COMPOSITION OF POWER SERIES

LAURENT BERGER AND SANDRA ROZENSZTAJN

The goal of this project is to study the composition of power series $f(X) = a_1X + a_2X^2 + \cdots$ with coefficients $\{a_i\}_{i\geq 1}$ in a field K such as $\mathbf{R}$ or $\mathbf{C}$ or $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$.

When $K = \mathbf{R}$ or $\mathbf{C}$, power series with coefficients in K occur as the Taylor series of infinitely differentiable functions. When K contains $\mathbf{F}_p$, those power series come from number theory. One theme of this project is therefore the interplay between analysis and arithmetic.

1. Composition of power series

Let K be a field and let $K[\![X]\!]$ denote the set of power series $f(X) = a_0 + a_1X + a_2X^2 + \cdots$ with coefficients $\{a_i\}_{i\geq 0}$ in K.

Let $K(\!(X)\!)$ denote the set of power series $f(X) = a_mX^m + a_{m+1}X^{m+1} + \cdots$ where $m \in \mathbf{Z}$ and with coefficients $\{a_i\}_{i\geq m}$ in K.

If $f(X) = \sum_{i=m}^{+\infty} a_iX^i \in K(\!(X)\!)$, let $\mathrm{val}_X(f)$ be the smallest $i \in \mathbf{Z}$ such that $a_i \neq 0$, so that $f(X) \in X^iK[\![X]\!]$ but $f(X) \notin X^{i+1}K[\![X]\!]$ (if $f = 0$, then $\mathrm{val}_X(0) = +\infty$). The integer $\mathrm{val}_X(f)$ is the *X-adic valuation* of f.

Exercise 1. *Prove that $K(\!(X)\!)$ is a field.*

Exercise 2. *Check that if $\{f_k\}_{k\geq 1}$ is a sequence of $K(\!(X)\!)$ such that $\mathrm{val}_X(f_k - f_{k+1}) \geq k$ for all $k \geq 1$, there exists $f \in K[\![X]\!]$ such that $\mathrm{val}_X(f - f_k) \geq k$ for all $k \geq 1$.*

In the sequel, this method of constructing power series by successive approximations will be a fundamental tool. In more fancy terms, $K(\!(X)\!)$ is *complete* for the X-adic topology.

Exercise 3. *Check that if $f(X) \in K(\!(X)\!)$ and $g(X) \in X \cdot K[\![X]\!]$, we can compose f and g, i.e. that the power series $f \circ g(X) = f(g(X))$ makes sense. Write down the first few coefficients of $f \circ g$ in terms of those of f and g when $f(X) \in K[\![X]\!]$.*

If $f \in X \cdot K[\![X]\!]$ and $n \geq 0$, let $f^{\circ n}$ be f composed with itself n times: $f^{\circ n} = f \circ \cdots \circ f$. If $f(X) = \sum_{i=m}^{+\infty} a_iX^i \in K(\!(X)\!)$, let $f'(X) = \sum_{i=m}^{+\infty} ia_iX^{i-1}$. In particular, if $f(X) = a_1X + a_2X^2 + \cdots$, then $f'(0) = a_1$.

Let $G(K)$ denote the set of power series $f(X) \in K[\![X]\!]$ such that $f(0) = 0$ and $f'(0) \neq 0$, i.e. $f(X) = a_1X + a_2X^2 + \cdots$ with $a_1 \neq 0$.

Exercise 4. *Prove that if $f(X) \in G(K)$, there exists a uniquely determined $g(X) \in G(K)$ such that $f(g(X)) = X$ and that then $g(f(X)) = X$. Write down the first few coefficients of g in terms of those of f.*

The power series g is the inverse of f for the composition and is denoted by $f^{\circ -1}$. If $f \in G(K)$, we therefore have at our disposal $f^{\circ n}$ for all $n \in \mathbf{Z}$.

The following exercise is not used in the sequel, but is one of the first important results concerning the composition of power series. It is due to Lagrange, around 1770. If $f(X) \in K(\!(X)\!)$ and $n \in \mathbf{Z}$, let $[X^n](f)$ denote the coefficient of X^n in $f(X)$.

