Non-abelian Chabauty study group

Giulio Bresciani, Julian L. Demeio, Guido Lido, Davide Lombardo

2017–2018

Contents

Chapter 1

Coleman integration

1.1 Integrating on Jacobians

Let $K_\mathfrak{p}$ be a p-adic field, that is, a finite extension of $\mathbb{Q}_p$, and let J be the Jacobian of a smooth curve $C/K_\mathfrak{p}$. The purpose of this chapter 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 1.1.1. In fact, the same construction goes through for any abelian variety over a p-adic field.

Lemma 1.1.2. *Let* $\mathrm{Cot}(J)$ *be the cotangent space to* J *at the origin. The evaluation map*

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

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 defined at 0 can be extended to a translation-invariant differential form. □

Lemma 1.1.3. *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 group 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, $\big(J(K_\mathfrak{p}) : B\big) =: N$ is finite[2], and we can set

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

One checks that $d\lambda_\omega = \omega$: this is clear on B, and by translation-invariance it is then true on all of J. 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 1.1.4. *We set $\int^P \omega = \lambda_\omega(P)$.*

Proposition 1.1.5. *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. We have $\int^P \omega = 0$ for all ω if and only if $\lambda_\omega(P) = 0$ for all ω. Denote by $\mathrm{Tan}\, J$ the tangent space at the origin to $J(K_\mathfrak{p})$ and consider the map

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

[1] a theorem of Mattuck [Mat55] says that $J(K_\mathfrak{p})$ contains an open subgroup isomorphic (as a topological group) to $\mathcal{O}_{K_\mathfrak{p}}^g$. 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.

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 $\mathrm{Tan}(J)$ is torsion-free, so $\mathrm{Tors}\, J(K_\mathfrak{p})$ is sent to 0 by ι. This proves that ι induces an injective map

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

or equivalently a pairing

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

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

□

1.2 Construction of $\int$ in the rigid setting

The construction of the integration map given in the previous section relies on the group structure of the Jacobian; in this section we shall sketch a much more general construction of the Coleman integral, which however relies on deeper results (specifically, the study of the eigenvalues of Frobenius on the so-called Monsky-Washnitzer cohomology of the variety for which we want to construct the integral).

1.2.1 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 $\overline{K}$.

1.2.2 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, it satisfies Weierstrass preparation and division:

Definition 1.2.1. *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 $g_i(0, \ldots, 0) = 0$.

Theorem 1.2.2. *The following hold:*

- *let $f \in T_n$ be such that $f(0,\dots,0) = 0$. Suppose that the power series $f(t_1,\dots,t_n)$ has at least one term involving only one variable[3] (say t_1): then we have $f = uW$ with u a unit and W a Weierstrass polynomial.*
- *given $f \in T_n$ and a Weierstrass polynomial g, there exist $q \in T_n$ and a Weierstrass polynomial r 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

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

To see that points need to have integral coordinates, 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 $B_n := \{(z_1,\dots,z_n) \in \overline{K}^n : |z_i| \leq 1\}$. An **affinoid algebra** is a K-algebra with a surjective map $T_n \to A$ for some n. The prototypical example is $A = T_2/(t_1t_2 - 1)$ (which is a p-adic analogue of $\mathbb{S}^1$):

$$\mathrm{Spm}(A) = \{(z_1,z_2) \in B_2 : z_1z_2 = 1\} = \left\{x \in \overline{K} : |x| = 1\right\}/\mathrm{Gal}(\overline{K}/K).$$

Remark 1.2.3. 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 1.2.4. Proofs for many useful facts concerning Tate algebras can be found in `http://www.mat.uc.cl/~rmenares/TateAlgebras.pdf`.

1.2.3 Monsky-Washnitzer cohomology

We shall work with the so-called wcfg algebras:

Definition 1.2.5. 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] Notice that one can always reduce to this situation by an appropriate change of variables.

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

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

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

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

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

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

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

Cohomology

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

Definition 1.2.7. *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 1.2.8. *(Elkik [Elk73], van der Porten [vdP86])*

1. *Let $\overline{A}$ be a smooth finitely generated k-algebra. There exists a flat wcfg algebra $A^\dagger$ such that $\overline{A} = A^\dagger/\pi$.*
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_0, f_1 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 $\widehat{A} \to \widehat{B}$. 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 1.2.9 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 1.2.9 below) are entirely down to the author of these notes.

3. Similar to 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

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

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

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

By Artin approximation (Theorem 1.2.6), we obtain the desired map $A \to B\langle T\rangle^\dagger$. □

It follows from Theorem 1.2.8 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 later evolved into rigid cohomology.

Lemma 1.2.9. *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. Without loss of generality, we can assume $A = \mathcal{T}_n^\dagger$ (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 $\overline{f}$. 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 presence of 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. □

The lift of Frobenius

The map

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

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

Proposition 1.2.10. *There is a map $\varphi : A^\dagger \to A^\dagger$ that is σ-linear and satisfies $\varphi(x) \equiv x^p \pmod{\pi}$.*

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

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

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 1.2.8 we obtain a map $\varphi : A^\dagger \to B^\dagger$ that lifts φ. In particular, we have $\varphi(x) \equiv x^p \pmod{\pi}$; moreover,

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

□

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

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

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 this map (which are usually called *the eigenvalues of the linear Frobenius*), we have the following deep theorem:

Theorem 1.2.11. *[Chi98] Each eigenvalue of φ^s acting on $H^i_{MW}(\overline{A}/K)$ is a q-Weil number[4] of integral weight contained in the interval $[i, 2i]$.*

Example 1.2.12 (Eigenvalues of Frobenius on the thrice-punctured projective line)**.** We take $X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$ as a variety over $\mathbb{Q}_p$. As (ring of regular functions of) an integral model we take $A = \mathbb{Z}_p[x, y, z]/(xy - 1, (1 - x)z - 1)$. We denote by $A^\dagger$ a weak completion of this algebra, that is,

$$A^\dagger = \left\{ \sum_{I \in \mathbb{N}^3} a_I t^I : a_I \in \mathbb{Z}_p, \exists r > 1 : \lim_{|I| \to \infty} |a_I| r^{|I|} = 0 \right\} / (xy - 1, (1 - x)z - 1),$$

where t is the vector of variables (x, y, z). A basis of $H^1_{MW}(\overline{A}/K)$ is given by $\omega_1 = \frac{dx}{x}$, $\omega_2 = \frac{dx}{1-x}$, or more formally $\omega_1 = y dx, \omega_2 = z dx$. As a lift of Frobenius we want to take

$$F : x \mapsto x^p, y \mapsto y^p;$$

[4] 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 $q = p^s = \#k$.

the question is, what is $F(z)$? We have

$$1 = F(1-x)F(z) = (1-x^p)F(z),$$

so we need to set

$$F(z) = \frac{1}{1-x^p} = \frac{1}{(1-x)^p + (1-x^p) - (1-x)^p}.$$

Let $H_p(z) := \frac{(1-x)^p - (1-x^p)}{p} \in \mathbb{Z}_p[x]$. Continuing with the previous computation,

$$\begin{aligned} F(z) &= \frac{1}{(1-x)^p - pH_p(x)} = \frac{z^p}{(z(1-x))^p - pz^pH_p(x)} \\ &= \frac{z^p}{1-pz^pH_p(x)} = z^p \sum_{n\geq 0} (pz^pH_p(x))^n. \end{aligned}$$

We claim that this series is in $A^\dagger$. To prove this, we need to show that it converges on a polydisk of radii strictly larger than 1. Since y does not appear in the series, we may work with x, z only. We claim that the series converges on

$$B := \{(x,z) \in \mathbb{Q}_p^2 : v_p(x) \geq -\frac{1}{4p}; \quad v_p(z) \geq -\frac{1}{4p}\}.$$

Indeed, if $(x,z) \in B$ we have

$$\begin{aligned} v_p(pz^pH_p(x)) &= 1 + pv_p(z) + v_p(H_p(x)) \geq 1 + pv_p(z) + \min\{\deg(H_p(x))v_p(x), 0\} \\ &\geq 1 + \left(-\frac{1}{4}\right) - p\frac{1}{4p} \geq \frac{1}{2}, \end{aligned}$$

so the n-th term in the series has valuation at least $n/2$, and the series converges. Finally, it is clear that $F(z) \equiv z^p \pmod{p}$, so F is indeed a lift of Frobenius. We now compute its action on Monsky-Washnitzer cohomology: we have

$$F^*\omega_1 = F^*(ydx) = y^p px^{p-1}dx = pydx = p\omega_1$$

and

$$F^*\omega_2 = F^*(zdx) = z^p \sum_{n\geq 0} (pz^pH_p(x))^n \cdot px^{p-1}dx.$$

We now need to determine the cohomology class of this differential form. We may observe that writing $F^*\omega_2 = a\omega_1 + b\omega_2 + \psi$ with ψ an exact form the constants a and b are determined by the residues of $F^*\omega_2$ at $x = 0$ and $x = 1$. Noticing that $F^*\omega_2$ is regular at $x = 0$ we obtain $a = 0$; as for b, taking for simplicity p odd (a similar calculation also works for $p = 2$) we may notice that $\deg H_p(x) = p - 1$, so when we write $pz^pH_p(x)$ as

a Laurent series in $(x-1)$ the largest degree that appears is $-p+(p-1)=-1$. On the other hand,

$$\begin{aligned} pz^p x^{p-1}dx &= p(1-x)^{-p}x^{p-1}dx = p(1-x)^{-p}(1+(x-1))^{p-1}dx \\ &= p(1-x)^{-p}\sum_{i=0}^{p-1}\binom{p-1}{i}(x-1)^i dx \\ &= -p\sum_{i=0}^{p-1}\binom{p-1}{i}(x-1)^{i-p}dx \end{aligned}$$

contains only terms of negative degree in $(x-1)$, so

$$pz^p x^{p-1}\sum_{n\geq 1}(pz^p H_p(x))^n dx,$$

as a Laurent series in $(x-1)$, contains only powers of exponent ≤ -2, and therefore has zero residue (in particular, it is an exact form). We are left with considering

$$\begin{aligned} -p\sum_{i=0}^{p-1}\binom{p-1}{i}(x-1)^{i-p}dx &= -p(x-1)^{-1}dx + (\text{terms of degree } \leq -2)dx \\ &= p\omega_2 + \text{exact form.} \end{aligned}$$

It follows that the action of Frobenius on $H^1_{MW}(\overline{A}/K)$ is multiplication by p.

In fact, it is interesting to notice that the computation for $p=2$ depends in a crucial way on the properties of the 2-adic topology: one finds that $F^*\omega_2$ is given by

$$2z^2 x dx\sum_{n\geq 0}2^n\left(1-\frac{1}{1-x}\right)^n = 2\left(\frac{1}{(1-x)^2}-\frac{1}{1-x}\right)\sum_{n\geq 0}2^n\left(1-\frac{1}{1-x}\right)^n,$$

and taking only the parts of degree -1 we find

$$F^*\omega_2 = \text{exact form} - \frac{2dx}{1-x}\sum_{n\geq 0}2^n = \frac{2dx}{1-x} + \text{exact form},$$

where the equality $\sum 2^n = -1$ of course makes sense only in the 2-adic topology.

1.2.4 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 1.2.13. *A **residue disk** U_x is the inverse image in X^{geo} under the reduction map of a geometric point $x : \mathrm{Spec}(\bar{k}) \to X_k$. By (smoothness and) Hensel's lemma, one sees that U_x is isomorphic to the space of geometric point of a unit polydisk.*

Definition 1.2.14. *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 $\Omega^{\bullet}_{A_{\mathrm{loc}}}$. Finally, we can 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
$$\varphi(\psi) = \sigma^{-1} \circ \psi \circ \varphi$$
2. On functions:
$$\varphi(f)(x) := \sigma(f(\varphi(x))$$

1.2.5 Construction of the Coleman integral

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

Theorem 1.2.15. *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. *$\varphi \circ \int = \int \circ \varphi$.*

Proof. Choose forms $\omega_1, \ldots, \omega_r \in \Omega^1_{A^\dagger} \otimes K$ whose images in $H^1_{MW}(\overline{A})$ form 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

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

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

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

Fix a vector of functions $F_{\underline{\omega}}$ representing[5] $\int \underline{\omega}$: then we have

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

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

Lemma 1.2.16. *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

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

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 1.2.11 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 $(\sigma - M)x = c$. □

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,

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

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

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

[5] 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.

which gives

$$\sigma F_{\underline{\omega}}(\varphi x) = MF_{\underline{\omega}}(x) + \underline{g}(x).$$

Since x and φx belong to the same residue disk, the difference $F_{\underline{\omega}}(\varphi x) - F_{\underline{\omega}}(x) = \underline{e}(x)$ 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 $F_{\underline{\omega}}(x)$.

□

Chapter 2

The method of Chabauty (via Coleman integration)

2.1 Introduction

In this chapter we work over a number field 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 $C(K)$, concerning which 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 a K-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 (theorems of Faltings, Vojta, Bombieri)

Given C/K, there is a K-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 Mordell-Weil theorem, $J(K)$ is a finitely generated abelian group. The purpose of this chapter is to discuss the Chabauty-Coleman theorem and some of its more refined versions:

Theorem 2.1.1 (Chabauty-Coleman)**.** *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.*

Recall that if P is any K-rational point on C, then the map

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

is an embedding. Since theorem 2.1.1 is trivial if $C(K)$ is empty, we can assume that a rational point exists, and therefore that we can embed C into its Jacobian.

2.2 Chabauty-Coleman

Given the theory of Coleman integration developed in the previous chapter, the proof of theorem 2.1.1 is not hard:

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 $\mathfrak{p}$ be a prime of good reduction of C, and let $P_1, \dots, P_r \in J(K)$ generate a subgroup of rank equal to $r = \operatorname{rank} J(K)$ (in other words, $N := \big(J(K) : \langle P_1, \dots, P_r \rangle\big)$ is finite). Consider the $K_\mathfrak{p}$-linear subspace R of $H^0(J, \Omega^1_J)$ given by

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

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 $N[Q - P] \in \langle P_1, \dots, P_r \rangle$, 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 $\int^{[Q-P]} \omega = 0$. 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 an analytic function on a curve are isolated and the curve is compact, there can only be finitely many of them as desired. □

2.3 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 2.3.1. *(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 2.3.2. 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 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 2.3.1) The idea is to count rational points according to their reduction modulo p. We have

$$\#C(\mathbb{Q}) = \sum_{\overline{P} \in C(\mathbb{F}_p)} \#\{P \in C(\mathbb{Q}) : P \equiv \overline{P} \pmod{p}\}. \tag{2.1}$$

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 2.1.1. 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 (2.1) 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 2.3.3. *(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 $b_{-1} = 0$. 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

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

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

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

□

Chapter 3

Gruppo fondamentale étale

In questo capitolo vogliamo introdurre il gruppo fondamentale étale e le principali costruzioni ad esso legate. Descriveremo la teoria con un certo dettaglio in questo caso, riservandoci di essere meno precisi per altri gruppi fondamentali che vedremo nel seguito (ovvero quello $\mathbb{Q}_p$-unipotente di De Rham e quello $\mathbb{Q}_p$-unipotente étale). Un'ottima referenza è il capitolo 5 di [Sza09], che ho anche usato come traccia. Per comodità, tutti gli schemi saranno localmente noetheriani, a meno che non venga specificato diversamente: la teoria funziona anche più in generale, ma diventa un po' più complicata. Chiameremo Ω un generico campo algebricamente chiuso.

3.1 Rivestimenti étale finiti

Come si può intuire dal nome, per sviluppare la teoria del gruppo fondamentale étale sono necessari i rivestimenti étale finiti, cioé morfismi di schemi étale, finiti e surgettivi. Vediamo un po' di fatti al riguardo.

Proposition 3.1.1 (5.3.1 di [Sza09])**.** *Sia $\varphi : X \to S$ un rivestimento étale finito e $s : S \to X$ una sezione di φ. Allora s induce un isomorfismo fra S e un sottoschema aperto e chiuso di X. In particolare, se S è connesso s induce dà un isomorfismo tra S e una componente connessa di X.*

Proof. Innanzitutto vediamo che il morfismo $s : S \to X$ è finito. Prendo un ricoprimento affine S_i di S, considero le controimmagini (ancora affini) $X_i = \varphi^{-1}(S_i)$ che danno un ricoprimento affine di X. A questo punto, $s^{-1}(X_i) = S_i$ è ancora affine, e quindi il morfismo s è affine. La condizione di finitezza sui fasci è immediata.

Ora s è iniettivo, perché è una sezione, e chiuso, perché è finito, e quindi è topologicamente un'immersione chiusa. Per verificare che sia un'immersione chiusa di schemi basta verificare la surgettività a livello di fasci strutturali, che è ovvia.

Per vedere che è un'immersione aperta, mostriamo prima che è un isomorfismo sulle spighe. Prendiamo quindi $q \in S$, e chiamiamo $p = s(q)$, $q = \varphi(p)$. Abbiamo due mappe

a livello di spighe

$$\mathcal{O}_{S,q} \xrightarrow{\varphi^\#} \mathcal{O}_{X,p} \xrightarrow{s^\#} \mathcal{O}_{S,q}$$

la cui composizione è l'identità. A livello di campi residui l'isomorfismo è ovvio, le mappe $k(q) \to k(p) \to k(q)$ sono tutte iniettive. Inoltre, siccome $\varphi : X \to S$ è étale (in realtà ci basta non ramificata), $\mathcal{O}_{X,p}\varphi^\#(m_q) = m_p$. Questo, più Nakayama, ci dice che $\varphi^\#$ è bigettiva, e quindi anche $s^\#$ lo è.

Visto che s è un isomorfismo sulle spighe, in particolare è piatta. Mappe piatte di tipo finito su schemi localmente noetheriani sono aperte, quindi s è anche un'immersione aperta. □

Corollary 3.1.2 (5.3.3 di [Sza09])**.** *Sia $\varphi : X \to S$ un rivestimento étale finito, Z uno schema connesso e $\psi_1, \psi_2 : Z \to X$ due morfismi tali che $\varphi \circ \psi_1 = \varphi \circ \psi_2$. Se $p : \operatorname{Spec}\Omega \to Z$ è un punto geometrico di Z tale che $\psi_1(p) = \psi_2(p)$, allora $\psi_1 = \psi_2$.*

Proof. Sostituendo X con $X \times_S Z$, possiamo supporre $Z = S$ e che ψ_1, ψ_2 siano due sezioni di φ. Abbiamo quindi un rivestimento étale su una base connessa, vogliamo mostrare che se due sezioni che coincidono in un punto geometrico allora coincidono ovunque. Ma questo è immediato usando la proposizione precedente. □

Corollary 3.1.3 (5.3.4 di [Sza09])**.** *Se $X \to S$ è un rivestimento étale finito e connesso di grado n, gli elementi non banali di $\operatorname{Aut}(X/S)$ agiscono senza punti fissi sulle fibre geometriche di $X \to S$. In particolare, $\operatorname{Aut}(X/S)$ è finito e agisce transitivamente sulle fibre geometriche se e solo se $|\operatorname{Aut}(X/S)| = n$.*

Definition 3.1.4. *Un rivestimento étale finito e connesso $X \to S$ è di* Galois *se $\operatorname{Aut}(X/S)$ agisce transitivamente sulle fibre geometriche.*

Remark 3.1.5. Grazie al Theorem 3.1.3, per controllare che un rivestimento sia di Galois basta guardare una sola fibra geometrica.

