CIRM

Troisième Rencontre Internationale sur les Polynômes à Valeurs Entières

Rencontre organisée par :
Sabine Evrard

29 novembre-3 décembre 2010

David Adam and Youssef Fares

On the dynamics of $\varphi : x \to x^p + a$ in a local field

Vol. 2, n° 2 (2010), p. 81-85.

<http://acirm.cedram.org/item?id=ACIRM_2010__2_2_81_0>

Centre international de rencontres mathématiques
U.M.S. 822 C.N.R.S./S.M.F.
Luminy (Marseille) France

Actes des rencontres du C.I.R.M.
Vol. **2** n° 2 (2010) 81-85

On the dynamics of $\varphi : x \to x^p + a$ in a local field

David Adam and Youssef Fares

Abstract

Let K be a local field, $a \in K$ and $\varphi : x \to x^p + a$ where p denotes the characteristic of the residue field. We prove that the minimal subsets of the dynamical system (K, φ) are cycles and describe the cycles of this system.

1. Introduction

A discrete dynamical system is a couple (X, g), where X is a metric space and $g : X \to X$ is a continuous map. First, recall some basic definitions.

Definitions 1. Let (X, g) be a discrete dynamical system and $x \in X$.
(1) The orbit of x is the set $\{g^n(x) \mid n \in \mathbb{N}\}$.
(2) The point x is *periodic* if there exists $r \in \mathbb{N}$ such that $g^r(x) = x$. The orbit of x is then called a cycle and its cardinality is the *period* of x.
(3) The point $x \in X$ is *recurrent* if x is an accumulation point of its orbit.
(4) The system (X, g) is *minimal* if, for all $z \in X$, the orbit of z is dense in X.
(5) A subset E of X is *minimal* if E is invariant by g and the subsystem (E, g) is minimal.

The existence of minimal subsets is given by the following theorem which is a consequence of Zorn's lemma.

Theorem 2 (Birkhoff)**.** *Every compact space admits minimal subsets.*

The case where K is a local field and $\varphi(x) = ax + b$ is well studied (for instance, see [2]). In this paper[1], we consider the dynamical system (K, φ) where K is a local field and $\varphi(x) = x^p + a$ (a is an element of K and p denotes the characteristic of the residue field). We prove that the minimal subsets of the system (K, φ) are cycles and we describe the set of all periods of φ.

2. Minimal subsets of the dynamical system $(K, x^p + a)$

Notation: K is a local field, that is, a field endowed with a discrete valuation v which is complete for the corresponding topology and whose residue field k is finite. We denote by V the valuation domain $\{x \in K \mid v(x) \geq 0\}$, $\mathfrak{M}$ its maximal ideal, q the cardinality of the residue field $k = V/\mathfrak{M}$, p the characteristic of k, thus $q = p^f$.

Recall that V is compact and K is locally compact.

Obviously, if $v(a) < 0$, then the system (K, φ) has no recurrent point. Thus, in what follows, we will assume that $v(a) \geq 0$. In this case, any recurrent point of (K, φ) admits a non-negative valuation, and hence, we will consider minimal subsets in V. Then, we have:

Proposition 3. *Let $a \in V$ and $\varphi(x) = x^p + a$. Every minimal subset of the system (V, φ) is a cycle of length $\leq q$.*

Text presented during the meeting "Third International Meeting on Integer-Valued Polynomials" organized by Sabine Evrard. 29 novembre-3 décembre 2010, C.I.R.M. (Luminy).
2000 *Mathematics Subject Classification.* 37B99, 11F85.
Key words. Dynamical systems, local fields.

[1]This paper was presented by Youssef Fares.

Proof. It follows from Proposition 4 below and Taylor's formula that two elements of a minimal subset E of V are non-congruent modulo $\mathfrak{M}$, and hence, E is necessarily finite. ☐

For extended versions of short or missing proofs, see [1].

Proposition 4. [3, Proposition 6] *Let E be a compact subset of K and let $f : E \to E$ be 1-lipschitzian. Then $f(E) = E$ if and only if f is an isometry, that is,*

$$v(f(x) - f(y)) = v(x - y),$$

for all $x, y \in E$.

