Algebra & Number Theory

Volume 9
2015
No. 7

msp

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2015 is US $255/year for the electronic version, and $440/year (+$55, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscribers address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

ALGEBRA AND NUMBER THEORY 9:7 (2015)
dx.doi.org/10.2140/ant.2015.9.1515

msp

Singular moduli that are algebraic units

Philipp Habegger

We prove that only finitely many j-invariants of elliptic curves with complex multiplication are algebraic units. A rephrased and generalized version of this result resembles Siegel's theorem on integral points of algebraic curves.

1. Introduction

A singular modulus is the j-invariant of an elliptic curve with complex multiplication; we treat them as complex numbers in this note. They are precisely the values of Klein's modular function $j : \mathbb{H} \to \mathbb{C}$ at imaginary quadratic arguments; here $\mathbb{H}$ denotes the upper half-plane in $\mathbb{C}$. For example, $j(\sqrt{-1}) = 1728$. Singular moduli are algebraic integers and the set of all singular moduli is stable under ring automorphisms of $\mathbb{C}$. We refer to [Lang 1987] for such classical facts.

At the AIM workshop on unlikely intersections in algebraic groups and Shimura varieties in Pisa, 2011 David Masser, motivated by [Bilu et al. 2013], asked if there are only finitely many singular moduli that are algebraic units. Here we provide a positive answer to this question.

Theorem 1. *At most finitely many singular moduli are algebraic units.*

Our theorem relies on several tools: Liouville's inequality from diophantine approximation, Duke's equidistribution theorem [1988], its generalization due to Clozel–Ullmo [2004], and Colmez's lower bound [1998] for the Faltings height of an elliptic curve with complex multiplication supplemented by [Nakkajima and Taguchi 1991].

A numerical computation involving `sage` reveals that no singular modulus of degree at most 100 over the rationals is an algebraic unit. There may be no such units at all. Currently, there is no way to be sure as Duke's theorem is not known to be effective.

Below, we formulate and prove a general finiteness theorem reminiscent of Siegel's theorem on integral points on curves. We will see in particular that there are only finitely many singular moduli j such that $j + 1$ is a unit. Such j do exist, since for instance $j((\sqrt{-3} + 1)/2) = 0$ is a singular modulus.

MSC2010: primary 11G18; secondary 11G50, 11J86, 14G35, 14G40.
Keywords: elliptic curves, complex multiplication, heights.

Suppose that X is a geometrically irreducible, smooth, projective curve defined over a number field F. We write $F[X \smallsetminus C]$ for the rational functions on X that are regular outside of a finite subset C of $X(F)$. Let $\mathbb{O}_F$ be the ring of algebraic integers of F. A subset $M \subset X(F) \smallsetminus C$ is called quasi-integral with respect to C if for all $f \in F[X \smallsetminus C]$, there exists $\lambda \in F \smallsetminus \{0\}$ such that $\lambda f(M) \subset \mathbb{O}_F$. By clearing denominators one sees that quasi-integral sets remain so after adding finitely many F-rational points. Siegel's theorem, see [Serre 1997, Chapter 7], states that a quasi-integral set is finite if $C \neq \varnothing$ and the genus of X is positive, or if the cardinality $\#C$ of C is at least 3.

Our extension of Theorem 1 deals with the question of finiteness for quasi-integral sets of special points on modular curves. Special points generalize singular moduli, we provide a definition for them below. Only finitely many singular moduli are rational over a fixed number field. Thus we adapt the notion of quasi-integrality in the following way. Let $\overline{F}$ be an algebraic closure of F and $\mathbb{O}_{\overline{F}}$ the ring of algebraic integers in $\overline{F}$. We again work with a finite set $C \subset X(\overline{F})$. A subset $M \subset X(\overline{F}) \smallsetminus C$ is called quasi-algebraic-integral with respect to C if for all $f \in \overline{F}[X \smallsetminus C]$ there is a $\lambda \in \overline{F} \smallsetminus \{0\}$ such that $\lambda f(M) \subset \mathbb{O}_{\overline{F}}$.

Let us recall some classical facts about modular curves. Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, i.e., Γ contains the kernel of the reduction homomorphism $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ for an $N \geq 1$. Then Γ acts on $\mathbb{H}$, as does any subgroup of $\mathrm{SL}_2(\mathbb{R})$, by fractional linear transformations. The quotient $\mathbb{H}/\Gamma$ can be equipped with the structure of an algebraic curve Y_Γ defined over a number field F. This algebraic curve has a natural compactification X_Γ, which is a geometrically irreducible, projective, smooth curve over F. The points of $X_\Gamma \smallsetminus Y_\Gamma$ are called the cusps of Y_Γ. We remark that $Y(1) = Y_{\mathrm{SL}_2(\mathbb{Z})}$ is the affine line, that the compactification is $\mathbb{P}^1$, and that there is a single cusp ∞. The natural map $\phi : Y_\Gamma \to Y(1)$ is algebraic. A point of $Y_\Gamma(\overline{F})$ is called special if it maps to a singular modulus under ϕ.

Theorem 2. *Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup and $F \subset \mathbb{C}$ a number field over which Y_Γ is defined. Let $C \subset X_\Gamma(\overline{F})$ be a finite set containing a point that is not a cusp of Y_Γ. Any set of special points in $Y_\Gamma(\overline{F})$ that is quasi-algebraic-integral with respect to C is finite.*

We require C to contain a noncusp for good reason. Indeed, as singular moduli are algebraic integers, the set of all singular moduli is a quasi-algebraic-integral subset of $Y(1)(\overline{\mathbb{Q}})$ with respect to $C = \{\infty\}$. We recover Theorem 1 from Theorem 2 by taking $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ and $C = \{0, \infty\}$. The proof of Theorem 2 relies on the same basic strategy as Theorem 1. However, instead of the Liouville inequality we require David and Hirata-Kohno's sharp lower bound for linear forms in elliptic logarithms [2009]. Earlier, Masser and others obtained lower bounds in this setting after A. Baker's initial work on linear forms in classical logarithms.

Our theorems are similar to M. Baker, Ih, and Rumely's result [2008] on roots of unity that are S-integral relative to a divisor of $\mathbb{G}_m$. Indeed, both finiteness results are based on an equidistribution statement. However, the Weil height of a root of unity is zero, whereas the height of a singular modulus can be arbitrarily large. Indeed, the quality of Colmez's growth estimate for the Faltings height plays a crucial role in our argument. Moreover, finiteness need not hold in the multiplicative setting if the support of the divisor consists of roots of unity. This is in contrast to Theorem 1 where the support of the corresponding divisor is the singular modulus 0. Finally, our work considers only the case where S consists only of the Archimedean places whereas M. Baker, Ih, and Rumely also allow finite places.

Gross and Zagier [1985] gave a formula for the norm of the j-invariant of certain elliptic curves with complex multiplication. However, the author was unable to deduce the finiteness statement in Theorem 1 from their result or from Dorman's extension [1988].

Habegger would like to thank the organizers of the AIM workshop in Pisa, 2011, for providing a stimulation environment. He also thanks Su-ion Ih for helpful remarks concerning his paper with M. Baker and Rumely.

2. Unitary Singular Moduli

In this section, $c_1, c_2, \ldots$ denote positive and absolute constants.

Let K be a number field. A finite place ν of K is a non-Archimedean absolute value that restricts to the p-adic absolute value on $\mathbb{Q}$ for some prime p. With this normalization we have $|p|_\nu = 1/p$. The completion of K with respect to ν is a field extension of degree d_ν of the completion of $\mathbb{Q}$ with respect to the p-adic absolute value. Let J be an algebraic number in a number field K. The absolute logarithmic Weil height of J, or just height for short, is

$$h(J) = \frac{1}{[K:\mathbb{Q}]}\left(\sum_\sigma \log\max\{1, |\sigma(J)|\} + \sum_\nu d_\nu \log\max\{1, |J|_\nu\}\right)$$

where σ runs over all field embeddings $\sigma : K \to \mathbb{C}$ and ν runs over all finite places of K. It is well-known that $h(J)$ does not change when we replace K by another number field containing J. For this and other facts on heights we refer to Sections 1.5 and 1.6 of [Bombieri and Gubler 2006].

We state a height lower bound for singular moduli that follows easily from a result of Colmez and of Nakkajima–Taguchi. See [Poonen 2001, Lemma 3] for a similar argument.

Lemma 3. *Let J be a singular modulus attached to an elliptic curve whose endomorphism ring is an order with discriminant $\Delta < 0$. Then*

$$h(J) \geq c_2 \log|\Delta| - c_3. \tag{1}$$

Proof. We write $\Delta = \Delta_0 f^2$ where $\Delta_0 < 0$ is a fundamental discriminant and f is the conductor of the endomorphism ring of E, an elliptic curve attached to j. In Corollaire 7, Colmez [1998] proved (1) with $h(J)$ replaced by the stable Faltings height of E when Δ is a fundamental discriminant, i.e., if $f = 1$. For $f > 1$ Nakkajima and Taguchi [1991] found that one must add

$$\frac{1}{2}\log f - \frac{1}{2}\sum_{p\mid f} e_f(p)\log p$$

to the stable Faltings height; here the sum runs over prime divisors p of f and

$$e_f(p) = \frac{1-\chi(p)}{p-\chi(p)}\frac{1-p^{-n}}{1-p^{-1}}$$

if $p^n \mid f$ but $p^{n+1} \nmid f$ and $\chi(p)$ is Kronecker's symbol $\left(\frac{\Delta_0}{p}\right)$. The arguments in the proof of [Habegger 2010, Lemma 4.2] give $\sum_{p\mid f} e_f(p)\log p \le c_1 \log\log \max\{3, f\}$. Therefore, the stable Faltings height of E is logarithmically bounded from below in terms of $|\Delta_0 f^2| = |\Delta|$.

By [Silverman 1986, Proposition 2.1], we can replace the stable Faltings height by $h(J)$ at the cost of adjusting the constants. □

Our strategy to prove Theorem 1 is as follows. Let J and Δ be as in Lemma 3. Assume in addition that J is an algebraic unit. We will find an upper bound for $h(J)$ that contradicts the previous lemma for sufficiently large $|\Delta|$. This will leave us with only finitely many Δ and hence finitely many J, as we will see.

The norm of J is ± 1 and the finite places do not contribute to the height of the algebraic integer J. Thus we can rewrite

$$h(J) = \frac{1}{D}\sum_{|\sigma(J)|>1} \log|\sigma(J)| = -\frac{1}{D}\sum_{|\sigma(J)|<1} \log|\sigma(J)| \tag{2}$$

where $D = [\mathbb{Q}(J):\mathbb{Q}]$ and where the sums run over field embeddings $\sigma : \mathbb{Q}(J) \to \mathbb{C}$.

For each σ we have $\sigma(J) = j(\tau_\sigma)$ for some τ_σ in the classical fundamental domain

$$\mathcal{F} = \left\{\tau \in \mathbb{H};\ \mathrm{Re}(\tau) \in (-1/2, 1/2],\ |\tau| \ge 1 \text{ and } \mathrm{Re}(\tau) \ge 0 \text{ if } |\tau| = 1\right\}$$

of the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$.

To bound the right-hand side of (2) from above we must control those conjugates $\sigma(J)$ that are small in modulus. Let $\epsilon \in (0, 1]$ be a parameter that is to be determined; the c_i will not depend on ϵ. We define

$$\Sigma_\epsilon = \{\tau \in \mathcal{F};\ |j(\tau)| < \epsilon\}.$$

The field embeddings that contribute most to the height of J are in

$$\Gamma_\epsilon = \{\sigma : \mathbb{Q}(J) \to \mathbb{C};\ \ \tau_\sigma \in \Sigma_\epsilon\}.$$

We estimate their number using equidistribution in the next lemma.

Lemma 4. *We have $\#\Gamma_\epsilon \le c_6 \epsilon^{2/3} D$ if D is sufficiently large with respect to ϵ.*

Proof. Let μ denote the hyperbolic measure on $\mathcal{F}$ with total mass 1, i.e.,

$$\mu(\Sigma) = \frac{3}{\pi} \int_{x+yi \in \Sigma} \frac{dx\, dy}{y^2} \tag{3}$$

for a measurable subset $\Sigma \subset \mathcal{F}$. Duke [1988] proved that the τ_σ are equidistributed with respect to μ as $\Delta \to -\infty$ runs over fundamental discriminants. For general discriminants, equidistribution follows from [Clozel and Ullmo 2004]. So, for $\Delta \to -\infty$, we get $|\#\Gamma_\epsilon / D - \mu(\Sigma_\epsilon)| \to 0$. To prove the lemma we will bound $\mu(\Sigma_\epsilon)$ in terms of ϵ.

Let ζ be the unique root of unity in $\mathbb{H}$ of order 6; it is a zero of j. By [Lang 1987, Chapter 3, Theorem 2], Klein's modular function j has a triple zero at ζ and at ζ^2 and does not vanish anywhere else on $\overline{\mathcal{F}}$, the closure of $\mathcal{F}$ in $\mathbb{H}$. So $\tau \mapsto j(\tau)(\tau-\zeta)^{-3}(\tau-\zeta^2)^{-3}$ does not vanish on $\overline{\mathcal{F}}$. Now j has a pole at infinity and so $|j(\tau)| > 1$ if the imaginary part of τ is sufficiently large. Therefore

$$|j(\tau)| \ge c_4 |\tau-\zeta|^3 |\tau-\zeta^2|^3 \ge \frac{c_4}{8} \min\{|\tau-\zeta|, |\tau-\zeta^2|\}^3 \tag{4}$$

for all $\tau \in \overline{\mathcal{F}}$ with $|j(\tau)| \le 1$ where $\max\{|\tau-\zeta|, |\tau-\zeta^2|\} \ge |\zeta-\zeta^2|/2 = \frac{1}{2}$ was used in the second inequality. Because the imaginary part of an element in $\mathcal{F}$ is at least $\sqrt{3}/2$ we can use (3) to estimate $\mu(\Sigma_\epsilon) \le c_5 \epsilon^{2/3}$. □

Using this lemma with (2) we can bound the height of J from above as

$$\begin{aligned} h(J) &= -\frac{1}{D}\Bigg(\sum_{|\sigma(J)|<\epsilon} \log|\sigma(J)| + \sum_{\epsilon \le |\sigma(J)|<1} \log|\sigma(J)| \Bigg) \\ &\le c_6 \epsilon^{2/3} \max_{|\sigma(J)|<\epsilon} \log(|\sigma(J)|^{-1}) + |\log \epsilon|. \end{aligned} \tag{5}$$

Soon we will use Liouville's inequality from diophantine approximation to bound $|j(\tau_\sigma)|$ from below if $\sigma \in \Gamma_\epsilon$. To do this, we require a bound for the height of τ_σ.

Lemma 5. *Each τ_σ is imaginary quadratic and we have $h(\tau_\sigma) \le \log \sqrt{|\Delta|}$.*

Proof. We abbreviate $\tau = \tau_\sigma$ and decompose $\Delta = \Delta_0 f^2$ as in the proof of Lemma 3. The endomorphism ring mentioned in Lemma 3 can be identified with $\mathbb{Z} + \omega f \mathbb{Z} \subset \mathbb{C}$ where $\omega = (\sqrt{\Delta_0} + \Delta_0)/2$. This ring acts on the lattice $\mathbb{Z} + \tau\mathbb{Z}$. So there exist

$a, b, c, d \in \mathbb{Z}$ with $\omega f = a + b\tau$, $\omega f \tau = c + d\tau$ and $b \neq 0$. We substitute the first equality into the second one and obtain

$$b\tau^2 + (a-d)\tau - c = 0. \tag{6}$$

Hence, τ is imaginary quadratic. We note that ωf is a root of $T^2-(a+d)T+ad-bc$. The discriminant of this polynomial is $(a+d)^2 - 4(ad-bc) = (\omega - \bar{\omega})^2 f^2 = \Delta$. Hence $\tau = (-(a-d) \pm \sqrt{\Delta})/2b$ and therefore $|\tau|^2 = ((a-d)^2 + |\Delta|)/(2b)^2$.

As τ lies in $\mathcal{F}$, we have $|\mathrm{Re}(\tau)| \leq 1/2$. This inequality implies $|a-d| \leq |b|$ and hence $|\tau|^2 \leq (b^2+|\Delta|)/(2b)^2$. By Proposition 1.6.6 of [Bombieri and Gubler 2006] the value $2h(\tau)$ is at most the logarithmic Mahler measure of $bT^2 + (a-d)T - c$. So $2h(\tau) \leq \log(|b||\tau|^2) \leq \log(|b|/4 + |\Delta|/(4|b|))$. The imaginary part of τ is at least $\sqrt{3}/2$ and so $|b| \leq \sqrt{|\Delta|/3}$. As $x \mapsto x + |\Delta|/x$ is decreasing on $[1, \sqrt{|\Delta|}]$, we conclude $2h(\tau) \leq \log((1+|\Delta|)/4) \leq \log|\Delta|$. □

Now we use Liouville's inequality to bound the conjugates of J away from zero.

Lemma 6. *We have* $\log|\sigma(J)| \geq -c_8 \log|\Delta|$ *for any* $\sigma : \mathbb{Q}(J) \to \mathbb{C}$.

Proof. We retain the notation of the proof of Lemma 4 and assume $|\tau_\sigma - \zeta| \leq |\tau_\sigma - \zeta^2|$; the reverse case is similar. According to (4), we have

$$|\sigma(J)| = |j(\tau_\sigma)| \geq c_7 |\tau_\sigma - \zeta|^3. \tag{7}$$

We also remark that $\tau_\sigma \neq \zeta$ since $\sigma(J) \neq 0 = j(\zeta)$. Liouville's inequality, see [Bombieri and Gubler 2006, Theorem 1.5.21], tells us

$$-\log|\tau_\sigma - \zeta| \leq [\mathbb{Q}(\tau_\sigma, \zeta) : \mathbb{Q}](h(\tau_\sigma) + h(\zeta) + \log 2).$$

But τ_σ and ζ are imaginary quadratic, so $[\mathbb{Q}(\tau_\sigma, \zeta) : \mathbb{Q}] \leq 4$. Moreover, $h(\zeta) = 0$ as ζ is a root of unity. The bound for $h(\tau_\sigma)$ from Lemma 5 yields

$$-\log|\tau_\sigma - \zeta| \leq 4 \log(2\sqrt{|\Delta|}).$$

The lemma now follows from $|\Delta| \geq 3$ and (7). □

Proof of Theorem 1. We will see soon how to fix ϵ in terms of the c_i. By a classical result of Hecke and Heilbronn [Davenport 1980, Chapter 21], there are only finitely many singular moduli whose degree over $\mathbb{Q}$ are bounded by a prescribed constant. So there is no loss of generality if we assume that D is large enough as in Lemma 4.

We use the previous lemma to bound the first term in (5) from above. Thus

$$h(J) \leq c_6 c_8 \epsilon^{2/3} \log|\Delta| + |\log \epsilon|.$$

We fix ϵ to satisfy $c_6 c_8 \epsilon^{2/3} < c_2/2$, where c_2 comes from the height lower bound in Lemma 3. With this choice we conclude that $|\Delta|$ is bounded from above by an absolute constant. By Lemma 5 and Northcott's theorem [Bombieri and Gubler 2006, Theorem 1.6.8] there are only finitely many possible τ_σ and thus only finitely many possible J. □

3. Proof of Theorem 2

We begin by stating a special case of David and Hirata–Kohno's deep lower bound for linear forms in n elliptic logarithms if $n = 2$ and when the elliptic logarithms are periods. Let E be an elliptic curve defined over a number field in $\mathbb{C}$. We fix a Weierstrass equation for E with coefficients in the said number field and a Weierstrass-$\wp$ function that induces a uniformization $\mathbb{C} \to E(\mathbb{C})$. This is a group homomorphism whose kernel $\omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ is a discrete subgroup of $\mathbb{C}$. We start numbering constants anew.

Lemma 7. *Let $d \geq 1$. There exists a constant $c_1 > 0$ depending on E, d, the choice of Weierstrass equation, and the choice $\omega_{1,2}$ with the following property. Suppose $\alpha, \beta \in \mathbb{C}$ are algebraic over $\mathbb{Q}$ of degree at most d and $\max\{1, h(\alpha), h(\beta)\} \leq \log B$ for some real number $B > 0$. If $\alpha\omega_1 + \beta\omega_2 \neq 0$, then*

$$\log|\alpha\omega_1 + \beta\omega_2| \geq -c_1 \log B. \tag{8}$$

Proof. This follows from [David and Hirata-Kohno 2009, Theorem 1.6]. □

In our application, the $\log B$ from (8) will be approximately $\log|\Delta|$ and will compete directly with the logarithmic lower bound of Lemma 3. It is thus essential that David and Hirata-Kohno's inequality is logarithmic in B. A worse dependency, such as $-c_1(\log B)(\log\log B)$, would not suffice.

We further distill this result into a formulation adapted to our application.

Lemma 8. *Let $\eta \in \mathbb{H}$ be such that $j(\eta)$ is an algebraic number. There exists a constant $c_2 > 0$ which may depend on η with the following property. If $\tau \neq \eta \in \mathbb{H}$ is imaginary quadratic with $\max\{1, h(\tau)\} \leq \log B$ for some real number $B > 0$, then*

$$\log|\tau - \eta| \geq -c_2 \log B.$$

Proof. The algebraic number $j(\eta)$ is the j-invariant on an elliptic curve as introduced before Lemma 7. We may assume that the periods $\omega_{1,2}$ satisfy $\eta = \omega_2/\omega_1$. As $\tau \neq \eta$, Lemma 7 with $\alpha = \tau$ and $\beta = -1$ implies $\log|\tau\omega_1 - \omega_2| \geq -c_1 \log B$. We subtract $\log|\omega_1|$ and obtain $\log|\tau - \eta| \geq -c_1 \log B - \log|\omega_1|$. This lemma follows with an appropriate c_2 as $\log B \geq 1$. □

Let us suppose that Γ, F, and C are as in Theorem 2. We recall that ϕ is the natural morphism $Y_\Gamma \to Y(1)$ and we may regard it as an element in the function field of X. We abbreviate $X = X_\Gamma$. In the following, we enlarge F to a number field for which $X(F)$ contains C and all poles of ϕ.

By hypothesis there is a $P_0 \in C$ that is not a cusp of Y_Γ. We write $J_0 \in F$ for the value of ϕ at P_0. The Riemann–Roch theorem provides a nonconstant, rational function $\psi \in F[X \smallsetminus \{P_0\}]$ that vanishes at the poles of ϕ. As ψ is regular outside of P_0, it must have a pole at P_0.

The functions ϕ and ψ^{-1} are algebraically dependent, i.e., there is an irreducible polynomial $R \in F[U, V]$ with $R(\phi, \psi^{-1}) = 0$. We observe $\deg_U R > 0$.

Lemma 9. *There exists a constant $c_5 \in (0, 1]$ which depends only on R with the following property. Let $K \supset F$ be a number field and $|\cdot|$ an absolute value on K that extends the Archimedean absolute value on $\mathbb{Q}$. If $u \in K$ and $v \in K \smallsetminus \{0\}$ with $R(u, v) = 0$, $|v| < c_5$, and $u \neq J_0$, then $\log|u - J_0| < (\log|v|)/(2 \deg_U R)$.*

Proof. In this proof, $c_{3,4} > 0$ depend only on R. We put $e = \deg_U R$ and write $R = r_0 + (U - J_0)r_1 + \cdots + (U - J_0)^e r_e$, with $r_i \in F[V]$ and $r_e \neq 0$.

By construction, the poles of ϕ are among the poles of ψ^{-1}. So ϕ, and thus $\phi - J_0$, are integral over the ring $F[\psi^{-1}]$, see for example [Matsumura 1989, Theorem 10.4]. Hence, r_e is constant and without loss of generality we may assume $r_e = 1$. Next we claim $r_i(0) = 0$ if $0 \leq i \leq e - 1$. If this were not the case, we could find $J_0' \neq J_0$ with $R(J_0', 0) = 0$. This is impossible by our choice of ψ. Therefore,

$$R = VQ + (U - J_0)^e$$

for some $Q \in F[U, V]$ with $\deg_U Q \leq e - 1$.

Now let u and v be as in the hypothesis; we will see how to fix $c_5 \in (0, 1]$ below. We have $|u - J_0|^e = |vQ(u, v)|$ and $|vQ(u, v)| \leq c_3 \max\{1, |u|\}^{e-1}$ as $|v| \leq 1$. If $|u| \geq \max\{1, 2|J_0|\}$, then $|u - J_0| \geq |u| - |J_0| \geq |u|/2$ and so $|u|^e \leq 2^e c_3 |u|^{e-1}$. We find $|u| \leq 2^e c_3$. In this case, $|u - J_0|^e = |vQ(u, v)| \leq c_4|v|$ for some $c_4 \geq 1$. After adjusting, c_4 the same bound holds if $|u| < \max\{1, 2|J_0|\}$. We set $c_5 = c_4^{-2}$ and observe $c_4|v| < |v|^{1/2}$ if $|v| < c_5$. Thus $|u - J_0|^e \leq |v|^{1/2} < 1$ and the lemma follows on taking the logarithm. □

Let us now prove Theorem 2. For this we must verify that a set $M \subset X(\overline{F})$ of special points that is quasi-algebraic-integral with respect to C is finite. By definition, M cannot contain the pole of ψ and without loss of generality we may assume that M does not contain its zeros either. Finally, we may assume that $J_0 \notin \phi(M)$. Let $\lambda \in F \smallsetminus \{0\}$ satisfy $\lambda\psi(M) \subset \mathbb{O}_{\overline{F}}$. To simplify notation we replace $\lambda\psi$ by ψ and adapt R accordingly.

We will use $c_6, c_7, \ldots$ to denote positive constants that may depend on Γ, F, C, and M. Suppose $P \in M$ and let $K \subset \overline{F}$ be a number field containing F and the values $\psi(P), \phi(P)$. Then, as usual,

$$\begin{aligned} h(\psi(P)) &= \frac{1}{[K : \mathbb{Q}]} \sum_{|\sigma(\psi(P))|>1} \log|\sigma(\psi(P))| \\ &= \frac{1}{[K : \mathbb{Q}]} \Bigg(\sum_{1<|\sigma(\psi(P))|\leq c_5^{-1}} \log|\sigma(\psi(P))| + \sum_{|\sigma(\psi(P))|>c_5^{-1}} \log|\sigma(\psi(P))| \Bigg) \\ &\leq -\log c_5 + \frac{1}{[K : \mathbb{Q}]} \sum_{|\sigma(\psi(P))|>c_5^{-1}} \log|\sigma(\psi(P))|, \end{aligned}$$

where the sums run over field embeddings $\sigma : K \to \mathbb{C}$. Say $J = \phi(P) \in K$, then $R(J, \psi(P)^{-1}) = 0$. We apply Lemma 9 to $u = J$ and $v = \psi(P)$ to obtain

$$h(\psi(P)) \le c_6\bigg(1 + \frac{1}{[K:\mathbb{Q}]} \sum_{|\sigma(J-J_0)|<1} -\log|\sigma(J-J_0)|\bigg). \tag{9}$$

We have already seen that R is not divisible by a linear polynomial in the variable V. So, [Bilu and Masser 2006, Proposition 5] and $R(J, \psi(P)^{-1}) = 0$ allow us to bound $h(J)$ from above linearly in terms of $h(\psi(P)^{-1}) = h(\psi(P))$. Together with (9) we get

$$\begin{aligned} h(J) &\le c_7\bigg(1 + \frac{1}{[K:\mathbb{Q}]} \sum_{|\sigma(J-J_0)|<1} -\log|\sigma(J-J_0)|\bigg) \\ &\le c_7\bigg(|\log\epsilon| + \frac{1}{[K:\mathbb{Q}]} \sum_{|\sigma(J-J_0)|<\epsilon} -\log|\sigma(J-J_0)|\bigg) \end{aligned} \tag{10}$$

for any $\epsilon \in (0, 1/2]$.

The points in M are special, so J is a singular modulus. An elliptic curve attached to J has complex multiplication by an order with discriminant $\Delta < 0$. As in the previous section, we will find an upper bound for $|\Delta|$.

For any embedding $\sigma : K \to \mathbb{C}$ we fix $\tau_\sigma \in \mathcal{F}$ with $j(\tau_\sigma) = \sigma(J)$. We now proceed as near (4) and apply [Lang 1987, Chapter 3, Theorem 2]. If ϵ is sufficiently small and if $|\sigma(J - J_0)| < \epsilon$, then

$$|\sigma(J-J_0)| \ge \begin{cases} c_8|\tau_\sigma - \eta_\sigma|^3 & \text{if } J_0 = 0, \\ c_8|\tau_\sigma - \eta_\sigma|^2 & \text{if } J_0 = 1728, \\ c_8|\tau_\sigma - \eta_\sigma| & \text{else.} \end{cases} \tag{11}$$

for some $\eta_\sigma \in \overline{\mathcal{F}}$ with $j(\eta_\sigma) = \sigma(J_0)$. It is harmless that there are 2 choices for η_σ on the boundary of $\overline{\mathcal{F}}$. We note that η_σ depends only on the base point J_0 and that τ_σ is imaginary quadratic. Thus Lemma 8 and the height bound for τ_σ in Lemma 5 yield $\log|\sigma(J - J_0)| \ge -c_9 \log|\Delta|$. We use this inequality and (10) to bound

$$h(J) \le c_{10}\bigg(\log|\epsilon| + \log|\Delta| \frac{\#\{\sigma : K \to \mathbb{C};\ |\sigma(J-J_0)| < \epsilon\}}{[K:\mathbb{Q}]}\bigg)$$

for all $\epsilon \in (0, 1/2]$.

The rest of the proof resembles the proof of Theorem 1. Indeed, we may assume that $[\mathbb{Q}(J) : \mathbb{Q}]$ is sufficiently large and as in Lemma 4 we use equidistribution to prove that $[K : \mathbb{Q}]^{-1}\#\{\sigma : K \to \mathbb{C};\ |\sigma(J - J_0)| < \epsilon\}$ is bounded from above linearly by a fixed power, derived from (11), of ϵ. Finally, we again use the height lower bound of Lemma 3 to fix an appropriate ϵ which leads to a bound on $|\Delta|$. As before, this leaves us with only finitely many possibilities for $J = \phi(P)$. □

References

[Baker et al. 2008] M. Baker, S.-i. Ih, and R. Rumely, "A finiteness property of torsion points", *Algebra Number Theory* **2**:2 (2008), 217–248. MR 2009g:11078 Zbl 1182.11030

[Bilu and Masser 2006] Y. F. Bilu and D. Masser, "A quick proof of Sprindzhuk's decomposition theorem", pp. 25–32 in *More sets, graphs and numbers*, edited by E. Győri et al., Bolyai Soc. Math. Stud. **15**, Springer, Berlin, 2006. MR 2007b:11031 Zbl 1147.11018

[Bilu et al. 2013] Y. Bilu, D. Masser, and U. Zannier, "An effective "theorem of André" for CM-points on a plane curve", *Math. Proc. Cambridge Philos. Soc.* **154**:1 (2013), 145–152. MR 3002589

[Bombieri and Gubler 2006] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, New Mathematical Monographs **4**, Cambridge Univ. Press, 2006. MR 2007a:11092 Zbl 1115.11034

[Clozel and Ullmo 2004] L. Clozel and E. Ullmo, "Équidistribution des points de Hecke", pp. 193–254 in *Contributions to automorphic forms, geometry, and number theory*, edited by H. Hida et al., Johns Hopkins Univ. Press, Baltimore, MD, 2004. MR 2005f:11090 Zbl 1068.11042

[Colmez 1998] P. Colmez, "Sur la hauteur de Faltings des variétés abéliennes à multiplication complexe", *Compositio Math.* **111**:3 (1998), 359–368. MR 99e:11074 Zbl 0918.11025

[Davenport 1980] H. Davenport, *Multiplicative number theory*, 2nd ed., Graduate Texts in Mathematics **74**, Springer-Verlag, New York, 1980. MR 82m:10001 Zbl 0453.10002

[David and Hirata-Kohno 2009] S. David and N. Hirata-Kohno, "Linear forms in elliptic logarithms", *J. Reine Angew. Math.* **628** (2009), 37–89. MR 2010c:11084 Zbl 1169.11034

[Dorman 1988] D. R. Dorman, "Special values of the elliptic modular function and factorization formulae", *J. Reine Angew. Math.* **383** (1988), 207–220. MR 89k:11026 Zbl 0626.10022

[Duke 1988] W. Duke, "Hyperbolic distribution problems and half-integral weight Maass forms", *Invent. Math.* **92**:1 (1988), 73–90. MR 89d:11033 Zbl 0628.10029

[Gross and Zagier 1985] B. H. Gross and D. B. Zagier, "On singular moduli", *J. Reine Angew. Math.* **355** (1985), 191–220. MR 86j:11041 Zbl 0545.10015

[Habegger 2010] P. Habegger, "Weakly bounded height on modular curves", *Acta Math. Vietnam.* **35**:1 (2010), 43–69. MR 2011g:11124 Zbl 1253.11070

[Lang 1987] S. Lang, *Elliptic functions*, 2nd ed., Graduate Texts in Mathematics **112**, Springer, New York, 1987. MR 88c:11028 Zbl 0615.14018

[Matsumura 1989] H. Matsumura, *Commutative ring theory*, 2nd ed., Cambridge Studies in Advanced Mathematics **8**, Cambridge Univ. Press, 1989. MR 90i:13001 Zbl 0666.13002

[Nakkajima and Taguchi 1991] Y. Nakkajima and Y. Taguchi, "A generalization of the Chowla-Selberg formula", *J. Reine Angew. Math.* **419** (1991), 119–124. MR 92g:11113 Zbl 0721.11045

[Poonen 2001] B. Poonen, "Spans of Hecke points on modular curves", *Math. Res. Lett.* **8**:5-6 (2001), 767–770. MR 2002k:11092 Zbl 1081.11043

[Serre 1997] J.-P. Serre, *Lectures on the Mordell–Weil theorem*, 3rd ed., Aspects of Mathematics **15**, Friedr. Vieweg & Sohn, Braunschweig, 1997. MR 2000m:11049 Zbl 0863.14013

[Silverman 1986] J. H. Silverman, "Heights and elliptic curves", pp. 253–265 in *Arithmetic geometry* (Storrs, Conn., 1984), edited by G. Cornell and J. H. Silverman, Springer, New York, 1986. MR 861979 Zbl 0603.14020

Communicated by Joseph Silverman
Received 2014-03-19 Revised 2015-05-30 Accepted 2015-07-15

philipp.habegger@unibas.ch *Departement Mathematik und Informatik, Universität Basel, Spiegelgasse 1, CH-4051 Basel, Switzerland*

msp

ALGEBRA AND NUMBER THEORY 9:7 (2015)
dx.doi.org/10.2140/ant.2015.9.1525

Irreducibility of the Gorenstein loci of Hilbert schemes via ray families

Gianfranco Casnati, Joachim Jelisiejew and Roberto Notari

We analyze the Gorenstein locus of the Hilbert scheme of d points on $\mathbb{P}^n$ i.e., the open subscheme parameterizing zero-dimensional Gorenstein subschemes of $\mathbb{P}^n$ of degree d. We give new sufficient criteria for smoothability and smoothness of points of the Gorenstein locus. In particular we prove that this locus is irreducible when $d \leq 13$ and find its components when $d = 14$.

