SEN'S THEOREM ON THE ITERATION OF WILDLY RAMIFIED FIELD AUTOMORPHISMS

JUAN RIVERA-LETELIER

In this expository note we give 2 proofs of the following theorem of Shankar Sen. Given a field k and a power series $f(T)$ in $k[[T]]$, denote by $\mathrm{ord}(f)$ the order of vanishing of f at zero. So, we have $\mathrm{ord}(f) := +\infty$ if $f(T)$ is identically zero and otherwise $\mathrm{ord}(f)$ is the lowest degree of a nonzero term of $f(T)$. On the other hand, put $f^0(T) := T$, and for each strictly positive integer j denote by $f^j(T)$ the j-th iterate of $f(T)$.

Theorem 1 ([Sen69, Theorem 1]). *Let p be a prime number, k a field of characteristic p, and*

$$f(T) = T + a_2 T^2 + \cdots$$

a power series in $k[[T]]$. For every nonnegative integer n, put

$$i_n := \mathrm{ord}\left(\frac{f^{p^n}(T) - T}{T}\right).$$

Then, for every strictly positive integer n such that i_n is finite we have

$$i_n \equiv i_{n-1} \mod p^n.$$

In §1 we give Sen's original proof. This proof is elementary and short, but rather tricky. In §2 we give (a simplified version of) Lubin's proof in [Lub95]. This proof is even shorter than Sen's original proof, and it is also conceptual: The number $i_n - i_{n-1}$ is interpreted as the number a periodic points of minimal period p^n of a "lift" of the power series $f(T)$. The proof given in §2 is taken from [LRL16, §3.1], where a higher order version of Sen's theorem is shown. See also [Li96, Theorem 3.1] for another variant of Lubin's proof.

Acknowledgments. The author would like to thank David Crnčević for a careful reading of this note.

1. Sen's original proof

Denote by $k((T))$ the field of Laurent power series, and extend the valuatioin ord to $k((T))$. For each nonzero integer μ, denote by $m(\mu)$ the largest integer $m \geq 0$ such that p^m divides μ.

Let $g_0(T)$ be the power series in $k[[T]]$ given by $g_0(T) := 1$, and for every strictly positive integer μ put

$$g_\mu(T) := \prod_{j=0}^{\mu-1} f^j(T).$$

Morevoer, for each stricly negative integer μ, put $g_\mu := 1/g_{-\mu}$.

Lemma 1. *For every integer μ we have*

$$\mathrm{ord}(g_\mu(T)) = \mu \text{ and } \mathrm{ord}(g_\mu \circ f(T) - g_\mu(T)) = \mu + i_{m(\mu)}.$$

Date: January 2013, revised May 2022.

Proof. If μ is nonnegative, then the first assertion follows from the observation that for every nonnegative integer j we have $\mathrm{ord}(f^j(T)) = 1$, and the second assertion follows from the identity $g_\mu \circ f(T) = g_\mu(T) \cdot f^\mu(T)/T$. The case where μ is strictly negative follows easily from the case where μ is nonnegative. □

Lemma 2. *Let $h(T)$ in $k((T))$ be nonzero. Then, for every integer μ satisfying $\mu \geq \mathrm{ord}(h)$ we can choose an element c_μ of k such that*

$$h = \sum_{\mu=\mathrm{ord}(h)}^{+\infty} c_\mu g_\mu. \tag{1.1}$$

Proof. For $\mu = \mathrm{ord}(h)$, let $c_{\mathrm{ord}(h)}$ be the coefficient of $T^{\mathrm{ord}(h)}$ in $h(T)$. Let μ be an integer satisfying $\mu \geq \mathrm{ord}(h)$, and such that for every m in $\{\mathrm{ord}(h), \ldots, \mu\}$ the coefficient c_m has been defined. Then, define $c_{\mu+1}$ as the coefficient of $T^{\mu+1}$ in $h(T) - \sum_{m=\mathrm{ord}(h)}^{\mu} c_m g_m$.