Theorem 5. *Let K be a local field with valuation domain V and let q be the cardinality of its residue field. Let $a \in V$ and $\varphi(x) = x^p + a$. Then there are only finitely many minimal subsets of the dynamical system (K, φ); they are cycles in V of lengths $r_1, r_2, \dots r_k$ and one has*

$$r_1 + r_2 + \cdots r_k = q.$$

Proof. Let $E_1, E_2, \dots E_s$ be distinct minimal subsets of (V, φ). By Proposition 3, they are cycles in V of lengths $r_1, r_2, \dots r_s$. On the one hand, we may verify that if a and $b \in V$ are in two distinct cycles, then necessarily $v(a - b) = 0$. Consequently, $r_1 + r_2 + \cdots r_s \leq q$. On the other hand, if $r_1 + r_2 + \cdots r_s < q$, then $E' = \{x \in V \mid v(x - y) = 0, \forall y \in \cup_{1 \leq i \leq s} E_i\} \neq \emptyset$. Since E' is an invariant compact subset of V, by Theorem 2, the subsystem (E', φ) admits a minimal subset E_{s+1} of cardinality r_{s+1}. By iteration of the procedure, we may conclude. ☐

Of course, $\varphi : x \in V \mapsto x^p + a \in V$ induces a map on the residue field $\overline{\varphi} : y \in k \mapsto y^p + \overline{a} \in k$ where $\overline{a}$ denotes the class of a modulo $\mathfrak{M}$.

Proposition 6. *The lengths of the cycles of φ in V and of the cycles of $\overline{\varphi}$ in k are the same.*

Proof. Every cycle of φ in V induces a cycle in k with the same length. The converse is a consequence of the following remark: if x_0 belongs to a cycle of length r and if $v(x - x_0) > 0$, then the sequence $\{\varphi^{nr}(x)\}_{n \geq 0}$ converges to x_0. ☐

3. Lengths of cycles

Recall that the set of periods of φ in V and of $\overline{\varphi}$ in k are the same and that $q = p^f$. We start with a simple remark.

Remarks 7. *Suppose that $f = 1$.*

1. *If $v(a) = 0$, every minimal subset of (K, φ) is a cycle of length p.*
2. *If $v(a) \geq 1$, the system (K, φ) admits exactly p fixed points.*

From now on, we suppose that $f \neq 1$. Let σ be the Frobenius of $k : \sigma(x) = x^p$ for all $x \in k$. The field k is a Galoisian extension of $\mathbb{F}_p$ of dimension f. By the normal basis theorem, there exists $w \in k$ such that $(w, \sigma(w), \dots \sigma^{f-1}(w))$ is a basis of k over $\mathbb{F}_p$. Thus, every element $x \in k$ can be written

$$x = \sum_{j=0}^{f-1} x_j w^{p^j} \qquad (x_j \in \mathbb{F}_p).$$

The trace $\mathrm{Tr}(x)$ of an element $x \in k$ relative to $\mathbb{F}_p$ is:

$$\mathrm{Tr}(x) = \sum_{j=0}^{f-1} \sigma^j(x).$$

An easy computation leads to the following lemma:

Lemma 8. *Let $x = \sum_{j=0}^{f-1} x_j w^{p^j} \in k$ and $s(x) = \sum_{j=0}^{f-1} x_j$. Then*

$$\mathrm{Tr}(x) = s(x)\mathrm{Tr}(w)$$

and, for every $n \in \mathbb{N}$, we have

$$\varphi^n(x) = x^{p^n} + a^{p^{n-1}} + \cdots a^p + a = \sigma^n(x) + \sum_{j=0}^{n-1} \sigma^j(a).$$

In particular,

Lemma 9. *Let* $r \in \mathbb{N}$ *and* $x \in k$. *If* $r = \alpha f + r_0$, $\alpha, r \in \mathbb{N}$, $r_0 < f$, *then*

$$\varphi^r(x) = \varphi^{r_0}(x) + \alpha s(a) \sum_{i=0}^{f-1} w^{p^i}.$$

Lemma 10. *If* r *is a period of* (V, φ), *then* r *divides* pf.

Proof. By the the previous lemma, for every $x \in k$, we have

$$\varphi^{pf}(x) = \varphi^0(x) + p\mathrm{Tr}(a) = x.$$

Consequently, r divides pf. □

We prove now that the set $Per(a)$ formed by the periods of the system (K, φ) depends only on $\mathrm{Tr}(a)$. First, we need some notations.

Notations:

(1) For every $n \in \mathbb{Z}$, we denote by $\theta(n)$ the unique non-negative integer such that $\theta(n) \equiv n \pmod f$ and $0 \leq \theta(n) < f$.

(2) For every $r \in \mathbb{N}$, we denote by $o(r)$ the order of the class of r in the group $\mathbb{Z}/f\mathbb{Z}$ and by $d(r)$ the non-negative integer such that:

$$o(r)r = d(r)f.$$

Lemma 11. *Let* L *be a field,* n *a positive integer and* $a_0, a_1 \ldots a_n$ *elements of* L. *The system*

$$\begin{cases} x_1 &= x_2 + a_1 \\ x_2 &= x_3 + a_2 \\ \vdots & \vdots \quad \vdots \\ x_{n-1} &= x_n + a_{n-1} \\ x_n &= x_1 + a_n \end{cases}$$

admits a solution in L^n *if and only if* $\sum_{i=1}^n a_i = 0$.
Futhermore, if $\sum_{i=1}^n a_i = 0$ *then the set of the solutions is an affine space of* L^n *of dimension* 1.