The proof is relatively self-contained and it does not rely on a computer algebra system. As a by-product, we give equations of the fourth secant variety to the d-th Veronese reembedding of $\mathbb{P}^n$ for $d \geq 4$.

A list of symbols can be found on page 1567.

Casnati and Notari are supported by the framework of PRIN 2010/11 "Geometria delle varietà algebriche", cofinanced by MIUR, and are members of GNSAGA of INdAM. Jelisiejew was partially supported by the project "Secant varieties, computational complexity, and toric degenerations" realized within the Homing Plus programme of Foundation for Polish Science, cofinanced by the European Union, Regional Development Fund. Jelisiejew is a doctoral fellow at the Warsaw Center of Mathematics and Computer Science financed by the Polish program KNOW. This paper is a part of the "Computational complexity, generalized Waring type problems and tensor decompositions" project within "Canaletto", the executive program for scientific and technological cooperation between Italy and Poland, 2013–2015.

MSC2010: primary 14C05; secondary 13H10, 14D15.

Keywords: Hilbert scheme of points, smoothability, Gorenstein algebra, secant variety.

1. Introduction

Let k be an algebraically closed field of characteristic neither 2 nor 3 and denote by $\mathcal{H}ilb_{p(t)}\mathbb{P}^N$ the Hilbert scheme parameterizing closed subschemes in $\mathbb{P}^N$ with fixed Hilbert polynomial $p(t) \in \mathbb{Q}[t]$. Since A. Grothendieck proved the existence of such a parameter space in 1966 (see [Grothendieck 1995]), the problem of dealing with $\mathcal{H}ilb_{p(t)}\mathbb{P}^N$ and its subloci has been a fruitful field, attracting the interest of many researchers in algebraic geometry.

Only to quickly mention some of the classical results which deserve, in our opinion, particular attention, we recall Hartshorne's [1966] proof of the connectedness of $\mathcal{H}ilb_{p(t)}\mathbb{P}^N$, the description of the locus of codimension-2, arithmetically Cohen–Macaulay subschemes due to J. Fogarty [1968] (for the dimension-zero case) and G. Ellingsrud [1975] (for higher dimensions) and of the study of the locus of codimension-3, arithmetically Gorenstein subschemes due to J. Kleppe and R. M. Miró-Roig [Miró-Roig 1992; Kleppe and Miró-Roig 1998].

If we restrict our attention to the case of zero-dimensional subschemes of degree d, i.e., subschemes with Hilbert polynomial $p(t) = d$, then the first significant results are due to Fogarty [1968] and to A. Iarrobino [1972].

Fogarty [1968] proves that $\mathcal{H}ilb_d\mathbb{P}^2$ is smooth, hence irreducible thanks to Hartshorne's connectedness result (the same result holds when one substitutes $\mathbb{P}^2$ by any smooth surface).

On the other hand, Iarrobino [1972] deals with the reducibility when $N \geq 3$ and d is large with respect to N. In order to better understand the result, recall that the locus of reduced schemes $\mathcal{R} \subseteq \mathcal{H}ilb_d\mathbb{P}^N$ is birational to a suitable open subset of the d-th symmetric product of $\mathbb{P}^N$, thus it is irreducible of dimension dN. We will denote by $\mathcal{H}ilb_d^{\mathrm{gen}}\mathbb{P}^N$ its closure in $\mathcal{H}ilb_d\mathbb{P}^N$. It is a well-known and easy fact that $\mathcal{H}ilb_d^{\mathrm{gen}}\mathbb{P}^N$ is an irreducible component of dimension dN, by construction. Iarrobino [1972] proves that $\mathcal{H}ilb_d\mathbb{P}^N$ is never irreducible when $d \gg N \geq 3$, showing that there is a family of schemes of dimension greater than dN. Such a family is thus necessarily contained in a component different from $\mathcal{H}ilb_d^{\mathrm{gen}}\mathbb{P}^N$.

D. A. Cartwright, D. Erman, M. Velasco and B. Viray [Cartwright et al. 2009] proved that already for $d = 8$ and $N \geq 4$, the scheme $\mathcal{H}ilb_d\mathbb{P}^N$ is reducible.

In view of these earlier works it seems reasonable to consider the irreducibility and smoothness of open loci in $\mathcal{H}ilb_d\mathbb{P}^N$ defined by particular algebraic and geometric properties. In the present paper we are interested in the locus $\mathcal{H}ilb_d^G\mathbb{P}^N$ of points in $\mathcal{H}ilb_d\mathbb{P}^N$ representing schemes which are Gorenstein. This is an important locus, e.g., it has an irreducible component $\mathcal{H}ilb_d^{G,\mathrm{gen}}\mathbb{P}^N := \mathcal{H}ilb_d^{\mathrm{gen}}\mathbb{P}^N \cap \mathcal{H}ilb_d^G\mathbb{P}^N$ of dimension dN containing all the points representing reduced schemes. Moreover, it is open, but in general not dense, in $\mathcal{H}ilb_d\mathbb{P}^N$. Recently, interesting interactions between $\mathcal{H}ilb_d^G\mathbb{P}^N$ and the geometry of secant varieties and general topology have

been found (see, for example, [Buczyńska and Buczyński 2014; Buczyński et al. $\geq$ 2015]).

Some results about $\mathcal{H}ilb_d^G \mathbb{P}^N$ are known. The irreducibility and smoothness of $\mathcal{H}ilb_d^G \mathbb{P}^N$ when $N \leq 3$ is part of folklore (see [Casnati and Notari 2009, Corollary 2.6] for more precise references). When $N \geq 4$, the properties of $\mathcal{H}ilb_d^G \mathbb{P}^N$ have been the subject of intensive study in recent years.

For example, it is classically known that $\mathcal{H}ilb_d^G \mathbb{P}^N$ is never irreducible for $d \geq 14$ and $N \geq 6$, at least when the characteristic of k is zero (see [Iarrobino and Emsalem 1978; Iarrobino and Kanev 1999]; see also [Casnati and Notari 2011]). Also, for $N = 4$ and $d \geq 140$, or $N = 5$ and $d \geq 42$, the scheme $\mathcal{H}ilb_d^G \mathbb{P}^N$ is reducible; see [Buczyńska and Buczyński 2014, Section 6, p. 81]. For fixed $N \in \{4, 5\}$, the minimal value of d for which this scheme is reducible is not known.

As reflected by the above references, it is natural to ask whether $\mathcal{H}ilb_d^G \mathbb{P}^N$ is irreducible when $d \leq 13$ and N is arbitrary. There is some evidence of an affirmative answer to this question. Indeed, Casnati and Notari [2009; 2011; 2014a; 2014b] studied the locus $\mathcal{H}ilb_d^G \mathbb{P}^N$ when $d \leq 11$ and N is arbitrary, proving its irreducibility and dealing in detail with its singular locus in a series of papers.

A key point in the study of a zero-dimensional scheme $X \subseteq \mathbb{P}^N$ is that it is abstractly isomorphic to Spec A, where A is an Artin k-algebra with $\dim_k(A) = d$. Moreover, the irreducible components of such an X correspond bijectively to those direct summands of A, which are local. Thus, in order to deal with $\mathcal{H}ilb_d \mathbb{P}^N$, it suffices to deal with the irreducible schemes in $\mathcal{H}ilb_{d'} \mathbb{P}^N$ for each $d' \leq d$.

In all of the aforementioned papers, the methods used in the study of $\mathcal{H}ilb_d^G \mathbb{P}^N$ rely on an almost explicit classification of the possible structure of local, Artin, Gorenstein k-algebras of length d. Once such a classification is obtained, the authors prove that all the corresponding irreducible schemes are smoothable, i.e., actually lie in $\mathcal{H}ilb_d^{G,\mathrm{gen}} \mathbb{P}^N$. To this purpose they explicitly construct a projective family flatly deforming the scheme they are interested in (or, equivalently, the underlying algebra) to reducible schemes that they know to be in $\mathcal{H}ilb_d^{G,\mathrm{gen}} \mathbb{P}^N$ because their components have lower degree.

Though such an approach sometimes seems to be too heavy in terms of calculations, it is only thanks to such a partial classification that it is possible to state precise results about the singularities of $\mathcal{H}ilb_d^G \mathbb{P}^N$.

However, there are families H_d of schemes of degree $d = 10$ and 11 for which an explicit algebraic description in the above sense cannot be obtained (see Section 3 of [Casnati and Notari 2011] for the case $d = 10$ and Section 4 of [Casnati and Notari 2014b] for $d = 11$). Nevertheless, using an alternative approach, the authors are still able to prove the irreducibility of $\mathcal{H}ilb_d^G \mathbb{P}^N$ and study its singular locus. Indeed, using Macaulay's theory of inverse systems, the authors check the irreducibility of

the aforementioned loci H_d inside $\mathcal{H}ilb_d^G\mathbb{P}^N$. Then they show the existence of a smooth point in $H_d \cap \mathcal{H}ilb_d^{G,\mathrm{gen}}\mathbb{P}^N$. Hence, it follows that $H_d \subseteq \mathcal{H}ilb_d^{G,\mathrm{gen}}\mathbb{P}^N$.

The aim of the present paper is to refine and generalize this method. First, we avoid a case-by-case approach by analyzing large classes of algebras. Second, in [Casnati and Notari 2011; 2014b] a direct check (e.g., using a computer algebra program) is required to compute the dimension of the tangent space to the Hilbert scheme at some specific points to conclude that they are smooth. We avoid the need for such computations by exhibiting classes of points which are smooth, making the paper self-contained.

Using this method, we finally prove the following two statements:

Theorem A. *If the characteristic of k is neither 2 nor 3, then $\mathcal{H}ilb_d^G\mathbb{P}^N$ is irreducible of dimension dN for each $d \leq 13$ and for $d = 14$ and $N \leq 5$.*

Theorem B. *If the characteristic of k is 0 and $N \geq 6$, then $\mathcal{H}ilb_{14}^G\mathbb{P}^N$ is connected and it has exactly two irreducible components, which are generically smooth.*

Theorem A has an interesting consequence regarding secant varieties of Veronese embeddings. Geramita [1999] conjectures that the ideal of the 2-nd secant variety (the variety of secant lines) of the d-th Veronese embedding of $\mathbb{P}^n$ is generated by the 3×3 minors of the i-th catalecticant matrix for $2 \leq i \leq d-2$. This conjecture was confirmed in [Raicu 2012]. As pointed out in [Buczyńska and Buczyński 2014, Section 8.1], Theorem A allows us to extend the above result as follows: if $r \leq 13$ and $2r \leq d$, then for every $r \leq i \leq d-r$ the set-theoretic equations of the r-th secant variety of the d-th Veronese embedding of $\mathbb{P}^n$ are given by the $(r+1) \times (r+1)$ minors of the i-th catalecticant matrix.

The proofs of Theorem A and Theorem B are highly interlaced and they follow from a long series of partial results. In order to better explain the ideas and methods behind their proofs, we will describe in the following lines the structure of the paper.

In our analysis we incorporate several tools. In Section 2 we recall the classical ones, most notably Macaulay's correspondence for local, Artinian, Gorenstein algebras and Macaulay's growth theorem. Moreover, we also list some criteria for checking the flatness of a family of algebras which will be repeatedly used throughout the whole paper.

In Section 3 we analyze Artin Gorenstein quotients of a power series ring and exploit the rich automorphism group of this ring to put the quotient into suitable *standard* form, extending a result of Iarrobino.

In Section 4 we further analyze the quotients, especially their dual socle generators. We also construct several irreducible subloci of the Hilbert scheme using the theory of secant varieties. We make a small contribution to this theory, showing

that the fourth secant variety to a Veronese reembedding of $\mathbb{P}^n$ is defined by minors of a suitable catalecticant matrix.

Section 5 introduces a central object in our study: a class of families, called ray families, for which we have relatively good control of the flatness and, in special cases, fibers. Most notably, Section 5B gives a class of *tangent-preserving* flat families, which enable us to construct smooth points on the Hilbert scheme of points without the necessity of heavy computations.

Finally, in Section 6, we give the proofs of Theorems A and B. It is worth mentioning that these results are rather easy consequences of the introduced machinery. We also prove the following general smoothability result (see Theorem 6.14), which has no restriction on the length of the algebra and generalizes the smoothability results from [Sally 1979; Casnati and Notari 2014a; Elias and Valla 2011].

Theorem C. *Let k be an algebraically closed field of characteristic neither 2 nor 3. Let A be a local Artin Gorenstein k-algebra with maximal ideal $\mathfrak{m}$.*

If $\dim_k(\mathfrak{m}^2/\mathfrak{m}^3) \leq 5$ and $\dim_k(\mathfrak{m}^3/\mathfrak{m}^4) \leq 2$, then Spec A *is smoothable.*

2. Preliminaries

Let n be a natural number. We let $(S, \mathfrak{m}_S, k)$ be the power series ring $k[\![\alpha_1, \ldots, \alpha_n]\!]$ of dimension n with a fixed basis $\alpha_1, \ldots, \alpha_n$. The basis chosen determines a polynomial ring $S_{\text{poly}} = k[\alpha_1, \ldots, \alpha_n] \subseteq S$. By P we denote the polynomial ring $k[x_1, \ldots, x_n]$. We will later define a duality between S and P; see Section 2B. We usually think of n being large enough, so that the considered local Artin algebras are quotients of S.

For $f \in P$, we say that f *does not contain* x_i if $f \in k[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$; and similarly for $\sigma \in S$ or $\sigma \in S_{\text{poly}}$. For $f \in P$, by f_d we denote the degree-d part of f, with respect to the total degree; and similarly for $\sigma \in S$.

By P_m and $P_{\leq m}$ we denote the space of homogeneous polynomials of degree m and (not necessarily homogeneous) polynomials of degree at most m, respectively. These spaces are naturally affine spaces over k, which equips them with a scheme structure.

Recall that S has a rich automorphism group: for every choice of elements $\sigma_1, \ldots, \sigma_n \in \mathfrak{m}_S$ that are linearly independent in $\mathfrak{m}_S/\mathfrak{m}_S^2$, there is a unique automorphism φ of S such that $\varphi(\alpha_i) = \sigma_i$ for $i = 1, 2, \ldots, n$. The existence of such automorphisms is employed in Section 4 to put the considered Artin Gorenstein algebras in a better form. See, e.g., [Elias and Rossi 2015, Section 2] for details and examples of this method.

Remark 2.1. For the reader's convenience, we introduce numerous examples, which illustrate the possible applications. In all these examples k may have arbitrary characteristic except 2 or 3, unless otherwise stated.

2A. ***Artin Gorenstein schemes and algebras.*** In this section we recall the basic facts about Artin Gorenstein algebras. For a more thorough treatment we refer to [Iarrobino and Kanev 1999; Eisenbud 1995; Casnati and Notari 2009; Jelisiejew 2014a].

Finite-type, zero-dimensional schemes correspond to Artin algebras. Every such algebra A splits as a finite product of its localizations at maximal ideals, which corresponds to the fact that the support of $\operatorname{Spec} A$ is finite and totally disconnected. Therefore, we will focus our interest on *local* Artin k-algebras. Since k is algebraically closed, such algebras have residue field k.

An important invariant of a local algebra $(A, \mathfrak{m}, k)$ is its Hilbert function H_A, defined by $H_A(l) = \dim_k \mathfrak{m}^l/\mathfrak{m}^{l+1}$. Since $H_A(l) = 0$ for $l \gg 0$, it is usual to write H_A as the vector of its nonzero values. The *socle degree* of A is the largest l such that $H_A(l) \neq 0$. Such an algebra is *Gorenstein* if the annihilator of $\mathfrak{m}$ is a one-dimensional vector space over k; see [Eisenbud 1995, Chapter 21].

We recall for the reader's benefit that a finite, not necessarily local, algebra A is Gorenstein if and only if all its localizations at maximal ideals are Gorenstein (in particular, it is meaningful to discuss the irreducibility of the Gorenstein locus in the Hilbert scheme by reducing to the study of deformations of local Gorenstein algebras; see Section 2D).

Since k is algebraically closed, we may write each Artin local algebra $(A, \mathfrak{m}, k)$ as a quotient of the power series ring $S = k[\![\alpha_1, \dots, \alpha_n]\!]$ when n is large enough; in fact, $n \geq H_A(1)$ is sufficient. Since $\dim_k A$ is finite, such a presentation gives a presentation $A = S_{\text{poly}}/I$, i.e., a point $[\operatorname{Spec} A]$ of the Hilbert scheme of $\mathbb{A}^n = \operatorname{Spec} S_{\text{poly}}$.

2B. ***Contraction map and apolar algebras.*** In this section we introduce the contraction mapping, which is closely related to Macaulay's inverse systems. We refer to [Iarrobino 1994; Eisenbud 1995, Chapter 21] for details and proofs.

Recall that $P = k[x_1, \dots, x_n]$ is a polynomial ring and $S = k[\![\alpha_1, \dots, \alpha_n]\!]$ is a power series ring. The k-algebra S acts on P by *contraction* (see [Iarrobino and Kanev 1999, Definition 1.1]). This action is denoted by $(\,\cdot\,) \lrcorner (\,\cdot\,) : S \times P \to P$ and defined as follows. Let $\boldsymbol{x}^{\boldsymbol{a}} = x_1^{a_1} \cdots x_n^{a_n} \in P$ and $\boldsymbol{\alpha}^{\boldsymbol{b}} = \alpha_1^{b_1} \cdots \alpha_n^{b_n} \in S$ be monomials. We write $\boldsymbol{a} \geq \boldsymbol{b}$ if and only if $a_i \geq b_i$ for all $1 \leq i \leq n$. Then

$$\boldsymbol{\alpha}^{\boldsymbol{b}} \lrcorner \boldsymbol{x}^{\boldsymbol{a}} := \begin{cases} \boldsymbol{x}^{\boldsymbol{a}-\boldsymbol{b}} & \text{if } \boldsymbol{a} \geq \boldsymbol{b}, \\ 0 & \text{otherwise.} \end{cases}$$

This action extends to $S \times P \to P$ by k-linearity on P and countable k-linearity on S.

The contraction action induces a perfect pairing between $S/\mathfrak{m}_S^{s+1}$ and $P_{\leq s}$, which restricts to a perfect pairing between the degree-s polynomials in S_{poly} and P. These pairings are compatible for different choices of s.

If $f \in P$ then a *derivative* of f is an element of the S-module Sf, i.e., an element of the form $\partial \lrcorner f$ for $\partial \in S$. By definition, these elements form an S-submodule of P, in particular a k-linear subspace.

Let $A = S/I$ be an Artin quotient of S; then A is local. The contraction action associates to A an S-submodule $M \subseteq P$ consisting of elements annihilated by I, so that A and M are dual. If A is Gorenstein, then the S-module M is cyclic, generated by a polynomial f of degree s equal to the socle degree of A. We call every such f a *dual socle generator of the Artin Gorenstein algebra* A. Unlike M, the polynomial f is *not determined uniquely by the choice of the presentation* $A = S/I$, however, if f and g are two dual socle generators, then $g = \partial \lrcorner f$, where $\partial \in S$ is invertible.

Conversely, let $f \in P$ be a polynomial of degree s. We can associate to it the ideal $I := \operatorname{ann}_S(f)$ such that $A := S/I$ is a local Artin Gorenstein algebra of socle degree s. We call I the *apolar ideal* of f and A the *apolar algebra* of f, which we denote as

$$A = \operatorname{Apolar}(f).$$

From the discussion above it follows that every local Artin Gorenstein algebra is an apolar algebra of some polynomial.

Remark 2.2. Recall that we may think of $S/\mathfrak{m}_S^{s+1}$ as the linear space dual to $P_{\leq s}$. An automorphism ψ of S or $S/\mathfrak{m}_S^{s+1}$ induces an automorphism ψ^* of the k-linear space $P_{\leq s}$. If $f \in P_{\leq s}$ and I is the apolar ideal of f, then $\psi(I)$ is the apolar ideal of $\psi^*(f)$. Moreover, f and $\psi^*(f)$ have the same degree.

2C. ***Iarrobino's symmetric decomposition of Hilbert function.*** One of the most important invariants possessed by a local Artin Gorenstein algebra is the symmetric decomposition of its Hilbert function, due to Iarrobino [1994]. To state the theorem it is convenient to define addition of vectors of different lengths position-wise: if $a = (a_0, \ldots, a_n)$ and $b = (b_0, \ldots, b_m)$ are vectors, then $a + b = (a_0 + b_0, \ldots, a_{\max(m,n)} + b_{\max(m,n)})$, where $a_i = 0$ for $i > n$ and $b_i = 0$ for $i > m$. In the following, all vectors are indexed starting from zero.

Let $(A, \mathfrak{m}, k)$ be a local Artin Gorenstein algebra. By $(0 : \mathfrak{m}^l)$ we denote the annihilator of $\mathfrak{m}^l$ in A. The chain $0 = (0 : \mathfrak{m}^0) \subseteq (0 : \mathfrak{m}^1) \subseteq \cdots$ defines a filtration on A. In general, it is different from the usual filtration $0 = \mathfrak{m}^{s+1} \subseteq \mathfrak{m}^s \subseteq \mathfrak{m}^{s-1} \subseteq \cdots$. The analysis of mutual position of these filtrations is the content of Theorem 2.3.

Theorem 2.3 (Iarrobino's symmetric decomposition of the Hilbert function). *Let* $(A, \mathfrak{m}, k)$ *be a local Artin Gorenstein algebra of socle degree* s *with Hilbert function* H_A. *Let*

$$\Delta_i(t) := \dim_k \frac{(0 : \mathfrak{m}^{s+1-i-t}) \cap \mathfrak{m}^t}{(0 : \mathfrak{m}^{s-i-t}) \cap \mathfrak{m}^t + (0 : \mathfrak{m}^{s+1-i-t}) \cap \mathfrak{m}^{t+1}} \quad \text{for } t = 0, 1, \ldots, s-i.$$

The vectors $\Delta_0, \Delta_1, \ldots, \Delta_s$ *have the following properties*:

(1) *The vector* Δ_i *has length* $s+1-i$ *and satisfies* $\Delta_i(t) = \Delta_i(s-i-t)$ *for all integers* $t \in [0, s-i]$.

(2) *The Hilbert function* H_A *is equal to the sum* $\sum_{i=0}^{s} \Delta_i$.

(3) *The vector* Δ_0 *is equal to the Hilbert function of a local Artin Gorenstein* graded *algebra of socle degree* s.

Let $(A, \mathfrak{m}, k)$ be a local Artin Gorenstein algebra. There are a few important remarks to make.

(1) Since Δ_0 is the Hilbert function of an algebra, we have $\Delta_0(0) = 1 = H_A(0)$. Thus, for every $i > 0$ we have $\Delta_i(0) = 0$. From symmetry, it follows that $\Delta_i(s+1-i) = 0$. In particular, $\Delta_s = (0)$ and $\Delta_{s-1} = (0, 0)$, so we may ignore these vectors. On the other hand, $\Delta_{s-2} = (0, q, 0)$ is in general nonzero and its importance is illustrated by Proposition 4.5.

(2) Suppose that $H_A = (1, n, 1, 1)$ for some $n > 0$. Then we have $\Delta_0 = (1, *, *, 1)$ and $\Delta_1 = (0, *, 0)$, thus $\Delta_0 = (1, *, 1, 1)$, so that $\Delta_0 = (1, 1, 1, 1)$ because of its symmetry. Then $\Delta_1 = (0, n-1, 0)$. Similarly, if $H_A = (1, n, e, 1)$ is the Hilbert function of a local Artin Gorenstein algebra, then $n \geq e$. This is a basic example of how Theorem 2.3 imposes restrictions on the Hilbert function of A.

(3) If A is graded, then $\Delta_0 = H_A$ and all other $\Delta_\bullet$ are zero vectors; see [Iarrobino 1994, Proposition 1.7].

(4) For every $a \leq s$ the partial sum $\sum_{i=0}^{a} \Delta_i$ is the Hilbert function of a local Artin graded algebra; see [Iarrobino 1994, Definition 1.3, Theorem 1.5]; see also [Iarrobino 1994, Subsection 1.F]. In particular, it satisfies Macaulay's growth theorem; see Section 2E. Thus, e.g., there is no local Artin Gorenstein algebra with Hilbert function decomposition satisfying $\Delta_0 = (1, 1, 1, 1, 1, 1)$ and $\Delta_1 = (0, 0, 1, 0, 0)$, because then $(\Delta_0 + \Delta_1)(1) = 1$ and $(\Delta_0 + \Delta_1)(2) = 2$.

Let us now analyze the case when $A = \mathrm{Apolar}(f) = S/\operatorname{ann}_S(f)$ is the apolar algebra of a polynomial $f \in P$, where $f = \sum_{i=0}^{s} f_i$ for some $f_i \in P_i$. Each local Artin Gorenstein algebra is isomorphic to such an algebra; see Section 2B. For the proofs of the following remarks, see [Iarrobino 1994].

(1) The vector Δ_0 is equal to the Hilbert function of $\mathrm{Apolar}(f_s)$, the apolar algebra of the leading form of f.

(2) If A is graded, then $\operatorname{ann}_S(f) = \operatorname{ann}_S(f_s)$, so that we may always assume that $f = f_s$. Moreover, in this case $H_A(m)$ is equal to $(Sf_s)_m$, the number of degree-m derivatives of f_s.

(3) Let f_1 and f_2 be polynomials of degree s such that $f_1 - f_2$ is a polynomial of degree $d < s$. Let $A_i = \mathrm{Apolar}(f_i)$ and let $\Delta_{A_i,m}$ be the symmetric decomposition of

the Hilbert function H_{A_i} of A_i for $i = 1, 2$. Then $\Delta_{A_1,m} = \Delta_{A_2,m}$ for all $m < s - d$; see [Iarrobino 1994, Lemma 1.10].

2D. ***Smoothability and unobstructedness.*** An Artin algebra A is called *smoothable* if it is a (finite flat) limit of smooth algebras, i.e., if there exists a finite flat family over an irreducible base with a special fiber isomorphic to Spec A and general fiber smooth. Recall that $A \simeq A_{\mathfrak{m}_1} \times \cdots \times A_{\mathfrak{m}_r}$, where the $\mathfrak{m}_i$ are maximal ideals of A. The algebra A is smoothable if all localizations $A_{\mathfrak{m}}$ at its maximal ideals are smoothable. The converse also holds, that is, if an algebra $A \simeq B_1 \times B_2$ is smoothable, then the algebras B_1 and B_2 are also smoothable; a complete and characteristic-free proof of this fact will appear shortly in [Buczyński and Jelisiejew 2014]. We say that a zero-dimensional scheme $Z = \operatorname{Spec} A$ is *smoothable* if the algebra A is smoothable.

It is crucial that every local Artin Gorenstein algebra A with $H_A(1) \leq 3$ is smoothable — see [Casnati and Notari 2009, Proposition 2.5] — which follows from the Buchsbaum–Eisenbud [1977] classification of resolutions. Also, complete intersections are smoothable. A complete intersection $Z \subseteq \mathbb{P}^n$ is smoothable by Bertini's theorem (see [Hartshorne 2010, Example 29.0.1], but note that Hartshorne uses a slightly weaker definition of smoothability, without a finiteness assumption). If $Z = \operatorname{Spec} A$ is a complete intersection in $\mathbb{A}^n$, then Z is a union of connected components of a complete intersection $Z' = \operatorname{Spec} B$ in $\mathbb{P}^n$, so that $B \simeq A \times C$ for some algebra C. The algebra B is smoothable since Z' is. Thus also the algebra A is smoothable, i.e., Z is smoothable.

Definition 2.4. A smoothable Artin algebra A of length d, corresponding to the subset Spec A of $\mathbb{P}^n$, is *unobstructed* if the tangent space to $\mathcal{H}ilb_d(\mathbb{P}^n)$ at the k-point $[\operatorname{Spec} A] =: p$ has dimension nd. If A is unobstructed, then p is a smooth point of the Hilbert scheme.

The unobstructedness is independent of n and the chosen embedding of Spec A into $\mathbb{P}^n$; see the discussion before [Casnati and Notari 2009, Lemma 2.3]. The argument above shows that algebras corresponding to complete intersections in $\mathbb{A}^n$ and $\mathbb{P}^n$ are unobstructed. Every local Artin Gorenstein algebra A with $H_A(1) \leq 3$ is unobstructed; see [Casnati and Notari 2009, Proposition 2.5]. Moreover, every local Artin Gorenstein algebra A with $H_A(1) \leq 2$ is a complete intersection in $\mathbb{A}^2$, by the Hilbert–Burch theorem.

Definition 2.5. An Artin algebra A is *limit-reducible* if there exists a flat family (over an irreducible base) whose special fiber is A and general fiber is reducible. An Artin algebra A is *strongly nonsmoothable* if it is not limit-reducible.

Clearly, strongly nonsmoothable algebras (other than $A = k$) are nonsmoothable. The definition of strong nonsmoothability is useful, because to show that there is

no nonsmoothable algebra of length less than d it is enough to show that there is no strongly nonsmoothable algebra of length less than d.

2E. ***Macaulay's growth theorem.*** We will recall Macaulay's growth theorem and Gotzmann's persistence theorem, which provide strong restrictions on the possible Hilbert functions of graded algebras. Fix $n \geq 1$. Let m be any natural number; then m may be uniquely written in the form

$$m = \binom{m_n}{n} + \binom{m_{n-1}}{n-1} + \cdots + \binom{m_1}{1},$$

where $m_n > m_{n-1} > \cdots > m_1$. We define

$$m^{\langle i \rangle} := \binom{m_n+1}{n+1} + \binom{m_{n-1}+1}{n} + \cdots + \binom{m_1+1}{2}.$$

It is useful to compute some initial values of the above-defined function: $1^{\langle n \rangle} = 1$ for all n, $3^{\langle 2 \rangle} = 4$, $4^{\langle 2 \rangle} = 5$, $6^{\langle 2 \rangle} = 10$ and $4^{\langle 3 \rangle} = 5$.

Theorem 2.6 (Macaulay's growth theorem). *If A is a graded quotient of a polynomial ring over k, then the Hilbert function H_A of A satisfies $H_A(m+1) \leq H_A(m)^{\langle m \rangle}$ for all m.*

Proof. See [Bruns and Herzog 1993, Theorem 4.2.10]. □

Note that the assumptions of Theorem 2.6 are satisfied for every local Artin k-algebra $(A, \mathfrak{m}, k)$, since its Hilbert function is by definition equal to the Hilbert function of the associated graded algebra.

