1 < \ldots < m_k < d$ and $|c_{d-m_i}|s_i^{d-m_i} = |c_{d-m_{i-1}}|s_i^{d-m_{i-1}}$ for each $i \in \{0,1,\ldots,k\}$. By construction, these s_i are points in $(0,r)$ at which the indices $d(s') = \max\{i \geq 1 : |c_i|s^i = s'\}$ drop by $m_i - m_{i-1}$ for $i > 0$ and by m_0 for s_0. Thus, if l is maximal such that $t = |y-c_0|$ has $|c_{d-m_{l+1}}|s_{l+1}^{d-m_{l+1}} < t \leq |c_{d-m_l}|s_l^{d-m_l}$, then $d(t) = d - m_0 - \sum_{i=1}^{l}(m_i - m_{i-1}) = d - m_l$. Now by the choice of maximal m_j at every step, if we consider $\max_{j\geq 1}\{|y-c_0|, |c_j|s_i^j\}$ for fixed i with $i \leq l$, the maximum will be assumed for indices $d - m_{i-1}$ and $d - m_i$. Thus, from the roots theorem, $d - m_{i-1} - (d - m_i) = m_i - m_{i-1}$ is the number of points of $C_{s_i}(a)$ which are mapped to y. Tallying up the total number of roots on such circles gives $m_0 + (m_1 - m_0) + \cdots + (m_l - m_{l-1}) = m_l$ points which are mapped to y. Together with the $d(t)$ points on $C_{s_t}(a)$ which have image y, there are thus at least $d = d(t) + m_l$ points in the pre-image of y.

We now need to see that our counting includes all possible pre-images of a given point. So suppose again that $|y-c_0| = t$, and let $z_0 \in \overline{D}_r(a)$ be a pre-image of y under f. Then g_y has a root on $C_{|z_0-a|}(a)$. From the roots theorem, there is more than one index for

which $\max_{i\geq 1}\{|y-c_0|, |c_i||z_0-a|^i\}$ is assumed. Thus, unless $|z_0-a| = s_t$ (for s_t as defined above), we must have that $|z_0 - a| = s_i$ for some $i \in \{0, 1, \ldots, k\}$. Hence, as asserted, f is a d-to-one mapping of $\overline{D}_r(a)$ onto $\overline{D}_{r'}(c_0)$. □

Throughout, our discussion will focus on dynamical systems where the underlying set is an algebraic variety or a subset thereof. We thus begin by fixing some relevant notation. We denote the scheme $\mathrm{Proj}K[x_0, \ldots, x_n]$ by $\mathbb{P}^n_K$, and its set of K-rational points by $\mathbb{P}^n(K)$. (The latter are the closed points of the scheme, which can be thought of as the set of all equivalence classes of $(n+1)$-tuples of elements of K, not all of which are zero, determined up to multiplication by a non-zero constant.)

When considering the K-rational points of the projective line $\mathbb{P}^1_K$ over the normed field $(K, |\cdot|)$, throughout we make the following identification:

$$\mathbb{P}^1(K) := \{[a:1] : a \in K\} \cup \{[1:0]\} = K \cup \infty.$$

Thereby we identify any $x \in K$ with the point $[x:1] \in \mathbb{P}^1(K)$.

Much of our work will focus on the dynamics of rational maps of projective spaces. Recall that a *rational map* $\phi : \mathbb{P}^n_K \to \mathbb{P}^n_K$ is a mapping which is determined by the action of a set of $(n+1)$ homogeneous polynomials of the same degree (say $\phi_0, \ldots, \phi_n$) on the elements $x_0, \ldots, x_n$. This induces a mapping of homogeneous co-ordinates for $\mathbb{P}^n(K)$ as follows: $\phi([x_0 : \ldots : x_n]) = [\phi_0(x_0, \ldots, x_n) : \ldots : \phi_n(x_0, \ldots, x_n)]$. $(\mathbb{P}^n(K), \phi)$ is then typical of the discrete dynamical systems which will be of interest to us.

Given a rational map $\phi : \mathbb{P}^1_K \to \mathbb{P}^1_K$, suppose that its action on $\mathbb{P}^1(K)$ can be defined by $\phi([x_0 : x_1]) = [\phi_0(x_0, x_1) : \phi_1(x_0, x_1)]$, where ϕ_0 and ϕ_1 are homogeneous polynomials of the same degree. Then, for $x \in K$, we have $\phi([x:1]) = [\phi_0(x,1) : \phi_1(x,1)]$ and this is the same as $\left[\dfrac{\phi_0(x,1)}{\phi_1(x,1)} : 1\right] =: [\phi(x) : 1]$ provided that $\phi_1(x,1) \neq 0$. ϕ can thus be viewed as a rational function in $K(z)$ defined everywhere on K except for possibly finitely many poles.

Our interest in power series is based on their providing a local description of the action of rational maps on $\mathbb{P}^1(K)$, as the following lemma illustrates:

Lemma 2.2 *If $(K, |\cdot|)$ is a non-archimedean valued field and $\phi(z) \in K(z)$ is a rational function, then ϕ has a power series expansion about any element of any disc on which it has no poles.*

Proof: Suppose that D is some disc of radius r which does not contain any poles of ϕ, and that $a \in D$ is arbitrary but fixed.

If $\phi(z) = \frac{g(z)}{h(z)}$, then $h(z) \neq 0$ for each $z \in D$ - in particular, $h(a) \neq 0$, so that if $h(z) = a_0 + a_1(z-a) + \cdots + a_n(z-a)^n$, then $a_0 \neq 0$. If h is constant, we are done, so suppose that the degree of h is at least 1. Then there exists some maximal $s > 0$ such that $|a_0| > |a_i||z-a|^i$ for all $z \in D_s(a)$ and for all $i \geq 1$. (i.e. s is the least real number for which $|a_0| = |a_j|s^j$ for some $j \geq 1$.) If D is a closed disc, then were r to be greater than or equal to s, from the roots theorem it would follow that h has a root in D; and if D is an open disc, then were r to be greater than s, this same conclusion would be reached. In either case then, $|a_0| > |a_i||z-a|^i$ for all $z \in D$ and for every $i \in \{1, \ldots, n\}$. From ultrametricity it then follows that $|a_1(z-a) + \cdots + a_n(z-a)^n| < |a_0|$. But then

$$\frac{|a_1(z-a) + \cdots + a_n(z-a)^n|}{|a_0|} < 1$$

for each $z \in D$. Now it is well known that if $|t| < 1$, then $\sum_{i=0}^{\infty} t^i = \frac{1}{1-t}$, so since

$$\frac{1}{h(z)} = \left(\frac{1}{a_0}\right)\left[\frac{1}{1 + \frac{a_1(z-a)+\cdots+a_n(z-a)^n}{a_0}}\right],$$

in fact

$$\frac{1}{h(z)} = \left(\frac{1}{a_0}\right)\sum_{i=0}^{\infty}\left[-\frac{a_1}{a_0}(z-a) - \cdots - \frac{a_n}{a_0}(z-a)^n\right]^i.$$

Multiplying this power series by $g(z)$ expanded about a yields the required power series expression for ϕ. □

Observation

If K is an algebraically closed field equipped with a non-trivial rank one valuation v, then $|K|$ is dense in $\mathbb{R}^+ \cup \{0\}$.

Proof: Suppose that $\alpha \in K$ has $|\alpha| \neq 0$ and $|\alpha| \neq 1$. (Such an element exists since the valuation is non-trivial.) Now for each n and l, $x^n - \alpha^l$ has a root in K, for every $l \in \mathbb{Z}$ and for all $n \in \mathbb{N}$ so if one such root is β, then $|\beta^n| = |\alpha^l|$, implying that $|\alpha|^{\frac{l}{n}} \in |K|$, for every $l, n \in \mathbb{Z}$ - i.e. $|\alpha|^r \in |K|$, for every $r \in \mathbb{Q}$.

Since $\mathbb{Q}$ is dense in $\mathbb{R}$, the set $|\alpha|^{\mathbb{Q}} \cup |\frac{1}{\alpha}|^{\mathbb{Q}}$ is dense in $\mathbb{R}^+$. Because we have shown that $|\alpha|^{\mathbb{Q}} \cup |\frac{1}{\alpha}|^{\mathbb{Q}} \subset |K|$, it then follows that $|K|$ is dense in $\mathbb{R}^+ \cup \{0\}$. □

Lemma 2.3 *If the power series* $f(z) = \sum_{i=0}^{\infty} c_i(z-a)^i \in K[[z]]$ *maps:*
(a) $\overline{D}_r(a)$ *d-to-one onto itself for* $d > 1$, *then* $\overline{D}_r(a)$ *contains precisely* d *fixed points of* f.
(b) $\overline{D}_r(a)$ *onto some disc* $\overline{D}_{r'}(a)$ *which properly contains it, then* $\overline{D}_r(a)$ *contains at least one fixed point of* f.

Proof: (a) Let $h(z) = f(z) - z = c_0 - a + (c_1 - 1)(z-a) + \sum_{i=2}^{\infty} c_i(z-a)^i$ and observe that $|h(z)| \leq r$ for every $z \in \overline{D}_r(a)$. Thus h is a mapping of $\overline{D}_r(a)$ into $\overline{D}_s(0)$ for some $s \leq r$. From Corollary 2.2(b), $d = \max\{i \geq 1 : |c_i|r^i = r\}$, so since $d > 1$, writing $h(z) = \sum_{i=0}^{\infty} b_i z^i$ where we set $b_0 = c_0 - a$; $b_1 = c_1 - 1$; and $b_i = c_i$ for every $i \geq 2$, then

$$d_h := \max\{i \geq 1 : |b_i|r^i = r\}$$

is the same as d. But then h is a d-fold mapping of $\overline{D}_r(a)$ onto some disc contained in $\overline{D}_r(0)$.

We claim that $0 \in h(\overline{D}_r(a))$.

If $|c_0 - a| = 0$, then this is clearly the case because $f(a) = c_0$.

Otherwise, since $|b_1| = |c_1 - 1| \leq \max\{|c_1|, 1\}$, it follows that $|b_1| \leq 1$ because $|c_1|r \leq r$ and hence $\max_{i\geq 1}\{|b_i|r^i\} = \max_{i\geq 1}\{|c_i|r^i\} = r = |c_d|r^d$, with $d > 1$. Thus, as in Corollary 2.2(b) we know that because $\max_{i\geq 1}\{|b_i|s^i\}$ ranges from r to 0 as s varies from r to 0, the continuity of the functions $|b_i|s^i$ for $s \in (0, r]$ ensures that if $0 < |c_0 - a| = t \leq r$, we can find $s_t \in (0, r]$ such that $\max\{|b_i|s_t^i\} = t$. But then, $\max_{i\geq 1}\{|c_0 - a|, |b_i|s_t^i\}$ is assumed for $|c_0 - a|$ and for some $|b_j|s_t^j$ with $j \geq 1$. From the roots theorem, h thus has a root on $C_{s_t}(a)$. But then $0 \in h(\overline{D}_r(a))$ as claimed.

Hence, some disc containing 0 is the d-fold image of $\overline{D}_r(a)$ under h from (b) of Corollary 2.2. This means that h has exactly d roots in $\overline{D}_r(a)$, and these are precisely the fixed points of f.

(b) Again let $h(z) = f(z) - z$, and again observe that $d_h = d = \max\{i \geq 1 : |b_i|r^i = r'\}$ because $d > 1$ as above. Now if $|c_0 - a| = 0$ then we are done, so suppose that $|c_0 - a| > 0$. Since $|c_0 - a| \leq r'$, as in (a) we know that we can find $s_t \in (0, r]$ such that $|c_0 - a| = \max_{i\geq 1}\{|b_i|s_t^i\}$ and h will then have a root on $C_{s_t}(a)$. □

Another interesting and related result which we shall require is the following:

Lemma 2.4 *If $\phi(z) \in K[z]$ is a non-constant polynomial and $\overline{D}_r(x) \subset K$ is any closed rational disc, then the pre-image of $\overline{D}_r(x)$ under ϕ is a finite union $D_1 \cup \ldots \cup D_\nu$ of closed rational discs, each of which maps m_i-to-one onto $\overline{D}_r(x)$ under the action of ϕ for some $m_i \geq 1$ for every $i \in \{1, \ldots, \nu\}$.*

Proof: Supposing that $0 \in \overline{D}_r(x)$, we aim firstly to construct discs about each of the roots of ϕ, which are mapped onto $\overline{D}_r(0)$. If $\alpha_0 \in K$ is a root of ϕ and $\deg \phi = d$ then we write $\phi(z) = \sum_{i=1}^{d} a_i(z - \alpha_0)^i$. We know from the continuity of the functions $|a_i|t^i$, and the fact that their values range from 0 to arbitrarily large as t varies in $[0, \infty)$, that there exists $t_0 \in (0, \infty)$ such that $\max_{1 \leq i \leq d}\{|a_i|t_0^i\} = r$. (Observe that since K is algebraically closed and $r \in |K|$, also $t_0 \in |K|$). Now consider $\overline{D}_{t_0}(\alpha_0)$: any $z \in \overline{D}_{t_0}(\alpha_0)$ has

$$|\phi(z)| = |\sum_{i=1}^{d} a_i(z - \alpha_0)^i| \leq \max_{1 \leq i \leq d}\{|a_i|t_0^i\} = r,$$

so that $\phi(\overline{D}_{t_0}(\alpha_0)) \subset \overline{D}_r(0)$. Moreover, given any $z_0 \in C_r(0)$, there exists $x_0 \in C_{t_0}(\alpha_0)$ such that $\phi(x_0) = z_0$ from the roots theorem: $\max_{1 \leq i \leq d}\{r, |a_i|t_0^i\} = r = |a_j|t_0^j$ for some j, so $\phi(z) - z_0 = -z_0 + \sum_{i=1}^{d} a_i(z - \alpha_0)^i$ has a root on $C_{t_0}(\alpha_0)$. Hence, with $\phi(\overline{D}_{t_0}(\alpha_0))$ being a disc and $C_r(0) \subset \phi(\overline{D}_{t_0}(\alpha_0))$, in fact $\phi(\overline{D}_{t_0}(\alpha_0)) = \overline{D}_r(0)$.

From the above together with Corollary 2.2, repeating this procedure for each root of ϕ yields a number (say ν) of disjoint, closed rational discs, each of which is mapped m_i-to-one onto $\overline{D}_r(0)$ for $m_i \geq 1$ for every $i \in \{1, \ldots, \nu\}$.

Now suppose that $z \in \overline{D}_r(0)$ has a pre-image under ϕ which is not in any of the discs D_i for $i \in \{1, \ldots, \nu\}$. Then the degree of ϕ must exceed $\sum_{i=1}^{\nu} m_i$. But then 0 also has more pre-images than $\sum_{i=1}^{\nu} m_i$ which implies that some root of ϕ is not in any of these discs. This absurdity proves that indeed, $\phi^{-1}(\overline{D}_r(0)) = D_1 \cup \ldots \cup D_\nu$.

Now suppose that $0 \notin \overline{D}_r(x)$. The mapping $\chi(z) := z + x$ is clearly a bijection of $\overline{D}_r(0)$ onto $\overline{D}_r(x)$, so the pre-image of $\overline{D}_r(0)$ under $\psi(z) := \phi \circ \chi(z)$ is equal to the pre-image of $\overline{D}_r(x)$ under ϕ. But ψ is a polynomial, so from what was shown above, we know that also in this case, the pre-image of $\overline{D}_r(x)$ under ϕ is the union of a finite number of closed rational discs, each of which is mapped m_i-to-one onto $\overline{D}_r(x)$ for some $m_i \geq 1$. □

Chapter 3

Julia and Fatou sets in non-archimedean dynamics

3.1 Dynamics and the derivative

One would expect that the derivative, being a local measure of the rate of change of a function, should have an important part to play in the study of dynamical systems. It is thus not altogether surprising that the derivative provides a valuable classification of all fixed and periodic points of those discrete dynamical systems in which the notion of "limit" is admissible. This classification is intimately related to the behaviour under iteration of points which are "close enough" to these fixed or periodic points.

Definition 3.1 *If $(K, |\cdot|)$ is a complete normed field and $(\mathbb{P}^1(K), \phi)$ is a discrete dynamical system, then the* multiplier *of a periodic point $x \in K \subset \mathbb{P}^1(K)$ of ϕ of exact period n (i.e. $\phi^n(x) = x$ and $\phi^m(x) \neq x$ for every $m < n$) is $(\phi^n)'(x)$.*
In particular, the multiplier of a fixed point x_0 of ϕ is $\phi'(x_0)$.
A periodic point of ϕ is:
super-attracting *if its multiplier has zero norm;*
attracting *if its multiplier has norm less than 1;*
neutral *if its multiplier is a unit;*
repelling *if its multiplier has norm greater than 1.*

To motivate this classification and to emphasize important dynamical properties of polynomials and rational functions, we state and prove certain interesting lemmas which will also be required at a later stage. Throughout, assume that (K, v) is an algebraically closed, complete, non-archimedean valued field.

Firstly observe that for polynomials, the denomination "non-repelling" is apt in describing fixed points with multipliers that are less than or equal to 1, since we have the following

Lemma 3.1 *If $\psi(z) \in K[z]$ is a polynomial of degree at least two, which has a finite, non-repelling fixed point x, then there exists a unique $r \in |K^*|$ such that $\psi(\overline{D}_r(x)) = \overline{D}_r(x)$ and $\psi : \overline{D}_r(x) \to \overline{D}_r(x)$ is m-to-one for some $m \geq 2$. Moreover, for every $t > r$, $\psi(\overline{D}_t(x))$ properly contains $\overline{D}_t(x)$.*

Proof: Let $\psi(z) = x + \sum_{i=1}^{d} c_i(z-x)^i$ where $d \geq 2$ is the degree of ψ. Observe that $\psi'(x) = c_1$, so since x is a non-repelling fixed point, $|c_1| \leq 1$. Also, from Corollary 2.2, for every $t \in \mathbb{R}$, $\psi(\overline{D}_t(x))$ is a (rational) closed disc, and because $\psi(x) = x$, $x \in \psi(\overline{D}_t(x))$. Thus, either $\overline{D}_t(x) \subset \psi(\overline{D}_t(x))$ or $\psi(\overline{D}_t(x)) \subset \overline{D}_t(x)$.

We carry out the proof along the following lines: firstly we show that the set $A := \{t \in \mathbb{R} : \psi(\overline{D}_t(x)) \supsetneq \overline{D}_t(x)\}$ is not empty, so we can define $r = \inf A$. We then prove that $r > 0$ and subsequently that $\inf A$ can be characterized in terms of the coefficients of ψ. In the process of doing so, we show that if $s < r$, then either $\psi(\overline{D}_s(x)) \subsetneq \overline{D}_s(x)$ or $\psi(\overline{D}_s(x)) = \overline{D}_s(x)$ but ψ is injective on this disc. Making further use of this characterization of r, we proceed to demonstrate that ψ is an m-to-one mapping of $\overline{D}_r(x)$ onto itself where $m \geq 2$. Finally we only need show that each $t > r$ is in A to complete the proof.

Firstly then, we show that for sufficiently large t, $\psi(\overline{D}_t(x)) \supsetneq \overline{D}_t(x)$:
for $z \in C_t(x) = \{z \in K : |z - x| = t\}$, we have that

$$|\psi(z) - x| = |\sum_{i=1}^{d} c_i(z-x)^i| \leq \max_{1 \leq i \leq d}\{|c_i|t^i\}.$$

Now from ultrametricity, because $|c_d|t^d > |c_i|t^i$ for all $1 \leq i < d$, if t is sufficiently large (so that $t^d \gg t^i$ for $1 \leq i < d$), in fact $|\psi(z) - x| = |c_d|t^d$. Thus if t is chosen so that both $|c_d|t^d > |c_i|t^i$ for all $1 \leq i < d$ and $|c_d|t^d > t$, then $\psi(\overline{D}_t(x)) \supsetneq \overline{D}_t(x)$.

Now it is meaningful to set $r = \inf\{t \in \mathbb{R} : \psi(\overline{D}_t(x)) \supsetneq \overline{D}_t(x)\}$. We prove that $r > 0$, by showing that for *all* positive s sufficiently small, $\overline{D}_s(x) \supseteq \psi(\overline{D}_s(x))$:
if $c_1 = 0$ and j is the least index for which $c_j \neq 0$, then $s \in \mathbb{R}$ can be chosen with $0 < s \ll 1$ so that $\max_{1 \leq i \leq d}\{|c_i|s^i\} = |c_j|s^j > |c_i|s^i$ for $d \geq i > j$. If $|c_j| < 1$, then it is clear that $|c_j|s^j < s$. This is also the case when $|c_j| \geq 1$, since we can choose $s < \frac{1}{|c_j|}$. Thus, in both cases, the image of $\overline{D}_s(x)$ is a disc of radius strictly less than s, from Corollary 2.2. It is evident that if $s_1 \in \mathbb{R}$ has $0 < s_1 < s$, then also $|c_j|s_1^j > |c_i|s_1^i$ for every

i with $j < i \leq d$. A similar argument to that for s then shows that $\overline{D}_{s_1}(x) \supseteq \psi(\overline{D}_{s_1}(x))$, and hence that $r > 0$ in this case.

On the other hand, if $c_1 \neq 0$, then if $s \in \mathbb{R}$ with $0 < s \ll 1$ is small enough, it follows that $\max_{1\leq i\leq d}\{|c_i|s^i\} = |c_1|s > |c_i|s^i$ for $d \geq i > 1$. But then, again applying Corollary 2.2, it is clear that $\overline{D}_s(x) \supseteq \psi(\overline{D}_s(x))$, since $|c_1| \leq 1$ so that $\max_{1\leq i\leq d}\{|c_i|s^i\} \leq s$. Now if $s_1 \in \mathbb{R}$ has $0 < s_1 < s$, then also $|c_1|s_1 > |c_i|s_1^i$ for every i with $1 < i \leq d$, so that again, $\overline{D}_{s_1}(x) \supseteq \psi(\overline{D}_{s_1}(x))$, and hence, $r > 0$.

Our next task is to give the promised characterization of r in terms of the coefficients of ψ. We thus define

$$r' = \min\{\frac{1}{|c_2|}, \frac{1}{\sqrt{|c_3|}}, \ldots, \frac{1}{\sqrt[i-1]{|c_i|}}, \ldots, \frac{1}{\sqrt[d-1]{|c_d|}}\}, \tag{3.1}$$

and set about proving that $r' = \inf A = r$. Firstly observe, though, that

$$s' := \max_{2\leq i\leq d}\{|c_i|r'^i\} = r'.$$

(Indeed, if $s' = |c_i|r'^i$, and $r' = \frac{1}{\sqrt[j-1]{|c_j|}}$, then we can show that $|c_j|r'^j \geq |c_i|r'^i$: since $\frac{1}{\sqrt[i-1]{|c_i|}} \geq \frac{1}{\sqrt[j-1]{|c_j|}}$, we have that $|c_i| \leq |c_j|^{\frac{i-1}{j-1}}$. Hence $-|c_i|.|c_j|^{\frac{-i}{j-1}} \geq -|c_j|^{\frac{-1}{j-1}}$ and as a result,

$$\begin{aligned} |c_j|r'^j - |c_i|r'^i &= |c_j|.|c_j|^{\frac{-j}{j-1}} - |c_i|.|c_j|^{\frac{-i}{j-1}} \\ &= |c_j|^{\frac{-1}{j-1}} - |c_i|.|c_j|^{\frac{-i}{j-1}} \\ &\geq |c_j|^{\frac{-1}{j-1}} - |c_j|^{\frac{-1}{j-1}} = 0. \end{aligned}$$

Hence,

$$s' = |c_j|r'^j = \frac{|c_j|}{\left(\sqrt[j-1]{|c_j|}\right)^j} = |c_j|^{\frac{-1}{j-1}} = r'.)$$

But then, since $|c_1| \leq 1$, $\max_{1\leq i\leq d}\{|c_i|r'^i\} = r'$.

In showing that $r' = r$, the first step is to see that r' is a lower bound for $A := \{t \in \mathbb{R} : \psi(\overline{D}_t(x)) \supsetneq \overline{D}_t(x)\}$.

If we take any $z \in \overline{D}_{r'}(x)$, then

$$\begin{aligned} |\psi(z) - x| &= |\sum_{i=1}^{d} c_i(z-x)^i| \\ &\leq \max_{1\leq i\leq d}\{|c_i||z-x|^i\} \\ &\leq \max_{1\leq i\leq d}\{|c_i|r'^i\} = r', \end{aligned}$$

so that $\psi(\overline{D}_{r'}(x)) \subset \overline{D}_{r'}(x)$. Now let $s < r'$, say $s = r' - \delta$ for some $\delta > 0$. Then, from the definition of r', we know that $r' - \delta < \frac{1}{\sqrt[i-1]{|c_i|}}$ for every $i \in \{2, \ldots, d\}$. Thus, $|c_i|(r' - \delta)^{i-1} < 1$ and this implies that $|c_i|(r' - \delta)^i < (r' - \delta)$ for every $i \in \{2, \ldots, d\}$. Now since $|c_1| \leq 1$, also $|c_1|(r' - \delta) \leq (r' - \delta)$, and consequently

$$\begin{aligned} |\psi(z) - x| &= |\sum_{i=1}^{d} c_i(z - x)^i| \\ &\leq \max_{1 \leq i \leq d}\{|c_i|(r' - \delta)^i\} \\ &\leq r' - \delta = s, \quad \text{for every } z \in \overline{D}_s(x). \end{aligned}$$

i.e. $\psi(\overline{D}_s(x)) \subset \overline{D}_s(x)$ for each s with $0 < s < r'$. This means that r' is a strict lower bound for A. (That is, if $t \in \mathbb{R}$ has $\psi(\overline{D}_t(x)) \supsetneq \overline{D}_t(x)$, then $t > r'$.)

Notice here that with $0 < s < r'$ and $z \in \overline{D}_s(x)$, $|\psi(z) - x| = s$ if and only if $|c_1| = 1$ (so that $|c_1|s = s = \max_{1 \leq i \leq d}\{|c_i|s^i\} > |c_j|s^j$ for every $j > 1$.) Thus, $\psi(\overline{D}_s(x))$ is properly contained in $\overline{D}_s(x)$ unless the index corresponding to the maximum of $\{|c_i|s^i : 1 \leq i \leq d\}$ is 1, in which case ψ maps $\overline{D}_s(x)$ 1-to-1 onto itself from Corollary 2.2. This fact will give the uniqueness of r with the stated properties, once we have shown that $r' = r$ and ψ maps $\overline{D}_{r'}(x)$ multiply-to-one onto itself but each disc $\overline{D}_t(x)$ with $t > r$ is properly contained in $\psi(\overline{D}_t(x))$.

Not only is r' a lower bound for A, but it also has the infinum property. In order to see this, let $\zeta > 0$ be given such that $r' + \zeta \in |K^*|$. There exists at least one j such that $r' + \zeta > \frac{1}{\sqrt[j-1]{|c_j|}}$ from the definition of r', and for this j, we thus have that $|c_j|(r' + \zeta)^{j-1} > 1$, implying that $|c_j|(r' + \zeta)^j > r' + \zeta$. Since $|c_1|(r' + \zeta) \leq r' + \zeta$, then $\max_{1 \leq i \leq d}\{|c_i|(r' + \zeta)^i\} = \max_{2 \leq i \leq d}\{|c_i|(r' + \zeta)^i\} > r' + \zeta$. Now by Corollary 2.2(b), $\psi(\overline{D}_{r'+\zeta}(x)) = \overline{D}_{r_1}(x)$ where $r_1 = \max_{1 \leq i \leq d}\{|c_i|(r' + \zeta)^i\} > r' + \zeta$. Thus $r' + \zeta \in A$. From the density of $|K^*|$ in $\mathbb{R}^+$, it then follows that given any $\varepsilon > 0$, there exists some $\zeta > 0$ with $\zeta \leq \varepsilon$ for which $r' + \zeta \in A$. Because r' is also a lower bound for A, we have that $r' = \inf A = r$ as claimed.

We would next like to see that ψ is an m-fold mapping of $\overline{D}_r(x)$ onto itself, for some $m \geq 2$. We have already seen that $\psi(\overline{D}_{r'}(x)) \subset \overline{D}_{r'}(x)$ - i.e. $\psi(\overline{D}_r(x)) \subset \overline{D}_r(x)$. Recall that the image of $\overline{D}_r(x)$ under ψ is a rational closed disc from Lemma 2.2. We proceed to show that there are points of the disc which are mapped to the circle $C_r(x)$: suppose that $\psi(\overline{D}_r(x)) \subsetneq \overline{D}_r(x)$. From the above discussion, we know that for almost all $\varepsilon > 0$ (all of those $\varepsilon > 0$ such that there is no root of $\psi(z) - x$ on $C_{r+\varepsilon}(x)$), then

$\overline{D}_{r+\varepsilon}(x) \subsetneq \psi(\overline{D}_{r+\varepsilon}(x))$, so that in particular, $\overline{D}_r(x) \subset \psi(\overline{D}_{r+\varepsilon}(x))$ for all such $\varepsilon > 0$. Let ε_0 be such a positive number. Thus if $z_0 \in C_r(x)$, then there exists $y \in C_{r+\zeta}(x)$ for some $0 < \zeta \leq \varepsilon_0$ such that $\psi(y) = z_0$, where ζ being positive is a consequence of the supposition that $\psi(\overline{D}_r(x)) \subsetneq \overline{D}_r(x)$. This means that on $C_{r+\zeta}(x)$, there is a root y to $\psi(z) - z_0 = x - z_0 + \sum_{i=1}^{d} c_i(z-x)^i$. However, we saw that $|c_i|(r+\zeta)^i > r + \zeta$ for some $i \in \{2, \ldots, d\}$. Thus, $\max_{1\leq i\leq d}\{|x - z_0|, |c_i|(r+\zeta)^i\} = \max_{1\leq i\leq d}\{|c_i|(r+\zeta)^i\}$. From the roots theorem, the maximum corresponds to two distinct indices $m > n$. But then if we consider $\psi(z) - x$ and the expression $\max_{1\leq i\leq d}\{|c_i|(r+\zeta)^i\}$ it follows from the roots theorem that $\psi(y_0) - x = 0$ for some $y_0 \in C_{r+\zeta}(x)$. Again applying the density of $|K|$ in $\mathbb{R}^+ \cup \{0\}$ it is evident that we would be able to find infinitely many roots of $\psi(z) - x$: we pick $\varepsilon_1 \in \mathbb{R}$ with $0 < \varepsilon_1 < \zeta$ and repeat the argument to obtain $0 < \zeta_1 \leq \varepsilon_1$ such that a root of $\psi(z) - x$ lies on $C_{r+\zeta_1}(x)$, and so on, choosing $0 < \varepsilon_2 < \zeta_1$. This is clearly a contradiction of the finiteness of the number of roots of $\psi(z) - x$, so in fact $(\overline{D_r(x)}) \subseteq \psi(\overline{D_r(x)})$.

We have thus seen that ψ maps $\overline{D_r(x)}$ m-to-one to itself (applying Corollary 2.2 to what has been shown above). Here $m \geq 2$ from the proof of Corollary 2.2: m corresponds to the maximum index for which $\max_{1\leq i\leq d}\{|c_i|r^i\}$ is attained, and we know from the definition of r' that this index is at least two.