Exercise 5 (Lagrange's inversion formula)**.** *Prove that if $f(X) \in G(\mathbf{C})$, then*

$$n \cdot [X^n](f^{\circ -1}) = [X^{-1}](\frac{1}{f^n}).$$

Prove that the same formula holds in any field K, not just $\mathbf{C}$.

2. The group $G(K)$

By the results of the previous section, the elements of $G(K)$ can be composed and have an inverse for the composition. Check that $(G(K), \circ)$ is a group, with X the identity element.

Exercise 6. *Let f be an element in $G(K)$. Show that the map $\pi_f : K(\!(X)\!) \to K(\!(X)\!)$, $u \mapsto u \circ f$ is a field automorphism, and that the map $\pi : (G(K), \circ) \to \mathrm{Aut}(K(\!(X)\!))$, $f \mapsto \pi_{f^{\circ -1}}$ is an injective group homomorphism. What is the image of π?*

If $f(X) = a_1 X + a_2 X^2 + \cdots$, let $i(f) = \mathrm{val}_X(f(X) - X) - 1$.

The number $i(f)$ is the *ramification number* of f, sometimes also called the *depth* of f. For example, $i(f) = 0$ if $a_1 \neq 1$, $i(X + X^k) = k - 1$ if $k \geq 2$, and $i(X) = +\infty$. Let $G_i(K)$ denote the set of $f \in G(K)$ such that $i(f) \geq i$, so that $G(K) = G_0(K)$.

Exercise 7. *Prove that if $f \in G_1(K)$, then $i(f^{\circ n}) = i(f)$ for $n \in \mathbf{Z}$ such that $n \neq 0$ in K.*

Exercise 8. *Prove that $i(f) = \mathrm{val}_X(g \circ f - g)$ for any $g \in G_1(K)$.*

Exercise 9. *Take i, r, $s \geq 1$.*

1. *Check that $G_i(K)$ is a subgroup of $G(K)$.*
2. *Prove that if $f(X) = X + a_{r+1}X^{r+1} + \cdots \in G_r(K)$ and $g(X) = X + b_{s+1}X^{s+1} + \cdots \in G_s(K)$, then $[f, g] = f^{\circ -1} \circ g^{\circ -1} \circ f \circ g(X) = X + (r - s)a_{r+1}b_{s+1}X^{r+s+1} + \cdots$.*
3. *Prove that $G_i(K)$ is a normal subgroup of $G(K)$, and that $[G_r(K), G_s(K)] \subset G_{r+s}(K)$.*
4. *If K is of characteristic p, can you compute $i([f, g])$?*

(5) *(more difficult) Is $G_i(K)$ a characteristic subgroup of $G(K)$, meaning that it is stable under* any *group automorphism of $G(K)$?*

If $f(X) = X + a_{i+1}X^{i+1} + \cdots \in G_1(K)$ with $a_{i+1} \neq 0$, let $\mathrm{coef}(f) = a_{i+1}$ denote the first nontrivial coefficient of f.

Exercise 10. *Prove that if f, $g \in G_1(K)$, then $i(g^{\circ -1} \circ f \circ g) = i(f)$ and $\mathrm{coef}(g^{\circ -1} \circ f \circ g) = \mathrm{coef}(f)$.*

The group $G(K)$ is studied for example in [Jen54]. Some of the above formulas are in §2 of [Klo00b] or in [Cam00].

3. The n-dispersal

For $k \geq 0$, consider the polynomial with coefficients in $\mathbf{Q}$

$$\binom{T}{k} = \frac{T(T-1)\cdots(T-(k-1))}{k!}.$$

If we plug in $T = n$ with $n \geq k$, we recover the usual binomial coefficients.