Remark 2.7. We will frequently use this easy consequence of Theorem 2.6:

Let A be a graded quotient of a polynomial ring over k. Suppose that $H_A(l) \leq l$ for some l. Then $H_A(l) = \binom{l}{l} + \binom{l-1}{l-1} + \cdots$ and $H_A(l)^{\langle l \rangle} = \binom{l+1}{l+1} + \binom{l}{l} + \cdots = H_A(l)$, thus $H_A(l+1) \leq H_A(l)$. It follows that the Hilbert function of H_A satisfies $H_A(l) \geq H_A(l+1) \geq H_A(l+2) \geq \cdots$. In particular, $H_A(m) \leq l$ for all $m \geq l$.

Theorem 2.8 (Gotzmann's persistence theorem). *Let $A = S_{\text{poly}}/I$ be a graded quotient of a polynomial ring S_{poly} over k and suppose that for some l we have $H_A(l+1) = H_A(l)^{\langle l \rangle}$ and that I is generated by elements of degree at most l. Then $H_A(m+1) = H_A(m)^{\langle m \rangle}$ for all $m \geq l$.*

Proof. See [Bruns and Herzog 1993, Theorem 4.3.3]. □

We will mostly use the following consequence of Theorem 2.8, for which we introduce some (nonstandard) notation. Let $I \subseteq S_{\text{poly}} = k[\alpha_1, \ldots, \alpha_n]$ be a graded ideal in a polynomial ring and $m \geq 0$. We say that I is *m-saturated* if, for all $l \leq m$ and $\sigma \in (S_{\text{poly}})_l$, the condition $\sigma \cdot (\alpha_1, \ldots, \alpha_n)^{m-l} \subseteq I$ implies $\sigma \in I$.

Lemma 2.9. *Let $S_{\text{poly}} = k[\alpha_1, \ldots, \alpha_n]$ be a polynomial ring with maximal ideal $\mathfrak{n} = (\alpha_1, \ldots, \alpha_n)$. Let $I \subseteq S_{\text{poly}}$ be a graded ideal and $A = S_{\text{poly}}/I$. Suppose that I is m-saturated for some $m \geq 2$. Then*:

(1) *If $H_A(m) = m+1$ and $H_A(m+1) = m+2$, then $H_A(l) = l+1$ for all $l \leq m$; in particular, $H_A(1) = 2$.*

(2) *If $H_A(m) = m+2$ and $H_A(m+1) = m+3$, then $H_A(l) = l+2$ for all $l \leq m$; in particular, $H_A(1) = 3$.*

Proof. (1) First, if $H_A(l) \leq l$ for some $l < m$ then, by Macaulay's growth theorem, $H_A(m) \leq l < m+1$, a contradiction. So it suffices to prove that $H_A(l) \leq l+1$ for all $l < m$.

Let J be the ideal generated by elements of degree at most m in I. We will prove that the graded ideal J of S_{poly} defines a $\mathbb{P}^1$ linearly embedded into $\mathbb{P}^{n-1}$.

Let $B = S_{\text{poly}}/J$. Then $H_B(m) = m+1$ and $H_B(m+1) \geq m+2$. Since $H_B(m) = m+1 = \binom{m+1}{m}$, we have $H_B(m)^{\langle m \rangle} = \binom{m+2}{m+1} = m+2$ and, by Theorem 2.6, we get $H_B(m+1) \leq m+2$, thus $H_B(m+1) = m+2$. Then, by Gotzmann's persistence theorem, $H_B(l) = l+1$ for all $l > m$. This implies that the Hilbert polynomial of $\operatorname{Proj} B \subseteq \mathbb{P}^{n-1}$ is $h_B(t) = t+1$, so that $\operatorname{Proj} B \subseteq \mathbb{P}^{n-1}$ is a linearly embedded $\mathbb{P}^1$. In particular, the Hilbert function and Hilbert polynomial of $\operatorname{Proj} B$ are equal for all arguments. By assumption, we have $J_l = J_l^{\text{sat}}$ for all $l < m$. Then $H_A(l) = H_{S_{\text{poly}}/J}(l) = H_{S_{\text{poly}}/J^{\text{sat}}}(l) = l+1$ for all $l < m$ and the claim of the lemma follows.

(2) The proof is similar to that of (1); we mention only the points where it changes. Let J be the ideal generated by elements of degree at most m in I and $B = S_{\text{poly}}/J$. Then $H_B(m) = m+2 = \binom{m+1}{m} + \binom{m-1}{m-1}$, thus $H_B(m+1) \leq \binom{m+2}{m+1} + \binom{m}{m} = m+3$ and B defines a closed subscheme of $\mathbb{P}^{n-1}$ with Hilbert polynomial $h_B(t) = t+2$. There are two isomorphism types of such subschemes: the union of $\mathbb{P}^1$ and a point, and $\mathbb{P}^1$ with an embedded double point. One checks that for these schemes the Hilbert polynomial is equal to the Hilbert function for all arguments and then proceeds as in the proof of part (1). □

Remark 2.10. If $A = S_{\text{poly}}/I$ is a graded Artin Gorenstein algebra of socle degree s, then it is m-saturated for every $m \leq s$. Indeed, we may assume that $A = \text{Apolar}(F)$ for some homogeneous $F \in P$ of degree s; then $I = \operatorname{ann}_S(F)$. Let $\mathfrak{n} = (\alpha_1, \ldots, \alpha_n) \subseteq k[\alpha_1, \ldots, \alpha_n] = S_{\text{poly}}$. Take $\sigma \in (S_{\text{poly}})_l$; then $\sigma \in I$ if and only if $\sigma \lrcorner F = 0$. Similarly, $\sigma \mathfrak{n}^{m-l} \subseteq I$ if and only if every element of $\mathfrak{n}^{m-l}$ annihilates $\sigma \lrcorner F$. Since $\sigma \lrcorner F$ is either a homogeneous polynomial of degree $s-l \geq m-l$ or it is zero, both conditions are equivalent.

Remark 2.11. Clearly, if two graded ideals I and J of S_{poly} agree up to degree m and I is m-saturated, then also J is m-saturated.

2F. *Flatness over* Spec $k[t]$. For further reference we explicitly state a purely elementary flatness criterion. Its formulation is a bit complicated, but this is precisely the form which is needed for the proofs. This criterion relies on the easy observation that the torsion-free modules over $k[t]$ are flat.

Proposition 2.12. *Suppose S is a k-module and $I \subseteq S[t]$ is a $k[t]$-submodule. Let $I_0 := I \cap S$. If, for every $\lambda \in k$, we have*

$$(t-\lambda) \cap I \subseteq (t-\lambda)I + I_0[t],$$

then $S[t]/I$ is a flat $k[t]$-module.

Proof. The ring $k[t]$ is a principal ideal domain; thus, a $k[t]$-module is flat if and only if it is torsion-free; see [Eisenbud 1995, Corollary 6.3]. Since every polynomial in $k[t]$ decomposes into linear factors, to prove that $M = S[t]/I$ is torsion-free it is enough to show that $t-\lambda$ are non-zerodivisors on M, i.e., that $(t-\lambda)x \in I$ implies $x \in I$ for all $x \in S[t]$, $\lambda \in k$.

Fix $\lambda \in k$ and suppose that $x \in S[t]$ is such that $(t-\lambda)x \in I$. Then, by assumption, $(t-\lambda)x \in (t-\lambda)I + I_0[t]$, so that $(t-\lambda)(x-i) \in I_0[t]$ for some $i \in I$. Since $S[t]/I_0[t] \simeq S/I_0[t]$ is a free $k[t]$-module, we have $x - i \in I_0[t] \subseteq I$ and so $x \in I$. □

Remark 2.13. Let $i_1, \ldots, i_r$ be the generators of I. To check the inclusion which is the assumption of Proposition 2.12, it is enough to check that $s \in (t-\lambda) \cap I$ implies $s \in (t-\lambda)I + I_0[t]$ for all $s = s_1 i_1 + \cdots + s_r i_r$, where $s_i \in S$.

Indeed, take an arbitrary element $s \in I$ and write $s = t_1 i_1 + \cdots + t_r i_r$, where $t_1, \ldots, t_r \in S[t]$. Dividing t_i by $t-\lambda$, we obtain $s = s_1 i_1 + \cdots + s_r i_r + (t-\lambda)i$, where $i \in I$ and $s_i \in S$. Let $s' = s_1 i_1 + \cdots + s_r i_r$; then $s \in (t-\lambda) \cap I$ if and only if $s' \in (t-\lambda) \cap I$, and $s \in (t-\lambda)I + I_0[t]$ if and only if $s' \in (t-\lambda)I + I_0[t]$.

Example 2.14. Consider $S = k[x, y]$ and $I = xyS[t] + (x^3 - tx)S[t] \subseteq S[t]$. Take an element $s_1 xy + s_2(x^3 - tx) \in I$ and suppose $s_1 xy + s_2(x^3 - tx) \in (t-\lambda)S[t]$. We want to prove that this element lies in $I_0[t] + (t-\lambda)I$. As in Remark 2.13, by subtracting an element of $I(t-\lambda)$ we may assume that s_1 and s_2 lie in S. Then $s_1 xy + s_2(x^3 - tx) \in (t-\lambda)S[t]$ if and only if $s_1 xy + s_2(x^3 - \lambda x) = 0$. In particular, we have $s_2 \in yS$, so that $s_2(x^3 - tx) \in xyS[t]$; then $s_1 xy + s_2(x^3 - tx) \in xyS[t] \subseteq I_0[t]$.

Similarly, we will frequently use the following easy observation:

Lemma 2.15. *Consider a ring $R = B[\alpha]$ graded by the degree of α. Let d be a natural number and $I \subseteq R$ be a homogeneous ideal generated in degrees less or equal to d.*

Let $q \in B[\alpha]$ be an element of α-degree strictly less than d such that for every $b \in B$ satisfying $b\alpha^d \in I$, we have $bq \in I$. Then, for every $r \in R$,

$$r(\alpha^d - q) \in I \quad \Longrightarrow \quad r\alpha^d \in I \quad \text{and} \quad rq \in I.$$

Proof. We apply induction on α-degree of r, the base case being $r = 0$. Write

$$r = \sum_{i=0}^{m} r_i \alpha^i, \quad \text{where} \quad r_i \in B.$$

The leading form of $r(\alpha^d - q)$ is $r_m \alpha^{m+d}$ and it lies in I. Since I is homogeneous and generated in degree at most d, we have $r_m \alpha^d \in I$. Then $r_m q \in I$ by assumption, so that $\hat{r} := r - r_m \alpha^m$ satisfies $\hat{r}(\alpha^d - q) \in I$. By induction we have $\hat{r}\alpha^d, \hat{r}q \in I$, then also $r\alpha^d, rq \in I$. □

3. Standard form of the dual generator

Definition 3.1. Let $f \in P = k[x_1, \dots, x_n]$ be a polynomial of degree s. Let $I = \operatorname{ann}_S(f)$ and $A = S/I = \operatorname{Apolar}(f)$. By $\Delta_\bullet$ we denote the decomposition of the Hilbert function of A and we set $e(a) := \sum_{t=0}^{a} \Delta_t(1)$.

We say that f *is in the standard form* if

$$f = f_0 + f_1 + f_2 + f_3 + \cdots + f_s, \quad \text{where} \quad f_i \in P_i \cap k[x_1, \dots, x_{e(s-i)}] \text{ for all } i.$$

Note that if f is in the standard form and $\partial \in \mathfrak{m}_S$, then $f + \partial \lrcorner f$ is also in the standard form. We say that an Artin Gorenstein algebra S/I is in the *standard form* if any (or every) dual socle generator of S/I is in the standard form; see Proposition 3.5 below.

Example 3.2. If $f = x_1^6 + x_2^5 + x_3^3$, then f is in the standard form. Indeed, $e(0) = 1$, $e(1) = 2$, $e(2) = 2$, $e(3) = 3$ so that we should check that $x_1^6 \in k[x_1]$, $x_2^5 \in k[x_1, x_2]$ and $x_3^3 \in k[x_1, x_2, x_3]$, which is true. To contrast, $g = x_3^6 + x_2^5 + x_1^3$ is not in the standard form, but may be put in the standard form via a change of variables.

The change of variables procedure of Example 3.2 may be generalized to prove that every local Artin Gorenstein algebra can be put in a standard form:

Proposition 3.3. *For every Artin Gorenstein algebra S/I there is an automorphism $\varphi : S \to S$ such that $S/\varphi(I)$ is in the standard form.*

Proof. See [Iarrobino 1994, Theorem 5.3AB]; the proof is rewritten in [Jelisiejew 2014a, Theorem 4.38]. □

The idea of the proof of Proposition 3.3 is to "linearize" some elements of S. This is quite technical and perhaps it can be best seen in the following example.

Example 3.4. Let $f = x_1^6 + x_1^4 x_2$. The annihilator of f in S is $(\alpha_2^2, \alpha_1^5 - \alpha_1^3\alpha_2)$, the Hilbert function of $\operatorname{Apolar}(f)$ is $(1, 2, 2, 2, 1, 1, 1)$ and the symmetric decomposition is

$$\Delta_0 = (1, 1, 1, 1, 1, 1, 1), \quad \Delta_1 = (0, 0, 0, 0, 0, 0), \quad \Delta_2 = (0, 1, 1, 1, 0).$$

This shows that $e(0) = 1$, $e(1) = 1$ and $e(2) = 2$. If f is in the standard form we should have $f_5 = x_1^4 x_2 \in k[x_1, \ldots, x_{e(1)}] = k[x_1]$. This means that f is not in the standard form. The "reason" for $e(1) = 1$ is the fact that $\alpha_1^3(\alpha_2 - \alpha_1^2)$ annihilates f, and the "reason" for $f_5 \notin k[x_1]$ is that $\alpha_2 - \alpha_1^2$ is not a linear form. Thus we make $\alpha_2 - \alpha_1^2$ a linear form by twisting by a suitable automorphism of S.

We define an automorphism $\psi : S \to S$ by $\psi(\alpha_1) = \alpha_1$ and $\psi(\alpha_2) = \alpha_2 + \alpha_1^2$, so that we have $\psi(\alpha_2 - \alpha_1^2) = \alpha_2$. The automorphism maps the annihilator of f to the ideal $I := ((\alpha_2 + \alpha_1^2)^2, \alpha_1^3\alpha_2)$. We will see that the algebra S/I is in the standard form and also find a particular dual generator obtained from f.

As mentioned in Remark 2.2, the automorphism ψ induces an automorphism ψ^* of the k-linear space $P_{\leq 6}$. This automorphism maps f to a dual socle generator $\psi^* f$ of S/I.

The element $F := \psi^* x_1^6$ is the only element of P such that $\psi(\alpha_1^7) \lrcorner F = \psi(\alpha_2) \lrcorner F = 0$, $\psi(\alpha_1^6)(F) = 1$ and $\psi(\alpha_1^l)(F) = 0$ for $l \leq 5$. Caution: in the last line we use evaluation on the functional and not the induced action (see Remark 2.2). One can compute that $\psi^* x_1^6 = x_1^6 - x_1^4 x_2 + x_1^2 x_2^2 - x_2^3$ and similarly $\psi^* x_1^4 x_2 = x_1^4 x_2 - 2x_1^2 x_2 + 3x_2^3$, so that $\psi^* f = x_1^6 - x_1^2 x_2^2 + 2x_2^3$. Now indeed $x_1^6 \in k[x_1]$, $x_1^2 x_2^2 \in k[x_1, x_2]$ and $2x_2^3 \in k[x_1, x_2]$, so the dual socle generator is in the standard form.

We note the following equivalent conditions for a dual socle generator to be in the standard form:

Proposition 3.5. *In the notation of Definition 3.1, the following conditions are equivalent for a polynomial $f \in P$:*

(1) *The polynomial f is in the standard form.*

(2) *For all r and i such that $r > e(s-i)$, we have $\mathfrak{m}_S^{i-1}\alpha_r \subseteq I = (f)^\perp$. Equivalently, for all r and i such that $r > e(i)$, we have $\mathfrak{m}_S^{s-i-1}\alpha_r \subseteq I = (f)^\perp$.*

Proof. Straightforward. □

Corollary 3.6. *Let $f \in P$ be such that the algebra S/I is in the standard form, where $I = \operatorname{ann}_S(f)$. Let φ be an automorphism of S given by*

$$\varphi(\alpha_i) = \kappa_i \alpha_i + q_i,$$

where q_i is such that $\deg(q_i \lrcorner f) \leq \deg(\alpha_i \lrcorner f)$ and $\kappa_i \in k \setminus \{0\}$. Then the algebra $S/\varphi^{-1}(I)$ is also in the standard form.

Proof. The algebras S/I and $S/\varphi^{-1}(I)$ are isomorphic; in particular, they have equal functions $e(\cdot)$. By Proposition 3.5 it suffices to prove that if, for some r and i, we have $\mathfrak{m}_S^r \alpha_i \subseteq I$, then $\mathfrak{m}_S^r \alpha_i \subseteq \varphi^{-1}(I)$. The latter condition is equivalent to $\mathfrak{m}_S^r \varphi(\alpha_i) \subseteq I$. If $\mathfrak{m}_S^r \alpha_i \lrcorner f = 0$ then $\deg(\alpha_i \lrcorner f) < r$ so, by assumption, $\deg(q_i \lrcorner f) < r$; thus $\mathfrak{m}_S^r q_i \lrcorner f = 0$ and $\mathfrak{m}_S^r \varphi(\alpha_i) = \mathfrak{m}_S^r(\kappa_i \alpha_i + q_i) \lrcorner f = 0$. □

Corollary 3.7. *Suppose that $q \in \mathfrak{m}_S^2$ does not contain α_i and let $\varphi : S \to S$ be an automorphism given by*

$$\varphi(\alpha_j) = \begin{cases} \alpha_j & \text{if } j \neq i, \\ \kappa_i \alpha_i + q & \text{if } j = i, \end{cases}$$

where $\kappa_i \in k \setminus \{0\}$. Suppose that S/I is in the standard form, where $I = \operatorname{ann}_S(f)$, and that $\deg(q \lrcorner f) \leq \deg(\alpha_i \lrcorner f)$. Then the algebras $S/\varphi(I)$ and $S/\varphi^{-1}(I)$ are also in the standard form.

Proof. Note that $\psi : S \to S$, given by $\psi(\alpha_j) = \alpha_j$ for $j \neq i$ and $\psi(\alpha_i) = \kappa_i^{-1}(\alpha_i - q)$, is an automorphism of S and, furthermore, $\psi(\kappa_i \alpha_i + q) = \alpha_i - q + q = \alpha_i$, so that $\psi = \varphi^{-1}$. Both φ and ψ satisfy assumptions of Corollary 3.6, so both $S/\varphi^{-1}(I)$ and $S/\psi^{-1}(I) = S/\varphi(I)$ are in the standard form. □

Remark 3.8. The assumption $q \in \mathfrak{m}_S^2$ of Corollary 3.7 is needed only to ensure that φ is an automorphism of S. On the other hand, the fact that q does not contain α_i is important, because it allows us to control φ^{-1} and, in particular, prove that $S/\varphi(I)$ is in the standard form.

The following corollary is a straightforward generalization of Corollary 3.7, but the notation is difficult. We first choose a set $\mathcal{K}$ of variables. The automorphism sends each variable from $\mathcal{K}$ to (a multiple of) itself plus a suitable polynomial in variables not appearing in $\mathcal{K}$.

Corollary 3.9. *Take $\mathcal{K} \subseteq \{1, 2, \ldots, n\}$ and $q_i \in \mathfrak{m}_S^2$ for $i \in \mathcal{K}$ which do not contain any variables from the set $\{\alpha_i\}_{i \in \mathcal{K}}$. Define $\varphi : S \to S$ by*

$$\varphi(\alpha_i) = \begin{cases} \alpha_i & \text{if } i \notin \mathcal{K} \\ \kappa_i \alpha_i + q_i & \text{if } i \in \mathcal{K}, \end{cases}$$

where $\kappa_i \in k \setminus \{0\}$. Suppose that S/I is in the standard form, where $I = \operatorname{ann}_S(f)$, and that $\deg(q_i \lrcorner f) \leq \deg(\alpha_i \lrcorner f)$ for all $i \in \mathcal{K}$. Then the algebras $S/\varphi(I)$ and $S/\varphi^{-1}(I)$ are also in the standard form. □

4. Special forms of dual socle generators

Recall that k is an algebraically closed field of characteristic neither 2 nor 3.

In the previous section we mentioned that for every local Artin Gorenstein algebra there exists a dual socle generator in the standard form; see Definition 3.1. In this section we will see that in most cases we can say more about this generator. Our main aim is to put the generator in the form $x^s + f$, where f contains no monomial divisible by a "high" power of x. We will use it to prove that families arising from certain ray decompositions (see Definition 5.2) are flat.

We begin with an easy observation.

Remark 4.1. Suppose that a polynomial $f \in P$ is such that $H_{\mathrm{Apolar}(f)}(1)$ equals the number of variables in P. Then any linear form in P is a derivative of f. If $\deg f > 1$ then the S-submodules Sf and $S(f - f_1 - f_0)$ are equal, so analyzing this modules we may assume $f_1 = f_0 = 0$, i.e., the linear part of f is zero.

Later we use this remark implicitly.

The following lemma provides a method to slightly improve the given dual socle generator. This improvement is the building block of all other results in this section.

Lemma 4.2. *Let $f \in P$ be a polynomial of degree s and A be the apolar algebra of f. Suppose that $\alpha_1^s \lrcorner f \neq 0$. For every i, let $d_i := \deg(\alpha_1\alpha_i \lrcorner f) + 2$.*

Then A is isomorphic to the apolar algebra of a polynomial $\hat{f}$ of degree s such that $\alpha_1^s \lrcorner \hat{f} = 1$ and $\alpha_1^{d_i-1}\alpha_i \lrcorner \hat{f} = 0$ for all $i \neq 1$. Moreover, the leading forms of f and $\hat{f}$ are equal up to a nonzero constant. If f is in the standard form, then $\hat{f}$ is also in the standard form.

Proof. By multiplying f by a nonzero constant we may assume that $\alpha_1^s \lrcorner f = 1$. Denote $I := \mathrm{ann}_S(f)$. Since $\deg(\alpha_1\alpha_i \lrcorner f) = d_i - 2$, the polynomial $\alpha_1^{d_i-1}\alpha_i \lrcorner f = \alpha_1^{d_i-2}(\alpha_1\alpha_i \lrcorner f)$ is constant; we denote it by λ_i. Then

$$(\alpha_1^{d_i-1}\alpha_i - \lambda_i\alpha_1^s) \lrcorner f = 0, \quad \text{so that} \quad \alpha_1^{d_i-1}(\alpha_i - \lambda_i\alpha_1^{s-d_i+1}) \in I.$$

Define an automorphism $\varphi : S \to S$ by

$$\varphi(\alpha_i) = \begin{cases} \alpha_1 & \text{if } i = 1, \\ \alpha_i - \lambda_i\alpha_1^{s-d_i+1} & \text{if } i \neq 1; \end{cases}$$

then $\alpha_1^{d_i-1}\alpha_i \in \varphi^{-1}(I)$ for all $i > 1$. The dual socle generator $\hat{f}$ of the algebra $S/\varphi^{-1}(I)$ has the required form. We can easily check that the graded algebras of $S/\varphi^{-1}(I)$ and S/I are equal; in particular, $\hat{f}$ and f have the same leading form, up to a nonzero constant.

Suppose now that f is in the standard form. Let $i \in \{1, \dots, n\}$. Then $d_i = \deg(\alpha_1\alpha_i \lrcorner f) + 2 \leq \deg(\alpha_i \lrcorner f) + 1$, so that $\deg(\alpha_1^{s-d_i+1} \lrcorner f) \leq d_i - 1 \leq \deg(\alpha_i \lrcorner f)$. Since φ is an automorphism of S, by Remark 3.8 we may apply Corollary 3.9 to φ. Then $S/\varphi(I)$ is in the standard form, so $\hat{f}$ is in the standard form by definition. □

Example 4.3. Let $f \in k[x_1, x_2, x_3, x_4]$ be a polynomial of degree s. Suppose that the leading form f_s of f can be written as $f_s = x_1^s + g_s$, where $g_s \in k[x_2, x_3, x_4]$. Then $\deg(\alpha_1\alpha_i \lrcorner f) \leq s - 3$ for all $i > 1$. Using Lemma 4.2, we produce $\hat{f} = x_1^s + h$ such that the apolar algebras of f and $\hat{f}$ are isomorphic and $\alpha_1^{s-2}\alpha_i \lrcorner h = 0$ for all $i \neq 1$. Then $\alpha_1^{s-2} \lrcorner h = \lambda_1 x_1 + \lambda_2$, where $\lambda_i \in k$ for $i = 1, 2$. After adding a suitable derivative to $\hat{f}$, we may assume $\lambda_1 = \lambda_2 = 0$, that is, $\alpha_1^{s-2} \lrcorner h = 0$.

Example 4.4. Suppose that a local Artin Gorenstein algebra A of socle degree s has Hilbert function equal to $(1, H_1, H_2, \dots, H_c, 1, \dots, 1)$. The standard form of

the dual socle generator of A is

$$f = x_1^s + \kappa_{s-1}x_1^{s-1} + \cdots + \kappa_{c+2}x_1^{c+2} + g,$$

where $\deg g \leq c+1$ and $\kappa_\bullet \in k$. By adding a suitable derivative we may, furthermore, make all $\kappa_i = 0$ and assume that $\alpha_1^{c+1} \lrcorner g = 0$. Using Lemma 4.2 we may also assume that $\alpha_1^c \alpha_j \lrcorner g = 0$ for every $j \neq 1$, so we may assume $\alpha_1^c \lrcorner g = 0$, arguing as in Example 4.3. This gives a dual socle generator

$$f = x_1^s + g,$$

where $\deg g \leq c+1$ and g does not contain monomials divisible by x_1^c.

The following proposition was proved in [Casnati and Notari 2014a] under the assumption that k is algebraically closed of characteristic zero and in [Jelisiejew 2014a, Theorem 5.1] under the assumption that $k = \mathbb{C}$. For completeness we include the proof (with no further assumptions on k other than the ones listed at the beginning of this section).

Proposition 4.5. *Let A be Artin local Gorenstein algebra of socle degree $s \geq 2$ such that the Hilbert function decomposition from Theorem 2.3 has $\Delta_{A,s-2} = (0, q, 0)$. Then A is isomorphic to the apolar algebra of a polynomial f such that f is in the standard form and the quadric part f_2 of f is a sum of q squares of variables not appearing in $f_{\geq 3}$ and a quadric in variables appearing in $f_{\geq 3}$.*

Proof. Let us take a standard dual socle generator $f \in P := k[x_1, \ldots, x_n]$ of the algebra A. Now we will twist f to obtain the required form of f_2. We may assume that $H_{\mathrm{Apolar}(f)}(1) = n$.

If $s = 2$, then the theorem follows from the fact that the quadric f may be diagonalized. Assume $s \geq 3$. Let $e := e(s-3) = \sum_{t=0}^{s-3} \Delta_{A,t}(1)$. We have $n = e(s-2) = f + q$, so that $f_{\geq 3} \in k[x_1, \ldots, x_e]$ and $f_2 \in k[x_1, \ldots, x_n]$. Note that $f_{\geq 3}$ is also in the standard form, so that every linear form in $x_1, \ldots, x_e$ is a derivative of $f_{\geq 3}$; see Remark 4.1.

First, we want to assure that $\alpha_n^2 \lrcorner f \neq 0$. If $\alpha_n \lrcorner f \in k[x_1, \ldots, x_e]$ then there exists an operator $\partial \in \mathfrak{m}_S^2$ such that $(\alpha_n - \partial) \lrcorner f = 0$. This contradicts the fact that f was in the standard form (see the discussion in Example 3.4). So we get that $\alpha_n \lrcorner f$ contains some x_r for $r > e$, i.e., f contains a monomial $x_r x_n$. A change of variables involving only x_r and x_n preserves the standard form and gives $\alpha_n^2 \lrcorner f \neq 0$.

Applying Lemma 4.2 to x_n, we see that f may be taken to be in the form $\hat{f} + x_n^2$, where $\hat{f}$ does not contain x_n, that is, $\hat{f} \in k[x_1, \ldots, x_{n-1}]$. We repeat the argument for $\hat{f}$. □

Example 4.6. If A is an algebra of socle degree 3, then $H_A = (1, n, e, 1)$ for some n and e. Moreover, $n \geq e$ and the symmetric decomposition of H_A is

$(1, e, e, 1) + (0, n-e, 0)$. By Proposition 4.5, we see that A is isomorphic to the apolar algebra of

$$f + \sum_{e<i\le n} x_i^2,$$

where $f \in k[x_1, \dots, x_e]$. This claim was first proved by Elias and Rossi [2012, Theorem 4.1].

4A. ***Irreducibility for fixed Hilbert function in two variables.*** Below we analyze local Artin Gorenstein algebras with Hilbert function $(1, 2, 2, \dots)$. Such algebras are (in some cases) classified up to isomorphism in [Elias and Valla 2011], but rather than such classification we need to know the geometry of their parameter space, which is analyzed (among other such spaces) in [Iarrobino 1977].

We need the following Proposition 4.7, which is part of folklore. We thank J. Buczyński for explaining the proof.

Let $r \ge 1$ be a natural number. By $\mathcal{H}ilb_r \operatorname{Spec} S$ we denote the Hilbert scheme of length r subschemes of the power series ring S. It is called the *punctual Hilbert scheme* because, as a set, $\mathcal{H}ilb_r \operatorname{Spec} S$ is equal to the set of length-r subschemes of $\mathbb{P}^n$ supported at a single fixed point.

We recall a classical construction. Let V be a constructible subset of $P_{\le s}$. Assume that the apolar algebra $\operatorname{Apolar}(f)$ has length r for every closed point $f \in V$. Then we may construct the incidence scheme $\{(f, \operatorname{Apolar}(f))\} \to V$, which is a finite flat family over V, and thus we obtain a morphism from V to $\mathcal{H}ilb_r \operatorname{Spec} S$. See [Jelisiejew 2014a, Proposition 4.39] for details.

Proposition 4.7. *Let $\mathcal{R} \subseteq \mathcal{H}ilb_r \operatorname{Spec} S$ be a constructible subset and $V \subseteq P$ denote the set of all possible dual socle generators of elements of $\mathcal{R}$. If $\mathcal{R}$ is irreducible, then also V is irreducible.*

Proof. Below, by k^* and S^* we denote the sets of invertible elements of k and S, respectively.

There is an induced surjective morphism φ from V to $\mathcal{R}$, as explained above. By construction, the fiber over $\varphi(f)$ is $S^* \lrcorner f$. The image $\mathcal{R}$ of φ is irreducible, so it is enough to show the existence of an open cover $\{H_i\}$ of $\mathcal{R}$ such that every $\varphi^{-1}(H_i)$ is irreducible.

Choose an element $f \in V$ and a section of $\mathfrak{m}_S/\operatorname{ann}_S(f)$ to $\mathfrak{m}_S$, that is, a linear subspace $\mathfrak{m}(f) \subseteq \mathfrak{m}_S$ such that $\mathfrak{m}(f) \to \mathfrak{m}_S/\operatorname{ann}_S(f)$ is bijective. Let $O(f) := \mathfrak{m}(f) + k \subseteq S$; then $S \lrcorner f = O(f) \lrcorner f$. Finally, let $O(f)^* := k^* + \mathfrak{m}(f)$, so that $\varphi^{-1}(\varphi(f)) = O(f)^* \lrcorner f$. Consider the set

$$U_f = \{g \in V \mid O(f) \cap \operatorname{ann}_S(g) = 0\} = \{g \in V \mid O(f) \lrcorner g = S \lrcorner g\}.$$

It is an open set in V and its image $H_f = \varphi(U_f)$ is open (hence irreducible) in the Hilbert scheme. Moreover, $U_f = \varphi^{-1}(H_f)$. For every $g \in U_f$ the fiber $\varphi^{-1}(\varphi(g))$ is equal to $O(f)^* \lrcorner g$.

By [Emsalem 1978, Proposition 18 and its Corollary] there is an open neighborhood $H'_f \subseteq H_f$ of $\varphi(f)$ such that the morphism $\varphi : \varphi^{-1}(H'_f) \to H'_f$ has a section i. Denoting $\varphi^{-1}(H'_f)$ by U'_f, we have a surjective morphism $O(f)^* \times H'_f \to U'_f$ mapping (σ, h) to $\sigma \lrcorner i(h)$. Since $O(f)^*$ and H'_f are irreducible, also U'_f is irreducible. Therefore, $\{H'_f\}$ forms a desired cover of $\mathcal{R}$ and so V is irreducible. □

Proposition 4.8. *Let $H = (1, 2, 2, *, \dots, *, 1)$ be a vector of length $s+1$. The set of polynomials $f \in k[x_1, x_2]$ such that $H_{\mathrm{Apolar}(f)} = H$ constitutes an irreducible subscheme of the affine space $k[x_1, x_2]_{\le s}$. A general member of this set has, up to an automorphism of P induced by an automorphism of S, the form $f + \partial \lrcorner f$, where $f = x_1^s + x_2^{s_2}$ for some $s_2 \le s$.*

Proof. Let $V \subseteq k[x_1, x_2]$ denote the set of those f such that $H_{\mathrm{Apolar}(f)} = H$. Then the image of V under the mapping sending f to $\mathrm{Apolar}(f)$ is irreducible by [Iarrobino 1977, Theorem 3.13]. By Proposition 4.7, the set V is irreducible.