Corollary 3.1.6 (5.3.7 di [Sza09])**.** *Sia $X \to S$ un rivestimento étale finito e connesso, $G \subseteq \operatorname{Aut}(X/S)$ un sottogruppo. Abbiamo una fattorizzazione*

$$X \to X/G \to S$$

dove tutte le mappe sono rivestimenti étale finiti. Se $X \to S$ è di Galois e $G = \operatorname{Aut}(X/S)$, allora $X/G \to S$ è un isomorofismo.

Proof. Localmente, se $X = \operatorname{Spec} A$ e $S = \operatorname{Spec} R$, X/G si costruisce come $\operatorname{Spec} A^G$. Ovviamente $X \to X/G$ è finita e surgettiva perché A è finito su R e quindi su A^G. Più complicato è dimostrare che A^G è finito su R, ma si fa, e quindi anche $X \to X/G$ è finita e surgettiva. La mappa al quoziente $X \to X/G$ è étale se e solo se l'azione di G sulle fibre geometriche è libera, che nel nostro caso è vero grazie al corollario precedente.

Visto che $X \to S$ è non ramificato e $X \to X/G$ è un rivestimento étale, segue che anche $X/G \to S$ è non ramificato (guardando le fibre). Similmente, la piattezza di $X/G \to S$ viene dall fatto che $X \to S$ è piatto e $X \to X/G$ fedelmente piatto.

Se $X \to S$ è di Galois e $G = \operatorname{Aut}(X/S)$, allora $X/G \to S$ è un rivestimento étale finito con fibre geometriche di cardinalità 1, quindi un isomorfismo. □

Proposition 3.1.7 (5.3.8 di [Sza09]). *Supponiamo di avere un diagramma di rivestimenti finiti e connessi*

$$\begin{array}{ccc} X & \xrightarrow{\pi} & Z \\ & \searrow^{\varphi} & \downarrow \psi \\ & & S \end{array}$$

dove $\varphi : X \to S$ è di Galois con gruppo $G = \mathrm{Aut}(X/S)$. Allora anche $X \to Z$ è di Galois con gruppo $H = \mathrm{Aut}(X/Z) \subseteq \mathrm{Aut}(X/S)$, in particolare $Z = X/H$.

Proof. Fissiamo un punto geometrico $z : \operatorname{Spec}\Omega \to Z$, e consideriamo due punti p, q nella fibra geometrica X_z. Per definizione di rivestimento di Galois, abbiamo un elemento $\sigma \in \mathrm{Aut}(X/S)$ tale che $\sigma(p) = q$. Grazie al Theorem 3.1.2, i due morfismi $\pi, \pi \circ \sigma : X \to Z$ sono uguali. Questo vuol dire che $\sigma \in \mathrm{Aut}(X/Z) \subseteq \mathrm{Aut}(X/S)$, e quindi l'azione di $\mathrm{Aut}(X/Z)$ su X è transitiva sulle fibre geometriche di $X \to Z$. □

Proposition 3.1.8 (5.3.9 di [Sza09]). *Sia $\varphi : X \to S$ un rivestimento étale finito e connesso. Allora esiste un morfismo $\pi : P \to X$ tale che $\varphi \circ \pi : P \to S$ è un rivestimento étale finito di Galois, e inoltre ogni S-morfismo da un rivestimento di Galois in X fattorizza attraverso π. Il rivestimento $P \to S$ è detto chiusura di Galois di $X \to S$.*

Proof. Consideriamo un punto geometrico $s : \operatorname{Spec}\Omega \to S$, e siano $\{x_1, \dots, x_n\}$ i punti della fibra geometrica X_s. Considerandoli una n-upla ordinata, ci danno un punto $x : \operatorname{Spec}\Omega \to X^n = X \times_S \cdots \times_S X$. Sia P la componente connessa di X^n contenente x. La composizione

$$\pi : P \to X^n \to X^{n-1} \to \dots X$$

è finita ed étale perché ciascuna mappa lo è, ed è surgettiva perché X è connesso e π ha immagina aperta e chiusa. Quindi π e $\varphi \circ \pi$ sono rivestimenti étale finiti.

Vogliamo ora vedere che $\mathrm{Aut}(P/S)$ agisce transitivamente sulla fibra di s. Sia

$$(x_{\sigma(1)}, \dots, x_{\sigma(n)}) : \operatorname{Spec}\Omega \to P \subseteq X^n$$

un elemento della fibra, dove $\sigma : \{1, \dots, n\} \to \{1, \dots, n\}$ è una funzione qualunque. Se mostriamo che σ è bigettiva, allora possiamo usare σ per permutare le coordinate di X^n ottenendo un automorfismo. Questo automorfismo manderebbe P in P, in quanto manda $(x_1, \dots, x_n)$ in $(x_{\sigma(1)}, \dots, x_{\sigma(n)})$, ed entrambi sono punti di P.

Supponiamo che σ non sia iniettiva, ad esempio $\sigma(1) = \sigma(2)$. Consideriamo $X = \Delta \subseteq X \times_S X$ la diagonale: grazie a Theorem 3.1.1, è un sottoschema aperto e chiuso. Quindi la proiezione sulle prime due coordinate $X^n \to X^2$ manda P sulla diagonale Δ: questo però è assurdo, perché il punto $(x_1, \dots, x_n)$ non mappa su Δ in quanto $x_1 \neq x_2$. □

3.2 Il gruppo fondamentale étale

Ora abbiamo tutti gli ingredienti per definire il gruppo fondamentale étale. In realtà la definizione potevamo darla fin dall'inizio, la differenza è che ora possiamo capirci qualcosa.

Fissiamo quindi uno schema S e un punto geometrico $s : \operatorname{Spec}\Omega \to S$. Chiamiamo Fet_S la categoria dei rivestimenti étale finiti di S, dove i morfismi sono dati dai morfismi di rivestimento. Abbiamo un funtore, detto *funtore fibra*, $F_s : \mathrm{Fet}_S \to \mathrm{Set}$ che associa ad ogni rivestimento étale $X \to S$ la fibra X_s. Allora $\pi_1(S,s)$ è semplicemente il gruppo degli automorfismi di F_s, cioé le trasformazioni naturali $F_s \to F_s$. Più concretamente, per ogni rivestimento $X \to S$ diamo una permutazione della fibra X_s e chiediamo che questa commuti con i morfismi di rivestimento $X' \to X$. Quindi $\pi_1(S,s)$ agisce naturalmente su ogni fibra X_s.

Detta così, non è molto chiaro a cosa serva. Ad esempio, non è chiaro che $\pi_1(S,s)$ non sia banale, anche avendo rivestimenti non banali di S.

Theorem 3.2.1 (Grothendieck)**.** *Sia S uno schema connesso, e $s : \operatorname{Spec}\Omega \to S$ un punto geometrico.*

1. *Il gruppo $\pi_1(S,s)$ è profinito, e la sua azione su X_s è continua per ogni rivestimento finito $X \to S$.*

2. *Il funtore F_s induce un'equivalenza fra Fet_S e la categoria degli insiemi finiti con un'azione continua di $\pi_1(S,s)$. Rivestimenti connessi corrispondono a insiemi con azione transitiva di $\pi_1(S,s)$, e rivestimenti di Galois corrispondono a quozienti finiti di $\pi_1(S,s)$.*

Example 3.2.2. Consideriamo il caso $S = \operatorname{Spec} k$, con k un campo. Un rivestimento étale di $\operatorname{Spec} k$ è semplicemente un'unione disgiunta di schemi della forma $\operatorname{Spec} L$, con L/k estensione finita e separabile. Il funtore fibra manda un rivestimento connesso $\operatorname{Spec} L$ in $\operatorname{Spec} L \otimes_k \Omega$, che è un insieme finito indicizzato dalle immersioni $L \to \Omega$. Queste immersioni hanno immagine contenuta nella chiusura separabile $k_s \subseteq \Omega$, e quindi $F_s(\operatorname{Spec} L) = \mathrm{Hom}_k(L, k_s)$. A questo punto è immediato vedere che $\pi_1(S,s) \simeq \mathrm{Gal}(k_s/k)$.

Remark 3.2.3. Supponiamo che esista un rivestimento étale universale, cioé un rivestimento $U \to S$ con un punto fissato $u : \operatorname{Spec}\Omega \to U$ nella fibra di s tale che, per ogni rivestimento $X \to S$ e $x \in X_s$, esiste un unico morfismo di rivestimenti $U \to X$ che manda u in x. Questo nei fatti non accadrà quasi mai, ma è comunque utile capire l'idea. Se U esiste, allora abbiamo per definizione un'identificazione funtoriale

$$F_s(X) = X_s = \mathrm{Hom}_S(U, X),$$

cioé il funtore fibra è rappresentabile, è un funtore $\mathrm{Hom}_S(U, -)$ per un certo oggetto $U \in \mathrm{Fet}_S$. A questo punto grazie al lemma di Yoneda gli autormofismi di F_s sono semplicemente gli automorfismi di U, cioé $\pi_S(S,s) = \mathrm{Aut}_S(U)$.

In generale non possiamo sperare di avere un rivestimento étale finito universale, perché avremo rivestimenti di grado arbitrariamente alto e quindi un rivestimento universale dovrebbe avere grado infinito. Nessun problema, anche se non c'è, ce lo inventiamo.

Definition 3.2.4. *Sia $\mathcal{C}$ una categoria, e $F : \mathcal{C} \to \mathrm{Set}$ un funtore. Diciamo che F è* pro-rappresentabile *se esiste un sistema proiettivo (P_i, φ_{ij}) in $\mathcal{C}$ indicizzato da un certo insieme parzialmente ordinato I e un isomorfismo funtoriale*

$$\varinjlim \mathrm{Hom}(P_i, X) \simeq F(X)$$

per ogni X in $\mathcal{C}$.

Proposition 3.2.5 (5.4.6 di [Sza09])**.** *Sotto le ipotesi del teorema, il funtore fibra F_s è pro-rappresentabile.*

Proof. Prendiamo come insieme I l'insieme di tutti i rivestimenti di Galois $P_i \to S$, e diciamo che $i \leq j$ se abbiamo un morfismo di rivestimenti $P_j \to P_i$. Questo insieme parzialmente ordinato è diretto, cioè per ogni coppia di rivestimenti di Galois P_i, P_j c'è un terzo rivestimento di Galois P_k con morfismi $P_k \to P_i$, $P_k \to P_j$. Per mostrarlo, consideriamo una componente connessa $X \subseteq P_i \times_S P_j$, è un rivestimento di S, la chiusura di Galois $P_k \to S$ costruita in Theorem 3.1.8 ha morfismi di rivesimento su P_i e P_j.

Ora che abbiamo gli oggetti del sistema inverso, dobbiamo scegliere un morfismo φ_{ij} per ogni $i \geq j$: tale morfismo esiste per come abbiamo definito l'ordine parziale, ma non è unico. Per ogni l, scegliamo un punto p_l nella fibra geometrica $F_s(P_i)$. Prendiamo un qualunque morfismo di rivestimenti $\varphi : P_i \to P_j$, visto che $P_j \to S$ è di Galois componendolo con un automorfismo di P_j troviamo un unico morfismo di rivestimenti φ_{ij} tale che $\varphi_{ij}(p_i) = p_j$, l'unicità viene da Theorem 3.1.2. Grazie all'unicità, è immediato verificare che se $k \leq i \leq j$ allora $\varphi_{ij} \circ \varphi_{ki} = \varphi_{kj}$.

Per ogni rivestimento $X \to S$, vogliamo ora dare un isomorfismo

$$\varinjlim \mathrm{Hom}_S(P_i, X) \simeq F_s(X)$$

funtoriale in X. Un elemento del limite diretto $\varinjlim \mathrm{Hom}_S(P_i, X)$ è semplicemente un elemento $\psi \in \mathrm{Hom}_S(P_{i_0}, X)$ per qualche i_0, questo ci dà un elemento $\psi(p_{i_0})$ in $F_s(X)$. Visto che $\varphi_{ij}(p_i) = p_j$, è immediato verificare che l'elemento di $F_s(X)$ non dipende dalla scelta di i_0.

L'iniettività della mappa $\varinjlim \mathrm{Hom}_S(P_i, X) \to F_s(X)$ è data dall'unicità delle mappe di rivestimenti puntati (vedi Theorem 3.1.2), mentra la surgettività è l'esistenza della chiusura di Galois (vedi Theorem 3.1.8). La funtorialità in X è ovvia. □

Una volta che sappiamo che il funtore fibra è pro-rappresentato da (P_i, φ_{ij}), per il lemma di Yoneda abbiamo che gli automorfismi del funtore fibra corrispondono agli automorfismi di (P_i, φ_{ij}), che sono $\varprojlim \mathrm{Aut}(P_i/S)$. Gli automorfismi di P_i però si compongono a destra, e quindi otteniamo

$$\pi_1(S, s) \simeq \varprojlim \mathrm{Aut}(P_i/S)^{\mathrm{op}}.$$

Abbiamo così ottenuto una presentazione di $\pi_1(S,s)$ come gruppo profinito, ma come agisce sulle fibre di un rivestimento $X \to S$? Se $g \in \pi_1(S,s)$ e $x \in X_s$, per Theorem 3.2.5 esiste un rivestimento di Galois $P_i \to S$ con un morfismo di rivestimenti $\psi : P_i \to X$ che manda p_i in x. L'elemento g proietta su un automorfismo g' di P_i, l'azione di g su x sarà data allora da

$$g \cdot x = \psi \circ g'(p_i) \in X_s$$

Quindi l'azione di $\pi_1(S,s)$ su X_s spezza attraverso un quoziente finito, ed è di conseguenza continua. Inoltre è evidente che, perché l'azione sia transitiva, è necessario e sufficiente che X sia connesso: intanto $\pi_1(S,s)$ mappa surgettivamente sui gruppi di automorfismi di rivestimenti di Galois (perché tutte le mappe di transizione nel sistema proiettivo sono surgettive), quindi agisce transitivamente sulla fibra di dei rivestimenti di Galois, si conclude poi notando che $P_i \to X$ surietta su una componente connessa. Se X è connesso, è evidente che lo stabilizzatore di x è normale in $\pi_1(S,s)$ se e solo se $X \to S$ è di Galois.

Prendiamo ora un insieme finito A con un'azione continua di $\pi_1(S,s)$, vogliamo trovare un rivestimento $X \to S$ tale che $X_s \simeq A$ come $\pi_1(S,s)$-insiemi. Grazie a quanto osservato prima sui rivestimenti connessi, basta fare il caso in cui l'azione su A è transitiva. Poiché l'azione è continua, esiste un rivestimento di Galois P_i tale che l'azione su A spezza attraverso P_i. Fissiamo un elemento $a \in A$, e consideriamo lo stabilizzatore $H \subseteq \mathrm{Aut}(P_i/S)$ di a. Chiamiamo X il quoziente P_i/H, sappiamo che è un rivestimento di S. Visto che l'azione su A è transitiva, abbiamo isomorfismi di $\pi_1(S,s)$ insiemi

$$X_s \simeq \mathrm{Aut}(P_i/S)/H \simeq A$$

da cui concludiamo la dimostrazione di Theorem 3.2.1.

Theorem 3.2.6. *Il gruppo fondamentale étale definisce un funtore dalla categoria degli schemi puntati alla categoria dei gruppi profiniti.*

Proof. Dato un morfismo di schemi puntati $(X,x) \to (Y,y)$, dobbiamo dare un morfismo $\pi_1(X,x) \to \pi_1(Y,y)$. Grazie al Theorem 3.2.1, per fare questo è sufficiente far agire $\pi_1(X,x)$ sulla fibra dei rivestimenti étale di Y. Ma questo è immediato: dato un rivestimento étale $Y' \to Y$, e detto $X' \to X$ il pullback a X, abbiamo un'identificazione naturale tra le fibre geometriche $X'_x \simeq Y'_y$ e quindi $\pi_1(X,x)$ agisce su Y'_y.

Il fatto che $\pi_1(X,x) \to \pi_1(Y,y)$ sia funtoriale in X e Y è una semplice verifica. □

3.3 Alcune proprietà

Mostriamo ora un po' di risultati di base sul gruppo fondamentale. Innanzitutto, vediamo che cambiando punto base abbiamo un isomorfismo.

Proposition 3.3.1. *Sia S uno schema connesso, e $s : \mathrm{Spec}\,\Omega \to S$, $t : \mathrm{Spec}\,\Omega' \to S$ due punti geometrici. Allora esiste un isomorfismo non canonico $\pi_1(S,s) \simeq \pi_1(S,t)$.*

Proof. Per mostrare l'isomorfismo, è sufficiente mostrare che sono isomorfi i funtori fibra, cioè $F_s \simeq F_t$. Grazie a Theorem 3.2.5, sappiamo che il funtore fibra F_s è prorappresentato dal sistema (P_i, φ_{ij}) dei rivestimenti di Galois. Analogamente F_t sarà prorappresentato da (P_i, ψ_{ij}): i rivestimenti di Galois sono gli stessi, ma φ_{ij} può essere diversa da ψ_{ij}. Ricordiamo che abbiamo una scelta di due punto p_i, q_i rispettivamente nella fibra di s e t, che che φ_{ij}, ψ_{ij} sono caratterizzati da $\varphi_{ij}(p_i) = p_j$, $\psi_{ij}(q_i) = q_j$.

