Coleman integrals and the Chabauty-Coleman method

Davide Lombardo

1 Introduction

- We work over number fields K
- A **curve** C/K is a smooth projective algebraic variety over K of dimension 1. Its **genus** is the dimension of $H^0(C, \Omega^1_C)$
- We are interested in the set $C(K)$. There is a well-known trichotomy:
  1. if C has genus 0, then $C(K)$ is either empty or infinite. In the latter case there is an isomorphism $C \cong \mathbb{P}^1_K$.
  2. if C has genus 1, then $C(K)$ is either empty or is a finitely generated abelian group (Mordell-Weil theorem for elliptic curves).
  3. if C has genus at least 2, then $C(K)$ is finite (Faltings, Vojta, Bombieri)
- Given C/K, there is a K-algebraic variety (in fact, an abelian variety) $J := \mathrm{Jac}(C)$, given by the identity component of the Picard scheme of C, that is a moduli space for degree-0 line bundles on C (i.e. degree 0 divisors modulo linear equivalence). By the general Mordell-Weil theorem, $J(K)$ is again a finitely generated abelian group.
- If P is any rational point on C, then the map

$$\begin{array}{ccc} C(K) & \to & J(K) \\ Q & \mapsto & [Q - P] \end{array}$$

  is an embedding.
- An elliptic curve is canonically isomorphic to its own Jacobian via the embedding $Q \mapsto [Q - O]$, where O is the origin of the group law.
- The purpose of this note is to
  1. Define the Coleman integral, both for Jacobians and for affinoid (rigid) spaces;
  2. Prove the Chabauty-Coleman theorem:

     Theorem 1.1. *Let C/K be a curve of genus g. Suppose that the rank r of $J(K)$ is strictly smaller than g: then $C(K)$ is finite.*

2 Integrating on Jacobians

In the previous set-up (C a curve over a number field K with Jacobian J), let $\mathfrak{p}$ be a place of K. The purpose of this section is to construct an integration map

$$\begin{array}{ccc} H^0(J,\Omega^1_J)\times J(K_\mathfrak{p}) & \to & K_\mathfrak{p} \\ (\omega,P) & \mapsto & \int^P \omega \end{array}$$

that satisfies:

1. $K_\mathfrak{p}$-linearity in ω;
2. additivity in P: $\int^{P+Q}\omega = \int^P \omega + \int^Q \omega$
3. non-degeneracy modulo torsion: $\int^P \omega = 0$ for all $\omega \in H^0(J,\Omega^1_J)$ if and only if P is torsion.

Remark 2.1. In fact, the construction goes through for any abelian variety over a p-adic field.

Lemma 2.2. *Let* $\mathrm{Cot}(J)$ *be the cotangent space to* J *at the origin. The evaluation map*

$$ev: \begin{array}{ccc} H^0(J,\Omega^1_J) & \to & \mathrm{Cot}(J) \\ \omega & \mapsto & \omega(0) \end{array}$$

is an isomorphism.

Proof. The map $P \mapsto \tau_P^*\omega$ (from J to $\mathrm{Cot}(J)$) is algebraic. Since J is complete and $\mathrm{Cot}(J)$ is affine, it must be constant. This proves that any differential form is translation invariant, so ev is injective. It is also surjective, for example because the two spaces have the same dimension, or because any differential form in 0 can be extended to a translation-invariant differential form. □

Lemma 2.3. *For any* $\omega \in H^0(J,\Omega^1_J)$ *there exists a unique analytic map* $\lambda_\omega : J(K_\mathfrak{p}) \to K_\mathfrak{p}$ *such that* $d\lambda_\omega = \omega$, $\lambda_\omega(0) = 0$, *and* $\lambda : J(K_\mathfrak{p}) \to K_\mathfrak{p}$ *is a homomorphism.*

Proof. Write $\omega(0) = \sum F_i dz_i$ for some $F_i \in K_\mathfrak{p}[[z_1,\dots,z_g]]$. By an obvious analogue to the Poincaré lemma, there exists $G \in K_\mathfrak{p}[[z_1,\dots,z_g]]$ such that $dG = \omega$, and G converges on some open ball B. Without loss of generality[1], we can assume that B is an (open) subgroup of $J(K_\mathfrak{p})$. By compactness, $(J(K_\mathfrak{p}) : B) =: N$ is finite[2], and we can set

$$\lambda_\omega(P) = \frac{1}{N} G(NP).$$

[1] a theorem of Mattuck [Mat55] says that $J(K_\mathfrak{p})$ is isomorphic (as a topological group) to $\mathcal{O}_{K_\mathfrak{p}}^g \times T$ with T finite. In particular, the images in $J(K_\mathfrak{p})$ of the sets $(\mathfrak{p}^j\mathcal{O}_{K_\mathfrak{p}})^g$ form a basis of neghbourhood around 0 consisting of open subgroups.

[2] this number should be thought of as a large power of p; however, due to the possible presence of torsion, it is not true in general that N is exactly a power of p.

One checks that $d\lambda_\omega = \omega$: this is clear on B, and by translation-invariance it is then true on all of J.[3]

To show that λ_ω is a homomorphism, notice that (at least when restricted to B) the map $\int_a^b \omega := \lambda_\omega(b) - \lambda_\omega(a)$ has all the formal properties of integration (by definition), hence for $a, b \in B$ such that $a + b \in B$ (which is automatic, because B is a subgroup) we have

$$\begin{aligned}\lambda_\omega(a+b) &= \int_0^{a+b} \omega = \int_0^a \omega + \int_a^{a+b} \omega \\ &= \int_0^a \omega + \int_0^b \tau_a^* \omega = \lambda_\omega(a) + \lambda_\omega(b).\end{aligned}$$

This easily implies that λ_ω is a homomorphism.