In the case $H = (1, 1, 1, \dots, 1)$ the claim (with $s_2 = 0$) follows directly from the existence of the standard form of a polynomial. Further in the proof, we assume $H(1) = 2$.

Let us take a general polynomial f such that $H_{\mathrm{Apolar}(f)} = H$. Then $\mathrm{ann}_S(f) = (q_1, q_2)$ is a complete intersection, where $q_1 \in S$ has order 2, that is, $q_1 \in \mathfrak{m}_S^2 \setminus \mathfrak{m}_S^3$. Since f is general, we may assume that the quadric part of q_1 has maximal rank, i.e., rank two; see also [Iarrobino 1977, Theorem 3.14]. Then, after a change of variables, $q_1 \equiv \alpha_1\alpha_2 \bmod \mathfrak{m}_S^3$. Since the leading form $\alpha_1\alpha_2$ of q_1 is reducible, $q_1 = \delta_1\delta_2$ for some $\delta_1, \delta_2 \in S$ such that $\delta_i \equiv \alpha_i \bmod \mathfrak{m}_S^2$ for $i = 1, 2$, see, e.g., [Kunz 2005, Theorem 16.6]. After an automorphism of S we may assume $\delta_i = \alpha_i$; then $\alpha_1\alpha_2 = q_1$ annihilates f, so that it has the required form. □

4B. ***Homogeneous forms and secant varieties.*** It is well known that if $F \in P_s$ is a form such that $H_{\mathrm{Apolar}(F)} = (1, 2, \dots, 2, 1)$ then the standard form of F is either $x_1^s + x_2^s$ or $x_1^{s-1}x_2$. In particular, the set of such forms in P is irreducible and in fact it is open in the so-called secant variety. This section is devoted to some generalizations of this result for the purposes of classifying leading forms of polynomials in P.

The following proposition is well known if the base field is of characteristic zero (see [Bernardi et al. 2011, Theorem 4] or [Landsberg and Ottaviani 2013]), but we could not find a reference for the positive characteristic case, so for completeness we include the proof.

Proposition 4.9. *Suppose that $F \in k[x_1, x_2, x_3]$ is a homogeneous polynomial of degree $s \ge 4$. The following conditions are equivalent*:

(1) *The algebra* Apolar(F) *has Hilbert function* H *beginning with* $H(1) = H(2) = H(3) = 3$, *i.e.*, $H = (1, 3, 3, 3, \ldots)$.

(2) *After a linear change of variables,* F *is in one of the forms*

$$x_1^s + x_2^s + x_3^s, \quad x_1^{s-1}x_2 + x_3^s, \quad \text{or} \quad x_1^{s-2}(x_1x_3 + x_2^2).$$

Furthermore, the set of forms in $k[x_1, x_2, x_3]_s$ *satisfying the above conditions is irreducible.*

Proof. For the characteristic zero case, see [Landsberg and Ottaviani 2013] and references therein.

Let $S = k[\alpha_1, \alpha_2, \alpha_3]$ be a polynomial ring dual to P. This notation is incoherent with the global notation, but it is more readable than S_{poly}.

Let $I := \operatorname{ann}_S(F)$ and $I_2 := \langle \theta_1, \theta_2, \theta_3 \rangle \subseteq S_2$ be the linear space of operators of degree 2 annihilating F. Let $A := S/I$, $J := (I_2) \subseteq S$ and $B := S/J$. Since A has length greater than $3 \cdot 3 > 2^3$, the ideal J is not a complete intersection. Let us analyze the Hilbert function of A. By symmetry of H_A, we have $H_A(s-1) = H_A(1) = 3$. By Remark 2.7 we have $3 = H_A(3) \geq H_A(4) \geq \cdots \geq H_A(s-1) = 3$, thus

$$H_A(m) = 3 \quad \text{for all } m = 1, 2, \ldots, s-1.$$

We will prove that the graded ideal J is saturated and defines a zero-dimensional scheme of degree 3 in $\mathbb{P}^2 = \operatorname{Proj} S$. First, $3 = H_A(3) \leq H_B(3) \leq 4$ by Macaulay's growth theorem. If $H_B(3) = 4$ then, by Lemma 2.9 and Remark 2.10, we have $H_A(1) = 2$, a contradiction. We have proved that $H_B(3) = 3$.

Now we want to prove that $H_B(4) = 3$. By Macaulay's growth theorem applied to $H_B(3) = 3$ we have $H_B(4) \leq 3$. If $s > 4$ then $H_A(4) = 3$, so $H_B(4) \geq 3$. Suppose $s = 4$. By Buchsbaum–Eisenbud [1977] we know that the minimal number of generators of I is odd. Moreover, we know that $A_n = B_n$ for $n < 4$, thus the generators of I have degree two or four. Since I_2 is not a complete intersection, there are at least two generators of degree 4, so $H_B(4) \geq H_A(4) + 2 = 3$.

From $H_B(3) = H_B(4) = 3$, by Gotzmann's persistence theorem we see that $H_B(m) = 3$ for all $m \geq 1$. Thus the scheme $\Gamma := V(J) \subseteq \operatorname{Proj} k[\alpha_1, \alpha_2, \alpha_3]$ is finite of degree 3 and J is saturated. In particular, the ideal $J = I(\Gamma)$ is contained in I.

We will use Γ to compute the possible forms of F, in the spirit of the apolarity lemma; see [Iarrobino and Kanev 1999, Lemma 1.15]. There are four possibilities for Γ:

(1) Γ is a union of three distinct, noncollinear points. After a change of basis, $\Gamma = \{[1:0:0]\} \cup \{[0:1:0]\} \cup \{[0:0:1]\}$; then $I_2 = (\alpha_1\alpha_2, \alpha_2\alpha_3, \alpha_3\alpha_1)$ and $F = x_1^s + x_2^s + x_3^s$.

(2) Γ is a union of a point and scheme of length two such that $\langle \Gamma \rangle = \mathbb{P}^2$. After a change of basis, $I_\Gamma = (\alpha_1^2, \alpha_1\alpha_2, \alpha_2\alpha_3)$, so that $F = x_3^{s-1}x_1 + x_2^s$.

(3) Γ is irreducible with support $[1:0:0]$ and it is not a 2-fat point. Then Γ is Gorenstein and so Γ may be taken as the curvilinear scheme defined by $(\alpha_3^2, \alpha_2\alpha_3, \alpha_1\alpha_3 - \alpha_2^2)$. Then, after a linear change of variables, $F = x_1^{s-1}x_3 + x_2^2x_1^{s-2}$.

(4) Γ is a 2-fat point supported at $[1:0:0]$. Then $I_\Gamma = (\alpha_2^2, \alpha_2\alpha_3, \alpha_3^2)$, so $F = x_1^{s-1}(\lambda_2 x_2 + \lambda_3 x_3)$ for some $\lambda_2, \lambda_3 \in k$. But then there is a degree-one operator in S annihilating F, a contradiction.

The set of forms F which are sums of three powers of linear forms is irreducible. To see that the forms satisfying the assumptions of the proposition constitute an irreducible subset of P_s we observe that every Γ as above is smoothable by [Cartwright et al. 2009]. The flat family proving the smoothability of Γ induces a family $F_t \to F$, such that F_λ is a sum of three powers of linear forms for $\lambda \neq 0$, see [Emsalem 1978, Section C2, Corollaire]. See also [Buczyńska and Buczyński 2014] for a generalization of this method. □

Proposition 4.10. *Let $s \geq 4$. Consider the set $\mathcal{S}$ of all forms $F \in k[x_1, x_2, x_3, x_4]$ of degree s such that the apolar algebra of F has Hilbert function* $(1, 4, 4, 4, \ldots, 4, 1)$. *This set is irreducible and its general member has the form $\ell_1^s + \ell_2^s + \ell_3^s + \ell_4^s$, where ℓ_1, ℓ_2, ℓ_3 and ℓ_4 are linearly independent linear forms.*

Proof. First, the set $\mathcal{S}_0$ of forms equal to $\ell_1^4 + \ell_2^4 + \ell_3^4 + \ell_4^4$, where ℓ_1, ℓ_2, ℓ_3 and ℓ_4 are linearly independent linear forms, is irreducible and contained in $\mathcal{S}$. Thus, it is enough to prove that $\mathcal{S}$ lies in the closure of $\mathcal{S}_0$.

We follow the proof of Proposition 4.9, omitting some details which can be found there. Let $S = k[\alpha_1, \alpha_2, \alpha_3, \alpha_4]$, $I := \operatorname{ann}_S(F)$ and $J := (I_2)$. Set $A = S/I$ and $B = S/J$. Then $H_B(2) = 4$ and $H_B(3)$ is either 4 or 5. If $H_B(3) = 5$ then, by Lemma 2.9, we have $H_B(1) = 3$, a contradiction. Thus $H_B(3) = 4$.

Now we would like to prove $H_B(4) = 4$. By Macaulay's growth theorem, $H_B(4) \leq 5$. By Lemma 2.9, $H_B(4) \neq 5$, thus $H_B(4) \leq 4$. If $s > 4$, then $H_B(4) \geq H_A(4) \geq 4$, so we concentrate on the case $s = 4$. Let us write the minimal free resolution of A, which is symmetric by [Eisenbud 1995, Corollary 21.16]:

$$0 \to S(-8) \to S(-4)^{\oplus a} \oplus S(-6)^{\oplus 6} \to S(-3)^{\oplus b} \oplus S(-4)^{\oplus c} \oplus S(-5)^{\oplus b} \to S(-2)^{\oplus 6} \oplus S(-4)^{\oplus a} \to S.$$

Calculating $H_A(3) = 4$ from the resolution, we get $b = 8$. Calculating $H_A(4) = 1$, we obtain $6 - 2a + c = 0$. Since $1 + a = H_B(4) \leq 4$ we have $a \leq 3$, so $a = 3$, $c = 0$ and $H_B(4) = 4$.

Now we calculate $H_B(5)$. If $s > 5$ then $H_B(5) = 4$, as before. If $s = 4$ then, extracting syzygies of I_2 from the above resolution, we see that $H_B(5) = 4 + \gamma$,

where $0 \le \gamma \le 8$; thus $H_B(5) = 4$ and $\gamma = 0$. If $s = 5$, then the resolution of A is

$$0 \to S(-9) \to S(-4)^{\oplus 3} \oplus S(-7)^{\oplus 6} \to S(-3)^{\oplus 8} \oplus S(-6)^{\oplus 8} \\ \to S(-5)^{\oplus 3} \oplus S(-2)^{\oplus 6} \to S.$$

So $H_B(5) = 56 - 20 \cdot 6 + 8 = 4$. Thus, as in the previous case, we see that J is the saturated ideal of a scheme Γ of degree 4. Then Γ is smoothable, by [Cartwright et al. 2009], and its smoothing induces a family $F_t \to F$, where $F_\lambda \in \mathcal{S}_0$ for $\lambda \neq 0$. □

The following corollary is a consequence of Proposition 4.10. This corollary is not used in the proofs of the main results, but it is of certain interest of its own and shows another connection with secant varieties. For simplicity and to refer to some results from [Landsberg and Ottaviani 2013], we assume that $k = \mathbb{C}$, but the claim holds for all fields of characteristic either zero or large enough.

To state the claim we introduce catalecticant matrices. Let $\varphi_{a,s-a} : S_a \times P_s \to P_{s-a}$ be the contraction mapping applied to homogeneous polynomials of degree s. For $F \in P_s$ we obtain $\varphi_{a,s-a}(F) : S_a \to P_{s-a}$, whose matrix is called the *a-catalecticant matrix*. It is straightforward to see that $\operatorname{rk} \varphi_{a,s-a}(F) = H_{\operatorname{Apolar}(F)}(a)$.

Corollary 4.11. *Let $s \ge 4$ and $k = \mathbb{C}$. The fourth secant variety to s-th Veronese reembedding of $\mathbb{P}^n$ is a subset $\sigma_4(v_s(\mathbb{P}^n)) \subseteq \mathbb{P}(P_s)$ set-theoretically defined by the condition* $\operatorname{rk} \varphi_{a,s-a} \le 4$, *where $a = \lfloor s/2 \rfloor$.*

Proof. Since $H_{\operatorname{Apolar}(F)}(a) \le 4$ for F which is a sum of four powers of linear forms, by semicontinuity every $F \in \sigma_4(v_s(\mathbb{P}^n))$ satisfies the above condition.

Let $F \in P_s$ be a form satisfying $\operatorname{rk} \varphi_{a,s-a}(F) \le 4$. Let $A = \operatorname{Apolar}(F)$ and $H = H_A$ be the Hilbert function of A. We want to reduce to the case where $H(n) = 4$ for all $0 < n < s$.

First we show that $H(n) \ge 4$ for all $0 < n < s$. If $H(1) \le 3$, then the claim follows from [Landsberg and Ottaviani 2013, Theorem 3.2.1(2)], so we assume $H(1) \ge 4$. Suppose that for some n satisfying $4 \le n < s$ we have $H(n) < 4$. Then, by Remark 2.7, we have $H(m) \le H(n)$ for all $m \ge n$, so that $H(1) = H(s-1) < 4$, a contradiction. Thus $H(n) \ge 4$ for all $n \ge 4$. Moreover, $H(3) \ge 4$ by Macaulay's growth theorem. Suppose now that $H(2) < 4$. By Theorem 2.6 the only possible case is $H(2) = 3$ and $H(3) = 4$. But then $H(1) = 2 < 4$ by Lemma 2.9, a contradiction. Thus we have proved that

$$H(n) \ge 4 \quad \text{for all } 0 < n < s. \tag{1}$$

We have $H(a) = 4$. If $s \ge 8$, then $a \ge 4$, so by Remark 2.7 we have $H(n) \le 4$ for all $n > a$. Then, by the symmetry $H(n) = H(s-n)$, we have $H(n) \le 4$ for all n. Together with $H(n) \ge 4$ for $0 < n < s$, we have $H(n) = 4$ for $0 < n < s$. Then $F \in \sigma_4(v_s(\mathbb{P}^n))$ by Proposition 4.10. If $a = 3$ (i.e., $s = 6$ or $s = 7$), then $H(4) \le 4$ by Lemma 2.9 and we finish the proof as in the case $s \ge 8$. If $s = 5$, then $a = 2$ and

the Hilbert function of A is $(1, n, 4, 4, n, 1)$. Again by Lemma 2.9, we have $n \leq 4$, thus $n = 4$ by (1) and Proposition 4.10 applies. If $s = 4$, then $H = (1, n, 4, n, 1)$. Suppose $n \geq 5$; then Lemma 2.9 gives $n \leq 3$, a contradiction. Thus $n = 4$ and Proposition 4.10 applies also to this case. □

Note that, for $s \geq 8$, Corollary 4.11 was also proved, in the case $k = \mathbb{C}$, in [Buczyńska and Buczyński 2014, Theorem 1.1].

5. Ray sums, ray families and their flatness

Recall that k is an algebraically closed field of characteristic neither 2 nor 3. Since $k[\![\alpha_i]\!]$ is a discrete valuation ring, all its ideals have the form $\alpha_i^\nu k[\![\alpha_i]\!]$ for some $\nu \geq 0$. We use this property to construct certain decompositions of the ideals in the power series ring $S = k[\![\alpha_1, \ldots, \alpha_n]\!]$.

Definition 5.1. Let I be an ideal of finite colength in the power series ring S and $\pi_i : k[\![\alpha_1, \ldots, \alpha_n]\!] \twoheadrightarrow k[\![\alpha_i]\!]$ be the projection defined by $\pi_i(\alpha_j) = 0$ for $j \neq i$ and $\pi_i(\alpha_i) = \alpha_i$.

The i-th *ray order* of I is a nonnegative integer $\nu = \operatorname{rord}_i(I)$ such that $\pi_i(I) = (\alpha_i^\nu)$.

By the discussion above, the ray order is well defined. Below, by $\mathfrak{p}_i$ we denote the kernel of π_i; this is the ideal generated by all variables except for α_i.

Definition 5.2. Let I be an ideal of finite colength in the power series ring S. A *ray decomposition* of I with respect to α_i consists of an ideal $J \subseteq S$ such that $J \subseteq I \cap \mathfrak{p}_i$ together with an element $q \in \mathfrak{p}_i$ and $\nu \in \mathbb{Z}_+$ such that

$$I = J + (\alpha_i^\nu - q)S.$$

Note that from Definition 5.1 it follows that, for every I and i, a ray decomposition (with $J = I \cap \mathfrak{p}_i$) exists and that $\nu = \operatorname{rord}_i(I)$ for every ray decomposition.

Definition 5.3. Let $S_{\mathrm{poly}} = k[\alpha_1, \ldots, \alpha_n] \subseteq S$. Let $I = J + (\alpha_i^\nu - q)S$ be a ray decomposition of a finite colength ideal $I \subseteq S$. Let $J_{\mathrm{poly}} = J \cap S_{\mathrm{poly}}$. The associated *lower ray family* is

$$k[t] \to \frac{S_{\mathrm{poly}}[t]}{J_{\mathrm{poly}}[t] + (\alpha_i^\nu - t \cdot \alpha_i - q)S_{\mathrm{poly}}[t]},$$

and the associated *upper ray family* is

$$k[t] \to \frac{S_{\mathrm{poly}}[t]}{J_{\mathrm{poly}}[t] + (\alpha_i^\nu - t \cdot \alpha_i^{\nu-1} - q)S_{\mathrm{poly}}[t]}.$$

If the lower (upper) family is flat over $k[t]$ we will call it a *lower (upper) ray degeneration*.

Note that the lower and upper ray degenerations agree for $\nu = 2$.

Remark 5.4. In all considered cases the quotient $S_{\mathrm{poly}}/J_{\mathrm{poly}}$ will be finite over k, so that every ray family will be finite over $k[t]$. Then every ray degeneration will give a morphism to the Hilbert scheme. We leave this to the reader.

Remark 5.5. In this remark for simplicity we assume that $i = 1$ in Definition 5.3. Below we write α instead of α_1. Let us look at the fibers of the upper ray family from this definition in a special case, when $\alpha \cdot q \in J$. The fiber over $t = 0$ is isomorphic to S/I. Let us take $\lambda \neq 0$ and analyze the fiber at $t = \lambda$. This fiber is supported at $(0, 0, \ldots, 0)$ and at $(0, \ldots, 0, \lambda, 0, \ldots, 0)$, where λ appears in the i-th position. In particular, this shows that the existence of an upper ray degeneration proves that the algebra S/I is limit-reducible; this is true also for the lower ray degeneration.

Now, $\alpha^{\nu+1} - \lambda\alpha^{\nu}$ is in the ideal defining the fiber of the upper ray family over $t = \lambda$. One may compute that, near $(0, \ldots, 0)$, the ideal defining the fiber is $(\lambda\alpha^{\nu-1} - q) + J$. Similarly, near $(0, \ldots, 0, \lambda, 0, \ldots, 0)$ it is $(\alpha - \lambda) + (q) + J$. The argument is similar to (though easier than) the proof of Proposition 5.10.

Most of the families constructed in [Cartwright et al. 2009; Casnati and Notari 2009] are ray degenerations.

Definition 5.6. For a nonzero polynomial $f \in P$ and $d \geq 2$, the d-th *ray sum of f with respect to a derivation* $\partial \in \mathfrak{m}_S$ is a polynomial $g \in P[x]$ given by

$$g = f + x^d \cdot \partial \lrcorner f + x^{2d} \cdot \partial^2 \lrcorner f + x^{3d} \cdot \partial^3 \lrcorner f + \cdots.$$

The following proposition shows that a ray sum naturally induces a ray decomposition, which can be computed explicitly.

Proposition 5.7. *Let g be the d-th ray sum of f with respect to $\partial \in \mathfrak{m}_S$ such that $\partial \lrcorner f \neq 0$. Let α be an element dual to x, so that $P[x]$ and $T := S[\![\alpha]\!]$ are dual. The annihilator of g in T is given by the formula*

$$\operatorname{ann}_T(g) = \operatorname{ann}_S(f) + \left(\sum_{i=1}^{d-1} k\alpha^i \right) \operatorname{ann}_S(\partial \lrcorner f) + (\alpha^d - \partial)T, \tag{2}$$

where the sum is of k-vector spaces. In particular, the ideal $\operatorname{ann}_T(g) \subseteq T$ *is generated by* $\operatorname{ann}_S(f)$, $\alpha \operatorname{ann}_S(\partial \lrcorner f)$ *and* $\alpha^d - \partial$. *The formula* (2) *is a ray decomposition of* $\operatorname{ann}_T(g)$ *with respect to α and with $J = \operatorname{ann}_S(f)T + \alpha \operatorname{ann}_S(\partial \lrcorner f)T$ and $q = \partial$.*

Proof. It is straightforward to see that the right-hand side of (2) lies in $\operatorname{ann}_T(g)$. Let us take any $\partial' \in \operatorname{ann}_T(g)$. Reducing the powers of α using $\alpha^d - \partial$, we can write

$$\partial' = \sigma_0 + \sigma_1\alpha + \cdots + \sigma_{k-1}\alpha^{d-1},$$

where the $\sigma_\bullet$ do not contain α. The action of this derivation on g gives

$$0 = \sigma_0 \lrcorner f + x\sigma_{d-1}\partial \lrcorner f + x^2\sigma_{d-2}\partial \lrcorner f + \cdots + x^{d-1}\sigma_1\partial \lrcorner f + x^d(\cdots).$$

We see that $\sigma_0 \in \operatorname{ann}_S(f)$ and $\sigma_i \in \operatorname{ann}_S(\partial \lrcorner f)$ for $i \geq 1$, so the equality is proved. It is also clear that $J \subseteq \mathfrak{m}_S T$ and $\operatorname{ann}_T(g) = J + (\alpha^d - \partial)T$, so that indeed we obtain a ray decomposition. □

Remark 5.8. It is not hard to compute the Hilbert function of the apolar algebra of a ray sum in some special cases. We mention one such case below. Let $f \in P$ be a polynomial satisfying $f_2 = f_1 = f_0 = 0$ and $\partial \in \mathfrak{m}_S^2$ be such that $\partial \lrcorner f = \ell$ is a linear form, so that $\partial^2 \lrcorner f = 0$. Let $A = \operatorname{Apolar}(f)$ and $B = \operatorname{Apolar}(f + x^2\ell)$. The only different values of H_A and H_B are $H_B(m) = H_A(m) + 1$ for $m = 1, 2$. The assumption $f_2 = f_1 = f_0 = 0$ is needed to ensure that the degrees of $\partial \lrcorner f$ and $\partial \lrcorner (f + x^2\ell)$ are equal for all ∂ not annihilating f.

5A. *Flatness of ray families.*

Proposition 5.9. *Let g be the d-th ray sum with respect to f and ∂. Then the corresponding upper and lower ray families are flat. Recall that these families are explicitly given as*

$$k[t] \to \frac{T_{\text{poly}}[t]}{J_{\text{poly}}[t] + (\alpha^d - t\alpha^{d-1} - \partial)T_{\text{poly}}[t]} \quad (\textit{upper ray family}), \tag{3}$$

$$k[t] \to \frac{T_{\text{poly}}[t]}{J_{\text{poly}}[t] + (\alpha^d - t\alpha - \partial)T_{\text{poly}}[t]} \quad (\textit{lower ray family}), \tag{4}$$

where T_{poly} is the fixed polynomial subring of T.

Proof. We start by proving the flatness of family (4).

We want to use Proposition 2.12. To simplify notation let $J := J_{\text{poly}}$. Denote by $\mathfrak{I}$ the ideal defining the family and suppose that some $z \in \mathfrak{I}$ lies in $(t - \lambda)$ for some $\lambda \in k$. Write z as $i + i_2(\alpha^d - t\alpha - \partial)$, where $i \in J[t]$, $i_2 \in T_{\text{poly}}[t]$, and note that by Remark 2.13 we may assume $i \in J$ and $i_2 \in T_{\text{poly}}$. Since $z \in (t - \lambda)$, we have that $i + i_2(\alpha_1^\nu - t\alpha_1^{\nu-1} - q) = 0$, so

$$i_2(\alpha^d - \lambda\alpha - \partial) = -i \in J.$$

By Proposition 5.7 the ideal J is homogeneous with respect to grading by α. More precisely it is equal to $J_0 + J_1\alpha$, where $J_0 = \operatorname{ann}_S(f)T$ and $J_1 = \operatorname{ann}_S(\partial \lrcorner f)T$ are generated by elements not containing α, so that J is generated by elements of α-degree at most one. We now check the assumptions of Lemma 2.15. Note that $\partial J \subseteq J_0$ by definition of J. If $r \in T_{\text{poly}}$ is such that $r\alpha^d \in J$, then $r \in J_1$, so that $r(\lambda\alpha + \partial) \in \alpha J_1 + J_0 \subseteq J$. Therefore, the assumptions are satisfied and the lemma shows that $i_2\alpha^d \in J$. Then $i_2\alpha \in J$; thus $i_2(\alpha^d - t\alpha) \in J[t] \subseteq (\mathfrak{I} \cap T_{\text{poly}})[t]$. Since $i_2\partial \in \mathfrak{I} \cap T_{\text{poly}}$ by definition, this implies that $i + i_2(\alpha^d - t\alpha - \partial) \in J[t] \subseteq (\mathfrak{I} \cap T_{\text{poly}})[t]$. Now the flatness follows from Proposition 2.12.

The same proof works equally well for the upper ray family: one should just replace α by α^{d-1} in appropriate places of the proof. For this reason, we leave the case of family (3) to the reader. □

Proposition 5.10. *Let us keep the notation of Proposition 5.9. Let $\lambda \in k \setminus \{0\}$. The fibers of family* (3) *and family* (4) *over $t - \lambda$ are reducible.*

Suppose that $\partial^2 \lrcorner f = 0$ and the characteristic of k does not divide $d - 1$. The fiber of the family (4) *over $t - \lambda$ is isomorphic to*

$$\operatorname{Spec} \operatorname{Apolar}(f) \sqcup (\operatorname{Spec} \operatorname{Apolar}(\partial f))^{\sqcup d-1}.$$

Proof. For both families the support of the fiber over $t - \lambda$ contains the origin. The support of the fiber of family (3) contains, furthermore, a point with $\alpha = \lambda$ and other coordinates equal to zero. The support of the fiber of family (4) contains a point with $\alpha = \omega$, where $\omega^{d-1} = \lambda$.

Now let us concentrate on family (4) and on the case $\partial^2 \lrcorner f = 0$. The support of the fiber over $t - \lambda$ is $(0, \dots, 0, 0)$ and $(0, \dots, 0, \omega)$, where $\omega^{d-1} = \lambda$ are $(d-1)$-st roots of λ, which are pairwise different because of the characteristic assumption. We will analyze the support point by point. By hypothesis, $\partial \in \operatorname{ann}_S(\partial \lrcorner f)$, so that $\alpha \cdot \partial \in J$; thus $\alpha^{d+1} - \lambda \cdot \alpha^2$ is in the ideal I of the fiber over $t = \lambda$.

Near $(0, 0, \dots, 0)$ the element $\alpha^{d-1} - \lambda$ is invertible, so α^2 is in the localization of the ideal I, thus $\alpha + \lambda^{-1}\partial$ is in the ideal. Now we check that the localization of I is equal to $\operatorname{ann}_S(f) + (\alpha + \lambda^{-1}\partial)T_{\text{poly}}$. Explicitly, one should check that

$$(\operatorname{ann}_S(f) + (\alpha + \lambda^{-1}\partial)T_{\text{poly}})_{(0,\dots,0)} = (\operatorname{ann}_S(f) + (\alpha^d - \lambda\alpha - \partial)T_{\text{poly}})_{(0,\dots,0)}.$$

Then the stalk of the fiber at $(0, \dots, 0)$ is isomorphic to $\operatorname{Spec} \operatorname{Apolar}(f)$.

Near $(0, 0, \dots, 0, \omega)$, the elements α and $(\alpha^{k+1} - \lambda \cdot \alpha^2)/(\alpha - \omega)$ are invertible, so $\operatorname{ann}_S(\partial \lrcorner f)$ and $\alpha - \omega$ are in the localization of I. This, along with the other inclusion, proves that this localization is generated by $\operatorname{ann}_S(\partial \lrcorner f)$ and $\alpha - \omega$ and thus the stalk of the fiber is isomorphic to $\operatorname{Spec} \operatorname{Apolar}(\partial f)$. □

We make the most important corollary explicit:

Corollary 5.11. *We keep the notation of Proposition 5.9. Suppose that* $\operatorname{char} k$ *does not divide $d - 1$ and $\partial^2 \lrcorner f = 0$. If both apolar algebras of f and $\partial \lrcorner f$ are smoothable then also the apolar algebra of every ray sum of f with respect to ∂ is smoothable.* □

Example 5.12. Let $f \in k[x_1, \dots, x_n]$ be a dual socle generator of an algebra A. Then the algebra $B = \operatorname{Apolar}(f + x_{n+1}^2)$ is limit-reducible: it is a limit of algebras of the form $A \times k$. In particular, if A is smoothable, then B is also smoothable.

Combining this with Proposition 4.5, we see that every local Gorenstein algebra A of socle degree s with $\Delta_{A,s-2} = (0, q, 0)$, where $q \neq 0$, is limit-reducible.

If $\deg f \geq 2$ then the Hilbert functions of the algebras $A = \mathrm{Apolar}(f)$ and $B = \mathrm{Apolar}(f + x_{n+1}^2)$ are related by $H_B(m) = H_A(m)$ for $m \neq 1$ and $H_B(1) = H_A(1) + 1$.

Above, we took advantage of the explicit form of ray decompositions coming from ray sums to analyze the resulting ray families in depth. In Proposition 5.13 below we prove the flatness of the upper ray family without such knowledge. The price paid for this is the fact that we get no information about the fibers of this family.

Proposition 5.13. *Let $f = x_1^s + g \in P$ be a polynomial of degree s such that $\alpha_1^c \lrcorner g = 0$ for some c satisfying $2c \leq s$. Then any ray decomposition $\mathrm{ann}_S(f) = (\alpha_1^\nu - q) + J$, where $J = \mathrm{ann}_S(f) \cap (\alpha_2, \ldots, \alpha_n)$, gives rise to an upper ray degeneration. In particular, $\mathrm{Apolar}(f)$ is limit-reducible.*

Proof. Let $\mathfrak{I} := (\alpha_1^\nu - t\alpha_1^{\nu-1} - q) + J$ be the ideal defining the ray family and recall that q, $J \subseteq \mathfrak{p}_1$, where $\mathfrak{p}_1 = (\alpha_2, \ldots, \alpha_n)$.

Since $\alpha_1^\nu - q \in \mathrm{ann}_S(f)$, we have $q \lrcorner g = q \lrcorner f = \alpha_1^\nu \lrcorner f = x_1^{s-\nu} + \alpha_1^\nu \lrcorner g$. Then $\alpha_1^{s-\nu}(q \lrcorner g) = \alpha_1^{s-\nu} \lrcorner x_1^{s-\nu} + \alpha_1^s \lrcorner g = 1$; thus $\alpha_1^{s-\nu} \lrcorner g \neq 0$. It follows that $s - \nu \leq c - 1$, so $\nu - 1 \geq s - c \geq c$; thus $\alpha_1^{\nu-1} \lrcorner g = 0$. For all $\gamma \in \mathfrak{p}_1$, we claim that

$$\gamma \cdot (\alpha_1^\nu - t\alpha_1^{\nu-1} - q) \in J[t]. \tag{5}$$

Note that $(\alpha_1^\nu - q) \lrcorner f = 0$ and $\alpha_1^{\nu-1}\gamma \lrcorner f = \alpha_1^{\nu-1}\gamma \lrcorner g = 0$. This means that $\alpha_1^{\nu-1}\gamma \in J$. Since $(\alpha_1^\nu - q)\gamma \in J$ always, we have proved (5).

Let $\mathfrak{I} \subseteq S_{\mathrm{poly}}[t]$ be the ideal defining the upper ray family. Take any $\lambda \in k$ and an element $i \in \mathfrak{I} \cap (t - \lambda)$. We will prove that $i \in \mathfrak{I}(t - \lambda) + \mathfrak{I}_0[t]$, where $\mathfrak{I}_0 = \mathfrak{I} \cap S$, then Proposition 2.12 asserts that $S[t]/\mathfrak{I}$ is flat. Write $i = i_1 + i_2(\alpha_1^\nu - t\alpha_1^{\nu-1} - q)$. As before, we may assume $i_1 \in J$ and $i_2 \in S$. Since $i \in (t - \lambda)$, we have $i_1 + i_2(\alpha_1^\nu - \lambda\alpha_1^{\nu-1} - q) = 0$. Since $i_1 \in \mathfrak{p}_1$, we also have $i_2 \in \mathfrak{p}_1$. But then by inclusion (5) we have $i_2(\alpha_1^\nu - t\alpha_1^{\nu-1} - q) \subseteq \mathfrak{I}_0[t]$. Since clearly $i_1 \in J \subseteq \mathfrak{I}_0[t]$, the assumptions of Proposition 2.12 are satisfied; thus the upper ray family is flat.