It remains to be seen that $A = \{t \in \mathbb{R} : t > r\}$. Pick any $\varepsilon > 0$. Then unless there exists a root to $\psi(z) - x$ on $C_{r+\varepsilon}(x)$, we know that $\psi(\overline{D}_{r+\varepsilon}(x)) \supsetneq \overline{D}_{r+\varepsilon}(x)$. Now suppose that $r + \varepsilon$ is a radius for which there exist roots of $\psi(z) - x$ on $C_{r+\varepsilon}(x)$.

We claim that for some $j \in \{2, \ldots, d\}$, there exists $\eta_j \in \mathbb{R}$ with $0 < \eta_j < \varepsilon$ such that for every $\alpha \in \mathbb{R}$ with $0 < \alpha < \eta_j$, then $|c_j|(r + \varepsilon - \alpha)^j > r + \varepsilon$. In proving this claim, observe that the functions $f_j(s) := |c_j|(r + \varepsilon - s)^j$ are continous and decreasing, so that because $f_j(0) > r + \varepsilon$ for some j as shown above, $f_j(0) = \lim_{s\to 0^+} f_j(s) > r + \varepsilon$. Now for each $\delta > 0$, there exists some $\eta_\delta > 0$ such that for all $s < \eta_\delta$, then $f_j(0) - f_j(s) < \delta$. Choose $\delta < f_j(0) - (r + \varepsilon)$. Then for $s < \eta_\delta := \eta_j$, $(f_j(s) - (r + \varepsilon)) > 0$ since otherwise, $f_j(0) - (r + \varepsilon) = f_j(0) - f_j(s) + f_j(s) - (r + \varepsilon) < \delta$. Thus $|c_j|(r + \varepsilon - s)^j > (r + \varepsilon)$ for all $s < \eta_j$.

Now for some $\alpha \in \mathbb{R}$ with $0 < \alpha < \eta_j$ we must have that $\max_{2\leq i\leq d}\{|c_i|(r + \varepsilon - \alpha)^i\} = \max_{1\leq i\leq d}\{|c_i|(r + \varepsilon - \alpha)^i\}$ is assumed for a single index, (as otherwise from the roots theorem there would have to be a root of $\psi(z) - x$ on $C_{r+\varepsilon-\alpha}(x)$, but there are only

finitely many roots of this polynomial whereas infinitely many $\alpha \in \mathbb{R}$ with $0 < \alpha < \eta$ and $(r + \varepsilon - \alpha) \in |K|$ exist from the density of $|K|$ in $\mathbb{R}^+ \cup \{0\}$). But then from ultrametricity, $|\psi(z) - x| = \max_{1 \leq i \leq d}\{|c_i|(r + \varepsilon - \alpha)^i\} > r + \varepsilon$ for all $z \in C_{r+\varepsilon-\alpha}(x)$. Hence, $\psi(\overline{D}_{r+\varepsilon}(x)) \supsetneq \overline{D}_{r+\varepsilon}(x)$. □

Bearing Corollary 2.2 in mind, the next lemma shows that iterates of points which are sufficiently close to an attracting fixed point of a power series map are indeed drawn to the attracting point under iteration:

Lemma 3.2 *If x_0 is an attracting fixed point of $\phi(z) \in K(z)$, a rational function which maps some open disc containing x_0, namely W, into itself, then for all $z \in W$, $\phi^n(z) \to x_0$ as $n \to \infty$.*

Proof: Let $W = D_r(x_0)$ and for $z \in W$, write $\phi(z) = x_0 + \sum_{i=1}^{\infty} c_i(z - x_0)^i$, where the power series converges since ϕ is well-defined on W. This means that $\max_{i \geq 1}\{|c_i||z - x_0|^i\}$ corresponds to a finite maximum index, for every $z \in W$. We firstly show that for each point z of W, $|\phi(z) - x_0| < |z - x_0|$, and then by a contradiction argument demonstrate that this is sufficient for the result to follow.

From the convergence of $\phi(z)$ on W it is clear that if s is sufficiently small ($0 < s \ll 1$), $\max_{i \geq 1}\{|c_i|s^i\} = |c_1|s > |c_j|s^j$ for every $j > 1$. Now owing to the continuity of the functions $|c_i|s^i$ as s increases from zero in $(0, r]$, there exists $s_0 > 0$ such that $|c_1|s_0 = |c_{i_0}|s_0^{i_0} = \max_{i \geq 1}\{|c_i|s^i\}$, for some $i_0 > 1$, and for every $s \in (0, s_0)$, $|c_1|s > |c_i|s^i$ whenever $i > 1$. Since x_0 is attracting, $|\phi'(x_0)| = |c_1| < 1$. This is why $|\phi(z) - x_0| < |z - x_0|$ for every $z \in \overline{D}_{s_0}(x_0)$: indeed,

$$\begin{aligned} |\phi(z) - x_0| &= |\sum_{i=1}^{\infty} c_i(z - x_0)^i| \\ &\leq \max_{i \geq 1}\{|c_i||z - x_0|^i\} = |c_1||z - x_0| < |z - x_0|. \end{aligned}$$

Now consider $z \in W \backslash \overline{D}_{s_0}(x_0)$ should r be greater than s_0. From the convergence of the power series expansion about x_0, there exists $L \in \mathbb{N}$ such that for every $i > L$ and for all $z \in W$, $\quad |c_i||z - x_0|^i < s_0$.

Let $M = \max\{2, L\}$. Then $|\sum_{i=M+1}^{N} c_i(z - x_0)^i| < s_0$ for every $N \in \mathbb{N}$ which is greater than M by ultrametricity and hence, $|\sum_{i=M+1}^{\infty} c_i(z - x_0)^i| \leq s_0$. Now define $\phi_M(z)$ to be the Mth partial sum of ϕ:

$$\phi_M(z) := \phi(z) - \sum_{i=M+1}^{\infty} c_i(z - x_0)^i = x_0 + \sum_{i=1}^{M} c_i(z - x_0)^i.$$

Let r_M denote the radius associated to ϕ_M under Lemma 3.1 - i.e., ϕ_M maps $\overline{D}_{r_M}(x_0)$ multiply-to-one onto itself and for all $r_0 > r_M$, $\phi(\overline{D}_{r_0}(x_0))$ properly contains $\overline{D}_{r_0}(x_0)$. Suppose that the radius r of W exceeds r_M. Then there exists $z_0 \in W$ (with $|z_0 - x_0| > r_M$) for which $|\phi_M(z_0) - x_0| \geq r$. (Should the contrary hold, then for any $z \in C_r(x_0)$ for which $|\phi_M(z) - x_0| > r$, there exists a sequence $(z_n)_{n\in\mathbb{N}}$ with limit z such that $z_n \in C_{r-\eta_n}(x_0)$ for every $n \in \mathbb{N}$ where $(\eta_n)_{n\in\mathbb{N}}$ is a strictly decreasing sequence of real numbers with limit 0 and for which $(r - \eta_n) \in |K|$ for every $n \in \mathbb{N}$, since K is both algebraically closed and complete. But then, $z_n \to z$ as $n \to \infty$ although we are assuming that $|\phi_M(z_n) - x_0| < r$ for every $n \in \mathbb{N}$ whereas $|\phi_M(z) - x_0| > r$. This contradicts the continuity of the polynomial map [1] ϕ_M.) But then for such a z_0, we would have that

$$\begin{aligned} |\phi(z_0) - x_0| &= \max\{|\phi_M(z_0) - x_0|, |\sum_{i=M+1}^{\infty} c_i(z_0 - x_0)^i|\} \\ &= |\phi_M(z_0) - x_0| \geq r, \end{aligned}$$

contradicting the fact that $\phi(W) \subset W$. Thus $r \leq r_M$. But then, for every $z \in W$, $|\phi_M(z) - x_0| < |z - x_0|$: indeed, with $|z - x_0| < r_M$, as in the proof of Lemma 3.1, $|z - x_0| < \frac{1}{\sqrt[i-1]{|c_i|}}$ for every $i \in \{2, \ldots, M\}$. This implies that $|c_i||z - x_0|^i < |z - x_0|$ for every $i \in \{2, \ldots, M\}$. Now since also $|c_1||z - x_0| < |z - x_0|$, we have that $|\phi_M(z) - x_0| \leq \max_{1\leq i\leq M}\{|c_i||z - x_0|^i\} < |z - x_0|$.

Because, for arbitrary $z \in W$, $|\phi(z) - x_0| \leq \max\{|\phi_M(z) - x_0|, |\sum_{i=M+1}^{\infty} c_i(z - x_0)^i|\}$ where $|\phi_M(z) - x_0| < |z - x_0|$ and $|\sum_{i=M+1}^{\infty} c_i(z - x_0)^i| \leq s_0$, it is true that $|\phi(z) - x_0| < |z - x_0|$ for all $z \in W \backslash \overline{D}_{s_0}(x_0)$.

We conclude the proof by the contradiction argument mentioned above: Suppose that some $z_0 \in W$ has iterates which never reach some closed disc $D := \overline{D}_{s_1}(x_0)$ of radius $s_1 < r$. Then since $(|\phi^n(z_0) - x_0|)_{n\in\mathbb{N}}$ is a strictly decreasing sequence (as shown above), which is bounded below by s_1, it has a limit, say $t \geq s_1$. Now consider the action of ϕ on $\overline{D}_t(x_0)$: from Lemma 2.3, we know that this image is also a closed disc, and from what has already been shown, with x_0 being a fixed point of ϕ, it is a disc about x_0 of radius strictly less than t, say it is t_0. Now pick any $t_1 \in (t_0, t) \cap |K|$. From Lemma 2.4, we know that $W \cap \phi^{-1}(D_{t_1}(x_0)$ is an open disc about x_0, of radius greater than t. But then

[1] The continuity of power series maps and hence also of polynomial maps in this setting follows from Corollary 2.2: any power series $\Upsilon(z) = \sum_{\mu=0}^{\infty} \upsilon_\mu z^\mu$ maps a given disc $\overline{D}_{r_0}(x_0)$ into some other disc of radius $r_1 = \max_{\mu>0}\{|\upsilon_\mu| r_0^\mu\}$. Thus, by choosing points sufficiently close to a given point, the images of the points can be made to lie in a disc of radius which is arbitrarily small.

the iterate of some iterate of z_0 is in $D_{t_1}(x_0)$, which is strictly contained in $\overline{D}_t(x_0)$. This is a contradiction, so in fact, the iterates of z_0 eventually end up in D, and as a result the limit of the sequence $(|\phi^n(z_0) - x_0|)_{n\in\mathbb{N}}$ is zero, and the iterates of z_0 thus *do* tend to x_0□

Other dynamical information pertaining to a given map can be unravelled by following the iterates of critical points (i.e., the zeros of the derivative). In complex dynamics, to each attracting periodic cycle of a polynomial map there corresponds some critical point which has iterates that tend to the periodic cycle. (See DEVANEY, [4], page 281.) In non-archimedean dynamics, a similar result which we shall need in a subsequent chapter, is true:

Lemma 3.3 *In the situation of Lemma 3.1, if m is not divisible by $char(\overline{K})$, then the disc $\overline{D_r}(x)$ contains a critical point of ψ.*

Proof: Again write $\psi(z) = x + \sum_{i=1}^{d} c_i(z-x)^i$. Then $\psi'(z) = \sum_{i=1}^{d} ic_i(z-x)^{i-1}$. Clearly

$$|m| = \underbrace{|1 + \cdots + 1|}_{m \text{ times}} \leq 1.$$

But at the same time $\overline{char(K)} \nmid m$, implying that $\overline{m} = m + \mathcal{M}_K \neq 0 + \mathcal{M}_K$ - i.e. $|m| \geq 1$. Thus in fact, $|m| = 1$. Now from the proofs of Corollary 2.2 and Lemma 3.1, we also know that m is the largest of the indices i such that $r = \frac{1}{\sqrt[i-1]{|c_i|}}$. (Recall that $r = \min\{\frac{1}{|c_2|}, \ldots, \frac{1}{\sqrt[i-1]{|c_i|}}, \ldots, \frac{1}{\sqrt[d-1]{|c_d|}}\}$.)

Now for $s \in (0, r]$, consider $M(s) := \max_{1\leq i\leq d}\{|ic_i|s^{i-1}\}$. Since x is a non-repelling fixed point, $|c_1| \leq 1$ and thus,

$$M(r) \geq |m||c_m| \left(\frac{1}{\sqrt[m-1]{|c_m|}}\right)^{m-1} = |m| = 1 \geq |c_1|.$$

For $s \in \mathbb{R}$ with $0 < s \ll 1$, $M(s) = |c_1|$. Now if $|c_1| = M(r)$ then the maximum corresponds to more than one index because $m > 1$, implying that there is a root of ψ' on $C_r(x)$ by the roots theorem. On the other hand, when $M(r) > |c_1|$, the highest index corresponding to the maximum $M(r)$ is greater than 1. But then, as in the proof of Corollary 2.2, the fact of $M(s) = |c_1|$ for sufficiently small s, together with the continuity of the functions $|kc_k|t^{k-1}$ of t, implies that there exists some $s_0 \in (0, r)$ such that $|ic_i|s_0^{i-1} = |jc_j|s_0^{j-1} = M(s_0)$, for some i, j with $d \geq i > j \geq 1$. Hence, from the roots theorem there is a root of ψ' on $C_{s_0}(x)$. □

3.2 Defining the JULIA and FATOU sets

In a monumental paper, *Mémoire sur l'itération des fonctions rationelles* pulished in 1918 when he was 25, GASTON JULIA gave a complete characterization of those points of the complex plane which do not tend to infinity under iteration of a rational function. Like any exceptional theorem, this characterization gave rise to a new mathematical definition, and the boundary of the set of points which JULIA identified now bears his name. However, JULIA worked with the notion of normality, in which compact sets are fundamental. In spaces such as (Ω_p, v_p) which are not locally compact, (i.e. not every point has a neighbourhood base consisting of compact sets), a definition of the JULIA set using normality is not very user-friendly. Instead, we make use of equicontinuity, which is equivalent to normality by the Theorem of ARZELA and ASCOLI.

Definition 3.2 *If (X, d_X) and (Y, d_Y) are metric spaces then a family of functions $G = \{g : X \to Y\}$ is* equicontinous *on X if there exists some $C > 0$ such that for every $x_0, x_1 \in X$ and for every $g \in G$, then $d_Y(g(x_0), g(x_1)) \leq C d_X(x_0, x_1)$.*

We are now in a position to precisely define the JULIA and FATOU sets of a given dynamical map.

Definition 3.3 *If (X, d_X) is a metric space and (X, ϕ) is a dynamical system, then denoting the restriction of ϕ^n to $S \subset X$ by $\phi^n|_S$ for each $n \in \mathbb{N}$, the* FATOU *set of ϕ is*

$$\mathcal{F}_\phi = \{x \in X : \{\phi^n|_U\}_{n\in\mathbb{N}} \text{is equicontinuous, where } U \text{ is some open neighbourhood of } x\}.$$

The JULIA *set of ϕ is $\mathcal{J}_\phi = X \backslash \mathcal{F}_\phi$, the complement of the* FATOU *set.*

For a given non-archimedean valued field (K, v), the metric on $\mathbb{P}^n(K)$ which is of interest to us is the *chordal* or *spherical* metric. On $\mathbb{P}^1(K)$, this is defined precisely in analogy to the spherical metric on the RIEMANN sphere $\mathbb{P}^1(\mathbb{C})$, which is determined from embedding $\mathbb{P}^1(\mathbb{C})$ in $\mathbb{R}^3$ and subsequently measuring the distances between points along the surface of the $\mathbb{R}^3$-sphere which is obtained. i.e. if $x^{(0)} = [x_0^{(0)} : x_1^{(0)}]$ and $x^{(1)} = [x_0^{(1)} : x_1^{(1)}] \in \mathbb{P}^1(K)$ and $|\cdot|$ is the norm arising from v, then we set

$$\|x^{(0)}, x^{(1)}\| = \frac{|x_0^{(0)} x_1^{(1)} - x_0^{(1)} x_1^{(0)}|}{\max\{|x_0^{(0)}|, |x_1^{(0)}|\} \max\{|x_0^{(1)}|, |x_1^{(1)}|\}}.$$

Notice that if $x^{(0)}, x^{(1)} \in \overline{D}_1(0)$, then we can write $x^{(i)} = [z_i : 1]$ where $|z_i| \leq 1$ for $i \in \{0, 1\}$, so that $\|x^{(0)}, x^{(1)}\| = |z_0 - z_1|$, which means that the spherical metric concurs with the norm from v, on the valuation ring.

More generally on $\mathbb{P}^n$ we have:

Definition 3.4 *If* $x^{(0)} = [x_0^{(0)} : \ldots : x_n^{(0)}]$ *and* $x^{(1)} = [x_0^{(1)} : \ldots : x_n^{(1)}] \in \mathbb{P}^n(K)$ *and* $|\cdot|$ *is the norm on* K *arising from* v*, then the chordal distance between* $x^{(0)}$ *and* $x^{(1)}$ *is:*

$$\|x^{(0)}, x^{(1)}\| = \frac{\max_{0 \leq i < j \leq n}\{|x_i^{(0)} x_j^{(1)} - x_i^{(1)} x_j^{(0)}|\}}{\max_{0 \leq \nu \leq n}\{|x_\nu^{(0)}|\} \ \max_{0 \leq \mu \leq n}\{|x_\mu^{(1)}|\}}.$$

3.3 Changing co-ordinates

If (K, v) is a non-archimedean valued field and $\phi : \mathbb{P}^n_K \to \mathbb{P}^n_K$ is a rational map, then for any automorphism f of $\mathbb{P}^n_K$, $\psi := f^{-1} \circ \phi \circ f$ is a rational map which exhibits the same dynamical behaviour as ϕ, but with respect to the co-ordinate change $x \mapsto f^{-1}(x)$: indeed if x_0 is a periodic point of ϕ, then $f^{-1}(x_0)$ is a periodic point of ψ because $\psi^m = f^{-1} \circ \phi^m \circ f$ for each $m \in \mathbb{N}$. Moreover, if $n = 1$ and x is fixed by ϕ, then

$$\begin{aligned}
|\psi'(f^{-1}(x))| &= |(f^{-1} \circ \phi \circ f)'(f^{-1}(x))| \\
&= |(f^{-1})'(\phi \circ f \circ f^{-1}(x))\phi'(f \circ f^{-1}(x))f'(f^{-1}(x))| \\
&= |(f^{-1})'(\phi(x))||\phi'(x)||f'(f^{-1}(x))| \\
&= |(f^{-1})'(x)||\phi'(x)||f'(f^{-1}(x))| \qquad \text{since } \phi(x) = x.
\end{aligned}$$

Because f and f^{-1} are inverse functions, in fact

$$|(f^{-1})'(x)| = \left|\frac{1}{f'(f^{-1}(x))}\right|,$$

and thus $|\psi'(f^{-1}(x))| = |\phi'(x)|$. Consequently, multipliers of fixed points (and similarly of periodic points) are preserved under these co-ordinate changes in the case of the projective line.

The automorphism group of $\mathbb{P}^n(K)$ is the matrix group $PGL(n+1, K)$, the projective general linear space of $n+1$ dimensions over K. This is because, to be injective, such morphisms must be linear, and for the action of a matrix group to be well-defined on projective n-space over K, it is necessary to identify any matrix A with λA for any $\lambda \in K^*$. (i.e. the group must be a *projective* linear space.)

For the frequent changes of co-ordinate we shall be employing to be meaningful, we also require that they do not affect the metrics we use. As is shown in [17], the chordal metric on $\mathbb{P}^n(K)$ is invariant under the action of $PGL(n+1, K)$.

3.4 Properties of the JULIA and FATOU sets in $\mathbb{P}^1(K)$

To give some flesh to the stark definitions stated above, we derive certain facts about the JULIA and FATOU sets of rational maps over $\mathbb{P}^1(K)$. After reinforcing the intuitive understanding of the FATOU set outlined in the introduction, in seeing that non-repelling fixed points belong to this set, we show that the FATOU set can never be empty in the non-archimedean situation. This is not true of the JULIA set, as we proceed to demonstrate.

From the definitions, one might expect that the JULIA and FATOU sets are the forward and backward iterates of themselves, a property which we prove carefully here, besides showing the rather more startling fact, (also true in complex dynamics), that the FATOU set of a map is identical to the FATOU set of any iterate of the map.

In what follows, let (K, v) be a complete non-archimedean valued field, and $\phi : \mathbb{P}^1_K \to \mathbb{P}^1_K$ be some rational map.

Proposition 3.1 *Any non-repelling fixed point of ϕ is in $\mathcal{F}_\phi$, whereas each repelling fixed point of ϕ is in $\mathcal{J}_\phi$.*

Proof: By a change of coordinates if necessary, we may assume that 0 is the fixed point of ϕ which is under discussion.

Suppose firstly that 0 is non-repelling. Thus, when by Lemma 2.2, in some sufficiently small disc $\overline{D}_r(0)$ we express ϕ as a power series $\phi(z) = \sum_{i=1}^{\infty} c_i z^i$, we have that $|\phi'(0)| = |c_1| \leq 1$, and as a result $r > 0$ can be chosen small enough to ensure that $|c_i| r^{i-1} \leq 1$ for every $i \geq 1$, with $r < 1$. But then from the agreement of the spherical metric with the norm from the valuation v, on $\overline{D}_r(0) \subset \overline{D}_1(0)$, we need only use the latter norm in investigating the equicontinuity of $\{\phi^n\}_{n\in\mathbb{N}}$ on $\overline{D}_r(0)$.

Let $x, y \in \overline{D}_r(0)$ be arbitrary. Then

$$\begin{aligned} |\phi(x) - \phi(y)| &= |\sum_{i=1}^{\infty} c_i (x^i - y^i)| \\ &= |x - y| |\sum_{i=1}^{\infty} \sum_{j=1}^{i-1} c_i x^{i-1-j} y^j| \end{aligned}$$

$$\begin{aligned} |\phi(x) - \phi(y)| &\leq |x-y| \max_{i\geq 1}\{|\sum_{j=1}^{i-1} c_i x^{i-1-j} y^j|\} \\ &\quad \text{from ultrametricity, since the series converges} \\ &\leq |x-y| \text{ from the choice of } r. \end{aligned}$$

$\{\phi^n\}_{n\in\mathbb{N}}$ is thus an equicontinous family on $\overline{D}_r(0)$, so $0 \in \mathcal{F}_\phi$.

In the case of a repelling fixed point, any power series expansion for ϕ in a sufficiently small disc $\overline{D}_s(0) \subsetneq \overline{D}_1(0)$, say $\phi(z) = \sum_{i=1}^{\infty} a_i z^i$, will have $|\phi'(0)| = |a_1| > 1$. Suppose now that even though this is the case, $0 \in \mathcal{F}_\phi$. Then there exists some open set V containing 0, on which $\{\phi^n\}_{n\in\mathbb{N}}$ is an equicontinous family. Let $\overline{D}_t(0)$ be a disc which is contained in both V and $\overline{D}_s(0)$ (which exists from the density of $|K|$ in $\mathbb{R}^+ \cup \{0\}$), and for which the radius is small enough so that $\max_{i\geq 1}\{|a_i|t^i\} = |a_1|t > |a_j|t^j$ for every $j > 1$. Now for each $y \in \overline{D}_t(0)$, $|\phi(y)| = |a_1 y|$ by ultrametricity. We proceed to show that every $y \in \overline{D}_s(0)$ where $0 < s < \dfrac{t}{|a_1^m|}$, satisfies $|\phi^m(y)| = |a_1^m y|$, from which a contradiction will follow: the image of y under ϕ is also in $\overline{D}_t(0)$ since $|\phi(y)| = |a_1 y| < \dfrac{|a_1|t}{|a_1^m|} < t$ (because $|a_1| > 1$). But then $|\phi(\phi(y))| = |a_1\phi(y)| = |a_1^2 y|$ and it is clear that by continuing inductively, in fact $|\phi^m(y)| = |a_1^m y|$ as claimed.

Consequently, if $C > 0$ were to be the constant of equicontinuity, so that

$$|a_1^m y| = |\phi^m(y)| = |\phi^m(y) - \phi^m(0)| \leq C|y - 0| = C|y|,$$

then we would have that $|a_1^m| \leq |C|$ for each $m \in \mathbb{N}$. Since $|a_1| > 1$, this is a contradiction. □

Proposition 3.2 *Denoting the multipliers of the fixed points of ϕ by λ_i for $i \in \{1, \ldots, n\}$, and supposing that $\lambda_i \notin \{0, 1\}$ for every i, then*

$$\sum_{i=1}^{n} \frac{1}{1-\lambda_i} = 1.$$

Proof: By means of a change of coordinates if necessary, we can assume that $\phi(z) = \frac{f(z)}{g(z)}$ where deg $g(z) \geq$ deg $f(z)$. Let $x_1, \ldots, x_n$ be the fixed points of ϕ. These are the roots of $zg(z) - f(z)$, and because $1 \neq \lambda_i = \phi'(x_i)$ for every $i \in \{1, \ldots, n\}$, they are all distinct: the roots of $\phi(z) - z$ are then not repeated. Since deg $f(z) <$ deg $zg(z)$, if a is the leading coefficient of $g(z)$ we can write $zg(z) - f(z) = a\prod_{i=1}^{n}(z - x_i) := a\psi(z)$, say. Now

observe that $\lambda_i = \phi'(x_i) = \dfrac{f'(x_i)}{g(x_i)} - \dfrac{f(x_i)g'(x_i)}{[g(x_i)]^2}$. Because $x_i g(x_i) = f(x_i)$ for each i, we have $\lambda_i = \dfrac{f'(x_i) - x_i g'(x_i)}{g(x_i)}$, so that with $a\psi'(z) = zg'(z) + g(z) - f'(z)$, we know that

$$\lambda_i = \frac{g(x_i) - a\psi'(x_i)}{g(x_i)} = 1 - \frac{a\psi'(x_i)}{g(x_i)}. \tag{3.2}$$

Consider, for any polynomial $u(z)$ of degree less than n, the polynomial $h(z) = u(z) - \sum_{i=1}^{n} \frac{u(x_i)}{\psi'(x_i)} \prod_{j \neq i} (z - x_i)$. The degree of $h(z)$ is also less than n, yet this polynomial has n distinct roots. It must therefore vanish identically so that $u(z) = \sum_{i=1}^{n} \frac{u(x_i)}{\psi'(x_i)} \prod_{j \neq i} (z - x_i)$ for any such polynomial $u(z)$. Thus, with deg $\frac{g(z)}{a} < n$, from (3.2) we can write

$$\frac{g(z)}{a} = \sum_{i=1}^{n} \frac{\psi'(x_i)}{1 - \lambda_i} \frac{1}{\psi'(x_i)} \prod_{j \neq i} (z - x_i) = \sum_{i=1}^{n} \frac{1}{1 - \lambda_i} \prod_{j \neq i} (z - x_i).$$

Comparing leading coefficients on both sides yields the desired identity. □

Corollary 3.1 $\mathcal{F}_\phi \neq \emptyset$.

Proof: If ϕ has a fixed point which is either super-attracting or neutral, then such a point is in the FATOU set of ϕ from Proposition 3.1. Supposing that ϕ has no such fixed point, we can apply Proposition 3.2, since then the multipliers λ_i (with notation as in Proposition 3.2) of the fixed points of ϕ are neither 0 nor 1. If we assume that each such fixed point is in $\mathcal{J}_\phi$, then by Proposition 3.1 each multiplier has $|\lambda_i| > 1$, so that $|1 - \lambda_i| > 1$. But then $|\sum_{i=1}^{n} \frac{1}{1-\lambda_i}| \leq \max\{|\frac{1}{1-\lambda_i}|\} < 1$, contradicting Proposition 3.2. □

Lemma 3.4 *There exists $C \geq 1$ such that given any $x^{(0)}, x^{(1)} \in \mathbb{P}^1(K)$, then*

$$\|\phi(x^{(0)}), \phi(x^{(1)})\| \leq C \|x^{(0)}, x^{(1)}\|.$$

Proof: For any $a, b \in \mathbb{P}^1(K)$, then $\|a, b\| \leq 1$, since if $a = [a_0 : a_1]$ and $b = [b_0 : b_1]$ then

$$\|a, b\| = \frac{|a_0 b_1 - b_0 a_1|}{\max\{|a_0|, |a_1|\} \max\{|b_0|, |b_1|\}} \leq \frac{\max\{|a_0|, |a_1|\} \max\{|b_0|, |b_1|\}}{\max\{|a_0|, |a_1|\} \max\{|b_0|, |b_1|\}}.$$

Thus, whenever $\|x^{(0)}, x^{(1)}\| = 1$, then the statement holds for any $C \geq 1$. Hence, we can suppose that $x^{(0)}$ and $x^{(1)}$ are in the same affine patch of $\mathbb{P}^1(K)$ - i.e., $\|x^{(0)}, x^{(1)}\| < 1$. WLOG suppose that $x^{(0)}, x^{(1)} \in \{x \in \mathbb{P}^1(K) : x = [z : 1] \text{ where } |z| \leq 1\}$. On the open

subset of this affine patch on which ϕ is defined, the map is uniquely determined by homogeneous polynomials $f, g \in \mathcal{O}_K[z]$ of the same degree, where at least one coefficient of f or g is a unit, such that $\phi([z:1]) = [f(z):g(z)]$ Now with ϕ being a rational map, we know that these polynomials share no non-trivial roots on the set on which they define the action of ϕ, and with K being algebraically closed, we can thus assume that they are relatively prime, although the coefficient-wise reduced polynomials may not have this property. Hence there exist $h_f, h_g \in \mathcal{O}_K[z]$ and $\pi \in \mathcal{M}_K \backslash \{0\}$ such that for some $\mu \geq 0$, then

$$h_f(z)f(z) + h_g(z)g(z) = \pi^\mu. \tag{3.3}$$

Suppose that $x^{(i)} = [z_i : 1]$ where $|z_i| \leq 1$ for $i \in \{0, 1\}$. Then we have

$$\|\phi(x^{(0)}), \phi(x^{(1)})\| = \frac{|f(z_0)g(z_1) - g(z_0)f(z_1)|}{\max\{|f(z_0)|, |g(z_0)|\} \max\{|f(z_1)|, |g(z_1)|\}}.$$

Now

$$\begin{array}{rl} & |f(z_0)g(z_1) - g(z_0)f(z_1)| \\ = & |f(z_0)(g(z_1) - g(z_0)) + g(z_0)(f(z_0) - f(z_1))| \\ \leq & \max\{|f(z_0)|, |g(z_0)|\} \max\{|g(z_1) - g(z_0)|, |f(z_0) - f(z_1)|\} \\ \leq & \max\{|f(z_0)|, |g(z_0)|\}|g|_G|f|_G|z_0 - z_1|. \end{array}$$

Moreover, from equation (3.3) we know that

$$\begin{array}{rcl} |\pi^\mu| & = & |h_f(z_1)f(z_1) + h_g(z_1)g(z_1)| \\ & \leq & \max\{|h_f(z_1)|, |h_g(z_1)|\} \max\{|f(z_1)|, |g(z_1)|\} \\ & \leq & \max\{|f(z_1)|, |g(z_1)|\}, \end{array}$$

since the coeffiecients of h_f and h_g are in $\mathcal{O}_K$, and consequently, combining these estimates with the formula for the chordal distance between $\phi(x^{(0)})$ and $\phi(x^{(1)})$, we have that

$$\|\phi(x^{(0)}), \phi(x^{(1)})\| \leq \frac{|f|_G|g|_G|z_0 - z_1|}{|\pi^\mu|}.$$

We let $C = \max\{1, \frac{|f|_G|g|_G}{|\pi^\mu|}\}$ to conclude the proof. □

This interesting result means that whenever $\frac{|f|_G|g|_G}{|\pi^\mu|} \leq 1$, then the JULIA set of ϕ is empty. Although this can never occur in the context of complex dynamics, in our situation it happens at least whenever $|\pi^\mu| = 1$, since f and g have coefficients in $\mathcal{O}_K$. Now $|\pi^\mu| = 1$ implies that the coefficient-wise reduced polynomials $\overline{f}$ and $\overline{g}$ have no common non-trivial roots (a condition which we shall later be terming "good reduction"). This will be the theme of our discussion in Chapter 4, which explores the relationship between good reduction and rational maps and polynomial maps being equicontinuous on their spaces of definition.

