SENN’S THEOREM ON ITERATION OF POWER SERIES

JONATHAN LUBIN

(Communicated by Lance W. Small)

Abstract. In the group of continuous automorphisms of the field of Laurent series in one variable over a field of characteristic \( p > 0 \), Sen’s Theorem describes the rapidity of convergence to the identity of the sequence formed by taking successive \( p \)-th powers of a given element. This paper gives a short proof of Sen’s Theorem, utilizing the methods of \( p \)-adic analysis in characteristic zero.

The theorem in question appears in Sen’s thesis [Sen], and is concerned with the group \( \mathcal{G}_{0,1}(k) \) of formal power series in one variable with no constant term, and first degree coefficient equal to 1, over a field \( k \) of characteristic \( p > 0 \), where the group law is composition of series. If we call the variable \( t \), this group is a closed subset of the discrete valuation ring \( k[[t]] \), namely, the set of all \( u(t) \) for which \( u \equiv t \mod{t^2} \). For the \((t)\)-adic filtration of group \( \mathcal{G}_{0,1} \), the successive quotients are isomorphic to the additive group \( k \). Thus if we call \( u^{\circ n} \) the \( n \)-fold iteration of \( u \) with itself, any time that \( u \equiv t \mod{t^n} \), we necessarily have \( u^{\circ p} \equiv t \mod{t^{n+1}} \). Sen’s Theorem says much more and is best stated in terms of the additive valuation \( v \) of \( k[[t]] \) normalized so that \( v(t) = 1 \). According to the theorem, if \( u^{\circ p} \) is not the identity, then \( v(u^{\circ p}(t) - t) \equiv v(u^{\circ p-1}(t) - t) \mod{p^n} \). Let us abbreviate notation by setting \( i_u(n) := v(u^{\circ p}(t) - t) \). Sen’s Theorem now says that if \( u^{\circ p} \) is not the identity, then \( i(n) \equiv i(n-1) \mod{p^n} \).

As examples of this phenomenon, we have, in characteristic 2, if \( u(t) = t + t^4 \), then \( i_u(n) = 2^{2^n} \); if \( u(t) = t + t^4 + t^5 \), then \( i_u(n) = 2^{n+2} \); and if \( u(t) = t + t^3 \), then \( i_u(n) = 1 + 2^{n+1} \). It is easy to see why the first two of these facts hold, since each of \( t + t^4 \) and \( t + t^4 + t^5 \) is an endomorphism of a formal group, and since in a formal-group endomorphism ring, the multiplication comes from substitution of power series. The first-mentioned series is an endomorphism of the additive formal group \( \mathcal{A}(x, y) = x + y \), whose endomorphism ring has characteristic 2, and in that ring \( t + t^4 \) is \( g = 1 + \phi \), \( \phi(t) = t^4 \). The powers \( g^{2^n} \) are

\[
(1 + \phi^2)(t) = t + t^{4^2}.
\]

Received by the editors September 29, 1992 and, in revised form, April 19, 1993.

1991 Mathematics Subject Classification. Primary 12J25; Secondary 11R37, 54H20.
The second-mentioned series is the endomorphism \([S]_t(t)\) of the multiplicative formal group \(\mathcal{M}(x, y) = x + y + xy\), whose endomorphism ring is isomorphic to the ring \(\mathbb{Z}_2\) of 2-adic integers, and the iterates of \([S](t)\) approach \([1](t) = t\) in the manner claimed because of the congruences \(5^{2^n} \equiv 1 \pmod{2^{n+2}}\), \(5^{2^n} \neq 1 \pmod{2^{n+3}}\). To see why the 2-power iterates of the last-mentioned series \(t + t^3\) approach the identity in the manner claimed is rather more difficult, and for this the reader is referred to [K].

In this note we give a short proof of Sen’s Theorem using the methods of \(p\)-adic analysis.