L'isomorfismo che cerchiamo è non canonico, bisogna fare una scelta: la facciamo ora. Per ogni i, scegliamo un punto p'_i nella fibra di s in modo tale che siano compatibili con i morfismi ψ_{ij}, cioè $\psi_{ij}(p'_i) = p'_j$: questo può essere fatto scegliendo i p'_i uno alla volta su rivestimenti sempre più grandi. Ora definiamo $\alpha_i : P_i \to P_i$ come l'unico automorfismo di rivestimenti tale che $\alpha_i(p_i) = p'_i$. Affermo che $(\alpha_i)_i$ dà un isomorfismo $\alpha : (P_i, \varphi_{ij}) \to (P_i, \psi_{ij})$. Questo vuol dire semplicemente che, per ogni $i \geq j$, il seguente diagramma commuta

$$\begin{array}{ccc} P_i & \xrightarrow{\alpha_i} & P_i \\ \downarrow{\scriptstyle \varphi_{ij}} & & \downarrow{\scriptstyle \psi_{ij}} \\ P_j & \xrightarrow{\alpha_j} & P_j \end{array}$$

Siccome tutti i morfismi in gioco sono morfismi di rivestimenti étale connessi, grazie a Theorem 3.1.2 basta verificare che le composizioni coincidono su un punto geometrico. In particolare,

$$\psi_{ij} \circ \alpha_i(p_i) = \psi_{ij}(p'_i) = p'_j$$
$$\alpha_j \circ \varphi_{ij}(p_i) = \alpha_j(p_j) = p'_j.$$

□

Remark 3.3.2. Nella proposizione precedente abbiamo costruito un isomorfismo non canonico tra i funtori fibra $F_s \simeq F_t$. Tale isomorfismo viene chiamato *cammino* da s a t: in topologia classica, un cammino tra due punti può essere sollevato ai rivestimenti, dando appunto un isomorfismo fra i funtori fibra.

Scegliamo ora due cammini (cioè due isomorfismi) diversi $\mu, \nu : F_s \to F_t$. La composizione

$$\lambda = \mu^{-1} \circ \nu$$

è un automorfismo di F_s, cioé un elemento di $\pi_1(S, s)$. L'isomorfismo $\varphi_\mu : \pi_1(S, s) \to \pi_1(S, t)$ definito da μ è

$$g \mapsto \mu \circ g \circ \mu^{-1},$$

e analogamente per ν. Da un calcolo diretto otteniamo quindi

$$\varphi_\nu(g) = \varphi_\mu(\lambda g \lambda^{-1}),$$

cioè che i due isomorfismi differiscono per un automorfismo interno di $\pi_1(S, s)$.

Vogliamo ora studiare come si comporta il gruppo fondamentale rispetto ai morfismi che tengono fisso il punto base.

Proposition 3.3.3. *Siano $(S, s), (S', s')$ due schemi connessi puntati, e $\varphi : S' \to S$ un morfismo tale che $\varphi(s') = s$. Chiamiamo $\varphi_* : \pi_1(S', s') \to \pi_1(S, s)$ l'omomorfismo indotto.*

1. *φ_* è banale se e solo se, per ogni rivestimento $X \to S$, $X \times_S S' \to S'$ è un rivestimento banale, cioè unione disgiunta di copie di S'.*

2. *φ_* è surgettivo se e solo se, per ogni rivestimento connesso $X \to S$, $X \times_S S'$ è ancora connesso.*

3. *φ_* è iniettivo se e solo se, per ogni rivestimento connesso $X' \to S'$, esiste un rivestimento $X \to S$ e un morfismo $X_i \to X'$ di rivestimenti di S', dove X_i è una componente connessa di $X \times_S S'$ (cioè i rivestimenti di S' provenienti da S sono cofinali in $\mathrm{Fet}_{S'}$).*

Proof. Ricordiamo brevemente come è definito φ_*: facciamo agire $\pi_1(S', s')$ sul funtore fibra di (S, s) prendendo il pullback dei rivestimenti di S. Usiamo la caratterizzazione di Theorem 3.2.1 che ci dice che il funtore fibra ci dà un'equivalenza di categorie tra la categoria dei rivestimenti di S e gli insiemi finiti con azione continua del gruppo fondamentale.

1. Dire che i rivestimenti di S diventano banali dopo il pullback a S' è equivalente a dire che per ogni insieme finito A con azione continua di $\pi_1(S, s)$, l'azione di $\pi_1(S', s')$ tramite φ_* è banale, e questo è equivalente a dire che φ_* è banale.

2. Dire il pullback di rivestimenti connessi è connesso è equivalente a dire che, se l'azione di $\pi_1(S, s)$ su un insieme finito A è continua e transitiva, l'azione di $\pi_1(S', s')$ tramite φ_* è ancora transitiva, e questo è equivalente a dire che φ_* è suriettivo.

3. La condizione è equivalente a chiedere che per ogni insieme finito A' con azione continua di $\pi_1(S', s')$ esiste un insieme finito A con azione continua di $\pi_1(S, s)$ e una mappa equivariante $A_i \to A'$, dove A_i è un sottoinsieme di A su cui $\pi_1(S', s')$ agisce transitivamente.

   Se $g' \in \pi_1(S', s')$ è diverso da 0, esiste un insieme A' con azione transitiva di $\pi_1(S', s')$ tale che l'azione di g' è non banale. Per ipotesi abbiamo un insieme finito A con azione di $\pi_1(S, s)$ e mappa equivariante $A_i \to A'$. Visto che l'azione su A' è transitiva, la mappa $A_i \to A'$ è surgettiva, e quindi g' agisce non banalmente anche su A_i. Di conseguenza, g' ha immagine non banale in $\pi_1(S, s)$.

   Il viceversa è più complesso e non lo dimostriamo, si può trovare in [Sza09, Corollary 5.5.8].

□

Corollary 3.3.4. *Siano $(S'', s'') \to (S', s') \to (S, s)$ morfismi di schemi connessi e puntati. La sequenza*

$$\pi_1(S'', s'') \to \pi_1(S', s') \to \pi_1(S, s)$$

è esatta se e solo se:

1. *per ogni rivestimento $X \to S$, il pullback $X \times_S S''$ è banale,*

2. *dato un rivestimento connesso $X' \to S'$ tale che $X' \times_{S'} S''$ ha una sezione su S'', esiste un rivestimento connesso $X \to S$ e un morfismo da una componente connessa di $X \times_S S'$ a X'.*

Proof. La prima condizione è equivalente a dire che la composizione dei due morfismi è 0. Per la seconda condizione rimandiamo a [Sza09, Corollary 5.5.9]. □

Abbiamo ora tutti gli strumenti per costruire la sequenza esatta di omotopia. Prendiamo uno schema X noetheriano su un campo k. Intuitivamente, possiamo pensare al morfismo $X \to \operatorname{Spec} k$ come a una fibrazione a fibra $X_{k_s} := X \times_{\operatorname{Spec} k} \operatorname{Spec} k_s$, dove k_s è una chiusura separabile di k. In topologia algebrica, quando ho una fibrazione questa mi dà una successione esatta lunga dei gruppi di omotopia. Qua succede una cosa analoga, esiste una sequenza esatta

$$1 \to \pi_1(X_{k_s}, \overline{x}) \to \pi_1(X, \overline{x}) \to \operatorname{Gal}(k_s/k) \to 1.$$

Il fatto che ci troviamo con una sequenza esatta corta e non lunga come in topologia è, sempre intuitivamente, conseguenza del fatto che X_{k_s} è connesso e quindi $\pi_0(X_{k_s}, \overline{x})$ è banale, mentre $\operatorname{Spec} k$ non ha omotopia in grado maggiore di uno perché il suo rivestimento universale $\operatorname{Spec} k_s$ è "veramente un punto" dal punto di vista dell'omotopia étale (al contrario di $\operatorname{Spec} k$), e quindi contraibile. Ma bando alle ciance, e dimostriamo qualcosa.

Abbiamo innanzitutto bisogno di un lemma preliminare.

Lemma 3.3.5. *Sia X uno schema di tipo finito su k, K/k un'estensione di campi qualunque, $Y \to X_K$ un morfismo di tipo finito. Allora esiste una sottoestensione $K/L/k$ finitamente generata su k e Z uno schema di tipo finito su L con un morfismo $Z \to X_L$ tale che $Z_K \simeq Y$ e tale che $Y \to X_K$ è il pullback di $Z \to X_L$.*

$$\begin{array}{ccc} Y & \longrightarrow & Z \\ \downarrow & \square & \downarrow \\ X_K & \longrightarrow & X_L \end{array}$$

Inoltre, se $L' \subseteq K$ è un'altra sottoestensione finitamente generata e $Z' \to X_{L'}$ è un altro morfismo che rispetta le condizioni di sopra, allora esiste un estensione finitamente generata $L'' \subseteq K$ contenente sia L che L' con un isomorfismo $Z_{L''} \simeq Z'_{L''}$ che fa commutare il diagramma

$$\begin{array}{ccc} Z_{L''} & \xrightarrow{\sim} & Z'_{L''} \\ \downarrow & & \downarrow \\ X_{L''} & = & X_{L''} \end{array}$$

Proof. Posso scrivere X come unione finita di aperti affini $X = \bigcup_i U_i = \bigcup_i \operatorname{Spec} A_i$ dove

$$A_i = k[x_1, \dots, x_n]/(f_1, \dots, f_r)$$

è una k-algebra finitamente generata per ogni i. Considero $U_{i,K} = \operatorname{Spec} A_i \otimes_k K = \operatorname{Spec} K[x_1, \dots, x_n]/(f_1, \dots, f_r)$ e le controimmagini $V_i \subseteq Y$. Nuovamente, posso ricoprire V_i con un numero finito di aperti affini $V_{i,j} = \operatorname{Spec} B_{i,j}$ dove $B_{i,j}$ è un'algebra finitamente generata su $A_i \otimes_k K$. Quindi $B_{i,j}$ è della forma

$$B_{i,j} = K[x_1, \dots, x_n, y_1, \dots, y_m]/(f_1, \dots, f_r, g_1 \dots, g_s)$$

dove i polinomi f sono nelle variabili x e coefficienti in k, mentre i polinomi g sono nelle variabili x e y e coefficienti in K.

Prendo $L \subseteq K$ l'estensione di k generata da tutti i coefficienti dei g_l al variare di i e j. Essendo un numero finito di polinomi, sono in numero finito. Questo ci dà degli anelli $B_{i,j,L}$ che sono estensioni finitamente generate di $A_i \otimes_k L$. Per costruire il nostro schema $Y' \to X_L$, ci mancano ancora le condizioni di incollamento per gli schemi $\operatorname{Spec} B_{i,j,L}$, ma anche queste si sistemano con un numero finito di coefficienti, e quindi a meno di allargare ulteriormente L si conclude.

La parte sull'unicità si dimostra in modo analogo. □

Remark 3.3.6. Nel lemma precedente, se K/k è un'estensione algebrica, la sottoestensione $L \subseteq K$ trovata è automaticamente finita su k.

Proposition 3.3.7. *Sia X uno schema noetheriano geometricamente connesso su k. Fissiamo una chiusura algebrica $\overline{k}/k$, e consideriamo la chiusura separabile $k_s \subseteq \overline{k}$. Sia $X_{k_s} = X \times_{\operatorname{Spec} k} \operatorname{Spec} k_s$ e fissiamo un punto geometrico $\overline{x}$ di X_{k_s} a valori in $\overline{k}$. La sequenza di gruppi profiniti*

$$1 \to \pi_1(X_{k_s}, \overline{x}) \to \pi_1(X, \overline{x}) \to \operatorname{Gal}(k_s/k) \to 1$$

è esatta.

Proof. La dimostrazione è essenzialmente un'applicazione dei criteri visti precedentemente nei Theorem 3.3.3 e Theorem 3.3.4. Procediamo con ordine.

- $\pi_1(X_{k_s}, \overline{x}) \to \pi_1(X, \overline{x})$ è iniettiva. Dobbiamo mostrare che per ogni rivestimento étale connesso $\overline{Y} \to X_{k_s}$, esiste un rivestimento $Y \to X$ e un morfismo di rivestimenti $Y' \to \overline{Y}$, dove Y' è una componente connessa di $Y \times_X X_{k_s} = Y_{k_s}$, cioè che possiamo "dominare" ogni rivestimento di X_{k_s} con una componente di un rivestimento proveniente da X.

  Per far questo, basta notare che, grazie al Theorem 3.3.5, esiste un'estensione finita e separabile L/k e un morfismo $Y \to X_L$ tale che, cambiando base a k_s, diventa $\overline{Y} \to X_{k_s}$. Il fatto che $\overline{Y} \to X_{k_s}$ sia un rivestimento étale finito implica per verifica diretta che anche $Y \to X_L$ è un rivestimento étale finito, e quindi anche la composizione $Y \to X$. Ora, se consideriamo $Y \times_X X_{k_s}$, questo è isomorfo a $Y \times_{\operatorname{Spec} k} (\operatorname{Spec} L \times_{\operatorname{Spec} k} \operatorname{Spec} k_s)$, e cioé d copie di $\overline{Y}$ dove d è il grado di L/k, da cui si conclude.

- Vediamo ora l'esattezza al centro, usando il Theorem 3.3.4. La prima condizione da verificare è che un rivestimento di $\operatorname{Spec} k$, portato a $\overline{X}$, diventi banale. Questo però è ovvio, in quanto i rivestimenti connessi di $\operatorname{Spec} k$ sono semplicemente estensioni finite e separabili L/k, e queste diventano banali già su $\operatorname{Spec} k_s$ e a maggior ragione su $\overline{X}$.

  La seconda condizione da verificare, più sottile, è che se $Y \to X$ è un rivestimento connesso il cui pullback $Y_{k_s} \to X_{k_s}$ ha una sezione $X_{k_s} \to Y_{k_s}$, allora esiste un'estensione finita e separabile L/k ed un morfismo di rivestimenti $X_L \to Y$. Ma dare un morfismo di rivestimenti $X_L \to Y$ è come dare una sezione di $Y_L \to X_L$, e noi abbiamo una sezione di $Y_{k_s} \to X_{k_s}$, e quindi si conclude applicando nuovamente il Theorem 3.3.5.

- Mostriamo infine la suriettività di $\pi_1(X, \overline{x}) \to \operatorname{Gal}(k_s/k)$. Notiamo che non abbiamo ancora usato l'ipotesi X geometricamente connesso, come in effetti ci aspettiamo dall'interpretazione topologica. Grazie a Theorem 3.3.3, questo è equivalente a chiedere che i rivestimenti connessi di $\operatorname{Spec} k$, tirati indietro a X, siano ancora connessi, e questo è precisamente il fatto che X sia geometricamente connesso.

□

Remark 3.3.8. Nel libro di Szamuely, viene usata l'ipotesi ulteriore che X sia geometricamente integro, che usa nel mostrare l'esattezza al centro. Questo gli permette sostanzialmente di ricondurre la dimostrazione a fatti di teoria dei campi, ma mi pare che anche la nostra dimostrazione funzioni.

Dimostrata la Theorem 3.3.7, val la pena spendere qualche minuto per enunciare uno dei problemi aperti più grossi riguardanti il gruppo fondamentale (e anche perché i metodi di Kim servirebbero proprio anche per questo problema aperto).

Sia $y \in X(k)$ un punto razionale, e $\overline{y}$ il punto geometrico associato. Per funtorialità del gruppo fondamentale, abbiamo una mappa $\operatorname{Gal}(k_s/k) \to \pi_1(X, \overline{y})$. Ci piacerebbe dire che questo morfismo dà una sezione della sequenza esatta corta appena vista, ma questo non è così immediato, perché abbiamo due punti base diversi, $\overline{x}$ e $\overline{y}$. Scegliamo quindi un cammino da $\overline{y}$ in $\overline{x}$, cioè un isomorfismo dei funtori fibra, questo ci dà un isomorfismo non canonico $\pi_1(X, \overline{y}) \simeq \pi_1(X, \overline{x})$. La composizione

$$\operatorname{Gal}(k_s/k) \to \pi_1(X, \overline{y}) \simeq \pi_1(X, \overline{x})$$

è una sezione, perché il seguente diagramma commuta

$$\begin{array}{ccc} \pi_1(X, \overline{y}) & \longrightarrow & \pi_1(X, \overline{x}) \\ & \searrow \quad \swarrow & \\ & \operatorname{Gal}(k_s/k) & \end{array}$$

Se cambiamo il cammino da $\overline{y}$ a $\overline{x}$, la sezione cambia per un automorfismo interno di $\pi_1(X, \overline{x})$. In realtà, il fatto che y sia un punto razione ci dice che l'automorfismo è definito da un elemento di $\pi_1(X_{k_s}, \overline{x})$.

Abbiamo quindi una funzione

$$X(k) \to \{\text{sezioni di } \pi_1(X, \overline{x}) \to \mathrm{Gal}(k_s/k)\}/\sim$$

dove consideriamo due sezioni equivalenti se differiscono per un automorfismo interno.

Conjecture 3.3.9. *(Congettura della sezione di Grothendieck) Sia X una curva proiettiva liscia e geometricamente connessa di genere almeno 2 su campo k finitamente generato su $\mathbb{Q}$. Allora la mappa*

$$X(k) \to \{\textit{sezioni di } \pi_1(X, \overline{x}) \to \mathrm{Gal}(\overline{k}/k)\}/\sim$$

è bigettiva.

Se la congettura è vera, abbiamo un modo di ricostruire i punti di una curva di genere almeno 2 guardando solo il gruppo fondamentale. Si sa che la mappa definita sopra è iniettiva per genere maggiore o uguale a 1, e che non può essere surgettiva in genere 1 appena la curva ellittica ha rango positivo. L'idea di Grothendieck è che, da genere 2, la struttura "anabeliana" (i.e. molto poco abeliana) del gruppo fondamentale impone restrizioni troppo forti all'esistenza di sezioni.

Andiamo avanti con le proprietà del gruppo fondamentale. D'ora in poi a volte tralascerò di scrivere il punto base, tornando a specificarlo quando fosse rilevante.

Proposition 3.3.10. *Sia k un campo algebricamente chiuso, e X, Y schemi connessi e noetheriani su k, con inoltre X proprio. Il morfismo naturale*

$$\pi_1(X \times Y) \to \pi_1(X) \times \pi_1(Y)$$

è un isomorfismo.