The above lemma is helpful in proving that the FATOU and JULIA sets are the forward and backward iterates of themselves:

Proposition 3.3 *$\mathcal{F}_\phi = \phi(\mathcal{F}_\phi) = \phi^{-1}(\mathcal{F}_\phi)$ and $\mathcal{J}_\phi = \phi(\mathcal{J}_\phi) = \phi^{-1}(\mathcal{J}_\phi)$.*

Proof: From the complementarity of the JULIA and FATOU sets, we need only show that the assertion is true for the FATOU set of ϕ. Furthermore, since the statements $\mathcal{F}_\phi \subseteq \phi^{-1}(\mathcal{F}_\phi)$ and $\phi(\mathcal{F}_\phi) \subseteq \mathcal{F}_\phi$ are logically equivalent, it is only necessary to prove that:
(1) $\phi^{-1}(\mathcal{F}_\phi) \subseteq \mathcal{F}_\phi$;
(2) $\mathcal{F}_\phi \subseteq \phi(\mathcal{F}_\phi)$; and
(3) $\phi(\mathcal{F}_\phi) \subseteq (\mathcal{F}_\phi)$.

To see (1), we invoke the Lemma 3.4: if $\omega \in \phi^{-1}(\mathcal{F}_\phi)$, then $\phi(\omega) \in \mathcal{F}_\phi$, so there exists $U \subseteq \mathbb{P}^1(K)$ which is an open neighbourhood of $\phi(\omega)$ such that $\{\phi^n\}_{n\in\mathbb{N}}$ is equicontinuous on U, say with constant of equicontinuity $C_U > 0$. Consider $\phi^{-1}(U)$, which is open owing to the continuity of any rational map on $\mathbb{P}^1(K)$. If $w, v \in \phi^{-1}(U)$, then for each $n \geq 1$, it follows that

$$\begin{aligned} \|\phi^{n+1}(w), \phi^{n+1}(v)\| &\leq C_U \|\phi(w), \phi(v)\| \\ &\leq C C_U \|w, v\| \end{aligned}$$

from the equicontinuity on U and from Lemma 3.4, (where $C > 0$ is as in the lemma). Now let $A = \max\{CC_U, C\}$. Then we have seen that $\|\phi^n(w), \phi^n(v)\| \leq A\|w, v\|$ for each $n \geq 1$. Thus $\{\phi^n\}_{n\in\mathbb{N}}$ is equicontinuous on $\phi^{-1}(U)$, an open set containing ω, so $\omega \in \mathcal{F}_\phi$, proving (1).

(2) is a consequence of the fact that K is algebraically closed, together with (1): indeed, if $\omega \in \mathcal{F}_\phi$, then since ϕ is built up of polynomials with coefficients in K, there exists $x \in \mathbb{P}^1(K)$ such that $\phi(x) - \omega = 0$. From (1), such an x is in $\mathcal{F}_\phi$, being in the pre-image of a point which is FATOU. But then $\omega \in \phi(\mathcal{F}_\phi)$, and we see that $\mathcal{F}_\phi \subseteq \phi(\mathcal{F}_\phi)$.

Finally we show (3): Pick $\omega \in \mathcal{F}_\phi$. Then let $U \subseteq \mathbb{P}^1(K)$ be an open set containing ω on which $\{\phi^n\}_{n\in\mathbb{N}}$ is equicontinuous. U contains some closed rational disc $\overline{D}_s(\omega)$ of sufficiently small radius so that none of the poles of ϕ are in $\overline{D}_s(\omega)$. Then ϕ has an expression as a power series on this disc, and consequently maps it to some other closed rational disc, say $\overline{D}_{s'}(\phi(\omega))$, from Corollary 2.2.
We show that $\{\phi^n\}_{n\in\mathbb{N}}$ is equicontinuous on the open disc $D_{s'}(\phi(\omega))$:
let C_D be a positive number such that for every $x, y \in \overline{D}_s(\omega)$ and for every $n \in \mathbb{N}$, $\|\phi^m(x), \phi^m(y)\| \leq C_D\|x, y\|$. Suppose now that no $T > 0$ exists such that for all $x, y \in$

$\overline{D}_s(\omega)$ and for each $m \in \mathbb{N}$, $\|\phi^{m+1}(x), \phi^{m+1}(y)\| \leq T\|\phi(x), \phi(y)\|$. Then for every $N \in \mathbb{N}$, there exist $x_N, y_N \in \overline{D}_s(\omega)$ and $n_N \in \mathbb{N}$ such that

$$\|\phi^{n_N}(x_N), \phi^{n_N}(y_N)\| > N\|\phi(x_N), \phi(y_N)\|. \tag{3.4}$$

Clearly, $\|\phi(x_N), \phi(y_N)\| \neq 0$ since otherwise $\|\phi^{n_N}(x_N), \phi^{n_N}(y_N)\|$ would also be zero. Because $\|x_N, y_N\| \leq \min\{1, s\}$ for every $x_N, y_N \in \overline{D}_s(\omega)$ (recall that $\overline{D}_s(\omega)$ is not a *chordal* disc) we can choose N sufficiently large so that

$$N\|\phi(x_N), \phi(y_N)\| > C_D\|x_N, y_N\|,$$

for any given $x_N, y_N \in \overline{D}_s(\omega)$. But then from equation (3.4) the equicontinuity of $\{\phi^n\}_{n\in\mathbb{N}}$ is contradicted. Consequently there in fact exists $T > 0$ such that $\|\phi^{m+1}(x), \phi^{m+1}(y)\| \leq T\|\phi(x), \phi(y)\|$ for every $x, y \in \overline{D}_s(\omega)$ and for every $m \in \mathbb{N}$. Thus, given any $u, v \in \overline{D}_{s'}(\phi(\omega)) = \phi(\overline{D}_s(\omega))$, we have that for each $m \in \mathbb{N}$,

$$\|\phi^{m+1}(x), \phi^{m+1}(y)\| \leq T\|\phi(x), \phi(y)\|$$

and $\{\phi^n\}_{n\in\mathbb{N}}$ is thus equicontinuous on $\overline{D}_{s'}(\phi(\omega))$, and in particular on the open set $D_s(\phi(\omega))$. Thus, $\phi(\omega) \in \mathcal{F}_\phi$ implying that (3) is true. □

Again applying Lemma 3.4, we have the following

Proposition 3.4 *$\mathcal{F}_{\phi^n} = \mathcal{F}_\phi$ and $\mathcal{J}_{\phi^n} = \mathcal{J}_\phi$ for every $n \in \mathbb{N}$.*

Proof: These statements are equivalent, so we prove them in one stroke by showing that $\mathcal{F}_{\phi^n} = \mathcal{F}_\phi$. Firstly notice that $\mathcal{F}_\phi \subset \mathcal{F}_{\phi^n}$ from the definition of the FATOU set. Now take any $\omega \in \mathcal{F}_{\phi^n}$ and let $U \subset \mathbb{P}^1(K)$ be any open set containing ω upon which $\{\phi^{rn}\}_{r\in\mathbb{N}}$ is equicontinuous. U then contains some open chordal disc, say D, containing ω, such that for some $C_D > 0$, $\|\phi^{rn}(x), \phi^{rn}(y)\| \leq C_D\|x, y\|$ for all $x, y \in D$, for every $r \in \mathbb{N}$.

Consider the morphisms $\{\phi, \ldots, \phi^{n-1}\}$ applied to $\phi^{rn}(D)$: from Lemma 3.4, it is evident that $\|\phi^{rn+i}(x), \phi^{rn+i}(y)\| \leq C^i C_D\|x, y\|$ for all $x, y \in D$, for every $r \in \mathbb{N}$ and for each $i \in \{1, \ldots, n-1\}$, where C is as in the lemma. But since $C \geq 1$, then $\|\phi^{rn+i}(x), \phi^{rn+i}(y)\| \leq C^n C_D\|x, y|$, and the family $\{\phi^{rn+i}\}_{r\in\mathbb{N};i\in\{1,\ldots,n-1\}} = \{\phi^m\}_{m\in\mathbb{N}}$ is thus equicontinuous on D. Consequently, $\omega \in \mathcal{F}_\phi$ and we are done. □

Corollary 3.2 *If x is a periodic point of ϕ which has multiplier λ having $|\lambda| \leq 1$, then $x \in \mathcal{F}_\phi$. Otherwise, $x \in \mathcal{J}_\phi$.*

Proof: x is a fixed point of ϕ^n for some $n \in \mathbb{N}$, and its multiplier is defined in terms of the derivative of the function ϕ^n precisely in the same way as the multiplier of a fixed point of ϕ is defined in terms of the derivative of ϕ itself. Thus, we can apply Proposition 3.1 to see that $x \in \mathcal{F}_{\phi^n}$ whenever $|\lambda| \leq 1$ and $x \in \mathcal{J}_{\phi^n}$ otherwise. The assertion thus follows from the above proposition. □

Chapter 4

Good reduction and equicontinuity

Throughout let (K, v) denote any non-archimedean valued field.

Definition 4.1 *A rational map $\phi : \mathbb{P}^n_K \to \mathbb{P}^n_K$ is said to have* good reduction *at v if it determines a morphism of $\mathbb{P}^n_K$ and with respect to a suitable choice of co-ordinates, the reduced rational map $\tilde{\phi} : \mathbb{P}^n_{\overline{K}} \to \mathbb{P}^n_{\overline{K}}$ is a morphism.*
Any rational map $\psi : \mathbb{P}^n_K \to \mathbb{P}^n_K$ which does not have good reduction at v has bad reduction *at v.*

Thus, a rational map $\phi : \mathbb{P}^n_K \to \mathbb{P}^n_K$ has good reduction if and only if it is a morphism and no points of $\mathbb{P}^n_{\overline{K}} = \text{Proj}\overline{K}[x_0, \ldots, x_n]$ are sent to the ideal generated by $\{x_0, \ldots, x_n\}$ under the action of $\tilde{\phi}$.

An example suffices to demonstrate the co-ordinate dependence of good reduction: for any prime p, the map $\phi(z) = \frac{z^2}{p} : \mathbb{P}^1(\Omega_p) \to \mathbb{P}^1(\Omega_p)$ has "bad reduction" (in the co-ordinate system in which it is written). Now consider the automorphism $f : z \mapsto pz$ of $\mathbb{P}^1(\Omega_p)$. Evidently $f^{-1} \circ \phi \circ f(z) = \frac{1}{p}\left(\frac{p^2 z^2}{p}\right) = z^2$ has good reduction, but represents the same map as ϕ viewed under a co-ordinate change (which, as we saw in Section 3.3 does not change the dynamic behaviour of the map). Thus, any dynamical facts which we derive for maps having "good reduction" will also be valid for maps such as ϕ which have good reduction in some co-ordinate system.

A more explicit characterization of those rational maps $\phi : \mathbb{P}^n_K \to \mathbb{P}^n_K$ having good reduction can be given: indeed, if $\phi_0, \ldots, \phi_n$ are representative homogeneous polynomials for ϕ, then its having good reduction is equivalent to the coefficient-wise reduced polynomials $\tilde{\phi_0}, \ldots, \tilde{\phi_n}$ having no non-trivial root in common. This situation is precisely described by the resultant $\tilde{\mathcal{R}} = Res(\tilde{\phi_0}, \ldots, \tilde{\phi_n})$ of the reduced polynomials being non-zero. Recall

that the resultant of a given system of $n+1$ polynomials in $n+1$ variables is a polynomial in the coefficients of these polynomials which itself has rational integer coefficients, and which vanishes precisely when the $n+1$ polynomials have a common non-trivial root. See Appendix A for a detailed algebraic discussion of the resultant.

In their paper, SILVERMAN and MORTON showed that there is a close link between a rational map being equicontinous and its having good reduction in some co-ordinate system: whenever a rational map $\phi(z) \in K(z)$ has good reduction, its JULIA set is empty. This result is not entirely unexpected in the light of the following

Observation

If (K, v) is a non-archimedean valued field and $\phi : \mathbb{P}^1_K \to \mathbb{P}^1_K$ is a rational map with good reduction, then $\mathbb{P}^1(K)$ can be covered by open unit (chordal) discs each of which is mapped into some other such disc by ϕ.

Proof:

We can express $\mathbb{P}^1(K)$ as $\mathbb{P}^1(K)\backslash\overline{D}_1(0) \cup (\bigcup_{a\in\mathcal{O}_K} D_1(a))$. Now $\mathbb{P}^1(K)\backslash\overline{D}_1(0)$ is an open chordal unit disc, since if $a, b \in \mathbb{P}^1(K)\backslash\overline{D}_1(0)$, then writing $a = [1 : a']$ and $b = [1 : b']$ where $|a'| < 1$ and $|b'| < 1$ we have that

$$\|a, b\| = |a' - b'| \leq \max\{|a|, |b|\} < 1.$$

Because the chordal metric agrees with the metric induced by v on $\overline{D}_1(0)$, each of the sets $D_1(a) \subset \overline{D}_1(0)$ for $a \in \mathcal{O}_K$, is also an open unit chordal disc. Now observe that these discs correspond to equivalence classes of points of $\mathbb{P}^1(K)$ modulo the maximal ideal $\mathcal{M}_K = D_1(0)$:

$$z \in \mathbb{P}^1(K)\backslash\overline{D}_1(0) \Leftrightarrow \overline{z} = \infty \text{ in } \mathbb{P}^1(\overline{K}) = \overline{K} \cup \{\infty\},$$

the projective line over the residue field of K, and for $a \in \mathcal{O}_K$,

$$z \in D_1(a) \Leftrightarrow |z - a| < 1 \Leftrightarrow z - a \in \mathcal{M}_K.$$

If ϕ is a rational map of $\mathbb{P}^1(K)$ to itself having good reduction, then the reduced map $\tilde{\phi} : \mathbb{P}^1(\overline{K}) \to \mathbb{P}^1(\overline{K})$ is well-defined, and ϕ consequently sends any of the discs $\mathbb{P}^1(K)\backslash\overline{D}_1(0)$ or $D_1(a)$ for $a \in \mathcal{O}_K$ to some other such disc. □

This shows that the good reduction of ϕ forces the map to have a strong local property: if $z_0, z_1 \in \mathbb{P}^1(K)$ have $\|z_0, z_1\| < 1$, then also $\|\phi^n(z_0), \phi^n(z_1)\| < 1$ for each $n \in \mathbb{N}$, which is not quite as strong as the equicontinuity of the family $\{\phi^n\}_{n\in\mathbb{N}}$, but corresponds to our

intuitive understanding of the FATOU set being the whole of $\mathbb{P}^1(K)$ since we think of this set as comprising those points whose iterates under ϕ do not move far apart if the original points are close.

MORTON and SILVERMAN in fact show that if K is the quotient field of a DEDEKIND domain, some chosen prime ideal of which determines the non-archimedean valuation with which K is endowed, then no points of $\mathbb{P}^1(K)$ are sent further apart by the action of any map with good reduction. In this chapter we discuss a standard generalization of this result with a view towards better understanding the dynamical behaviour of maps from a given curve to itself via embedding into $\mathbb{P}^n(K)$. We also introduce a non-archimedean MANDELBROT set and in so doing show that quadratic polynomials in $K[z]$ have good reduction in some co-ordinate system if and only if they have empty JULIA set (ignoring the case where $char(\overline{K}) = 2$). BENEDETTO has extensively investigated the question of when a given rational map having empty JULIA set is sufficient to imply that there exists some co-ordinate system in which the map has good reduction, in [2], and we report on his fascinating findings in Section 4.3.

4.1 The Theorem of MORTON and SILVERMAN

Suppose that $(K, |\cdot|)$ is a non-archimedean normed field. We have seen how the chordal metric $\|\cdot,\cdot\|$ is defined on $\mathbb{P}^n(K)$, and in Chapter 2 defined the GAUSS norm on a polynomial ring with coefficients in a normed field.

Now given a rational map $\psi : \mathbb{P}^n_K \to \mathbb{P}^n_K$, there exist homogeneous polynomials of the same degree, $\psi_0, \ldots, \psi_n \in \mathcal{O}_K[x_0, \ldots, x_n]$, for which

$$\max_{0 \leq i \leq n} \{|\psi_i|_G\} = 1$$

and $\psi([x_0 : \ldots : x_n]) = [\psi_0(x_0, \ldots, x_n) : \ldots : \psi_n(x_0, \ldots, x_n)]$. This follows since we can multiply any given representative polynomials for ψ by a suitable constant to obtain that all coefficients of some new set of representative polynomials are in $\mathcal{O}_K$, and at least one such coefficient is a unit. If we moreover require that these representative polynomials have no common factors, then it is clear that they are unique up to multiplication by a unit.

Supposing that $\phi : \mathbb{P}^n_K \to \mathbb{P}^n_K$ is a given rational map, let $\phi_0, \ldots, \phi_n \in \mathcal{O}_K[x_0, \ldots, x_n]$ be such a fixed set of homogeneous representative polynomials for ϕ. Then if $\mathcal{R} =$

$\text{Res}(\phi_0, \ldots, \phi_n)$ is the resultant of these polynomials, we have:

Proposition 4.1 *If* $x^{(0)} = [x_0^{(0)} : \ldots : x_n^{(0)}]$ *and* $x^{(1)} = [x_0^{(1)} : \ldots : x_n^{(1)}] \in \mathbb{P}^n(K)$, *then* $|\mathcal{R}|^2 \|\phi(x^{(0)}), \phi(x^{(1)})\| \leq \|x^{(0)}, x^{(1)}\|$.

Proof:

In Appendix A we show that there exists $\tau \in \mathbb{N}$ such that for all $i \in \{0, \ldots, n\}, x_i^\tau \mathcal{R} \equiv 0 \pmod{\phi_0, \ldots, \phi_n}$. Now since the coefficients of the ϕ_i are fixed, $\mathcal{R} \in \mathcal{O}_K$. Thus, the polynomials $x_i^\tau \mathcal{R}$ are homogeneous, so since the ϕ_i are also all homogeneous, the polynomials $f_i^{(j)} \in \mathcal{O}_K[x_0, \ldots, x_n]$ such that $\sum_{i=0}^{n} f_i^{(j)} \phi_i = x_j^\tau \mathcal{R}$ for each j, must be homogeneous as well and all have the same degree, say d.

We pick homogeneous co-ordinates for $x^{(0)}$ and $x^{(1)}$ such that $\max_{0 \leq j \leq n}\{|x_j^{(i)}|\} = 1$ for $i \in \{0, 1\}$. It then follows that

$$\|x^{(0)}, x^{(1)}\| = \frac{\max_{0 \leq i < j \leq n}\{|x_i^{(0)} x_j^{(1)} - x_j^{(0)} x_i^{(1)}|\}}{\max_{0 \leq \mu \leq n}\{|x_\mu^{(0)}|\} \max_{0 \leq \nu \leq n}\{|x_\nu^{(1)}|\}} = \max_{0 \leq i < j \leq n}\{|x_i^{(0)} x_j^{(1)} - x_j^{(0)} x_i^{(1)}|\}. \quad (4.1)$$

For notational convenience, set

$$|\alpha_0, \ldots, \alpha_r| := \max_{0 \leq i \leq r}\{|\alpha_i|\}$$

where $\alpha_0, \ldots, \alpha_r \in K$, and denote $(x_0^{(i)}, \ldots, x_n^{(i)})$ by $\boldsymbol{x}^{(i)}$ for $i \in \{0, 1\}$.

Then we have $|\mathcal{R}| = |\mathcal{R}||x_0^{(i)}, \ldots, x_n^{(i)}|^\tau$ from the choice of homogeneous co-ordinates for $x^{(0)}$ and $x^{(1)}$. But then for each of $i = 0$ and $i = 1$, it follows that

$$\begin{aligned}
|\mathcal{R}| &= |\mathcal{R}x_0^{(i)\tau}, \ldots, \mathcal{R}x_n^{(i)\tau}| \\
&= |\sum_{k=0}^{n} f_k^{(0)}(\boldsymbol{x}^{(i)})\phi_k(\boldsymbol{x}^{(i)}), \ldots, \sum_{k=0}^{n} f_k^{(n)}(\boldsymbol{x}^{(i)})\phi_k(\boldsymbol{x}^{(i)})| \\
&\leq |f_0^{(0)}(\boldsymbol{x}^{(i)}), \ldots, f_n^{(0)}(\boldsymbol{x}^{(i)}), f_0^{(1)}(\boldsymbol{x}^{(i)}), \ldots, f_n^{(n)}(\boldsymbol{x}^{(i)})||\phi_0(\boldsymbol{x}^{(i)}), \ldots, \phi_n(\boldsymbol{x}^{(i)})| \\
&\quad \text{(from ultrametricity)} \\
&\leq \max_{0 \leq k,j \leq n}\{|f_k^{(j)}|_G\}|\boldsymbol{x}^{(i)}|^d |\phi_0(\boldsymbol{x}^{(i)}), \ldots, \phi_n(\boldsymbol{x}^{(i)})| \text{ where } d \text{ is the degree of } f_i^{(j)} \\
&\leq |\phi_0(\boldsymbol{x}^{(i)}), \ldots, \phi_n(\boldsymbol{x}^{(i)})| \text{ since } f_i^{(j)} \in \mathcal{O}_K[x_0, \ldots, x_n], \text{ for every } i, j \in \{0, \ldots, n\}.
\end{aligned}$$

For each i and j in $\{0, \ldots, n\}$ we now consider the polynomial

$$\begin{aligned}
&\Omega_{i,j}(X_0^{(0)}, \ldots, X_n^{(0)}, X_0^{(1)}, \ldots, X_n^{(1)}) \\
&= \phi_i(X_0^{(0)}, \ldots, X_n^{(0)})\phi_j(X_0^{(1)}, \ldots, X_n^{(1)}) - \phi_j(X_0^{(0)}, \ldots, X_n^{(0)})\phi_i(X_0^{(1)}, \ldots, X_n^{(1)}),
\end{aligned}$$

which is bihomogeneous and vanishes for $[X_0^{(0)}, \ldots, X_n^{(0)}] = [X_0^{(1)}, \ldots, X_n^{(1)}]$ - i.e. for $X_m^{(0)} X_l^{(1)} = X_m^{(1)} X_t^{(0)}$ for any $m, l, t \in \{0, \ldots, n\}$ In particular, these polynomials also

vanish for $t = l$, so that for each i and j in $\{0, \ldots, n\}$ there exists a bihomogeneous polynomial
$\psi_{i,j} \in \mathcal{O}_K[X_0^{(0)}, \ldots, X_n^{(0)}, X_0^{(1)}, \ldots, X_n^{(1)}]$ such that

$$\begin{aligned}&(X_i^{(0)}X_j^{(1)} - X_i^{(1)}X_j^{(0)})\psi_{i,j}(X_0^{(0)}, \ldots, X_n^{(0)}, X_0^{(1)}, \ldots, X_n^{(1)})\\ &= \phi_i(X_0^{(0)}, \ldots, X_n^{(0)})\phi_j(X_0^{(1)}, \ldots, X_n^{(1)}) - \phi_j(X_0^{(0)}, \ldots, X_n^{(0)})\phi_i(X_0^{(1)}, \ldots, X_n^{(1)})\\ &= \Omega_{i,j}(X_0^{(0)}, \ldots, X_n^{(0)}, X_0^{(1)}, \ldots, X_n^{(1)}).\end{aligned}$$

(We know that the coefficients of $\psi_{i,j}$ are in $\mathcal{O}_K$ because of the multiplicativity of the GAUSS norm on $K[X_0^{(0)}, \ldots, X_n^{(0)}, X_0^{(1)}, \ldots, X_n^{(1)}]$.)

But then

$$\begin{aligned}\|x^{(0)}, x^{(1)}\| &= \max_{0\le i\le j\le n}\{|x_i^{(0)}x_j^{(1)} - x_j^{(0)}x_i^{(1)}|\}\\ &\geq \max_{0\le i\le j\le n}\{|\Omega_{i,j}(x_0^{(0)}, \ldots, x_n^{(0)}, x_0^{(1)}, \ldots, x_n^{(1)})|\}\\ &\quad \text{(since the coefficients of } \psi_{i,j} \text{ are in } \mathcal{O}_K)\\ &= \max_{0\le i\le j\le n}\{|\phi_i(\boldsymbol{x}^{(0)})\phi_j(\boldsymbol{x}^{(1)}) - \phi_j(\boldsymbol{x}^{(0)})\phi_i(\boldsymbol{x}^{(1)})|\}\\ &= \|\phi(x^{(0)}), \phi(x^{(1)})\|\ |\phi_0(\boldsymbol{x}^{(0)}), \ldots, \phi_n(\boldsymbol{x}^{(0)})|\ |\phi_0(\boldsymbol{x}^{(1)}), \ldots, \phi_n(\boldsymbol{x}^{(1)})|\\ &\geq \|\phi(x^{(0)}), \phi(x^{(1)})\|\ |\mathcal{R}|^2\end{aligned}$$

since we showed that $|\mathcal{R}| \le \max_{0\le k\le n}\{|\phi_k(\boldsymbol{x}^{(i)})|\}$ for $i \in \{0, 1\}$. □

Theorem 4.1 *If $\phi : \mathbb{P}_K^n \to \mathbb{P}_K^n$ is a rational map which has good reduction, then $\mathcal{J}_\phi = \emptyset$.*

Proof: Let $\phi([x_0 : \ldots : x_n]) = [\phi_0(x_0, \ldots, x_n) : \ldots : \phi_n(x_0, \ldots, x_n)]$ where $\max_{0\le i\le n}\{|\phi_i|_G\} = 1$ as before, and let $\mathcal{R}$ again denote the resultant of $\phi_0, \ldots, \phi_n$. Because $\mathcal{R}$ is a polynomial in the coefficients of $\phi_0, \ldots, \phi_n$, and the reduction of these polynomials is coefficient-wise, the reduction of $\mathcal{R}$, say $\tilde{\mathcal{R}}$, is the resultant of the reduced polynomials $\tilde{\phi_0}, \ldots, \tilde{\phi_n}$. Now since ϕ has good reduction, $\tilde{\mathcal{R}} \neq 0$. But then $\mathcal{R}$ is a unit, and hence $|\mathcal{R}| = 1$.

Thus, from the above proposition, for any $x^{(0)}$ and $x^{(1)} \in \mathbb{P}^n(K)$, we know that

$$\|\phi(x^{(0)}), \phi(x^{(1)})\| \le \frac{1}{|\mathcal{R}|^2}\|x^{(0)}, x^{(1)}\| = \|x^{(0)}, x^{(1)}\|.$$

Hence, $\{\phi^m\}_{m\in\mathbb{N}}$ is an equicontinous family on any open subset of $\mathbb{P}^n(K)$. □

Suppose now that C is a smooth projective curve defined over the non-archimedean valued field (K, v). If $\phi_C : C \to C$ is a map which, via some non-singular embedding $\mu : C \to \mathbb{P}^n(K)$ can be lifted to a rational map $\phi : \mathbb{P}^n(K) \to \mathbb{P}^n(K)$, then what we have shown can shed light on the dynamical system (C, ϕ_C) provided ϕ has good reduction. To

be sure of this, we would need to know that distinct non-singular embeddings of C in projective spaces over K induce equivalent topologies on the image of C in these respective spaces (equipped with spherical metrics arising from the norm on K), since otherwise it is conceivable that different embeddings would render distinct dynamical behaviour on the images of C. The following result, from RUMELY'S text [17, Theorem 1.1.1], gives precisely the information we require for the discussion of metric-related properties of the dynamical system (C, ϕ_C) to be meaningful:

Theorem 4.2 *If C and K are as above and μ and ν are non-singular embeddings of C into $\mathbb{P}^n(K)$ and $\mathbb{P}^m(K)$ respectively, then the spherical metrics on points of $\mu(C)$ and $\nu(C)$ in these respective projective spaces are equivalent.*

A spin-off of Theorem 4.1 is then the following

Corollary 4.1 *If C, K and ϕ_C are as above and $\mu : C \to \mathbb{P}^n(K)$ is a non-singular embedding such that ϕ_C can be lifted to a rational map $\phi : \mathbb{P}^n_K \to \mathbb{P}^n_K$, then whenever ϕ has good reduction, the* JULIA *set of ϕ_C (in the dynamical system (C, ϕ_C)) is empty.*

4.2 The Non-archimedean MANDELBROT Set

In Complex Dynamics, the MANDELBROT set M of a family of parameter-dependent functions $\Lambda = \{f_c : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C}) \mid c \in \mathbb{C}\}$ is defined to be the set of parameter values c for which the iterates $f_c^n(0)$ remain bounded for each $n \in \mathbb{N}$. When reference is made to "the MANDELBROT set," without mention of the family of functions, it is understood that this set is with respect to the family $\{z \mapsto z^2 + c : c \in \mathbb{C}\}$, where z is a parameter at 0.

Since the notion of the iterates of zero remaining bounded is well-defined in the setting of a field equipped with a non-archimedean, rank one valuation, we can investigate an analogously defined set in the context of Non-archimedean Dynamical Systems:

Definition 4.2 *If (K, v) is a non-archimedean valued field, v has rank one, and for $c \in K$ we let $\phi_c(z) = z^2 + c$, then*

$$M := \{c \in K : \ \forall n \in \mathbb{N}, |\phi_c^n(0)| < N_c \text{ for some } N_c \in \mathbb{N}\},$$

is the non-archimedean MANDELBROT *set for quadratic polynomials.*

Proposition 4.2 *M is the closed unit disc $\overline{D}_1(0)$ - i.e. the valuation ring $\mathcal{O}_K$ of K.*

Proof: Consider the iterates of 0 under ϕ: $\phi_c(0) = c$; $\phi_c^2(0) = c^2 + c$; $\phi_c^3(0) = c^4 + 2c^3 + c^2 + c$; and $\phi_c^n(0) = c^{2^{n-1}} + \sum_{i=0}^{n-2} k(i)c^{2^i}$ where $k(i)$ is a non-negative integer for each i. When $c \in M$ then these iterates remain bounded, and this occurs precisely when $|c| \leq 1$ by ultrametricity. □

At first sight this may appear rather uninteresting, but a beautiful analogy exists to the fact that in the archimedean case, the MANDELBROT set turns out to be a fascinating archive of information about the JULIA sets of the functions $g_c(z) = z^2 + c$. (For example, if $c \in M$, then the JULIA set is connected, whereas it is totally disconnected otherwise, in which case it is known as "FATOU dust"). In short, we have the following:

Proposition 4.3 *Whenever $char(\overline{K}) \neq 2$, then*
(I) $c \in M \Leftrightarrow \phi_c$ has good reduction in some co-ordinate, and
(II) if $c \notin M$, then $\mathcal{J}_{\phi_c} \neq \emptyset$.