Now, Remark 5.5 shows that a general fiber of the upper ray degeneration is reducible; thus, $\mathrm{Apolar}(f)$ is a flat limit of reducible algebras, so limit-reducible. □

Example 5.14. Let $f \in k[x_1, x_2, x_3, x_4]$ be a polynomial of degree 4. Suppose that the leading form f_4 of f can be written as $f_4 = x_1^4 + g_4$, where $g_4 \in k[x_2, x_3, x_4]$. We will prove that $\mathrm{Apolar}(f)$ is limit-reducible. By Example 4.3 we may assume that $f = x_1^4 + g$, where $\alpha_1^2 \lrcorner g = 0$. By Proposition 5.13 we see that $\mathrm{Apolar}(f)$ is limit-reducible.

Example 5.15. Suppose that an Artin local Gorenstein algebra A has Hilbert function $H_A = (1, H_1, \ldots, H_c, 1, \ldots, 1)$ and socle degree $s \geq 2c$. By Example 4.4 we may assume that $A \simeq \mathrm{Apolar}(x_1^s + g)$, where $\alpha_1^c \lrcorner g = 0$ and $\deg g \leq c + 1$. Then

by Proposition 5.13 we obtain a flat degeneration

$$k[t] \to \frac{S[t]}{(\alpha_1^\nu - t\alpha_1^{\nu-1} - q) + J}. \tag{6}$$

Thus A is limit-reducible in the sense of Definition 2.5. Let us take $\lambda \neq 0$. By Remark 5.5 the fiber over $t = \lambda$ is supported at $(0, 0, \dots, 0)$ and at $(\lambda, 0, \dots, 0)$ and the ideal defining this fiber near $(0, 0, \dots, 0)$ is $I_0 = (\lambda\alpha_1^{\nu-1} - q) + J$. From the proof of 5.13 it follows that $\alpha_1^{\nu-1} \lrcorner g = 0$. Then one can check that I_0 lies in the annihilator of $\lambda^{-1}x_1^{s-1} + g$. Since $\sigma \lrcorner (x_1^s + g) = \sigma \lrcorner (\lambda^{-1}x_1^{s-1} + g)$ for every σ in $(\alpha_2, \dots, \alpha_n)$, one calculates that the apolar algebra of $\lambda^{-1}x_1^{s-1} + g$ has Hilbert function $(1, H_1, \dots, H_c, 1, \dots, 1)$ and socle degree $s-1$. Then $\dim_k \operatorname{Apolar}(x_1^{s-1}+g) = \dim_k \operatorname{Apolar}(\lambda^{-1}x_1^s + g) - 1$. Therefore, the fiber is a union of a point and of $\operatorname{Spec} \operatorname{Apolar}(\lambda^{-1}x_1^s + g)$, i.e., the degeneration (6) peels one point off A.

5B. ***Tangent-preserving ray degenerations.*** A (finite) ray degeneration gives a morphism from $\operatorname{Spec} k[t]$ to the Hilbert scheme, that is, a curve on the Hilbert scheme $\mathcal{H}ilb(\mathbb{P}^n)$. In this section we prove that in some cases the dimension of the tangent space to $\mathcal{H}ilb(\mathbb{P}^n)$ is constant along this curve. This enables us to prove that certain points of this scheme are smooth without the need for lengthy computations.

This section seems to be the most technical part of the paper, so we include even more examples. The most important results here are Theorem 5.18 together with Corollary 5.20; see examples below Corollary 5.20 for applications.

Recall (e.g., [Jelisiejew 2014a, Proposition 4.10] or [Casnati and Notari 2009]) that the dimension of the tangent space to $\mathcal{H}ilb(\mathbb{P}^n)$ at a k-point corresponding to a Gorenstein scheme $\operatorname{Spec} S/I$ is $\dim_k S/I^2 - \dim_k S/I$.

Lemma 5.16. *Let $d \geq 2$. Let g be the d-th ray sum of $f \in P$ with respect to $\partial \in S$ such that $\partial^2 \lrcorner f = 0$. Denote $I := \operatorname{ann}_S(f)$ and $J := \operatorname{ann}_S(\partial \lrcorner f)$. Take $T = S[\![\alpha]\!]$ to be the ring dual to $P[x]$ and let*

$$\mathfrak{I} := (I + J\alpha + (\alpha^d - t\alpha - \partial)) \cdot T[t]$$

be the ideal in $T[t]$ defining the associated lower ray degeneration; see Proposition 5.9. Then the family $k[t] \to T[t]/\mathfrak{I}^2$ is flat if and only if $(I^2 : \partial) \cap I \cap J^2 \subseteq I \cdot J$.

Proof. To prove flatness we will use Proposition 2.12. Take an element $i \in \mathfrak{I}^2 \cap (t-\lambda)$. We want to prove that $i \in \mathfrak{I}^2(t-\lambda) + \mathfrak{I}_0[t]$, where $\mathfrak{I}_0[t] = \mathfrak{I}^2 \cap T$. Let $\mathcal{J} := (I + J\alpha)T$. Subtracting a suitable element of $\mathfrak{I}^2(t - \lambda)$, we may assume that

$$i = i_1 + i_2(\alpha^d - t\alpha - \partial) + i_3(\alpha^d - t\alpha - \partial)^2,$$

where $i_1 \in \mathcal{J}^2$, $i_2 \in \mathcal{J}$ and $i_3 \in T$. We will in fact show that $i \in \mathfrak{I}^2(t - \lambda) + \mathcal{J}^2[t]$.

To simplify notation, denote $\sigma = \alpha^d - \lambda\alpha - \partial$. Note that $J\sigma \subseteq \mathcal{J}$. We have $i_1 + i_2\sigma + i_3\sigma^2 = 0$. Let $j_3 := i_3\sigma$. We want to apply Lemma 2.15; below, we check its assumptions. The ideal $\mathcal{J}$ is homogeneous with respect to α, generated in degrees less than d. Let $s \in T$ be an element satisfying $s\alpha^d \in \mathcal{J}$. Then $s \in J$, which implies $s(\lambda\alpha + \partial) \in \mathcal{J}$. By Lemma 2.15 and $i_3\sigma^2 = j_3\sigma \in \mathcal{J}$ we obtain $j_3\alpha^d \in \mathcal{J}$, so $i_3\sigma\alpha^d \in \mathcal{J}$. Applying the same argument to $i_3\alpha^d$ we obtain $i_3\alpha^{2d} \in \mathcal{J}$, therefore $i_3 \in JT$. Then

$$\begin{aligned} i_3(\alpha^d - t\alpha - \partial)^2 - i_3\sigma(\alpha^d - t\alpha - \partial) &= i_3\alpha(t-\lambda)(\alpha^d - t\alpha - \partial) \\ &\in \mathcal{J}(t-\lambda)(\alpha^d - t\alpha - \partial) \subseteq \mathfrak{I}^2(t-\lambda). \end{aligned}$$

Subtracting this element from i and substituting $i_2 := i_2 + i_3\sigma$, we may assume $i_3 = 0$. We obtain

$$0 = i_1 + i_2\sigma = i_1 + i_2(\alpha^d - \lambda\alpha - \partial). \tag{7}$$

Let $i_2 = j_2 + v_2\alpha$, where $j_2 \in S$, i.e., it does not contain α. Since $i_2 \in \mathcal{J}$, we have $j_2 \in I$. As before, we have $v_2\alpha((\alpha^d - t\alpha - \partial) - \sigma) = v_2\alpha^2(t-\lambda) \in \mathfrak{I}^2(t-\lambda)$, so that we may assume $v_2 = 0$.

Comparing the top α-degree terms of (7), we see that $j_2 \in J^2$. Comparing the terms of (7) not containing α, we deduce that $j_2\partial \in I^2$; thus $j_2 \in (I^2 : \partial)$. Jointly, $j_2 \in I \cap J^2 \cap (I^2 : \partial)$; thus $j_2 \in IJ$ by assumption. But then $j_2\alpha \in \mathcal{J}^2$, so $j_2(\alpha^d - t\alpha - \partial) \in \mathcal{J}^2[t]$ and, since $i_1 \in \mathcal{J}^2$, the element i lies in $\mathcal{J}^2[t] \subseteq \mathfrak{I}_0[t]$. Thus the assumptions of Proposition 2.12 are satisfied and the family $T[t]/\mathfrak{I}^2$ is flat over $k[t]$.

The converse is easier: one takes $i_2 \in I \cap J^2 \cap (I^2 : \partial)$ such that $i_2 \notin IJ$. On one hand, the element $j := i_2(\alpha^d - \partial)$ lies in $\mathcal{J}^2$ and we get that $i_2(\alpha^d - t\alpha - \partial) - j = ti_2\alpha \in \mathfrak{I}^2$. On the other hand, if $i_2\alpha \in \mathfrak{I}^2$, then $i_2\alpha \in (\mathfrak{I}^2 + (t)) \cap T = (\mathcal{J} + (\alpha^d - \partial))^2$, which is not the case. □

Remark 5.17. Let us keep the notation of Lemma 5.16. Fix $\lambda \in k \setminus \{0\}$ and suppose that the characteristic of k does not divide $d-1$. The supports of the fibers of $S[t]/\mathfrak{I}$, $\mathfrak{I}/\mathfrak{I}^2$ and $S[t]/\mathfrak{I}^2$ over $t = \lambda$ are finite and equal. In particular, from Proposition 5.10 it follows that the dimension of the fiber of $\mathfrak{I}/\mathfrak{I}^2$ over $t - \lambda$ is equal to $\tan(f) + (d-1)\tan(\partial \lrcorner f)$, where $\tan(h) = \dim_k \operatorname{ann}_S(h)/\operatorname{ann}_S(h)^2$ is the dimension of the tangent space to the point of the Hilbert scheme corresponding to $\operatorname{Spec} S/\operatorname{ann}_S(h)$.

Theorem 5.18. *Suppose that a polynomial $f \in P$ corresponds to a smoothable, unobstructed algebra* $\operatorname{Apolar}(f)$. *Let $\partial \in S$ be such that $\partial^2 \lrcorner f = 0$ and the algebra* $\operatorname{Apolar}(\partial \lrcorner f)$ *is smoothable and unobstructed. The following are equivalent*:

(1) *The d-th ray sum of f with respect to ∂ is unobstructed for some d such that* $2 \le d \le \operatorname{char} k$ (*or* $2 \le d$ *if* $\operatorname{char} k = 0$).

(1a) *The d-th ray sum of f with respect to ∂ is unobstructed for all d such that* $2 \le d \le \operatorname{char} k$ (*or* $2 \le d$ *if* $\operatorname{char} k = 0$).

(2) *The $k[t]$-module $\mathfrak{I}/\mathfrak{I}^2$ is flat, where $\mathfrak{I}$ is the ideal defining the lower ray family of the d-th ray sum for some* $2 \le d \le \operatorname{char} k$ (*or* $2 \le d$ *if* $\operatorname{char} k = 0$); *see Definition 5.3.*

(2a) *The $k[t]$-module $\mathfrak{I}/\mathfrak{I}^2$ is flat, where $\mathfrak{I}$ is the ideal defining the lower ray family of the d-th ray sum for every* $2 \le d \le \operatorname{char} k$ (*or* $2 \le d$ *if* $\operatorname{char} k = 0$); *see Definition 5.3.*

(3) *The family $k[t] \to S[t]/\mathfrak{I}^2$ is flat, where $\mathfrak{I}$ is the ideal defining the lower ray family of the d-th ray sum for some* $2 \le d \le \operatorname{char} k$ (*or* $2 \le d$ *if* $\operatorname{char} k = 0$).

(3a) *The family $k[t] \to S[t]/\mathfrak{I}^2$ is flat, where $\mathfrak{I}$ is the ideal defining the lower ray family of the d-th ray sum for every* $2 \le d \le \operatorname{char} k$ (*or* $2 \le d$ *if* $\operatorname{char} k = 0$).

(4) *The following inclusion* (*equivalent to equality*) *of ideals in S holds: $I \cap J^2 \cap (I^2 : \partial) \subseteq I \cdot J$, where $I = \operatorname{ann}_S(f)$ and $J = \operatorname{ann}_S(\partial \lrcorner f)$.*

Proof. It is straightforward to check that the inclusion $I \cdot J \subseteq I \cap J^2 \cap (I^2 : \partial) \subseteq I \cdot J$ in point (4) always holds, thus the other inclusion is equivalent to equality.

(3) $\iff$ (4) $\iff$ (3a): The equivalence of (3) and (4) follows from Lemma 5.16. Since (4) is independent of d, the equivalence of (4) and (3a) also follows.

(2) $\iff$ (3) and (2a) $\iff$ (3a): We have an exact sequence of $k[t]$-modules

$$0 \to \mathfrak{I}/\mathfrak{I}^2 \to S[t]/\mathfrak{I}^2 \to S[t]/\mathfrak{I} \to 0.$$

Since $S[t]/\mathfrak{I}$ is a flat $k[t]$-module by Proposition 5.9, we see from the long exact sequence of Tor that $\mathfrak{I}/\mathfrak{I}^2$ is flat if and only if $S[t]/\mathfrak{I}^2$ is flat.

(1) $\iff$ (2) and (1a) $\iff$ (2a): Let $g \in P[x]$ be the d-th ray sum of f with respect to ∂. We may consider $\operatorname{Apolar}(g)$, $\operatorname{Apolar}(f)$ and $\operatorname{Apolar}(\partial \lrcorner f)$ as quotients of a polynomial ring T_{poly}, corresponding to points of the Hilbert scheme. The dimension of the tangent space at $\operatorname{Apolar}(g)$ is given by $\dim_k \mathfrak{I}/\mathfrak{I}^2 \otimes k[t]/t = \dim_k \mathfrak{I}/(\mathfrak{I}^2 + (t))$. By Remark 5.17 it is equal to the sum of the dimension of the tangent space at $\operatorname{Apolar}(f)$ and $d-1$ times the dimension of the tangent space to $\operatorname{Apolar}(\partial \lrcorner f)$. Since both algebras are smoothable and unobstructed, we conclude that $\operatorname{Apolar}(g)$ is also unobstructed. On the other hand, if $\operatorname{Apolar}(g)$ is unobstructed, then $\mathfrak{I}/\mathfrak{I}^2$ is a finite $k[t]$-module such that the length of the fiber $\mathfrak{I}/\mathfrak{I}^2 \otimes k[t]/\mathfrak{m}$ does not depend on the choice of the maximal ideal $\mathfrak{m} \subseteq k[t]$. Then $\mathfrak{I}/\mathfrak{I}^2$ is flat, by [Hartshorne 1977, Exercise II.5.8 or Theorem III.9.9] applied to the associated sheaf. □

Remark 5.19. The condition from point (4) of Theorem 5.18 seems very technical. It is enlightening to look at the images of $(I^2 : \partial) \cap I$ and $I \cdot J$ in I/I^2. The image of $(I^2 : \partial) \cap I$ is the annihilator of ∂ in I/I^2. This annihilator clearly contains

$(I : \partial) \cdot I/I^2 = J \cdot I/I^2$. This shows that if the S/I-module I/I^2 is "nice", for example free, we should have an equality $(I^2 : \partial) \cap I = I \cdot J$. More generally, this equality is connected to the syzygies of I/I^2.

In the remainder of this subsection we will prove that in several situations the conditions of Theorem 5.18 are satisfied.

Corollary 5.20. *We keep the notation and assumptions of Theorem 5.18. Suppose further that the algebra* $S/I = \mathrm{Apolar}(f)$ *is a complete intersection. Then the equivalent conditions of Theorem 5.18 are satisfied.*

Proof. Since S/I is a complete intersection, the S/I-module I/I^2 is free; see, e.g., [Matsumura 1986, Theorem 16.2] and discussion above it or [Eisenbud 1995, Exercise 17.12a]. This implies that $(I^2 : \partial) \cap I = (I : \partial)I = JI$, because $J = \mathrm{ann}_S(\partial \lrcorner f) = \{s \in S \mid s\partial \lrcorner f = 0\} = (\mathrm{ann}_S(f) : \partial) = (I : \partial)$. Thus the condition from point (4) of Theorem 5.18 is satisfied. □

Example 5.21. If $A = S/I$ is a complete intersection, then it is smoothable and unobstructed (see Section 2D). The apolar algebras of monomials are complete intersections, therefore the assumptions of Theorem 5.18 are satisfied, for example, for $f = x_1^2x_2^2x_3$ and $\partial = \alpha_2^2$. Now Corollary 5.20 implies that the equivalent conditions of the theorem are also satisfied; thus $x_1^2x_2^2x_3 + x_4^d x_1^2 x_3 = (x_2^2x_3)(x_1^2 + x_4^d)$ is unobstructed for every $d \geq 2$ (provided $\mathrm{char}\, k = 0$ or $d \leq \mathrm{char}\, k$). Similarly, $x_1^2x_2x_3 + x_4^2x_1$ is unobstructed and has Hilbert function $(1, 4, 5, 3, 1)$.

Example 5.22. Let $f = (x_1^2 + x_2^2)x_3$; then $\mathrm{ann}_S(f) = (\alpha_1^2 - \alpha_2^2, \alpha_1\alpha_2, \alpha_3^2)$ is a complete intersection. Take $\partial = \alpha_1\alpha_3$, then $\partial \lrcorner f = x_1$ and $\partial^2 \lrcorner f = 0$; thus $f + x_4^2 \partial \lrcorner f = x_1^2x_3 + x_2^2x_3 + x_4^2x_1$ is unobstructed. Note that by Remark 5.8 the apolar algebra of this polynomial has Hilbert function $(1, 4, 4, 1)$.

Proposition 5.23. *Let* $f \in P$ *be such that* $\mathrm{Apolar}(f)$ *is a complete intersection.*

Let d *be a natural number. Suppose that* $\mathrm{char}\, k = 0$ *or* $d \leq \mathrm{char}\, k$. *Take* $\partial \in S$ *such that* $\partial^2 \lrcorner f = 0$ *and* $\mathrm{Apolar}(\partial \lrcorner f)$ *is also a complete intersection. Let* $g \in P[y]$ *be the* d*-th ray sum* f *with respect to* ∂, *i.e.*, $g = f + y^d \partial \lrcorner f$.

Suppose that $\deg \partial \lrcorner f > 0$. *Let* β *be the variable dual to* y *and* $\sigma \in S$ *be such that* $\sigma \lrcorner (\partial \lrcorner f) = 1$. *Take* $\varphi := \sigma\beta \in T = S[\![\beta]\!]$. *Let* h *be any ray sum of* g *with respect to* φ; *explicitly*,

$$h = f + y^d \partial \lrcorner f + z^m y^{d-1}$$

for some $m \geq 2$.

Then the algebra $\mathrm{Apolar}(h)$ *is unobstructed.*

Proof. First note that $\varphi \lrcorner g = y^{d-1}$ and so $\varphi^2 \lrcorner g = \sigma \lrcorner y^{d-2} = 0$, since $\sigma \in \mathfrak{m}_S$. Therefore, indeed, h has the presented form.

From Corollary 5.20 it follows that Apolar(g) is unobstructed. Since $\varphi \lrcorner g = y^{d-1}$, the algebra Apolar$(\varphi \lrcorner g)$ is unobstructed as well. Now, by Theorem 5.18 it remains to prove that

$$(I_g^2 : \varphi) \cap I_g \cap J_g^2 \subseteq I_g J_g, \tag{8}$$

where $I_g = \operatorname{ann}_T(g)$, $J_g = \operatorname{ann}_T(\varphi \lrcorner g)$. The rest of the proof is a technical verification of this claim. Denote $I_f := \operatorname{ann}_S(f)$ and $J_f := \operatorname{ann}_S(\partial \lrcorner f)$; note that we take annihilators in S. By Proposition 5.7 we have $I_g = I_f T + \beta J_f T + (\beta^d - \partial)T$. Consider $\gamma \in T$ lying in $(I_g^2 : \varphi) \cap I_g \cap J_g^2$. Write $\gamma = \gamma_0 + \gamma_1\beta + \gamma_2\beta^2 + \cdots$, where $\gamma_i \in S$, so they do not contain β. We will prove that $\gamma \in I_g J_g$.

First, since $(\beta^d - \partial)^2 \in I_g J_g$ we may reduce powers of β in γ using this element and so we assume $\gamma_i = 0$ for $i \geq 2d$. Let us take $i < 2d$. Since $\gamma \in J_g^2 = (\operatorname{ann}_T(y^{d-1}))^2 = (\mathfrak{m}_S, \beta^d)^2$, we see that $\gamma_i \in \mathfrak{m}_S \subseteq J_g$. For $i > d$ we have $\beta^i \in I_g$, so that $\gamma_i \beta^i \in J_g I_g$ and we may assume $\gamma_i = 0$. Moreover, $\beta^d \gamma_d - \partial\gamma_d \in I_g J_g$, so we may also assume $\gamma_d = 0$, obtaining

$$\gamma = \gamma_0 + \cdots + \gamma_{d-1}\beta^{d-1}.$$

From the explicit description of I_g in Proposition 5.7 it follows that $\gamma_i \in J_f$ for all i.

Let $M = I_g^2 \cap \varphi T = I_g^2 \cap J_f \beta T$. Then, for γ as above we have $\gamma\varphi \in M$, so we will analyze the module M. Recall that

$$I_g^2 = I_f^2 \cdot T + \beta I_f J_f \cdot T + \beta^2 J_f^2 \cdot T + (\beta^d - \partial) I_f \cdot T + (\beta^d - \partial)\beta J_f \cdot T + (\beta^d - \partial)^2 \cdot T. \tag{9}$$

We claim that

$$M \subseteq I_f^2 \cdot T + \beta I_f J_f \cdot T + \beta^2 J_f^2 \cdot T + (\beta^d - \partial)\beta J_f \cdot T. \tag{10}$$

We have $I_g^2 \subseteq J_f \cdot T + (\beta^d - \partial)^2 \cdot T$ so, if an element of I_g^2 lies in $J_f \cdot T$, then its coefficient associated to $(\beta^d - \partial)^2$ in presentation (9) is an element of J_f, by Lemma 2.15. Since $J_f \cdot (\beta^d - \partial) \subseteq I_f + \beta J_f$, we may ignore the term $(\beta^d - \partial)^2$:

$$M \subseteq I_f^2 \cdot T + \beta I_f J_f \cdot T + \beta^2 J_f^2 \cdot T + (\beta^d - \partial) I_f \cdot T + (\beta^d - \partial)\beta J_f \cdot T. \tag{11}$$

Choose an element of M and let $i \in I_f \cdot T$ be the coefficient of this element associated to $(\beta^d - \partial)$. Since $I_f T \cap \beta T \subseteq J_f T$, we may assume that i does not contain β, i.e., $i \in I_f$. Now, if an element of the right-hand side of (11) lies in $\beta \cdot T$, then the coefficient i satisfies $i \cdot \partial \in I_f^2$, so that $i \in (I_f^2 : \partial)$. Since I_f is a complete intersection ideal, the S/I_f-module I_f/I_f^2 is free; see Corollary 5.20 for references. Then we have $(I_f^2 : \partial) = (I_f : \partial) I_f$ and $i \in (I_f : \partial) I_f = I_f J_f$. Then $i \cdot (\beta^d - \partial) \subseteq I_f^2 + \beta \cdot I_f \cdot J_f$ and so the inclusion (10) is proved. We return to the proof of proposition.

From Lemma 2.15 applied to the ideal $J_f^2 T$ and the element $\beta(\beta^d - \partial)$, and the fact that $\beta\partial J_f^2 \subseteq I_g^2$, we compute that $M \cap \{\delta \mid \deg_\beta \delta \leq d\}$ is a subset

of $I_f^2 \cdot T + \beta \cdot I_f J_f \cdot T + \beta^2 J_f^2 \cdot T$. Then $\gamma\varphi = \gamma\beta\sigma$ lies in this set, so that $\gamma_0 \in (I_f J_f : \sigma)$ and $\gamma_n \in (J_f^2 : \sigma)$ for $n > 1$. Since Apolar(f) and Apolar$(\partial \lrcorner f)$ are complete intersections, we have $\gamma_0 \in I_f \mathfrak{m}_S$ and $\gamma_i \in J_f \mathfrak{m}_S$ for $i \geq 1$. It follows that $\gamma \in I_g \mathfrak{m}_S \subseteq I_g J_g$. □

Example 5.24. Let $f \in P$ be a polynomial such that $A = \text{Apolar}(f)$ is a complete intersection. Take ∂ such that $\partial \lrcorner f = x_1$ and $\partial^2 \lrcorner f = 0$. Then the apolar algebra of $f + y_1^d x_1 + y_2^m y_1^{d-1}$ is unobstructed for any $d, m \geq 2$ (less or equal to $\operatorname{char} k$ if it is nonzero). In particular, $g = f + y_1^2 x_1 + y_2^2 y_1$ is unobstructed.

Continuing Example 5.22, if $f = x_1^2 x_3 + x_2^2 x_3$; then $x_1^2 x_3 + x_2^2 x_3 + x_4^2 x_1 + x_5^2 x_4$ is unobstructed. The apolar algebra of this polynomial has Hilbert function $(1, 5, 5, 1)$.

Let $g = x_1^2 x_3 + x_2^2 x_3 + x_4^2 x_1$, then $x_1^2 x_3 + x_2^2 x_3 + x_4^2 x_1 + x_5^2 x_4$ is a ray sum of g with respect to $\partial = \alpha_4 \alpha_1$. Let $I := \text{ann}_S(g)$ and $J := (I : \partial)$. In contrast with Corollary 5.20 and Example 5.22 one may check that all three terms, I, J^2 and $(I^2 : \partial)$, are necessary to obtain equality in the inclusion (8) for g and ∂, that is, no two ideals of I, J^2, $(I^2 : \partial)$ have intersection equal to IJ.

Example 5.25. Let $f = x_1^5 + x_2^4$. Then the annihilator of f in $k[\alpha_1, \alpha_2]$ is a complete intersection, and this is true for every $f \in k[x_1, x_2]$. Let $g = f + x_3^2 x_1^2$ be the second ray sum of f with respect to α_1^3 and $h = g + x_4^2 x_3$ be the second ray sum of g with respect to $\alpha_3 \alpha_1^2$. Then the apolar algebra of

$$h = x_1^5 + x_2^4 + x_3^2 x_1^2 + x_4^2 x_3$$

is smoothable and not obstructed. It has Hilbert function $(1, 4, 4, 3, 1, 1)$.

Remark 5.26. The assumption $\deg \partial \lrcorner f > 0$ in Proposition 5.23 is necessary: the polynomial $h = x_1 x_2 x_3 + x_4^2 + x_5^2 x_4$ is obstructed, with length 12 and tangent space dimension $67 > 12 \cdot 5$ over $k = \mathbb{C}$. The polynomial g is the fourth ray sum of $x_1 x_2 x_3$ with respect to $\alpha_1 \alpha_2 \alpha_3$ and h is the second ray sum of $g = x_1 x_2 x_3 + x_4^2$ with respect to α_4; thus this example satisfies the assumptions of Proposition 5.23 except for $\deg \partial \lrcorner f > 0$. Note that in this case $\alpha_4^2 \lrcorner g \neq 0$.

6. Proof of the main theorem and comments on the degree 14 case

6A. ***Preliminary results.*** Let $r \geq 1$ be a natural number and V be a constructible subset of $P_{\leq s}$. Assume that the apolar algebra Apolar(f) has length r for every closed point $f \in V$. We may construct the incidence scheme $\{(f, \text{Apolar}(f))\} \to V$, which is a finite flat family over V, and thus we obtain a morphism from V to the (punctual) Hilbert scheme of r points on an appropriate $\mathbb{P}^n$. See [Jelisiejew 2014a, Proposition 4.39] for details.

Consider $f \in P_{\leq s}$. The apolar algebra of f has length at most r if and only if the matrix of partials $S_{\leq s} f$ has rank at most r. This is a closed condition, so we obtain the following remark:

Remark 6.1. Let s be a positive integer and $V \subseteq P_{\leq s}$ be a constructible subset. Then the set U, consisting of $f \in V$ such that the apolar algebra of f has maximal length (among the elements of V), is open in V. In particular, if V is irreducible then U is also irreducible.

Example 6.2. Let $P_{\geq 4} = k[x_1, \ldots, x_n]_{\geq 4}$ be the space of polynomials that are sums of monomials of degree at least 4. Suppose that the set $V \subseteq P_{\geq 4}$ parameterizing algebras with fixed Hilbert function H is irreducible. Then also the set W of polynomials $f \in P$ such that $f_{\geq 4} \in V$ is irreducible. Let $e := H(1)$ and suppose that the symmetric decomposition of H has zero rows $\Delta_{s-3} = (0, 0, 0, 0)$ and $\Delta_{s-2} = (0, 0, 0)$, where $s = \deg f$. We claim that a general element of W corresponds to an algebra B with Hilbert function $H_{\max} = H + (0, n-e, n-e, 0)$. Indeed, since we may only vary the degree-three part of the polynomial, the function H_B has the form $H + (0, a, a, 0) + (0, b, 0)$ for some a, b such that $a + b \leq n - e$. Therefore, algebras with Hilbert function $H_{\max}$ are precisely the algebras of maximal possible length. Since $H_{\max}$ is attained for $f_{\geq 4} + x_{e+1}^3 + \cdots + x_n^3$, the claim follows from Remark 6.1.

6B. ***Lemmas on Hilbert functions.*** In the following, H_A denotes the Hilbert function of an algebra A.

Lemma 6.3. *Suppose that A is a local Artin Gorenstein algebra of socle degree $s \geq 3$ such that $\Delta_{A,s-2} = (0, 0, 0)$. Then* $\operatorname{len} A \geq 2(H_A(1) + 1)$. *Furthermore, equality occurs if and only if $s = 3$.*

Proof. Consider the symmetric decomposition $\Delta_\bullet = \Delta_{A,\bullet}$ of H_A. From symmetry we have $\sum_j \Delta_0(j) \geq 2 + 2\Delta_0(1)$, with equality only if Δ_0 has no terms between 1 and $s-1$, i.e., when $s = 3$. Similarly, $\sum_j \Delta_i(j) \geq 2\Delta_i(1)$ for all $1 \leq i < s-2$. Summing these inequalities we obtain

$$\operatorname{len} A = \sum_{i<s-2} \sum_j \Delta_i(j) \geq 2 + \sum_{i<s-2} 2\Delta_i(1) = 2 + 2H_A(1). \qquad \square$$

Lemma 6.4. *Let A be a local Artin Gorenstein algebra of length at most* 14. *Suppose that* $4 \leq H_A(1) \leq 5$. *Then* $H_A(2) \leq 5$.

Proof. Let s be the socle degree of A. If $H_A(2) \geq 6$, then $H_A(3) + H_A(4) + \cdots \leq 3$; thus $s \in \{3, 4, 5\}$. The cases $s = 3$ and $s = 5$ immediately lead to contradiction — it is impossible to get the required symmetric decomposition. We will consider the case $s = 4$. In this case, $H_A = (1, *, *, *, 1)$ and its symmetric decomposition is $(1, e, q, e, 1) + (0, m, m, 0) + (0, t, 0)$. Then $e = H_A(3) \leq 14 - 2 - 4 - 6 = 2$. Since $H_A(1) < H_A(2)$ we have $e < q$. This can only happen if $e = 2$ and $q = 3$. But then $14 \geq \operatorname{len} A = 9 + 2m + t$; thus $m \leq 2$ and $H_A(2) = m + q \leq 5$, a contradiction. $\square$

Lemma 6.5. *There does not exist a local Artin Gorenstein algebra with Hilbert function*

$$(1, 4, 3, 4, 1, \ldots, 1).$$

Proof. See [Iarrobino 1994, pp. 99–100] for the proof or [Casnati et al. 2014, Lemma 5.3] for a generalization. We provide a sketch for completeness. Suppose such an algebra A exists and fix its dual socle generator $f \in k[x_1, \ldots, x_4]_s$ in the standard form. Let $I = \operatorname{ann}_S(f)$. The proof relies on two observations. First, the leading term of f is, up to a constant, equal to x_1^s and in fact we may take $f = x_1^s + f_{\leq 4}$. Moreover, from the symmetric decomposition it follows that the Hilbert functions of $\operatorname{Apolar}(x_1^s + f_4)$ and $\operatorname{Apolar}(f)$ are equal. Second, $h(3) = 4 = 3^{\langle 2\rangle} = h(2)^{\langle 2\rangle}$ is the maximal growth, so arguing similarly as in Lemma 2.9 we may assume that the degree-two part, I_2, of the ideal of $\operatorname{gr} A$ is equal to $((\alpha_3, \alpha_4)S)_2$. Then any derivative of $\alpha_3 \lrcorner f_4$ is a derivative of x_1^s, so a power of x_1. It follows that $\alpha_3 \lrcorner f_4$ itself is a power of x_1; similarly, $\alpha_4 \lrcorner f_4$ is a power of x_1. It follows that $f_4 \in x_1^3 \cdot k[x_1, x_2, x_3, x_4] + k[x_1, x_2]$, but then f_4 is annihilated by a linear form, which contradicts the fact that f is in the standard form. □

The following lemmas essentially deal with the limit-reducibility in the case $(1, 4, 4, 3, 1, 1)$. Here the method is straightforward, but the cost is that the proof is broken into several cases and quite long.