Finally, uniqueness follows from local uniqueness at zero combined with the requirement that λ_ω be a homomorphism. □

Definition 2.4. *We set* $\int^P \omega = \lambda_\omega(P)$.

Proposition 2.5. *This definition satisfies conditions (1)-(3) in the definition of the Coleman integral.*

Proof. 1. Let ω_1, ω_2 be two elements of $H^0(J, \Omega^1_J)$ and $\lambda_{\omega_1}, \lambda_{\omega_2}$ be the two associated homomorphisms. Set $\lambda := \lambda_{\omega_1} + \lambda_{\omega_2}$: we want to prove that $\lambda = \lambda_{\omega_1+\omega_2}$. This follows by uniqueness of $\lambda_{\omega_1+\omega_2}$ and linearity of d, since $\lambda(0) = 0$, $d\lambda = d(\lambda_{\omega_1} + \lambda_{\omega_2}) = \omega_1 + \omega_2$, and λ is a homomorphism.

2. Direct consequence of the previous lemma.

[3] let me do the exercise. The differential of $\frac{1}{N}G(Nx)$ at a point p is $\frac{1}{N}[N]^*\left((dG)(Np)\right)$, where $[N]^* : (T_{Np}J)^\vee \to T_p(J)^\vee$ is the pull-back via the multiplication-by-N map. Now $(dG)(Np) = \omega(Np)$ since $dG = \omega$ on B and $Np \in B$, and $\omega(Np) = \tau^*_{-Np}(\omega(0))$ by translation-invariance, therefore

$$d\left(\frac{1}{N}G(Nx)\right)(p) = \frac{1}{N}[N]^*\tau^*_{-Np}(\omega(0));$$

moreover, $[N]^* \circ (\tau_{-Np})^* = (\tau_{-Np} \circ [N])^* = ([N] \circ \tau_{-p})^* = \tau^*_{-p} \circ [N]^*$. Since $[N]^*$ is $N \cdot \mathrm{Id}$, we obtain

$$d\left(\frac{1}{N}G(Nx)\right)(p) = \frac{1}{N}[N]^*\tau^*_{-Np}(\omega(0)) = \frac{1}{N}\tau^*_{-p} \circ [N]^*\omega(0) = \frac{1}{N}\tau^*_{-p}(N\omega(0)) = \tau^*_{-p}\omega(0) = \omega(p),$$

where in the last step we have again used the translation-invariance of ω. Finally, to see that $[N]^*$ is $N \cdot \mathrm{Id}$, one proceeds by induction: for $N = 1$ it is clear, and to pass from N to $N + 1$ we can consider

$$J \xrightarrow{\Delta} J \times J \xrightarrow{(N,1)} J \times J \xrightarrow{+} J.$$

This reduces the problem to checking that the differential of the sum is indeed the sum, and this is true by linearity, because $J \xrightarrow{(id,0)} J \times J \xrightarrow{+} J$ and $J \xrightarrow{(0,id)} J \times J \xrightarrow{+} J$ are both the identity on the tangent space.

3. We have $\int^P \omega = 0$ for all ω if and only if $\lambda_\omega(P) = 0$ for all ω. Denote by $\operatorname{Tan} J$ the tangent space at the origin to $J(K_\mathfrak{p})$ and consider the map

$$\begin{array}{rccc} \iota: & J(K_\mathfrak{p}) & \to & \operatorname{Tan}(J) \\ & x & \mapsto & (\omega \mapsto \lambda_\omega(x)). \end{array}$$

We claim that this is a locally injective homomorphism. Linearity is clear, and local injectivity follows from the fact that the differential at 0 of this map is the identity (indeed $d\lambda_\omega|_0 = \omega$). In particular, $\ker \iota$ is finite, and hence a subgroup of the group of torsion points. On the other hand $\operatorname{Tan}(J)$ is torsion-free, so $\operatorname{Tors} J(K_\mathfrak{p})$ is sent to 0 by ι. This proves that ι induces an injective map

$$J(K_\mathfrak{p})/\operatorname{Tors} J(K_\mathfrak{p}) \hookrightarrow \operatorname{Tan}(J)$$

or equivalently a pairing

$$J(K_\mathfrak{p})/\operatorname{Tors} J(K_\mathfrak{p}) \times \operatorname{Tan}(J)^\vee \to K_\mathfrak{p}$$

which is non-degenerate on the left. Since we have a canonical identification of $\operatorname{Tan}(J)^\vee$ with $H^0\left(J(K_\mathfrak{p}), \Omega^1_J\right)$ we are done.

□

3 Chabauty-Coleman

We are ready to prove Theorem 1.1:

Proof. If $C(K)$ is empty there is nothing to prove, so assume that $C(K) \neq \emptyset$ and pick $P \in C(K)$. This allows us to embed $C(K)$ in $J(K)$ via $Q \mapsto [Q - P]$.