Let $\widehat{h}(T)$ be given by the right side of (1.1). By the first assertion of Lemma 1, for every integer μ satisfying $\mu \geq \mathrm{ord}(h)$ we have

$$\mathrm{ord}(h - \widehat{h}) \geq \max\left\{ \mathrm{ord}\left(h - \sum_{m=\mathrm{ord}(h)}^{\mu} c_m g_m \right), \mathrm{ord}\left(\sum_{m=\mu+1}^{+\infty} c_m g_m \right) \right\} \geq \mu + 1.$$

Taking $\mu \to +\infty$, we obtain the lemma. □

Lemma 3. *Let n be a strictly positive integer such that i_{n-1} is finite, and suppose that for every j in $\{1, \ldots, n-1\}$ we have*

$$i_{j-1} \equiv i_j \bmod p^j.$$

Then the following properties hold:

1. *For every integer μ satisfying $m(\mu) \leq n-1$, we have*
$$\mu + i_{m(\mu)} \neq i_{n-1};$$
2. *For every pair of distinct integers μ and μ' satisfying $m(\mu) \leq n-1$ and $m(\mu') \leq n-1$, we have*
$$\mu + i_{m(\mu)} \neq \mu' + i_{m(\mu')};$$
3. *For every Laurent power series $h(T)$ in $k((T))$ satisfying*
$$\mathrm{ord}(h(T)) \geq i_{n-1} - i_n + 1,$$
we have
$$\mathrm{ord}(h \circ f(T) - h(T)) \neq i_{n-1}.$$

Proof. To prove item 1, note that $p^{m(\mu)+1}$ divides $i_{n-1} - i_{m(\mu)}$. Thus $\mu \neq i_{n-1} - i_{m(\mu)}$ and therefore $\mu + i_{m(\mu)} \neq i_{n-1}$.

To prove item 2, note that the case where $m(\mu) = m(\mu')$ is trivial. Suppose $m(\mu) \neq m(\mu')$. Interchanging μ and μ' if necessary, we assume $m(\mu) \geq m(\mu') + 1$. Then, our hypotheses imply that $p^{m(\mu')+1}$ divides $i_{m(\mu)} - i_{m(\mu')}$. On the other hand, $p^{m(\mu')+1}$ does not divide $\mu - \mu'$, so we have

$$\mu - \mu' \neq i_{m(\mu)} - i_{m(\mu)}.$$

This implies item 2.

To prove item 3, for each integer μ satisfying $\mu \geq \mathrm{ord}(h)$ let c_μ be given by Lemma 2 so we have (1.1). If μ is an integer satisfying $\mu \geq \mathrm{ord}(h)$ and $m(\mu) \geq n$, then we have

$$\mathrm{ord}(g_\mu \circ f(T) - g_\mu(T)) = \mu + i_{m(\mu)} \geq \mathrm{ord}(h) + i_n \geq i_{n-1} + 1.$$

Write

$$h \circ f(T) - h(T) = \sum_{\substack{\mu=\mathrm{ord}(h) \\ m(\mu)\leq n-1}}^{+\infty} c_\mu(g_\mu \circ f(T) - g_\mu(T)) + \sum_{\substack{\mu=\mathrm{ord}(h) \\ m(\mu)\geq n}}^{+\infty} c_\mu(g_\mu \circ f(T) - g_\mu(T)).$$

By the considerations above, the order of second sum is at least $i_{n-1}+1$. On the other hand, by Lemma 1 and items 1 and 2, the orders of the terms in the first sum above are pairwise distinct and none of them is equal to i_{n-1}. Combined, these properties imply that the order of $h \circ f(T) - h(T)$ is different from i_{n-1}. This completes the proof of the lemma. □

First proof of Theorem 1. We proceed by induction. Let n be an strictly positive integer and suppose that for every power series $g(T)$ in $k((T))$ that is tangent to the identity at $T = 0$ and for every j in $\{1, \ldots, n-1\}$ we have

$$\mathrm{ord}\left(\frac{g^{p^j}(T) - T}{T}\right) \equiv \mathrm{ord}\left(\frac{g^{p^{j-1}}(T) - T}{T}\right) \mod p^j.$$