Lemma 6.6. *Let $f = x_1^5 + f_4$ be a polynomial such that $H_{\operatorname{Apolar}(f)}(2) < H_{\operatorname{Apolar}(f_4)}(2)$. Let $\mathcal{Q} = S_2 \cap \operatorname{ann}_S(x_1^5) \subseteq S_2$. Then $x_1^2 \in \mathcal{Q} f_4$ and $\operatorname{ann}_S(f_4)_2 \subseteq \mathcal{Q}$.*

Proof. Note that $\dim \mathcal{Q} f_4 \geq \dim S_2 f_4 - 1 = H_{\operatorname{Apolar}(f_4)}(2) - 1$. If $\operatorname{ann}_S(f_4)_2 \not\subseteq \mathcal{Q}$, then there is a $q \in \mathcal{Q}$ such that $\alpha_1^2 - q \in \operatorname{ann}_S(f_4)$. Then $\mathcal{Q} f_4 = S_2 f_4$ and we obtain a contradiction. Suppose that $x_1^2 \notin \mathcal{Q} f_4$. Then the degree-two partials of f contain a direct sum of kx_1^2 and $\mathcal{Q} f_4$, so they are at least $H_{\operatorname{Apolar}(f_4)}(2)$-dimensional, so that $H_{\operatorname{Apolar}(f)}(2) \geq H_{\operatorname{Apolar}(f_4)}(2)$, a contradiction. □

Lemma 6.7. *Let $f = x_1^5 + f_4 \in P$ be a polynomial with $H_{\operatorname{Apolar}(f)} = (1, 3, 3, 3, 1, 1)$ and $H_{\operatorname{Apolar}(f_4)} = (1, 3, 4, 3, 1)$. Suppose that $\alpha_1^3 \lrcorner f_4 = 0$ and that $(\operatorname{ann}_S(f_4))_2$ defines a complete intersection. Then $\operatorname{Apolar}(f_4)$ and $\operatorname{Apolar}(f)$ are complete intersections.*

Proof. Let $I := \operatorname{ann}_S(f_4)$. First we will prove that $\operatorname{ann}_S(f_4) = (q_1, q_2, c)$, where $\langle q_1, q_2\rangle = I_2$ and $c \in I_3$. Then, of course, $\operatorname{Apolar}(f_4)$ is a complete intersection. By assumption, q_1 and q_2 form a regular sequence. Thus there are no syzygies of degree at most three in the minimal resolution of $\operatorname{Apolar}(f_4)$. By the symmetry of the minimal resolution — see [Eisenbud 1995, Corollary 21.16] — there are no generators of degree at least four in the minimal generating set of I. Thus I is generated in degrees two and three. But $H_{S/(q_1,q_2)}(3) = 4 = H_{S/I}(3) + 1$; thus there

is a cubic c such that $I_3 = kc \oplus (q_1, q_2)_3$, then $(q_1, q_2, c) = I$, so $\mathrm{Apolar}(f_4) = S/I$ is a complete intersection.

Let $\mathcal{Q} := \mathrm{ann}_S(x_1^5) \cap S_2 \subseteq S_2$. By Lemma 6.6 we have $q_1, q_2 \in \mathcal{Q}$, so that $\alpha_1^3 \in I \setminus (q_1, q_2)$, then $I = (q_1, q_2, \alpha_1^3)$. Moreover, by the same lemma, there exists $\sigma \in \mathcal{Q}$ such that $\sigma \lrcorner f_4 = x_1^2$.

Now we prove $\mathrm{Apolar}(f)$ is a complete intersection. Let $J := (q_1, q_2, \alpha_1^3 - \sigma) \subseteq \mathrm{ann}_S(f)$. We will prove that S/J is a complete intersection. Since q_1, q_2, α_1^3 is a regular sequence, the set $S/(q_1, q_2)$ is a cone over a scheme of dimension zero and α_1^3 does not vanish identically on any of its components. Since σ has degree two, $\alpha_1^3 - \sigma$ also does not vanish identically on any of the components of $\mathrm{Spec}\, S/(q_1, q_2)$; thus $\mathrm{Spec}\, S/J$ has dimension zero, so it is a complete intersection (see also [Valabrega and Valla 1978, Corollary 2.4, Remark 2.5]). Then the quotient by J has length at most $\deg(q_1)\deg(q_2)\deg(\alpha_1^3 - \sigma) = 12 = \dim_k S/\mathrm{ann}_S(f)$. Since $J \subseteq \mathrm{ann}_S(f)$, we have $\mathrm{ann}_S(f) = J$ and $\mathrm{Apolar}(f)$ is a complete intersection. □

Lemma 6.8. *Let* $f = x_1^5 + f_4 + g$, *where* $\deg g \leq 3$, *be a polynomial such that* $H_{\mathrm{Apolar}(f_{\geq 4})} = (1, 3, 3, 3, 1, 1)$ *and* $H_{\mathrm{Apolar}(f_4)} = (1, 3, 4, 3, 1)$. *Suppose that* $\alpha_1^3 \lrcorner f_4 = 0$ *and that* $(\mathrm{ann}_S(f_4))_2$ *does not define a complete intersection. Then* $\mathrm{Apolar}(f)$ *is limit-reducible.*

Proof. Let $\langle q_1, q_2\rangle = (\mathrm{ann}_S(f_4))_2$. Since q_1, q_2 do not form a regular sequence, we have, after a linear transformation φ, two possibilities: $q_1 = \alpha_1\alpha_2$ and $q_2 = \alpha_1\alpha_3$, or $q_1 = \alpha_1^2$ and $q_2 = \alpha_1\alpha_2$. Let β be the image of α_1 under φ, so that $\beta^3 \lrcorner f_4 = 0$.

Suppose first that $q_1 = \alpha_1\alpha_2$ and $q_2 = \alpha_1\alpha_3$. If β is, up to a constant, equal to α_1, then $\alpha_1\alpha_2$, $\alpha_1\alpha_3$, $\alpha_1^3 \in \mathrm{ann}_S(f_4)$, so that α_1^2 is in the socle of $\mathrm{Apolar}(f_4)$, a contradiction. Thus we may assume, after another change of variables, that $\beta = \alpha_2$, $q_1 = \alpha_1\alpha_2$ and $q_2 = \alpha_1\alpha_3$. Then $f = x_2^5 + f_4 + \hat{g} = x_2^5 + x_1^4 + \hat{h} + \hat{g}$, where $\hat{h} \in k[x_1, x_3]$ and $\deg(\hat{g}) \leq 3$. Then, by Lemma 4.2, we may assume that $\alpha_1^2 \lrcorner f = 0$, so $\mathrm{Apolar}(f)$ is limit-reducible by Proposition 5.13. See also Example 5.14 (the degree assumption in the example can easily be modified).

Suppose now that $q_1 = \alpha_1^2$ and $q_2 = \alpha_1\alpha_2$. If β is not a linear combination of α_1 and α_2, then we may assume $\beta = \alpha_3$. Let m in f_4 be any monomial divisible by x_1. Since $q_1, q_2 \in \mathrm{ann}_S(f_4)$, we see that $m = \lambda x_1 x_3^3$ for some $\lambda \in k$. But, since $\beta^3 \in \mathrm{ann}_S(f_4)$, we have $m = 0$. Thus f_4 does not contain x_1, so $H_{\mathrm{Apolar}(f_4)}(1) < 3$, a contradiction. Thus $\beta \in \langle\alpha_1, \alpha_2\rangle$. Suppose $\beta = \lambda\alpha_1$ for some $\lambda \in k \setminus \{0\}$. Applying Lemma 6.6 to $f_{\geq 4}$ we see that x_1^2 is a derivative of f_4, so $\beta^2 \lrcorner f_4 \neq 0$, but $\beta^2 \lrcorner f_4 = \lambda^2 q_1 \lrcorner f_4 = 0$, a contradiction. Thus $\beta = \lambda_1\alpha_1 + \lambda_2\alpha_2$ and, changing α_2, we may assume that $\beta = \alpha_2$. This substitution does not change $\langle\alpha_1^2, \alpha_1\alpha_2\rangle$. Now we directly check that $f_4 = x_3^2(\kappa_1 x_1 x_3 + \kappa_2 x_2^2 + \kappa_3 x_2 x_3 + \kappa_4 x_3^2)$ for some $\kappa_\bullet \in k$. Since x_1 is a derivative of f, we have $\kappa_1 \neq 0$. Then a nonzero element $\kappa_2\alpha_1\alpha_3 - \kappa_1\alpha_2^2$ annihilates f_4, a contradiction with $H_{\mathrm{Apolar}(f_4)}(2) = 4$. □

Lemma 6.9. *Let a quartic f_4 be such that $H_{\mathrm{Apolar}(f_4)} = (1, 3, 3, 3, 1)$ and $\alpha_1^3 \lrcorner f_4 = 0$. Then $H_{\mathrm{Apolar}(x_1^5+f_4)}(2) \geq 4$.*

Proof. Let $\mathcal{Q} = \mathrm{ann}_S(x_1^5)_2 \subseteq S_2$. Let I denote the apolar ideal of f_4. By Proposition 4.9 we see that I is minimally generated by three elements of degree two and two elements of degree four. In particular, there are no cubics in the generating set. Since $\alpha_1^3 \in I_3$, there is an element in $\sigma \in I_2$ such that $\sigma = \alpha_1^2 - q$, where $q \in \mathcal{Q}$. Therefore, $\mathcal{Q} \lrcorner f_4 = S_2 \lrcorner f_4$. Moreover, σ does not annihilate x_1^2, so that x_1^2 is not a partial of f_4. We see that x_1^2 and $\mathcal{Q} \lrcorner f_4$ are leading forms of partials of $x_1^5 + f_4$; thus

$$H_{\mathrm{Apolar}(x_1^5+f_4)}(2) \geq 1 + \dim(\mathcal{Q} \lrcorner f_4) = 1 + \dim(S_2 \lrcorner f_4) = 1 + H_{\mathrm{Apolar}(f_4)}(2) = 4. \quad \square$$

Remark 6.10. Given the assumptions of Lemma 6.9, it is not hard to deduce that $H_{\mathrm{Apolar}(x_1^5+f_4)} = (1, 3, 4, 3, 1, 1)$ by analyzing the possible symmetric decompositions. We do not need this stronger statement, so we omit the proof.

6C. ***Proofs.*** The following proposition generalizes results about algebras with Hilbert function $(1, 5, 5, 1)$ obtained in [Jelisiejew 2014b; Bertone et al. 2012].

Proposition 6.11. *Let A be a local Artin Gorenstein algebra of socle degree three and $H_A(2) \leq 5$. Then A is smoothable.*

Proof. Suppose that the Hilbert function of A is $(1, n, e, 1)$. By Proposition 4.5 the dual socle generator of A may be put in the form $f + x_{e+1}^2 + \cdots + x_n^2$, where $f \in k[x_1, \ldots, x_e]$. By repeated use of Example 5.12 we see that A is a limit of algebras of the form $\mathrm{Apolar}(f) \times k^{\oplus n-e}$. Thus it is smoothable if and only if $B = \mathrm{Apolar}(f)$ is.

Let $e := H_A(2)$; then $H_B = (1, e, e, 1)$. If $H_B(1) = e \leq 3$, then B is smoothable. It remains to consider $4 \leq e \leq 5$. The set of points corresponding to algebras with Hilbert function $(1, e, e, 1)$ is irreducible in $\mathcal{H}ilb_{2e+2}(\mathbb{P}^e)$, by Remark 6.1 for the obvious parameterization (as mentioned in [Iarrobino 1984, Theorem I, p. 350]); thus, it will be enough to find a smooth point in this set which corresponds to a smoothable algebra. The cases $e = 4$ and $e = 5$ are considered in Examples 5.22 and 5.24, respectively. $\square$

Remark 6.12. The claim of Proposition 6.11 holds true if we replace the assumption $H_A(2) \leq 5$ by $H_A(2) = 7$, thanks to the smoothability of local Artin Gorenstein algebras with Hilbert function $(1, 7, 7, 1)$; see [Bertone et al. 2012]. We will not use this result.

Lemma 6.13. *Let A be a local Artin Gorenstein algebra with Hilbert function H_A beginning with $H_A(0) = 1$, $H_A(1) = 4$, $H_A(2) = 5$, $H_A(3) \leq 2$. Then A is smoothable.*

Proof. Let f be a dual socle generator of A in the standard form. It follows from Macaulay's growth theorem that $H_A(m) \leq 2$ for all $m \geq 3$, so that $H_A = (1, 4, 5, 2, 2, \ldots, 2, 1, \ldots, 1)$. Let s be the socle degree of A.

Let $\Delta_{A,s-2} = (0, q, 0)$ be the $(s-2)$-nd row of the symmetric decomposition of H_A. If $q > 0$, then by Example 5.12 we know that A is limit-reducible; it is a limit of algebras of the form $B \times k$ such that $H_B(1) = H_A(1) - 1 = 3$. Then the algebra B is smoothable (see [Casnati and Notari 2009, Proposition 2.5]), so A is also smoothable. In the following we assume that $q = 0$.

We claim that $f_{\geq 4} \in k[x_1, x_2]$. Indeed, the symmetric decomposition of the Hilbert function is either $(1, 1, \ldots, 1)+(0, 1, \ldots, 1, 0)+(0, 0, 1, 0, 0)+(0, 2, 2, 0)$ or $(1, 2, \ldots, 2, 1) + (0, 0, 1, 0, 0) + (0, 2, 2, 0)$. Thus, $e(s-3) = \sum_{i\geq 3} \Delta_i(1) = 2$, so that $f_{\geq 4} \in k[x_1, x_2]$ and $H_{\mathrm{Apolar}(f_{\geq 4})}(1) = 2$; in particular, x_1 is a derivative of $f_{\geq 4}$, i.e., there exists a $\partial \in S$ such that $\partial \lrcorner f_{\geq 4} = x_1$. Then we may assume $\partial \in \mathfrak{m}_S^3$, so $\partial^2 \lrcorner f = 0$.

Let us fix $f_{\geq 4}$ and consider the set of all polynomials of the form $h = f_{\geq 4} + g$, where $g \in k[x_1, x_2, x_3, x_4]$ has degree at most three. By Example 6.2 the apolar algebra of a general such polynomial will have Hilbert function H_A. The set of polynomials h with fixed $h_{\geq 4} = f_{\geq 4}$ such that $H_{\mathrm{Apolar}(h)} = H_A$ is irreducible. This set contains $h := f_{\geq 4} + x_3^2 x_1 + x_4^2 x_3$. To finish the proof is it enough to show that h is smoothable and unobstructed. Since $\mathrm{Apolar}(f_{\geq 4})$ is a complete intersection, this follows from Example 5.24. □

The following Theorem 6.14 generalizes numerous earlier smoothability results on stretched (by Sally, [1979]), 2-stretched (by Casnati and Notari [2014a]) and almost-stretched (by Elias and Valla [2011]) algebras. It is important to understand that, in contrast with the mentioned papers, we avoid a full classification of algebras. In the course of the proof we give some partial classification.

Theorem 6.14. *Let A be a local Artin Gorenstein algebra with Hilbert function H_A satisfying $H_A(2) \leq 5$ and $H_A(3) \leq 2$. Then A is smoothable.*

Proof. We proceed by induction on $\operatorname{len} A$, the case $\operatorname{len} A = 1$ being trivial. If A has socle degree three, then the result follows from Proposition 6.11. Suppose that A has socle degree $s \geq 4$.

Let f be a dual socle generator of A in the standard form. If the symmetric decomposition of H_A has a term $\Delta_{s-2} = (0, q, 0)$ with $q \neq 0$, then by Example 5.12, we have that A is a limit of algebras of the form $B \times k$, where B satisfies the assumptions $H_B(2) \leq 5$ and $H_B(2) \leq 2$ on the Hilbert function. Then B is smoothable by induction, so also A is smoothable. Further in the proof we assume that $\Delta_{A,s-2} = (0, 0, 0)$.

We would like to understand the symmetric decomposition of the Hilbert function H_A of A. Since H_A satisfies the Macaulay growth condition (see Section 2E) it

follows that $H_A = (1, n, m, 2, 2, \dots, 2, 1, \dots, 1)$, where the number of twos is possibly zero. If follows that the possible symmetric decompositions of the Hilbert function are:

(1) $(1, 2, 2, \dots, 2, 1) + (0, 0, 1, 0, 0) + (0, n-3, n-3, 0)$,

(2) $(1, 1, 1 \dots, 1, 1) + (0, 1, 1, \dots, 1, 0) + (0, 0, 1, 0, 0) + (0, n-3, n-3, 0)$,

(3) $(1, 1, 1 \dots, 1, 1) + (0, 1, 2, 1, 0) + (0, n-3, n-3, 0)$,

(4) $(1, \dots, 1) + (0, n-1, n-1, 0)$,

(5) $(1, 2, \dots, 2, 1) + (0, n-2, n-2, 0)$,

(6) $(1, \dots, 1) + (0, 1, \dots, 1, 0) + (0, n-2, n-2, 0)$,

and that the decomposition is uniquely determined by the Hilbert function. In all cases we have $H_A(1) \le H_A(2) \le 5$, so $f \in k[x_1, \dots, x_5]$. Let us analyze the first three cases. In each of them we have $H_A(2) = H_A(1) + 1$. If $H_A(1) \le 3$, then A is smoothable; see [Casnati and Notari 2009, Corollary 2.4]. Suppose $H_A(1) \ge 4$. Since $H_A(2) \le 5$, we have $H_A(2) = 5$ and $H_A(1) = 4$. In this case the result follows from Lemma 6.13 above.

It remains to analyze the three remaining cases. The proof is similar to the proof of Lemma 6.13, however here it essentially depends on induction. Let $f_{\ge 4}$ be the sum of homogeneous components of f which have degree at least four. Since f is in the standard form, we have $f_{\ge 4} \in k[x_1, x_2]$. The decomposition of the Hilbert function $\mathrm{Apolar}(f_{\ge 4})$ is one of the decompositions $(1, \dots, 1)$, $(1, 2 \dots, 2, 1)$ or $(1, \dots, 1) + (0, 1, \dots, 1, 0)$, depending on the decomposition of the Hilbert function of $\mathrm{Apolar}(f)$.

Let us fix a vector $\hat{h} = (1, 2, 2, 2, \dots, 2, 1, 1, \dots, 1)$ and take the sets

$$V_1 := \{f \in k[x_1, x_2] \mid H_{\mathrm{Apolar}(f)} = \hat{h}\} \quad \text{and} \quad V_2 := \{f \in k[x_1, \dots, x_n] \mid f_{\ge 4} \in V_1\}.$$

By Proposition 4.8 the set V_1 is irreducible and thus V_2 is also irreducible. The Hilbert function of the apolar algebra of a general member of V_2 is, by Example 6.2, equal to H_A. It remains to show that the apolar algebra of this general member is smoothable.

Proposition 4.8 implies that the general member of V_2 has (after a nonlinear change of coordinates) the form $f + \partial \lrcorner f$, where $f = x_1^s + x_2^{s_2} + g$ for some g of degree at most three. Using Lemma 4.2 we may assume (after another nonlinear change of coordinates) that $\alpha_1^2 \lrcorner g = 0$.

Let $B := \mathrm{Apolar}(x_1^s + x_2^{s_2} + g)$. We will show that B is smoothable. Since $s \ge 4 = 2 \cdot 2$, Proposition 5.13 shows that B is limit-reducible. Analyzing the fibers of the resulting degeneration, as in Example 5.15, we see that they have the form $B' \times k$, where $B' = \mathrm{Apolar}(\hat{f})$ and $\hat{f} = \lambda^{-1} x_1^{s-1} + x_2^{s_2} + g$. Then $H_{B'}(3) = H_{\mathrm{Apolar}(\hat{f}_{\ge 4})}(3) \le 2$. Moreover, $\hat{f} \in k[x_1, \dots, x_5]$, so that $H_{B'}(1) \le 5$. Now, analyzing the possible

symmetric decompositions of $H_{B'}$, which are listed above, we see that $H_{B'}(2) \leq H_{B'}(1) = 5$. It follows from induction on the length that B' is smoothable; thus $B' \times k$ and B are smoothable. □

Proposition 6.15. *Let A be a local Artin Gorenstein algebra of socle degree four satisfying* $\operatorname{len} A \leq 14$. *Then A is smoothable.*

Proof. We proceed by induction on the length of A. Then, by Proposition 6.11 (and the fact that all algebras of socle degree at most two are smoothable), we may assume that all algebras of socle degree *at most* four and length less than $\operatorname{len} A$ are smoothable.

If $\Delta_{A,1} = (0, q, 0)$ with $q \neq 0$, then by Example 5.12 the algebra A is a limit of algebras of the form $A' \times k$, where A' has socle degree four. Hence A is smoothable. Therefore we assume $q = 0$. Then $H_A(1) \leq 5$ by Lemma 6.3. Moreover, we may assume $H_A(1) \geq 4$, since otherwise A is smoothable by [Casnati and Notari 2009, Corollary 2.4].

The symmetric decomposition of H_A is $(1, n, m, n, 1) + (0, p, p, 0)$ for some n, m and p. By the fact that $n \leq 5$ and Stanley's result [1996, p. 67], we have $n \leq m$; thus $n \leq 4$ and $H_A(2) \leq H_A(1) \leq 5$. Due to $\operatorname{len} A \leq 14$, we have four cases, $n = 1, 2, 3, 4$, and five possible shapes of Hilbert functions, $H_A = (1, *, *, 1, 1)$, $H_A = (1, *, *, 2, 1)$, $H_A = (1, 4, 4, 3, 1)$, $H_A = (1, 4, 4, 4, 1)$ or $H_A = (1, 4, 5, 3, 1)$.

The conclusion in the first two cases follows from Theorem 6.14. In the remaining cases we first look for a suitable irreducible set of dual socle generators parameterizing algebras with prescribed H_A. We examine the case $H_A = (1, 4, 4, 3, 1)$. Consider the set of $f \in P = k[x_1, x_2, x_3, x_4]$ in the standard form and such that the apolar algebra of f has Hilbert function H_A. We claim that this set is irreducible. Since the leading form f_4 of such an f has Hilbert function $(1, 3, 3, 3, 1)$, the set of possible leading forms is irreducible by Proposition 4.9. Then the irreducibility follows from Example 6.2. The irreducibility in the cases $H_A = (1, 4, 4, 4, 1)$ and $H_A = (1, 4, 5, 3, 1)$ follows similarly from Proposition 4.10 together with Example 6.2. In the first two cases we see that f_4 is a sum of powers of variables; then Example 5.14 shows that the apolar algebra A of a general f is limit-reducible. More precisely, A is a limit of algebras of the form $A' \times k$, where A' has socle degree at most four (compare Example 5.15). Then A is smoothable. In the last case, Example 5.21 gives an unobstructed algebra in this irreducible set. This completes the proof. □

Lemma 6.16. *Let A be a local Artin Gorenstein algebra with Hilbert function* $(1, 4, 4, 3, 1, 1)$. *Then A is limit-reducible.*

Proof. Let $s = 5$ be the socle degree of A. If $\Delta_{A,s-2} \neq (0, 0, 0)$ then A is limit-reducible by Example 5.12, so we assume $\Delta_{A,s-2} = (0, 0, 0)$. The only possible

symmetric decomposition of the Hilbert function H_A with $\Delta_{A,s-2} = (0, 0, 0)$ is

$$(1, 4, 4, 3, 1, 1) = (1, 1, 1, 1, 1, 1) + (0, 2, 2, 2, 0) + (0, 1, 1, 0). \tag{12}$$

Let us take a dual socle generator f of A. We assume that f is in the standard form $f = x_1^5 + f_4 + g$, where $\deg g \leq 3$. Then $H_{\mathrm{Apolar}(x_1^5+f_4)} = (1, 3, 3, 3, 1, 1)$. We analyze the possible Hilbert functions of $B = \mathrm{Apolar}(f_4)$. By Lemma 4.2 we may assume that $\alpha_1^3 \lrcorner f_4 = 0$. Suppose first that $H_B(1) \leq 2$. From (12) it follows that $H_{\mathrm{Apolar}(x_1^5+f_4)}(1) = 3$, so that $H_B(1) = 2$ and we may assume that $f_4 \in k[x_2, x_3]$. Then, by Lemma 4.2, we may further assume $\alpha_1^2 \lrcorner (f - x_1^5) = 0$; then Proposition 5.13 asserts that $A = \mathrm{Apolar}(f)$ is limit-reducible.

Suppose now that $H_B(1) = 3$. Since x_1^5 is annihilated by a codimension-one space of quadrics, we have $H_B(2) \leq H_A(2) + 1$, so there are two possibilities: $H_B = (1, 3, 3, 3, 1)$ or $H_B = (1, 3, 4, 3, 1)$. By Lemma 6.9 the case $H_B = (1, 3, 3, 3, 1)$ is not possible, so that $H_B = (1, 3, 4, 3, 1)$. Now, by Lemma 6.8, we may consider only the case when $(\mathrm{ann}_S(f_4))_2$ is a complete intersection; then, by Lemma 6.7, we have that $\mathrm{Apolar}(x_1^5 + f_4)$ is a complete intersection. In this case we will actually prove that A is smoothable.

By Example 6.2, the set W of polynomials f with fixed leading polynomial $f_{\geq 4}$ and Hilbert function $H_{\mathrm{Apolar}(f)} = (1, 4, 4, 3, 1, 1)$ is irreducible. Consider the apolar algebra B of the polynomial $x_1^5 + f_4 + x_4^2 x_1 \in W$. By Proposition 5.10, this algebra is the limit of smoothable algebras $\mathrm{Apolar}(x_1^5 + f_4) \times \mathrm{Apolar}(x_1)$, so it is smoothable. By Corollary 5.20, the algebra B is unobstructed. Thus the apolar algebra of every element of W is smoothable; in particular A is smoothable. □

Now we are ready to prove Theorem 6.17, which is the algebraic counterpart of Theorems A and B.

Theorem 6.17. *Let A be an Artin Gorenstein algebra of length at most* 14. *Then either A is smoothable or it is local with Hilbert function* $(1, 6, 6, 1)$. *In particular, if A has length at most* 13, *then A is smoothable.*

Proof. By the discussion in Section 2D it is enough to consider local algebras. Let A be a local algebra of length at most 14 and of socle degree s. By H we denote the Hilbert function of A. As mentioned in Section 2D it is enough to prove A is limit-reducible. On the contrary, suppose that A is strongly nonsmoothable in the sense of Definition 2.5. By Example 5.12 we have $\Delta_{A,s-2} = (0, 0, 0)$. Then, by Lemma 6.3, we see that either $H = (1, 6, 6, 1)$ or $H(1) \leq 5$. It is enough to consider $H(1) \leq 5$. If $s = 3$ then $H(2) \leq H(1) \leq 5$, so by Proposition 6.11 we may assume $s > 3$. By Proposition 6.15 it follows that we may consider only $s \geq 5$.

If $H(1) \leq 3$ then A is smoothable by [Casnati and Notari 2009, Corollary 2.4]; thus we may assume $H(1) \geq 4$. By Lemma 6.4 we see that $H(2) \leq 5$. Then, by Theorem 6.14, we may reduce to the case $H(3) \geq 3$. By Macaulay's growth theorem

we have $H(2) \geq 3$. Then $\sum_{i>3} H(i) \leq 14-11$, so we are left with several possibilities: $H = (1, 4, 3, 3, 1, 1, 1)$, $H = (1, 4, 3, 3, 2, 1)$ or $H = (1, *, *, *, 1, 1)$. In the first two cases it follows from the symmetric decomposition that $\Delta_{A,s-2} \neq (0, 0, 0)$, which is a contradiction. We examine the last case. By Lemma 6.5 there does not exist an algebra with Hilbert function $(1, 4, 3, 4, 1, 1)$. Thus the only possibilities are $(1, 4, 3, 3, 1, 1)$, $(1, 5, 3, 3, 1, 1)$ and $(1, 4, 4, 3, 1, 1)$. Once more, it can be checked directly that in the first two cases $\Delta_{A,s-2} \neq (0, 0, 0)$. The last case is the content of Lemma 6.16. □

Remark 6.18. Assume $\operatorname{char} k = 0$. Iarrobino and Emsalem [1978] analyzed the tangent space to the Hilbert scheme. Iarrobino and Kanev [1999, Lemma 6.21] claim that using Macaulay they are able to check that the tangent space to $\mathcal{H}ilb_6(\mathbb{P}^{14})$ has dimension 76 at a point corresponding to a general local Gorenstein algebra A with Hilbert function $(1, 6, 6, 1)$; see [Casnati and Notari 2011] for further details. Since $76 < (1+6+6+1)\cdot 6$ this shows that A is nonsmoothable. Moreover, since all algebras of degree at most 13 are smoothable, A is strongly nonsmoothable.

To prove Theorem B, we need to show that the nonsmoothable part of $\mathcal{H}ilb^G_{14}\mathbb{P}^n$ (for $n \geq 6$) is irreducible. The algebraic version of (a generalization of) this statement is the following lemma:

Lemma 6.19. *Let $n \geq m$ be natural numbers and $V \subseteq P_{\leq 3} = k[x_1, \ldots, x_n]_{\leq 3}$ be the set of $f \in P$ such that $H_{\mathrm{Apolar}(f)} = (1, m, m, 1)$. Then V is constructible and irreducible.*

Proof. Let $V_{\mathrm{gr}} = V \cap P_3$ denote the set of *graded* algebras with Hilbert function $(1, m, m, 1)$. This is a constructible subset of P_3. To an element $f_3 \in V_{\mathrm{gr}}$ we may associate the tangent space to $\mathrm{Apolar}(f_3)$, which is isomorphic to $S_2 \lrcorner f_3$. We define

$$\big\{(f_3, [W]) \in V_{\mathrm{gr}} \times \mathrm{Gr}(m, n) \mid W \supseteq S_2 \lrcorner f_3\big\},$$

which is an open subset in a vector bundle $\big\{(f_3, [W]) \in P_3 \times \mathrm{Gr}(m, n) \mid W \supseteq S_2 \lrcorner f_3\big\}$ over $\mathrm{Gr}(m, n)$, given by the condition $\dim S_2 \lrcorner f_3 \geq m$. Let $f \in V$ and write it as $f = f_3 + f_{\leq 2}$, where $\deg f_{\leq 2} \leq 2$. Then $H_{\mathrm{Apolar}(f_3)} = (1, m, m, 1)$. Therefore, we obtain a morphism $\varphi : V \to V_{\mathrm{gr}}$ sending f to f_3. We will analyze its fibers. Let $f_3 \in V_{\mathrm{gr}}$ and $f = f_3 + f_{\leq 2} \in P_{\leq 3}$, where $\deg f_{\leq 2} \leq 2$. Then $H_{\mathrm{Apolar}(f)} = (1, M, m, 1)$ for some $M \geq m$. Moreover, $M = m$ if and only if $\alpha \lrcorner f_{\leq 2}$ is a partial of f_3 for every α annihilating f_3. The fiber of φ over f is an affine subspace of $P_{\leq 2}$ defined by these conditions and the morphism, writing $f = f_3 + f_{\leq 2}$,

$$\big\{(f, [W]) \in V \times \mathrm{Gr}(m, n) \mid W \supseteq S_2 \lrcorner f_3\big\} \to \big\{(f_3, [W]) \in V_{\mathrm{gr}} \times \mathrm{Gr}(m, n) \mid W \supseteq S_2 \lrcorner f_3\big\}$$

is a projection from a vector bundle, which is thus irreducible. Since V admits a surjection from this bundle, it is irreducible as well. Moreover, the above shows that V is constructible. □

Proof of Theorems A and B. The locus of points of the Hilbert scheme corresponding to smooth (i.e., reduced) algebras of length d is irreducible, as an image of an open subset of the d-symmetric product of $\mathbb{P}^n$, and smooth. The locus of points corresponding to smoothable algebras is the closure of the aforementioned locus, so it is also irreducible. If $d \leq 13$, or $d \leq 14$ and $n \leq 5$, this locus is the whole Hilbert scheme by Theorem 6.17, and the claim follows.