Proof. Diamo solo un'idea della dimostrazione. L'omomorfismo $\pi_1(X \times Y) \to \pi_1(X) \times \pi_1(Y)$ può essere inserito in un diagramma commutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \pi_1(X) & \longrightarrow & \pi_1(X \times Y) & \longrightarrow & \pi_1(Y) & & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \pi_1(X) & \longrightarrow & \pi_1(X) \times \pi_1(Y) & \longrightarrow & \pi_1(Y) & \longrightarrow & 0 \end{array}$$

dove la mappa $\pi_1(X) \to \pi_1(X \times Y)$ è data dal punto base di Y che induce una sezione $X \to X \times Y$. La riga inferiore è ovviamente esatta, si dimostra che lo è anche quella superiore in maniera simile a quanto fatto in Theorem 3.3.7. Si applica quindi il lemma dei 5 per ottenere che la mappa verticale al centro è un isomorfismo. □

Remark 3.3.11. Nella proposizione precedente è fastidioso che sia necessaria l'ipotesi X proprio, visto che in topologia non è così. La dimostrazione dell'esattezza della riga in alto, però, si basa pesantemente su quest'ipotesi, non vedo modo di farne a meno.

Proposition 3.3.12. *Sia $k \subseteq K$ un'estensione di campi algebricamente chiusi, e X uno schema proprio e connesso su k. La mappa naturale $\pi_1(X_K) \to \pi_1(X)$ è un isomorfismo.*

Proof. La suriettività è semplice: basta mostrare che il pullback di rivestimenti connessi è connesso. Ma è un fatto generale che, una volta che uno schema è connesso su un campo algebricamente chiuso, il suo pullback su qualunque campo è ancora connesso.

Per l'iniettività, dobbiamo mostrare che i rivestimenti di X_K provenienti da X sono cofinali. L'idea è semplice: vorremmo applicare Theorem 3.3.10 per ottenere $\pi_1(X_K) \simeq \pi_1(X) \times \pi_1(\operatorname{Spec} K) \simeq \pi_1(X)$. Questo però non è fattibile, perché K non è noetheriano su k. L'idea è allora ricondursi a una sottoestensione finitamente generata di K, fare uno spreading out, applicare Theorem 3.3.10 e tornare a restringersi ai campi di funzioni.

Prendiamo quindi un rivestimento connesso $Y \to X_K$. Grazie al Theorem 3.3.5, troviamo una sottoestensione finitamente generata $k' \subseteq K$ e un rivestimento étale $Y' \to X_{k'}$ tale che $Y \simeq Y' \times_{\operatorname{Spec} k'} \operatorname{Spec} K$. Possiamo trovare uno spreading out $\mathcal{Y} \to X \times_k T$ dove T è uno schema di tipo finito su k, integro, con campo delle funzioni $k(T) = k'$ e tale che $Y' \to X_{k'}$ è la fibra generica di $\mathcal{Y} \to X \times_k T$. A patto di rimpicciolire T, possiamo supporre che $\mathcal{Y} \to X \times_k T$ sia ancora un rivestimento étale. Visto che X è proprio, possiamo applicare Theorem 3.3.10 e abbiamo $\pi_1(X \times T) \simeq \pi_1(X) \times \pi_1(T)$. Questo ci dice che possiamo dominare il rivestimento $\mathcal{Y} \to X \times_k T$ con una coppia di rivestimenti $Z \to X$, $T' \to T$,

$$Z \times T' \to \mathcal{Y} \to X \times T.$$

Restringiamoci quindi al punto generico di T, abbiamo

$$Z \times \operatorname{Spec} k(T') \to Y' \to X_{k'}.$$

Estendiamo ora il campo base da k' a K, e otteniamo

$$Z \times \operatorname{Spec}(k(T') \otimes_{k'} K) \to Y \to X_K$$

dove $k(T') \otimes_{k'} K$ è un prodotto di copie di K, in quanto $k(T')$ è finito su $k' = k(T)$ e K è algebricamente chiuso. Scegliendo una di queste copie, otteniamo un morfismo $Z_K \to Y$, come desiderato. □

Dato uno schema di tipo finito su $\mathbb{C}$, è possibile definire lo spazio analitico associato X^{an}.

Theorem 3.3.13. *Sia X uno schema connesso di tipo finito su $\mathbb{C}$. Il funtore $(Y \to X) \mapsto (Y^{\mathrm{an}} \to X^{\mathrm{an}})$ che associa a un rivestimento $Y \to X$ il rivestimento di spazi analitici associato induce un'equivalenza fra la categoria dei rivestimenti étale finiti di X e la categoria dei rivestimenti finiti di X^{an}. Di conseguenza, abbiamo un isomorfismo indotto*

$$\widehat{\pi_1^{\mathrm{top}}(X^{\mathrm{an}})} \simeq \pi_1(X)$$

dove il termine a sinistra è il completamento profinito del gruppo fondamentale topologico di X^{an}.

Proof. Essenzialmente, è il teorema di esistenza di Riemann. Vedi [sga03, Exposé XII, Corollaire 5.2]. □

Grazie al Theorem 3.3.13, alla Theorem 3.3.12 e alla Theorem 3.3.7, nel caso di campi di caratteristica 0 è sempre possibile esprimere il gruppo fondamentale étale in maniera abbastanza esplicita: otterremo sempre un'estensione del completamento profinito di un gruppo fondamentale topologico con il gruppo di Galois assoluto del campo base.

Concludiamo quest'introduzione con il calcolo del gruppo fondamentale nel caso di varietà abeliane. Potremmo anche limitarci alla strategia appena mostrata, ma almeno in questo caso relativamente semplice è utile sporcarsi un po' le mani (oltre al fatto che funziona anche in caratteristica positiva).

Proposition 3.3.14. *Sia A una varietà abeliana su un campo algebricamente chiuso k. Dato un rivestimento connesso $\varphi : Y \to A$, possiamo dare allo schema Y una struttura di varietà abeliana tale che φ sia un omomorfismo.*

Proof. È sufficiente fare il caso in cui $Y \to A$ sia un rivestimento di Galois. Supponiamo non lo sia, e prendiamo la chiusura di Galois $Y' \to Y \to A$. Supponendo di aver dimostrato la proposizione nel caso di un rivestimento di Galois, Y' è una varietà abeliana e $Y' \to A$ è un isomorfismo. Ora, il gruppo degli automorfismi $\mathrm{Aut}(Y'/A)$ è chiaramente isomorfo a $\ker(Y' \to A)$ che è abeliano, ma allora tutti i suoi sottogruppi sono normali, di conseguenza $Y \to A$ era già un rivestimento di Galois.

Supponiamo quindi che $Y \to A$ sia un rivestimento di Galois con gruppo di automorfismi $G = \mathrm{Aut}(Y/A)$. Consideriamo la mappa di moltiplicazione $m_A : A \times A \to A$, e prendiamo il pullback di Y lungo m_A:

$$\begin{array}{ccc} Y' = (A \times A) \times_A Y & \longrightarrow & Y \\ \downarrow & & \downarrow \varphi \\ A \times A & \xrightarrow{m_a} & A \end{array}$$

Y' è connessa: infatti Y è connessa e tutte le fibre di $Y' \to Y$ sono connesse, perché sono isomorfe a copie di A.

Quindi $Y' \to A \times A$ è un rivestimento di Galois con gruppo di automorfismi $G = \mathrm{Aut}(Y/A)$. Grazie al fatto che $\pi_1(A \times A) \simeq \pi_1(A) \times \pi_1(A)$, abbiamo una coppia di rivestimenti di Galois $Z_1 \to A$, $Z_2 \to A$ con gruppi di automorfismi G_1, G_2 e un morfismo di rivestimenti $Z_1 \times Z_2 \to Y' \to A \times A$ corrispondente a un morfismo surgettivo $G_1 \times G_2 \to G$. Sia H il ker di tale morfismo, a meno di sostituire Z_i con $Z_i/(H \cap G_i)$, possiamo supporre che $G_i \to G$ sia iniettiva.

Quindi i G_i possono essere identificati con due sottogruppi di G che commutano fra di loro e che lo generano. Ma se restringiamo tutto a $A \times \{0\}$ otteniamo un diagramma

del tipo

$$\begin{array}{ccccc} Z_1 \times G_2 & \longrightarrow & Z_1 \times Z_2 & & \\ \downarrow & & \downarrow & & \\ Y & \longrightarrow & Y' & \longrightarrow & Y \\ \downarrow & & \downarrow & & \downarrow \\ A \times \{0\} & \longrightarrow & A \times A & \longrightarrow & A \end{array}$$

e $Z_1 \to A$ ha gruppo di automorfismi G_1, quindi in realtà $G_1 = G$. Lo stesso vale per G_2, da cui otteniamo che G è commutativo. Inoltre abbiamo isomorfismi $Z_i \simeq Y$ e una mappa $m_Y : Y \times Y \to Y' \to Y$. Fissiamo un punto $0_Y \in Y$ sopra $0_A \in A$. Modificando m_Y per un automorfismo di Y, possiamo supporre $m_Y(0_Y, 0_Y) = 0_Y$. A questo punto è fatta: dobbiamo solo verificare che m_Y rispetta associatività, inverso, identità, commutatività. Vediamo ad esempio l'associatività, le altre sono analoghe.

Abbiamo due morfismi $Y \times Y \times Y \to Y$, il primo moltiplica prima le due coordinate, il secondo moltiplica prima le ultime due. La due composizioni $Y \times Y \times Y \to Y \to A$ sono uguali, perché m_A è associativa. Visto che $Y \to A$ è un rivestimento, basta quindi verificare che i due morfismi coincidono in un punto, ad esempio $(0_Y, 0_Y, 0_Y)$. □

Corollary 3.3.15. *Sia n un intero multiplo del grado di φ. Allora c'è una mappa $\psi : A \to Y$ e un diagramma commutativo*

$$\begin{array}{ccc} A & \xrightarrow{\psi} & Y \\ & \searrow^{n_A} & \downarrow \varphi \\ & & A \end{array}$$

Proof. Consideriamo il morfismo di moltiplicazione $n_Y : Y \to Y$, per ipotesi $\ker \varphi \subseteq \ker n_Y = Y[n]$, quindi n_Y induce un morfismo $\psi : Y/\ker \varphi \simeq A \to Y/Y[n] \simeq Y$ che soddisfa $\psi \circ \varphi = n_Y$. Consideriamo la composizione $\varphi \circ \psi \circ \varphi : Y \to A$, abbiamo

$$\varphi \circ \psi \circ \varphi = \varphi \circ n_Y = n_A \circ \varphi$$

dove $\varphi \circ n_Y = n_A \circ \varphi$ perché φ è un omomorfismo. Ma allora $\varphi \circ \psi = n_A$, perché φ è un rivestimento étale e i due morfismi coincidono in 0_A. □

Abbiamo quindi (quasi) dimostrato il seguente teorema.

Theorem 3.3.16. *Sia A una varietà abeliana su un campo algebricamente chiuso. Il gruppo fondamentale di A è commutativo, e c'è un isomorfismo naturale*

$$\pi_1(A) \simeq T(A) = \prod_l T_l(A)$$

Proof. Se n è coprimo con la caratteristica di k, il morfismo $n_A : A \to A$ è un rivestimento di Galois con gruppo $\ker(n_A) \simeq A[n]$. Infatti $\ker n_A$ è uno schema in gruppi finito di

ordine coprimo con chark, ed è quindi étale. Su un campo algebricamente chiuso un gruppo étale finito è semplicemente un gruppo finito, e la mappa naturale $\ker(n_A) \to A[n]$ è bigettiva.

Se la caratteristica di k divide n, $\ker n_A$ è uno schema in gruppi non ridotto con una mappa naturale $\ker \varphi \to A[n]$ che è ancora bigettiva, ma non è un isomorfismo di schemi in gruppi: è surgettivo con kernel dato da un gruppo non ridotto concentrato in un punto. Chiamiamo $\nu_n \subseteq \ker n_A$ questo sottogruppo connesso. È uno schema in gruppi finito che agisce su A, possiamo farne il quoziente A/ν_n: la costruzione è esattamente la stessa dei quozienti per gruppi finiti. Siccome ν_n è un sottogruppo di A, A/ν_n eredita la struttura di varietà abeliana, inoltre la moltiplicazione $n : A \to A$ induce un omomorfismo di varietà abeliane $A/\nu_n \to A$ con kernel $\ker n_A/\nu \simeq A[n]$, ed è quindi étale. Affermo che i rivestimenti della forma $A/\nu_n \to A$ sono cofinali nei rivestimenti étale di A, il che implica $\pi_1(A) \simeq T(A)$ come voluto.

Prendiamo quindi un rivestimento qualunque $\varphi : Y \to A$. Grazie ai risultati precedenti, sappiamo che φ è un morfismo di varietà abeliane e abbiamo una fattorizzazione $A \to Y \to A$ della moltiplicazione per n, dove n è un qualunque intero multiplo del grado di φ. Consideriano $\nu_n \subseteq \ker n_A$: siccome φ è étale, $\nu_n \subseteq \ker \varphi$, e abbiamo quindi un momrfismo di rivestimenti $A/\nu_n \to Y$. □

Remark 3.3.17. Nel libro di Szamuely, temo che la parte specifica della caratteristica positiva sia sbagliata. Ad un certo punto ha una mappa fra varietà abeliane bigettiva sui punti e da questo conclude che è un isomorfismo, che però è falso perché la mappa in generale è ramificata.

3.4 Schemi in gruppi

Un punto di vista che risulta molto utile è quello degli schemi in gruppi. Uno schema in gruppi è semplicemente un oggetto gruppo nella categoria degli schemi: come abbiamo i gruppi topologici che sono gruppi con una struttura topologica, i gruppi di Lie che sono gruppi con una struttura differenziale e i gruppi algebrici che sono gruppi con una struttura di varietà algebrica su $\mathbb{C}$, così abbiamo gli schemi in gruppi. Come però sappiamo, se non siamo su un campo algebricamente chiuso i punti di uno schema dicono ben poco sullo schema stesso, quindi la nozione di "schema con una struttura di gruppo" è un po' troppo ingenua per funzionare, ma l'idea è giusta (e volendo si può formalizzarla usando il lemma di Yoneda). In generale, un'ottima referenza per la teoria degli schemi in gruppi è [Wat79].

La definizione più semplice è la seguente. Fissato un campo base k, uno schema in gruppi su k è uno schema G su k con un dato di certe mappe che rispettano certe relazioni. Le mappe sono la moltiplicazione, l'identità e l'inverso:

$$G \times G \xrightarrow{m} G \qquad \operatorname{Spec} k \xrightarrow{e} G$$

$$G \xrightarrow{i} G$$

mentre le relazioni sono l'associatività e il fatto che la moltiplicazione per l'inverso dà l'identità:

$$\begin{array}{ccc} G\times G\times G & \xrightarrow{m\times \mathrm{id}} & G\times G \\ \downarrow{\scriptstyle \mathrm{id}\times m} & & \downarrow{\scriptstyle m} \\ G\times G & \xrightarrow{m} & G \end{array} \qquad \begin{array}{ccccc} G & \xrightarrow{\Delta} & G\times G & \xrightarrow{\mathrm{id}\times i} & G\times G \\ \downarrow & & & & \downarrow{\scriptstyle m} \\ \operatorname{Spec} k & & \xrightarrow{\qquad e \qquad} & & G \end{array}$$

Lavorare con questa definizione si può fare, ma è un po' fastidioso. Il modo migliore di pensare a uno schema in gruppi è il punto di vista funtoriale che usa il lemma di Yoneda, ma non voglio allontanarmi troppo dallo scopo di questi seminari. Se a qualcuno interessa, possiamo farci quattro chiacchiere.

Example 3.4.1. Le varietà abeliane sono schemi in gruppi. Uno schema in gruppi proprio e connesso è automaticamente una varietà abeliana.

Example 3.4.2. Dato un gruppo G, possiamo formare lo schema in gruppi discreto associato semplicemente prendendo l'unione disgiunta di copie di $\operatorname{Spec} k$ per ogni elemento di G. La struttura di gruppo di G dà automaticamente la struttura di schema in gruppi allo schema discreto associato, e normalmente si confonde fra i due.

Example 3.4.3. Il gruppo moltiplicativo $\mathbb{G}_m = \operatorname{Spec} k[x]_x$ e il gruppo additivo $\mathbb{G}_a = \operatorname{Spec} k[x]$. Una maniera semplice di scrivere le mappe è mettersi nel caso $k = \mathbb{C}$, scrivere le mappe tra gli anelli e poi accorgersi che essere sui complessi era perfettamente inutile.

Example 3.4.4. Tutti i vari GL_n, SL_n, O_n etc. hanno una struttura naturale di schema in gruppo.

Example 3.4.5. Lo schema in gruppi delle radici delle radici n-esime dell'unità

$$\mu_n = \operatorname{Spec} k[x]/(x^n - 1).$$

Come prima, una maniera semplice di scrivere le mappe è di farlo prima sui complessi.

Se n non è multiplo della caratteristica del campo e se in k abbiamo tutte le radici n-esime dell'unità, allora μ_n è isomorfo a $\mathbb{Z}/n$. Molti ragionamenti, ad esempio su un campo di numeri, che iniziano con la frase "supponiamo che in k ci siano le radici dell'unità n-esime" potrebbero evitare questa ipotesi semplicemente usando μ_n al posto di $\mathbb{Z}/n$. Uno dei motivi per cui spesso il gruppo delle radici dell'unità è quello giusto è che esiste una successione esatta corta

$$1 \to \mu_n \to \mathbb{G}_m \xrightarrow{n} \mathbb{G}_m \to 1$$

Ad esempio la teoria di Kummer si può tirare fuori dalla successione esatta lunga associata a questa successione esatta corta.

Example 3.4.6. Sia G un gruppo profinito, e consideriamo un campo k. Pensiamo k con la topologia discreta, e G con la topologia di gruppo profinito. Chiamiamo k^G l'anello delle funzioni continue $G \to k$. Allora un esercizio non troppo difficile è mostrare che $\operatorname{Spec} k^G$ è naturalmente omeomorfo a G, e su $\operatorname{Spec} k^G$ possiamo mettere una struttura di schema in gruppo compatibile con la struttura di gruppo di G. In questo modo possiamo immergere la categoria dei gruppi profiniti in quella degli schemi in gruppi: anche se il punto di vista topologico può essere più comodo per un analisi fine dei gruppi profiniti, altre volte la stuttura algebrica è più naturale, e sapere che le due cose sono equivalenti è utile.

Uno schema in gruppi si dice finito se è finito come schema. Attenzione, finito non vuol dire discreto: μ_n è finito ma può non essere discreto se non abbiamo le radici dell'unità in k. Uno schema in gruppi è profinito se è limite proiettivo di schemi finiti. Una cosa importante da sapere è che i gruppi finiti su campi di caratteristica zero sono sempre étale. Essendo in caratteristica zero e avendo uno schema finito, questo vuol dire semplicemente che lo schema deve essere ridotto.

Se G è uno schema in gruppi e T uno schema su k, allora l'insieme dei morfismi di k schemi da T in G eredita una naturale struttura di gruppo.