Without loss of generality, we may assume that the field \(\kappa\) is perfect. The trick is to lift \(u\) in a particular way to a series \(U(x)\) in characteristic zero. (The choice of a complete discrete valuation ring \(\wp\) of characteristic zero to serve as constant ring for \(U\) is not crucial: the Witt ring \(W(\kappa)\) will do.) As usual in \(p\)-adic analysis, we pass from the original ground ring \(\wp\) to its integral closure \(\mathcal{D}\) in an algebraic closure of the fraction field \(k\) of \(\wp\). Of course, \(\mathcal{D}\) is neither Noetherian nor complete, but every series considered will have its coefficients in a finite algebraic extension of \(k\), in which the integer ring is complete and Noetherian. Call \(\mathfrak{m}\) the maximal ideal of \(\mathcal{D}\). The number \(i(n)\) defined above is now the “Weierstrass degree” of the series \(U^{op^n}(t) - t\), and \(i(n)\) is thus the number of fixed points in \(\mathfrak{m}\) of \(U^{op^n}\), taking account of multiplicity. The idea is to choose the series \(U\) so that each periodic point of order dividing \(p^n\) has multiplicity at most one in every iterate of \(U\). The existence of such a series will make a proof of Sen’s Theorem easy. The note closes with a construction of the series \(U\).

**Theorem.** Let \(\wp\) be a complete discrete valuation ring of characteristic zero, maximal ideal \(\mathfrak{m}\), and residue field \(\kappa\) of characteristic \(p > 0\). Let \(U(t)\) be a series in \(\wp[[t]]\) for which \(U(0) = 0\), and suppose that \(n\) is a positive integer such that \(U^{op^n}(t) \neq t \pmod{\mathfrak{m}}\) and all roots of \(U^{op^n}(t) - t\) in \(\mathfrak{m}\) are simple. Then for all \(m\) with \(0 < m \leq n\), \(i_U(m - 1) \equiv i_U(m) \pmod{p^m}\).

**Proof.** For each \(m \geq 1\) let \(Q_m(t)\) be defined by

\[
Q_m(t) = \frac{U^{op^m}(t) - t}{U^{op^{m-1}}(t) - t}.
\]

The quotient is a series in \(\wp[[t]]\) since for any series \(f \in \wp[[t]]\) with \(f(0) = 0\) we have \((f(t) - t)(f^{op^m}(t) - t)\). Put \(Q_0(t) = U(t) - t\). Our hypothesis on multiplicities says that no two of the series \(Q_0, Q_1, \ldots, Q_n\) have any roots in common. Thus the set of roots of \(Q_m\) in \(\mathfrak{m}\) is exactly the set of points of \(\mathfrak{m}\) that lie in an orbit of cardinality \(p^m\) under the action of \(U\). Since, for \(m \geq 1\), the Weierstrass degree of \(Q_m\) is \(i_U(m) - i_U(m - 1)\), the proof is done.

All the difficulty in Sen’s Theorem is pushed into the construction of a lifting of the given \(u(t) \in \kappa[[t]]\) to a series \(U(t) \in \wp[[t]]\) of the desired form.

**Proposition.** Let \(\kappa\) be a field of characteristic \(p > 0\), and let \(u\) be a series in \(\kappa[[t]]\) with \(u(t) \equiv t \pmod{t^2}\). If \(n\) is an integer such that \(U^{op^n}(t) \neq t\), then there is a complete discrete valuation ring \((\omega, \mathfrak{m})\) of characteristic zero, such that \(\omega/\mathfrak{m}\) contains \(\kappa\), and a lifting \(U\) of \(u\) to \(\omega[[t]]\), such that all the roots of \(U^{op^n}(t) - t\) in \(\mathfrak{m}\) are simple.
Proof. First we find any complete discrete valuation ring at all, \((\mathfrak{o}_0, \mathfrak{m}_0)\), whose residue field contains \(\kappa\) : the Witt ring of the perfect closure of \(\kappa\) will do. Lift \(u\) in any way to a series \(U_0 \in \mathfrak{o}_0[[t]]\) without constant term. Our strategy is to choose a ring \((\mathfrak{o}, \mathfrak{m})\) that is the integer ring of a finite algebraic extension of the fraction field of \(\mathfrak{o}_0\) and modify \(U_0\) by adding a carefully chosen \(\Delta \in p^N \mathfrak{o}[[t]]\) so that \(U = U_0 + \Delta\) satisfies the desired conditions. We make frequent use of the continuity of the roots of a series over \(\mathfrak{o}\), by which we mean that if \(\xi f(t) \in \mathfrak{o}[[\xi]][[t]]\) and if \(\rho \in \mathfrak{m}\) is a root of multiplicity \(\mu\) of \(o f\), then for all \(\alpha\) in a sufficiently high power of \(\mathfrak{m}\), there are precisely \(\mu\) roots of \(o f\), counting multiplicity, that correspond to \(\rho\). In particular, when \(f\) is varied slightly in a suitably small open set about \(o f\), the multiplicities of roots cannot increase.