Exercise 11. *Let p be a prime number and take $a/b \in \mathbf{Q}$ with $p \nmid b$. Write $\binom{a/b}{k} = x/y$.*

(1) *Prove that $p \nmid y$.*
(2) *Use this to define $\binom{a/b}{k} \in \mathbf{F}_p$*

Let K be any field and take $c = a/b \in \mathbf{Q}$, with $p \nmid b$ if K is of characteristic p. Let $(1+X)^c$ denote the power series

$$(1+X)^c = \sum_{k=0}^{+\infty} \binom{c}{k} X^k.$$

Exercise 12. *Prove that $(1+X)^{c_1} \cdot (1+X)^{c_2} = (1+X)^{c_1+c_2}$ if c_1, c_2 are as above.*

If $h(X) \in 1 + X \cdot K[\![X]\!]$, let $h(X)^c = (1+X)^c \circ (h(X) - 1)$.

Exercise 13. *Take $n \geq 1$ such that $n \neq 0$ in K. If $f(X) \in G_1(K)$, write $f(X) = X \cdot h(X)$ with $h(X) \in 1 + X \cdot K[\![X]\!]$ and let $f_n(X) = X \cdot h(X^n)^{1/n}$. Prove that $(f \circ g)_n = f_n \circ g_n$.*

The map $f \mapsto f_n$ is therefore a group homomorphism from $(G_1(K), \circ)$ to itself, called the *n-dispersal*. What is the effect of the dispersal on $i(f)$?

Exercise 14. *Compute the kernel and the image of the n-dispersal map.*

4. Conjugacy of power series over $\mathbf{C}$

We first investigate the conjugacy of power series with coefficients in $\mathbf{C}$. If f, $g \in G(\mathbf{C})$, we say that f and g are *conjugate* and write $f \sim g$ to mean that there exists $h(X) \in G(K)$ such that $h^{\circ -1} \circ f \circ h = g$ (note: h is in $G(K)$ so $h'(0)$ can be any element of $\mathbf{C}^\times$).

Exercise 15. *Prove that if $f \in G(\mathbf{C})$ is such that $f'(0)^n \neq 1$ for every $n \geq 1$, then $f(X) \sim f'(0) \cdot X$.*

This allows you to compute the *centralizer* (aka the *commutant*) of such an f.

Exercise 16. *Prove that if $f \in G(\mathbf{C})$ is such that $f'(0)^n \neq 1$ for every $n \geq 1$, then for all $c \in K^\times$ there exists a unique $g \in G(\mathbf{C})$ such that $g'(0) = c$ and $g \circ f = f \circ g$.*

Exercise 17. *Prove that if $f \in G_1(\mathbf{C})$, $f \neq X$, there exists $c \in \mathbf{C}$ and $n \geq 1$ such that $f(X) \sim X + X^{n+1} + cX^{2n+1}$.*

Prove that if $X + X^{n+1} + cX^{2n+1} \sim X + X^{m+1} + dX^{2m+1}$, then $n = m$ and $c = d$.

Exercise 18. *Let $f \in G(\mathbf{C})$ be such that there exists $k \geq 2$ with $f^{\circ k}(X) = X$. Prove that $f'(0)^k = 1$ and that $f(X) \sim f'(0) \cdot X$.*

Exercise 19. *Finally, assume that $f'(0)$ is of order $k \geq 2$ in $\mathbf{C}^\times$, but that $f^{\circ k}(X) \neq X$. Prove that $f(X) \sim f'(0) \cdot X + 1/(kf'(0)) \cdot X^{n+1} + cX^{2n+1}$ for some $c \in \mathbf{C}$.*

Exercise 20. *For f as in Exercises 17, 18 and 19, can you compute the centralizer of f?*

In the above exercises, what properties of the field $\mathbf{C}$ did you use? Which conclusions still hold if K is of characteristic p? Most of the material in this section comes from §3 of [Sch70].

5. Sen's theorem

Let K be a field of characteristic p and take $f \in G_1(K)$. By Exercise 7, we have $i(f^{\circ n}) = i(f)$ if $p \nmid n$, so it makes sense to look at $i(f^{\circ p^n})$ only. Let $i_n(f) = i(f^{\circ p^n})$ for $n \geq 0$. The goal of this section is to prove the following theorem, which is due to Shankar Sen (see [Sen69]).