Proposition 12. *Let* $a \in k$ *and* $\varphi(x) = x^p + a$. *For every* $r \in \mathbb{N}$, *the equation* $\varphi^r(x) = x$ *admits a solution in* k *if and only if* $d(r)s(a) = 0$ *in* $\mathbb{F}_p$. *In which case, the equation* $\varphi^r(x) = x$ *has* $p^{\frac{f}{o(r)}}$ *solutions.*

Proof. Write $r = \alpha f + r_0$ with $\alpha, r \in \mathbb{N}$ and $r_0 < f$, $a = \sum_{j=0}^{l-1} a_j w^{p^j}$ with $a_j \in \mathbb{F}_p$ and, for every $x \in k$, $x = \sum_{j=0}^{f-1} x_j w^{p^j}$ with $x_i \in \mathbb{F}_p$. The equation $\varphi^r(x) = x$ is equivalent to the following system with f equations and f unknowns x_m $(0 \leq m < f)$:

$$x_{\theta(i-jr_0)} + \sum_{l=0}^{r_0-1} a_{\theta(i-(j-1)r_0-l)} + \alpha s(a) = x_{\theta(i-(j-1)r_0)}$$

where $0 \leq i < f/o(r_0)$ and $0 \leq j < o(r_o)$.

Furthermore, for every i $(0 \leq i < f/o(r_0))$, by Lemma 11, the system

$$\Sigma_i : \quad x_{\theta(i-jr_0)} + \sum_{l=0}^{r_0-1} a_{\theta(i-(j-1)r_0-l)} + \alpha s(a) = x_{\theta(i-(j-1)r_0)} \quad (0 \leq j < o(r_0))$$

admits a solution if and only if

$$\sum_{j=0}^{o(r_0)-1} \left(\sum_{l=0}^{r_0-1} a_{\theta(i-(j-1)r_0-l)} + \alpha s(a) \right) = 0,$$

that is, if and only if $d(r)s(a) = 0$.

Since the systems Σ_i $(0 \leq i < f/o(r))$ are independent, the equation $\varphi^r(x) = x$ has a solution if and only if $d(r)s(a) = 0$. Moreover, if $d(r)s(a) = 0$, each system Σ_i admits p solutions, and hence, the equation $\varphi^r(x) = x$ has $p^{\frac{f}{o(r)}}$ solutions. □

In order to describe the set $Per(a)$ of periods of (K, φ) we distinguish two cases:

3.1. **The case** $\mathrm{Tr}(a)=0$.

Note first that $s(a)=0$ is equivalent to $\mathrm{Tr}(a)=0$. According to Proposition 12, for every $r\in\mathbb{N}$, the equation $\varphi^r(x)=x$ admits at least one solution.

Theorem 13. *Let $a\in k$ and $\varphi(x)=x^p+a$. If $\mathrm{Tr}(a)=0$, the set $Per(a)$ of periods of φ is the set of divisors of f.*

Proof. Since $\varphi^f(x)=x$ for every $x\in k$, f is a multiple of every element of $Per(a)$. Conversely, let $r\in\mathbb{N}$ be a divisor of f and denote by $r'\in\mathbb{N}$ any strict divisor of r. The order of r (resp. r') in $\mathbb{Z}/f\mathbb{Z}$ is f/r (resp. f/r'). By Proposition 12,

$$\mathrm{Card}\left(\bigcup_{\substack{r'|r\\ r'\neq r}}\{x\in k\mid\varphi^{r'}(x)=x\}\right)\leq\sum_{\substack{r'|r\\ r'\neq r}}p^{\frac{f}{f/r'}}\leq\sum_{r'=1}^{[r/2]}p^{\frac{fr'}{f}}<p^{\frac{f}{f/r}}.$$

Hence, there exists cycles with length r. ☐

Corollary 14. *If $a\in V$ is such that $\mathrm{Tr}(\overline{a})=0$, then 1 and f are elements of $Per(a)$. In particular, the equation $x^p+a=x$ admits p solutions in K.*

3.2. **The case** $\mathrm{Tr}(a)\neq 0$.