Note that for $n = 1$ this assertion is vacuously true. Suppose that there was a power series $f(T)$ in $k((T))$ that is tangent to the identity at $T = 0$ and such that

$$i_n \not\equiv i_{n-1} \mod p^n.$$

Applying the induction hypothesis to $g = f^p$, we would have

$$i_n \equiv i_{n-1} \mod p^{n-1}.$$

Thus, $n-1$ would be the largest nonnegative integer m such that p^m divides $i_{n-1} - i_n$. Put

$$s := i_{n-1} - i_n \text{ and } \widehat{g}_s(T) := \prod_{j=0}^{s-1} f^{jp}(T),$$

and note that by Lemma 1 with f replaced by f^p we have $\mathrm{ord}(\widehat{g}_s) = s$ and

$$\mathrm{ord}(\widehat{g}_s \circ f^p(T) - \widehat{g}_s(T)) = s + \mathrm{ord}\left(\frac{f^{ps}(T) - T}{T}\right) = s + i_n = i_{n-1}.$$

On the other hand, putting

$$h(T) := \widehat{g}_s(T) + \widehat{g}_s \circ f(T) + \cdots + \widehat{g}_s \circ f^{p-1}(T),$$

we have

$$\mathrm{ord}(h) \geq \mathrm{ord}(\widehat{g}_s) + 1 = i_{n-1} - i_n + 1$$

and

$$\mathrm{ord}(h \circ f(T) - h(T)) = \mathrm{ord}(\widehat{g}_s \circ f^p(T) - \widehat{g}_s(T)) = i_{n-1}.$$

We thus obtain a contradiction with Lemma 3(3). This proves the theorem in the case where $n = 1$, and the induction step in the case where $n \geq 2$. Thus, the proof of the theorem is complete. □

2. A simplified version of Lubin's proof

We follow Lubin's strategy of lifting the power series to a field of characteristic zero, where $i_n - i_{n-1}$ can be interpreted as the cardinality of a certain set of periodic orbits of minimal period p^n, see [Lub95]. The main difficulty in this approach is to find a lift whose periodic points are simple. Lubin achieved this through an inductive perturbative procedure. We use that all the periodic points of a generic polynomial are simple.

Lemma 4. *Let K be an algebraically closed field of characteristic zero, let $d \geq 2$ be an integer, and let $a_0, \ldots, a_d$ be elements of K that are algebraically independent over the prime field of K. Then, all of the periodic points of the polynomial*

$$a_0 + a_1 z + \cdots + a_d z^d$$

in K are simple.

Proof. Suppose there were an integer n satisfying $n \geq 1$ and a periodic point z_0 of period n of P that is not simple, so that $(P^n)'(z_0)$ is a root of unity. Denote by $\mathbb{Q}$ the prime field of K, and let $\sigma\colon \mathbb{Q}[z_0, a_0, \ldots, a_d] \to \mathbb{C}$ be a ring homomorphism such that for every j in $\{0, \ldots, d-1\}$ we have $\sigma(a_j) = 0$ and such that $\sigma(a_d) = 1$. Then $\sigma(P)(z) = z^d$ and $\sigma(z_0)$ is a periodic point of period n of $\sigma(P)$, so $|\sigma(z_0)| = 1$ and

$$|\sigma((P^n)'(z_0))| = |(\sigma(P)^n)'(\sigma(z_0))| = |d^n \sigma(z_0)^{d^n - 1}| = d^n.$$

However, $|\sigma((P^n)'(z_0))| = 1$ because by hypothesis $(P^n)'(z_0)$ is a root of unity. This contradiction completes the proof of the lemma. □

Given an ultrametric filed K, denote by $\mathcal{O}_K$ its ring of integers, by $\mathfrak{m}_K$ the maximal ideal of $\mathcal{O}_K$, and by $\widetilde{K}$ the residue filed $\mathcal{O}_K/\mathfrak{m}_K$ of K. The *reduction* of a power series $f(z)$ in $\mathcal{O}_K[[z]]$ is the power series $\widetilde{f}(T)$ in $\widetilde{K}[[T]]$ obtained by taking the reduction of the coefficients of $f(z)$. The *Weierstrass degree* $\operatorname{wideg}(f)$ of $f(z)$ is defined by $\operatorname{wideg}(f) := \operatorname{ord}(\widetilde{f}(T))$. In the case where K is algebraically closed and $\operatorname{wideg}(f)$ is finite, $\operatorname{wideg}(f)$ is equal to the number of zeros of $f(z)$ in $\mathfrak{m}_K$ counted with multiplicity, see for example [Lan02, §VI, Theorem 9.2].