Proof:
If $c \in M$, then $|c| \leq 1$ and for such c, $\phi_c([x : y]) = [x^2 + cy^2 : y^2]$ has good reduction.

Now suppose that $c \notin M$. Then $|c| > 1$, and we claim that this implies that ϕ_c has a repelling fixed point. Indeed, z_0 is a finite fixed point of ϕ_c if and only if $z_0 = \frac{1}{2} + \frac{\alpha_0}{2}$ where $\alpha_0^2 = 1 - 4c$, so because $|c| > 1$, we know that $|1 - 4c| > 1$ (since $char(\overline{K}) \neq 2$), which implies that $|\alpha_0|$ and $|1 + \alpha_0| = |2z_0| = |\phi_c'(z_0)|$ are in turn greater than 1, and thus that z_0 is a repelling fixed point of ϕ_c. Such a point is in the JULIA set of ϕ_c,(i.e. (II) is true,) so ϕ_c has bad reduction from the Theorem of MORTON and SILVERMAN. □

Suppose that K is also algebraically closed. Then, because each quadratic polynomial $a_2x^2 + a_1x + a_0 \in K[x]$ has the form $z^2 + c \in K[z]$ under the co-ordinate change $x \mapsto \frac{z}{a_{2,0}} - \frac{a_1}{2a_2}$ (for $a_{2,0}$ being a root of $z^2 - a_2$ in K), M happens to catalogue all quadratic polynomials having good reduction in some co-ordinate system. Hence, from the Theorem of MORTON and SILVERMAN together with the proposition, we see that in the case of quadratic polynomials this is *equivalent* to having an empty JULIA set (provided that $char(\overline{K}) \neq 2$).

BENEDETTO has studied this question of equivalence of good reduction to empty JULIA set in a much more general context, and we next turn our attention to his results in this direction.

4.3 Polynomials with good reduction

In studying the extent to which having empty JULIA set is equivalent to a map having good reduction, BENEDETTO [2] has proved the following for polynomial maps:

Theorem 4.3 *If* $char(\overline{K}) = 0$ *or* $char(\overline{K}) = p \geq d-1$, *and* $\psi(z) \in K[z]$ *is a polynomial of degree* d, *then the* JULIA *set* $\mathcal{J}_\psi$ *of* ψ *is empty if and only if* ψ *has good reduction.*

Proof: We have seen that good reduction is sufficient for the JULIA set to be empty. To prove the converse, firstly observe that if ψ is constant or linear, then there exists a co-ordinate system in which ψ has good reduction. Suppose that deg $\psi \geq 2$, and notice that each fixed point of ψ must be non-repelling for the JULIA set to be empty (from Proposition 3.1), and we are thus in a position to apply Lemma 3.1.

Suppose that $char(\overline{K}) > d$. We proceed to show that there exists a disc which is the d-fold image of itself under ψ, from which the good reduction of ψ will be an easy consequence. This we do by showing that all of those critical points of ψ which are sufficiently close to fixed points of the map, are all contained in such a disc. The proof of this fact is fairly technical, and relies on some of the results shown in earlier chapters.

Let

$$S_1 := \{a \in K : \psi'(a) = 0 \text{ and } a \in \overline{D}_{r_x}(x) \text{ for some fixed point } x \text{ of } \psi\}$$

where r_x is the radius associated to x under ψ in Lemma 3.1. Similarly, if y is a periodic point of ψ with exact period n_y, we let $r_{(y,n_y)}$ be the radius associated to y under ψ^{n_y}. Note that y is a *non-repelling* fixed point of ψ^{n_y}, since $\mathcal{J}_{\psi^{n_y}} = \mathcal{J}_\psi$ (from Proposition 3.4). Then we set

$$S_2 := \{a \in K \backslash S_1 : \psi'(a) = 0 \text{ and } a \in \overline{D}_{r_{(y,n_y)}}(y) \text{ for some fixed point } y \text{ of } \psi^{n_y}\}.$$

Now for any $a \in S_1 \cup S_2$, if $a \in \overline{D}_{r_{(x,n_x)}}(x) \cap \overline{D}_{r_{(y,n_y)}}(y)$, then the association of a to $r_a = r_{(x,n_x)}$ is well-defined: firstly $\overline{D}_{r_{(x,n_x)}}(a) = \overline{D}_{r_{(x,n_x)}}(x) \subset \overline{D}_{r_{(y,n_y)}}(y) = \overline{D}_{r_{(y,n_y)}}(a)$ or $\overline{D}_{r_{(x,n_x)}}(x) \supset \overline{D}_{r_{(y,n_y)}}(y)$ since the two discs have non-empty intersection. Moreover, $\psi^{n_x n_y} = (\psi^{n_x})^{n_y}$ maps $\overline{D}_{r_{(x,n_x)}}(x)$ multiply-to-one onto itself, and $\psi^{n_x n_y} = (\psi^{n_y})^{n_x}$ acts similarly on $\overline{D}_{r_{(y,n_y)}}(y)$, so from the uniqueness of the radius associated to $\psi^{n_x n_y}$ in Lemma 3.1 such that this polynomial maps some disc about a non-repelling fixed point multiply-to-one onto itself, in fact $r_{(x,n_x)} = r_{(y,n_y)}$.

For any $a \in S_1 \cup S_2$, let N_a be the minimum period of all periodic points in $\overline{D}_{r_a}(a)$, which exists from the well-ordering of $\mathbb{N}$. Only finitely many critical points exist since ψ' is a polynomial, so we can choose some prime q which strictly exceeds N_a for each $a \in S_1 \cup S_2$.

If w is a fixed point of ψ^q, then we claim that there exists $\alpha \in \overline{D}_{r_{(w,q)}}(w) \cap S_1$. In the first place, ψ^q maps $\overline{D}_{r_{(w,q)}}(w)$ m-to-one onto itself for some $m > 1$ as the degree of ψ^q exceeds 1. Each factor of m is at most d, since any point in $\overline{D}_{r_{(w,q)}}(w)$ can have at most d pre-images in $\psi^{-1}(\overline{D}_{r_{(w,q)}}(w))$, each of which can have at most d pre-images in $\psi^{-1}(\psi^{-1}(\overline{D}_{r_{(w,q)}}(w)))$, and so on, with the total number of pre-images being m, the product of the number of pre-images at each step. Because $char(\overline{K}) > d$, we thus know that $char(\overline{K}) \nmid m$. Hence from Lemma 3.3 we know that $\overline{D}_{r_{(w,q)}}(w)$ contains a critical point of ψ, say b. Now from the definition of N_b, there exists some y of exact period N_b such that $b \in \overline{D}_{r_{(y,N_b)}}(y)$. Setting $r_b = r_{(y,N_b)}$, the same argument as before suffices to show that $\overline{D}_{r_{(w,q)}}(w) = \overline{D}_{r_{(y,N_b)}}(y) = \overline{D}_{r_b}(b)$.

However, in this case we also know that q and N_b are relatively prime, so since both ψ^q and ψ^{N_b} map $\overline{D}_{r_b}(b)$ onto itself, ψ also does. If we again think of the possible numbers of pre-images of the disc under the action of ψ it is evident that ψ maps $\overline{D}_{r_b}(b)$ multiply-to-one onto itself (where the multiple is $\sqrt[q]{m}$), as ψ^q maps $\overline{D}_{r_b}(b)$ m-to-one onto itself and $m > 1$. But then, $\overline{D}_{r_b}(b)$ contains $\sqrt[q]{m}$ fixed points of ψ from Lemma 2.3(a), so that $N_b = 1$ and $b \in S_1$. i.e. $\overline{D}_{r_{(w,q)}}(w) \cap S_1$ is non-empty, as claimed.

If $a \in \overline{D}_{r_{(w,q)}}(w) \cap S_1$, notice that our former discussion showed that $\overline{D}_{r_a}(a) = \overline{D}_{r_{(w,q)}}(w)$. Now let the set of discs $\{\overline{D}_{r_a}(a) : a \in S_1\}$ be denoted by $\{D_1, D_2, \ldots, D_v\}$ where $D_i \cap D_k = \emptyset$ for all $i \neq k$. Each such disc D_i contains a fixed point, say x_i, of ψ and is the m_i-fold image of itself under ψ, where $2 \leq m_i \leq d$ for each $i \in \{1, \ldots, v\}$ from Lemma 3.1. Now from Lemma 2.3(a), it follows that the total number of fixed points in each disc is precisely m_i. But then $\sum_{i=1}^{v} m_i = d$.

At the same time, we know that any fixed point w of ψ^q has $\overline{D}_{r_{(w,q)}}(w) = \overline{D}_{r_a}(a)$ for some $a \in S_1$. Thus, because $\overline{D}_{r_a}(a) = D_j$ is then the m_j^q-fold image of itself under ψ^q, from Lemma 2.3(a) this disc contains m_j^q of the d^q fixed points of ψ^q. Now each of the fixed points of ψ is also fixed by ψ^q, so that in *every* disc D_i there is some fixed point of ψ^q, and each such disc thus contains m_i^q of the d^q fixed points of ψ^q. Hence we know that $\sum_{i=1}^{v} m_i^q = d^q$. However, with d, q and m_i all at least 2 for all $i \in \{1, \ldots, v\}$, the only way for this to be tenable with $\sum_{i=1}^{v} m_i = d$ is for $v = 1$. Then, some disc $\overline{D}_{r_a}(a)$ is the $m_1 = d$-fold

image of itself under ψ, as asserted initially.

A co-ordinate change suffices to move this disc to the valuation ring $\overline{D}_1(0)$. For this disc to then be the d-fold image of itself under a polynomial (say ψ_0) of degree d, ψ_0 must have coefficients in $\overline{D}_1(0)$ and its leading coefficient must be a unit. (Indeed, from the proof of Lemma 3.1, we know that $r = 1 = \min_{2\leq i\leq d}\{\frac{1}{\sqrt[i-1]{|c_i|}}\} = \frac{1}{\sqrt[d-1]{|c_d|}}$ when we write $\psi_0(z) = \sum_{i=1}^{d} c_i z^i$. Thus $|c_d| = 1$ and $\max_{2\leq i\leq d-1}\{|c_i|\} \leq 1$. Here, $|c_1| \leq 1$ also, since 0 must be a non-repelling fixed point of ψ_0). But such a polynomial has good reduction, since we can express it as $\psi_0([x : y]) = [\sum_{i=1}^{d} c_i x^i y^{d-i} : y^d]$, where $|c_d| = 1$ implies that the only shared root of $\overline{\sum_{i=1}^{d} c_i x^i y^{d-i}}$ and $\overline{y^d}$ is trivial.

To complete the proof, we consider the more general situation of deg $\psi \leq char(\overline{K}) + 1 = p + 1$. Observe that in the above discussion, the characteristic of $\overline{K}$ is only important in allowing us to use a lemma which guarantees the existence of a critical point in a certain disc about a periodic point of ψ. Thus, we aim to show that if, as before, w is a fixed point of ψ^q where q is as above and ψ maps $\overline{D}_{r_{(w,q)}}(w)$ m-to-one onto itself as in Lemma 3.1, then $char(\overline{K}) \nmid m$. Lemma 3.3, is then applicable and we use it to see that $\overline{D}_{r_{(w,q)}}(w)$ contains a critical point. We can then proceed making use of the same argument as before. Along the way, we shall eliminate certain cases where the good reduction is more immediately seen.

We can assume that by means of some co-ordinate change if necessary, ψ is monic and fixes 0. Let $\psi(z) = z^d + c_{d-1}z^{d-1} + \cdots + c_1 z$ and define $r := \max\{|x| : x \in K \text{ and } \psi(x) = 0\}$. If $z \in K$ has $|z| > r$, then we claim that $|\psi(z)| = |z^d| > |z|$ in all cases where the good reduction is not readily seen: firstly, from the roots theorem, if z has $|z| > r$, then $\max_{1\leq i\leq d}\{|c_i z^i|\}$ corresponds to a unique index. For z sufficiently large, this maximum is $|z^d|$, so that if $s := \min\{a \in \mathbb{R} : a > 0 \text{ and } \max_{1\leq i\leq d}\{|c_i|a^i\} = a^d\}$, then $s \leq r$. (Since otherwise, if $s > r$, there exists $t \in \mathbb{R}$, with $r < t < s$, for which $\max_{1\leq i\leq d}\{|c_i|t^i\} > t^d$. But then from the continuity of the functions $|c_i|w^i$ and the fact that the index corresponding to the maximum decreases as w decreases from s to t, there exists $v \in (t, s]$ such that $\max_{1\leq i\leq d}\{|c_i|v^i\} = v^d = |c_j|v^j$ for some $j \in \{1, \ldots, d-1\}$. Because K is algebraically closed, there exists $\gamma \in K$ such that $\gamma^{d-j} - c_j = 0$ and such a γ has $|\gamma| = v$, so that $v \in |K|$. From the roots theorem, this implies that there exists $x \in K$ with $|x| = v$, for which $\psi(x) = 0$. This is a contradiction to the choice of r.) Thus, $\max_{1\leq i\leq d}\{|c_i z^i|\} = |z^d| > |c_j z^j|$

for each $z \in K$ with $|z| > r$ and for each $j \in \{1, \ldots, d-1\}$. From ultrametricity, then $|\psi(z)| = |z^d|$ for all such z.

Now let $s = \min_{2 \leq i \leq d}\{\frac{1}{\sqrt[i-1]{|c_i|}}\}$. Since $\mathcal{J}_\psi = \emptyset$, 0 must be a non-repelling fixed point of ψ, and it follows from the proof of Lemma 3.1 that ψ maps $\overline{D}_s(0)$ multiply-to-one onto itself. If $r \leq s$, then there exist d pre-images of 0 in $\overline{D}_r(0) \subset \overline{D}_s(0)$, so that ψ must map $\overline{D}_s(0)$ d-to-one onto itself, and as above there thus exists a co-ordinate system in which ψ has good reduction. So suppose that $s < 1$. Then there exists c_j with $|c_j| > 1$, so that $v(c_j) < 0$. Now because ψ is monic, $(d, 0)$ lies on the NEWTON polygon of ψ, and hence, with some coefficient of ψ having negative valuation, there is a segment of positive gradient on the NEWTON polygon. Thus, some root of ψ has negative valuation, and norm greater than or equal to 1. i.e., $r \geq 1$. Now if $|z| > r$, this implies that $|z^d| > |z|$ from the multiplicativity of the norm.

In what follows, we can thus assume that $|z| > r$ implies that $|\psi(z)| = |z^d| > |z|$.

From Lemma 2.4, $\psi^{-1}(\overline{D}_r(0))$ is a finite union of closed rational discs, each of which is mapped m_i-to-one onto $\overline{D}_r(0)$ for some $m_i \geq 1$ associated to each of these discs. Let $\psi^{-1}(\overline{D}_r(0)) := D_1 \cup \ldots \cup D_u$ denote this union.

Observe that $\psi^{-1}(\overline{D}_r(0)) \subset \overline{D}_r(0)$ since if $z \in K$ has $|z| > r$, then $\psi(z) \notin \overline{D}_r(0)$.

If $u = 1$, then $\psi^{-1}(\overline{D}_r(0)) = \overline{D}_y(0)$ is some closed rational disc containing 0 and each other root of ψ. Thus $\overline{D}_r(0) \subset \psi^{-1}(\overline{D}_r(0))$. Because also $\psi^{-1}(\overline{D}_r(0)) \subset \overline{D}_r(0)$, we thus know that $\psi^{-1}(\overline{D}_r(0)) = \overline{D}_r(0)$. However, since d pre-images of 0 occur in $\psi^{-1}(\overline{D}_r(0))$, this disc maps d-to-one onto itself and as before, ψ has good reduction in some co-ordinate system.

So suppose that $u > 1$, and take any D_i with $i \in \{1, \ldots, u\}$. We know that $D_i \subset \psi(\overline{D}_r(0)) \subset \overline{D}_r(0)$, but more than this can be said: since the discs D_i are disjoint by assumption, also $D_i \subsetneq \overline{D}_r(0)$. Because $\psi(D_i) = \overline{D}_r(0) \supsetneq D_i$, from Lemma 2.3(b), D_i contains a fixed point a_i of ψ. Again because $\mathcal{J}_\psi$ is empty, we know that a_i is non-repelling, and thus, Lemma 3.1 is applicable in giving the unique radius t_i such that ψ maps $\overline{D}_{t_i}(a_i)$ multiply-to-one onto itself. If for some i, $D_i \subset \overline{D}_{t_i}(a_i)$, then $\overline{D}_r(0) = \psi(D_i) \subset \psi(\overline{D}_{t_i}(a_i)) = \overline{D}_{t_i}(a_i)$, so that $\overline{D}_{t_i}(a_i) = \overline{D}_{t_i}(0)$ where $t_i \geq r$. (Of course, if $t_i > r$, then ψ would map certain points of $\overline{D}_{t_i}(a_i)$ outside this disc, so in fact $t_i = r$.) Now because there are thus d pre-images of 0 under ψ in $\overline{D}_{t_i}(0)$, this disc is the d-fold image of itself under ψ and the mapping once again has good reduction under some co-ordinate change. Thus suppose

that $\overline{D}_{t_i}(a_i) \subset D_i$ for each $i \in \{1, \ldots, u\}$. In this case, D_i maps multiply-to-one onto $\overline{D}_r(0)$ for each i. Hence, with u being greater than 1, ψ can map any D_i at most $(d-2)$-to-one onto $\overline{D}_r(0)$. Any disc D which ψ maps into $\overline{D}_r(0)$ is a subset of D_i for some $i \in \{1, \ldots, u\}$. Thus, ψ maps D at most $(d-2)$-to-one onto its image. Hence, with $d-2 < char(\overline{K})$ by assumption, we know that for any $l \in \mathbb{N}$, whenever ψ^l maps some disc multiply-to-one into $\overline{D}_r(0)$, then $char(\overline{K})$ does not divide this multiple. This is what we aimed to see, since all periodic points of ψ are in $\overline{D}_r(0)$ (as $|\psi(z)| > |z|$ for all z with $|z| > r$), so that with w, q and $\overline{D}_{r_{(w,q)}}(w)$ as above, $\overline{D}_{r_{(w,q)}}(w) \subset \overline{D}_r(0)$, and if ψ^q maps $\overline{D}_{r_{(w,q)}}(w)$ m-to-one onto itself, then $char(\overline{K}) \nmid m$ and we are in a position to apply Lemma 3.3 and proceed as formerly. □

It is interesting to see an example of a map having sufficiently high degree with bad reduction as well as an empty JULIA set. The example we shall discuss shows that in the case of the residue field having characteristic 2, the bound given in the above theorem is sharp. The sharpness of the bound also turns out to hold in the case for residue fields of any odd prime characteristic, as an example in [2] shows.

Of course, it is in general not easy to show that a map has bad reduction, but this task is facilitated by the following

Proposition 4.4 *If $\phi(z) \in K(z)$ is a rational map with an attracting fixed point at ∞, and the set of iterates of zero under ϕ is bounded, then for ϕ to have bad reduction it is sufficient that for each $c \in K^*$, $c^{-1}\phi(cz)$ does not have good reduction as written.*

Proof: Suppose that although ϕ is a rational map satisfying the hypotheses of the proposition, there is some co-ordinate system in which ϕ has good reduction. Let $h \in PGL(2, K)$ be an automorphism which effects a change to this co-ordinate system - i.e. $h^{-1} \circ \phi \circ h$ has good reduction.

We claim that any element of $PGL(2, \mathcal{O}_K)$ has good reduction:
indeed, if $f \in PGL(2, \mathcal{O}_K)$, say $f([x : y]) = [ax + by : cx + dy]$ where $a, b, c, d \in \mathcal{O}_K$ and at least one of a, b, c, d is a unit, then the determinant $ad - bc$ is a unit, so $\overline{ad - bc} \neq 0$, implying that $\overline{a}x + \overline{b}y = \overline{c}x + \overline{d} = 0$ has a unique solution, namely $(0, 0)$, and consequently f has good reduction.

Moreover, from this discussion we see that any such $f \in PGL(2, \mathcal{O}_K)$ has a reduction $\overline{f}$ which is non-constant. Being a morphism of $\mathbb{P}^1_{\overline{K}}$ to itself, $\overline{f}$ is thus surjective. (See [19,

I.2].) Consequently, with $\overline{\psi} = \overline{h^{-1} \circ \phi \circ h}$ being well defined, given any $g \in PGL(2, \mathcal{O}_K)$, also $g^{-1} \in PGL(2, \mathcal{O}_K)$ so that $\overline{g^{-1}} \circ \overline{h^{-1} \circ \phi \circ h} \circ \overline{g}$ is well-defined from the surjectivity of g and g^{-1}. Hence, $\psi := g^{-1} \circ h^{-1} \circ \phi \circ h \circ g$ also has good reduction for any $g \in PGL(2, \mathcal{O}_K)$ - in particular for a g which is chosen so that ∞ is an attracting fixed point of ψ. (Recall that co-ordinate changes do not change multipliers, so we can obtain that ∞ is an *attracting* fixed point under ψ.)

We would now like to apply Lemma 3.2 to the open neighbourhood $W_\infty := \{z \in \mathbb{P}^1(K) : \overline{z} = \infty + \mathcal{M}_K\}$ about the attracting fixed point ∞. Consequently, we aim now to show that $\psi(W_\infty) \subset W_\infty$, and do this with the aid of HENSEL'S Lemma for Power Series (Lemma 2.1).

By means of some co-ordinate change taking ∞ to $a \in K$ and ψ to χ, we know that χ has a power series expansion about a, say $\chi(z) = \sum_{i=0}^{\infty} \alpha_i (z-a)^i$. Then let $\overline{\omega}(z + \mathcal{M}_K) = \overline{\chi}(z + \mathcal{M}_K) - (a + \mathcal{M}_K) \in \overline{K}[[z + \mathcal{M}_K]]$. This power series converges so there exist representatives for the coefficients of $\overline{\omega}$ such that ω is a power series which reduces to $\overline{\omega}$ and for which all but a finite number of the coefficients are in $\mathcal{M}_K$. Thus, ω is congruent to a polynomial modulo $\mathcal{M}_K$.

Now $(z + \mathcal{M}_K) - (a + \mathcal{M}_K)$ divides $\omega(z + \mathcal{M}_K)$, so that we can write

$$\omega(z) \equiv (z-a)^l \mu(z) \nu(z) \pmod{\mathcal{M}_K}$$

where

- $l \geq 0$;
- $\overline{x} = a + \mathcal{M}_K$ for each root x of μ;
- $\overline{y} \neq a + \mathcal{M}_K$ for any root y of ν;
- deg $\mu(z) + l > 0$;
- μ is monic; and
- $\mu, \nu \in \mathcal{O}_K[z]$.

Then the reduced polynomials $\overline{\mu}$ and $\overline{\nu}$ are relatively prime, so from HENSEL'S Lemma for Power Series $\omega(z)$ can be expressed as $\rho(z)\tau(z)$ where $\rho(z) \in \mathcal{O}_K[z]$ has $\rho(z) \equiv (z-a)^l \mu(z) (\mathrm{mod} \mathcal{M}_K)$ and $\tau(z) \in \mathcal{O}_K[[z]]$ satisfies $\tau(z) \equiv \nu(z) (\mathrm{mod} \mathcal{M}_K)$.

Pick any $x_0 \in W_a = \{z \in \mathbb{P}^1(K) : \overline{z} = a + \mathcal{M}_K\}$ - i.e., $x_0 - a \in \mathcal{M}_K$. Then

$$\rho(x_0) \equiv (x_0 - a)^l \mu(x_0) \equiv 0 \pmod{\mathcal{M}_K}$$

since each root of $(z-a)^l\mu(z)$ reduces to $a + \mathcal{M}_K$. But then $\chi(x_0) - a \in \mathcal{M}_K$ and thus, $\chi(W_a) \subset W_a$. Reversing the change of co-ordinates we effected in order to show this, we find that $\psi(W_\infty) \subset W_\infty$ as claimed.

From Lemma 3.2, the iterates of each point of W_∞ then tend to ∞.

The point 0 may have moved under the change of co-ordinates, but not to any point with unbounded iterates. (i.e, if $0 \mapsto x$ under $(h \circ g)^{-1}$, then $\{\psi^n(x)\}_{n\in\mathbb{N}}$ is a bounded set.) Hence $x = (h \circ g)^{-1}(0) \notin W_\infty$. From the definition of the spherical metric, it is clear that all distances on $\mathbb{P}^1(K)$ are less than or equal to 1. If two points of $\mathbb{P}^1(K)$ are closer together than 1, then their reductions modulo $\mathcal{M}_K$ are equal. Thus the spherical distance from x to ∞ is 1. But then $x \in \overline{D}_1(0)$ since otherwise, were $|x| > 1$, then there would be homogeneous co-ordinates for x given by x_0 and 1 such that $x = [x_0 : 1]$ where $|x_0| > 1$; and as a result $\|x, \infty\| = \frac{1}{|x_0|} < 1$ which is not true. It thus follows that the mapping $q(z) = z + x$ is a mapping in $PGL(2, \mathcal{O}_K)$ because we can write $q([s : t]) = [s + xt : t]$ where 1 and x are both in $\mathcal{O}_K$ and the determinant is 1 which is a unit.

But then as before, the map $q^{-1} \circ \psi \circ q$ has good reduction and is a map for which the iterates of 0 remain bounded and ∞ is an attracting fixed point. However, with $q^{-1} \circ \psi \circ q = (h \circ g \circ q)^{-1} \circ \phi \circ (h \circ g \circ q)$, we see that $(h \circ g \circ q)^{-1}$ is a linear map which fixes 0 and ∞. Thus it is of the form $z \mapsto \frac{1}{c}z$ for some $c \in K^*$. But then $c^{-1}\phi(cz)$ has good reduction, which is a contradiction to our assumption that ϕ satisfy the conditions of the proposition. □

Example

Claim: *The polynomial* $\phi(z) = z^4 + \frac{1}{\sqrt{2}}z^2 : \mathbb{P}^1(\Omega_2) \to \mathbb{P}^1(\Omega_2)$ *has bad reduction as well as having an empty* JULIA *set.*

Proof of claim: Let x and y be homogeneous co-ordinates for z (so that $z = [x : y]$), and let $q_c(z) = cz$ for each $c \in {\Omega_2}^*$. Then $\phi(z) = \phi([x : y]) = [\sqrt{2}x^4 + x^2y^2 : \sqrt{2}y^4]$, so that

$$\begin{aligned} c^{-1}\phi(cz) &= q^{-1} \circ \phi([cx : y]) \\ &= q^{-1} \circ [\sqrt{2}c^4x^4 + c^2x^2y^2 : \sqrt{2}y^4] \\ &= [\sqrt{2}c^3x^4 + cx^2y^2 : \sqrt{2}y^4]. \end{aligned}$$

Because $\sqrt{2}y^4$ always reduces to the zero polynomial, we consider various possibilities for the norm of c and show that in each case, the first polynomial has a meaningful reduction (in which case any of its non-trivial roots are shared by the zero polynomial) or that multiplying each of the polynomials $\sqrt{2}c^3x^4 + cx^2y^2$ and $\sqrt{2}y^4$ by suitable factors yields meaningful reduction to polynomials sharing non-trivial roots. Firstly, if $|c| < 1$, then the reduction of $\sqrt{2}c^3x^4 + cx^2y^2$ is 0, so that $c^{-1}\phi(cz)$ has bad reduction in such cases; if $|c| = 1$, then the polynomial x^2y^2 is the reduction of the first homogeneous polynomial representing $c^{-1}\phi(cz)$ so that again $c^{-1}\phi(cz)$ has bad reduction; and if $|c| > 1$, then we write $c^{-1}\phi(cz) = [\sqrt{2}x^4 + c^{-2}x^2y^2 : c^{-3}\sqrt{2}y^4]$, from which it is clear that both polynomials reducing to 0 implies that $c^{-1}\phi(cz)$ has bad reduction once again. Because ϕ is a map which fixes both 0 and ∞, from the above proposition we know that ϕ has bad reduction.

If $|z| > 2^{2^{-2}}$, then $|z^4| > |\sqrt{2}z^2|$, and hence $|\phi(z)| = |z^4|$ for all $z \in W := \mathbb{P}^1(\Omega_2)\backslash\overline{D}_{2^{2-2}}(0)$. But because $2^{2^{-2}} > 1$, this means that $\phi(W) \subset W$. From Lemma 3.2, with $\infty \in W$ being an attracting fixed point of ϕ, it follows that the iterates of all points of W tend to ∞. Thus, given any open set U about ∞, then for any $z \in W$, there exists some $n \in \mathbb{N}$ such that $\phi^n(z) \in U$. In particular, with $\infty \in \mathcal{F}_\phi$ (from Proposition 3.1), there exists some open set about ∞ which is contained in $\mathcal{F}_\phi$ by the definition of the FATOU set. Because $\mathcal{F}_\phi = \mathcal{F}_{\phi^n} = \phi^{-n}(\mathcal{F}_{\phi^n})$ for each $n \in \mathbb{N}$ (from Propositions 3.4 and forwards) it then follows that each point of W is in $\mathcal{F}_\phi$.

Now let $z \in \overline{D}_{2^{2-2}}(0)$ be arbitrary, and pick any $u \in \overline{D}_{2^{-2-1}}(z)$. If we let $w = z - u$ so that $u = z - w$, then

$$\begin{aligned}
|\phi(z) - \phi(u)| &= |z^4 + \frac{1}{\sqrt{2}}z^2 - (z-w)^4 - \frac{1}{\sqrt{2}}(z-w)^2| \\
&= |z^4 - (z-w)^4 + \frac{1}{\sqrt{2}}[z^2 - (z-w)^2]| \\
&= |[z^2 - (z-w)^2][z^2 + (z-w)^2 + \frac{1}{\sqrt{2}}]|
\end{aligned}$$

Now here, $|z^2 + (z-w)^2 + \frac{1}{\sqrt{2}}| \leq |\frac{1}{\sqrt{2}}|$ since $|z|^2 \leq 2^{2^{-1}} = |\frac{1}{\sqrt{2}}|$ and $|z-w|^2 \leq 2^{-1} < |\frac{1}{\sqrt{2}}|$. Thus,

$$\begin{aligned}
|\phi(z) - \phi(u)| &= 2^{2^{-1}}|z^2 - (z-w)^2| \\
&= 2^{2^{-1}}|2zw - w^2| \\
&\leq 2^{2^{-1}}|w|\max\{|2z|, |w|\} \\
&\leq 2^{2^{-1}}|w|\max\{2^{-1}2^{2^{-2}}, 2^{-2^{-1}}\}
\end{aligned}$$

$$\leq \quad |w| = |z - u|$$

from which we see that $z \in \mathcal{F}_\phi$ and hence that $\mathcal{J}_\phi = \emptyset$. □

Chapter 5

Two finiteness theorems

In this final chapter, we are concerned with two marvellous results which in different contexts ensure the finiteness of the numbers of points of varieties which satisfy certain dynamical criteria under morphisms of these varieties to themselves.

The first theorem we present is that of NORTHCOTT stating that the total number of preperiodic points of morphisms of certain varieties over a number field, which are rational relative to any of the number fields of a given degree over $\mathbb{Q}$, is always finite. This classical result is not specific to the case of non-archimedean dynamical systems, but it fits well into our discussion.

Returning to the special situation of non-archimedean dynamics, we subsequently discuss a more recent development in the work of MORTON and SILVERMAN, who succeeded in showing that the number of attracting periodic points under a separable morphism of the projective line over a valued field to itself is finite, whenever the morphism has good reduction. The proof of this fact relies on basic tools from Algebraic Geometry and the study of Function Fields, which we forge en route.