Now consider the case $d = 14$ and $n \geq 6$. Let $\mathcal{V}$ be the set of points of the Hilbert scheme corresponding to local Gorenstein algebras with Hilbert function $(1, 6, 6, 1)$. By Remark 6.18 these are the only nonsmoothable algebras of length 14; thus they deform only to local algebras with the same Hilbert function. Therefore, $\mathcal{V}$ is a sum of irreducible components of the Hilbert scheme. We will prove that $\mathcal{V}$ is an irreducible set whose general point is smooth.

Let $\mathcal{V}_p \subseteq \mathcal{V}$ denote the set consisting of schemes supported at a fixed point $p \in \mathbb{P}^n$. Then $\mathcal{V}$ is dominated by a set $\mathcal{V}_p \times \mathbb{P}^n$. Note that an irreducible scheme supported at a point p may be identified with a Gorenstein quotient of the power series ring having Hilbert function $(1, 6, 6, 1)$. These quotients are parameterized by the dual generators. More precisely, the set of V of $f \in k[x_1, \ldots, x_n]_{\leq 3}$ such that $H_{\mathrm{Apolar}(f)} = (1, 6, 6, 1)$ gives a morphism

$$V \to \mathcal{V}_p \subseteq \mathcal{H}ilb^G_{14}\mathbb{P}^n$$

which sends f to Spec Apolar(f) supported at p (see Section 6A). Since $V \to \mathcal{V}_p$ is surjective and V is irreducible by Lemma 6.19, we see that $\mathcal{V}_p$ is irreducible. Then $\mathcal{V}$ is irreducible as well.

Take a smooth point of $\mathcal{H}ilb^G_{14}\mathbb{P}^6$ which corresponds to an algebra A with Hilbert function $(1, 6, 6, 1)$. Then any point of $\mathcal{H}ilb^G_{14}\mathbb{P}^n$ corresponding to an embedding Spec $A \subseteq \mathbb{P}^n$ is smooth, by [Casnati and Notari 2009, Lemma 2.3]. This concludes the proof. □

List of symbols

All symbols appearing below are defined in Section 2.

- k is an algebraically closed field of characteristic $\neq 2, 3$.
- $P = k[x_1, \ldots, x_n]$ is a polynomial ring in n variables and fixed basis.
- $S = k[\![\alpha_1, \ldots, \alpha_n]\!]$ is a power series ring dual (see Section 2B) to P, with a fixed (dual) basis.
- $\mathfrak{m}_S$ is the maximal ideal of S.
- $S_{\mathrm{poly}} = k[\alpha_1, \ldots, \alpha_n]$ is a polynomial subring of S defined by the choice of the basis.
- H_A is the Hilbert function of a local Artin algebra A.

- $\Delta_{A,i}$, Δ_i is the i-th row of the symmetric decomposition of the Hilbert function of a local Artin Gorenstein algebra A; see Theorem 2.3.
- $e(a)$ is the a-th "embedding dimension", which is equal to $\sum_{t=0}^{a} \Delta_t(1)$; see Definition 3.1.
- $\operatorname{ann}_S(f)$ is the annihilator of $f \in P$ with respect to the action of S.
- $\operatorname{Apolar}(f)$ is the apolar algebra of $f \in P$, equal to $S/\operatorname{ann}_S(f)$.

Acknowledgements

We wish to express our thanks to A. A. Iarrobino and P. M. Marques for inspiring conversations. Moreover we are also sincerely grateful to W. Buczyńska and J. Buczyński for their care, support and hospitality during the preparation of this paper. We also thank Buczyński for explaining the proof of Proposition 4.7. We thank the referee for careful reading and suggesting a number of improvements. The examples were obtained with the help of the Magma computing software; see [Bosma et al. 1997].

References

[Bernardi et al. 2011] A. Bernardi, A. Gimigliano, and M. Idà, "Computing symmetric rank for symmetric tensors", *J. Symbolic Comput.* **46**:1 (2011), 34–53. MR 2012h:14126 Zbl 1211.14057

[Bertone et al. 2012] C. Bertone, F. Cioffi, and M. Roggero, "A division algorithm in an affine framework for flat families covering Hilbert schemes", preprint, 2012. arXiv 1211.7264

[Bosma et al. 1997] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system, I: The user language", *J. Symbolic Comput.* **24**:3–4 (1997), 235–265. MR 1484478 Zbl 0898.68039

[Bruns and Herzog 1993] W. Bruns and J. Herzog, *Cohen–Macaulay rings*, Cambridge Studies in Advanced Mathematics **39**, Cambridge University Press, 1993. MR 95h:13020 Zbl 0985.35075

[Buchsbaum and Eisenbud 1977] D. A. Buchsbaum and D. Eisenbud, "Algebra structures for finite free resolutions, and some structure theorems for ideals of codimension 3", *Amer. J. Math.* **99**:3 (1977), 447–485. MR 56 #11983 Zbl 0373.13006

[Buczyńska and Buczyński 2014] W. Buczyńska and J. Buczyński, "Secant varieties to high degree Veronese reembeddings, catalecticant matrices and smoothable Gorenstein schemes", *J. Algebraic Geom.* **23**:1 (2014), 63–90. MR 3121848 Zbl 1295.14047

[Buczyński and Jelisiejew 2014] J. Buczyński and J. Jelisiejew, "On smoothability", preprint, 2014, available at www.mimuw.edu.pl/ jjelisiejew/pdf/OnSmoothability06062014.pdf.

[Buczyński et al. $\geq$ 2015] J. Buczyński, T. Januszkiewicz, J. Jelisiejew, and M. Michałek, "On the existence of k-regular maps", submitted.

[Cartwright et al. 2009] D. A. Cartwright, D. Erman, M. Velasco, and B. Viray, "Hilbert schemes of 8 points", *Algebra Number Theory* **3**:7 (2009), 763–795. MR 2011c:14010 Zbl 1187.14005

[Casnati and Notari 2009] G. Casnati and R. Notari, "On the Gorenstein locus of some punctual Hilbert schemes", *J. Pure Appl. Algebra* **213**:11 (2009), 2055–2074. MR 2010g:14003 Zbl 1169.14003

[Casnati and Notari 2011] G. Casnati and R. Notari, "On the irreducibility and the singularities of the Gorenstein locus of the punctual Hilbert scheme of degree 10", *J. Pure Appl. Algebra* **215**:6 (2011), 1243–1254. MR 2012c:14007 Zbl 0837.58029

[Casnati and Notari 2014a] G. Casnati and R. Notari, "A structure theorem for 2-stretched Gorenstein algebras", preprint, 2014. To appear in *J. Comm. Algebra*. arXiv 1312.2191

[Casnati and Notari 2014b] G. Casnati and R. Notari, "On the Gorenstein locus of the punctual Hilbert scheme of degree 11", *J. Pure Appl. Algebra* **218**:9 (2014), 1635–1651. MR 3188862 Zbl 1287.13013

[Casnati et al. 2014] G. Casnati, J. Jelisiejew, and R. Notari, "On the rationality of Poincarè series of Gorenstein algebras via Macaulay's correspondence", preprint, 2014. To appear in *Rocky Mountain J. Math.* arXiv 1307.1676

[Eisenbud 1995] D. Eisenbud, *Commutative algebra: with a view toward algebraic geometry*, Graduate Texts in Mathematics **150**, Springer, New York, 1995. MR 97a:13001 Zbl 0819.13001

[Elias and Rossi 2012] J. Elias and M. E. Rossi, "Isomorphism classes of short Gorenstein local rings via Macaulay's inverse system", *Trans. Amer. Math. Soc.* **364**:9 (2012), 4589–4604. MR 2922602 Zbl 1281.13015

[Elias and Rossi 2015] J. Elias and M. E. Rossi, "Analytic isomorphisms of compressed local algebras", *Proc. Amer. Math. Soc.* **143**:3 (2015), 973–987. MR 3293715 Zbl 1314.13041

[Elias and Valla 2011] J. Elias and G. Valla, "Isomorphism classes of certain Artinian Gorenstein algebras", *Algebr. Represent. Theory* **14**:3 (2011), 429–448. MR 2012c:13059 Zbl 1248.13022

[Ellingsrud 1975] G. Ellingsrud, "Sur le schéma de Hilbert des variétés de codimension 2 dans $\mathbb{P}^e$ à cône de Cohen–Macaulay", *Ann. Sci. École Norm. Sup.* (4) **8**:4 (1975), 423–431. MR 52 #13831 Zbl 0325.14002

[Emsalem 1978] J. Emsalem, "Géométrie des points épais", *Bull. Soc. Math. France* **106**:4 (1978), 399–416. MR 80j:14008 Zbl 0396.13017

[Fogarty 1968] J. Fogarty, "Algebraic families on an algebraic surface", *Amer. J. Math* **90** (1968), 511–521. MR 38 #5778 Zbl 0176.18401

[Geramita 1999] A. V. Geramita, "Catalecticant varieties", pp. 143–156 in *Commutative algebra and algebraic geometry (Ferrara)*, edited by F. van Oystaeyen, Lecture Notes in Pure and Appl. Math. **206**, Dekker, New York, 1999. MR 2000f:14075 Zbl 0957.13007

[Grothendieck 1995] A. Grothendieck, "Techniques de construction et théorèmes d'existence en géométrie algébrique, IV: Les schémas de Hilbert", Exposé No. 221, 249–276 in *Séminaire Bourbaki*, vol. 6, Soc. Math. France, Paris, 1995. MR 1611822 Zbl 1031.00546

[Hartshorne 1966] R. Hartshorne, "Connectedness of the Hilbert scheme", *Inst. Hautes Études Sci. Publ. Math.* 29 (1966), 5–48. MR 35 #4232 Zbl 0171.41502

[Hartshorne 1977] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics **52**, Springer, New York, 1977. MR 57 #3116 Zbl 0367.14001

[Hartshorne 2010] R. Hartshorne, *Deformation theory*, Graduate Texts in Mathematics **257**, Springer, New York, 2010. MR 2011c:14023 Zbl 1186.14004

[Iarrobino 1972] A. Iarrobino, "Reducibility of the families of 0-dimensional schemes on a variety", *Invent. Math.* **15** (1972), 72–77. MR 46 #170 Zbl 0227.14006

[Iarrobino 1977] A. A. Iarrobino, *Punctual Hilbert schemes*, Mem. Amer. Math. Soc. **188**, Amer. Math. Soc., Providence, RI, 1977. MR 58 #5667 Zbl 0355.14001

[Iarrobino 1984] A. Iarrobino, "Compressed algebras: Artin algebras having given socle degrees and maximal length", *Trans. Amer. Math. Soc.* **285**:1 (1984), 337–378. MR 85j:13030 Zbl 0548.13009

[Iarrobino 1994] A. A. Iarrobino, *Associated graded algebra of a Gorenstein Artin algebra*, Mem. Amer. Math. Soc. **514**, Amer. Math. Soc., Providence, RI, 1994. MR 94f:13009 Zbl 0793.13010

[Iarrobino and Emsalem 1978] A. Iarrobino and J. Emsalem, "Some zero-dimensional generic singularities; finite algebras having small tangent space", *Compositio Math.* **36**:2 (1978), 145–188. MR 81c:14004 Zbl 0393.14002

[Iarrobino and Kanev 1999] A. Iarrobino and V. Kanev, *Power sums, Gorenstein algebras, and determinantal loci*, Lecture Notes in Mathematics **1721**, Springer, Berlin, 1999. MR 2001d:14056 Zbl 0942.14026

[Jelisiejew 2014a] J. Jelisiejew, "Deformations of zero-dimensional schemes and applications", preprint, 2014. arXiv 1307.8108

[Jelisiejew 2014b] J. Jelisiejew, "Local finite-dimensional Gorenstein k-algebras having Hilbert function $(1, 5, 5, 1)$ are smoothable", *J. Algebra Appl.* **13**:8 (2014), 1450056, 7. MR 3225123 Zbl 1317.13040

[Kleppe and Miró-Roig 1998] J. O. Kleppe and R. M. Miró-Roig, "The dimension of the Hilbert scheme of Gorenstein codimension 3 subschemes", *J. Pure Appl. Algebra* **127**:1 (1998), 73–82. MR 99a:14002 Zbl 0949.14003

[Kunz 2005] E. Kunz, *Introduction to plane algebraic curves*, Birkhäuser, Boston, 2005. MR 2006b: 14001 Zbl 1078.14041

[Landsberg and Ottaviani 2013] J. M. Landsberg and G. Ottaviani, "Equations for secant varieties of Veronese and other varieties", *Ann. Mat. Pura Appl.* (4) **192**:4 (2013), 569–606. MR 3081636 Zbl 1274.14058

[Matsumura 1986] H. Matsumura, *Commutative ring theory*, Cambridge Studies in Advanced Mathematics **8**, Cambridge University Press, 1986. MR 88h:13001 Zbl 0603.13001

[Miró-Roig 1992] R. M. Miró-Roig, "Nonobstructedness of Gorenstein subschemes of codimension 3 in $\mathbb{P}^n$", *Beiträge Algebra Geom.* **33** (1992), 131–138. MR 93d:14071 Zbl 0766.14001

[Raicu 2012] C. Raicu, "Secant varieties of Segre–Veronese varieties", *Algebra Number Theory* **6**:8 (2012), 1817–1868. MR 3033528 Zbl 1273.14102

[Sally 1979] J. D. Sally, "Stretched Gorenstein rings", *J. London Math. Soc.* (2) **20**:1 (1979), 19–26. MR 80k:14006 Zbl 0402.13018

[Stanley 1996] R. P. Stanley, *Combinatorics and commutative algebra*, 2nd ed., Progress in Mathematics **41**, Birkhäuser, Boston, 1996. MR 98h:05001 Zbl 0838.13008

[Valabrega and Valla 1978] P. Valabrega and G. Valla, "Form rings and regular sequences", *Nagoya Math. J.* **72** (1978), 93–101. MR 80d:14010 Zbl 0362.13007

Communicated by Ravi Vakil
Received 2014-09-13 Revised 2015-04-18 Accepted 2015-06-17

gianfranco.casnati@polito.it *Dipartimento di Scienze Matematiche, Politecnico di Torino, corso Duca degli Abruzzi 24, I-10129 Torino, Italy*

j.jelisiejew@mimuw.edu.pl *Faculty of Mathematics, Informatics, and Mechanics, University of Warsaw, Banacha 2, 02-097 Warsaw, Poland*

roberto.notari@polimi.it *Dipartimento di Matematica "Francesco Brioschi", Politecnico di Milano, via Bonardi 9, I-20133 Milano, Italy*

msp

ALGEBRA AND NUMBER THEORY 9:7 (2015)
dx.doi.org/10.2140/ant.2015.9.1571

p-adic heights of Heegner points on Shimura curves

Daniel Disegni

Let f be a primitive Hilbert modular form of parallel weight 2 and level N for the totally real field F, and let p be a rational prime coprime to $2N$. If f is ordinary at p and E is a CM extension of F of relative discriminant Δ prime to Np, we give an explicit construction of the p-adic Rankin–Selberg L-function $L_p(f_E, \cdot)$. When the sign of its functional equation is -1, we show, under the assumption that all primes $\wp \mid p$ are principal ideals of $\mathbb{O}_F$ that split in $\mathbb{O}_E$, that its central derivative is given by the p-adic height of a Heegner point on the abelian variety A associated with f.

This p-adic Gross–Zagier formula generalises the result obtained by Perrin-Riou when $F = \mathbb{Q}$ and (N, E) satisfies the so-called Heegner condition. We deduce applications to both the p-adic and the classical Birch and Swinnerton-Dyer conjectures for A.

A list of symbols can be found on page 1641.

MSC2010: primary 11G40; secondary 11F41, 11G18, 11F33, 11G50.

Keywords: Gross–Zagier, Heegner points, p-adic L-functions, Hilbert modular forms, p-adic heights, Birch and Swinnerton-Dyer conjecture.

Introduction

In this work, we generalise the p-adic analogue of the Gross–Zagier formula of [Perrin-Riou 1987] to totally real fields, in a generality similar to [Zhang 2001a; 2001b; 2004]. We describe here the main result and its applications.

The p-adic Rankin–Selberg L-function. Let f be a primitive (that is, a normalised new eigenform) Hilbert modular form of parallel weight 2, level N and trivial character for the totally real field F of degree g and discriminant D_F. Let p be a rational prime coprime to $2N$. Fix embeddings ι_∞ and ι_p of the algebraic closure $\overline{\mathbb{Q}}$ of F into $\mathbb{C}$ and $\overline{\mathbb{Q}}_p$, respectively; we let v denote the valuation on $\overline{\mathbb{Q}}_p$, normalised by $v(p) = 1$.

Let $E \subset \overline{\mathbb{Q}}$ be a CM (that is, quadratic and purely imaginary) extension of F of relative discriminant Δ coprime to $D_F N p$; let

$$\varepsilon = \varepsilon_{E/F} \colon F_{\boldsymbol{A}}^\times / F^\times \to \{\pm 1\}$$

be the associated Hecke character and $\mathfrak{N} = N_{E/F}$ be the relative norm. If

$$\mathscr{W} \colon E_{\boldsymbol{A}}^\times / E^\times \to \overline{\mathbb{Q}}^\times$$

is a finite-order Hecke character[1] of conductor $\mathfrak{f} = \mathfrak{f}(\mathscr{W})$ prime to $N\Delta$, the Rankin–Selberg L-function $L(f_E, \mathscr{W}, s)$ is the entire function defined for $\operatorname{Re} s > \frac{3}{2}$ by

$$L(f_E, \mathscr{W}, s) = L^{N\Delta(\mathscr{W})}(\varepsilon\mathscr{W}|_{F_{\boldsymbol{A}}^\times}, 2s-1) \sum_m \frac{a(f,m) r_{\mathscr{W}}(m)}{\boldsymbol{N}m^s},$$

where $\Delta(\mathscr{W}) = \Delta\mathfrak{N}(\mathfrak{f})$, $r_{\mathscr{W}}(m) = \sum_{\mathfrak{N}(\mathfrak{a})=m} \mathscr{W}(\mathfrak{a})$ (the sum running over all nonzero ideals of $\mathbb{O}_E$) and

$$L^{N\Delta(\mathscr{W})}(\varepsilon\mathscr{W}|_{\mathbb{O}_F}, s) = \sum_{(m, N\Delta(\mathscr{W}))=1} \varepsilon(m)\mathscr{W}(m)\boldsymbol{N}m^{-s}.$$

This L-function admits a p-adic analogue (Section 4). Let E'_∞ be the maximal abelian extension of E unramified outside p and $\mathscr{G}' = \operatorname{Gal}(E'_\infty/E)$.[2] (It has rank $1 + \delta + g$ over $\mathbb{Z}_p$, where δ is the Leopoldt defect of F.) For each prime $\wp$ of $\mathbb{O}_F$ dividing p, let

$$P_{\wp,f}(X) = X^2 - a(f,\wp)X + \boldsymbol{N}\wp$$

be the $\wp$-th Hecke polynomial of f, and assume that $v(\iota_p(a(f,\wp))) = 0$; in this case, f is said to be *ordinary*, and there is a unique root $\alpha_\wp \in \overline{\mathbb{Q}}$ of $P_{\wp,f}(X)$ such

[1] We will use the same notation throughout for a Hecke character, the associated ideal character and the associated Galois character.

[2] The reason for the notation is that later in the paper we will denote by E_∞ the maximal $\mathbb{Z}_p$-subextension of E'_∞.

that $\iota_p(\alpha_\wp)$ is a p-adic unit. Let $L \subset \overline{\mathbb{Q}}_p$ be the finite extension of $\mathbb{Q}_p$ generated by the Fourier coefficients $a(f,m)$ of f and by the $\alpha_\wp$ for $\wp \mid p$.

Theorem A. *There exists a unique element $L_p(f_E)$ of $\mathbb{O}_L[\![\mathcal{G}']\!] \otimes_{\mathbb{O}_L} L$ satisfying the interpolation property*

$$L_p(f_E)(\mathcal{W}) = \frac{\mathcal{W}(d_F^{(p)})\tau(\overline{\mathcal{W}})\boldsymbol{N}(\Delta(\mathcal{W}))^{1/2}V_p(f,\mathcal{W})\overline{\mathcal{W}}(\Delta)}{\alpha_{\mathfrak{f}}\Omega_f}L(f_E,\overline{\mathcal{W}},1)$$

for all finite-order characters $\mathcal{W}$ of $\mathcal{G}'$ of conductor $\mathfrak{f}(\mathcal{W})$. Here both sides are algebraic numbers,[3] *$\overline{\mathcal{W}} = \mathcal{W}^{-1}$ and*

$$\Omega_f = (8\pi^2)^g\langle f, f\rangle_N$$

with $\langle\cdot,\cdot\rangle_N$ the Petersson inner product (1.1.2); *$\tau(\overline{\mathcal{W}})$ is a normalised Gauss sum*; *$V_p(f,\mathcal{W})$ is a product of partial Euler factors at p*; *and finally $\alpha_{\mathfrak{f}} = \prod_{\wp\mid p}\alpha_\wp^{v_\wp(\mathfrak{N}(\mathfrak{f}))}$.*

This is essentially a special case of [Panchishkin 1988; Hida 1991]; we reprove it entirely here (see Section 4, especially Theorem 4.3.4) because the precise construction of $L_p(f_E)$ will be crucial for us. It is obtained, using a technique of Hida and Perrin-Riou, by applying a p-adic analogue of the functional "Petersson product with f" to a convolution Φ of Eisenstein and theta measures on $\mathcal{G}'$ valued in p-adic modular forms (so that $\Phi = \Phi(\mathcal{W})$ is an analogue of the kernel of the classical Rankin–Selberg convolution). The approach we follow is adelic; one novelty introduced here is that the theta measure is constructed via the Weil representation, which seems very natural and would generalise well to higher-rank cases.

On the other hand, Manin [1976], Dimitrov [2013] and others have constructed a p-adic L-function $L_p(f,\cdot) \in \mathbb{O}_L[\![\mathcal{G}_F]\!]$ as an analogue of the standard L-function $L(f,s)$, where $\mathcal{G}'_F$ is the Galois group of the maximal abelian extension of F unramified outside p; it is characterised by the interpolation property

$$L_p(f,\chi) = \chi(d_F^{(p)})\frac{\tau(\overline{\chi})\boldsymbol{N}(\mathfrak{f}(\chi))^{1/2}}{\alpha_{\mathfrak{f}(\chi)}}\frac{L(f,\overline{\chi},1)}{\Omega_f^+}$$

for all finite-order characters χ of conductor $\mathfrak{f}(\chi)$ that are trivial at infinity and ramified at all primes $v \mid p$. (Here Ω_f^+ is a suitable period (see Section 9.1) and $\tau(\chi)$ is again a normalised Gauss sum.) The corresponding formula for complex L-functions implies a factorisation (4.4.1)

$$L_p(f_E,\chi\circ\mathfrak{N}) = \chi(\Delta)^2\frac{\Omega_f^+\Omega_{f_\varepsilon}^+}{D_E^{-1/2}\Omega_f}L_p(f,\chi)L_p(f_\varepsilon,\chi),$$

where f_ε is the form with coefficients $a(f_\varepsilon,m) = \varepsilon(m)a(f,m)$ and $D_E = \boldsymbol{N}(\Delta)$.

[3] By a well-known theorem of [Shimura 1978]. They are compared via ι_p^{-1} and ι_∞^{-1}.

Heegner points on Shimura curves and the main theorem. Suppose that $\varepsilon(N) = (-1)^{g-1}$, where $g = [F : \mathbb{Q}]$. Then for each embedding $\tau\colon F \to \mathbb{C}$, there is a quaternion algebra $B(\tau)$ over F ramified exactly at the finite places $v \mid N$ for which $\varepsilon(N_v) = -1$ and the infinite places different from τ; it admits an embedding $\rho\colon E \hookrightarrow B(\tau)$, and we can consider an order R of $B(\tau)$ of discriminant N and containing $\rho(\mathbb{O}_E)$. These data define a *Shimura curve* X. It is an algebraic curve over F, whose complex points for any embedding $\tau\colon F \to \mathbb{C}$ are described by

$$X(\mathbb{C}_\tau) = B(\tau)^\times \setminus \mathfrak{H}^{\pm} \times \widehat{B}(\tau)^\times / \widehat{F}^\times \widehat{R}^\times \cup \{\text{cusps}\}.$$

It plays the role of the modular curve $X_0(N)$ in the works of Gross and Zagier [1986] and Perrin-Riou [1987], who consider the case $F = \mathbb{Q}$ and $\varepsilon(v) = 1$ for all $v \mid N$ (it is only in this case that the set of cusps is not empty).

The curve X is connected but not geometrically connected. Let $J(X)$ be its Albanese ($\cong$ Jacobian) variety; it is an abelian variety defined over F, geometrically isomorphic to the product of the Albanese varieties of the geometrically connected components of X. There is a natural map $\iota\colon X \to J(X) \otimes \mathbb{Q}$ given by $\iota(x) = [x] - [\xi]$, where $[\xi] \in \mathrm{Cl}(X) \otimes \mathbb{Q}$ is a canonical divisor class constructed in [Zhang 2001a] having degree 1 in every geometrically connected component of X; an integer multiple of ι gives a morphism $X \to J(X)$ defined over F.

As in the modular curve case, the curve X admits a finite collection of *Heegner points* defined over the Hilbert class field H of E and permuted simply transitively by $\mathrm{Gal}(H/E)$. They are the points represented by (x_0, t) for $t \in \widehat{E}^\times / E^\times \widehat{F}^\times \hat{\mathbb{O}}_E^\times$ when we use the complex description above and view $E \subset B$ via ρ. We let y be any such Heegner point, and let $[z]$ denote the class

$$[z] = u^{-1} \iota(\mathrm{Tr}_{H/E}\, y) \in J(X)(E) \otimes \mathbb{Q},$$

where $u = [\mathbb{O}_E^\times : \mathbb{O}_F^\times]$.

As a consequence of Jacquet–Langlands theory, the Hecke algebra on Hilbert modular forms of level N acts through its quaternionic quotient on $J(X)$. Let $z_f \in J(X)(E) \otimes \overline{\mathbb{Q}}$ be the f-component of $[z]$.

Heights and the formula. On any curve X over a number field E, there is a notion (Section 5.2) of p-adic height $\langle \cdot, \cdot \rangle_\ell$ attached to the auxiliary choices of splittings of the Hodge filtrations on $H^1_{\mathrm{dR}}(X/E_w)$ for $w \mid p$ and of a *p-adic logarithm* $\ell\colon E_{\boldsymbol{A}}^\times / E^\times \to \mathbb{Q}_p$. It is a symmetric bilinear pairing on the group of degree-0 divisors on X modulo rational equivalence, which we can view as a pairing on $J(X)(E)$. More generally, for any abelian variety A/E, there is defined a p-adic height pairing on $A(E) \times A^\vee(E)$. In our case, there is a canonical choice for the Hodge splittings on the f-components of the Albanese variety $J(X)$, given by the unit root subspaces, and we choose our height pairing on $J(X)$ to be compatible with this choice.

Under the assumption $\varepsilon(N) = (-1)^{g-1}$, the value $L_p(f_E, \mathbb{1})$ is zero by the complex functional equation and the interpolation property; in fact, we have more generally $L_p(f_E, \mathcal{W}) = 0$ for any anticyclotomic character $\mathcal{W}$ of $\mathcal{G}$. We can then consider its derivative in a cyclotomic direction. Let thus $\mathcal{W}$ be a Hecke character of E induced from a Hecke character of F taking values in $1 + p\mathbb{Z}_p \subset \mathbb{Z}_p^\times$, and assume $\mathcal{W}$ is ramified at all places dividing p. The derivative of $L_p(f_E)$ in the $\mathcal{W}$-direction is

$$L'_{p,\mathcal{W}}(f_E, \mathbb{1}) = \frac{d}{ds}\bigg|_{s=0} L_p(f_E)(\mathcal{W}^s).$$

Theorem B. *Assume that $\Delta_{E/F}$ is totally odd and that every prime $\wp \mid p$ is a principal ideal in $\mathcal{O}_F$ and splits in $\mathcal{O}_E$. Suppose that $\varepsilon_{E/F}(N) = (-1)^{g-1}$. Then $L_p(f_E, \mathbb{1}) = 0$ and*

$$L'_{p,\mathcal{W}}(f_E, \mathbb{1}) = D_F^{-2} \prod_{\wp \mid p} \left(1 - \frac{1}{\alpha_\wp}\right)^2 \left(1 - \frac{1}{\varepsilon(\wp)\alpha_\wp}\right)^2 \langle z_f, z_f \rangle_{\mathcal{W}}$$

where $\langle \cdot, \cdot \rangle_{\mathcal{W}}$ is the height pairing on $J(X)(E)$ associated with the logarithm $\ell = \frac{d}{ds}\big|_{s=0} \mathcal{W}^s$.

The hypothesis that the primes $\wp \mid p$ are principal is a technical assumption that intervenes only in Proposition 8.1.1.[4] The assumption that they split in E is essential to the argument, but like the assumption on $\Delta_{E/F}$, it can be removed a posteriori if the left-hand side of the formula below is nonzero — see Section 8.2.

Applications to the conjecture of Birch and Swinnerton-Dyer. It is conjectured that to any Hilbert modular newform f one can attach a simple abelian variety $A = A_f$ over F, characterised uniquely up to isogeny[5] by the equality of L-functions

$$L(A, s) = \prod_{\sigma : M_f \to \mathbb{C}} L(f^\sigma, s).$$

Here $M = M_f$ is the field generated by the Fourier coefficients of f; A has dimension $[M : \mathbb{Q}]$, and its endomorphism algebra contains M (we say that A is *of* $\mathrm{GL}_2(M)$*-type*; in fact since F is totally real, A is of *strict* GL_2-type; that is, its endomorphism algebra equals M — see, e.g., [Yuan et al. 2013, Lemma 3.3]). The conjecture is known to be true [Zhang 2001a, Theorem B] when

$$\text{either } [F : \mathbb{Q}] \text{ is odd or } v(N) \text{ is odd for some finite place } v \qquad (*)$$

(the assumptions of Theorem B above imply that one of these conditions holds); in this case, A is a quotient ϕ of $J(X)$ for a suitable Shimura curve X of the type

[4] A somewhat more sophisticated approach to our main result should remove this and other restrictions [Disegni 2015].

[5] Thanks to Faltings's isogeny theorem [1983].

described above. Vice versa, any abelian variety of GL_2-type (for some field M) over a totally real field F is conjectured to be associated with a Hilbert modular form f as above. This is known to be true for all elliptic curves A over F when F is $\mathbb{Q}$ or a real quadratic field and for all but possibly finitely many geometric isomorphism classes if F is a general totally real field (see [Le Hung 2014], whose result is somewhat stronger than this, and [Freitas et al. 2015]; the results build on the method of Wiles for $F = \mathbb{Q}$).

In view of known $\mathrm{Aut}(\mathbb{C}/\mathbb{Q})$-equivariance properties of automorphic L-functions and the above equality, the order of vanishing of $L(A, s)$ at $s = 1$ will be an integer multiple $r[M : \mathbb{Q}]$ of the dimension of A. We call r the *M-order of vanishing* of $L(A, s)$ or the *analytic M-rank* of A.

Conjecture (Birch and Swinnerton-Dyer). *Let A be an abelian variety of $\mathrm{GL}_2(M)$-type over a totally real field F of degree g.*

(1) *The M-order of vanishing of $L(A, s)$ at $s = 1$ is equal to the dimension of $A(F)_{\mathbb{Q}}$ as M-vector space.*

(2) *The Tate–Shafarevich group $Ш(A/F)$ is finite, and the leading term of $L(A, s)$ at $s = 1$ is given by*

$$\frac{L^*(A, 1)}{\Omega_A} = D_F^{-d/2} |Ш(A/F)| R_A \prod_{v \nmid \infty} c_v = \mathrm{BSD}(A),$$

where $d = \dim A = [M : \mathbb{Q}]$, the c_v are the Tamagawa numbers of A at finite places (*almost all equal to* 1),

$$\Omega_A = \prod_{\tau\colon F \to \mathbb{R}} \int_{A(\mathbb{R}_\tau)} |\omega_A|_\tau$$

for a Néron differential[6] *ω_A and*

$$R_A = \frac{\det\langle x_i, y_j\rangle}{[A(F) : \sum \mathbb{Z} x_i][A^\vee(F) : \sum \mathbb{Z} y_j]}$$

is the regulator of the Néron–Tate height paring on $A(F) \times A^\vee(F)$, defined using any subsets $\{x_i\}$ and $\{y_j\}$ of $A(F)$ and $A^\vee(F)$ inducing bases of $A(F)_{\mathbb{Q}}$ and $A^\vee(F)_{\mathbb{Q}}$.