Theorem 1 (Sen)**.** *If $f \in G_1(K)$ and $n \geq 1$, then $i_n(f) \equiv i_{n-1}(f) \bmod p^n$.*

If $i_n(f) = +\infty$, we agree that the congruence holds.

Exercise 21. *Prove that if $i_n(f) \neq +\infty$, then $i_{n+1}(f) > i_n(f)$.*

Exercise 22. *Prove that if $i_n(f) \neq +\infty$, the following are equivalent:*

(1) *for all* $1 \leq j \leq n$, *we have* $i_j(f) \equiv i_{j-1}(f) \bmod p^j$;
(2) *the integers* $m + i(f^{\circ m})$ *are pairwise distinct, as* m *runs through the set of integers* ≥ 1 *not divisible by* p^{n+1}.

Prove that the integers in (2) above are also distinct from $i_n(f)$.

Take $g \in G_1(K)$. For $m \geq 1$, let $w_m = \prod_{i=0}^{m-1} g^{\circ i}(X)$. Let $w_0 = 1$ and for $m \leq -1$, let $w_m = 1/w_{-m} \in K(\!(X)\!)$.

Exercise 23. *Prove that* $\mathrm{val}_X(w_m) = m$ *and that* $\mathrm{val}_X(w_m \circ g - w_m) = m + i(g^{\circ m})$.

Exercise 24. *Prove that if* $g \in G_1(K)$ *and* $h \in K(\!(X)\!)$, *we can write* $h = \sum_{m \geq \mathrm{val}_X(h)} h_m$ *where for each* m, *either* $h_m = 0$ *or* $\mathrm{val}_X(h_m) = m$ *and* $\mathrm{val}_X(h_m \circ g - h_m) = m + i(g^{\circ m})$.

You can now prove Sen's theorem, by induction on n. Assume that for all $g \in G_1(K)$ and all $1 \leq j \leq n$, we have $i_j(g) \equiv i_{j-1}(g) \bmod p^j$. Take $f \in G_1(K)$ such that $i_n(f) \not\equiv i_{n+1}(f) \bmod p^{n+1}$. Applying the induction hypothesis to $g = f^{\circ p}$, we get $i_n(f) \equiv i_{n+1}(f) \bmod p^n$. Let $s = i_n(f) - i_{n+1}(f)$.

Exercise 25. *By applying Exercise 23 to* $g = f^p$ *and* $m = s$, *show that there is an element* $z \in K(\!(X)\!)$ *such that* $\mathrm{val}_X(z) = s$ *and* $\mathrm{val}_X(z \circ f^{\circ p} - z) = i_n(f)$.

Let $h = z \circ f^{\circ p-1} + z \circ f^{\circ p-2} + \cdots + z$ and let $y = h \circ f - h$.

Exercise 26. *Prove that* $\mathrm{val}_X(h) > s$ *and that* $\mathrm{val}_X(y) = i_n(f)$.

Write $h = \sum_{m \geq \mathrm{val}_X(h)} h_m$ as in Exercise 24 (with $g = f$) and let $y_m = h_m \circ f - h_m$ so that $y = \sum_{m \geq \mathrm{val}_X(h)} y_m$.

Exercise 27. *Prove that the integers* $\mathrm{val}_X(y_m)$ *with* $p^{n+1} \nmid m$ *are pairwise distinct and also distinct from* $i_n(f)$. *Prove that* $\mathrm{val}_X(y_m) > \mathrm{val}_X(y)$ *for all* m *divisible by* p^{n+1}.

Finish the proof of Sen's theorem.

6. Calculation of ramification numbers

In this section, K is a field of characteristic p. Sen's theorem gives us one property of the sequence $\{i_n(f)\}_{n \geq 0}$ of the ramification numbers of an $f \in G_1(K)$, but actually computing this sequence is quite difficult in general.