Let $P_1, \ldots, P_r \in J(K)$ generate a subgroup of rank equal to $r = \operatorname{rank} J(K)$ (in other words, $N := (J(K) : \langle P_1, \ldots, P_r \rangle) < \infty$). Consider the $K_\mathfrak{p}$-linear subspace R of $H^0(J, \Omega^1_J)$ given by

$$R = \{\omega \in H^0(J, \Omega^1_J) : \int^{P_i} \omega = 0 \quad \forall i = 1, \ldots, r\}.$$

Since $H^0(J, \Omega^1_J)$ is a g-dimensional vector space and $\int^{P_i} : H^0(J, \Omega^1_J) \to K_\mathfrak{p}$ is a linear map, R is the intersection of r codimension-1 subspaces and therefore has dimension $\geq g - r > 0$. Pick $\omega \in R \setminus \{0\}$ and let Q be a point of $C(K)$. By definition of N we have $N[Q - P] \in \langle P_1, \ldots, P_r \rangle$, so we obtain $N[Q - P] = \sum n_i P_i$ for certain $n_i \in \mathbb{Z}$. In particular,

$$N \int^{[Q-P]} \omega = \int^{N[Q-P]} \omega = \int^{\sum n_i P_i} \omega = \sum n_i \int^{P_i} \omega = \sum n_i \cdot 0 = 0,$$

so that in particular $\int^{[Q-P]} \omega = 0$. By our construction of the Coleman integral, this means that there is a nonzero analytic function $\lambda_\omega : J(K_\mathfrak{p}) \to K_\mathfrak{p}$ that vanishes on $[Q - P]$, and

this for every $[Q-P]$ that belongs to $C(K)$ (seen as a subvariety of $J(K_\mathfrak{p})$). By restriction, we obtain an analytic function

$$\lambda_\omega : C(K_\mathfrak{p}) \to K_\mathfrak{p}$$

that vanishes on $C(K)$. This function is nonzero since $d\lambda_\omega = \omega$ is nonzero on C (recall that there is a natural bijection between the differential forms on C and on J). Since the zeroes of analytic function on a curve are isolated and the curve is compact, there can only be finitely many of them as desired. □

4 Strassman's theorem; quantitative bounds on the number of rational points

In this section we prove Strassman's theorem on the number of zeroes of an analytic function and use it to establish the following more precise version of the Chabauty-Coleman theorem:

Theorem 4.1. *(Quantitative Chabauty-Coleman) Let $C/\mathbb{Q}$ be a nice (=smooth projective) curve and $p \geq 3$ be a prime at which C has good reduction. If* $\operatorname{rank} J(K) < g(C)$ *we have*

$$\#C(\mathbb{Q}) \leq \#C(\mathbb{F}_p) + 2g - 2 + \left\lfloor \frac{2g-2}{p-2} \right\rfloor.$$

Example 4.2. *Consider the curve (or rather, the unique smooth projective curve birational to the curve given by the affine model)*

$$C : y^2 = x(x-1)(x-2)(x-5)(x-6)$$

over $\mathbb{Q}$. One can show that $\operatorname{rank} J(\mathbb{Q})$ *is 1, and that 7 is a prime of good reduction for C. Furthermore, $C(\mathbb{Q})$ contains at least 10 points, namely*

$$\infty, (0,0), (1,0), (2,0), (5,0), (6,0), (3, \pm 6), (10, \pm 120).$$

On the other hand we have $\#C(\mathbb{F}_7) = 8$, so by the quantitative version of Chabauty-Coleman we obtain

$$\#C(\mathbb{Q}) \leq 8 + 2(2-1) + 0 = 10.$$

Since we already found ten points this is actually an equality, and we have determined the set $C(\mathbb{Q})$.

Proof. (of Theorem 4.1) The idea is to count rational points according to their reduction modulo p. We have

$$\#C(\mathbb{Q}) = \sum_{\overline{P} \in C(\mathbb{F}_p)} \#\{P \in C(\mathbb{Q}) : P \equiv \overline{P} \pmod{p}\}. \tag{1}$$

The good reduction assumption implies that J also has good reduction at p; this means that there exists an abelian variety $\mathcal{J}$ over $\mathbb{Z}_p$ whose generic fiber is J, and also implies that

the space of $\mathbb{Z}_p$-regular differentials $H^0(\mathcal{J}, \Omega^1_{\mathcal{J}})$ is a lattice inside $H^0(J, \Omega^1_J)$ (see Section 2.1 of [McC94]). Finally, the special fiber $\mathcal{J}_{\mathbb{F}_p}$ of $\mathcal{J}$ is the Jacobian of the curve $C/\mathbb{F}_p$.

Let ω be the differential form constructed during the proof of theorem 1.1. Up to scaling by a power of p, we can assume that ω is in $H^0(\mathcal{J}, \Omega^1_{\mathcal{J}})$ and does not reduce to 0 in $H^0(\mathcal{J}_{\mathbb{F}_p}, \Omega^1_{\mathcal{J}_{\mathbb{F}_p}})$. Denote by $\overline{\omega}$ the reduction of ω in $H^0(\mathcal{J}_{\mathbb{F}_p}, \Omega^1_{\mathcal{J}_{\mathbb{F}_p}})$, and by $v_{\overline{P}}(\overline{\omega})$ the valuation (=order of vanishing) of $\overline{\omega}$) at $\overline{P}$.

We shall show that every term in the sum (1) is bounded by $1 + v_{\overline{P}}(\overline{\omega}) + \lfloor \frac{v_{\overline{P}}(\overline{\omega})}{p-2} \rfloor$. Two possibilities arise:

- either the set $\{P \in C(\mathbb{Q}) : P \equiv \overline{P} \pmod{p}\}$ is empty, in which case its order is certainly bounded by $1 + v_{\overline{P}}(\overline{\omega}) + \lfloor \frac{v_{\overline{P}}(\overline{\omega})}{p-2} \rfloor$;
- or $\{P \in C(\mathbb{Q}) : P \equiv \overline{P} \pmod{p}\} \neq \emptyset$, in which case we can fix $P \in C(\mathbb{Q})$ that reduces to $\overline{P}$. If P' is another point that also reduces to $\overline{P}$ we have

$$\int^P \omega = \int^{P'} \omega = 0,$$

and therefore

$$\int^{P-P'} \omega = 0.$$

Fix a local parameter t around P and write $\omega = \sum_{i \geq 0} a_i t^i dt$; notice that this differential form is nonzero, because differential forms on $C/\mathbb{F}_p$ and on $\mathcal{J}_{\mathbb{F}_p}$ correspond bijectively to each other. We obtain

$$0 = \int^{P-P'} \omega = \int_0^{t(P')} \sum_{i \geq 0} a_i t^i dt = \sum_{i \geq 0} a_i \frac{t(P')^{i+1}}{i+1}.$$