5.1 The finiteness of the number of rational preperiodic points on a variety

Let V be a variety in projective n-space over $\mathbb{C}$ (i.e. $\mathbb{P}^n(\mathbb{C})$), given by the zero set of a finite number of homogeneous polynomials with coefficients in a number field K. We turn our attention to the K-rational preperiodic points of V with respect to some morphism $\phi : V \longrightarrow V$ given by $\phi([x_0 : \ldots : x_n]) = [\phi_0(x_0, \ldots, x_n) : \ldots : \phi_n(x_0, \ldots, x_n)]$, where $\phi_i(x_0, \ldots, x_n) \in K[x_0, \ldots, x_n]$ for each i. By K-rational points of V we mean those points

of the variety for which there exist homogeneous co-ordinates where each co-ordinate lies in K. As ϕ is a well-defined map on V, the ϕ_i are not all zero at any point of V, and each is a homogeneous form of the same degree, say l. In 1948, NORTHCOTT showed that if $l \geq 2$, i.e. if ϕ is not linear, then there are at most finitely many preperiodic points of ϕ which are rational relative to any of the number fields of a given degree over $\mathbb{Q}$. In particular, there is at most a finite number of K-rational preperiodic points on the variety.

To prove his result, NORTHCOTT introduces an arithmetic function (which we shall define in a moment) with respect to which he shows a crucial property: namely that the set of all points of V which are rational relative to *any* number field of a chosen degree over $\mathbb{Q}$, for which the value under this arithmetic function is bounded by some given positive integer, is finite. To conclude the proof, he then merely needs to show that each preperiodic point which is rational relative to some number field K, is bounded under this function, by some constant depending only on V, ϕ and the degree of $K \mid \mathbb{Q}$.

If $\boldsymbol{\xi} = [\xi_0 : \ldots : \xi_n]$ is an K-rational point of V and $\xi_0, \ldots, \xi_n$ are homogeneous co-ordinates which are in $\mathcal{O}_K$, we define $\mathcal{I}_{\boldsymbol{\xi}}$ to be the ideal $(\xi_0) + \cdots + (\xi_n)$ in $\mathcal{O}_K$, and set

$$A_K(\boldsymbol{\xi}) = \frac{\prod_\sigma (|\xi_0^\sigma| + \cdots + |\xi_n^\sigma|)}{|N_{K|\mathbb{Q}}(\mathcal{I}_{\boldsymbol{\xi}})|}$$

where the product is over all $\mathbb{Q}$-isomorphisms σ of K in $\mathbb{C}$, the absolute value signs denote the usual (archimedean) norm on $\mathbb{C}$, and $N_{K|\mathbb{Q}}(\mathcal{I}_{\boldsymbol{\xi}})$ is the norm of the ideal $\mathcal{I}_{\boldsymbol{\xi}}$ in $\mathbb{Q}$. (See Appendix B for a precise definition of $N_{K|\mathbb{Q}}(\mathcal{I}_{\boldsymbol{\xi}})$).

Observe that A_K is independent of the choice of homogeneous co-ordinates for $\boldsymbol{\xi}$, and that if E is a finite extension of K, then $A_E(\boldsymbol{\xi}) = (A_K(\boldsymbol{\xi}))^{[E:K]}$ since $\boldsymbol{\xi}$ is K-rational and $[E : K]$ $\mathbb{Q}$-isomorphisms of E extend each $\mathbb{Q}$-isomorphism of K.

Theorem 5.1 *If $m, r \in \mathbb{N}$ and Σ_K denotes the set of all K-rational points $\boldsymbol{\xi}$ in $\mathbb{P}^n(\mathbb{C})$ which satisfy $A_K(\boldsymbol{\xi}) \leq r$, then*

$$X := \bigcup_{[K:\mathbb{Q}]=m} \Sigma_K$$

is a finite set.

Proof:

Take an arbitrary $\boldsymbol{\xi} \in X$. Then for some number field K, $\boldsymbol{\xi} \in \Sigma_K$. Suppose that $\boldsymbol{\xi} = [\xi_0 : \ldots : \xi_n]$ where $(\xi_0, \ldots, \xi_n)$ are homogeneous co-ordinates for $\boldsymbol{\xi}$ lying in K. Define

$\mathcal{I} := (\xi_0) + \cdots + (\xi_n)$ and let

$$f(x_0, \ldots, x_n) = \frac{\prod_\sigma (\xi_0^\sigma x_0 + \cdots + \xi_n^\sigma x_n)}{|N_{K|\mathbb{Q}}(\mathcal{I})|}.$$

We claim that $f(x_0, \ldots, x_n) \in \mathbb{Z}[x_0, \ldots, x_n]$:

For each term of f, the numerator of the coefficients is a symmetric function of terms of the form $\xi_{i_1}^{\sigma_1} \ldots \xi_{i_m}^{\sigma_m}$, where the $\mathbb{Q}$-isomorphisms of K are denoted by $\sigma_1, \ldots, \sigma_m$, so each such expression is fixed under the action of σ_j for each j. Now form the normal closure of $E := \mathbb{Q}(\xi_1, \ldots, \xi_n)$ and denote it by N. Although N is not necessarily contained in K, each $\mathbb{Q}$-automorphism of N is (trivially) the extension of some $\mathbb{Q}$-isomorphism of E, each of which is the restriction of some $\mathbb{Q}$-isomorphism of K to E. Hence, each $\mathbb{Q}$-automorphism of N *also* fixes the numerator of each coefficient. Because $N \mid \mathbb{Q}$ is a GALOIS extension, the numerators of the coefficients of f are thus all in $\mathbb{Q}$. Now $|N_{K|\mathbb{Q}}(\mathcal{I})| \in \mathbb{Z}$, (see Appendix B) so that in fact $f(x_0, \ldots, x_n) \in \mathbb{Q}[x_0, \ldots, x_n]$. We proceed to show that the coefficients are integers: pick any $a = \xi_{i_1}^{\sigma_1} \ldots \xi_{i_m}^{\sigma_m}$ and now view the normal closure of K, say L. Let $\mathcal{I}' = \mathcal{I}\mathcal{O}_L$. We claim that $a \in N_{L|\mathbb{Q}}(\mathcal{I}')\mathcal{O}_L$: indeed,

$$a^{[L:K]} \in \prod_{\sigma \in G(L|\mathbb{Q})} (\mathcal{I}')^\sigma,$$

since precisely $[L : K]$ $\mathbb{Q}$-isomorphisms of L extend each $\mathbb{Q}$-isomorphism of K. Now in Appendix B this product is seen to be precisely $N_{L|\mathbb{Q}}(\mathcal{I}')\mathcal{O}_L$. Because $N_{L|\mathbb{Q}}(\mathcal{I}')$ is principal, writing the absolute value of a generator of this $\mathbb{Z}$ ideal as $|N_{L|\mathbb{Q}}(\mathcal{I}')|$, it hence follow that

$$\frac{a^{[L:K]}}{|N_{L|\mathbb{Q}}(\mathcal{I}')|} \in \mathcal{O}_L.$$

From the definition of the norm of an ideal, it is clear that

$$N_{L|\mathbb{Q}}(\mathcal{I}') = N_{K|\mathbb{Q}}(N_{L|K}(\mathcal{I}')).$$

Because $\mathcal{I}' = \mathcal{I}\mathcal{O}_L$, we then see that

$$\begin{aligned} N_{L|\mathbb{Q}}(\mathcal{I}') &= N_{K|\mathbb{Q}}(N_{L|K}(\mathcal{I}\mathcal{O}_L)) \\ &= N_{K|\mathbb{Q}}(\mathcal{I}^{[L:K]}) \\ &= [N_{K|\mathbb{Q}}(\mathcal{I})]^{[L:K]}. \end{aligned}$$

But then

$$\frac{a^{[L:K]}}{|N_{K|\mathbb{Q}}(\mathcal{I})|^{[L:K]}} \in \mathcal{O}_L.$$

Because $\frac{a}{|N_{K|\mathbb{Q}}(\mathcal{I})|} \in L$ is a root of the polynomial

$$x^{[L:K]} - \frac{a^{[L:K]}}{|N_{K|\mathbb{Q}}(\mathcal{I})|^{[L:K]}},$$

the element $\frac{a}{|N_{K|\mathbb{Q}}(\mathcal{I})|}$ is integral over $\mathcal{O}_L$ and hence is in $\mathcal{O}_L$. Similarly, each of the other terms in the coefficient in which $\frac{a}{|N_{K|\mathbb{Q}}(\mathcal{I})|}$ appears is in $\mathcal{O}_L$. The coefficient itself is thus also in $\mathcal{O}_L$.

But we showed above that $f(x_0, \ldots, x_n) \in \mathbb{Q}[x_0, \ldots, x_n]$, so that this coefficient is in $\mathbb{Q}$. Since $\mathbb{Q} \cap \mathcal{O}_L = \mathbb{Z}$, it thus follows that f has integer coefficients as claimed.

Further, notice that $(\xi_0 x_0 + \cdots + \xi_n x_n)$ is a factor of f. Also, because $A_K(\boldsymbol{\xi}) \leq r$, we know that

$$\frac{|\xi_{i_1}^{\sigma_1} \ldots \xi_{i_m}^{\sigma_m}|}{|N_{K|\mathbb{Q}}(\mathcal{I})|} \leq r$$

for each possible product $\xi_{i_1}^{\sigma_1} \ldots \xi_{i_m}^{\sigma_m}$. The number of terms of a symmetric function of $(n+1)$ variables with degree m is $(n+1)^m$, so this is the maximum number of terms in the coefficient of each term of f. Hence, $r(n+1)^m$ is an upper bound for the norms of all coefficients of f.

We have shown that any point $[\xi_0 : \ldots : \xi_n]$ of X corresponds to a factor $(\xi_0 x_0 + \cdots + \xi_n x_n)$ of a form, which like f has degree m and integer coefficients with norm less than or equal to $r(n+1)^m$. However, it is clear that only finitely many such forms exist. Thus, in factoring this finite number of forms over $\mathbb{C}$, the total number of their factors of the type $(\alpha_0 x_0 + \cdots + \alpha_n x_n)$ is also finite because of the bound on the degrees of the forms. There are thus only finitely many candidates for the points of X. □

Suppose that V is the zero set of the forms $f_1, \ldots, f_s \in K[x_0, \ldots, x_n]$. As the first step towards showing the boundedness of K-rational preperiodic points of V under A_K, we prove the following:

Lemma 5.1 *Any point $\boldsymbol{\lambda} = [\lambda_0 : \ldots : \lambda_n]$ of V satisfies*

$$\frac{(|\lambda_0| + \cdots + |\lambda_n|)^l}{|\phi_0(\boldsymbol{\lambda})| + \cdots + |\phi_n(\boldsymbol{\lambda})|} \leq c,$$

where l is the degree of ϕ and c is some (real) constant which depends only on the coefficients of the f_i and the ϕ_j in $\mathbb{C}$.

Proof:

Let $[\alpha_0 : \ldots : \alpha_n] \in V$ with $|\alpha_0| + \cdots + |\alpha_n| = 1$. All points having such co-ordinates,

viewed as points of affine $(n+1)$ space, form a closed and bounded (and hence compact) subset, say S, of $\mathbb{C}^{n+1}$. It is well known that any continuous real-valued function assumes its maximum on such a set. Now

$$g(x_0, \ldots, x_n) = \frac{(|x_0| + \cdots + |x_n|)^l}{|\phi_0(\boldsymbol{x})| + \cdots + |\phi_n(\boldsymbol{x})|}$$

is a continuous real-valued function on S :

Each point of S gives the co-ordinates of a point of V, and for each $\boldsymbol{\alpha} \in V$, $|\phi_0(\boldsymbol{\alpha})| + \cdots + |\phi_n(\boldsymbol{\alpha})| \neq 0$ by the assumption that ϕ is a well defined function on V. Hence, choosing homogeneous co-ordinates $\boldsymbol{\beta} = (\beta_0, \ldots, \beta_n)$ for $\boldsymbol{\alpha}$ which give a point of S, we know that $|\phi_0(\boldsymbol{\beta})| + \cdots + |\phi_n(\boldsymbol{\beta})| \neq 0$ for all $\boldsymbol{\beta} \in S$.

Denote by c the maximum of g on S and observe that c depends only on the coefficients of the f_i and the ϕ_j. Now take any point $\boldsymbol{\lambda} = [\lambda_0 : \ldots : \lambda_n]$ of V. Then there exist homogeneous co-ordinates of $\boldsymbol{\lambda}$ which describe a point of S, (say $(\lambda_0', \ldots, \lambda_n')$), so since the ϕ_j are homogeneous of degree l, $g(\lambda_0', \ldots, \lambda_n') = g(\lambda_0, \ldots, \lambda_n)$ and this proves the lemma. □

Now for f_i and ϕ_j as above, denote by K_0 the subfield of K which is the smallest number field containing the coefficients of the f_i and ϕ_j. By assumption, no common root of $\phi_0, \ldots, \phi_n$ is also a common root of $f_1, \ldots, f_s$. Hence it follows that we can write

$$\sum_{\nu} A'_{i\nu}(\boldsymbol{x})\phi_\nu(\boldsymbol{x}) + \sum_{\mu} B'_{i\mu}(\boldsymbol{x})f_\mu(\boldsymbol{x}) = x_i^{\kappa_i},$$

where $A'_{i\nu}(\boldsymbol{x})$ and $B'_{i\mu}(\boldsymbol{x}) \in K_0[x_0, \ldots, x_n]$. (See [21], page 6 for the details.) Choosing $\rho = \max_i\{\kappa_i\}$, we can multiply each expression by a suitable power of x_i and by some rational integer C, to obtain

$$\sum_{\nu} A_{i\nu}(\boldsymbol{x})\phi_\nu(\boldsymbol{x}) + \sum_{\mu} B_{i\mu}(\boldsymbol{x})f_\mu(\boldsymbol{x}) = Cx_i^{\rho}, \tag{5.1}$$

for $i \in \{0, \ldots, n\}$, where $A_{i\nu}(\boldsymbol{x})$ and $B_{i\mu}(\boldsymbol{x})$ have coefficients in $\mathcal{O}_{K_0}$ for each i, j, ν and μ. Using the above lemma together with (5.1), we can prove:

Theorem 5.2 *Any K-rational point $\boldsymbol{\xi}$ of V satisfies:*

$$A_K^l(\boldsymbol{\xi}) \leq M^{[K:\mathbb{Q}]} A_K(\phi(\boldsymbol{\xi})),$$

where M is a constant depending only on V and ϕ (but not on K.)

Proof:

If $\boldsymbol{\xi} = [\xi_0 : \ldots : \xi_n]$ is any K-rational point of V, let $\mathcal{I} = (\xi_0) + \cdots + (\xi_n)$ and then let E be some number field in which each ideal of K is principal, (see Appendix B) say $\mathcal{I}\mathcal{O}_E = (t)$. But then $\boldsymbol{\xi} = [\frac{\xi_0}{t} : \ldots : \frac{\xi_n}{t}]$ is in $\mathbb{P}^n(\mathbb{C})$, and denoting $\frac{\xi_i}{t}$ by ζ_i, we have that

$$(\zeta_0) + \cdots + (\zeta_n) = (1). \tag{5.2}$$

$\phi(\boldsymbol{\xi})$ is similarly an K-rational point (since K_0 as defined above is contained in K) so that we can also find homogeneous co-ordinates $(\upsilon_0, \ldots, \upsilon_n)$ for $\phi(\boldsymbol{\xi})$ in E such that

$$(\upsilon_0) + \cdots + (\upsilon_n) = (1). \tag{5.3}$$

Then we have that

$$[\upsilon_0 : \ldots : \upsilon_n] = [\phi_0(\xi_0, \ldots, \xi_n) : \ldots : \phi_n(\xi_0, \ldots, \xi_n)]$$

which implies that there exists $\eta \in E$ such that $\phi_i(\boldsymbol{\xi}) = \eta\upsilon_i$ for $i \in 0, 1, \ldots, n$. But then, from (5.3), we know that

$$(\phi_0(\boldsymbol{\xi})) + \cdots + (\phi_n(\boldsymbol{\xi})) = (\eta). \tag{5.4}$$

From Lemma 5.1, we know that

$$\frac{(|\zeta_0| + |\zeta_1| + \cdots + |\zeta_n|)^l}{|\eta|(|\upsilon_0| + |\upsilon_1| + \cdots + |\upsilon_n|)} \leq c'$$

for some c' depending only on V and on ϕ. Now for any given $\mathbb{Q}$-isomorphism of E, say τ, then denoting the variety defined by the conjugates of the defining forms of V by V^τ, it follows that

$$[\zeta_0^\tau : \ldots : \zeta_n^\tau] \in V^\tau.$$

Under ϕ_i^τ the point $(\zeta_0^\tau, \ldots, \zeta_n^\tau)$ will have image $\eta^\tau \upsilon_i^\tau$ for each i, so that

$$\frac{(|\zeta_0^\tau| + |\zeta_1^\tau| + \cdots + |\zeta_n^\tau|)^l}{|\eta^\tau|(|\upsilon_0^\tau| + |\upsilon_1^\tau| + \cdots + |\upsilon_n^\tau|)} \leq c_{(\tau)}.$$

Here $c_{(\tau)}$ is a constant which depends on the coefficients of the defining forms of V^τ and on the coefficients of the forms ϕ_i^τ in precisely the same way as c' depends on the coefficients of the f_i and the ϕ_j. But the product over all $\mathbb{Q}$-isomorphisms τ of E then yields:

$$\frac{\prod_\tau (|\zeta_0^\tau| + |\zeta_1^\tau| + \cdots + |\zeta_n^\tau|)^l}{\prod_\sigma |\eta^\sigma|(|\upsilon_0^\sigma| + |\upsilon_1^\sigma| + \cdots + |\upsilon_n^\sigma|)} \leq c^{[E:\mathbb{Q}]}, \tag{5.5}$$

where $c = max_\tau\{c', c_{(\tau)}\}$. Now from (5.2) and (5.3) we know that

$$|N_{E|\mathbb{Q}}((\zeta_0) + \cdots + (\zeta_n))| = |N_{E|\mathbb{Q}}((1))| = 1$$

and also $|N_{E|\mathbb{Q}}((v_0) + \cdots + (v_n))| = 1$, so (5.5) can be rewritten as:

$$A_E^l(\boldsymbol{\xi}) \leq c^{[E:\mathbb{Q}]}|N_{E|\mathbb{Q}}(\eta)|A_E(\phi(\boldsymbol{\xi})). \tag{5.6}$$

We now find a bound on $|N_{E|\mathbb{Q}}(\eta)|$ and use our knowledge of the form of A_E in terms of A_K to complete the proof: from the expressions in (5.1), namely

$$\sum_\nu A_{i\nu}(\boldsymbol{\xi})\phi_\nu(\boldsymbol{\xi}) + \sum_\mu B_{i\mu}(\boldsymbol{\xi})f_\mu(\boldsymbol{\xi}) = C\xi_i^\rho,$$

for each i, where the coefficients of the $A_{i\nu}$ and the $B_{i\mu}$ are algebraic integers, we find that for our point $\boldsymbol{\xi} = [\zeta_0 : \ldots : \zeta_n]$ of V,

$$\sum_\nu A_{i\nu}(\boldsymbol{\xi})\phi_\nu(\boldsymbol{\xi}) = C\zeta_i^\rho$$

for each i. But then

$$(C)[(\zeta_0)^\rho + \cdots + (\zeta_n)^\rho] \subseteq (\phi_0(\boldsymbol{\xi})) + \cdots + (\phi_n(\boldsymbol{\xi})),$$

as $A_{i\nu}(\boldsymbol{\xi}) \in \mathcal{O}_E$ for each i and ν. From (5.4) it then follows that

$$(C)[(\zeta_0)^\rho + \cdots + (\zeta_n)^\rho] \subseteq (\eta).$$

Thus, because $(\zeta_0) + \cdots + (\zeta_n) = (1)$ implies $(\zeta_0)^\rho + \cdots + (\zeta_n)^\rho = (1)$ (see Appendix B), in fact $(C) \subseteq (\eta)$. But then $C = \eta t$ for some $t \in \mathcal{O}_E$, and hence

$$|N_{E|\mathbb{Q}}(\eta)| = \frac{|N_{E|\mathbb{Q}}(C)|}{|N_{E|\mathbb{Q}}(t)|}.$$

Of course, $|N_{E|\mathbb{Q}}(t)| \in \mathbb{Z}$, and C is itself a rational integer, so that $|N_{E|\mathbb{Q}}(C)| = C^{[E:\mathbb{Q}]}$. Hence,

$$|N_{E|\mathbb{Q}}(\eta)| = \frac{C^{[E:\mathbb{Q}]}}{|N_{E|\mathbb{Q}}(t)|} \leq C^{[E:\mathbb{Q}]}.$$

Combining this with (5.6), we thus have:

$$A_E^l(\boldsymbol{\xi}) \leq c^{[E:\mathbb{Q}]}C^{[E:\mathbb{Q}]}A_E(\phi(\boldsymbol{\xi})).$$

Let $M = cC$ and observe that M depends only on V and ϕ. Using the fact that $A_E(\boldsymbol{v}) = (A_K(\boldsymbol{v}))^{[E:K]}$ for each K-rational point $\boldsymbol{v}$ of V, and extracting $[E : K]$th roots on each side of the inequality yields:

$$A_K^l(\boldsymbol{\xi}) \leq M^{[K:\mathbb{Q}]}A_K(\phi(\boldsymbol{\xi})).\square$$

The properties we have derived thus far with respect to the arithmetic function A_K are valid for any K-rational points of a given variety. In order to complete the proof of the finiteness of the set of all K-rational preperiodic points, we use the bound in the above theorem to show that such preperiodic points are all elements of the set X of Theorem 5.1, i.e. that they are K-rational points which are bounded above under the action of A_K by some fixed positive integer. This we do by means of the following

Lemma 5.2 *Let ξ be any K-rational point of V which is preperiodic under the action of ϕ on V. Then*

$$A_K(\xi) \leq M^{\frac{[K:\mathbb{Q}]}{l-1}},$$

where M is the constant of Theorem 5.2.

Proof:

Suppose that ξ is some K-rational preperiodic point of V such that

$$A_K(\xi) > M^{\frac{[K:\mathbb{Q}]}{l-1}},$$

and let the image set of ξ with respect to succesive application of ϕ be $\{\xi = \xi^{(0)}, \xi^{(1)} = \phi(\xi), \ldots, \xi^{(s)} = \phi^s(\xi)\}$ for some finite s. Now

$$\begin{aligned} A_K^l(\xi^{(0)}) &\leq M^{[K:\mathbb{Q}]} A_K(\phi(\xi)) \\ &= M^{[K:\mathbb{Q}]} A_K(\xi^{(1)}) \end{aligned}$$

from Theorem 5.2, giving

$$\frac{A_K(\xi^{(1)})}{A_K(\xi^{(0)})} \geq \frac{A_K^{(l-1)}(\xi^{(0)})}{M^{[K:\mathbb{Q}]}} = \left[\frac{A_K(\xi^{(0)})}{M^{\frac{[K:\mathbb{Q}]}{l-1}}}\right]^{(l-1)} > 1.$$

But then $A_K(\xi^{(1)}) > A_K(\xi^{(0)})$ and $A_K(\xi^{(0)}) > M^{\frac{[K:\mathbb{Q}]}{l-1}}$, so $A_K(\xi^{(1)}) > M^{\frac{[K:\mathbb{Q}]}{l-1}}$, which shows that the argument can be repeated ($\xi^{(1)}$ is also a point of V) which would then yield

$$A_K(\xi^{(0)}) < A_K(\xi^{(1)}) < \ldots < A_K(\xi^{(s)}) < A_K(\xi^{(t)})$$

for some t with $1 \leq t < s$ (since ξ is preperiodic). i.e. $A_K(\xi^{(t)}) < A_K(\xi^{(t)})$. This absurdity proves the lemma. □

A synthesis of Lemma 5.2 and Theorem 5.1 produces:

Theorem 5.3 (Northcott) *If $\phi : V \longrightarrow V$ is a non-linear morphism of a variety V, (which is defined over a number field K), and the coefficients of the forms defining the action of ϕ are all algebraic integers, then the set of preperiodic points of V which are rational relative to any of the number fields of a fixed degree over $\mathbb{Q}$, is finite.*

5.2 The finiteness of the number of attracting periodic points under a separable morphism

A morphism $\phi : \mathbb{P}^1_K \to \mathbb{P}^1_K$ which has good reduction can only have non-repelling periodic points since the JULIA set of such a morphism is empty (see Chapter 4), and all periodic points of the FATOU set of ϕ are non-repelling (see Chapter 3). More can be said when the reduced map $\tilde{\phi}$ is separable (i.e. when the function field[1] $F(\mathbb{P}^1(\overline{K}))$ is a separable extension of $F(\tilde{\phi}(\mathbb{P}^1(\overline{K})))$: in this case, MORTON and SILVERMAN have shown that ϕ can have at most finitely many attracting fixed points. Their proof makes use of the finiteness of the number of ramification points under a separable morphism between curves, as well as information pertaining to the zero-cycles of certain intersections of subvarieties of $\mathbb{P}^1_K \times \mathbb{P}^1_K$ and of $\mathbb{P}^1_{\overline{K}} \times \mathbb{P}^1_{\overline{K}}$ respectively.

In discussing their proof, we firstly expound technical machinery related to the mapping on the cotangent spaces at points on a curve which is induced by a morphism acting on the curve, thereafter defining the relevant cycles and describing properties of direct bearing to this proof.

5.2.1 The mapping on the cotangent space induced by a morphism

Let P be a point on a smooth projective curve X which is defined over a field K, and suppose that $\phi : X \to X$ is a morphism. P has an affine neighbourhood A, for which we can choose co-ordinates such that P is at the origin $(0, \ldots, 0)$ in $A \subset \mathbb{A}^n(K)$. With X being a curve, its points in this affine set are the zeros of a system of polynomials $\{f_i(x_1, \ldots, x_n) : i = 1, \ldots, m\}$. Writing $f_i(x_1, \ldots, x_n) = L_i(x_1, \ldots, x_n) + g_i(x_1, \ldots, x_n)$ where L_i is linear in $\{x_1, \ldots, x_n\}$, but the degree of each term of g_i is greater than or equal to 2 (which is possible since $f_i(P) = f_i((0, \ldots, 0)) = 0$), we define the tangent space $\Theta_{P,X}$ of X at P to be the zero set of $\{L_i : i = 1, \ldots, m\}$ in $\mathbb{A}^n(K)$. The space of linear forms on $\Theta_{P,X}$ (i.e. its dual space $\Theta^*_{P,X}$) is referred to as the *cotangent space* of X at P.

A useful characterization of the cotangent space which facilitates the definition of a map of the cotangent space, is the following:

Proposition 5.1 *For any $P \in X$, a smooth projective curve defined over a field K, if*

[1] See [6], page 16 or [14], page 29 for the definition of the *function field* $F(X)$ of a variety X.

$\mathcal{M}_P$ is the maximal ideal of the ring of regular functions at P, then

$$\Theta^*_{P,X} \cong \mathcal{M}_P/\mathcal{M}_P^2 \text{ as } K\text{-vector spaces.}$$

Proof: As before, we can restrict our attention to some affine neighbourhood A of P since our concern is with local properties of the curve at P. Thus suppose that $A \subset \mathbb{A}^n(K)$ and that $P = (y_1, \ldots, y_n)$ in A.

Now the homogeneous co-ordinate ring $\Gamma(X)$ of X is made up from the glueing of affine co-ordinate rings corresponding to each of the affine neighbourhoods which can be chosen to irredundantly cover X. We thus restrict our attention to the affine co-ordinate ring which is associated to A in this construction, and denote it by $\Gamma_X(A)$. Then if $\mathcal{I}_X(A)$ is the ideal of X viewed in this patch of the co-ordinate ring $\Gamma(X)$, we know that $\Gamma_X(A) = K[x_1, \ldots, x_n]/(\mathcal{I}_X(A))$.

Now let $\mathfrak{m}_P = \{f \in \Gamma_X(A) : f(P) = 0\}$. Because the ring of regular functions at P is isomorphic to the localization of the affine co-ordinate ring $\Gamma_X(A)$ at $\mathfrak{m}_P$, (see [6, Theorem I.3.2(c)]), we know that the maximal ideals of these rings are isomorphic. i.e, $\mathcal{M}_P \cong \mathfrak{m}_P$. Hence $\mathcal{M}_P/\mathcal{M}_P^2 \cong \mathfrak{m}_P/\mathfrak{m}_P^2$ and we thus proceed to exhibit an isomorphism of $\mathfrak{m}_P/\mathfrak{m}_P^2$ onto $\Theta^*_{P,X}$.

Now for any $H \in K[x_1, \ldots, x_n]$, let

$$d_P H = \sum_{i=1}^{n} \frac{\partial H}{\partial x_i}(P)(x_i - y_i).$$

Clearly,

$$d_P(H + J) = d_P H + d_P J \tag{5.7}$$

and

$$d_P(HJ) = H(P)d_P J + J(P)d_P H \tag{5.8}$$

for any H and $J \in K[x_1, \ldots, x_n]$. Moreover, if $\mathcal{I}_X(A)$ is given by $\mathcal{I}_X(A) = (F_1, \ldots, F_r)$, then $\Theta_{P,X}$ is defined by $d_P F_1 = \cdots = d_P F_r = 0$: this follows because if $T = (x_1, \ldots, x_n)$, then in the TAYLOR expansions $F_i(T) = F_i(P) + F_i^{(1)}(T) + \cdots + F_i^{(l_i)}(T)$ for each i, where $F_i^{(j)}(T)$ is homogeneous of degree j, the zeros of the linear terms $F_i^{(1)}(T) = d_P F_i$ determine the tangent space.

Now let $g \in \Gamma_X(A)$ be arbitrary. Then g is determined modulo $\mathcal{I}_X(A)$ by the restriction of some polynomial $G \in K[x_1, \ldots, x_n]$ to A. Supposing that $P = (0, \ldots, 0)$ in A, it follows that $d_P G$ is a linear form. If we let $d_P g = d_P G$, and view this form as a mapping of

the tangent space of X at P, then the association of g to $d_P g$ is well-defined: if F is an arbitrary element of $\mathcal{I}_X(A)$, then g is also determined by the restriction of $F+G$ to X. However, $F = H_1F_1 + \cdots + H_rF_r$ where $H_i \in K[x_1, \ldots, x_n]$ and $d_P F_i$ is the zero form on the tangent space for each i. Thus, applying (5.7) and (5.8) to the sum of products of functions H_iF_i (where $F_i(P) = 0$ and $d_P F_i = 0$ for every i), we see that $d_P F = 0$, and consequently, $d_P(G+F) = d_P G + d_P F = d_P G$.

We claim that d_P is a mapping of $\mathfrak{m}_P$ onto $\Theta^*_{P,X}$ which produces the required isomorphism: In order to see this, we firstly show that $d_P(\mathfrak{m}_P) = \Theta^*_{P,X}$: each $f \in \Gamma_X(A)$ vanishing at P is mapped to a linear form on $\mathbb{A}^n$ and hence on $\Theta_{P,X}$. Also, each linear form of $\Theta^*_{P,X}$, say θ, is the image under d_P of some $\kappa \in \mathfrak{m}_P$, because with $P = (0, \ldots, 0)$ in A as above, any polynomial mapping of A say γ, having a TAYLOR expansion at P given by $\gamma(T) = \gamma(P) + \theta(T) + \gamma_2(T) + \ldots + \gamma_t(T)$, has $d_P(\gamma) = \theta$; so that also $d_P(\gamma - \gamma(P)) = \theta$, where $\gamma - \gamma(P) \in \mathfrak{m}_P$.