Exercise 28. *Let* H *be the set of power series* $\sum_{i \geq 0} a_i X^{p^i} \in \mathbf{F}_p[\![X]\!]$ *with* $a_0 = 1$. *Prove that* H *is a subgroup of* $G_1(\mathbf{F}_p)$ *and that the map* $H \to (1 + X \cdot \mathbf{F}_p[\![X]\!], \times)$ *given by* $\sum_{i \geq 0} a_i X^{p^i} \mapsto \sum_{i \geq 0} a_i X^i$ *is a group homomorphism.*

Prove that if $f(X) \in H$ *and* $i(f) = p^k - 1$, *then* $i_n(f) = p^{kp^n} - 1$ *for* $n \geq 1$.

Exercise 29. *If $a \in \mathbf{Z}_{\geq 1}$, let $f_a(X) = (1+X)^a - 1$. Compute $i_n(f_{1+p})$ for $n \geq 1$ and $p \neq 2$.*

The following is a direct corollary of Sen's theorem.

Exercise 30. *Prove that if $f \in G_1(K)$ and $n \geq 0$, then $i_n(f) \geq 1 + p + \cdots + p^n$.*

If $p \neq 2$, a power series $f \in G_1(K)$ such that $i_n(f) = 1 + p + \cdots + p^n$ for all $n \geq 0$ is called *minimally ramified*. If $p \neq 2$, there exists such a power series, but proving this is not so easy. Can you find one?

The power series f_{1+p} of Exercise 29 is not minimally ramified, but can be transformed into one. Recall that if $k \geq 0$, there is a uniquely determined polynomial, the kth Chebyshev polynomial $T_k(X) \in \mathbf{Z}[X]$, such that $T_k(\cos(\theta)) = \cos(k\theta)$. Let $P_k(X) = 2(1 - T_k(1 - X/2))$ and let $Y(X) = -X^2/(1+X)$.

Exercise 31. *Take $p \neq 2$. Prove that $P_k(Y(X)) = Y(f_k(X))$, that $P_k \in G_1(\mathbf{F}_p)$ if $k \equiv 1 \bmod p$ and that in this case $i_n(P_k) = i_n(f_k)/2$.*

Prove that if $p = 3$, $P_4(X) \in G_1(\mathbf{F}_3)$ is minimally ramified.

This can be generalized to all $p \neq 2$, but is more difficult.

Exercise 32 (more difficult)**.** *Find a way to define $f_\omega(X) \in \mathbf{F}_p[\![X]\!]$ for all ω such that $\omega^{p-1} = 1$ (this can be done using p-adic numbers, for example). Let $Y = \prod_{\omega^{p-1}=1} f_\omega(X)$. Prove that for all $k \equiv 1 \bmod p$, there exists a power series $g_k(X)$ such that $g_k \circ Y = Y \circ f_k$, and that then $i(g_k) = i(f_k)/(p-1)$. This shows that g_{1+p} is minimally ramified.*

In another direction, the main result of [Kea92] says that if $i_0(f) = 1$ and $i_1(f) = 1 + bp$ with $1 \leq b \leq p-2$, then $i_n(f) = 1 + bp + \cdots + bp^n$ for all $n \geq 1$.

Exercise 33. *Take $p \neq 2$. Using Keating's theorem, prove that $X + X^2 + aX^3 \in \mathbf{F}_p[\![X]\!]$ is minimally ramified if $a \neq 1$. Can you prove this directly?*

The power series g_k are called the *condensation* of the f_k. Minimally ramified power series are defined and studied in [LMS02]. The case $p = 2$ is a bit different from the rest.

7. Klopsch's theorem

In Exercise 18, you classified the elements $f \in G(\mathbf{C})$ of order n up to conjugacy, for $n \geq 1$.

Exercise 34. *Check that the same conclusion holds if K is of characteristic p and $p \nmid n$.*

You will now classify the elements $f \in G_1(K)$ of order p, up to conjugacy under $G_1(K)$, when K is of characteristic p.

Exercise 35. *Let $f \in G(K)$ be an element of order p. Show that $f \in G_1(K)$.*

Conversely, show that if $f \in G_1(K)$ is of finite order n, then n is a power of p.