An application of Strassman's theorem (see below) implies that the number of solutions to this equation with $t(P') \in p\mathbb{Z}_p$ is at most $1 + v_{\overline{P}}(\overline{\omega}) + \lfloor \frac{v_{\overline{P}}(\overline{\omega})}{p-2} \rfloor$ (the quantity $d := v_{\overline{P}}(\overline{\omega})$ appears naturally: indeed, d is precisely the first index for which a_d is nonzero modulo p, which is useful to apply Strassman's theorem).

Therefore we obtain

$$\begin{aligned}
\#C(\mathbb{Q}) &= \sum_{\overline{P} \in C(\mathbb{F}_p)} \#\{P \in C(\mathbb{Q}) : P \equiv \overline{P} \pmod{p}\} \\
&\leq \sum_{\overline{P} \in C(\mathbb{F}_p)} 1 + v_{\overline{P}}(\overline{\omega}) + \left\lfloor \frac{v_{\overline{P}}(\overline{\omega})}{p-2} \right\rfloor \\
&\leq \#C(\mathbb{F}_p) + \deg \operatorname{div}(\overline{\omega}) + \left\lfloor \frac{\deg \operatorname{div} \overline{\omega}}{p-2} \right\rfloor \\
&= \#C(\mathbb{F}_p) + 2g - 2 + \left\lfloor \frac{2g-2}{p-2} \right\rfloor.
\end{aligned}$$

□

Theorem 4.3. *(Strassman) Let $f = \sum_{n\geq 0} a_n x^n \in \mathbb{Q}_p[[x]]$. Suppose that $|a_n| \to 0$ as $n \to \infty$ and that f is not identically zero, and let*

$$r := \min v_p(a_n), \quad N = N(f) := \max\{n : v_p(a_n) = r\}.$$

Then the equation $f(x) = 0$ has at most N solutions in $\mathbb{Z}_p$.

Proof. Multiplying by a power of p we can ensure that $f \in \mathbb{Z}_p[x]$ and the minimal valuation of a coefficient is 0. We proceed by induction on N. If $r = 0$, then all the a_n with $n > 0$ are divisible by p, while a_0 is a p-adic unit. It follows that $f(x) \equiv a_0 \in \mathbb{Z}_p^\times$ for all $x \in \mathbb{Z}_p$, hence $f(x) \neq 0$ for all x as claimed.

Now suppose we have proved the statement for some N, and consider the case of $N+1$. If $f(x) = 0$ has no solutions in $\mathbb{Z}_p$ we are done, so assume there is a solution x_0; the case $x_0 = 0$ is trivial, so assume $x_0 \neq 0$. Write

$$f(x) = (x - x_0)g(x).$$

If we can check that $g(x) = \sum b_m x^m$ satisfies the hypothesis of Strassman's theorem with $N(g) \leq N$ we are done. For all $n \geq 0$ we have

$$a_n = b_{n-1} - x_0 b_n,$$

where by convention $b_{n-1} = 0$. The power series $g(x)$ still converges on $\mathbb{Z}_p$, so $|b_n| \to 0$ as $n \to \infty$. It is clear that

$$\begin{aligned} b_n &= a_{n+1} + x_0 b_{n+1} \\ &= a_{n+1} + x_0(a_{n+2} + x_0 b_{n+2}) \\ &= \cdots = \sum_{j\geq 0} a_{n+1+j} x_0^j. \end{aligned}$$

This series converges, because we have

$$|a_{n+1+j} x_0^j| = \frac{|a_{n+1+j} x_0^{n+1+j}|}{|x_0^{n+1}|}$$

and we know that the general term of $f(x)$, which is $|a_{n+1+j} x_0^{n+1+j}|$, tends to 0. It follows that

$$|b_n| = \left|\sum_{j\geq 0} a_{n+1+j} x_0^j\right| \leq \max_j \left|a_{n+1+j} x_0^j\right| \leq \max_j |a_{n+1+j}|$$

In particular, since a_t is not a unit for any $t > N + 1$, we have that for $m \geq N + 1$

$$|b_m| \leq \max_j |a_{m+1+j}| \leq \max_{t\geq N+2} |a_t| < 1,$$

so every b_m with $m \geq N+1$ is divisible by p. Since at least one of the b_m is a unit (otherwise we would have $g(x) \equiv 0 \pmod p$, hence $f(x) \equiv 0 \pmod p$ in $\mathbb{Z}_p[x]$, contradiction) we are done.

Incidentally, one has $N(g) = N(f) - 1 = N$: indeed, using the fact that $p \mid a_{N+j}$ for every $j \geq 2$ we obtain

$$b_N = \sum_{j \geq 0} a_{N+1+j} x_0^j = a_{N+1} + \sum_{j \geq 1} a_{N+1+j} x_0^j \equiv a_{N+1} \not\equiv 0 \pmod{p}.$$

□

5 Construction of $\int$ in the rigid setting

5.1 Notation

Let K be a p-adic field (finitely generated extension of $\mathbb{Q}_p$) with ring of integers R, uniformizer π, and quotient field k. For later use, we fix an automorphism σ of K that reduces to the p-power map on k and extend it to $\overline{K}$.