Furthermore, $ker(d_P) = \mathfrak{m}_P^2$, as we proceed to show: suppose that $g \in \mathfrak{m}_P$ has $d_P g = 0$ and that G is some polynomial such that $d_P G = d_P g$. Now since $\Theta_{P,X}$ is defined by $d_P F_1 = \cdots = d_P F_r = 0$, each linear form on $\Theta_{P,X}$ is defined moldulo the linear forms $d_P F_i$ for $i \in \{1, \ldots, r\}$ - in other words, $\{d_P F_1, \ldots, d_P F_r\}$ spans the null-space of $\Theta^*_{P,X}$. Now $d_P G$ is a linear form which vanishes on $\Theta_{P,X}$, and is thus an element of this null-space. Thus, there exist $\lambda_1, \ldots, \lambda_r \in K$ such that

$$d_P G = \lambda_1 d_P F_1 + \cdots + \lambda_r d_P F_r. \tag{5.9}$$

Let $G_1 = G - \lambda_1 F_1 - \cdots - \lambda_r F_r$, so that $G_1(P) = G(P) - \lambda_1 F_1(P) - \cdots - \lambda_r F_r(P) = G(P) = 0$ since $G|_X = g$ and $g \in \mathfrak{m}_P$ implies that $g(P) = 0$. Also, $d_P G_1 = 0$ from (5.9) together with (5.7) and (5.8), and consequently, G_1 has no constant or linear terms. However, $G_1|_X = G|_X = g$ since $F_i(Q) = 0$ for all $Q \in X$ and for each i. Thus, g is an element of the square of the ideal generated by $\{x_1, \ldots, x_n\}$, which we denote by $(x_1, \ldots, x_n)^2$. Since $P = (0, \ldots, 0)$, it is evident that $\mathfrak{m}_P = (x_1, \ldots, x_n)$, and as a result $g \in \mathfrak{m}_P^2$. Hence, $ker(d_P) = \mathfrak{m}_P^2$, proving the claim, since then $\mathfrak{m}_P/\mathfrak{m}_P^2 \cong \Theta^*_{P,X}$. □

If X is as above, any given morphism $\phi : X \to X$ induces a map ϕ^* of $\Theta^*_{\phi(P),X}$ to $\Theta^*_{(P),X}$ given by $l \mapsto l \circ \phi$ for any $l \in \mathcal{M}_{\phi(P)}/\mathcal{M}^2_{\phi(P)}$.

Suppose now that P is a fixed point of ϕ and z is a uniformizer for the ring of regular functions at P (i.e. z vanishes to order 1 at P). Owing to the fact that ϕ is a morphism which fixes P, and also because $z \in \mathcal{M}_P$, it follows that $z \circ \phi \in \mathcal{M}_P$, so that $z \circ \phi$

is expressible as a power series in z with no constant term. But then it is clear that $(z+\mathcal{M}_P^2)\circ\phi \equiv \phi^*(P)z \pmod{\mathcal{M}_P^2}$, where the scalar $\phi^*(P)$ determines the map on the parameter z up to order 2. i.e.,

$$z\circ\phi = \phi^*(P)z + O(z^2), \tag{5.10}$$

where $O(z^2)$ denotes terms vanishing at P to order greater than or equal to 2. Now the mapping on any $l \in \mathcal{M}_P/\mathcal{M}_P^2$ is also determined by this scalar: l is expressible as a power series in z with no constant term, so an arbitrary term of this power series is uz^r, some regular function at P, where $u \in K$, and $r \geq 1$. Then

$$\begin{aligned} uz^r\circ\phi &= (u\circ\phi)(z\circ\phi)^r \\ &= u(z\circ\phi)^r \qquad \text{since } u\in K \\ &= u(\phi^*(P)z + O(z^2))^r. \end{aligned}$$

Considering what happens term for term under the mapping on the cotangent space applied to l, it is then clear that $l\circ\phi = \phi^*(P)u_1z + O(z^2)$ where $u_1 \in K$ is the coefficient of z in l. Since $O(z^2) \in \mathcal{M}_P^2$ in every case, the scalar $\phi^*(P)$ determines the map modulo $\mathcal{M}_P^2$.

Proposition 5.2 *With notation as above, when $X = \mathbb{P}^1$ and $P \in \mathbb{P}^1(K)$ is a fixed point of ϕ, then the scalar $\phi^*(P)$ is given by $\phi'(P)$, the derivative of ϕ at P*

Proof: $\mathbb{P}^1(K)$ is the zero set of the homogeneous polynomial $f(x,y) = 0$, so the tangent space of any point of $\mathbb{P}^1(K)$ barring $[1:0]$ is isomorphic to $\mathbb{A}^1(K)$. (We know that the dimension of the tangent space of a variety is the same as that of the variety from [6, Theorem I.3.2(c)] since the ring of regular functions at P is a regular local ring.) Suppose that $P = [0:1]$ under some co-ordinate change if necessary. Now each linear form on $\mathbb{A}^1(K)$ can be written as $l(z) = \alpha z$ for some $\alpha \in K$, where z is a uniformizing parameter at P.

As explained in Chapter 2 we can view ϕ as a rational function of some affine neighbourhood of $P = [0:1]$. i.e., ϕ is the quotient of two polynomials, the denominator of which has no zeros on this neighbourhood. At P we can hence write ϕ as a power series using its TAYLOR expansion: $\phi(z) = \phi(P) + \phi'(P)z + O(z^2)$, where $O(z^2)$ again denotes terms vanishing to order greater than one at P. Here $\phi(P)$ is the image of the point corresponding

to P in the embedding of K into $\mathbb{P}^1(K)$, under the rational function ϕ. i.e. $\phi(P) = \phi(0)$, so since ϕ fixes P, in fact $\phi(P) = 0$, and we have that $\phi(z) = \phi'(P)z + O(z^2)$.

Thus,

$$l \circ \phi(z) \equiv \alpha\phi'(P)z + O(z^2) \pmod{\mathcal{M}_P^2}.$$

However, in the text we saw that $l \circ \phi(z) \equiv \phi^*(P)\alpha z \pmod{\mathcal{M}_P^2}$ since $\alpha \in K$ is the coefficient of the linear term in the expansion of l as a power series about z.

It then follows that with $\alpha\phi'(P)$ and $\alpha\phi^*(P)$ being constants, in fact $\phi'(P) = \phi^*(P)$. □

The next lemma describes a situation which will prove to be of direct bearing to our subsequent discussion, but we firstly require a definition:

Definition 5.1 *A ramification point of a morphism $\chi : X \to Y$ of smooth projective curves is a point $P \in X$ such that if t is a uniformizer of $\mathcal{O}_{\chi(P),Y}$, then $v_P(t \circ \chi) > 1$ (where v_P denotes the valuation on $\mathcal{O}_{P,X}$).*

If such a morphism $\chi : X \to Y$ induces a mapping $\chi^\#$ of the function field $F(Y)$ of Y into the function field $F(X)$ in such a way that $F(X) \mid \chi^\#(F(Y))$ is a separable extension, then the morphism is referred to as being *separable*. A separable morphism of smooth projective curves can have at most finitely many ramification points. (See STICHTENOTH [20], page 82 : under the separability assumption, the support of the divisor which registers the ramification at any place of a function field is finite.)

If the curve X has genus greater than 1 and $\chi : X \to X$ is separable, then from the RIEMANN-HURWITZ formula, (see [20, Chapter III]), it induces an automorphism of the curve. This means that the function fields $F(X)$ and $\chi^\#(F(X))$ are isomorphic, so there are no ramification points.

Notice that if $X = Y$ in our definition, and P is fixed by χ, then P is a ramification point of χ if and only if $v_P(t \circ \chi) > 1$, which is equivalent to $v_P(\chi^*(P)t + O(t^2)) > 1$, which in turn holds if and only if $\chi^*(P) = 0$. We proceed to generalize this fact in the form in which we shall later require it:

Lemma 5.3 *If ψ is a morphism of a smooth projective curve Y to itself and $Q \in Y$ is a fixed point of ψ^m such that the mapping $(\psi^m)^*$ of the cotangent space $\Theta_{Q,Y}^*$ to itself is the zero mapping (i.e. $(\psi^m)^*(Q) = 0$), then some point in the orbit of Q under ψ is a ramification point of ψ.*

Proof: Suppose to the contrary that there is no ramification at any point in the orbit of Q under ψ. Let y denote a uniformizer of $\mathcal{O}_Q$, the ring of regular functions at Q, and for each $i \in \{1, \ldots, m\}$ notate the valuation on the ring $\mathcal{O}_{\psi^i(Q)}$ by $v_{\psi^i(Q)}$. Then since there is no ramification at $\psi^{m-1}(Q)$, we know that $v_{\psi^{m-1}(Q)}(y \circ \psi) = 1$. (Here we are viewing y as a uniformizer of $\mathcal{O}_{\psi^m(Q)}$, which is - trivially - admissible since $\psi^m(Q) = Q$.) But then $y \circ \psi$ is a uniformizer of $\mathcal{O}_{\psi^{m-1}(Q)}$, so because there is no ramification at $\psi^{m-2}(Q)$, it similaraly follows that $v_{\psi^{m-2}(Q)}(y \circ \psi^2) = v_{\psi^{m-2}(Q)}((y \circ \psi) \circ \psi) = 1$, and $y \circ \psi^2$ is a uniformizer of $\mathcal{O}_{\psi^{m-2}(Q)}$. Continuing in this way, we find that $y \circ \psi^m$ is a uniformizer of $\mathcal{O}_Q$. However, we showed that $y \circ \psi^m = (\psi^m)^*(Q)y + O(y^2)$ (with notation as above), so that in this case, $y \circ \psi^m = O(y^2)$. But this means that $v_Q(y \circ \psi^m) \geq 2$, a contradiction. There *is* thus some ramification point in the orbit of Q under ψ as asserted. □

Observation: From the finiteness of the number of ramification points on a smooth projective curve Y under a given separable morphism $\psi : Y \to Y$, it follows that there are only finitely many periodic points P_i of Y for which $(\psi^{m_i})^*(P_i) = 0$ (where m_i is the period of P_i).

5.2.2 Cycles of periodic points

Let X be a smooth projective curve and denote the diagonal of $X \times X$ (i.e. the subvariety of $X \times X$ defined by the equation $z_1 = z_2$ if the points of $X \times X$ are given by pairs (z_1, z_2)), by $\Delta(X)$. If $\phi : X \to X$ is a morphism, we let $\Gamma(\phi)$ denote the graph of ϕ : $\Gamma(\phi) := \{(P, \phi(P)) : P \in X\} \subset X \times X$. Now $\Delta(X) \cap \Gamma(\phi)$ is a finite set of points or it is empty whenever it is not the whole diagonal: indeed, observe that both $\Gamma(\phi)$ and $\Delta(X)$ are isomorphic to X. They are thus curves (i.e. varieties having dimension 1), which are irreducible if we assume that X is irreducible. The intersection of any two curves is a variety with dimension 1 or 0. Being irreducible, the diagonal cannot have a proper subvariety of dimension 1. Thus the intersection is either the whole diagonal (when ϕ is the identity mapping); it is a finite set of points; or it is empty.

Suppose then that ϕ is not the identity and let P be any point of the intersection of $\Delta(X)$ and $\Gamma(\phi)$. If z is a local parameter for the ring $\mathcal{O}_{P,X}$ (the ring of regular functions at P), then locally around P, the intersection of $\Delta(X)$ and $\Gamma(\phi)$ corresponds to the zeros of $z \circ \phi - z$: this is because as subvarieties of $X \times X$, $\Delta(X)$ and $\Gamma(\phi)$ can be thought of as the roots of the polynomials $z_1 - z_2$ and $z_1 \circ \phi - z_2$ respectively, where again the points

of $X \times X$ are given by pairs (z_1, z_2). Because ϕ is a morphism, $z \circ \phi \in \mathcal{O}_{P,X}$, and since $z \circ \phi(P) = 0$, it follows that $z \circ \phi - z \in z^e \mathcal{O}_{P,X}$ for some $e \geq 1$. We denote by $a_P(\phi)$ the greatest e for which this occurs. (When $P \notin \Delta(X) \cap \Gamma(\phi)$, we set $a_P(\phi) = 0$.) It is clear that $a_P(\phi)$ indicates the multiplicity to which P is a root of $z \circ \phi - z$ - i.e. the multiplicity of P as a point of the intersection of $\Delta(X)$ and $\Gamma(\phi)$.[2] If we work with ϕ^n instead of ϕ, we write $a_P(\phi^n) = a_P(\phi, n)$. Now we define the divisor

$$Z_n(\phi) := \sum_{P \in \Delta(X) \cap \Gamma(\phi)} a_P(\phi, n) P,$$

which we shall refer to as the cycle of n-periodic points of ϕ,[3] as clearly,

$$P \in Supp\{Z_n(\phi)\} \Leftrightarrow \phi^n(P) = P.$$

The points appearing in $Z_n(\phi)$ may not have exact period n, so in order to eliminate superfluous information, we define the cycle of essential n-periodic points as

$$Z_n^*(\phi) := \sum_{d|n} \mu\left(\frac{n}{d}\right) Z_d(\phi) \quad := \sum_{P \in Supp\{Z_n(\phi)\}} a_P^*(\phi, n) P$$

where $\mu(\cdot)$ is the MÖBIUS function,

$$\mu(T) = \begin{cases} 1 & \text{if } T = 1; \\ 0 & \text{if } p^2 | T \text{ for some prime } p; \\ (-1)^t & \text{if } T = p_1 \ldots p_t \text{ where } p_1, \ldots, p_t \text{ are distinct primes.} \end{cases}$$

We will show that although this cycle includes all points of exact period n, it may include others as well. The reason that it is particularly useful is that we can relatively easily derive information about the cycle with the aid of well-known properties of the MÖBIUS function. Effectively, using little more than the standard facts from elementary number theory that $\mu(\cdot)$ is multiplicative and if $T > 1$, then $\sum_{d|T} \mu\left(\frac{T}{d}\right) = 0$, we can give a precise description of those n for which a periodic point P of a map $\phi : X \to X$ has $a_P^*(\phi, n) \geq 1$. In order to do this, we shall frequently require the following

Auxilliary Lemma *If X is a smooth projective curve defined over a field K, and $P \in X$ is a fixed point of the morphism $\phi : X \to X$, then*

(1) $a_P(\phi, n) \geq a_P(\phi, 1)$ for every $n \geq 1$, and

(2) $a_P(\phi, n) > a_P(\phi, 1)$ if and only if either:

[2] In the study of intersections of varieties (Intersection Theory), $a_P(\phi)$ corresponds to the index of intersection of the varieties $\Delta(X)$ and $\Gamma(\phi)$ at P.

[3] In the language of Intersection Theory, this is a zero-cycle on X since points are zero-dimensional.

(i) $a_P(\phi, 1) = 1$ *and* $(\phi^*)(P)^n = 1$ *or*
(ii) $a_P(\phi, 1) > 1$ *and* $n = 0$ *in* K,
in the latter of which cases, $a_P(\phi, n) \geq 2a_P(\phi, 1) - 1$.

Proof: For notational convenience, let $a_P(\phi) = e$. Now if z is a uniformizer at P, then by definition, $z \circ \phi - z \in z^e \mathcal{O}_{P,X}$. Hence, $a_P(\phi) = e \geq 1$, and we can set

$$z \circ \phi = z + O(z^e) \tag{5.11}$$

where $O(z^e)$ represents terms vanishing to order greater than or equal to e at P. But then $z \circ \phi^2 = z \circ \phi + O(z^e) \circ \phi$, where because ϕ fixes P, $O(z^e) \circ \phi = O(z^e)$. Substituting (5.11) into this identity yields that

$$z \circ \phi^2 = z + O(z^e) + O(z^e) = z + O(z^e).$$

Repeating this procedure gives that $z \circ \phi^i = z + O(z^e)$ for every $i \geq 1$.

If $h \in \mathcal{O}_{P,X} \backslash z\mathcal{O}_{P,X}$, it has a power series expansion about P, (i.e. in terms of the parameter z). Now for any $u \in K$ and for each $t \geq 1$,

$$\begin{aligned} uz^t \circ \phi^i &= (u \circ \phi)(z \circ \phi^i)^t \\ &= u(z \circ \phi^i)^t \qquad \text{since } u \in K \\ &= u(z + O(z^e))^t \\ &= uz^t + O(z^{e+t-1}). \end{aligned}$$

Thus

$$h \circ \phi^i = h + O(z^e) \tag{5.12}$$

for all $i \geq 1$, considering what occurs under composition by ϕ^i term for term.

Setting

$$z \circ \phi = z + z^e g \tag{5.13}$$

for some g which is a unit in $\mathcal{O}_{P,X}$ (i.e. $g \in \mathcal{O}_{P,X} \backslash z\mathcal{O}_{P,X}$) we have that

$$\begin{aligned} z \circ \phi^2 &= z \circ \phi + z^e g \circ \phi \\ &= z + z^e g + z^e(\phi) g(\phi) \qquad \text{from (5.13)} \\ &= z + z^e g + (z \circ \phi)^e (g(\phi)) \\ &= z + z^e g + (z + z^e g)^e (g(\phi)) \qquad \text{from (5.13)} \\ &= z + z^e g + (z^e + O(z^{e+e-1}))(g \circ \phi) \\ &= z + z^e g + z^e (g \circ \phi) + O(z^{2e-1}). \end{aligned}$$

Suppose that for some $k \in \mathbb{N}$ it were true that $z \circ \phi^k = z + z^e \sum_{i=0}^{k-1} g \circ \phi^i + O(z^{2e-1})$. Then

$$\begin{aligned} & z \circ \phi^{k+1} \\ = \; & z \circ \phi + z^e (\sum_{i=0}^{k-1} g \circ \phi^i) \circ \phi + O(z^{2e-1}) \\ = \; & z + z^e g + (z^e + O(z^{2e-1}))(\sum_{i=1}^{k} g \circ \phi^i) + O(z^{2e-1}) \\ & \text{(as in the above calculation and from (5.13))} \\ = \; & z + z^e (\sum_{i=0}^{(k+1)-1} g \circ \phi^i) + O(z^{2e-1}) \end{aligned}$$

so that by induction, it follows that

$$z \circ \phi^n = z + z^e \sum_{i=0}^{n-1} g \circ \phi^i + O(z^{2e-1}) \tag{5.14}$$

for each $n \geq 1$. Now since $g \in \mathcal{O}_{P,X} \backslash z\mathcal{O}_{P,X}$, from (5.12) we know that also $g \circ \phi^i = g + O(z^e)$ for each $i \geq 1$. Substituting this into (5.14) gives

$$z \circ \phi^n = z + z^e(ng + O(z^e)) + O(z^{2e-1}) = z + nz^e g + O(z^{2e-1}).$$

Then

$$a_P(\phi, n) = v_P(z \circ \phi^n - z) = v_P(nz^e g + O(z^{2e-1})) \geq e = a_P(\phi, 1),$$

proving (1).

Furthermore, if $e = a_P(\phi, 1) \geq 2$, then $2e - 1 > e$, so

$$a_P(\phi, n) = v_P(z \circ \phi^n - z) = v_P(nz^e g + O(z^{2e-1})) \begin{cases} = e & \text{if } n \neq 0 \text{ in } K \\ \geq 2e-1 & \text{if } n = 0 \text{ in } K, \end{cases}$$

showing that (2)(ii) is true.

Finally we consider the case of $a_P(\phi, 1) = 1$. Then $z \circ \phi - z \in z\mathcal{O}_{P,X}$, so that for some $f \in \mathcal{O}_{P,X} \backslash z\mathcal{O}_{P,X}$, $z \circ \phi = zf$. Thus

$$\begin{aligned} z \circ \phi^2 &= zf \circ \phi \\ &= (z \circ \phi)(f \circ \phi) \\ &= (zf)(f \circ \phi) \end{aligned}$$

and if for some $k \in \mathbb{N}$, it is true that $z \circ \phi^k = z \prod_{i=0}^{k-1} f \circ \phi^i$, it follows that

$$z \circ \phi^{k+1} = (z \prod_{i=0}^{k-1} f \circ \phi^i) \circ \phi$$

$$\begin{aligned} &= (z \circ \phi)(\prod_{i=1}^{k} f \circ \phi^i) \\ &= (zf)(\prod_{i=1}^{(k+1)-1} f \circ \phi^i) \\ &= z \prod_{i=0}^{(k+1)-1} f \circ \phi^i \end{aligned}$$

so that by induction, $z \circ \phi^n = z \prod_{i=0}^{n-1} f \circ \phi^i$ for each $n \geq 1$. But then

$$(z \circ \phi^n - z)(P) = z(P)(\prod_{i=0}^{n-1} f \circ \phi^i(P) - 1) = z(P)(f^n(P) - 1).$$

Now since $zf = z \circ \phi = \phi^*(P)z + O(z^2)$ and f has a power series expansion in terms of z, $f(z) = f(P) + O(z)$ at P, it follows that $f(P) = \phi^*(P)$. Consequently,

$$(z \circ \phi^n - z)(P) = z(P)(f^n(P) - 1) = z(P)([\phi^*(P)]^n - 1)$$

so that

$$a_P(\phi, n) = v_P(z \circ \phi^n - z) \begin{cases} = 1 & \text{if } [\phi^*(P)]^n \neq 1 \\ \geq 2 & \text{if } [\phi^*(P)]^n = 1. \end{cases}$$

This proves the lemma. □

Using the Auxilliary Lemma, we can now prove a result which gives applicable information about the cycles defined above:

Lemma 5.4 *Suppose that X/K is a smooth projective curve defined over a field K of characteristic p, and $\phi : X \to X$ is a non-constant morphism defined over K for which the n-fold composition is not the identity mapping on X. Let $P \in X$ be fixed. Denote by m the exact period of P, setting $m = \infty$ if P is not a periodic point of ϕ; and let r be the multiplicative period of $(\phi^m)^*(P)$ in the unit group of some algebraic closure of K, with $r = \infty$ whenever $m = \infty$ or $(\phi^m)^*(P)$ is not a root of unity.*

Then with notation as in the definition of the essential cycle of n-periodic points of ϕ, $Z_n^*(\phi)$,

(1) $a_P^*(\phi, n) \geq 0$ for all $n \geq 1$ and

(2) for $n \geq 1$, $a_P^*(\phi, n) \geq 1$ if and only if:

(i) $n = m$ or

(ii) $n = mr$ (where, if $r = 1$, then $a_P^*(\phi, n) \geq 2$) or

(iii) $n = p^s mr$ *for some* $s \geq 1$,

in the latter of which cases, $a_P^*(\phi, n) \geq 2^{s-1}(a_P(\phi, mr) - 1)$.

Proof: Firstly notice that we can write $a_P^*(\phi, n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) a_P(\phi, d)$ from the definition of $Z_n^*(\phi)$.

If $\phi^n(P) \neq P$, also $\phi^d(P) \neq P$ for each d dividing n, so that by definition, $a_P(\phi, d) = 0$ for all such d, and hence, $a_P^*(\phi, n) = 0$. This proves the proposition in this case.

For the remainder of the proof, suppose then that $\phi^n(P) = P$ and P has exact period m. Then $m|n$, so let N be the positive integer such that $n = Nm$.

The proof is most conveniently handled by considering the following cases:

(α) $N = 1$

(β) $N > 1$ and $r = 1$ (i) $N \neq 0$ in K

(ii) $N = 0$ in K

(γ) $N > 1$ and $r > 1$ (i) $a_P^*(\phi^m, N) \geq 2$

(ii) $a_P^*(\phi^m, N) = 1$.

We firstly make some observations which will ease the discussion.

Let z be a uniformizer at P (i.e. z is a local parameter for $\mathcal{O}_{P,X}$, the ring of regular functions at P). By the definition of the cycles of periodic points of ϕ, $a_P(\phi^t, m)$ is the order to which $z \circ (\phi^t)^m - z = z \circ \phi^{tm} - z$ vanishes at P. It is thus clear that

$$a_P(\phi^t, m) = a_P(\phi^{tm}, 1) = a_P(\phi, tm). \tag{5.15}$$

Now

$$a_P^*(\phi, n) = \sum_{d|n \text{ with } m|d} \mu\left(\frac{n}{d}\right) a_P(\phi, d)$$

since $\phi^d(P) \neq P$ whenever $m \nmid d$, so that for such d, $a_P(\phi, d) = 0$ as above. Setting $d = mt$, this gives

$$\begin{aligned} a_P^*(\phi, n) &= \sum_{t|\frac{n}{m}} \mu\left(\frac{n}{mt}\right) a_P(\phi, mt) \\ &= \sum_{t|N} \mu\left(\frac{N}{t}\right) a_P(\phi^m, t) \qquad \text{using (5.15)} \qquad (5.16) \\ &= a_P^*(\phi^m, N) \qquad \text{by definition.} \end{aligned}$$

From equation (5.10) and the definition of $a_P(\phi, m)$, we know that

$$\begin{aligned} a_P(\phi, m) &= v_P(z \circ \phi^m - z) \\ &= v_P((\phi^m)^*(P)z + O(z^2) - z) \\ &= v_P(((\phi^m)^*(P) - 1)z + O(z^2)) \begin{cases} = 1 & \text{if } (\phi^m)^*(P) \neq 1 \\ \geq 2 & \text{if } (\phi^m)^*(P) = 1. \end{cases} \end{aligned}$$

i.e.

$$a_P(\phi^m, 1) \geq 2 \Leftrightarrow r = 1. \tag{5.17}$$

Case(α): $N = 1$.

Then $n = m$ so that $a_P^*(\phi, n) = a_P^*(\phi^m, 1)$ from (5.15) and this in turn is equal to $a_P(\phi^m, 1)$ by definition. Since P is fixed by ϕ^m, $a_P(\phi^m, 1) \geq 1$ always. Moreover, from (5.17), $a_P(\phi^m, 1) \geq 2 \Leftrightarrow r = 1$. This shows that the assertions concerning the case of $n = m$ are true.

Case(β)(i): $N > 1$, $N \neq 0$ in K and $r = 1$.

From (5.17), $a_P(\phi^m, 1) \geq 2$, so since $\phi^m(P) = P$, it follows from the Auxilliary Lemma applied to ϕ^m that $a_P(\phi^m, N) = a_P(\phi^m, 1)$. Now for any $d|N$, also $d \neq 0$ in K, so for all such d, also $a_P(\phi^m, d) = a_P(\phi^m, 1)$ from the Auxilliary Lemma. But now

$$\begin{aligned} a_P^*(\phi, n) &= \sum_{d|N} \mu\left(\tfrac{N}{d}\right) a_P(\phi^m, d) \\ &= \left(\sum_{d|N} \mu\left(\tfrac{n}{d}\right)\right) a_P(\phi^m, 1) \\ &= 0 \end{aligned}$$

since $N > 1$ so we can apply the standard property of the Möbius function mentioned above.

Because of our assumptions on N and r, it is not possible for n to be given by m, mr or $p^s mr$ for any $s \geq 1$. Thus, we have proved the proposition in this case.

Case(β)(ii): $N > 1$, $N = 0$ in K and $r = 1$.

Let $N = p^t M$ for some $t \geq 1$, where $p \nmid M$. Again, $a_P(\phi^m, 1) \geq 2$ from (5.17). Now

$$\begin{aligned} a_P^*(\phi, n) &= \sum_{c|N} \mu\left(\tfrac{N}{c}\right) a_P(\phi^m, c) \\ &= \sum_{i=0}^{t} \sum_{d|M} \mu\left(\tfrac{N}{p^i d}\right) a_P(\phi^m, p^i d) \\ &\quad \text{since } c|N \text{ implies that } c = p^i d \text{ for some } i \in \{1, \ldots, t\} \text{ and some } d|M. \\ &= \sum_{i=0}^{t} \sum_{d|M} \mu\left(\tfrac{p^{t-i}M}{d}\right) a_P(\phi^m, p^i d). \end{aligned}$$

Applying the Auxilliary Lemma to ϕ^m we know that

$$a_P(\phi^{mp^i}, 1) = a_P(\phi^m, p^i) \geq a_P(\phi^m, 1) \geq 2$$

for each i. Now since P is fixed by ϕ^{mp^i} for each i, the Auxilliary Lemma is applicable to this map, and we obtain that $a_P(\phi^m, p^i d) = a_P(\phi^m, p^i)$ subject to the salvo that $p \nmid d$. Thus, because the MÖBIUS function is multiplicative,

$$\begin{aligned} a_P^*(\phi, n) &= \sum_{i=0}^{t} \sum_{d|M} \mu\left(\tfrac{p^{t-i}M}{d}\right) a_P(\phi^m, p^i d) \\ &= \sum_{i=0}^{t} \sum_{d|M} \mu(p^{t-i})\mu\left(\tfrac{M}{d}\right) a_P(\phi^m, p^i) \\ &= \left[\sum_{i=0}^{t} \mu(p^{t-i}) a_P(\phi^m, p^i)\right] \left[\sum_{d|M} \mu\left(\tfrac{M}{d}\right)\right] \\ &= \begin{cases} 0 & \text{if } M \geq 2 \\ a_P(\phi^m, p^t) - a_P(\phi^m, p^{t-1}) & \text{if } M = 1. \end{cases} \end{aligned}$$

where we use that definition of the MÖBIUS function and its property, used before, that $\sum_{d|M} \mu\left(\frac{M}{d}\right) = 0$ unless $M = 1$.

From part (2)(ii) of the Auxilliary Lemma, $a_P(\phi^m, p^{t-1}.p) > a_P(\phi^m, p^{t-1})$, so that (1) of *this* lemma is true in this case. Moreover, $a_P^*(\phi, n)$ is zero unless $M = 1$, in which case $n = p^t m = p^t mr$ (since $r = 1$).

It remains to be shown here (when $n = p^t mr$) that $a_P^*(\phi, n) \geq 2^{t-1}(a_P(\phi, mr) - 1)$. To show this, we use the bound given in the Auxilliary Lemma applied to ϕ^{mp^i} and taking $n = p$: then for each $i \geq 0$,

$$\begin{aligned} a_P(\phi^m, p^{i+1}) &= a_P(\phi^{mp^i}, p) \\ &\geq 2a_P(\phi^{mp^i}, 1) - 1 \\ &= 2a_P(\phi^m, p^i) - 1 \end{aligned} \tag{5.18}$$

(where again we apply (5.15)). Now we write this as

$$a_P(\phi^m, p^{i+1}) - 1 \geq 2(a_P(\phi^m, p^i) - 1) \tag{5.19}$$

for each $i \geq 0$.

Then

$$a_P^*(\phi, n) = a_P(\phi^m, p^t) - a_P(\phi^m, p^{t-1})$$

$$\begin{aligned}
&\geq 2a_P(\phi^m, p^{t-1}) - 1 - a_P(\phi^m, p^{t-1}) \qquad \text{from (5.18)} \\
&= a_P(\phi^m, p^{t-1}) - 1 \\
&\geq 2^{t-1}(a_P(\phi^m, 1) - 1) \qquad \text{applying (5.19) } t-1 \text{ times} \\
&= 2^{t-1}(a_P(\phi, mr) - 1) \qquad \text{using (5.15), and recalling that } r = 1.
\end{aligned}$$

Case(γ)(i): $N > 1$ and $r > 1$; $a_P(\phi^m, N) = 1$.