Fissiamo un campo k, L/k un'estensione di Galois e G uno schema in gruppi. Allora $\operatorname{Gal}(L/k)$ agisce su $G(L)$ con automorfismi di gruppo, e possiamo costruire il prodotto semidiretto $G(L) \rtimes \operatorname{Gal}(L/k)$. Questo ci dà una successione esatta corta

$$1 \to G(L) \to G(L) \rtimes \operatorname{Gal}(L/k) \to \operatorname{Gal}(L/k) \to 1$$

Quando si fa coomologia di Galois, si ha un gruppo con un'azione di un gruppo di Galois: la maggior parte delle volte viene dalla costruzione che abbiamo appena fatto.

Il motivo per cui ci interessano gli schemi in gruppi è che il gruppo fondamentale étale, come molte delle sue varianti che andremo a vedere, ha una naturale struttura di schemi in gruppi. Cioè, dato uno schema X su un campo k e un punto base *razionale* $x \in X(k)$ (per avere uno schema in gruppi non basta un punto geometrico), esiste uno schema in gruppi profinito $\underline{\pi}_1(X, x)$ tale che il gruppo fondamentale étale $\pi_1(X, \overline{x})$ è naturalmente isomorfo a $\underline{\pi}_1(X, x)(k_s) \rtimes \operatorname{Gal}(k_s/k)$. Inoltre, la sequenza esatta corta scritta sopra coincide con la sequenza esatta di omotopia vista nella precedente sezione.

Non andremo nei dettagli di come si fa questa costruzione, ma vorrei darvi almeno un'idea. Consideriamo i rivestimenti étale $E \to X$ con le seguenti due proprietà:

- nella fibra E_x c'è un punto razionale,
- $E_{k_s} \to X_{k_s}$ è un rivestimento di Galois.

Allora esiste uno schema in gruppi $\underline{\operatorname{Aut}}(E/X)^{\mathrm{op}}$ tale che, per ogni estensione L, il gruppo $\underline{\operatorname{Aut}}(E/X)^{\mathrm{op}}(L)$ è il gruppo (opposto) degli automorfismi di $E_L \to X_L$. Lo schema in gruppi fondamentale sarà il limite proiettivo degli schemi in gruppi $\underline{\operatorname{Aut}}(E/X)^{\mathrm{op}}$.

Example 3.4.7. Se A è una varietà abeliana su un campo k che prenderemo per semplicità di caratteristica zero, allora il kernel $A[n]$ della moltiplicazione per n ha una naturale

struttura di schema in gruppo. Questo permette di generalizzare il calcolo del gruppo fondamentale di una varietà abeliana anche nel caso di un campo non algebricamente chiuso:

$$\underline{\pi}_1(A, 0) = \varprojlim_n A[n].$$

Un punto di vista molto interessante sugli schemi in gruppi affini è quello della dualità tannakiana: l'idea è di associare a un gruppo la sua categoria delle rappresentazioni arricchita con la struttura di prodotto tensore. Descrivendo bene la struttura della categoria delle rappresentazioni, si arriva a un set di assiomi che definiscono quella che si chiama una *categoria tannakiana neutrale*, e si dimostra che il funtore che associa a un gruppo le sue rappresentazioni dà un'equivalenza fra la categoria degli schemi in gruppi affini e quella delle categorie tannakiane neutrali. Per questa parte di seminario non scrivo appunti, ma rimando all'ottimo articolo di Deligne e Milne [DMOS82]. Una versione TEXata dell'articolo è reperibile online direttamente dal sito di Milne.

Chapter 4

The De Rham unipotent fundamental group

4.1 Introduction

In this chapter we describe the De Rham unipotent fundamental group of a p-adic variety, both as an abstract object and in a concrete realization due to Deligne. We will only state the main results without proof; the interested reader is referred to Deligne's foundational paper [Del89].

We start by recalling the notion of a **unipotent vector bundle with connection**:

Definition 4.1.1. *Let X be a variety over a p-adic field K and let $\mathcal{V}$ be a $\mathbb{Q}_p$-vector bundle on X. A **connection** on $\mathcal{V}$ is a morphism of bundles*

$$\nabla : \mathcal{V} \to \mathcal{V} \otimes \Omega^1_X$$

that satisfies Leibniz's rule, that is,

$$\nabla(fs) = s \otimes df + f\nabla(s)$$

*for all $f \in \mathcal{O}_X$ and all sections s of $\mathcal{V}$. A bundle with connection will be denoted by $(\mathcal{V}, \nabla)$ or simply by $\mathcal{V}$ when no confusion can arise. A vector bundle with connection $(\mathcal{V}, \nabla)$ on X is said to be **unipotent** if there exists a filtration by sub-bundles*

$$\mathcal{V}_0 \subset \mathcal{V}_1 \subset \cdots \subset \mathcal{V}_n = \mathcal{V}$$

*such that the successive quotients $\mathcal{V}_{i+1}/\mathcal{V}_i$ are isomorphic to the trivial bundle with connection $(\mathcal{O}_X^{r_i}, d)$ for some $r_i \geq 1$. The minimal possible n is called the **unipotency index** of the bundle.*

Finally, we denote by $\mathcal{U}n^\nabla(X)$ the category of unipotent bundles with connection on X, and by $\mathcal{U}n_n^\nabla(X)$ the subcategory generated by unipotent bundles of index at most n.

4.2 Definition of $\pi_{1,DR}$

We now construct the De Rham unipotent fundamental group in a way analogous to what we've done for the topological and étale fundamental groups. Namely, we define it as the group of automorphisms of a certain **fiber functor**: recall that both the topological and the étale fundamental groups of X based at $x \in X$ can be seen as the groups of automorphisms of the functor that takes a cover $S \to X$ to the set S_x (see section 3.2).

Definition 4.2.1. *The **evaluation** (or **fiber**) functor at a point $b \in X(K)$ is*

$$\begin{array}{rccc} ev_b: & \mathcal{U}n^\nabla(X) & \to & \mathbb{Q}_p - \text{vector spaces} \\ & (\mathcal{V},\nabla) & \mapsto & \mathcal{V}_b \end{array}$$

We can also introduce finite-level versions, which are simply given by restricting ev_b to the subcategory $\mathcal{U}n_n(x)$:

$$\begin{array}{rccc} ev_{b,n}: & \mathcal{U}n_n^\nabla(X) & \to & \mathbb{Q}_p - \text{vector spaces} \\ & (\mathcal{V},\nabla) & \mapsto & \mathcal{V}_b \end{array}$$

The De Rham fundamental group is the automorphism group of this functor:

Definition 4.2.2. *The **De Rham unipotent fundamental group** of X based at b is*

$$\pi_{1,DR}(X,b) := \mathrm{Aut}^\otimes(ev_b),$$

where $\mathrm{Aut}^\otimes$ denotes the set of $\otimes$-compatible automorphisms. This group is the inverse limit of the various $[\pi_{1,DR}]_n$, which are defined as the tensor-automorphism groups of $ev_{b,n}$.

Remark 4.2.3. Concretely, this means the following: an element γ of $\pi_{1,DR}$ is the data, for every vector bundle with connection $(\mathcal{V},\nabla)$, of an automorphism $\gamma_\mathcal{V} : \mathcal{V}_b \to \mathcal{V}_b$ which is functorial in $\mathcal{V}$ and such that, given $\mathcal{V}_1$ and $\mathcal{V}_2$, one has

$$\gamma_{\mathcal{V}_1\otimes\mathcal{V}_2} = \gamma_{\mathcal{V}_1} \otimes \gamma_{\mathcal{V}_2}.$$

Remark 4.2.4. Just like in the case of the étale fundamental group, $\pi_{1,DR}$ is actually a (pro-algebraic) group *scheme*. To describe the group scheme structure, taking the point of view of functors one needs to specify what $\pi_{1,DR}(L)$ is, for every K-scheme L. The answer is very simple: for every such scheme L we have the base change X_L, together with a point b_L, and therefore an evaluation functor $ev_{b_L} : \mathcal{U}_n^\nabla(X_L) \to \mathbb{Q}_p - \mathrm{Vect}$. The value of the functor $\pi_{1,DR}$ on L is then $\pi_{1,DR}(L) = \mathrm{Aut}^\otimes(ev_{b_L})$.

Remark 4.2.5. There is a natural filtration on $\pi_{1,DR}$, constructed as follows. We set $[\pi_{1,DR}]^1 = [\pi_{1,DR}, \pi_{1,DR}]$ to be the commutator subgroup, and inductively

$$[\pi_{1,DR}]^n = \left[[\pi_{1,DR}]^{n-1}, \pi_{1,DR}\right].$$

We also set $[\pi_{1,DR}]_n = \pi_{1,DR}/[\pi_{1,DR}]^n$. A formal verification shows that $[\pi_{1,DR}]_n$ agrees with the $[\pi_{1,DR}]_n$ previously defined (the automorphism groups of $ev_{b,n}$); furthermore, $\pi_{1,DR}$ (which is a *pro*-algebraic group) is the inverse limit of its quotients $[\pi_{1,DR}]_n$.

4.3 The case of the thrice-punctured projective line

We now specialize the discussion to the case of $X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$. In this special situation there is a canonical choice for the basepoint, which however is what is sometimes called a **tangential** basepoint, and which is often denoted by $(0, \partial/\partial t)$ ('the tangent vector at 0 in the direction of 1'). We shall not worry too much about the precise definition of this basepoint; all that is important is that, with this privileged choice of basepoint, Deligne has given a concrete description of $\pi_{1,DR}$ and of its quotients $[\pi_{1,DR}]_n$, which we now recall.

Let $V = \mathbb{Q}_p \ll A, B \gg$ be the completed free algebra on two noncommuting variables A, B, and let $I = (A, B)$ be the (bilateral) augmentation ideal. Then V is in a natural way a Hopf algebra, with comultiplication defined by the rule

$$\Delta(A) = 1 \otimes A + A \otimes 1, \quad \Delta(B) = 1 \otimes B + B \otimes 1.$$

This multiplication is co-commutative, that is, $\sigma(\Delta(x)) = \Delta(x)$ for all $x \in V$, where

$$\sigma : V \otimes V \to V \otimes V$$

in the swap map. This implies that the dual $V^\vee$ of V is a *commutative* algebra: its Spec is the algebraic group $\pi_{1,DR}$ of $\mathbb{P}^1$ minus three points (with tangential basepoint $(0, \partial/\partial t)$). It is also useful to read $\pi_{1,DR}$ as a *subset* of V itself: one has that $\pi_{1,DR}(\mathbb{Q}_p)$ is the set of **group-like** elements of V, that is, elements $g \in V$ such that

$$\Delta(g) = g \otimes g, \quad g - 1 \in I.$$

By a slight abuse of notation, and for compatibility with Kim's papers, we will denote by I^n the n-th iterated commutator of the ideal I (so that $I^1 = I, I^2 = [I, I]$ and $I^3 = [I, I^2]$). For all $n \geq 1$ one then obtains that V/I^{n+1} is the Hopf algebra corresponding to $[\pi_{1,DR}]_n$, which can again be interpreted as the set of group-like elements in this quotient Hopf algebra.

Remark 4.3.1. One should think of A and B as the fundamental loops around the two punctures at 0 and 1.

Example 4.3.2. (De Rham fundamental group in depth 1 and 2) Consider $[\pi_{1,DR}]_1$, the fundamental group in depth 1. This is just the abelianization of $[\pi_{1,DR}]$, so (by analogy with the topological fundamental group) we expect to find two copies of the fundamental group of the affine line minus a single point, which is simply the free group on one generator (hence, in the $\mathbb{Q}_p$-unipotent setting, should just be a copy of the additive group $\mathbb{Q}_p$). This is indeed what happens: the quotient V/I^2 is simply the completed (commutative) polynomial algebra $\mathbb{Q}_p[[A, B]]$, and we now show that the set of group-like elements is given by $\{\exp(mA + nB) \;\big|\; m, n \in \mathbb{Q}_p\}$, with the natural addition law of $\mathbb{Q}_p^2$.

Let $g = \sum_{i,j} c_{ij} A^i B^j$ be a group-like element. Then one computes without difficulty

$$\Delta(g) = \sum_{a,b,c,d} c_{a+c,b+d} \binom{a+b}{a} \binom{c+d}{c} A^a B^b \otimes A^c B^d$$

and

$$g \otimes g = \sum_{a,b,c,d} c_{a,b} c_{c,d} A^a B^b \otimes A^c B^d,$$

so – since these two expressions must agree – we have

$$c_{a,b} c_{c,d} = \binom{a+b}{a} \binom{c+d}{c} c_{a+c,b+d} \quad \forall a,b,c,d \geq 1. \tag{4.1}$$

Using the fact that $c_{0,0} = 1$ for every group-like element, from this formula one sees easily that g is determined by $c_{1,0}$ and $c_{0,1}$. In particular, if $c_{1,0} = c_{0,1} = 0$, equation (4.1) implies $c_{i,j} = 0$ for all pairs (i,j) with $i + j \geq 1$. Now observe that, for every $m \in \mathbb{Q}_p$ and $n \in \mathbb{Q}_p$, the elements $\exp(mA)$ and $\exp(nB)$ are group-like (this is an obvious verification), and therefore so is the product

$$\begin{aligned} \exp(mA)\exp(nB) &= (1 + mA + \frac{1}{2}m^2A^2 + \cdots)(1 + nB + \frac{1}{2}n^2B^2 + \cdots) \\ &= 1 + mA + nB + \cdots \end{aligned}$$

By the uniqueness statement proven above, this is the only group-like element whose part in degree ≤ 1 is $1 + mA + nB$, and we have therefore established a bijection between group-like elements in V/I^2 and $\mathbb{Q}_p^2$. Finally, the map

$$\begin{array}{rccc} \varphi: & \left(\mathbb{Q}_p^2, +\right) & \to & \{g \in V/I^2 : \Delta(g) = g \otimes g\} \\ & (m,n) & \mapsto & \exp(mA)\exp(nB) \end{array}$$

is a group isomorphism: indeed, we have already seen that it is a bijection, and we have

$$\begin{aligned} \varphi(m_1,n_1)\varphi(m_2,n_2) &= \exp(m_1A)\exp(n_1B)\exp(m_2A)\exp(n_2B) \\ &= \exp(m_1A + n_1B + m_2A + n_2B) \\ &= \exp(m_1A + m_2A)\exp(n_1B + n_2B) \\ &= \varphi(m_1 + m_2, n_1 + n_2) \end{aligned}$$

since A, B commute in V/I^2.

A similar, but more tedious, computation allows one to show that $[\pi_{1,DR}]_2$ is isomorphic to the so-called **Heisenberg group** $\mathbb{H}$, namely the group of upper-triangular 3×3 matrices (with coefficients in $\mathbb{Q}_p$) all of whose diagonal coefficients are equal to 1. More precisely, one sees that a group-like element in V/I^3 is determined by the coefficients a, b, c of A, B, AB respectively; as above, one deduces that

$$\begin{aligned} \exp(bB)\exp(aA)\exp(c[A,B]) &= (1 + bB + \cdots)(1 + aA + \cdots)(1 + c[A,B] + \cdots) \\ &= 1 + aA + bB + abBA + c(AB - BA) + \cdots \\ &= 1 + aA + bB + cAB + \cdots \end{aligned}$$

is the unique group-like element with the given coefficients of A, B and AB. The order of the exponentials is essential here: if we multiply $\exp(aA)\exp(bB)$ in *this* order we get the wrong coefficient for AB. Finally, noticing that

$$\begin{aligned}(1+a_1A+b_1B+c_1AB+\cdots)(1+a_2A+b_2B+c_2AB+\cdots)\\ = 1+(a_1+a_2)A+(b_1+b_2)B+(a_1b_2+c_1+c_2)AB+\cdots\end{aligned} \tag{4.2}$$

one sees that the map

$$\begin{array}{rccc}\varphi: & \mathbb{H} & \to & \{g\in V/I^3 : \Delta(g)=g\otimes g\}\\ & \begin{pmatrix}1&a&c\\0&1&b\\0&0&1\end{pmatrix} & \mapsto & \exp(bB)\exp(aA)\exp(c[A,B])\end{array}$$

is a group isomorphism: notice that multiplication in $\mathbb{H}$ is given by

$$\begin{pmatrix}1&a_1&c_1\\0&1&b_1\\0&0&1\end{pmatrix}\begin{pmatrix}1&a_2&c_2\\0&1&b_2\\0&0&1\end{pmatrix}=\begin{pmatrix}1&a_1+a_2&a_1b_2+c_1+c_2\\0&1&b_1+b_2\\0&0&1\end{pmatrix},$$

which is precisely the same as the multiplication rule given by equation (4.2).

4.4 Further constructions

Recall that, in usual topology or in the étale setting (see Theorem 3.3.1), the fundamental groups based at two different points b, x are noncanonically isomorphic. Any isomorphism comes from a path $b \to x$, and furthermore the space of all isomorphisms between $\pi_1(X,b)$ and $\pi_1(X,x)$ carries an action of both $\pi_1(X,b)$ and $\pi_1(X,x)$: indeed, given a homotopy class of paths $b \to x$, we can either pre-compose it with a loop based at b, or post-compose it with a path based at x, and obtain a different homotopy class of paths $b \to x$.

More precisely, the space $\pi_1(X;b,x)$ of continuous paths up to homotopy joining b to x is a torsor under $\pi_1(X,b)$, in the sense that, given any two such paths γ_1, γ_2, there is a unique element $\gamma \in \pi_1(X,b)$ such that γ_1 is homotopic to $\gamma \circ \gamma_2$, where $\circ$ denotes composition of paths. In other words, **once we choose a path** $b \to x$, the space $\pi_1(X;b,x)$ and the group $\pi_1(X,b)$ are identified. Moreover, different homotopy classes of paths correspond to different identifications, and all identifications come from paths. Since in our setting the fundamental groups are the automorphism groups of the fiber functors, it is natural to abstract this remark in the following definition:

Definition 4.4.1. *The (De Rham unipotent)* ***fundamental groupoid****, or path torsor, is*

$$\pi_{1,DR}(X;b,x) = \mathrm{Iso}^{\otimes}(ev_b, ev_x).$$

Elements of this space should be thought of as paths from b to x. Furthermore, precisely as in the topological case, $\pi_{1,DR}(X;b,x)$ has a natural structure of (left) $\pi_{1,DR}(X,b)$-torsor.