5.2 Affine rigid geometry

The Tate algebra is

$$T_n := K\langle t_1, \ldots, t_n \rangle := \left\{ \sum a_I t^I : \lim_{|I| \to \infty} |a_I| \to 0 \right\}.$$

It is a very nice ring! For example, we have Weierstrass preparation and division:

Theorem 5.1. *A Weierstrass polynomial is $f(t_1, \ldots, t_n) = t_1^m + t_1^{m-1} g_{m-1}(t_2, \ldots, t_m) + \cdots + g_0(t_2, \ldots, t_m)$, where each g_i is an element of T_{n-1} and $g_i(0, \ldots, 0) = 0$.*

- *for any $f \in T_n$ such that $f(0, \ldots, 0) = 0$, we have $f = uW$ with u a unit and W a Weierstrass polynomial.*
- *given $f, g \in T_n$, there exist $q \in T_n$ and r a Weierstrass polynomial such that $f = qg + r$.*

We also have a version of Noether's normalization, and therefore the weak Nullstellensatz: every maximal ideal is a Galois conjugacy class of geometric points: more formally,

$$\mathrm{Spm}(T_n) = \{K - \text{homomorphism } \psi : T_n \to \overline{K}\}/\mathrm{Gal}(\overline{K}/K)$$

The maximal spectrum of the Tate algebra is therefore

$$\mathrm{Spm}(T_n) = \left\{(z_1, \ldots, z_n) \in \overline{K}^n : |z_i| \leq 1\right\}/\mathrm{Gal}(\overline{K}/K).$$

To see that points need to have integral coordinates, just notice that if $z_i \in \overline{K}^\times$ is non-integral, then $t_i - z_i = -z_i(1 - z_i^{-1} t_i)$ is a unit in T_n, so it cannot map to zero.

The **unit polydisk** is $B_n := \{(z_1, \ldots, z_n) \in \overline{K}^n : |z_i| \leq 1\}$. An **affinoid algebra** is a K-algebra with a surjective map $T_n \to A$ for some n. Prototypical example:

$$A = T_2/(t_1 t_2 - 1), \quad \mathrm{Spm}(A) = \{(z_1, z_2) \in B_2 : z_1 z_2 = 1\} = \left\{x \in \overline{K} : |x| = 1\right\}/\mathrm{Gal}(\overline{K}/K).$$

Remark 5.2. T_n is a Banach algebra with respect to the so-called Gauss norm: for a series $f = \sum a_I x^I$, its Gauss norm is $\|f\| = \max_I |a_I|$. Every affinoid algebra inherits a structure of Banach algebra (the Gauss norm passes to the quotient because any ideal in the Tate algebra is topologically closed).

Remark 5.3. The notes `http://www.mat.uc.cl/~rmenares/TateAlgebras.pdf` contain proofs for many useful facts concerning Tate algebras.

5.3 Monsky-Washnitzer cohomology

We shall work with the so-called wcfg algebras:

Definition 5.4. *1. The **standard weakly complete finitely generated (wcfg) algebra** is*

$$\mathcal{T}_n^\dagger = \left\{ \sum a_I t^I : a_I \in R, \exists r > 1 \text{ such that } \lim_{|I|\to\infty} |a_I| r^{|I|} = 0 \right\}.$$

*2. A **wcfg algebra** is an R-algebra $A^\dagger$ with a surjective homomorphism $\mathcal{T}_n^\dagger \to A^\dagger$.*

3. Given a wcfg algebra $A^\dagger$, its (π-adic) completion is $\hat{A} := \varprojlim_n A^\dagger/\pi^n A^\dagger$.

Notice that the Gauss norm on the Tate algebra T_n restricts to a norm on $\mathcal{T}_n^\dagger$ (with respect to this norm $\mathcal{T}_n^\dagger$ is not complete). We shall need the following theorem, which is a consequence of the so-called *Artin approximation* property:

Theorem 5.5. *(see [vdP86] and the references therein) The following hold:*

- *Let $\varepsilon > 0$. Given a diagram of wcfg algebras*

$$\begin{array}{ccc} & & A \\ & & \downarrow f \\ B/J & \xleftarrow{g} & B \end{array}$$

and a morphism $\hat{u} : \hat{A} \to \hat{B}$ such that $\hat{f} = \hat{g} \circ \hat{u}$, there exists a morphism $u : A \to B$ such that $f = g \circ u$ and $|u - \hat{u}| \leq \varepsilon$.

- *Let $\varepsilon > 0$. Given a diagram of wcfg algebras*

$$\begin{array}{ccc} & & A \\ & & \uparrow f \\ C & \xrightarrow{g} & B \end{array}$$

and a morphism $\hat{u} : \hat{A} \to \hat{B}$ such that $\hat{g} = \hat{f} \circ \hat{u}$, there exists a morphism $u : A \to B$ such that $f = g \circ u$ and $|u - \hat{u}| \leq \varepsilon$.

5.3.1 Differentials

The modules of differentials associated with $A^\dagger = \mathcal{T}_n^\dagger/\langle f_1, \ldots, f_m\rangle$ are

$$\Omega^1_{A^\dagger} := \frac{\bigoplus A^\dagger dt_i}{\left\langle \frac{\partial f_j}{\partial t_i} dt_i \;\middle|\; j = 1, \ldots, m \right\rangle_{A^\dagger}}$$

and

$$\Omega^k_{A^\dagger} := \Lambda^k \Omega^1_{A^\dagger}.$$

They are projective $A^\dagger$-modules. The de Rham complex $\Omega^\bullet_{A^\dagger}$ is

$$0 \to \Omega^0_{A^\dagger} \to \Omega^1_{A^\dagger} \to \cdots \to \Omega^k_{A^\dagger}.$$

5.3.2 Cohomology

If if $A^\dagger$ is a wcfg algebra then $\overline{A} = A^\dagger/\pi$ is an honest finitely generated k-algebra.