Take $\lambda \in K$ and $n \geq 1$ such that $p \nmid n$. Let

$$F(n, \lambda) = \frac{X}{(1 - n\lambda X^n)^{1/n}}.$$

Exercise 36. *Compute $F(n, \lambda) \circ F(n, \mu)$, and deduce that $F(n, \lambda)^{\circ p} = X$.*

Exercise 37. *Show that if $(n, \lambda) \neq (n', \lambda')$ and λ, λ' are not both zero, then $F(n, \lambda)$ and $F(n', \lambda')$ are not conjugate in $G_1(K)$.*

Theorem 2 (Klopsch)**.** *If $f \in G_1(K)$ is such that $f^{\circ p} = X$, there exists $m \geq 1$ with $p \nmid m$, and $\lambda \in K$ and $g \in G_1(K)$ such that $g \circ f \circ g^{\circ -1} = F(m, \lambda)$.*

From Exercise 37 above, we see that if f is of order p, then m and λ are uniquely determined. Klopsch gives two proofs of his theorem in [Klo00a], one which uses only computations with power series, and one which uses a bit of Galois theory. The proof given here is an adaptation of the second one, along the lines of [BCPS15]. Recall first Artin's lemma (see for instance theorem 1.8 in VI §1 of [Lan02]).

Exercise 38. *If F is a field and if G is a finite group of automorphisms of F, then F is a finite extension of F^G which is Galois with Galois group G.*

Take $F = K(\!(X)\!)$. If $f \in G_1(K)$, then f defines an automorphism π_f of F as in Exercise 6. Let G be the group of automorphisms of F generated by π_f for an element f of order p, so that $G \simeq \mathbf{Z}/p\mathbf{Z}$. Let $M = F^G$. If F and G are as above and $x \in F$, let $\mathrm{Tr}(x) = \sum_{g \in G} g(x)$ be its trace.

Exercise 39. *Show that there exists $\theta \in F$ such that $\mathrm{Tr}(\theta) = 1$.*

Hint: this is true in any Galois extension, but in case $G = \mathbf{Z}/p\mathbf{Z}$, there is a simple proof. Take any $y \in F$ not in M, and assume that $\mathrm{Tr}(y) = \mathrm{Tr}(y^2) = \cdots = \mathrm{Tr}(y^{p-1}) = 0$. Prove that the minimal polynomial of y over M is then of the form $X^p - a = 0$, and that this contradicts the fact that F/M is Galois.

Exercise 40. *Show that M contains an element Y with $\mathrm{val}_X(Y) = p$.*

Exercise 41. *Let $\alpha_0 = \pi_f(\theta) + 2\pi_f^2(\theta) + \cdots + (p-1)\pi_f^{p-1}(\theta) \in F$.*

(1) *Compute $\pi_f(\alpha_0) - \alpha_0$*

(2) *Show that $\mathrm{val}_X(\alpha_0) < 0$.*

(3) *Show that* $\alpha_0^p - \alpha_0 \in M$ *and that* $F = M(\alpha_0)$.
(4) *Show that we can find some* $z \in M$ *such that* $\alpha = \alpha_0 + z$ *satisfies* $p \nmid \mathrm{val}_X(\alpha)$ *and* $\mathrm{val}_X(\alpha) < 0$.

Let $m = -\mathrm{val}_X(\alpha)$ so that $m \geq 1$ and $p \nmid m$. Let α_{-m} be the coefficient of X^{-m} in α.

Exercise 42. *Let* $\beta = (\alpha/\alpha_{-m})^{-1/m}$. *By considering the action of* π_f *on* α, *show that we have* $\beta \circ f \circ \beta^{\circ -1} = F(m, \lambda)$ *with* $\lambda = 1/(m\alpha_{-m})$.

This finishes the proof of Klopsch's theorem. We can show a little more about M.