The universal pro-bundle with connection A final object which is useful in many parts of the theory is the universal pro-bundle with connection (which is an analogue in this setting of the universal covering space in topology). As usual, one can give a general abstract definition, but in the case of $\mathbb{P}^1 \setminus \{0,1,\infty\}$ it also admits a simple description: it is the trivial (pro-)bundle $\mathcal{V}$ with fiber V (i.e. $\mathcal{V} = V \otimes \mathcal{O}_X$) and connection given by

$$\begin{array}{rccc} \nabla: & \mathcal{V} & \to & \mathcal{V} \otimes \Omega^1_X \\ & f & \mapsto & -Af \otimes \frac{dt}{t} - Bf \otimes \frac{dt}{1-t}, \end{array}$$

where $f \in V$. Essentially by definition, the coordinates of a flat section of $\mathcal{V}$ (or, more precisely, of $\mathcal{V} \otimes \mathcal{O}_X^\dagger$, the bundle in which we allow the coefficient functions to be Coleman functions) are given by iterated Coleman integrals.

Proposition 4.4.2. *Let $v \in V$ and s be a flat section of $\mathcal{V}$ with value v at the base point. Then $s = \sum_w \mathrm{Li}^w(z)wv$, where w varies over all words in A, B.*

Remark 4.4.3. The values of the iterated integrals $\mathrm{Li}^w(z)$ depend (only) on the determination the p-adic logarithm, that is, on $\log(p)$.

Proof. Write $f = \sum_w f_w w$ for a section. If f is the flat section with value 1 at the basepoint, then one checks that fv is the flat section with value $v \in V$ at b. Thus it suffices to describe f in the case $v = 1$. The equation $\nabla f = 0$ gives

$$0 = \sum_w df_w w - f_w(Aw \otimes \frac{dt}{t} + Bw\frac{dt}{1-t},$$

that is,

$$df_{Aw} = f_w \frac{dt}{t}, \quad df_{Bw} = f_w \frac{dt}{1-t},$$

which together with the conditions $f_1(b) = 1$ and $f_w(b) = 0$ for $w \neq 1$ yields $f_w = \mathrm{Li}^w(z)$. □

4.5 The canonical De Rham invariant path

In the case of $X = \mathbb{P}^1 \setminus \{0,1,\infty\}$, a theorem of Deligne shows that a unipotent bundle with connection extends canonically to a unipotent bundle with connection having at most logarithmic singularities near the punctures. Moreover, this bundle is *canonically trivial* (as a bundle, not as a bundle with connection). This allows one to define a **canonical trivialization** of the path torsor[1]. As a special case, consider the universal pro-bundle with connection introduced in the previous section: we have $\mathcal{V} = V \otimes \mathcal{O}_X$, whose canonical extension is, more or less by definition (since the given connection has

[1]Recall that this means that we need to give, for every bundle with connection $\mathcal{W}$ and for every point $x \in X$, a (functorial) isomorphism $\mathcal{W}_b \cong \mathcal{W}_x$.

only mild singularities at 0, 1, ∞), $V \otimes \mathcal{O}_X$ on all of $\mathbb{P}^1$. The canonical trivialization of the path torsor assigns to the point x the obvious isomorphism:

$$\mathcal{V}_x \cong V \cong \mathcal{V}_b.^{2}$$

[2] Although this is just a special case, the universality of the pro-bundle $\mathcal{V}$ makes this sufficient to get a trivialization of the path torsor.

Chapter 5

Proof of Siegel's theorem over $\mathbb{Q}$

5.1 Introduction

The purpose of this chapter is to explain Kim's approach [Kim05] to Siegel's theorem on S-units in the special case of the S-units of $\mathbb{Q}$:

Theorem 5.1.1. *Let S be a finite set of primes of $\mathbb{Z}$, and let $X = \mathbb{P}^1_{\mathbb{Z}} \setminus \{0, 1, \infty\}$. The set $X(\mathbb{Z}[1/S])$ is finite.*

The idea, which is of course a generalization of the Chabauty-Coleman approach to rational points on curves, is to describe $X(\mathbb{Z}[1/S])$ as the set of zeroes of a not-everywhere-vanishing analytic function defined on $X(\mathbb{Z}_p)$, where p is an auxiliary prime not in S.

5.2 De Rham Unipotent Fundamental Group

We briefly recall the main results from chapter 4.

Definition 5.2.1. *Let $Un^\nabla(X)$ be the category of unipotent vector bundles with connection on X. We have $\pi_{1,DR}(X; b) = \mathrm{Aut}^\otimes(e_b)$, where $e_b : Un^\nabla(X) \to \mathrm{Vec}_{\mathbb{Q}_p}$ is the evaluation functor at b.*

Remark 5.2.2. Let $V = \mathbb{Q}_p \ll A, B \gg \otimes \mathcal{O}_X$ be the universal pro-bundle with connection on X. There is a natural structure of Hopf algebra on $\mathbb{Q}_p << A, B >>$ defined by $\Delta(A) = 1 \otimes A + A \otimes 1$, $\Delta(B) = 1 \otimes B + B \otimes 1$ such that $\pi_{1,DR}(X)(\mathbb{Q}_p)$ corresponds to the set of group-like elements of $\mathbb{Q}_p \ll A, B \gg$. Recall that a group-like element is an x such that $\Delta(x) = x \otimes x$. Moreover, $\pi_{1,DR} \cong \mathrm{Spec}(\mathbb{Q}_p \ll A, B \gg^\vee)$.

Definition 5.2.3. *The **unipotent Albanese map** of level n is*

$$UAlb_n = \pi_n \circ UAlb,$$

where $\pi_n : \pi_{1,DR} \to [\pi_{1,DR}]_n$ is the natural projection and

$$\begin{array}{rccc} UAlb: & X(\mathbb{Q}_p) & \to & \pi_{1,DR}(\mathbb{Q}_p) \\ & z & \mapsto & \left(\mathrm{Li}^w(z)\right)_{w \text{ word of length} \leq n} \end{array}$$

Here

$$\mathrm{Li}^w(z) = \int \cdots \int^z w,$$

where the iterated integral over a word w is obtained by replacing $A \to \frac{dz}{z}$, $B \to \frac{dz}{1-z}$, and then integrating in order, so that, for example:

$$\int^z AB = \int_b^z \left(\int_b^{t_2} \frac{dt_1}{t_1} \right) \frac{dt_2}{1-t_2}.$$

The (single) integrals are of course Coleman's integrals from chapter 1.

Remark 5.2.4. More precisely, the unipotent Albanese map sends z to the formal series $\sum_{w \text{ word}} \mathrm{Li}^w(z) w \in V$. One should check that any such element is group-like, and therefore represents a point in $\pi_{1,DR}(\mathbb{Q}_p)$.

The following theorem is not hard to show, and can be proven by a trick involving the fact that the p-adic logarithm is well-defined up to its value at p.

Theorem 5.2.5 (Kim 2005)**.** *The functions $\mathrm{Li}^w(z)$ are $\mathbb{Q}_p$-linearly independent.*

Proof. [Kim05, Theorem 1] □

5.3 The fundamental diagram

We now describe Kim's replacement for the diagram appearing in the Chabauty-Coleman theory, namely:

$$\begin{array}{ccccc} X(\mathbb{Q}) & \longrightarrow & X(\mathbb{Q}_p) & \xrightarrow{\int} & T_e \operatorname{Jac}(X) \\ \downarrow & & \downarrow & \nearrow_{\int} & \\ J(\mathbb{Q}) & \xrightarrow[\mathrm{loc}_p]{} & J(\mathbb{Q}_p) & & \end{array}$$

Recall that the main idea of the classical Chabauty method is to show that the image of $J(\mathbb{Q})$ is contained in a proper closed subset of $T_e \operatorname{Jac}(X)$, which allows one to find a nonzero analytic function on $T_e \operatorname{Jac}(C)$ that vanishes on $J(\mathbb{Q})$; by pull-back, this gives a nonzero analytic function on $X(\mathbb{Q}_p)$ whose finitely many zeroes contain $X(\mathbb{Q})$. Notice that a fundamental part of this construction is the fact that the image of $X(\mathbb{Q}_p)$ via the integration map $\int$ is Zariski-dense in $T_e \operatorname{Jac}(X)$, so that pulling back any nonzero function (on $T_e \operatorname{Jac}(X)$) gives a nonzero function (on X).

To describe the analogue of this diagram in Kim's theory, we shall need to fix some notation and introduce an auxiliary prime:

Definition 5.3.1. *Let S be a finite set of primes, $p \notin S$, $T = S \cup \{p\}$, $\overline{\mathbb{Q}}^T$ be the maximal extension of $\mathbb{Q}$ unramified outside T, $G_p = \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ and $\Gamma_T = \mathrm{Gal}(\overline{\mathbb{Q}}^T/\mathbb{Q})$.*

Kim's fundamental diagram is as follows:

$$\begin{array}{ccccc} X(\mathbb{Z}[1/S]) & \longrightarrow & X(\mathbb{Q}_p) & \xrightarrow{UAlb_n} & [\pi_{1,DR}]_n(\mathbb{Q}_p) \\ \downarrow & & \downarrow & \nearrow_{D} & \\ H^1_f(\Gamma_T, [\pi_{1,\acute{e}t}]_n) & \xrightarrow[\mathrm{loc}_p]{} & H^1_f(G_p, [\pi_{1,\acute{e}t}]_n) & & \end{array}$$

With some work, one sees that this diagram is commutative. Furthermore, as a consequence of Theorem 5.2.5, the image of the map $UAlb_n$ is Zariski-dense. The sets $H^1_f(\Gamma_T, [\pi_{1,\acute{e}t}]_n)$ and $H^1_f(G_p, [\pi_{1,\acute{e}t}]_n)$ that appear on the bottom line are cohomology sets, parametrizing torsors (on a point) under the action of $[\pi_{1,\acute{e}t}]_n$; the subscript $_f$ denotes certain local conditions at p which we will not get into. On the other hand, it is important to point out at the outset that even though these spaces are defined as abstract cohomology sets, Kim proves [1]that they can be identified with the $\mathbb{Q}_p$-points of affine algebraic varieties, and that the maps loc_p and D are also algebraic maps, so that it makes sense to speak about dimensions, Zariski-closed subsets, etc.

5.4 The Unipotent Étale Fundamental group

Definition 5.4.1. *We let $Un(\overline{X})$ be the category of unipotent lisse[2] $\mathbb{Q}_p$-sheaves. The **unipotent étale fundamental group** $\pi_{1,\acute{e}t}(\overline{X}, b) = \mathrm{Aut}^{\otimes}(e_b)$, where e_b is again the fiber functor at b, $e_b : Un(\overline{X}) \to \mathrm{Vec}_{\mathbb{Q}_p}$. We also define the **fundamental groupoid**, or path torsor, as*

$$\pi_{1,\acute{e}t}(\overline{X}; b, p) = \mathrm{Iso}^{\otimes}(e_b, e_p)$$

Remark 5.4.2. If one ignores the Galois action, there is an isomorphism

$$\pi_{1,\acute{e}t} \cong \mathrm{Spec}\left(\mathbb{Q}_p \ll A, B \gg^{\vee}\right),$$

where the dual is in the sense of topological vector spaces. However, $\pi_{1,\acute{e}t}$ has a natural Galois action.

More precisely, our $\pi_{1,\acute{e}t}$ is the $\mathbb{Q}_p$-unipotent completion of $\widetilde{\pi}_{1,\acute{e}t}$, the usual étale fundamental group, which certainly comes equipped with a Galois action. One has for example $[\pi_{1,\acute{e}t}]_1 \cong \mathbb{Q}_p(1)A \oplus \mathbb{Q}_p(1)B$, where $\mathbb{Q}_p(1)$ is the 1-dimensional $\mathbb{Q}_p$ vector space on which Galois acts via the cyclotomic character.

[1]Here, the unipotence of the groups $[\pi_{1,\acute{e}t}]_n$ and $[\pi_{1,DR}]_n(\mathbb{Q}_p)$ plays a fundamental role.

[2]i.e. locally constant in the étale topology

We also define

$$1 \to [\pi_{1,\acute{e}t}]^n \to [\pi_{1,\acute{e}t}] \to [\pi_{1,\acute{e}t}]_n \to 1,$$

where $[\pi_{1,\acute{e}t}]^n = [[\pi_{1,\acute{e}t}]^{n-1}, \pi_{1,\acute{e}t}]$. The following sequence is exact by definition:

$$1 \to [\pi_{1,\acute{e}t}]^n/[\pi_{1,\acute{e}t}]^{n+1} \to [\pi_{1,\acute{e}t}]_{n+1} \to [\pi_{1,\acute{e}t}]_n \to 1,$$

and the Galois action on the first term can be computed since there is a natural surjection

$$(\mathbb{Q}_p(1)^{r_n})^{\otimes n} \cong [\pi_{1,\acute{e}t}]_1^{\otimes n} \twoheadrightarrow [\pi_{1,\acute{e}t}]^n/[\pi_{1,\acute{e}t}]^{n+1}.$$

This implies

$$[\pi_{1,\acute{e}t}]^n/[\pi_{1,\acute{e}t}]^{n+1} \cong \mathbb{Q}_p(n)^{r_n}$$

for some integer r_n.

Remark 5.4.3. The Galois action just described matches the computation of Theorem 1.2.12: indeed, A and B should be thought of as corresponding to the differential forms $\frac{dz}{z}$ and $\frac{dz}{1-z}$, and the action of Frobenius on these forms is indeed multiplication by p, which is the same as the value of the cyclotomic character on Frobenius.

We may now define the **Kummer map** as

$$\begin{array}{ccc} X(\mathbb{Z}[1/S]) & \to & H^1(\Gamma_T, [\pi_{1,\acute{e}t}]) \\ P & \mapsto & [\pi_{1,\acute{e}t}(\overline{X}; b, P)] \end{array}$$

This makes sense, because (exactly as in the usual étale case and in the unipotent De Rham case) the path space $\pi_{1,\acute{e}t}(\overline{X}; b, P)$ is naturally a torsor under $\pi_{1,\acute{e}t}$.

5.4.1 Example

We compute $H^1(\Gamma_T, \mathbb{Q}_p(1))$ for $T = \{\ell\} \cup \{p\}$, p odd. There is a natural exact sequence

$$1 \to \mu_{p^k} \to \overline{\mathbb{Z}[1/T]}^\times \xrightarrow{p^k} \overline{\mathbb{Z}[1/T]}^\times \to 1$$

which induces

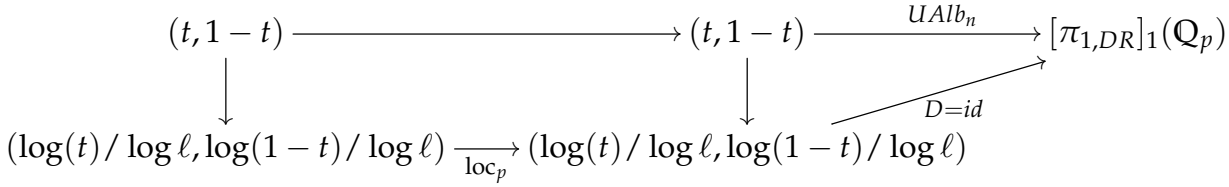
$$1 \to \mathbb{Z}[1/T]^\times/\mathbb{Z}[1/T]^{\times p^k} \xrightarrow{\sim} H^1(\Gamma_T, \mu_{p^k}) \to \mathrm{Cl}(\mathbb{Z}[1/T]) \to 1$$

Since $\mathbb{Z}[1/T]^\times/\mathbb{Z}[1/T]^{\times p^k} \cong (\mathbb{Z}/p^k\mathbb{Z})^{\oplus 2}$, by passing to the limit we find $H^1(\Gamma_T, \mathbb{Z}_p(1)) \cong \mathbb{Z}_p^2$ and $H^1(\Gamma_T, \mathbb{Q}_p(1)) \cong \mathbb{Q}_p^2$. From this, one sees that the map

$$X(\mathbb{Z}[1/S]) \to H^1(\Gamma_T, [\pi_{1,\acute{e}t}]_n) \cong \mathbb{Q}_p^4$$

sends $(t, 1-t)$ to $(\log(t)/\log(\ell), \log(t)/\log(p), \log(1-t)/\log(\ell), \log(1-t)/\log(p))$.

The full diagram looks as follows:



where we write the cohomology spaces as $\mathbb{Q}_p^2$ because of the subscript $_f$, which is there to – roughly – make sure that out of the T-units we only keep the S-units.

5.5 The morphism D

The group $H^1_f(G_p, [\pi_{1,\acute{e}t}]_n)$ parametrizes (certain) torsors under $[\pi_{1,\acute{e}t}]_n$ over a point. Let $\mathfrak{P}$ be a $\mathbb{Q}_p$-algebra whose spectrum is $\mathcal{P}$, a torsor whose class $P = [\mathcal{P}]$ lies in $H^1(G_p, [\pi_{1,\acute{e}t}]_n)$. The map D is defined as follows. First, with $[\mathcal{P}]$ we associate

$$\overline{D}([\mathcal{P}]) = \text{Spec}\left(\mathfrak{P} \otimes_{\mathbb{Q}_p} B^{DR}\right)^{G_p},$$

where B^{DR} is the ring of De Rham periods. This is a torsor over $[\pi_{1,DR}]_n$; the "f" condition ensures that:

- $\overline{D}(P)$ is endowed with a canonical Frobenius action, and $D(P)^{\varphi=1}$ is a single point;
- $\overline{D}(P)$ also has a Hodge filtration, and $F^0\overline{D}(P)$ also consists of a single point[3].

Thus it makes sense to define

$$D(\mathcal{P}) = \overline{D}(P)^{\varphi=1}/F_0\overline{D}(P)$$

as the trasponder[4] from $F_0\overline{D}(P)$ to $\overline{D}(P)^{\varphi=1}$.

When $\mathcal{P}$ is the path torsor $\pi_{1,DR}(X; b, x)$ (see definition 4.4.1), this transponder can be described fairly explicitly: it is the unique element of $\pi_{1,DR}$ whose action brings the canonical De Rham invariant path $\gamma_{DR}(x)$ (section 4.5) to the Frobenius invariant path $\gamma_F(x)$. The De Rham invariant path is given, for every $x \in X$, by the isomorphism

$$\mathcal{V}_b \cong V \cong \mathcal{V}_x,$$

while the Frobenius invariant path $\gamma_F(x)$ is constructed as follows: given $v \in \mathcal{V}_b \cong V$, one considers the unique flat section f of $\mathcal{V} \otimes \mathcal{O}_X^\dagger$ with value v at b, and $\gamma_F(x)(v)$ is the value of f at x. By proposition 4.4.2, this value is $\sum_w \text{Li}^w(x)wv$, and therefore the unique element of $\pi_{1,DR}$ that transports $\gamma_{DR}(x)$ to $\gamma_F(x)$ is $\sum_w \text{Li}^w(x)w$.