Definition 5.6. *The Monsky-Washnitzer cohomology of $\overline{A}$, denoted by $H_{MW}(\overline{A}/K)$, is the cohomology of the de Rham complex $\Omega^\bullet_{A^\dagger} \otimes K$.*

It is a theorem of Berthelot [Ber97] that $H^i_{MW}(\overline{A}/K)$ is a finite-dimensional K-vector space for all i.

Theorem 5.7. *(Elkik [Elk73], van der Porten [vdP86])*

1. *Let $\bar{A}$ be a smooth finitely generated k-algebra. There exists a flat wcfg algebra $A^\dagger$ such that $\bar{A} = A^\dagger/\pi$.*
2. *Any two such lifts are isomorphic.*
3. *Any morphism $\overline{f} : \overline{A} \to \overline{B}$ can be lifted to a morphism $f^\dagger : A^\dagger \to B^\dagger$.*
4. *Any two maps f_1, f_2 with the same reduction modulo π induce homotopic maps $\Omega^\bullet_{A^\dagger} \otimes K \to \Omega^\bullet_{B^\dagger} \otimes K$.*

Proof. 1. It suffices to show that there is a smooth lift, and then weakly-complete it. Existence of the smooth lift is shown in [Elk73].

2. By flatness and the fact that $\overline{A}$ is smooth, one obtains that $A/\pi^n A$ and $B/\pi^n B$ are smooth over $R/\pi^n R$ for all n. In particular, there is a projective system of morphisms $\hat{A} \to \hat{B}$. By Artin approximation, there is a morphism $i : A \to B$ which is an isomorphism modulo π. We want to show that it is an isomorphism. By flatness, $A/\pi A \cong \pi^n A/\pi^{n+1} A$ and $B/\pi B \cong \pi^n B/\pi^{n+1} B$, hence in particular $\ker i \subseteq \bigcap_n \pi^n A = (0)$. As for surjectiveness, see Lemma 5.8 below.

   
   In [vdP86] it is claimed that surjectivity modulo π is "a consequence of the Weierstrass theorems", but no details are given. Any errors in the previous proof (or in Lemma 5.8 below) are entirely down to me.

3. Same as 2.

4. We only give a sketch. The idea is to mimic the proof of Poincaré's lemma: we look for maps $\alpha_0, \alpha_1 : B\langle T\rangle^\dagger \to B^\dagger$ and $f : B\langle T\rangle^\dagger \to B^\dagger$ such that $f_i = \alpha_i \circ f$. We define α_i by sending T to i. Now

$$\Omega^{q+1}(B\langle T\rangle^\dagger/K) = B\langle T\rangle^\dagger \otimes_B \Omega^{q+1}(B/K) \oplus B\langle T\rangle^\dagger dT \otimes \Omega^q(B\langle T\rangle^\dagger/K)$$

and one defines δ_q to be 0 on the first summand and

$$g \otimes \omega \mapsto \left(\int_0^1 g(t)dt\right)\omega$$

on the second. One then checks

$$\alpha_{1,*} - \alpha_{0,*} = d\delta_{q-1} + \delta_q d : \Omega^q(A/K) \to \Omega^q(B/K).$$

Morally, we want to define f by $a \mapsto (1-T)f_0(a) + Tf_1(a)$. Clearly this won't be an algebra homomorphism in general.

Set $S = pT$ and define

$$\begin{array}{ccc} A & \to & \hat{B}[[S]]/(S^2 - pS) \\ a & \mapsto & f_0(a) + \frac{f_1(a)-f_0(a)}{p}S. \end{array}$$

Now this is an algebra homomorphism, and by (formal) smoothness it lifts to

$$\hat{A} \to \hat{B}[[S]] \subset \hat{B}\langle T\rangle.$$

By Artin approximation (Theorem 5.5), we obtain the desired map $A \to B\langle T\rangle^\dagger$.

□

It follows from Theorem 5.7 that the cohomology of $\overline{A}$ does not depend on the lift $A^\dagger$; moreover, $A \mapsto H^1_{MW}(\overline{A}/K)$ is functorial. This Monsky-Washnitzer cohomology is a nice cohomological theory which (if I understand correctly) later evolved into rigid cohomology.

Lemma 5.8. *Let A, B be wcfg algebras and $i : A \to B$ be a map such that $\bar{i}$ (the reduction of i modulo π) is surjective. Then i is surjective.*

Proof. Wlog $A = \mathcal{T}_n^\dagger$ (just write A as a quotient of some $\mathcal{T}_n^\dagger$). For some $m \geq 0$, there is a surjective map f (extending i) from $A' = A\langle x_{n+1}, \ldots, x_{n+m}\rangle^\dagger$ to B. Take m minimal: if $m = 0$ we are done. Otherwise, since $\bar{i}$ is surjective we can find $a \in A$ such that $x_{n+m} - a$ is in the kernel of $\bar{f}$. Then we can write $x_{m+n} - a = a' + \pi r$ with $a' \in \ker f$, $r \in A'$ (to see this, simply notice that $\ker f$ is generated by π and $\ker \overline{f}$). We now have that $A\langle x_{n+1}, \ldots, x_{n+m-1}\rangle^\dagger \to A'/(a')$ is onto (essentially, just keep replacing x_{m+n} with $a + \pi r$: the series converges because of the π). Since a' is in the kernel of f, this gives a surjective map $A\langle x_{n+1}, \ldots, x_{n+m-1}\rangle^\dagger \to B$, contradicting the minimality of m. □