We recall also that a fixed point \(\zeta\) of \(f(t)\) has multiplicity greater than 1 if and only if \(f'(\zeta) = 1\) and that \(\zeta\) will be a multiple root of \(f^{\circ r}(t) - t\) if and only if \(f'(\zeta)\) is an \(r\)th root of 1. The last tool used in the proof is the observation that if \(\Lambda \in \mathfrak{o}[[t]]\) is a series that vanishes at all roots of \(U_0^{\circ n}(x) - x\) and if \(U = U_0 + \Delta\), then every fixed point of \(U_0^{\circ n}\) is a fixed point of \(U^{\circ n}\). We will modify the original \(U_0\) in this way by increments that successively decrease the multiplicity of each fixed point of \(U^{\circ n}\) to 1. Note that our modified series has only finitely many periodic points of order dividing \(p^n\) since \(U^{\circ n}(t) \neq t\).

Now for the details: In case a fixed point \(\zeta\) of \(U\) itself is a fixed point of multiplicity greater than 1 in an iterate, we may assume (after perhaps making a finite extension of the base) that \(\zeta = 0\), so that \(U^{\circ p}(t) - t\) takes the form \(t^e G(t)\), with \(G(0) \neq 0\) and \(e > 1\). The hypothesis on \(U\) is that \(U'(0) = w\) is a root of 1, so we set \(\xi U(t) := U(t) + \xi t G(t)\), which, for small enough nonzero \(\xi\), has \(\xi U'(0) \neq w\), but so close to \(w\) that it cannot be a root of 1. Therefore, no iterate of the new series has a fixed point of multiplicity greater than 1 at 0.

A slightly more complicated situation is the one where \(\zeta\) is a periodic point of order \(p^r\), with \(1 \leq r \leq n\). Call \(\zeta_i := U^{\circ i}(\zeta)\), so that \(\zeta_i \neq \zeta\) if \(0 < i < p^r\). The hypothesis on \(\zeta\) implies that

\[
U^{\circ p^n}(t) - t = G(t) \prod_{i=0}^{p^r-1} (t - \zeta_i)^{e_i},
\]

where \(G\) is nonzero at all the \(\zeta_i\)'s and where \(e_0 > 1\). We now set \(\Delta(t) = \sum_{i \neq \zeta} (t - \zeta_i)^2\) and \(\xi U := U + \xi \Delta\). This has among its periodic points of order dividing \(p^n\) the corresponding periodic points of \(U\), and since the hypothesis on \(\zeta\) implies that \(U^{\circ p^i}(\zeta) = w\), a root of 1, we will be done when we show that we can adjust \(\xi\) so that \(\xi U^{\circ p^i}(\zeta)\) is so close to \(w\) that it cannot be a root of 1. We have

\[
\xi U^{\circ p^i}(\zeta) = \prod_{i=0}^{p^r-1} \xi U'(\xi U^{\circ i}(\zeta)) = \xi U'(\zeta) \prod_{i=1}^{p^r-1} \xi U'(\zeta_i) = (U'(\zeta) + \xi \Delta'(\zeta)) \prod_{i=1}^{p^r-1} U'(\zeta_i) = w + \xi \Delta'(\zeta) \prod_{i=1}^{p^r-1} U'(\zeta_i),
\]

and since we have constructed \(\Delta\) so that \(\Delta'(\zeta) \neq 0\), the proof is done.
References


Department of Mathematics, Brown University, Box 1917, Providence, Rhode Island 02912

E-mail address: ma406000@brownvm.brown.edu