[3] This is true only for $X \subset \mathbb{P}_1$, while the preceding point is true for a general (smooth) curve X.

[4] the unique element in the group acting on the torsor that acts on one element and brings it to the other

5.6 Proof of Siegel's theorem by Kim's method

Given our setting, to prove Siegel's theorem it suffices to establish the following **Claim.** There exists $n \gg 0$ such that

$$\dim_{\mathbb{Q}_p} H^1_f(\Gamma_T, [\pi_{1,\acute{e}t}]_n) < \dim_{\mathbb{Q}_p} [\pi_{1,DR}]_n.$$

Remark 5.6.1. It is not hard to see that the sets $H^1(\Gamma_T, [\pi_{1,\acute{e}t}]_n)$ and $H^1(G_p, [\pi_{1,\acute{e}t}]_n)$ are the $\mathbb{Q}_p$-points of algebraic varieties; Kim claims that the same is true for $H^1_f(\Gamma_T, [\pi_{1,\acute{e}t}]_n)$ and $H^1_f(G_p, [\pi_{1,\acute{e}t}]_n)$, but the authors of the present text can only prove that they are *constructible*. Luckily, this is not a big deal for the proof.

Remark 5.6.2. It is clear that the claim implies Siegel's theorem by the argument already sketched. Indeed, if the inequality in the claim holds, we can choose a nonzero regular function on $[\pi_{1,DR}]_n(\mathbb{Q}_p)$ which vanishes on the image of $H^1_f(\Gamma_T, [\pi_{1,\acute{e}t}]_n)$. Since the image of $X(\mathbb{Z}_p)$ in $[\pi_{1,DR}]_n(\mathbb{Q}_p)$ is Zariski-dense, the pull-back of this function to $X(\mathbb{Z}_p)$ is nonzero, and therefore has finitely many zeroes. The commutativity of the fundamental diagram in Kim's theory then implies that $X(\mathbb{Z}[1/S])$ is contained in this finite set of zeroes.

Before moving to the proof of Siegel's theorem, we sketch the argument showing that the sets $H^1(\Gamma_T, [\pi_{1,\acute{e}t}]_n)$ are (the $\mathbb{Q}_p$-points of) affine algebraic varieties:

Proof. The proof is by induction on n, and relies on the fact that

$$H^0(\Gamma_T, [\pi_{1,\acute{e}t}]^n / [\pi_{1,\acute{e}t}]^{n+1}) = 0.$$

One looks at the exact sequence

$$\begin{aligned} H^0(\Gamma_T, [\pi_{1,\acute{e}t}]_n) \to H^1(\Gamma_T, [\pi_{1,\acute{e}t}]^n / [\pi_{1,\acute{e}t}]^{n+1}) \to H^1(\Gamma_T, [\pi_{1,\acute{e}t}]_{n+1}) \\ \to H^1(\Gamma_T, [\pi_{1,\acute{e}t}]_n) \to H^2(\Gamma_T, [\pi_{1,\acute{e}t}]^n / [\pi_{1,\acute{e}t}]^{n+1}) \end{aligned}$$

and shows the following:

- $H^0(\Gamma_T, [\pi_{1,\acute{e}t}]_n) = 0$ (by induction)
- $H^1(\Gamma_T, [\pi_{1,\acute{e}t}]^n / [\pi_{1,\acute{e}t}]^{n+1})$ and $H^2(\Gamma_T, [\pi_{1,\acute{e}t}]^n / [\pi_{1,\acute{e}t}]^{n+1})$ are (represented by) $\mathbb{Q}_p$-vector spaces: this follows from the fact that $[\pi_{1,\acute{e}t}]^n / [\pi_{1,\acute{e}t}]^{n+1} \cong \bigoplus \mathbb{Q}_p(n+1)$
- the map $H^1(\Gamma_T, [\pi_{1,\acute{e}t}]_{n+1}) \to H^1(\Gamma_T, [\pi_{1,\acute{e}t}]_n)$ has a section: to show this, one notices that $H^1(\Gamma_T, [\pi_{1,\acute{e}t}]^n / [\pi_{1,\acute{e}t}]^{n+1}) \to H^1(\Gamma_T, [\pi_{1,\acute{e}t}]_{n+1}) \to H^1(\Gamma_T, [\pi_{1,\acute{e}t}]_n)$ is a torsor[5]; finally, a torsor over an affine variety has a section.

[5] since $[\pi_{1,\acute{e}t}]^n / [\pi_{1,\acute{e}t}]^{n+1}$ is central in $[\pi_{1,\acute{e}t}]_{n+1}$, one sees that $H^1(\Gamma_T, [\pi_{1,\acute{e}t}]^n / [\pi_{1,\acute{e}t}]^{n+1})$ is a group and that it acts on the middle term of the short exact sequence $H^1(\Gamma_T, [\pi_{1,\acute{e}t}]^n / [\pi_{1,\acute{e}t}]^{n+1}) \to H^1(\Gamma_T, [\pi_{1,\acute{e}t}]_{n+1}) \to H^1(\Gamma_T, [\pi_{1,\acute{e}t}]_n)$.

- As a consequence, $H^1(\Gamma_T, [\pi_{1,\acute{e}t}]_{n+1})$ is the product of $H^1(\Gamma_T, [\pi_{1,\acute{e}t}]^n/[\pi_{1,\acute{e}t}]^{n+1})$, which is a $\mathbb{Q}_p$-vector space, and of the fiber of the map

$$H^1(\Gamma_T, [\pi_{1,\acute{e}t}]_n) \to H^2(\Gamma_T, [\pi_{1,\acute{e}t}]^n/[\pi_{1,\acute{e}t}]^{n+1}).$$

  By the inductive hypothesis, this is an algebraic map between affine varieties, hence the fiber over $0 \in H^2(\Gamma_T, [\pi_{1,\acute{e}t}]^n/[\pi_{1,\acute{e}t}]^{n+1})$ is in turn an affine algebraic variety.

□

Proof of Siegel's theorem. We compute the two sides of the inequality separately. $[\pi_{1,DR}]_n$ is a pro-unipotent group; we work with the algebra

$$\mathbb{Q}_p \ll A, B \gg = \mathrm{Env}(\mathrm{Lie}([\pi_{1,DR}]))^\sim,$$

where $\sim$ denotes the completion with respect to the augmentation ideal, and Env is the universal enveloping algebra. Standard general theory shows that

$$\mathbb{Q}_p \ll A, B \gg \cong \bigotimes_{n=0}^{\infty} \mathrm{Env}\left([\pi_{1,DR}]^n/[\pi_{1,DR}]^{n+1}\right),$$

so one gets the generating function for the dimensions $r_n = \dim[\pi_{1,DR}]^n/[\pi_{1,DR}]^{n+1}$:

$$\prod_{d\geq 1} \frac{1}{(1-z^d)^{r_d}} = \frac{1}{1-2z}.$$

Sketch of proof: both spaces are naturally graded. The degree d part of $\mathbb{Q}_p \ll A, B \gg$ is the vector space on words of length d, which has dimension 2^d, hence the generating function for the left hand side is $\sum 2^d z^d = \frac{1}{1-2z}$. On the right hand side we get the infinite product of the generating functions of $\mathrm{Env}\left([\pi_{1,DR}]^n/[\pi_{1,DR}]^{n+1}\right)$, each of which is easy to compute (the z^d is due to the fact that the generators of $[\pi_{1,DR}]^d/[\pi_{1,DR}]^{d+1}$ are in degree d). From the previous formula we get $\sum_{k|n} k r_k = 2^n$, which by Möbius inversion leads to $r_n \sim \frac{2^n}{n}$. Finally,

$$\dim_{\mathbb{Q}_p}[\pi_{1,DR}]_n = \sum_{k\leq n} r_k.$$

On the other hand, we can also estimate the dimension of $H^1_f(\Gamma_T, [\pi_{1,\acute{e}t}]_n)$. We need an upper bound, so we start by trivially bounding $\dim_{\mathbb{Q}_p} H^1_f(\Gamma_T, [\pi_{1,\acute{e}t}]_n)$ with $\dim_{\mathbb{Q}_p} H^1(\Gamma_T, [\pi_{1,\acute{e}t}]_n)$. We now look at the long exact sequence in cohomology

$$\begin{aligned} 0 \to \quad & H^1(\Gamma_T, [\pi_{1,\acute{e}t}]^n/[\pi_{1,\acute{e}t}]^{n+1}) \to \quad H^1(\Gamma_T, [\pi_{1,\acute{e}t}]_n) \to \quad H^1(\Gamma_T, [\pi_{1,\acute{e}t}]_{n-1}) \\ \to \quad & H^2(\Gamma_T, [\pi_{1,\acute{e}t}]^n/[\pi_{1,\acute{e}t}]^{n+1}) = \quad H^2(\Gamma_T, \mathbb{Q}_p(n)^{r_n}) = 0, \end{aligned}$$

where the last equality follows from a theorem of Soulé [Sou79] (which is not necessary here, but will be necessary in a moment). We have also used $H^0(\Gamma_T, [\pi_{1,ét}]_{n-1}) = 0$, which is easy to prove by induction on n.

We also need a formula [NSW08, Theorem 8.7.4] for the (additive) Euler-Poincaré characteristic:

$$h^0(\Gamma_T, \mathbb{Q}_p(n)) - h^1(\Gamma_T, \mathbb{Q}_p(n)) + h^2(\Gamma_T, \mathbb{Q}_p(n)) = -\dim \mathbb{Q}_p(n)^-,$$

where the superscript "$-$" denotes the -1-eigenspace for complex conjugation. Now h^0 vanishes ($n \geq 1$), and so does h^2 by Soulé's theorem in [Sou79]. The error term $-\dim \mathbb{Q}_p(n)^-$ is 0 for n even and -1 for n odd, so

$$h^1(\Gamma_T, \mathbb{Q}_p(n)) = \begin{cases} 0, n \text{ even} \\ 1, n \geq 3 \text{ odd} \end{cases}$$

Finally, $h^1(\Gamma_T, \mathbb{Q}_p(1)) = 2 \operatorname{rank} \mathbb{Z}[1/T]^\times = 2\#T =: R$. The inequality we need to prove is

$$\dim_{\mathbb{Q}_p} H^1(\Gamma_T, [\pi_{1,ét}]_n) < \dim_{\mathbb{Q}_p} [\pi_{1,DR}]_n,$$

that is,

$$R + r_3 + r_5 + \cdots + r_{2\lceil n/2 \rceil - 1} < r_1 + \cdots + r_n,$$

which is true for large n because the r_i go to infinity, and there are more terms on the right than on the left.

□

5.7 Example

In the case $S = \{\ell\}$, $T = \{\ell, p\}$, $n = 2$ the fundamental diagram

$$\begin{array}{ccccc} X(\mathbb{Z}[1/S]) & \longrightarrow & X(\mathbb{Q}_p) & \xrightarrow{UAlb_n} & [\pi_{1,DR}]_n(\mathbb{Q}_p) \\ \downarrow & & \downarrow & \nearrow_{D} & \\ H^1_f(\Gamma_T, [\pi_{1,ét}]_n) & \xrightarrow[\text{loc}_p]{} & H^1_f(G_p, [\pi_{1,ét}]_n) & & \end{array}$$

looks like

$$\begin{array}{ccccc} t & \longrightarrow & t & \xrightarrow{UAlb_2} & \mathbb{H} \\ \downarrow & & \downarrow & \nearrow_{D} & \\ \left(\frac{\log t}{\log \ell}, \frac{\log(1-t)}{\log \ell}\right) & \xrightarrow[\text{loc}_p]{} & H^1_f(G_p, [\pi_{1,ét}]_n) & & \end{array}$$

where $\mathbb{H}$ is the Heisenberg group[6] and the composite map from $H^1_f(\Gamma_T, [\pi_{1,\acute{e}t}]_2) = H^1_f(\Gamma_T, [\pi_{1,\acute{e}t}]_1)$ (this equality follows from Soulé's theorem) to $\mathbb{H}$ is

$$\begin{array}{ccc} H^1_f(\Gamma_T, [\pi_{1,\acute{e}t}]_1) \cong \mathbb{Q}_p^2 & \to & \mathbb{H} \\ (x, y) & \mapsto & \begin{pmatrix} 1 & x\log\ell & \frac{1}{2}(\log\ell)^2 xy \\ 0 & 1 & y\log\ell \\ 0 & 0 & 1 \end{pmatrix}. \end{array}$$

Since $UAlb_2(t) = \begin{pmatrix} 1 & \log t & \mathrm{Li}_2(t) \\ 0 & 1 & \log(1-t) \\ 0 & 0 & 1 \end{pmatrix}$, it follows that the function

$$\mathrm{Li}_2(t) - 2(\log t)(\log(1-t))$$

vanishes on $X(\mathbb{Z}[1/S])$. It is interesting to notice that this function has precisely 9 zeroes on $X(\mathbb{Z}_{11})$: three of them are given by

$$\{-1, 2, \frac{1}{2}\} = X(\mathbb{Z}[1/2]),$$

the other nine by

$$\left\{\frac{-1\pm\sqrt{5}}{2}, \frac{1\pm\sqrt{5}}{2}, \frac{3\pm\sqrt{5}}{2}\right\} = X(\mathcal{O}_{\mathbb{Q}(\sqrt{5})}).$$

It is a well-known fact that the only rings of S-integers with unit rank 1 having nontrivial S-units are precisely $\mathbb{Z}[1/2]$ and $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$.

[6] see chapter 4

Chapter 6

Period rings

6.1 Witt vectors

6.1.1 Idea

From $\mathbb{F}_p$ one can reconstruct $\mathbb{Z}_p$. How? Consider $\mathbb{F}_p$ as $\mathbb{Z}/p\mathbb{Z}$; by *reconstruct*, we mean *define sum and product on* $\mathbb{Z}_p$*, starting from those of* $\mathbb{F}_p$.

So, start with (say) the sum on $\mathbb{Z}/p\mathbb{Z}$, and consider how to extend them to $\mathbb{Z}/p^2\mathbb{Z}$. Take two elements $a_0 + a_1 p$, $b_0 + b_1 p$ where a_i, b_i are taken in a set of representatives $T_p = \{\alpha_0, \dots, \alpha_{p-1}\}$ which we will fix later[1]. We want to express the sum

$$(a_0 + b_0) + (a_1 + b_1)p$$

in terms of our representatives. Say that $(a_0 + b_0) \equiv (a_0 + b_0)_{\bmod p} \pmod p$, with $(a_0 + b_0)_{\bmod p} \in T_p$; then we write

$$(a_0 + b_0) + (a_1 + b_1)p = (a_0 + b_0)_{\bmod p} + (a_0 + b_0 - (a_0 + b_0)_{\bmod p}) + (a_1 + b_1)p.$$

Remark 6.1.1. Observe that

$$(a_0 + b_0) \equiv (a_0 + b_0)_{\bmod p} \pmod p$$

implies

$$(a_0 + b_0)^p \equiv (a_0 + b_0)^p_{\bmod p} \pmod{p^2}.$$

Hence, if we choose the representative T_p to be the Teichmüller representatives (i.e. those that satisfy $\alpha_i^p = \alpha_i$), we obtain the following expression:

$$(a_0 + b_0)^p \equiv (a_0 + b_0)^p_{\bmod p} = (a_0 + b_0)_{\bmod p}$$

One may use a similar argument to "construct", starting from the operations of sum and product on $\mathbb{Z}/p^{n-1}\mathbb{Z}$, the ones on $\mathbb{Z}/p^n/\mathbb{Z}$. Hence, working by induction and then taking the inverse limit $\lim \mathbb{Z}/p^n/\mathbb{Z}$, there should be an (algebraic) way to construct the operations of sum and product on $\mathbb{Z}_p$, starting from those of $\mathbb{F}_p$. This will be made more formal in the next paragraphs.

[1] In the end, our choice is going to be that of the Teichmüller representatives.

6.1.2 Definition

Definition 6.1.2. *In the context of the Witt vectors of $\mathbb{F}_p$, given an element $\alpha \in \mathbb{F}_p$, we write $[\alpha]$ for its Teichmüller lift in $\mathbb{Z}_p$.*

More generally, let R be a **perfect** ring of characteristic p.

Definition 6.1.3. *We define $W(R)$, the **Witt vectors of** R, as:*

$$W(R) := \left\{ \sum_{k\geq 0} [\alpha_k] p^k | \alpha_k \in R \right\},$$

with sum and product defined analogously to the above, namely

$$+ \left(\sum_{k\geq 0} [a_k] p^k, \sum_{h\geq 0} [b_h] p^h \right) = \sum_{i\geq 0} [S_i(a_k, b_h)] p^i$$

$$\times \left(\sum_{k\geq 0} [a_k] p^k, \sum_{h\geq 0} [b_h] p^h \right) = \sum_{i\geq 0} [P_i(a_k, b_h)] p^i$$

where the $S_i, P_i \in R[a_k^{\frac{1}{p^n}}, b_h^{\frac{1}{p^n}}]_{n\in\mathbb{N}}$ are polynomials, and the $[a_k]$ are formal elements of $W(R)$. [2].

One may construct the polynomials S_i and P_i as follows. Let $W_n : W(R) \to R$, the *Witt polynomials*, be defined as:

$$W_n \left(\sum_{k\geq 0} [\alpha_k] p^k \right) := \sum_{k\leq n} p^k \alpha_k^{p^{n-k}}.$$

Then, the polynomials S_i and P_i are the unique polynomials that satisfy the following equalities in $\mathbb{Z}[a_k^{p^{-m}}, b_h^{p^{-m}}]_{m\in\mathbb{N}}$, for each $n \in \mathbb{N}$:

$$W_n \left(\sum_{i\geq 0} [S_i(a_k, b_h)^{p^{-n+i}}] p^i \right) = W_n \left(\sum_{k\geq 0} [a_k^{p^{-n+k}}] p^k \right) + W_n \left(\sum_{k\geq 0} [b_k^{p^{-n+k}}] p^k \right),$$

and:

$$W_n \left(\sum_{i\geq 0} [P_i(a_k, b_h)^{p^{-n+i}}] p^i \right) = W_n \left(\sum_{k\geq 0} [a_k^{p^{-n+k}}] p^k \right) \cdot W_n \left(\sum_{k\geq 0} [b_k^{p^{-n+k}}] p^k \right).$$

[2] Which will turn out to be, by construction the Teichmüller representatives (see below)

Remark 6.1.4. The polynomials $S_i(a_k, b_h)$ involve fractional powers of the variables: for example,

$$S_1(a_0, b_0, a_1, b_1) = \frac{a_0 + b_0 - (a_0^{1/p} + b_0^{1/p})^p}{p} + a_1 + b_1.$$

Moreover, S_i (and P_i) depend at most on the variables to the power $1/p^i$, and the variables that appear are all the a_j and all the b_k with $j, k \leq i$.