5.3.3 The lift of Frobenius

The map[4]

$$\begin{array}{ccc} \overline{A} & \to & \overline{A} \\ x & \mapsto & x^p \end{array}$$

can be lifted to a map $A^\dagger \to A^\dagger$. This lift can be chosen so as to be σ-linear:

Proposition 5.9. *There is a map $\phi : A^\dagger \to A^\dagger$ that is σ-linear and satisfies $\phi(x) \equiv x^p \pmod{\pi}$.*

Proof. Consider the algebra $\overline{B}/k$ which is the same as $\overline{A}$ as a ring, but for which the structure map $k \to \overline{B}$ is $k \xrightarrow{x^p} k \to \overline{B} = \overline{A}$. The algebra $B^\dagger$ which is the same as $A^\dagger$ as a ring, but for which the structure map is $R \xrightarrow{\sigma} R \to B^\dagger$, is a lift of $\overline{B}$. The map

$$\varphi : \begin{array}{ccc} \overline{A} & \to & \overline{B} \\ x & \mapsto & x^p \end{array}$$

is a homomorphism of k-algebras: indeed it is certainly a homomorphism of rings, and

$$\varphi(\lambda a) = \lambda^p a^p = \lambda^p \varphi(a) = \lambda \cdot_{\overline{B}} \varphi(a).$$

By Theorem 5.7 we obtain that there is a map $\phi : A^\dagger \to B^\dagger$ that lifts φ. In particular, we have $\phi(x) \equiv x^p \pmod{\pi}$; moreover,

$$\phi(\lambda \bullet_{A^\dagger} a) = \lambda \bullet_{B^\dagger} \phi(a) = \sigma(\lambda) \bullet_{A^\dagger} \phi(a).$$

□

The map ϕ just construced induces by functoriality a σ-linear map

$$\phi : H^i_{MW}(\overline{A}) \to H^i_{MW}(\overline{A}/K).$$

If $\#k = q = p^s$, the s-th iterate of $x \mapsto x^p$ is k-linear, so its lift (by the same proof as above) induces a *linear* automorphism ϕ^s of $H^i_{MW}(\overline{A}/K)$.

Concerning the eigenvalues of Frobenius, we have the following deep theorem:

Theorem 5.10. *[Chi98] Each eigenvalue of ϕ^s acting on $H^i_{MW}(\overline{A}/K)$ is a q-Weil number[5] of integral weight contained in the interval $[i, 2i]$.*

[4] this is always a map of rings in characteristic p... convince yourself of this

[5] recall that a *q-Weil number* of weight i is an algebraic number α whose absolute value is $q^{i/2}$ under any complex embedding. Here $q = p^s = \#k$.

5.4 Specialization; the algebra of locally analytic functions

Let $A^\dagger = \mathcal{T}_n^\dagger/I$ be a wcfg algebra. The completion of $A^\dagger$ with respect to the Gauss norm induced from $\mathcal{T}_n^\dagger$ is the algebra $A = T_n/I$. We then obtain an affinoid space $X = \mathrm{Spm}(A)$ and a reduction $X_k = \mathrm{Spec}(\overline{A})$. The geometric points X^{geo} of X are the K-linear homomorphisms $A \to \overline{K}$.

There is a reduction map, defined at the level of geometric points by

$$\begin{array}{ccc} X^{geo} & \to & X_k \\ (\psi : A \to L \subset \overline{K}) & \mapsto & \left(\overline{\psi} : A/\pi \to \mathcal{O}_L/\pi_L\right). \end{array}$$

The definition works because (as we have already seen) ψ sends A to $\mathcal{O}_L$.

Definition 5.11. *A **residue disk** U_x is the inverse image in X^{geo} under the reduction map of a geometric point $x : \mathrm{Spec}(\overline{k}) \to X_k$. By (smoothness and) Hensel's lemma, one sees that U_x is isomorphic to the space of geometric point of a unit polydisk.*

Definition 5.12. *A K-**locally analytic function** on X is a map*

$$f : X^{geo} \to \overline{K}$$

such that

- *f is $\mathrm{Gal}(\overline{K}/K)$-equivariant, that is, for any $\tau \in \mathrm{Gal}(\overline{K}/K)$ we have $f(\tau(x)) = \tau(f(x))$;*
- *on each residue disk, f is defined by a convergent power series.*

The K-locally analytic functions on X form a K-algebra A_{loc} containing A.

There are natural modules of differentials $\Omega^\bullet_{A_{\mathrm{loc}}}$. Next we define an action of ϕ on points and functions.

1. On points: given a morphism $(\psi : A \to \overline{K}) \in X^{geo}$, we define
$$\phi(\psi) = \sigma^{-1} \circ \psi \circ \phi$$
2. On functions:
$$\phi(f)(x) := \sigma(f(\phi(x))$$

5.5 Construction of the Coleman integral

We can now construct the Coleman integral on an affinoid space:

Theorem 5.13. *Let $A^\dagger$ be a wcfg algebra. There is a unique K-linear integration map*

$$\int : \left(\Omega^1_{A^\dagger} \otimes K\right)^{d=0} \to A_{\mathrm{loc}}/K$$

satisfying:

1. *$d \circ \int$ is the canonical map $(\Omega^1_{A^\dagger} \otimes K)^{d=0} \to \Omega^1_{A_{\mathrm{loc}}}$*

2. *$\int \circ d$ is the canonical map $A^\dagger \otimes K \to A_{\mathrm{loc}}/K$*

3. *$\phi \circ \int = \int \circ \phi$.*

Proof. Choose forms $\omega_1, \ldots, \omega_r \in \Omega^1_{A^\dagger} \otimes K$ whose images in $H^1_{MW}(\overline{A})$ are a basis. It suffices to integrate the ω_i's: indeed a general 1-form ω will have the form $\omega = \sum \alpha_i \omega_i + df$ for some $(A^\dagger \otimes K)$-function f, so the formal properties of integration force $\int \omega = \sum \alpha \int \omega_i + f$.