Since $\phi^m(P) = P$, by definition $a_P(\phi^m, 1) \geq 1$.

Now if $d|N$, then applying (1) of the Auxilliary Lemma to first ϕ^{md} and then to ϕ^m, we have that

$$\begin{aligned}
1 = a_P(\phi^m, N) &= a_P(\phi^{md}, \frac{N}{d}) \qquad \text{from (5.15)} \\
&\geq a_P(\phi^{md}, 1) \qquad \text{from (1) of the Auxilliary Lemma} \\
&= a_P(\phi^m, d) \qquad \text{from (5.15)} \\
&\geq a_P(\phi^m, 1) \qquad \text{from (1) of the Auxilliary Lemma} \\
&\geq 1 \qquad \text{as noted above.}
\end{aligned}$$

Thus $a_P(\phi^m, d) = 1$ for all d dividing N. Then

$$a_P^*(\phi, n) = a_P^*(\phi^m, N) = \sum_{d|N} \mu\left(\frac{N}{d}\right) a_P(\phi^m, d) = \sum_{d|N} \mu\left(\frac{N}{d}\right) = 0$$

since $N > 1$.

We complete the proof in this case by showing that it is not possible for n to be given by any of m, mr or $p^s mr$ for any $s \geq 1$. Clearly $m \neq n$ (as $N > 1$ implies that $n > m$) so unless $r < \infty$ we are done.

Suppose then that $r < \infty$ and $n = mr$ or $n = p^s mr$ for some $s \geq 1$. Then $[(\phi^m)^*(P)]^r = 1$, so since $a_P(\phi^m, 1) = 1$ as shown above, (2)(i) of the Auxilliary Lemma shows that $a_P(\phi^m, r) > a_P(\phi^m, 1) = 1$. However, $r = N$ or $rp^s = N$ by assumption and the definition of N - i.e, $r|N$. Consequently,

$$1 = a_P(\phi^m, N) = a_P(\phi^m, \left(\frac{N}{r}\right) r) \geq a_P(\phi^m, r)$$

from (1) of the Auxilliary Lemma. But then $1 < a_P(\phi^m, r) \leq 1$ which is a contradiction.

Case(γ)(ii): $N > 1$ and $r > 1$; $a_P(\phi^m, N) \geq 2$.

From (5.17), $a_P(\phi^m, 1) = 1$. Hence, assuming $a_P(\phi^m, N) \geq 2$ implies that $(\phi^m)^*(P)$ is an

Nth root of unity from (2)(i) of the Auxilliary Lemma. Because $(\phi^m)^*(P)$ is a primitive rth root of unity by the definition of r, we again have that $r|N$ - say $N = rM$. Let $\psi = \phi^{mr}$. We proceed to show that once we have defined analogous variables to r and m with respect to ψ, then ψ is a function to which certain of the cases already proven are applicable. This will yield sufficient information about $a_P^*(\phi, n)$ to conclulde the proof.

Firstly observe from (2)(i) of the Auxilliary Lemma that

$$a_P(\psi, 1) = a_P(\phi^m, r) > a_P(\phi^m, 1) = 1,$$

and because of $(\phi^m)^*(P)$ being a primitive rth root of unity, if $r \nmid d$, then $a_P(\phi^m, d) = 1$. Now recall that $a_P^*(\phi, n) = \sum_{d|N} \mu\left(\frac{N}{d}\right) a_P(\phi^m, d)$ from (5.16). This we can rewrite as

$$a_P^*(\phi, n) = \sum_{d|N, r\nmid d} \mu\left(\frac{N}{d}\right) a_P(\phi^m, d) + \sum_{d|\frac{N}{r}} \mu\left(\frac{N}{rd}\right) a_P(\phi^m, rd).$$

We successively consider the sums on the right hand side:
in the first place, with $a_P(\phi^m, d) = 1$ for each $d|N$ such that $r \nmid d$,

$$\begin{aligned} \sum_{d|N, r\nmid d} \mu\left(\frac{N}{d}\right) a_P(\phi^m, d) &= \sum_{d|N, r\nmid d} \mu\left(\frac{N}{d}\right) \\ &= \sum_{d|N} \mu\left(\frac{N}{d}\right) - \sum_{d|\frac{N}{r}} \mu\left(\frac{N}{rd}\right) \\ &= \begin{cases} 0 & \text{if } N > r \\ -1 & \text{if } N = r \end{cases} \end{aligned}$$

as we are assuming that $N > 1$ so we can apply the property of the MÖBIUS function used formerly.

Now with $M = \frac{N}{r}$ and $a_P(\phi^m, rd) = a_P(\phi^{mr}, d) = a_P(\psi, 1)$, the second sum becomes

$$\sum_{d|M} \mu\left(\frac{M}{d}\right) a_P(\psi, d) = a_P^*(\psi, M) \text{ by the definition of } Z_M^*(\psi).$$

Consequently, combining these findings we obtain:

$$a_P^*(\phi, n) = \begin{cases} a_P^*(\psi, M) & \text{if } N > r \text{ (i.e. if } M > 1) \\ a_P^*(\psi, M) - 1 & \text{if } N = r \text{ (i.e. if } M = 1). \end{cases}$$

Because $a_P(\psi, 1) \geq 2$, we know that $v_P(z \circ \psi - z) = v_P(\psi^*(P)z + O(z^2) - z) = v_P((\psi^*(P) - 1)z + O(z^2)) \geq 2$, and hence that $\psi^*(P) = 1$ - i.e. the multiplicative period of $\psi^*(P)$ in

the unit group of some algebraic closure $\overline{K}$ of K say r_ψ, is 1. Moreover, P is fixed by ψ, which means that the exact period of P under ψ, say m_ψ, is 1. Now consider the lemma we aim to prove here, but with reference to ψ. Since $r_\psi = 1$, **Cases** (α) and (β) are applicable, and we have shown the lemma to hold in these situations.

Thus, $a_P^*(\psi, M) \geq 0$ for all $M \geq 1$, and $a_P^*(\psi, M) > 1$ if and only if either $M = m_\psi = 1$ (which is the same as $M = m_\psi r_\psi = 1$, in which case $a_P^*(\psi, M) \geq 2$), or $M = p^s m_\psi r_\psi = p^s$ for some $s \geq 1$, which occurs concurrently with $a_P^*(\psi, M) \geq 2^{s-1}(a_P(\psi, 1) - 1)$. There are 3 subcases to consider:

Firstly, if $M \neq p^s$ for any $s \geq 0$ then from the above, $a_P^*(\psi, M) = 0$. But because in this case $M > 1$, we find that $a_P^*(\phi, n) = a_P^*(\psi, M) = 0$. Recall that $n = Nm$. Thus, here $n \neq m$ (as $N > 1$); and $n \neq mr$ or $p^s mr$ for any $s \geq 1$ (since $N \neq p^s r$ for any $s \geq 0$), so that we are done in this case.

In the second place, when $M = 1$, then $N = r$, so that $a_P^*(\phi, n) = a_P^*(\psi, M) - 1$. But here, also $a_P^*(\psi, M) \geq 2$, implying that $a_P^*(\phi, n) \geq 1$. This corresponds to the case of $n = mr$ by the definition of N, and since $r \neq 1$ there is nothing more to be shown.

Finally, if M is some power of p other than 1, say $M = p^s$ where $s \geq 1$, then from the application of what we have already shown to ψ, we know that $a_P^*(\psi, M) \geq 1$, so that $a_P^*(\phi, n)$ being equal to $a_P^*(\psi, M)$ in this case implies that $a_P^*(\phi, n) \geq 1$. Here, $n = p^s mr$ by the definitions of M and N. Also, $a_P^*(\psi, M) \geq 2^{s-1}(a_P(\psi, 1) - 1)$ from whence $a_P^*(\phi, n) \geq 2^{s-1}(a_P(\phi^{mr}, 1) - 1) = 2^{s-1}(a_P(\phi, mr) - 1)$ which concludes the proof. □

A final result we shall require states that the reduction of the cycle of n-periodic points is the same as the cycle of n-periodic points of the reduced map, subject to certain conditions on the original map:

Lemma 5.5 *Suppose that (K, v) is a valued field. If $\phi : \mathbb{P}^1_K \to \mathbb{P}^1_K$ is non-constant morphism having good reduction; n is some positive integer; and $\tilde{\phi}$ denotes the reduced map of ϕ; then*

$$Z_n(\tilde{\phi}) = \widetilde{Z_n(\phi)}.$$

Proof: Firstly observe that $\tilde{\phi}$ is non-constant:

Because ϕ is not constant, the fact that it is a morphism of one smooth projective curve to another ensures that it is surjective (see SILVERMAN [19, I.2]). Now given any point Q of $\mathbb{P}^1(\overline{K})$, there exists some point of $\mathbb{P}^1(K)$ which does not reduce to Q under reduction modulo the maximal ideal $\mathcal{M}_v$ of the valuation ring of K. Denoting the reduction map

by $\omega : \mathbb{P}^1(K) \to \mathbb{P}^1(\overline{K})$, then we have established that there are distinct points in the image of $\omega \circ \phi$. However,

$$\begin{array}{ccc} \mathbb{P}^1(K) & \xrightarrow{\phi} & \mathbb{P}^1(K) \\ \omega \downarrow & & \downarrow \omega \\ \mathbb{P}^1(\overline{K}) & \xrightarrow{\tilde{\phi}} & \mathbb{P}^1(\overline{K}) \end{array}$$

commutes from the definition of reduction and because ϕ has good reduction. Thus, it is not possible for $\tilde{\phi}$ to be a constant morphism.

Now we again apply the result guaranteeing the surjectivity of non-constant morphisms between smooth projective curves to $\tilde{\phi} : \mathbb{P}^1(\overline{K}) \to \mathbb{P}^1(\overline{K})$. This implies that since $\tilde{\phi}$ is a well-defined mapping of $\mathbb{P}^1(\overline{K})$, $\tilde{\phi^n}$ also is.

Thus there exist homogeneous polynomials $\phi_n^{(0)}(x,y)$ and $\phi_n^{(1)}(x,y)$ in $K[x,y]$ such that $\phi^n = [\phi_n^{(0)} : \phi_n^{(1)}]$ and $\tilde{\phi_n^{(0)}}$ and $\tilde{\phi_n^{(1)}}$ share no common non-trivial roots, so that $\tilde{\phi^n} = [\tilde{\phi_n^{(0)}} : \tilde{\phi_n^{(1)}}]$.

Now if $P = [x : y]$ is a fixed point of ϕ^n, then $y\phi_n^{(0)}(x,y) - x\phi_n^{(1)}(x,y) = 0$ - in fact the roots of this equation with their corresponding multiplicities determine $Z_n(\phi)$ because ϕ^n is given by $[\phi_n^{(0)}(x_0,x_1) : \phi_n^{(1)}(x_0,x_1)]$ at each point $[x_0 : x_1]$ of $\mathbb{P}^1(K)$. Reducing this equation modulo $\mathcal{M}_v$ thus gives the reduction of $Z_n(\phi)$. However, the roots of the reduced equation $y\tilde{\phi_n^{(0)}}(x,y) - x\tilde{\phi_n^{(1)}}(x,y) = 0$ together with their multiplicities determine $Z_n(\tilde{\phi})$ just as the previous equation yields $Z_n(\phi)$. Hence, $Z_n(\tilde{\phi}) = \widetilde{Z_n(\phi)}$ as asserted. □

The following trivial consequence of this lemma will be used to prove the main result of this section:

Corollary 5.1 *For K, ϕ, n and $\tilde{\phi}$ as above, then*

$$Z_n^*(\tilde{\phi}) = \widetilde{Z_n^*(\phi)}.$$

5.2.3 The main theorem

With the necessary equipment in hand, we are now in a position to prove the following

Theorem 5.4 (Morton & Silverman) *Suppose that (K,v) is a discretely valued field with valuation ring $\mathcal{O}_K$, and $\phi : \mathbb{P}^1_K \to \mathbb{P}^1_K$ is a morphism of degree at least 2 which has good reduction. Then if the reduced map $\tilde{\phi}$ is separable, ϕ has at most finitely many attracting periodic points.*

Proof: If ϕ has no attracting periodic points, then we are done, so suppose that P is some point of exact period m under ϕ, which is attracting - i.e., $|(\phi^m)'(P)| < 1$. In reduction modulo the maximal ideal, denoting the reduction of P by $\tilde{P}$, this becomes:

$$(\tilde{\phi^m})'(\tilde{P}) = 0. \tag{5.20}$$

From the chain rule,

$$\begin{aligned}
(\tilde{\phi^m})'(\tilde{P}) &= [\tilde{\phi}(\tilde{\phi}^{m-1}(\tilde{P}))]' \\
&= \tilde{\phi}'(\tilde{\phi}^{m-1}(\tilde{P}))[\tilde{\phi}^{m-1}(\tilde{P})]' \\
&= \tilde{\phi}'(\tilde{\phi}^{m-1}(\tilde{P}))[\tilde{\phi}(\tilde{\phi}^{m-2}(\tilde{P}))]' \\
&= \tilde{\phi}'(\tilde{\phi}^{m-1}(\tilde{P}))\tilde{\phi}'(\tilde{\phi}^{m-2}(\tilde{P}))[\tilde{\phi}^{m-2}(\tilde{P})]' \\
&\vdots \\
&= \tilde{\phi}'(\tilde{\phi}^{m-1}(\tilde{P}))\tilde{\phi}'(\tilde{\phi}^{m-2}(\tilde{P}))\ldots\tilde{\phi}'(\tilde{P}) \\
&= \prod_{i=0}^{m-1} \tilde{\phi}'(\tilde{\phi}^i(\tilde{P})).
\end{aligned}$$

Now let n be the exact period of the reduced point $\tilde{P}$, so that $n|m$ and $\tilde{\phi}^n(\tilde{P}) = \tilde{P}$. Then we can rewrite this product as

$$[\prod_{i=0}^{n-1} \tilde{\phi}'(\tilde{\phi}^i(\tilde{P}))]^{\frac{m}{n}}.$$

Applying what was shown above from the chain rule in reverse, this is nothing other than

$$[(\tilde{\phi^n})'(\tilde{P})]^{\frac{m}{n}}.$$

But then in $\mathbb{P}^1(\overline{K})$, it follows from (5.20) that

$$\begin{aligned}
0 &= (\tilde{\phi^m})'(\tilde{P}) \\
&= [(\tilde{\phi^n})'(\tilde{P})]^{\frac{m}{n}}
\end{aligned}$$

so that, $(\tilde{\phi^n})'(\tilde{P}) = 0$.

Now from Proposition 5.2, the derivative at $\tilde{P}$ of $\tilde{\phi^n}$ is precisely the scalar $(\tilde{\phi^n})^*(\tilde{P})$ involved in the mapping of the cotangent space of $\mathbb{P}^1(\overline{K})$ at $\tilde{P}$ induced by $\tilde{\phi^n}$. Lemma 5.3 is thus applicable here, and informs us that there is some ramification point in the orbit of $\tilde{P}$ under $\tilde{\phi}$. Notice that such a point also has exact period n. Furthermore, there are only finitely many such ramification points due to the separability of the map $\tilde{\phi}$. (This was pointed out in the discussion immediately preceding Lemma 5.3.)

Now we make use of the information we have gleaned about the zero-cycles we defined: because $(\tilde{\phi^n})^*(\tilde{P})$ is not a root of unity, we know from Lemma 5.4 that $a_{\tilde{P}}(\tilde{\phi}, w) \geq 1$ if and only if $w = n$, (where we are using the notation of the definitions of the cycles). However, $a_P^*(\phi, m) \geq 1$ from Lemma 5.4 since m is the exact period of P under ϕ. This means that $P \in Supp(Z_m^*(\phi))$. But then since $Z_m^*(\tilde{\phi}) = \widetilde{Z_m^*(\phi)}$ from Corollary 5.1, it follows that $\tilde{P} \in Supp(Z_m^*(\tilde{\phi}))$. Thus $n = m$, and P consequently has the same exact period as one of the finitely many ramification points of $\tilde{\phi}$.

Let $k \geq 1$. We make use of our former notation $\Delta(\mathbb{P}^1_K)$ for the diagonal of $\mathbb{P}^1_K \times \mathbb{P}^1_K$ and $\Gamma(\phi^k)$ for the graph of ϕ^k. Recall that because ϕ is not the identity mapping, $\Delta(\mathbb{P}^1_K)$ and $\Gamma(\phi^k)$ can intersect at most at a finite number of points. There are thus at most finitely many fixed points of ϕ^k for any $k \geq 1$. Hence, the set of all points which have the same period as any one of the finite number of ramification points of ϕ, is finite. Consequently, P is one of at most finitely many attracting periodic points of ϕ. □

Appendix A

Resultants

Elimination theory embodies an algebraic study of systems of equations, seeking conditions for the existence of solutions and explicit formulae for such solutions. Linear Algebra can thus be reckoned as a branch of this subject, where determinants are special tools giving conditions for the solubility of systems of equations. In the more general setting, *resultants* are suitable tools for providing a simple criterion for the existence of solutions.

Given a system of polynomials in one variable with indetermiate coefficients, it is possible to show that there exists a polynomial in these coefficients, called the *resultant*, which vanishes if and only if the polynomials have a common root. When more than one variable is involved, and the number of variables strictly exceeds the number of polynomials, we have to settle for a "resultant system" (which is a finite set of polynomials in the coefficients) which vanish identically if and only if the original polynomials have a shared root. On the other hand, a system of n polynomials in n variables admits a single resultant polynomial.

Our treatment of these and other facts follows that of VAN DER WAERDEN in [21].

A.1 The resultant of two polynomials in a single variable

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ and $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$ be polynomials in x with coefficients in some field K. We do not exclude the possibility of a_n or b_m being zero, i.e. that the degree of $f(x)$ may be lower than n and that of $g(x)$ may be lower than m. (Writing $f(x)$ in this form, commencing with a possibly vanishing first term $a_n x^n$, we call n the *formal degree* of $f(x)$ and a_n is referred to as the *formal*

leading coefficient .) Nevertheless for our discussion we may assume that either a_n or b_m is non-zero — WLOG suppose that a_n is non-zero.

EULER showed that $f(x)$ and $g(x)$ have a common non-constant factor if and only if there exist polynomials $h(x)$ and $k(x)$ which are relatively prime over K with the property that

$$h(x)f(x) = k(x)g(x) \tag{A.1}$$

where deg $h(x) \leq m-1$ and deg $k(x) \leq n-1$. Indeed, if such polynomials exist, then because each irreducible factor of $f(x)$ must appear in $k(x)g(x)$ to the same multiplicity as it appears in $f(x)$ itself, but the degree of $k(x)$ is less than that of $f(x)$ (since $a_n \neq 0$) , some irreducible factor of $f(x)$ appears also in $g(x)$. Conversely, if $\phi(x)$ is a non-constant factor of both $f(x)$ and $g(x)$, then we have that $f(x) = \phi(x)k(x)$ and $g(x) = \phi(x)h(x)$ for some polynomials h, k of the required degrees, from which the equation A.1 follows.

Supposing that $h(x) = c_{m-1}x^{m-1} + c_{m-2}x^{m-2} + \cdots + c_1x + c_0$ and $k(x) = d_{n-1}x^{n-1} + d_{n-2}x^{n-2} + \cdots + d_1x + d_0$ with formal leading coefficients c_{m-1} and d_{n-1} respectively, sustituting into A.1 and equating coefficients of distinct powers of x yields:

$$c_{m-1}a_n = d_{n-1}b_m$$

$$c_{m-1}a_{n-1} + c_{m-2}a_n = d_{n-1}b_{m-1} + d_{n-2}b_m$$

$$\cdots\cdots\cdots$$

$$c_1a_0 + c_0a_1 = d_1b_0 + d_0b_1$$

$$c_0a_0 = d_0b_0$$

This is a system of $n+m$ linear, homogeneous equations in the $n+m$ "unknowns" $c_{m-1}, \ldots, c_0, -d_{n-1}, \ldots, -d_0$. The determinant of this system has the following form once columns and rows have been exchanged, known as the SYLVERSTER resultant:

$$\mathcal{R} = \begin{vmatrix} a_n & \ldots & a_0 & 0 & 0 & \ldots & 0 \\ 0 & a_n & \ldots & a_0 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & a_n & \ldots & a_0 \\ b_m & \ldots & b_0 & 0 & 0 & \ldots & 0 \\ 0 & b_m & \ldots & b_0 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & b_m & \ldots & b_0 \end{vmatrix}$$

Remarks:

(1) Observe that the resultant is homogeneous of degree m in the a_i and is homogeneous of degree n in the b_j.

(2) Since only a_n and b_m appear in the first column of the determinant, $\mathcal{R}$ vanishes not only when f and g have a common factor, but also when $a_n = b_m = 0$, which would be contrary to our initial assumption of at least one of the formal leading coefficients being non-vanishing. A careful analysis involving the transforming of f and g to homogeneous polynomials by the introduction of a second variable reveals that in fact $\mathcal{R} = 0$ whenever $a_n = b_m = 0$. For the details, see VAN DER WAERDEN [21].

(3) The resultant of f and g is a polynomial in the coefficients of f and g which has integer coefficients.

An important property of the resultant may be derived as follows:

$\mathcal{R}$ is precisely the determinant of the following system of equations:

$$\begin{array}{lcl}
x^{m-1}f(x) & = & a_n x^{m+n-1} + a_{n-1}x^{m+n-2} + \ldots + a_1 x^m + a_0 x^{m-1} \\
x^{m-2}f(x) & = & a_n x^{m+n-2} + a_{n-1}x^{m+n-3} + \ldots + a_1 x^{m-1} + a_0 x^{m-2} \\
\vdots & \vdots & \vdots \\
f(x) & = & a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \\
x^{n-1}g(x) & = & b_m x^{m+n-1} + b_{m-1}x^{m+n-2} + \cdots + b_1 x^n + b_0 x^{n-1} \\
x^{n-2}g(x) & = & b_m x^{m+n-2} + b_{m-1}x^{m+n-3} + \cdots + b_1 x^{n-1} + b_0 x^{n-2} \\
\vdots & \vdots & \vdots \\
g(x) & = & b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0
\end{array}$$

Assuming that $\mathcal{R}$ does not vanish as a formal expression of the indeterminate coefficients of f and g, we can apply CRAMER'S rule about the last column of the right hand side, to obtain that $1.\mathcal{R} = Af + Bg$ where A and B are polynomials in x and in the indeterminate coefficients a_μ and b_ν, with integer coefficients. This implies that $\mathcal{R}$ is in the ideal generated by f and g, which we denote as: $\mathcal{R} \equiv 0(f, g)$. Similar application of CRAMER'S rule about the relevant column yields polynomials A_τ and B_τ with integer coefficients, in x, the a_μ and the b_ν, such that

$$x^\tau \mathcal{R} = A_\tau f + B_\tau g \text{ for } \tau = 1, 2, \ldots, m + n - 1. \tag{A.2}$$

A.2 The resultant of many polynomials in one variable

Theorem A.1 *If $f_1, \ldots, f_r$ is a system of r polynomials in one variable, of given degree and having indeterminate coefficients, then there exists a system $D_1, \ldots, D_h$ of integer polynomials in the coefficients, such that once values of the coefficients are specified in some field K, then the conditions $D_1 = 0, D_2 = 0, \ldots, D_h = 0$ hold if and only if either the polynomials $f_1, \ldots, f_r$ have a common root in some extension of K, or all of the formal leading coefficients of $f_1, \ldots, f_r$ vanish.*

Proof: We make use of KRONECKER'S elimination method.
Firstly we convert $f_1, \ldots, f_r$ into a system of polynomials of the same degree: if $n = \max_i\{\deg f_i\}$, then we multiply each polynomial f_j of lower degree k_j by both x^{n-k_j} and $(x-1)^{n-k_j}$, thereby obtaining two polynomials from each such f_j both of degree n and sharing any common roots which the original system of polynomials may have for any given specification of the values of the (indeterminate) coefficients. Denote the new system of (possibly more) polynomials by $g_1, \ldots, g_s$. Now for indeterminates $u_1, \ldots, u_s$ and $v_1, \ldots, v_s$, let $g_u := u_1 g_1 + \ldots + u_s g_s$ and $g_v := v_1 g_1 + \ldots + v_s g_s$.

It is a triviality that any common factor of g_u and g_v (upon some specification of the coefficients of the g_i s) must be a rational expression involving x and the u_i s, as well as being a rational expression involving x and the v_j s. However, since the u_i s do not appear in g_v they are indeterminates which cannot appear in any factor of g_v. Any common factor of g_u and g_v would thus have to be independent of the u_i s and similarly, we see that none of the v_j s could appear in the common factor. Thus, any common factor of g_u and g_v would in fact have to appear as a common factor of $g_1, \ldots, g_s$, from the definitions of g_u and g_v.

We thus see that the polynomials g_u and g_v have a root in common if and only if the polynomials $g_1, \ldots, g_s$ share a common root. However, viewed as polynomials in the single variable of which $f_1, \ldots, f_r$ are polynomials, with indeterminate coefficients, the polynomials g_u and g_v satisfy $g_u = g_v = 0$ or one or other of their leading coefficients vanish if and only if their resultant $\mathcal{R}$ vanishes identically in the u_i and the v_j . Arranging $\mathcal{R}$ in powers of the u_i and the v_j and denoting the coefficients by $D_1, \ldots, D_h$ then $\mathcal{R} = 0$ identically in the u_i and the v_j if and only if $D_1 = 0, D_2 = 0, \ldots, D_h = 0$. However, by construction and from the definition of the SYLVESTER resultant, we know that $D_1, \ldots, D_h$

are integer polynomials in the indeterminate coefficients of $f_1, \ldots, f_r$, thereby completing the proof. □

The system $D_1, \ldots, D_h$ is called the resultant system of the polynomials $f_1, \ldots, f_r$. As shown above in Section A.1, $\mathcal{R} \equiv 0(g_u, g_v)$ which is the equivalent to

$$\mathcal{R} \equiv 0(g_1, \ldots, g_s) \equiv 0(f_1, \ldots, f_r)$$

so arranging terms on both sides according to powers of the u_i and the v_j and using the independence of these indeterminates it follows also that

$$D_1, \ldots, D_h \equiv 0(f_1, \ldots, f_r).$$

Once again, the case of the vanishing of all leading coefficients can be formally dealt with by the introduction of a second variable to produce homogeneous polynomials. For further details see VAN DER WAERDEN [21] .

A.3 r polynomials in n variables.

If $f_1, \ldots, f_r$ are homogeneous, non-constant polynomials in the n variables $x_1, \ldots, x_n$, then applying KRONECKER'S elimination method as detailed above to these expressions viewed as polynomials in x_1, yields a resultant system comprising of polynomials $D_1, \ldots, D_h$ in the coefficients of the polynomials and in $x_2, \ldots, x_n$.

Theorem A.2 *The system of polynomials $f_1, \ldots, f_r$ has a non-trivial common root if and only if $D_1, \ldots, D_h$ also have a non-trivial shared root when viewed as polynomials in $x_2, \ldots, x_n$.*

Proof: Case 1: There exists some power of x_1 alone in at least one of $f_1, \ldots, f_r$.

Then given any non-trivial root $(\xi_1, \ldots, \xi_{n-1})$ of $D_1, \ldots, D_h$, this can be viewed as a specification of the coefficients yielding

$$D_1 = 0, D_2 = 0, \ldots, D_h = 0,$$

thereby implying that there exists some common root (clearly also non-trivial) $(\xi_0, \xi_1, \ldots, \xi_{n-1})$ of $f_1, \ldots, f_r$ by the property of the resultant system shown above (in Section A.2).

Conversely, if $(\xi_1, \ldots, \xi_n)$ is a given non-trivial common root of $f_1, \ldots, f_r$, then $D_1, \ldots, D_h$ vanish identically on $(\xi_2, \ldots, \xi_n)$ which is also non-trivial since assuming otherwise, would give that also $\xi_1 = 0$: in the case at hand, we have that for some λ, there is an f_λ which has a term of the form cx_1^m, so considering $f_\lambda(\xi_1, 0, \ldots, 0) = 0$ it is immediately clear that $\xi_1 = 0$ (recall that f_λ is homogeneous).

Case 2: There is no non-vanishing term in x_1 alone, in any of $f_1, \ldots, f_r$.
This case corresponds to the case of the vanishing of the formal leading coefficients of the polynomials in the variable x_1, so that here, $D_1, \ldots, D_h$ vanish identically and $(1, \ldots, 1)$ is thus a non-trivial common root of the polynomials of the resultant system, whereas $(1, 0, \ldots, 0)$ is a non-trivial root of each of $f_1, \ldots, f_r$. □

By construction the polynomials $D_1, \ldots, D_h$ are homogeneous in $x_2, \ldots, x_n$, so the procedure can be repeated to eliminate x_2 and subsequently $x_3, \ldots, x_{n-1}$; obtaining a system of forms in x_n alone: $b_1 x_n^{s_1}, \ldots, b_k x_n^{s_k}$. These forms share a common non-trivial root if and only if the coefficients, which are integer polynomials in the coefficients of $f_1, \ldots, f_r$, vanish, and this is the case if and only if $f_1, \ldots, f_r$ have a common non-trivial root by the inductive construction.

Since they provide a condition of this kind for the existence of a non-trivial solution of $f_1, \ldots, f_r$, the polynomials $b_1, \ldots, b_k$ are a resultant system for the forms $f_1, \ldots, f_r$. Because of the relation

$$D_1, \ldots, D_h \equiv 0(f_1, \ldots, f_r),$$

we see that also

$$b_i x_n^{s_i} \equiv 0(f_1, \ldots, f_r).$$

A.4 Inertial forms and the resultant of n forms in n variables

Whereas in the general case of r forms in n variables, an entire system of possibly very many polynomials is required to give a necessary and sufficient condition for the existence of a non-trivial common root of these forms, when $r = n$, a single resultant polynomial suffices for this purpose. We show this by introducing the so-called "inertial forms":
Let

$$f_1 = a_{11}x_1^{\alpha_1} + a_{12}x_1^{\alpha_1 - 1}x_2 + \cdots + a_{1\omega}x_n^{\alpha_1}$$

$$\begin{aligned} f_2 &= a_{21}x_1^{\alpha_2} + a_{22}x_1^{\alpha_2-1}x_2 + \cdots + a_{2\omega}x_n^{\alpha_2} \\ &\vdots \quad \vdots \quad \vdots \\ f_r &= a_{r1}x_1^{\alpha_r} + a_{r2}x_1^{\alpha_r-1}x_2 + \cdots + a_{r\omega}x_n^{\alpha_r} \end{aligned}$$

be r forms of dgrees $\alpha_1, \ldots, \alpha_r$ in which all possible terms of these degrees with indeterminate coefficients appear.

Definition A.1 *Any* integer *polynomial* T *in* $a_{11}, \ldots, a_{1\omega}, a_{21}, \ldots, a_{2\omega}, \ldots, a_{r1}, \ldots, a_{r\omega}$ *satisfying*

$$x_i^\tau T \equiv 0(f_1, \ldots, f_r) \tag{A.3}$$

for some i *and some* τ *is a* HURWITZ *inertial form of the system* $f_1, \ldots, f_r$.

Observe that the resultant system $b_1, \ldots, b_k$ formed above (in Section A.3) is comprised of inertial forms.