Exercise 43. *Show that any nonzero element* $z \in M$ *satisfies* $p \mid \mathrm{val}_X(z)$. *Deduce from this that* $M = K(\!(Y)\!)$, *where* Y *is the element defined in Exercise 40.*

Exercise 44. *Suppose that* f_1 *and* f_2 *are two elements of order* p, *giving rise to two fields* M_1 *and* M_2 *as above, with* α_1 *and* α_2 *such that* $F = M_i(\alpha_i)$. *Assume that* $m_1 = m_2$ *and* $\alpha_{1,-m} = \alpha_{2,-m}$ *where* $m = m_i$, *and let* $\beta_i = (\alpha_i/\alpha_{i,-m})^{-1/m}$ *and* $\beta = \beta_1^{\circ -1} \circ \beta_2$.
Prove that the map $u \mapsto u \circ \beta$ *from* F *to* F *sends* M_1 *to* M_2, *and that* $G_2 = \beta^{\circ -1} \circ G_1 \circ \beta$.

Can you redo Exercise 34 using the Galois theoretic approach of this section?
We finish with an example of an element of order 4 in $G_1(\mathbf{F}_2)$ (see [CS10]).

Exercise 45. *Let* $f(X) = X + X^2 + \sum_{j=0}^{+\infty} \sum_{\ell=0}^{2^j-1} X^{6\cdot 2^j + 2\ell} \in \mathbf{F}_2[\![X]\!]$. *Prove that*

$$f(X) = \frac{X}{1+X} + \frac{g(X)}{(1+X)^2},$$

where $g(X) = \sum_{i=0}^{+\infty} (X^3 + X^4)^{2^i}$ *so that* $g(X)^2 - g(X) = X^3 + X^4$, *and then that* f *is of order* 4 *in* $G_1(\mathbf{F}_2)$.

Finding explicit elements of $G_1(\mathbf{F}_p)$ of order p^n with $n > 1$ seems to be a hard problem.

8. Suggestions for further study

There are a number of questions about the goup $G_1(K)$ that you can think about.

(1) The group $G_1(\mathbf{F}_p)$ is known as the *wild group* and also as the *Nottingham group* (other more exotic names are proposed in [dSF00]). It has many interesting properties, see for instance [Cam00]. For example, a theorem of Rachel Camina states that every finite group with p^n elements can be realized as a subgroup of $G_1(\mathbf{F}_p)$. Another property of $G_1(\mathbf{F}_p)$ is that it is infinite but any proper quotient of it is a finite group.

(2) Klopsch's theorem is generalized to elements of order p^n in [Jea09] and [Lub11] (see also [BCPS15]), but the constructions use a lot of number theory. In general, realizing finite groups with p^n elements (*p-groups*) as subgroups of $G_1(\mathbf{F}_p)$ can be done using Galois theory, see for instance [Cam97]. Finding *explicit* power series giving these realizations is quite another matter! Can you find an element of order 9 in $G_1(\mathbf{F}_3)$?

(3) Suppose that K is of characteristic p. For which sequences $\{i_n\}_{n\geq 0}$ does there exist a power series $f \in G_1(K)$ such that $i_n(f) = i_n$ for all $n \geq 0$? This question is answered in [LS98], but as in §7, this involves viewing the subgroups of $G_1(K)$ as the Galois groups of certain field extensions, and using a lot of *ramification theory*. Can you find a more hands-on proof, for certain sequences at least? Likewise, can you prove Keating's theorem (from Exercise 33) using only computations with power series?

(4) Suppose that K is of characteristic p and take f, $g \in G_1(K)$. If f and g are conjugate by an element of $G_1(K)$, then $i_n(f) = i_n(g)$ for all $n \geq 0$ and $\mathrm{coef}(f^{\circ p^n}) = \mathrm{coef}(g^{\circ p^n})$ for all $n \geq 0$. Are those two conditions on two power series f and g sufficient for f and g to be conjugate? Klopsch's theorem implies that the answer is yes if $i_n(f) = i_n(g) = +\infty$ for $n \geq 1$. If f, $g \in G_1(\mathbf{F}_p)$ are minimally ramified, one is conjugate to a power of the other in $G_1(K)$ where K is an extension of $\mathbf{F}_p$, see Prop 4.6 of [LMS02]. Once again, the proof uses advanced number theory. Can you find a proof that uses only computations with power series? Some slightly more ramified series are studied in [Fra16]. The general question of conjugacy seems to be open and a nice problem to work on!