Lemma 15. *Let $a\in k$ be such that $\mathrm{Tr}(a)\neq 0$ and let $r\in\mathbb{N}$. The equation $\varphi^r(x)=x$ has a solution in k if and only if $v_p(r)>v_p(f)$ where v_p denotes the p-adic valuation.*

Proof. Following Proposition 12, the equation $\varphi^r(x)=x$ has a solution in k if and only if p divides $d(r)$. As $o(r)r=d(r)f$, the divisibility of $d(r)$ by p is equivalent to $v_p(r)>v_p(f)$. ☐

Theorem 16. *Let $a\in V$ be such that $\mathrm{Tr}(\overline{a})\neq 0$. Write $f=p^nf_0$ where f_0 and p are coprime. Then $r\in\mathbb{N}$ is a period of (V,φ) if and only if $r=p^{n+1}d$ where d is a divisor of f_0.*

Proof. Obviously, $o(pf)=1$ and, by Lemma 12, the equation $\varphi^{pf}(x)=x$ has p^f solutions. Consequently, every $x\in k$ satisfies $\varphi^{pf}(x)=x$. Hence, every $r\in Per(a)$ divides pf. Since by Lemma 15, $v_p(r)>v_p(f)$, we deduce that $r=p^{n+1}d$ where d is a divisor of f_0. Conversely, let $r=p^{n+1}d$ where d is a divisor of f_0. In the same way as in the proof of Theorem 13, one shows that there exist elements of k belonging to a cycle of period r and not belonging to a cycle of period $r'<r$. ☐

Corollary 17. *Let $a\in V$ be such that $\mathrm{Tr}(\overline{a})\neq 0$. If $p\nmid f$, then the set of periods of φ is*

$$Per(a)=\{pd\mid d|f\}.$$

4. Conjugacy

Recall that two dynamical systems (X,g) and (Y,h) are conjugate if there exists an homeomorphism $S:X\longrightarrow Y$ such that the following diagram is commutative:

$$\begin{array}{ccc} X & \xrightarrow{g} & X\\ {\scriptstyle S}\big\downarrow & & \big\downarrow{\scriptstyle S}\\ Y & \xrightarrow{h} & Y\end{array}$$

In this section, we assume that the local field K has a positive characteristic.

Let a and b be two elements of V and consider $\varphi_a(x)=x^p+a$ and $\varphi_b(x)=x^p+b$. We will give conditions for the systems (K,φ_a) and (K,φ_b) to be conjugate. Obviously, if the systems (K,φ_a) and (K,φ_b) are conjugate then the lengths of their cycles are the same, and either $s(\overline{a})=0$ and $s(\overline{b})=0$, or $s(\overline{a})\neq 0$ and $s(\overline{b})\neq 0$. We prove now the converse.

Lemma 18. *Let $c\in V$ be such that $s(\overline{c})=0$. Then the equation $x^p-x-c=0$ admits a solution in V.*

Proof. Since k is a cyclic extension of $\mathbb{F}_p$, according to the additive form of Hilbert's Theorem 90, the equation $\sigma(x)-x=\overline{c}$ admits a solution in k. Equivalently, the polynomial $x^p-x-\overline{c}$ has a root in k and, by Hensel lemma, the polynomial x^p-x-c admits a root in V. ☐

Theorem 19. *Let K be a local field of characteristic $p > 0$ and let $a, b \in V$. Then the systems (K, φ_a) and (K, φ_b) are conjugate if and only if either $s(\overline{a}) = 0$ and $s(\overline{b}) = 0$, or $s(\overline{a})s(\overline{b}) \neq 0$.*

Proof. We just need to show that if either $s(\overline{a}) = 0$ and $s(\overline{b}) = 0$, or $s(\overline{a})s(\overline{b}) \neq 0$, then the systems (K, φ_a) and (K, φ_b) are conjugate. We distinguish two cases.
Case 1: $s(\overline{a}) = s(\overline{b}) = 0$. In this case, $s(\overline{a} - \overline{b}) = 0$ and, by Lemma 18, there exists $\alpha \in V$ such that $\alpha^p - \alpha - (a - b) = 0$. Let $f(x) = x + \alpha$, then $f \circ \varphi_a = \varphi_b \circ f$.
Case 2: $s(\overline{a})s(\overline{b}) \neq 0$. In this case, there exists $\alpha_0 \in \mathbb{F}_p^*$ such that $\alpha_0 s(\overline{a}) = s(\overline{b})$, or equivalently, such that $s(\alpha_0\overline{a} - \overline{b}) = 0$. Let $\alpha \in V$ be such that $\overline{\alpha} = \alpha_0$. Since $s(\overline{\alpha a - b}) = 0$, by Lemma 18, there exists $\beta \in V$ such that $\beta^p - \beta - (\alpha a - b) = 0$. Let $f(X) = \alpha X + \beta$, then $f \circ \varphi_a = \varphi_b \circ f$. $\square$

References

[1] D. Adam and Y. Fares, On two like-affine dynamical systems in a local field, preprint.
[2] A.-H. Fan and Y. Fares, Minimal subsystems of affine dynamics on local fields, *Arch. Math.* **96** (2011), 423–434.
[3] Y. Fares, Factorial preservation, *Arch. Math.* **83** (2004), 497–506.