Theorem A.3 *The set* $\mathcal{I}$ *of all inertial forms of* $f_1, \ldots, f_r$ *is a prime ideal in the ring of polynomials with integer coefficients in the variables*
$a_{11}, \ldots, a_{1\omega}, a_{21}, \ldots, a_{2\omega}, \ldots, a_{r1}, \ldots, a_{r\omega}$.

Proof: We give a characterization of the inertial forms from which the assertion follows easily:
Set

$$\begin{aligned} f_1 &= f_1^* + a_{1\omega}x_n^{\alpha_1} \\ &\vdots \quad \vdots \quad \vdots \\ f_r &= f_r^* + a_{r\omega}x_n^{\alpha_r} \end{aligned}$$

and then substitute

$$\begin{aligned} a_{1\omega} &= -\frac{f_1^*}{x_n^{\alpha_1}} \\ &\vdots \quad \vdots \quad \vdots \\ a_{r\omega} &= -\frac{f_r^*}{x_n^{\alpha_r}} \end{aligned}$$

in these expressions to obtain that $f_1, \ldots, f_r$ vanish.
If T is any inertial form such that for some $i \neq n$

$$x_i^\tau T \equiv 0(f_1, \ldots, f_r),$$

then this substitution leaves x_i unaffected so that

$$T(a_{11}, \ldots, -\frac{f_1^*}{x_n^{\alpha_1}}, \ldots, a_{r1}, \ldots, -\frac{f_r^*}{x_n^{\alpha_r}}) = 0 \tag{A.4}$$

Conversely, should some integral polynomial $T(a_{11}, \ldots, a_{1\omega}, \ldots, a_{r1}, \ldots, a_{r\omega})$ satisfy A.4, then T can be arranged in powers of

$$(a_{1\omega} + \frac{f_1^*}{x_n^{\alpha_1}}), \ldots, (a_{r\omega} + \frac{f_r^*}{x_n^{\alpha_r}}).$$

Now T vanishes whenever these expressions are all zero, so that in the space of fractions with denominator x_n^λ, we have that

$$T \equiv 0(a_{1\omega} + \frac{f_1^*}{x_n^{\alpha_1}}, \ldots, a_{r\omega} + \frac{f_r^*}{x_n^{\alpha_r}}).$$

Clearing denominators by multiplying by the highest power of x_n which occurs, we find that

$$\begin{aligned} x_n^\tau T &\equiv 0 \quad (x_n^{\beta_1}[a_{1\omega}x_n^{\alpha_1} + f_1^*], \ldots, x_n^{\beta_r}[a_{r\omega}x_n^{\alpha_r} + f_r^*]) \\ &\equiv 0 \quad (f_1, \ldots, f_r). \end{aligned}$$

Thus T is an inertial form.

Now we have shown that A.3 being true for some x_i implies that A.4 is true, while A.4 implies that A.3 is true for x_n. i. e. A.3 being true for x_i implies A.3 is true for x_n, and thus, because x_n can play no special role, A.3 being valid for some x_i implies it holds for each x_j. Hence, A.4 implying that A.3 is true for x_n means that A.4 being valid implies that A.3 is true for each x_i, so A.4 and A.3 are equivalent and A.4 is thus also a characterization of the inertial forms.

We are now in a position to prove the theorem: it is clear from A.4 that the difference of two inertial forms is also an inertial form, and that any multiple of an inertial form by a polynomial with integral coefficients is also an inertial form. $\mathcal{I}$ is thus an ideal, which is prime since if T_1 and T_2 are polynomials and T_1T_2 satisfies A.4, then either one or other of T_1 and T_2 satisfies A.4. □

The inertial forms can be used instead of a resultant system: if $(f_1, \ldots, f_r)$ share a common non-trivial root, then since any inertial form T satisfies

$$x_i^\tau T \equiv 0(f_1, \ldots, f_r)$$

for *each* x_i, at least one of which is non-trivial since the root is non-trivial, so the vanishing of the right hand side means that T is also zero. On the other hand, if all of the inertial

forms are zero, then in particular the resultant system is zero, and hence the forms $f_1, \ldots, f_r$ have a non-trivial root in common. Any basis for the ideal of inertial forms thus suffices as a resultant system. This fact, together with the following two propositions, will be used to describe the resultant polynomial of n forms in n variables:

Proposition A.1 *For a system of n forms in n variables, there are no non-zero inertial forms which are independent of $a_{r\omega} = a_{n\omega}$.*

Proof: Assume to the contrary that there exists some non-zero inertial form T which is independent of $a_{n\omega}$. Then from A.4 follows that $(-\frac{f_1^*}{x_n^{\alpha_1}}, \ldots, -\frac{f_{n-1}^*}{x_n^{\alpha_{n-1}}})$ are algebraically dependent. This dependence will remain unaffected if we set $x_n = 1$. This gives a sequence of polynomials $[-f_1^*]_{x_n=1}, \ldots, [-f_{n-1}^*]_{x_n=1}$ which are algebraically dependent with respect to a ring of polynomials in $a_{11}, \ldots, a_{1\omega-1}, a_{21}, \ldots, a_{2\omega-1}, \ldots, a_{n1}, \ldots, a_{n\omega-1}$. We now make use of the following

Lemma A.1 *When a sequence of polynomials $f_1, \ldots, f_s$ in the indeterminates $a_1, \ldots, a_p, x_1, \ldots, x_q$ are algebraically independent in a polynomial ring $K[a_1, \ldots, a_p]$ (where K is an integral domain), then this dependence remains at any specification of $a_p = \alpha$ for some $\alpha \in K$.*

Proof: We know that there exists some polynomial F such that

$$F(a_{11}, \ldots, a_p, \ldots, f_1, \ldots, f_s) = 0 \tag{A.5}$$

but for indeterminates $z_1, \ldots, z_s$, we have that

$$F(a_{11}, \ldots, a_p, z_1, \ldots, z_s) \neq 0. \tag{A.6}$$

We can assume that $a_p - \alpha$ is not a factor of $F(a, z)$ since otherwise we could divide both A.5 and A.6 by this factor. But then, substituting $a_p = \alpha$ in A.6 would mean that

$$F(a_{11}, \ldots, a_{p-1}, \alpha, z_1, \ldots, z_s) \neq 0$$

and the validity of A.5, (i.e. the algebraic dependence) would be unaffected by this substitution, completing the proof of the lemma. □

Applying the lemma repeatedly, we can substitute for

$$a_{11}, \ldots, a_{1\omega-1}, a_{21}, \ldots, a_{2\omega-1}, \ldots, a_{n1}, \ldots, a_{n\omega-1}$$

in any way without losing the algebraic dependence. In particular, we can sustitute for the indeterminates in such a way that f_1^* becomes $x_1^{\alpha_1}$, f_2^* becomes $x_2^{\alpha_2}$ and so on, without the algebraic dependence being affected. But then $x_1^{\alpha_1}, \ldots, x_{n-1}^{\alpha_{n-1}}$ are algebraically dependent, which is untrue. □

Now we show the existence of some non-zero inertial form:

Proposition A.2 *There exists a non-vanishing inertial form D for any system $f_1, \ldots, f_n$ of n forms in n variables.*

Proof: Suppose that the respective degrees of $f_1, \ldots, f_n$ are given by $l_1, \ldots, l_n$. Now let $\sum_{i=1}^{n}(l_i - 1) = l - 1$. Arrange the products of $x_1, \ldots, x_n$ of total degree l as follows: begin with those in which $x_1^{l_1}$ appears, followed by those in which $x_2^{l_2}$ appears but $x_1^{l_1}$ does *not* appear, and so on, until listing those terms with $x_n^{l_n}$ but without $x_1^{l_1}$ or $x_2^{l_2}$ etc.. (It is evident that any product in which there is no factor $x_i^{l_i}$ for any i, has degree strictly less than l from the definition of l.) We now denote by $H_{l-l_1}^{(1)}x_1^{l_1}, H_{l-l_1}^{(2)}x_1^{l_1}, \ldots, H_{l-l_1}^{(k_1)}x_1^{l_1}$ the products of degree l where $x_1^{l_1}$ appears, and similarly write $H_{l-l_2}^{(\nu)}x_2^{l_2}, H_{l-l_3}^{(\nu)}x_3^{l_3}, \ldots, H_{l-l_n}^{(\nu)}x_n^{l_n}$. Using the n forms $f_1, \ldots, f_n$, we form the polynomials $H_{l-l_i}^{(\nu)}f_i$, which in number equal the number of products of degree l listed above. Writing

$$H_{l-l_i}^{(\nu)}f_i = \sum_{\mu} a_{\nu\mu}^{(i)} H_l^{(\mu)},$$

we denote the determinant of the (evidently square) coefficient matrix, by D. Substituting to obtain $f_i = x_i^{l_i}$ for each i, the determinant is 1, so it does not vanish identically.

To

$$(a_{\nu\mu}^{(i)})_{i,\nu,\mu}[H_l^{(\mu)}]_{(\mu)} = [H_{l-l_i}^{(\nu)}f_i]_{\nu,i}$$

we apply CRAMER'S rule to solve for $H_l^{(\mu)}$: then some linear combination of f_i (with coefficients which are polynomials) equals $DH_l^{(\mu)}$ for each μ. Considering the cases when $H_l^{(\mu)} = x_i^l$, we obtain:

$$x_i^l D \equiv 0(f_1, \ldots, f_n).$$

D is thus a non-vanishing inertial form. □

We now turn our attention to producing the unique resultant polynomial of the given system $f_1, \ldots, f_n$ of n forms in n variables: the ideal $\mathcal{I}$ of inertial forms of $f_1, \ldots, f_n$ is not the zero ideal from the above proposition, and from the preceding result, we thus know that there exists a polynomial, say P in $\mathcal{I}$ of minimal degree in $a_{r\omega}$. If this polynomial is

reducible, then $\mathcal{I}$ being a prime ideal ensures that some irreducible factor of P is also in $\mathcal{I}$. Denote this factor by $\mathcal{R}$ and observe that $\mathcal{R}$ must have the same degree in $a_{r\omega}$ as that of P.

Proposition A.3 *$\mathcal{R}$ generates $\mathcal{I}$, which is thus a principal ideal.*

Proof: Let T be any inertial form in $\mathcal{I}$. We show that $\mathcal{R} \mid T$:
Arrange $\mathcal{R}$ in descending powers of $a_{r\omega}$: $\mathcal{R} = Sa_{r\omega}^{\lambda} + \ldots (\lambda > 0)$. T's degree in $a_{r\omega}$ is less than or equal to λ, so by subtracting a suitable multiple of $\mathcal{R}$from S^jT for some $j \geq 0$, we can obtain a polynomial expression $T' = S^jT - Q\mathcal{R}$ of degree in $a_{r\omega}$ which is strictly less than λ. However, T' is in $\mathcal{I}$, so λ being the minimal degree in $a_{r\omega}$ of polynomials in $\mathcal{I}$ implies that T' must vanish. Thus $\mathcal{R} \mid S^jT$. S is independent of $a_{r\omega}$, though, so in fact, $\mathcal{R} \mid T$. □

$\mathcal{R}$ is referred to as the resultant of the system $f_1, \ldots, f_n$, since it is a basis for the ideal of inertial forms and thus vanishes if and only if $f_1, \ldots, f_n$ have a common non-trivial root.

Remark: Since $\mathcal{R}$ is an inertial form,

$$x_i^{\tau_i}\mathcal{R} \equiv 0(f_1, \ldots, f_n) \quad \text{for each } i \in 1, \ldots, n.$$

Appendix B

Elements of Algebraic Number Theory

Here we list certain standard theorems and definitions from Algebraic Number Theory, and use the catalogued facts to prove results required in the text of the thesis (namely Lemmas B.2 and B.1, and Corollary B.1 below).

B.1 The Chinese remainder theorem

Lemma B.1 *Given a commutative ring with identity, R, in which $\mathcal{I}_1, \ldots, \mathcal{I}_n$ are co-maximal ideals (i.e., $\mathcal{I}_1 + \cdots + \mathcal{I}_n = R$), then for any $l_1, \ldots, l_n \in \mathbb{N}\backslash\{0\}$, also*

$$\mathcal{I}_1^{l_1} + \cdots + \mathcal{I}_n^{l_n} = R.$$

Proof: For any $r \in \mathbb{N}$, $R = R^{nr} = (\mathcal{I}_1 + \cdots + \mathcal{I}_n)^{nr} \subseteq \sum_{i_1+\cdots+i_n=nr} \mathcal{I}_1^{i_1} \ldots \mathcal{I}_n^{i_n}$. Now if $i_1 + \cdots + i_n = nr$, then at least one index i_k must be greater than or equal to r. Hence, $R \subseteq \sum_{i_1+\cdots+i_n=nr} \mathcal{I}_1^{i_1} \ldots \mathcal{I}_n^{i_n} \subseteq \mathcal{I}_1^r + \cdots + \mathcal{I}_n^r$
i.e., $\mathcal{I}_1^r + \cdots + \mathcal{I}_n^r = R$ for every $r \in \mathbb{N}$.

Now let $l_1, \ldots, l_n$ be arbitrary positive integers and suppose that $m = \max_{1 \leq i \leq n}\{l_i\}$. Then

$$R \supseteq \mathcal{I}_1^{l_1} + \cdots + \mathcal{I}_n^{l_n} \supseteq \mathcal{I}_1^m + \cdots + \mathcal{I}_n^m = R,$$

proving the assertion. □

Theorem B.1 (Chinese Remainder Theorem) *If $\mathcal{I}_1, \ldots, \mathcal{I}_r$ are pairwise co-maximal ideals in a commutative ring with identity R, then given any $s_1, \ldots, s_r \in R$, there exists $x \in R$ such that $x - s_i \in \mathcal{I}_i$ for every $i \in \{1, \ldots, r\}$.*

B.2 Ideals in number fields

Definition B.1 *A* number field *is a finite (hence algebraic) extension of* $\mathbb{Q}$*, the rational numbers.*

The proof of Lemma B.2 depends on the following classical notions and theorems:

Definition B.2 *A* DEDEKIND domain *is an integrally closed integral domain which is noetherian and in which each non-zero prime ideal is maximal.*

Theorem B.2 *The ring of integers* $\mathcal{O}_K$ *of any number field* K *(i.e. the integral closure of the integers* $\mathbb{Z}$ *in the number field) is a* DEDEKIND *domain.*

Theorem B.3 *In a* DEDEKIND *domain, each non-zero ideal can be factorized uniquely as a product of prime ideals.*

Definition B.3 *A* fractional ideal *of a* DEDEKIND *domain* $\mathcal{O}$ *is a non-zero, finitely generated* $\mathcal{O}$*-submodule of the field of fractions of* $\mathcal{O}$*.*

If $\mathcal{O}$ is a DEDEKIND domain with field of fractions K, then since it is noetherian, each $\mathcal{O}$-ideal is finitely generated and is thus a fractional ideal. $\mathcal{O}$-ideals are referred to as integral ideals in this context.
It is easily shown that a characterization of fractional ideals of $\mathcal{O}$ is the following: given that M is a non-zero $\mathcal{O}$-submodule of K,

$$M \text{ is a fractional ideal of } \mathcal{O} \Leftrightarrow \exists a \in K^* \text{ such that } aM \subseteq \mathcal{O}.$$

Theorem B.4 *The fractional ideals of a* DEDEKIND *domain form a free abelian group under multiplication, usually denoted by* $Div(\mathcal{O})$ *and referred to as the group of divisors of* $\mathcal{O}$*.*

Denoting the subgroup of $Div(\mathcal{O})$ consisting of the principal fractional ideals by $Prin(\mathcal{O})$, we form $Cl(\mathcal{O}) := Div(\mathcal{O})/Prin(\mathcal{O})$, the (ideal) class group of $\mathcal{O}$.

Theorem B.5 (DIRICHLET) *The order of* $Cl(\mathcal{O})$ *is finite whenever* $\mathcal{O}$ *is the ring of integers of a number field.*

Lemma B.2 *Given any number field K, then there exists some finite extension $E \mid K$ such that for every ideal $\mathcal{I}$ of $\mathcal{O}_K$, the $\mathcal{O}_E$ ideal $\mathcal{I}\mathcal{O}_E$ is principal.*

Proof: Let h denote the class number of $\mathcal{O}_K$, the ring of integers of K, and suppose that the class group is given by $Cl(\mathcal{O}_K) = \{\overline{\mathcal{I}_1}, \ldots, \overline{\mathcal{I}_h}\}$, where $\mathcal{I}_j$ is some fractional ideal which is a representative of the ideal class $\overline{\mathcal{I}_j}$, for each j. In order to show the existence of the field E, it will therefore suffice to show that given any representative ideal, there exists a finite extension of K in which this ideal becomes principal, since principal ideals clearly remain principal in any (finite) field extension, and the composite of the fields thus obtained for the finite number of representative ideals will also be a finite extension of K. Thus pick any representative ideal, say $\mathcal{I}$, and denote by $\overline{\mathcal{I}}$ its image in the class group. Because the order of this group is h and its identity is $Prin(\mathcal{O}_K)$, we see that $\overline{\mathcal{I}}^h = Prin(\mathcal{O}_K)$. Thus, $\mathcal{I}^h \in Prin(\mathcal{O}_K)$, say $\mathcal{I}^h = (z)$. Now consider $\underline{\mathcal{I}} = \mathcal{I}\mathcal{O}_L$ where $L = K(\sqrt[h]{z})$. Here, $\underline{\mathcal{I}} = (\sqrt[h]{z})$, because of the unique factorization of ideals in DEDEKIND domains: indeed, since $\underline{\mathcal{I}}^h = (z)$ as $\mathcal{O}_L$-ideals and $(\sqrt[h]{z})^h = (z)$ in $\mathcal{O}_L$, we have that $\underline{\mathcal{I}}^h = (\sqrt[h]{z})^h$ implying that $\underline{\mathcal{I}} = (z)$ from the unique factorization. Thus $\mathcal{I}\mathcal{O}_L$ is principal in L, a finite extension of K. □

B.3 The norm of an ideal in a number field

If $L|K$ is an algebraic extension of fields, then we can map the elements of L to K by means of the norm function, which encodes vital algebraic information since it is built up of the K-isomorphisms of L. If the extension is separable, the norm of an element of L is defined as the product of the conjugates of the element. If, moreover, A is a domain which is integrally closed in its quotient field K, and B is the integral closure of A in some finite separable extension L of K, then the norm function maps B into A : indeed, the conjugates of any element of B are also integral over A, and hence also their product (the norm of this element) is in B. But the norm is then in $K \cap B = A$. In particular then, if $L|K$ is a finite extension of number fields, we know that the norm function maps the ring of integers of L into that of K.

It is also possible to define a mapping of the ideals of a number field to ideals of some subfield (containing $\mathbb{Q}$) of which this field is a finite extension. This mapping is also referred to as a "norm" with respect to the given field extension, and we proceed to define it here and explain an essential property which is needed in the thesis:

Suppose that L is a finite separable extension of K, some number field and let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$.

Then since $\mathcal{O}_L$ is a DEDEKIND domain, there exists a unique factorization of $\mathfrak{p}\mathcal{O}_L$ as a product of prime ideals, say $\mathfrak{p}\mathcal{O}_L = \mathcal{P}_1^{e_1} \dots \mathcal{P}_r^{e_r}$. In this factorization, precisely those prime $\mathcal{O}_L$-ideals J occur for which $J \cap \mathcal{O}_K = \mathfrak{p}$. (These are the prime ideals which are said to "lie above $\mathfrak{p}$"). Indeed, since $\mathfrak{p} \subseteq \mathfrak{p}\mathcal{O}_L = \mathcal{P}_1^{e_1} \dots \mathcal{P}_r^{e_r} \subseteq \mathcal{P}_i$ for each $i \in \{1, \dots, r\}$, each of these ideals lies above $\mathfrak{p}$; and if $\mathcal{Q}$ is some prime $\mathcal{O}_L$-ideal which lies above $\mathfrak{p}$, then $\mathcal{P}_1^{e_1} \dots \mathcal{P}_r^{e_r} = \mathfrak{p}\mathcal{O}_L \subseteq \mathcal{Q}$, so since $\mathcal{Q}$ is prime, $\mathcal{P}_j \subseteq \mathcal{Q}$ for some j, but $\mathcal{O}_L$ being a DEDEKIND domain means that each non-zero prime ideal is maximal and hence that $\mathcal{P}_j = \mathcal{Q}$. Now for any such prime ideal $\mathcal{P}_i$ lying above $\mathfrak{p}$, we define
$e(\mathcal{P}_i|\mathfrak{p}) = e_i$, to be the *ramification index of* $\mathcal{P}_i$ *over* $\mathfrak{p}$, and $f(\mathcal{P}_i|\mathfrak{p}) = f_i$, the *residue class degree of* $\mathcal{P}_i$ *over* $\mathfrak{p}$ is the degree of $\mathcal{O}_L/\mathcal{P}_i$ as a field extension of $\mathcal{O}_K/\mathfrak{p}$.
Then we define the norm of $\mathcal{P}_i$ with respect to the extension $L|K$ as : $N_{L|K}(\mathcal{P}_i) = \mathfrak{p}^{f_i}$.

Definition B.4 *If L and K are as above and $\mathcal{I}$ is an ideal of L having unique factorization as a product of prime ideals given by $\mathcal{I} = \prod_{i=1}^{m} \mathcal{Q}_i^{r_i}$, then*

$$N_{L|K}(\mathcal{I}) := \prod_{i=1}^{m} (N_{L|K}(\mathcal{Q}_i))^{r_i}$$

is the norm of $\mathcal{I}$ with respect to the extension $L|K$.

Observation

$N_{L|K}(\mathcal{I})$ is an ideal of K.

Notation

If $K = \mathbb{Q}$, then $\mathcal{O}_K = \mathbb{Z}$ is a principal ideal domain, and we denote the absolute value of a generator of $N_{L|\mathbb{Q}}(\mathcal{I})$ by $|N_{L|\mathbb{Q}}(\mathcal{I})|$.

Proposition B.1 *([10, Proposition 21]) If L, K and $\mathcal{O}_L$ are as above, then given any prime ideal $\mathfrak{p}$ of K, if $\mathcal{P}_i$ are the primes lying above $\mathfrak{p}$ for $i \in \{1, \dots, r\}$, then*

$$[L : K] = \sum_{\mathcal{P}_i|\mathfrak{p}} e_i f_i.$$

Corollary B.1 *If $L|K$ is a* GALOIS *extension and $\mathcal{I}$ is any ideal of L, then denoting the* GALOIS *group of $L|K$ by G, we have that*

$$N_{L|K}(\mathcal{I})\mathcal{O}_L = \prod_{\tau \in G} \mathcal{I}^{\tau}.$$

Proof: Firstly observe that for any prime ideal $\mathfrak{p}$ of K, the prime ideals lying above $\mathfrak{p}$ are conjugates: suppose to the contrary that $\mathcal{Q}$ is a prime ideal lying above $\mathfrak{p}$ which is not a conjugate of some other prime ideal $\mathcal{P}$ which also lies above $\mathfrak{p}$. Then, since $\mathcal{Q}$ and $\mathcal{P}$ are non-equal maximal ideals, they are co-maximal, and trivially $\mathcal{Q}$ and the conjugates of $\mathcal{P}$ are thus also co-maximal so that from the Chinese Remainder Theorem, there exists $a \in \mathcal{Q} \setminus \bigcup_{\tau \in G} \mathcal{P}^\tau$. But then $a^\sigma \notin \bigcup_{\tau \in G} \mathcal{P}^\tau$ for every $\sigma \in G$, so that $\prod_{\sigma \in G} a^\sigma \notin \bigcup_{\tau \in G} \mathcal{P}^\tau$ as each of the ideals $\mathcal{P}^\tau$ is prime. However, $\prod_{\sigma \in G} a^\sigma = N_{L|K}(a) \in \mathcal{O}_K$ because $a \in \mathcal{O}_L$ and $\prod_{\sigma \in G} a^\sigma \in \mathcal{Q}$, so that $\prod_{\sigma \in G} a^\sigma \in \mathcal{Q} \cap \mathcal{O}_K = \mathfrak{p}$, while $\prod_{\sigma \in G} a^\sigma \notin \mathcal{P}$, which is a contradiction.

Now suppose that $\mathfrak{p}\mathcal{O}_L = \mathcal{P}_1^{e_1} \dots \mathcal{P}_r^{e_r}$ where $\mathcal{P}_1, \dots, \mathcal{P}_r$ are the distinct primes lying above $\mathfrak{p}$. Then with $\mathfrak{p} \subset K$, it follows that $\mathfrak{p}\mathcal{O}_L = (\mathfrak{p}\mathcal{O}_L)^\tau$ for each $\tau \in G$. Thus $\mathfrak{p}\mathcal{O}_L = (\mathcal{P}_1 \dots \mathcal{P}_r)^e$ for some index e which is the shared index of ramification of each prime lying above $\mathfrak{p}$. It is also easy to see that $f_i = f_j$ for every $i, j \in \{1, \dots, r\}$ since any basis for $\mathcal{O}_L/\mathcal{P}_i$ over $\mathcal{O}_K/\mathfrak{p}$ is mapped to a basis of $\mathcal{O}_L/\mathcal{P}_i^\tau$ by $\tau \in G$. Thus, from the above Proposition, setting $f_i = f$, we have that $efr = [L : K]$.

Moreover,

$$N_{L|K}(\mathcal{P}_i)\mathcal{O}_L = \mathfrak{p}^f\mathcal{O}_L = (\mathfrak{p}\mathcal{O}_L)^f = ((\mathcal{P}_1 \dots \mathcal{P}_r)^e)^f = (\mathcal{P}_1 \dots \mathcal{P}_r)^{ef},$$

where $\mathcal{P}_1, \dots, \mathcal{P}_r$ are the distinct conjugates of $\mathcal{P}_i$ for any $i \in \{1, \dots, r\}$. Now we know that $(\mathcal{P}_1 \dots \mathcal{P}_r)^{ef} = \prod_{\tau \in G} \mathcal{P}_i^\tau$ for any $i \in \{1, \dots, r\}$, as each $\mathcal{P}_i$ has precisely r conjugates (including itself) and $(\mathcal{P}_1 \dots \mathcal{P}_r)^e = (\mathcal{P}_1^\tau \dots \mathcal{P}_r^\tau)^e$ for all $\tau \in G$ (from $\mathfrak{p}\mathcal{O}_L = (\mathfrak{p}\mathcal{O}_L)^\tau$ for every $\tau \in G$) implies that the $efr = [L : K] = \#G$ automorphisms of G must act transitively on these conjugates. The result then follows from the definition of $N_{L|K}(\mathcal{I})$.□

Glossary of notation

$\mathbb{N}$	the natural numbers
$\mathbb{Q}$	the rational numbers
$\mathbb{R}$	the real numbers
$\mathbb{C}$	the complex numbers
Ω_p	the completion of the algebraic closure of the completion of $\mathbb{Q}$ under the p-adic metric
$v_p(\cdot)$	the p-adic valuation
(K, v)	the valued field K
$(K, \lvert\cdot\rvert)$	the normed field K
$\lvert K^* \rvert$	the value group of the valuation on the normed field K
$\mathcal{O}_K$	the valuation ring of the valued field K
$\mathcal{M}_K$	the maximal ideal of $\mathcal{O}_K$
$\overline{K}$	the residue field $\mathcal{O}_K/\mathcal{M}_K$
$v_G(\cdot)$	the GAUSS valuation arising from the valuation v
$\lvert\cdot\rvert_G$	the GAUSS norm arising from the norm $\lvert\cdot\rvert$
$R[z]$	polynomial ring with coefficients in the ring R
$R(z)$	rational functions in z with coefficients in the ring R
$R[[z]]$	ring of formal power series in z with coefficients in the ring R
$R\{z\}$	the algebra of convergent power series in z with coefficients in the ring R
$\mathbb{P}^n_K$	the scheme $\mathrm{Proj}K[x_0, \ldots, x_n]$
$\mathbb{P}^n(K)$	K-rational points of $\mathbb{P}^n_K$
$D_r(x)$	the open disc of radius r about x : $\{z : \lvert z - x\rvert < r\}$
$\overline{D}_r(x)$	the closed disc of radius r about x : $\{z : \lvert z - x\rvert \leq r\}$
$C_r(x)$	the circle of radius r about x : $\{z : \lvert z - x\rvert = r\}$
$\deg f$	the degree of the polynomial f
$\phi'(x)$	the derivative of the rational function ϕ viewed as a quotient of polynomials

$\Theta_{P,X}$	the tangent space of X at the point P
$\Theta^*_{P,X}$	the cotangent space of X at the point P
$\phi^*(P)$	the scalar determining the mapping of the cotangent space at P associated to ϕ
$F(X)$	the function field of the variety X
$\mu(\cdot)$	the MÖBIUS function
$Z_n(\phi)$	the cycle of n-periodic points of ϕ
$Z^*_n(\phi)$	the cycle of essential n-periodic points of ϕ

References

[1] R L Benedetto, *Fatou Components in p-adic Dynamics,* Ph.D. Thesis, Brown University, 1998.

[2] R L Benedetto, *Reduction, Dynamics and Julia Sets of Rational Functions,* to appear: J. Number Theory, 1999.

[3] S Bosch, U Günter and R Remmert, *Non-archimedean Analysis,* Springer-Verlag Berlin Heidelberg, 1984.

[4] R L Devaney, *An Introduction to Chaotic Dynamical Systems,* Second Edition, Addison-Wesley, Redwood City California,1989.

[5] O Endler, *Valuation Theory,* Springer-Verlag Berlin Heidelberg, 1972.

[6] R Hartshorne, *Algebraic Geometry,* Springer-Verlag New York, 1977.

[7] L - C Hsia, *A weak Néron model with applications to p-adic dynamical systems,* Compositio Math., **100** (1996), 277-304.

[8] S Kawaguchi, *A remark on periodic points on varieties over a field of finite type over* $\mathbb{Q}$, preprint, 1999.

[9] N Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta Functions,* Springer-Verlag New York, 1977.

[10] S Lang, *Algebraic Number Theory,* Addison-Wesley, Reading Massachusetts, 1970.

[11] P J McCarthy, *Algebraic Extensions of Fields,* Dover Publications, New York, 1991.

[12] L Merel, *Bournes pour la torsion des courbes elliptiques sur les corps de nombres,* Invent. Math., **124**, no. 1-3 (1996), 437-449.

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

[14] D Mumford, *The Red Book of Varieties and Schemes, Lecture Notes in Mathematics:* **1358**, Springer-Verlag Berlin Heidelberg, 1988.

[15] D G Northcott, *Periodic Points on an Algebraic Variety,* Annals of Math., **51** No.1 (1950), 167-177.

[16] H -O Peitgen and P H Richter, *The Beauty of Fractals,* Springer-Verlag Berlin Heidelberg, 1986.

[17] R S Rumely, *Capacity Theory on Algebraic Curves, Lecture Notes in Mathematics:* **1378**, Springer-Verlag Berlin Heidelberg, 1980.

[18] I R Shafarevich, *Basic Algebraic Geometry,* Springer-Verlag Berlin Heidelberg, 1977.

[19] J H Silverman, *The Arithmetic of Elliptic Curves,* Springer-Verlag New York, 1986.

[20] H Stichtenoth, *Algebraic Function Fields and Codes,* Springer-Verlag Berlin Heidelberg, 1993.

[21] B L van der Waerden, *Algebra,* Dritte Auflage, Springer-Verlag Berlin Göttingen Heidelberg, 1955.