(5) In §4, you proved that power series in $G(\mathbf{C})$ could be conjugated to have a special form, called a *normal form*. Is the same true in $G(K)$ when K is of characteristic p? Is the following assertion true for at least some f in $G(K)$: there exists $k_0 = k_0(f)$ such that if $k \geq k_0$ and $\mathrm{val}_X(f - g) \geq k$, then f and g are conjugate? In other words, is any power series that looks sufficiently like f conjugate to f? In classical analysis, this would be known as an instance of a *sufficient jet*.

(6) In [Lub94], Lubin considers power series with coefficients in the p-adic integers, and asks a question about when two such power series can commute for the composition. This question is still not answered, although a number of subcases have been treated. Lubin's paper is very well written.

References

[BCPS15] Frauke Maria Bleher, Ted Chinburg, Bjorn Poonen, and Peter Symonds, *Automorphisms of Harbater-Katz-Gabber curves*, arxiv:1509.02139, 2015.

[Cam97] Rachel Camina, *Subgroups of the Nottingham group*, J. Algebra **196** (1997), no. 1, 101–113.

[Cam00] ———, *The Nottingham group*, New horizons in pro-p groups, Progr. Math., vol. 184, Birkhäuser Boston, Boston, MA, 2000, pp. 205–221.

[CS10] Ted Chinburg and Peter Symonds, *An element of order* 4 *in the Nottingham group at the prime* 2, arXiv:1009.5135, 2010.

[dSF00] Marcus du Sautoy and Ivan Fesenko, *Where the wild things are: ramification groups and the Nottingham group*, New horizons in pro-p groups, Progr. Math., vol. 184, Birkhäuser Boston, Boston, MA, 2000, pp. 287–328.

[Fra16] Jonas Fransson, *Complete classification of* 2*-ramified power series*, arxiv:1601.03622, 2016.

[Jea09] Sandrine Jean, *Conjugacy classes of series in positive characteristic and Witt vectors*, J. Théor. Nombres Bordeaux **21** (2009), no. 2, 263–284.

[Jen54] Stephen Arthur Jennings, *Substitution groups of formal power series*, Canadian J. Math. **6** (1954), 325–340.

[Kea92] Kevin Keating, *Automorphisms and extensions of* $k((t))$, J. Number Theory **41** (1992), no. 3, 314–321.

[Klo00a] Benjamin Klopsch, *Automorphisms of the Nottingham group*, J. Algebra **223** (2000), no. 1, 37–56.

[Klo00b] ———, *Normal subgroups in substitution groups of formal power series*, J. Algebra **228** (2000), no. 1, 91–106.

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

[LMS02] François Laubie, Abbas Movahhedi, and Alain Salinier, *Systèmes dynamiques non archimédiens et corps des normes*, Compositio Math. **132** (2002), no. 1, 57–98.

[LS98] François Laubie and Mustapha Saïne, *Ramification of some automorphisms of local fields*, J. Number Theory **72** (1998), no. 2, 174–182.

[Lub94] Jonathan Lubin, *Non-Archimedean dynamical systems*, Compositio Math. **94** (1994), no. 3, 321–346.

[Lub11] ———, *Torsion in the Nottingham group*, Bull. Lond. Math. Soc. **43** (2011), no. 3, 547–560.

[Sch70] Stephen Scheinberg, *Power series in one variable*, J. Math. Anal. Appl. **31** (1970), 321–333.

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

[Yor90] Iain O. York, *The group of formal power series under substitution*, Ph.D. thesis, University of Nottingham, 1990.

Laurent Berger, ÉNS de Lyon, Lyon, France
E-mail address: laurent.berger@ens-lyon.fr
URL: perso.ens-lyon.fr/laurent.berger/

Sandra Rozensztajn, ÉNS de Lyon, Lyon, France
E-mail address: sandra.rozensztajn@ens-lyon.fr
URL: perso.ens-lyon.fr/sandra.rozensztajn/