If $\underline{\omega}$ is the (column) vector of forms ω_i, then there exists a matrix $M \in \mathrm{M}_{r\times r}(K)$ such that

$$\phi\underline{\omega} = M\underline{\omega} + d\underline{g}$$

for some $\underline{g} \in (A^\dagger \otimes K)^r$. Applying $\int$ to this equality and using linearity and the fact that ϕ and $\int$ commute we find

$$\phi \int \underline{\omega} = M \int \underline{\omega} + \underline{g}.$$

Fix a vector of functions $F_{\underline{\omega}}$ representing[6] $\int \underline{\omega}$: then we have

$$\phi F_{\underline{\omega}} = M F_{\underline{\omega}} + \underline{g} + \underline{c}$$

for some vector of constants $\underline{c}$.

Lemma 5.14. *The map $\sigma - M : K^r \to K^r$ is bijective.*

Proof. By linearity and final-dimensionality of the vector spaces involved, it suffices to show injectivity. Fix $c \in K^r$ and consider the equation

$$(\sigma - M)x = c :$$

rewriting it as $\sigma x = Mx + c$ and applying σ, one obtains

$$\sigma^2 x = \sigma(Mx) + \sigma(c) = \sigma(M)\sigma(x) + \sigma(c) = \sigma(M)(Mx + c) + \sigma(c);$$

continuing in this way, we arrive at

$$x = \sigma^s x = \sigma^{s-1}(M) \cdots \sigma(M)Mx + q,$$

where q has some (complicated) expression in terms of σ, M, and c. We now notice that $F := \sigma^{s-1}(M) \cdots \sigma(M)M$ is precisely the matrix of the "linear Frobenius" (i.e. ϕ^s) acting on $H^1_{MW}(\overline{A}/K)$, so by Theorem 5.10 the matrix $(I - F)$ is invertible (1 is not an eigenvalue of F). Since the equation we are trying to solve is $(I - F)x = q$, this proves that there is at most one solution to our original equation $(\sigma - M)x = c$. □

[6] integration takes values in functions *up to constants*: we let $F_{\underline{\omega}}$ be a fixed function in the equivalence class of $\int \underline{\omega}$. Equivalently, we fix an arbitrary integration constant for each of the ω_i's.

In particular, there is a vector of constants $\underline{d}$ such that $(\sigma - M)(\underline{d}) = -\underline{c}$. Replacing $F_{\underline{\omega}}$ with $F_{\underline{\omega}} + \underline{d}$ we can assume $\underline{c} = 0$: indeed,

$$\phi(F_{\underline{\omega}} + \underline{d}) - M(F_{\underline{\omega}} + \underline{d}) = \underline{g} + \underline{c} + (\sigma - M)(\underline{d}) = \underline{g} + \underline{c} - \underline{c} = \underline{g},$$

where we have used the fact that ϕ acts as σ on constants.

Now since $dF_{\underline{\omega}} = \underline{\omega}$ it suffices to determine $F_{\underline{\omega}}$ on a single point in each residue disk: the reason for this is that *on a residue disk* the formal integral makes sense by definition of $\Omega^1_{A^\dagger}$, so that $F_{\underline{\omega}}$ and the formal integral of $\underline{\omega}$ might differ at most by a constant. Take any point x. Then

$$(\phi F_{\underline{\omega}})(x) = M F_{\underline{\omega}}(x) + \underline{g}(x),$$

which gives

$$\sigma F_{\underline{\omega}}(\phi x) = M F_{\underline{\omega}}(x) + \underline{g}(x).$$

Since x and ϕx belong to the same residue disk, the difference $F_{\underline{\omega}}(\phi x) - F_{\underline{\omega}}(x) = \underline{e}(x)$ is uniquely determined by $\underline{\omega}$ (and is found by formal integration). The previous equation can then be rewritten as

$$(\sigma - M)(F_{\underline{\omega}}(x)) = \underline{g}(x) - \sigma(\underline{e}(x)),$$

which (since $\sigma - M$ is bijective) uniquely determines $F_{\underline{\omega}}(x)$.

□

References

[Ber97] Pierre Berthelot. Finitude et pureté cohomologique en cohomologie rigide. *Invent. Math.*, 128(2):329–377, 1997. With an appendix in English by Aise Johan de Jong.

[Chi98] Bruno Chiarellotto. Weights in rigid cohomology applications to unipotent F-isocrystals. *Ann. Sci. École Norm. Sup. (4)*, 31(5):683–715, 1998.

[Elk73] Renée Elkik. Solutions d'équations à coefficients dans un anneau hensélien. *Ann. Sci. École Norm. Sup. (4)*, 6:553–603 (1974), 1973.

[Mat55] Arthur Mattuck. Abelian varieties over p-adic ground fields. *Ann. of Math. (2)*, 62:92–119, 1955.

[McC94] William G. McCallum. On the method of Coleman and Chabauty. *Math. Ann.*, 299(3):565–596, 1994.

[vdP86] Marius van der Put. The cohomology of Monsky and Washnitzer. *Mém. Soc. Math. France (N.S.)*, (23):4, 33–59, 1986. Introductions aux cohomologies p-adiques (Luminy, 1984).