6.1.3 Teichmüller representatives

Let A be a ring of characteristic 0, complete for the topology induced by a maximal ideal $\mathfrak{m}$, and let $R := A/\mathfrak{m}$ be of characteristic p and perfect. One defines the Teichmüller representative as follows: for $x \in R$, we set

$$[x] := \lim_{k \to \infty} \widetilde{x^{-p^k}}^{p^k} \in A,$$

where $\widetilde{r}$ denotes any lift of r to A.

Remark 6.1.5.

- $[x]$ exists and does not depend on the choice of the lift (by a 'lifting the exponent'-kind of lemma),
- $[x] \equiv x \pmod{\mathfrak{m}}$,
- $[xy] = [x][y]$.

6.1.4 Properties of the Witt vectors

- $W(R)$ is complete wrt the topology generated by the ideal (p); the quotient $W(R)/pW(R)$ is isomorphic to R.
- $\alpha_k \in R \Rightarrow [\alpha_k]$ is exactly the Teichmüller representative of α_k.
- For $R = \mathbb{F}_{p^k}$, $W(R)$ is the ring of integers of K, the unique unramified extension of $\mathbb{Q}_p$ of degree k.

Lemma 6.1.6. *Let R be a perfect ring of characteristic p, A complete wrt an ideal $I < A$, $\mathrm{char}(A/I) = p$. Given a homomorphism $\varphi : R \to A/I$, there exists a unique homomorphism $\widetilde{\varphi} : W(R) \to A$ that lifts φ.*

Corollary 6.1.7. *Let $p \in \mathbb{N}$ be a prime, and let A be a ring such that $R = A/(p)$, is a perfect ring of characteristic p, A is complete and Hausdorrf in the (p)-topology, and p is not a zero-divisor (or, equivalently, when R is a field, p is not nilpotent). Then $A \cong W(R)$, and the isomorphism is compatible with the equality $R = A/(p)$ and isomorphism $W(R)/pW(R) \cong R$.*

6.2 Period rings

6.2.1 Idea

A way to think about the comparison theorem between De Rham and Betti cohomology is the following:

Theorem 6.2.1. *Let X be a smooth manifold/$\mathbb{R}$. There is a perfect pairing*

$$H_k(X,\mathbb{R}) \times H^k_{dR}(X,\mathbb{R}) \to \mathbb{R},$$

given by $(\gamma,[\omega]) \mapsto \int_\gamma \omega$. As a consequence, $H^k_{dR}(X,\mathbb{R}) \cong H^k(X,\mathbb{R})$.

We'd like something similar for p-adic varieties:

$$H^k_{dR}(X,\mathbb{Q}_p) \cong H^k_{\text{crys}}\left(\overline{X},\mathbb{Q}_p\right),$$

where $\overline{X} = X \times_{\operatorname{Spec}\mathbb{Z}_p} \operatorname{Spec}\mathbb{F}_p$.

Unfortunately, although these two are going to be isomorphic (in fact, we will prove they are vector spaces of the same dimension), the isomorphism is not going to be functorial. The comparison isomorphism will become natural only after extension to some (huge) ring.

This kind of phenomena may be seen also in the isomorphism $H^k_{dR}(X,\mathbb{Q}) \cong H^k(X,\mathbb{Q})$, which exists (by dimension counting), but in order to make the isomorphism functorial one needs to basechange to $\mathbb{R}$.

6.2.2 Periods for the cyclotomic character

First attempt: $\mathbb{C}_p$ (Sen)

Let $\mathbb{C}_p := \widehat{\overline{\mathbb{Q}_p}}$.

Theorem 6.2.2. *(Ax-Sen-Tate) Let $H < G_{\mathbb{Q}_p}$ be a closed subgroup. Then $\mathbb{C}_p^H = \widehat{\overline{\mathbb{Q}_p}^H}$.*

From now on, K is a finite extension of $\mathbb{Q}_p$, and F is the maximal unramified subextension of K

Theorem 6.2.3. *(Tate) Let $\psi : G_K \to \mathbb{Z}_p^\times$ be a character such that*

- *$\psi|_{H_K} = 1$, where $H_K = \operatorname{Gal}\left(\overline{K}/K_\infty\right)$ and $K_\infty = \bigcup_{n\geq 0} K(\mu_{p^n})$.*
- *ψ does not factor through a finite group*

Then $H^0(G_K,\mathbb{C}_p(\psi^{-1})) = \{0\}$, where

$$H^0(G_K,\mathbb{C}_p(\psi^{-1})) = \{x \in \mathbb{C}_p : gx = \psi(g)x,\ \forall g \in G_K\}$$

Definition 6.2.4. *The cyclotomic character $\chi : G_K \to \mathbb{Z}_p^\times$ is the only character such that $g(\zeta) = \zeta^{\chi(g)}$ for all p^n-th root of unity ζ.*

The cyclotomic character (and its powers) is an example of character that satisfies the hypothesis of Theorem 6.2.3.

Observe that Tate's theorem suggests that $\mathbb{C}_p$ is *not* the right period ring: the cyclotomic character arises from geometry, so we would like our period ring to contain periods for the cyclotomic character – in other words, if R is a 'good' period ring, one should have:

$$\dim H^0(G_K, R(\psi^{-1})) = 1.$$

Theorem 6.2.5. *(Sen)*

$$H^1(H_K, \mathrm{GL}(d, \mathbb{C}_p)) = \{0\},$$

which implies the following: if V is a G_K-representation, then $(V \otimes_{\mathbb{Q}_p} \mathbb{C}_p)^{H_K}$ is a $\widehat{K_\infty}$-vector space of dimension $\dim_K V$.

What we *want* is an analogous theorem for all representations (or at least all representations coming from geometry).

6.2.3 Hodge-Tate representations

Definition 6.2.6. *V a G_K-representation is **Hodge-Tate** if*

$$\left(V \otimes_K \bigoplus_{i=-\infty}^{\infty} \mathbb{C}_p(i) \right)^{G_K}$$

is a K-vector space of dimension $\dim_K V$. We write $(h_j)_{j=1}^{\dim_K V}$ for the Hodge-Tate weights of this representation, that is, integers such that

$$(V \otimes_K \bigoplus \mathbb{C}_p(i))^{G_K} \cong \bigoplus_{j=1}^{\dim_K V} K(-h_j)$$

6.2.4 Construction of $\mathbb{B}^{\mathrm{dR}}$

$$\widetilde{E}^+ := \varprojlim_{x \to x^p} \mathcal{O}_{\mathbb{C}_p} = \{(x^{(0)}, x^{(1)}, x^{(2)}, \cdots) : (x^{(i+1)})^p = x^{(i)}\}$$

Fix once and for all an element $\varepsilon = (\mu_{p^n})$, where μ_{p^n} is a primitive p^n-th root of unity.

We make $\widetilde{E}^+$ into a ring by setting

$$(x+y)^{(i)} = \lim_{k \to \infty} \left(x^{(i+k)} + y^{(i+k)} \right)^{p^k}$$

and

$$(xy)^{(i)} = x^{(i)} y^{(i)}.$$

Properties of $\widetilde{E}^+$

- $\operatorname{char} \widetilde{E}^+ = p$
- $\mathbb{F}_p((\varepsilon - 1)) \subset \widetilde{E} := \widetilde{E}^+[(\varepsilon - 1)^{-1}]$
- $\widetilde{E}^+ \cong \varprojlim_{x \to x^p} \mathcal{O}_{\mathbb{C}_p}/(p)$[3]
- $\widetilde{E}^+$ is perfect (since raising to the p-th power is nothing but a shift).

We will denote the fraction field of $\widetilde{E}^+$ by $\widetilde{E}$.

Definition 6.2.7. *We define a valuation on $\widetilde{E}$, as $v_E(x) := v_p(x^{(0)})$, for $x \in \widetilde{E}$.*

Remark 6.2.8. $v_p(\varepsilon - 1) = \frac{p}{p-1}$. Indeed,

$$(\varepsilon - 1)^{(0)} = \lim_{n \to \infty} \left(\mu_{p^n} - 1\right)^{p^n},$$

and $\left(\mu_{p^n} - 1\right)^{p^n}$ has valuation $p^n \frac{1}{\varphi(p^n)} = \frac{p}{p-1}$.

Definition 6.2.9. $\widetilde{A}^+ := W(\widetilde{E}^+)$ *and*

$$\widetilde{B}^+ := \widetilde{A}^+[1/p] = \left\{ \sum_{k \gg -\infty} p^k [x_k] : x_k \in \widetilde{E}^+ \right\}$$

Remark 6.2.10. These objects depend only on p and not on the field K (finite extension of $\mathbb{Q}_p$).

Remark 6.2.11. There is a canonical embedding (in particular, this is Galois equivariant) of $\overline{\mathbb{F}_p}$ in $\widetilde{E}^+$ (this is simply given by taking Teichmüller representatives). One may then lift (through Lemma 6.1.6) this embedding to a (Galois equivariant) embedding of $\mathcal{O}_{K^{nr}}$ in $\widetilde{B}^+$. In partiucar, we have that $\mathcal{O}_F \hookrightarrow (\widetilde{B}^+)^{G_K}$.

Definition 6.2.12.

$$\begin{array}{rccc} \overline{\theta}: & \widetilde{E}^+ & \to & \mathcal{O}_{\mathbb{C}_p}/(p) \\ & (x^{(i)}) & \mapsto & \overline{x^{(0)}} \end{array}$$

By the universal property of the Witt vectors (Lemma 6.1.6), there are lifts $\theta : \widetilde{A}^+ \to \mathcal{O}_{\mathbb{C}_p}$ and $\theta : \widetilde{B}^+ \to \mathbb{C}_p$.

Remark 6.2.13.

- θ is surjective (obvious).

[3] This is a ring with the obvious componentwise operations

- $\theta(\sum p^k[x_k]) = \sum p^k x_k^{(0)}$. To see this, notice that:

$$\theta([x_k]) = \lim_{n\to\infty}(x_k^{(n)})^{p^n} = x_k^{(0)}.$$

- Recall $\varepsilon = (\mu_{p^n})$. Define $\varepsilon_1 = (\mu_{p^{n+1}})$, so that $\varepsilon_1^p = \varepsilon$. We then have that:

$$\theta\left(1 + [\varepsilon_1] + \ldots + [\varepsilon_1]^{p-1}\right) = 0,$$

because $\theta([\varepsilon_1])$ is a p-th root of unity and $1 + x + \cdots + x^{p-1}$ is the p-th cyclotomic polynomial. Here $[\cdot]$ is the Teichmüller lift from $\widetilde{E}^+$ to $\widetilde{A}^+$.

Proposition 6.2.14. *Let* $\omega := 1 + [\varepsilon_1] + \ldots + [\varepsilon_1]^{p-1} = \frac{[\varepsilon]-1}{[\varepsilon_1]-1}$. *Then, considering* θ *as a map* $\widetilde{B}^+ \to \mathbb{C}_p$, *we have*

$$\ker\theta = (\omega).$$

Proof. $\ker\overline{\theta} = \{x \in \widetilde{E}^+ : v_E(x) \geq 1\}$. Moreover, $v(\omega) = 1$, so $\omega\widetilde{A}^+ \subseteq \ker\theta$ (where now $\theta : \widetilde{A}^+ \to \mathcal{O}_{\mathbb{C}_p}$), and we know $\overline{\omega}\widetilde{E}^+ = \ker\overline{\theta}$. Hence the map

$$\omega\widetilde{A}^+ \hookrightarrow \ker\theta$$

is surjective modulo p, and since everything is p-adically complete it's surjective *tout court*. □

Hance, we have a morphism

$$\theta : \widetilde{B}^+ \to \mathbb{C}_p$$

with kernel generated by ω.

Definition 6.2.15.

$$\mathbb{B}_+^{dR} = \varprojlim_{k\to\infty} \widetilde{B}^+/(\omega)^k$$

and

$$\mathbb{B}^{\mathrm{dR}} = \mathbb{B}_+^{\mathrm{dR}}[1/\omega]$$

One can show that $\mathbb{B}^{\mathrm{dR}}$ is a field.

Definition 6.2.16. $\mathbb{B}^{\mathrm{dR}}$ *contains the following element, which one has to think as "*$\log[\varepsilon]$*",*

$$t := -\sum_{k\geq 1}\frac{(1-[\varepsilon])^k}{k}.$$

Remark 6.2.17. We have a period for the cyclotomic character!

$$g(t) = g\log[\varepsilon] = \log[\varepsilon^{\chi(g)}] = \chi(g)\log[\varepsilon] = \chi(g)\cdot t$$

Moreover, $(\omega) = (t)$ in $\mathbb{B}_+^{\mathrm{dR}}$ (the ratio is invertible in the ω-adic completion)

Definition 6.2.18.

$$\mathrm{Fil}^i \mathbb{B}^{\mathrm{dR}} = t^i \mathbb{B}^{\mathrm{dR}}_+$$

We have

$$\mathrm{gr}\, \mathbb{B}^{\mathrm{dR}} = \bigoplus_{i=-\infty}^{\infty} \mathbb{C}_p(i),$$

because t generates the kernel of θ, whose quotient is $\mathbb{C}_p$, and we know the action of Galois on t.

Proposition 6.2.19. [4]

$$(\mathbb{B}^{\mathrm{dR}})^{G_K} = K$$

Definition 6.2.20. *Let $V/\mathbb{Q}_p$ be a G_K-representation. We say that V is **de Rham admissible** if*

$$\dim_K \left(V \otimes_{\mathbb{Q}_p} \mathbb{B}^{\mathrm{dR}}\right)^{G_K} = \dim_K V.$$

Remark 6.2.21. If V is de Rham admissible, by passing to the associated graded ring, we see that V is also Hodge-Tate.

6.2.5 $\mathbb{B}_{\mathrm{cris}}$

Motivation: on $\widetilde{E}^+$ there is a natural Frobenius φ. This can be lifted to $\widetilde{\varphi} : \widetilde{A}^+ \to \widetilde{A}^+$ and therefore to $\widetilde{B}^+ \to \widetilde{B}^+$. However,

$$\widetilde{\varphi}(\omega) = \widetilde{\varphi}(1 + [\varepsilon_1] + \ldots + [\varepsilon_1]^{p-1}) = 1 + [\varepsilon] + \ldots + [\varepsilon]^{p-1} \equiv p \pmod{(\omega)}$$

so $\widetilde{\varphi}$ does not preserve the ω-adic topology, hence it does not extend to the completion. We can do better:

Definition 6.2.22.

$$\mathbb{B}^+_{\mathrm{cris}} := \left\{ x \in \mathbb{B}^+_{\mathrm{dR}} : \exists x_k \to 0 \text{ in } \widetilde{B}^+ \text{ such that } x = \sum_k x_k \frac{\omega^k}{k} \right\},$$

where convergence is with respect to the valuation v_E. We further define

$$\mathbb{B}_{\mathrm{cris}} = \mathbb{B}^+_{\mathrm{cris}}[1/t]$$

The definition is given in such a way that $\widetilde{\varphi}$ extends naturally to $\mathbb{B}^+_{\mathrm{cris}}$.

Remark 6.2.23. Notice that we invert t and not ω (is it really different?). Also, $\mathbb{B}_{\mathrm{cris}}$ is not a field: $\omega - p$ is not invertible.

[4] we're not sure about the embedding of K in $\mathbb{B}^{\mathrm{dR}}$

Proposition 6.2.24.

$$(\mathbb{B}_{\text{cris}})^{G_K} = F$$

Definition 6.2.25. *Let V be a $\mathbb{Q}_p$-representation. We set*

$$\mathbb{D}_{\text{cris}}(V) = (V \otimes_{\mathbb{Q}_p} \mathbb{B}_{\text{cris}})^{G_K}.$$

Remark 6.2.26. $\mathbb{D}_{\text{cris}}(V)$ has a σ_F-semilinear automorphism; moreover, $\mathbb{D}_{\text{cris}}(V) \otimes_F K$ has a natural filtration coming from $\mathbb{B}_{\text{dR}}$.

Remark 6.2.27. Frobenius is **not** an automorphism of $\mathbb{B}_{\text{cris}}$.

Exercise 6.2.28. *Fix a sequence $\{r_n\} \subseteq \mathbb{Z}$. There exists $x_r \in \bigcap_{k\geq 0} \varphi^k \mathbb{B}_{\text{cris}}$ such that $\varphi^{-n}(x_r) \in \text{Fil}^{r_n} \mathbb{B}_{\text{dR}} \setminus \text{Fil}^{r_n+1} \mathbb{B}_{\text{dR}}$.*

Bibliography

[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.

[Del89] P. Deligne. Le groupe fondamental de la droite projective moins trois points. In *Galois groups over* $\mathbf{Q}$ *(Berkeley, CA, 1987)*, volume 16 of *Math. Sci. Res. Inst. Publ.*, pages 79–297. Springer, New York, 1989.

[DMOS82] Pierre Deligne, James S. Milne, Arthur Ogus, and Kuang-yen Shih. *Hodge cycles, motives, and Shimura varieties*, volume 900 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin-New York, 1982.

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

[Kim05] Minhyong Kim. The motivic fundamental group of $\mathbf{P}^1 \setminus \{0, 1, \infty\}$ and the theorem of Siegel. *Invent. Math.*, 161(3):629–656, 2005.

[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.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.

[sga03] *Revêtements étales et groupe fondamental (SGA 1)*, volume 3 of *Documents Mathématiques (Paris) [Mathematical Documents (Paris)]*. Société Mathématique de France, Paris, 2003. Séminaire de géométrie algébrique du Bois Marie 1960–61. [Algebraic Geometry Seminar of Bois Marie 1960-61], Directed by A. Grothendieck, With two papers by M. Raynaud, Updated and

annotated reprint of the 1971 original [Lecture Notes in Math., 224, Springer, Berlin; MR0354651 (50 #7129)].

[Sou79] C. Soulé. *K*-théorie des anneaux d'entiers de corps de nombres et cohomologie étale. *Invent. Math.*, 55(3):251–295, 1979.

[Sza09] Tamás Szamuely. *Galois groups and fundamental groups*, volume 117 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2009.

[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).

[Wat79] William C. Waterhouse. *Introduction to affine group schemes*, volume 66 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979.