Second proof of Theorem 1. Let α in k be such that

$$f^{p^{n-1}}(T) \equiv T + \alpha T^{i_{n-1}} \mod T^{i_{n-1}+1}.$$

An induction argument shows that for every integer m satisyfing $m \geq 1$, we have

$$f^{mp^{n-1}}(T) \equiv T + m\alpha T^{i_{n-1}} \mod T^{i_{n-1}+1}.$$

Taking $m = p$, we obtain $f^{p^n}(T) \equiv T \mod T^{i_{n-1}+1}$ and therefore $i_n \geq i_{n-1} + 1$.

To prove the second assertion, we assume without loss of generality k is algebraically closed and therefore perfect. Then, there is an algebraically closed field K of characteristic zero that is complete with respect to a non-trivial ultrametric norm and such that its residue field $\widetilde{K}$ is isomorphic to k, see for example [Ser68, II, *Théorème* 3]. We identify k and $\widetilde{K}$. Then K is uncountable and therefore we can choose for each j in $\{1, \ldots, i_n\}$ an element a_j of $\mathcal{O}_K$ such that the $a_1, \ldots, a_{i_n+1}$ are algebraically independent over the prime field of K and such that the reduction $\widetilde{P}(T)$ of the polynomial

$$P(z) = a_1 z + \cdots + a_{i_n+1} z^{i_n+1}$$

in $\mathcal{O}_K[[z]]$ satisfies $\widetilde{P}(T) \equiv f(T) \mod T^{i_n+2}$. Then

$$\operatorname{wideg}\left(P^{p^{n-1}}(z) - z\right) = i_{n-1} + 1 \text{ and } \operatorname{wideg}\left(P^{p^n}(z) - z\right) = i_n + 1$$

and by Lemma 4 all the periodic points of P are simple. It follows that the set Z of all zeros of $P^{p^n}(z) - z$ in $\mathfrak{m}_K$ that are not zeros of $P^{p^{n-1}}(z) - z$, consists of all the periodic points of P in $\mathfrak{m}_K$ whose minimal period is p^n. Since $P(\mathfrak{m}_K) = \mathfrak{m}_K$, it follows that Z is a union of periodic orbits of minimal period p^n, so p^n divides $\#Z$. Since

$$\#Z = \operatorname{wideg}\left(P^{p^n}(z) - z\right) - \operatorname{wideg}\left(P^{p^{n-1}}(z) - z\right) = i_n - i_{n-1},$$

this proves that $i_n - i_{n-1}$ is divisible by p^n and completes the proof of the theorem. □

References

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[Li96] Hua-Chieh Li. p-adic periodic points and Sen's theorem. *J. Number Theory*, 56(2):309–318, 1996.

[LRL16] Karl-Olof Lindahl and Juan Rivera-Letelier. Optimal cycles in ultrametric dynamics and minimally ramified power series. *Compos. Math.*, 152(1):187–222, 2016.

[Lub95] Jonathan Lubin. Sen's theorem on iteration of power series. *Proc. Amer. Math. Soc.*, 123(1):63–66, 1995.

[Sen69] Shankar Sen. On automorphisms of local fields. *Ann. of Math. (2)*, 90:33–46, 1969.

[Ser68] Jean-Pierre Serre. *Corps locaux*. Hermann, Paris, 1968. Deuxième édition, Publications de l'Université de Nancago, No. VIII.

Department of Mathematics, University of Rochester. Hylan Building, Rochester, NY 14627, U.S.A.
Email address: riveraletelier@gmail.com
URL: http://rivera-letelier.org/