By the automorphic description of $L(A, s)$ and [Shimura 1978], we know that $L(A, s)/\prod_{\sigma\colon M_f \to \mathbb{C}} \Omega_{f^\sigma}^+$ is an algebraic number. Comparison with the Birch and Swinnerton-Dyer conjecture suggests the following conjecture:

[6] When it exists, which is only guaranteed if $F = \mathbb{Q}$. Otherwise, we take for ω_A any generator of $H^0(A, \Omega^d_{A/F})$ and to define Ω_A we divide by the product of the indices $[H^0(\mathcal{A}_v, \Omega^d_{\mathcal{A}_v/\mathcal{O}_{F,v}}) : \mathcal{O}_{F,v}\widetilde{\omega_A}]$ of (the extension of) ω_A in the space of top differentials on the local Néron models $\mathcal{A}_v/\mathcal{O}_{F,v}$ of A.

Conjecture (period conjecture). *We have*

$$\Omega_A \sim \prod_{\sigma\,:\,M_f\to\mathbb{C}} \Omega^+_{f^\sigma} \quad \text{in } \mathbb{C}^\times/\overline{\mathbb{Q}}^\times.$$

The conjecture is known for $F=\mathbb{Q}$ [Shimura 1981] or when A has complex multiplication (over $\overline{\mathbb{Q}}$) [Blasius 1986]; see Section 9 below for a more precise conjecture and some further evidence and motivation.

Assuming the conjecture, we can define a p-adic L-function $L_p(A)$ for A by

$$L_p(A) = \frac{\prod_\sigma \Omega^+_{f^\sigma}}{\Omega_A} \prod_{\sigma\,:\,M_f\to\mathbb{C}} L_p(f^\sigma)$$

for any prime p such that A has good ordinary reduction at all primes above p.

Then, fixing a ramified Hecke character $\nu\colon \mathcal{G}'_F \to 1+p\mathbb{Z}_p \subset \mathbb{Z}_p^\times$ that we omit from the notation, one can formulate a p-adic version of the Birch and Swinnerton-Dyer conjecture similarly as above for $L_p(A,\nu^s)$:[7] the conjectural formula reads

$$\prod_{\wp\mid p}(1-\alpha_\wp^{-1})^{-2} L_p^*(A,\mathbb{1}) = \mathrm{BSD}_p(A)$$

where $\mathrm{BSD}_p(A)$ differs from $\mathrm{BSD}(A)$ only in the regulator term, which is now the regulator of the p-adic height pairing on $A(F)\times A^\vee(F)$ associated with the p-adic logarithm ℓ deduced from ν as in Theorem B. One can also formulate a main conjecture of Iwasawa theory for $L_p(A)$ [Schneider 1985].

Then, just as in [Perrin-Riou 1987], we can deduce the following arithmetic application of Theorem B:

Theorem C. *Assume the period conjecture holds for the abelian variety $A=A_f$ and that A satisfies $(*)$. For an ordinary prime $p>2$ decomposing into principal prime ideals in $\mathcal{O}_F$:*

(1) *The following are equivalent*:
   (a) *The p-adic L-function $L_p(A,\nu^s)$ has M_f-order of vanishing $r\le 1$ at the central point.*
   (b) *The complex L-function $L(A,s)$ has M_f-order of vanishing $r\le 1$ at the central point, and the p-adic height pairing associated with ν is nonvanishing on $A(F)$.*

(2) *If either of the above assumptions holds, the rank parts of the classical and the p-adic Birch and Swinnerton-Dyer conjecture are true for A and the Tate–Shafarevich group of A is finite.*

[7] Here $s\in\mathbb{Z}_p$ and the central point is $s=0$, corresponding to $\nu^0=\mathbb{1}$.

(3) *If moreover the cyclotomic Iwasawa main conjecture is true for A, then the classical and the p-adic Birch and Swinnerton-Dyer formulas for A are true up to a p-adic unit.*

Proof. In part (1), the statement follows trivially from the construction of $L_p(A)$ if $r = 0$; if $r = 1$, both conditions are equivalent to the assertion that, for a suitable CM extension E, the Heegner point $z_f = z_{f,E}$ is nontorsion: this is obvious from our main theorem in case (a); in case (b), by [Zhang 2001a; 2001b] (generalising [Gross and Zagier 1986; Kolyvagin 1988; Kolyvagin and Logachëv 1991]), the Heegner point

$$P = \sum_\sigma \mathrm{Tr}_{E/F}\, \phi(z_{f^\sigma,E}) \in A(F) \otimes \mathbb{Q}$$

(with $\phi\colon J(X) \to A$) generates $A(F) \otimes \mathbb{Q}$ as M_f-vector space so that the p-adic height pairing on $A(F)$ is nonvanishing if and only if it is nonzero at z_f. Part (2) then follows from (1) and [Zhang 2001a; 2001b].

Schneider [1985] proves an "arithmetic" version of the p-adic Birch–Swinnerton-Dyer formula for (the Iwasawa L-function associated with) A, which under the assumption of (3) can be compared to the analytic p-adic formula as explained in [Perrin-Riou 1987] to deduce the p-adic Birch and Swinnerton-Dyer formula up to a p-adic unit. In the analytic rank-0 case, the classical Birch and Swinnerton-Dyer formula follows immediately. In the case of analytic rank 1, recall that the main result of [Zhang 2001a; 2004] is, in our normalisation, the formula

$$\frac{L'(f_E, 1)}{\Omega_f} = \frac{1}{D_F^2 D_E^{1/2}} \langle z_f, z_f \rangle =: D_E^{-1/2}\, \mathrm{GZ}(f_E)$$

(where $\langle \cdot, \cdot \rangle$ denotes the Néron–Tate height), whereas we introduce the notation $\mathrm{GZ}_p(f_E)$ to write our formula (for any fixed ramified cyclotomic character $\mathcal{W} = \nu \circ \mathfrak{N}$) as

$$L_p'(f_E, \mathbb{1}) = \prod_{\wp \mid p} \left(1 - \frac{1}{\alpha_\wp}\right)^2 \left(1 - \frac{1}{\varepsilon(\wp)\alpha_\wp}\right)^2 \mathrm{GZ}_p(f_E).$$

Then, after choosing E suitably so that $L(f_\varepsilon, 1) \neq 0$ (which can be done by [Bump et al. 1990; Waldspurger 1985]), we can argue as in [Perrin-Riou 1987] to compare the p-adic and the complex Birch and Swinnerton-Dyer formulas via the corresponding Gross–Zagier formulas to get the result. Namely, we have

$$\begin{aligned} \frac{L^*(A, 1)}{\Omega_A\, \mathrm{BSD}(A)} &= \frac{\prod_\sigma \Omega^+_{f^\sigma}}{\Omega_A} \frac{1}{\mathrm{BSD}(A)} \prod_\sigma \frac{L'(f_E^\sigma, 1)}{\Omega_{f^\sigma}} \frac{\Omega_{f^\sigma}}{\Omega^+_{f^\sigma}\Omega^+_{f_\varepsilon^\sigma}} \frac{\Omega^+_{f_\varepsilon^\sigma}}{L(f_\varepsilon^\sigma, 1)} \\ &= \frac{\prod_\sigma \Omega^+_{f^\sigma}}{\Omega_A} \frac{\prod_\sigma \mathrm{GZ}(f_E^\sigma)}{\mathrm{BSD}(A)} \prod_\sigma \frac{D_E^{-1/2}\Omega_{f^\sigma}}{\Omega^+_{f^\sigma}\Omega^+_{f_\varepsilon^\sigma}} \frac{\Omega^+_{f_\varepsilon^\sigma}}{L(f_\varepsilon^\sigma, 1)} \end{aligned}$$

by the complex Gross–Zagier formula and the factorisation of $L(f_E, s)$. Similarly,

$$\prod_{\wp|p}(1-\alpha_\wp^{-1})^{-2}\frac{L_p^*(A,1)}{\mathrm{BSD}_p(A)} = \frac{\prod_\sigma \Omega^+_{f^\sigma}}{\Omega_A}\frac{\prod_\sigma \mathrm{GZ}_p(f_E^\sigma)}{\mathrm{BSD}_p(A)}\prod_\sigma \frac{D_E^{-1/2}\Omega_{f^\sigma}}{\Omega^+_{f^\sigma}\Omega^+_{f_\varepsilon^\sigma}}\frac{\Omega^+_{f_\varepsilon^\sigma}}{L(f_\varepsilon^\sigma,1)}$$

by the p-adic Gross–Zagier formula, the factorisation of $L_p(f_E)$ and the interpolation property of $L_p(f_\varepsilon)$. Since we are assuming to know that the left-hand side of the last formula is a p-adic unit, the result follows from observing the equality

$$\frac{\prod_\sigma \mathrm{GZ}(f_E^\sigma)}{\mathrm{BSD}(A)} = \frac{\prod_\sigma \mathrm{GZ}_p(f_E^\sigma)}{\mathrm{BSD}_p(A)}$$

of rational numbers.[8] □

Alternative approaches to the Birch and Swinnerton-Dyer formula in rank 1 have recently been proposed, at least for the case $F = \mathbb{Q}$, by Wei Zhang [2014] and Xin Wan.

Discussion of the assumptions. The conjecture on periods could be dispensed of if one were willing to work with a "wrong" p-adic L-function for A (namely, one without the period ratio appearing in the definition above). Then at least the rank part of the p-adic Birch and Swinnerton-Dyer conjecture makes sense and parts (1) and (2) of Theorem C hold. The nonvanishing of the p-adic height pairing is only known for CM elliptic curves [Bertrand 1984]. The Iwasawa main conjecture is known in most cases for ordinary elliptic curves over $\mathbb{Q}$ thanks to the work of Rubin, Kato and Skinner and Urban [2014]. For Hilbert modular forms, one divisibility in the CM case is proved by [Hsieh 2014]; results on the general case are obtained by [Wan 2013]. We can then record the following unconditional result, whose assumptions are inherited from [Hsieh 2014]:

Theorem D. *Let A/F be an elliptic curve with complex multiplication by the ring of integers $\mathbb{O}_K$ of an imaginary quadratic field K. Let $K' = FK$, and let $h^-_{K'} = h_{K'}/h_K$ be the relative class number of K'/F. Let $p \nmid 6h^-_{K'}D_F$ be a prime such that, for all primes $\wp \mid p$, $\wp$ is principal and A has good ordinary reduction at $\wp$. Suppose that A satisfies $(*)$ and that $\mathrm{ord}_{s=1}L(A,s) \le 1$. Then*

$$v_p\left(\frac{L^*(A,1)}{R_A\Omega_A}\right) \le v_p\left(|Ш(A/F)|\prod_{v\nmid\infty} c_v\right).$$

[8] The rationality of the ratios follows from the fact that the z_{f^σ} essentially belong to $J(X)(F)$ — that is, they belong to the $+1$-eigenspace for the action of $\mathrm{Gal}(E/F)$ on $J(X)(E)\otimes\bar{\mathbb{Q}}$ — and that, in this sense, their images $\phi(z_{f^\sigma})$ form a $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-invariant basis of $A(F)\otimes\bar{\mathbb{Q}}$, orthogonal for the height pairing.

Results toward the divisibility in the opposite direction can be obtained from the method of Kolyvagin; see [Kolyvagin 1991] (for $F = \mathbb{Q}$) and [Howard 2004] (for general F but excluding the CM case).

Plan of the proof. The proof of the main formula follows the strategy of [Perrin-Riou 1987]. It is enough (see Section 8) to study the case where $\mathcal{W}$ is cyclotomic ($\mathcal{W} = \mathcal{W}^c$) since both sides of the formula are zero when $\mathcal{W}$ is anticyclotomic ($\mathcal{W}\mathcal{W}^c = \mathbb{1}$).

In the first part of this paper, we construct the measure Φ on $\mathcal{G}$ valued in p-adic modular forms such that $L_p(f_E)(\mathcal{W})$ essentially equals $l_{f_\alpha}(\Phi(\mathcal{W}))$, where l_{f_α} is a p-adic analogue of the functional "Petersson product with f" on p-adic modular forms. This allows us to write

$$L'_{p,\mathcal{W}}(f_E, \mathbb{1}) \doteq l_{f_\alpha}(\Phi'_{\mathcal{W}}),$$

where $\doteq$ denotes equality up to suitable nonzero factors and $\Phi'_{\mathcal{W}} = \frac{d}{ds}\big|_{s=0}\Phi(\mathcal{W}^s)$ is a p-adic Hilbert modular form.

On the other hand, there is a modular form Ψ with Fourier coefficients given by $\langle z, T(m)z\rangle_{\mathcal{W}}$ so that $l_{f_\alpha}(\Psi) \doteq \langle z_f, z_f\rangle_{\mathcal{W}}$. It can be essentially written as a sum of modular forms $\Psi_{\mathrm{fin}} + \Psi_p$, where Ψ_{fin} encodes the local contributions to the height from places not dividing p and $\Psi_p = \sum \Psi_{\wp}$, the contribution from the places $\wp$ above p. Then we can show by explicit computation that the Fourier coefficients of Φ' are equal to the Fourier coefficients of Ψ_{fin} up to the action of suitable Hecke operators at p. The desired formula then follows once we show that $l_{f_\alpha}(\Psi_p)$ vanishes. To prove this, we examine the effect of the operator $U_{\wp}$ on $\Psi_{\wp}$ and find that, in a suitable quotient space, the ordinary projection of $\Psi_{\wp}$ is zero. The study of $\Psi_{\wp}$ follows the methods of Perrin-Riou.

One difficulty in the approach just outlined is that compared to the case of modular curves there are no cusps available so that in this case the divisors z and $T(m)z$ have intersecting supports and the decomposition of the height pairing into a sum of local pairings is not available. Our solution to this problem, which is inspired by [Zhang 2001a], is to make use of p-adic Arakelov theory as developed by [Besser 2005] (see Section 5.3) and work consistently in a suitable quotiented space of Fourier coefficients.

Perspective. The original Gross–Zagier formula has undergone an impressive transformation since its first appearance in 1986, culminating in the recent book of Yuan, Zhang and Zhang [Yuan et al. 2013]. Obviously, this work is only a first step in catching up on the p-adic side.[9] The latter has also seen important developments, with generalisations to the nonordinary case, by [Kobayashi 2013] and, to the case

[9]For a more accomplished attempt, see [Disegni 2015].

of higher weights, by [Nekovář 1995; Shnidman 2014]. It would certainly be of interest to generalise those results to the setting of the present work.[10]

Results similar to those presented here were recently obtained in the thesis of Li Ma (Paris 6).

Part I. p-adic L-function and measures

This part is dedicated to the construction of the measure giving the p-adic Rankin–Selberg L-function $L_p(f_E)$ and to the computation of its Fourier coefficients.

1. p-adic modular forms

1.1. ***Hilbert modular forms.*** Let us define compact subgroups of $\boldsymbol{GL}_2(\boldsymbol{A}^\infty)$:

- $K_0(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \boldsymbol{GL}_2(\hat{\mathbb{O}}_F) \;\middle|\; c \equiv 0 \bmod N\hat{\mathbb{O}}_F \right\}$ if N is an ideal of $\mathbb{O}_F$,
- $K_1(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in K_0(N) \;\middle|\; a \equiv 1 \bmod N\hat{\mathbb{O}}_F \right\}$.

Let k be an element of $\mathbb{Z}_{\geq 0}^{\mathrm{Hom}(F,\bar{\mathbb{Q}})}$ and ψ be a character of $F_{\boldsymbol{A}}^\times / F^\times$ of conductor dividing N satisfying $\psi_v(-1) = (-1)^{k_v}$ for $v \mid \infty$. A *Hilbert modular form* of weight k, level $K_1(N)$ and character ψ is a smooth function

$$f\colon\ \boldsymbol{GL}_2(F) \setminus \boldsymbol{GL}_2(\boldsymbol{A}_F) \to \mathbb{C}$$

of *moderate growth*[11] satisfying[12]

$$f\left(\begin{pmatrix} z & \\ & z \end{pmatrix} g \begin{pmatrix} a & b \\ c & d \end{pmatrix} r(\theta)\right) = \psi(z)\psi_N(a)\boldsymbol{e}_\infty(k\cdot\theta) f(g)$$

for each $z \in F_{\boldsymbol{A}}^\times$, $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in K_0(N)$ and $\theta = (\theta_v)_{v|\infty} \in F_\infty$, with $r(\theta) = \prod_{v|\infty} r(\theta_v)$ and

$$r(\theta_v) = \begin{pmatrix} \cos\theta_v & \sin\theta_v \\ -\sin\theta_v & \cos\theta_v \end{pmatrix} \in \boldsymbol{SO}_2(F_v).$$

If k is constant, we say that f has parallel weight; in this work, we will be almost exclusively concerned with forms of parallel weight, and we will assume that we are in this situation for the rest of this section.

[10] Results in the nonordinary case were presented in a preliminary version of this paper, assuming a suitable construction of p-adic L-functions generalising [Urban 2014]; I hope to present them in revised form in a future work.

[11] That is, for every g, the function $\boldsymbol{A}^\times \ni y \mapsto f\left(\left(\begin{smallmatrix} y & \\ & 1 \end{smallmatrix}\right) g\right)$ grows at most polynomially in $|y|$ as $|y| \to \infty$.

[12] Recall the notation $\psi_N = \prod_{v|N} \psi_v$.

We call f holomorphic if, for each $x^\infty \in \boldsymbol{A}^\infty$ and $y^\infty \in F_{\boldsymbol{A}^\infty}^\times$, the function on $\mathfrak{H}^{\mathrm{Hom}(F,\bar{\mathbb{Q}})} = \{x_\infty + iy_\infty \in F \otimes \mathbb{C} \mid y_\infty > 0\}$

$$x_\infty + iy_\infty \mapsto \psi^{-1}(y)|y|^{-k/2} f\begin{pmatrix} y & x \\ & 1 \end{pmatrix}$$

is holomorphic; in this case, such function determines f.

Petersson inner product. We define a Haar measure dg on $Z(\boldsymbol{A}_F) \setminus \boldsymbol{GL}_2(\boldsymbol{A}_F)$ (where $Z \cong \boldsymbol{G}_m$ denotes the centre of $\boldsymbol{GL}_2$) as follows. Recall the Iwasawa decomposition

$$\boldsymbol{GL}_2(\boldsymbol{A}_F) = B(\boldsymbol{A}_F)K_0(1)K_\infty \tag{1.1.1}$$

where $K_\infty = \prod_{v|\infty} \boldsymbol{SO}_2(F_v)$. Let $dk = \bigotimes_v dk_v$ be the Haar measure on $K = K_0(1)K_\infty$ with volume 1 on each component. Let $dx = \bigotimes_v dx_v$ be the Haar measure such that dx_v is the usual Lebesgue measure on $\mathbb{R}$ if $v \mid \infty$ and $\mathbb{O}_{F,v}$ has volume 1 if $v \nmid \infty$. Finally let $d^\times x = \bigotimes_v d^\times x_v$ on $F_{\boldsymbol{A}}^\times$ be the product of the measures given by $d^\times x_v = |dx_v/x_v|$ if $v \mid \infty$ and by the condition that $\mathbb{O}_{F,v}^\times$ has volume 1 if $v \mid \infty$. Then we can use the Iwasawa decomposition $g = \left(\begin{smallmatrix} z & \\ & z \end{smallmatrix}\right)\left(\begin{smallmatrix} y & x \\ & 1 \end{smallmatrix}\right)k$ to define

$$\int_{Z(\boldsymbol{A})\backslash \boldsymbol{GL}_2(\boldsymbol{A})} f(g)\,dg = \int_{F_{\boldsymbol{A}}^\times} \int_{\boldsymbol{A}} \int_K f\left(\begin{pmatrix} y & x \\ & 1 \end{pmatrix} k\right) dk\,dx\,\frac{d^\times y}{|y|}.$$

The Petersson inner product of two forms f_1 and f_2 on $\mathrm{GL}_2(F)\setminus \mathrm{GL}_2(\boldsymbol{A})$ such that $f_1 f_2$ is invariant under $Z(\boldsymbol{A})$ is defined by

$$\langle f_1, f_2\rangle_{\mathrm{Pet}} = \int_{Z(\boldsymbol{A})\backslash \boldsymbol{GL}_2(\boldsymbol{A})} \overline{f_1(g)} f_2(g)\,dg$$

whenever this converges (this is ensured if either f_1 or f_2 is a cuspform as defined below). It will be convenient to introduce a level-specific inner product on forms f and g of level N:

$$\langle f, g\rangle_N = \frac{\langle f, g\rangle_{\mathrm{Pet}}}{\mu(N)} \tag{1.1.2}$$

where $\mu(N)$ is the measure of $K_0(N)$.

1.2. ***Fourier expansion.*** Let f be a (not necessarily holomorphic) Hilbert modular form. We can expand it as

$$f(g) = C_f(g) + \sum_{\alpha \in F^\times} W_f\left(\begin{pmatrix} \alpha & \\ & 1 \end{pmatrix} g\right)$$

where

$$C_f(g) = D_F^{-1/2} \int_{\mathbf{A}/F} f\left(\begin{pmatrix} 1 & x \\ & 1 \end{pmatrix} g\right) dx,$$
$$W_f(g) = D_F^{-1/2} \int_{\mathbf{A}/F} f\left(\begin{pmatrix} 1 & x \\ & 1 \end{pmatrix} g\right) \boldsymbol{e}(-x)\, dx$$

are called the *constant term* and the *Whittaker function* of f, respectively. The form f is called *cuspidal* if its constant term C_f is identically zero. The functions of y obtained by restricting the constant term and the Whittaker function to the elements $\left(\begin{smallmatrix} y & \\ & 1 \end{smallmatrix}\right)$ are called the *Whittaker coefficients* of f. When f is holomorphic, they vanish unless $y_\infty > 0$ and otherwise have the simple form

$$C_f\begin{pmatrix} y & x \\ & 1 \end{pmatrix} = \tilde{a}^0(f, y) = \psi(y)|y|^{k/2} a(f, 0),$$
$$W_f\begin{pmatrix} y & x \\ & 1 \end{pmatrix} = \tilde{a}(f, y)\boldsymbol{e}_\infty(iy_\infty)\boldsymbol{e}(x) = \psi(y)|y|^{k/2} a(f, y^\infty d_F)\boldsymbol{e}_\infty(iy_\infty)\boldsymbol{e}(x)$$

for functions $\tilde{a}^0(f, y)$ and $\tilde{a}(f, y)$ of $y \in F_{\mathbf{A}}^{\infty,\times}$, which we call the *Whittaker–Fourier coefficients* of f, and a function $a(f, m)$ of the fractional ideals m of F that vanishes on nonintegral ideals whose values are called the *Fourier coefficients* of f.

For any $\mathbb{Z}$-submodule A of $\mathbb{C}$, we denote by $M_k(K_1(N), \psi, A)$ the space of holomorphic Hilbert modular forms with Fourier coefficients in A of weight k, level $K_1(N)$ and character ψ and by $S_k(K_1(N), \psi, A)$ its subspace of cuspidal forms. When the character ψ is trivial, we denote those spaces simply by $M_k(K_0(N), A)$ and $S_k(K_0(N), A)$, whereas linear combinations of forms of level $K_1(N)$ with different characters form the space $M_k(K_1(N), A)$. The notion of Whittaker–Fourier coefficients extends by linearity to the spaces $M_k(K_1(N), \mathbb{C})$.

We can allow more general coefficients: if A is a $\mathbb{Z}[1/N]$-algebra, we define $S_k(K_0(N), A) = S_k(K_0(N), \mathbb{Z}[1/N]) \otimes A$; this is well-defined thanks to the q-expansion principle [Andreatta and Goren 2005].

1.3. ***p-adic modular forms.*** Let N and P be coprime ideals of $\mathbb{O}_F$ and ψ a character of conductor dividing N. If f is a holomorphic form of weight k, level $K_1(NP)$ and prime-to-P character ψ (that is, f is a linear combination of forms of level NP and character $\psi\psi'$ with ψ' a character of conductor dividing P), we associate to it the *formal q-expansion coefficients*

$$a_p(f, y^\infty) = \psi^{-1}(y)|y|^{-k/2}\tilde{a}(f, y).$$

If ψ' is trivial, we set $a_p(f, m) = a_p(f, y^\infty)$ if m is the ideal $m = y^\infty d_F$.

Let N be an ideal prime to p and ψ a character of level dividing N. Consider the space of classical modular forms $M_k(K_1(Np^\infty), \overline{\mathbb{Q}})$ with character whose prime-to-p part is equal to ψ, and endow it with the norm given by the maximum of the p-adic absolute values (for the chosen embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$) of the Fourier coefficients. Its completion

$$\boldsymbol{M}_k(K_1(N), \psi, \mathbb{C}_p)$$

of this space is a p-adic Banach space called the space of *p-adic modular forms* of weight k, *tame level* $K_1(N)$ and tame character ψ. We view $M_k(K_1(Np^r, \psi\psi', \mathscr{A})$ (for any character ψ' of conductor divisible only by primes above p) as a subset of $\boldsymbol{M}_k(K_1(N), \psi, \mathscr{A})$ via the q-expansion map.

If $\mathscr{A}$ is a complete $\mathbb{Z}_p$-submodule of $\mathbb{C}_p$, we also write $\boldsymbol{M}_k(K_1(N), \psi, \mathscr{A})$ with obvious meaning and $\boldsymbol{S}_k(K_1(N), \psi, \mathscr{A})$ or $\boldsymbol{S}_k(K_0(N), \mathscr{A})$ (in the case of trivial tame character) for cuspforms; when $k = 2$, we simply write

$$\boldsymbol{S}_N(\mathscr{A}) = \boldsymbol{S}_2(K_0(N), \mathscr{A})$$

or just $\boldsymbol{S}_N$ if $\mathscr{A} = \mathbb{Q}_p$ or $\mathscr{A} = \mathbb{C}_p$ (as understood from context).

1.4. ***Operators acting on modular forms.*** There is a natural action of the group algebra $\mathbb{Q}[\boldsymbol{GL}_2(\boldsymbol{A}^\infty)]$ on modular forms induced by right translation. Here we describe several interesting operators arising from this action.

Let m be an ideal of $\mathbb{O}_F$ and $\pi_m \in F^\times_{\boldsymbol{A}^\infty}$ a generator of $m\hat{\mathbb{O}}_F$ that is trivial at places not dividing m.

The operator $[m]\colon M_k(K_1(N), \psi) \to M_k(K_1(Nm), \psi)$ is defined by

$$[m]f(g) = \boldsymbol{N}(m)^{-k/2} f\left(g \begin{pmatrix} 1 & \\ & \pi_m \end{pmatrix}\right). \tag{1.4.1}$$

It acts on Fourier coefficients by

$$a([m]f, n) = a(f, m^{-1}n).$$

If χ is a Hecke character of F, we denote by $f|\chi$ the form with coefficients

$$a(f|\chi, n) = \chi(n)a(f, n).$$

For any double coset decomposition

$$K_1(N) \begin{pmatrix} \pi_m & \\ & 1 \end{pmatrix} K_1(N) = \coprod_i \gamma_i K_1(N),$$

the *Hecke operator* $T(m)$ is defined by the following level-preserving action on forms f in $M_k(K_1(N))$:

$$T(m)f(g) = \boldsymbol{N}(m)^{k/2-1} \sum_i f(g\gamma_i).$$

For m prime to N, its effect on Fourier coefficients of forms with trivial character is described by

$$a(T(m)f, n) = \sum_{d|(m,n)} \boldsymbol{N}(d)^{k/2-1} a(f, mn/d^2).$$

When m divides N, we can pick as double coset representatives the matrices

$$\gamma_i = \begin{pmatrix} \pi_m & c_i \\ & 1 \end{pmatrix}$$

for $\{c_i\} \subset \hat{\mathbb{O}}_F$ a set of representatives for $\mathbb{O}_F/m\mathbb{O}_F$. Then the operator $T(m)$ is more commonly denoted $U(m)$, and we will usually follow this practice. It acts on Fourier coefficients of forms with trivial character by

$$a(U(m)f, n) = \boldsymbol{N}(m)^{k/2-1} a(f, mn).$$

Let $\boldsymbol{T}_N$ be the (commutative) subring of End $S_2(K_0(N), \mathbb{Z})$ generated by the $T(m)$ for m prime to N. A form f that is an eigenfunction of all the operators in $\boldsymbol{T}_N$ is called a Hecke *eigenform*. It is called a *primitive* form if moreover it is normalised by $a(f, 1) = 1$ and it is a newform (see Section 1.5 below for the definition) of some level dividing N.

As usual [Perrin-Riou 1987, Lemme 1.10], we will need the following well-known lemma to ensure the modularity of certain generating functions:

Lemma 1.4.1. *Let A be a $\mathbb{Q}$-algebra. For each linear form*

$$a : \boldsymbol{T}_N \to A,$$

there is a unique modular form in $\bigoplus_{N'|N} S_k^{\mathrm{new}}(K_0(N'), A)$ whose Fourier coefficients are given by $a(T(m))$ for all m prime to N.

Proof. In [Zhang 2001a, Corollary 3.18], the result is stated and proved when $A = \mathbb{C}$ as a consequence of the existence of a pairing $(T, f) \mapsto a_1(Tf)$ between $\boldsymbol{T}_N$ and the space of modular forms of interest. But this pairing is defined over $\mathbb{Q}$; hence, the result is true for $A = \mathbb{Q}$ and by extending scalars for any $\mathbb{Q}$-algebra A. □

Atkin–Lehner theory. For any nonzero ideal M of $\mathbb{O}_F$, let $W_M \in \boldsymbol{GL}_2(\boldsymbol{A}^\infty)$ be a matrix with components

$$W_{M,v} = \begin{pmatrix} & 1 \\ -\pi_v^{v(M)} & \end{pmatrix} \quad \text{if } v \mid M, \qquad W_{M,v} = \begin{pmatrix} 1 & \\ & 1 \end{pmatrix} \quad \text{if } v \nmid M \tag{1.4.2}$$

where π_v is a uniformiser at v. We denote by the same name W_M the operator acting on modular forms of level N and trivial character by

$$W_M f(g) = f(gW_M);$$

it is self-adjoint for the Petersson inner product, and when M is prime to N, it is proportional to the operator $[M]$ of (1.4.1). On the other hand when M equals N, or more generally M divides N and is coprime to NM^{-1}, the operator W_M is an involution and its action is particularly interesting. In this case, extending the definition to forms of level $K_1(N)$ and character[13] $\psi = \psi_{(M)}\psi_{(NM^{-1})}$ with $\psi_{(C)}$ of conductor dividing C, we have

$$W_M f(g) = \psi_{(M)}^{-1}(\det g)\psi_{(M)}^{-1}(\pi_M) f(gW_M) \tag{1.4.3}$$

where π_M is the idele with nontrivial components only at $v \mid M$ and given there by $\pi_v^{v(M)}$. It is easy to check that this definition is independent of the choice of uniformisers. The effect of the W_M-action on newforms is described by Atkin–Lehner theory; we summarise it here (in the case $M = N$), referring to [Casselman 1973] for the details.

Let π be an irreducible infinite-dimensional automorphic representation of $\boldsymbol{GL}_2(\boldsymbol{A}_F)$ of central character ψ. Up to scaling, there is a unique *newform* f in the space of π. It is characterised by either equivalent property: it is fixed by a subgroup $K_1(N)$ with N minimal among the N' for which $\pi^{K_1(N')} \neq 0$ or its Mellin transform is (a multiple of) the L-function $L(\pi, s)$ of π. In the case of a holomorphic cuspform, this is equivalent to requiring that it belongs to the space of newforms defined in Section 1.5 below. There is a functional equation relating the L-function $L(s, \pi)$ of π and the L-function $L(1-s, \tilde{\pi})$ of the contragredient representation; as $\tilde{\pi} \cong \psi^{-1} \cdot \bar{\pi}$, it translates into the following description of the action of W_N on newforms. Suppose that the eigenform $f \in S_k(K_1(N), \psi)$ is a newform in the representation π it generates; then we have

$$W_N f(g) = (-i)^{[F:\mathbb{Q}]k}\tau(f) f^{\rho}(g) \tag{1.4.4}$$

where f^{ρ} is the form with coefficients

$$a(f^{\rho}, m) = \overline{a(f, m)} \tag{1.4.5}$$

and $\tau(f) = \tau(\pi)$ is an algebraic number of complex absolute value 1.

Trace of a modular form. The *trace* of a modular form f of level ND and trivial character is the form of level N

$$\mathrm{Tr}_{ND/N}(f)(g) = \sum_{\gamma \in K_0(N)/K_0(ND)} f(g\gamma).$$

[13]Notice that a decomposition of ψ as described is only unique up to class group characters (that is, Hecke characters of level 1). We will only be using the operator W_M for M a proper divisor of N in a case in which a decomposition is naturally given.

It is the adjoint of inclusion of forms of level N for the rescaled Petersson product:

$$\langle f, \mathrm{Tr}_{ND/N}\, g\rangle_N = \langle f, g\rangle_{ND}$$

if f has level N and g has level D.

Suppose that D is squarefree and prime to N, in which case we can write $\mathrm{Tr}_D = \mathrm{Tr}_{ND/N}$ without risk of ambiguity. A set of coset representatives for $K_0(N)/K_0(ND)$ is given by elements $\gamma_{j,\delta}$ for $\delta \mid D$, $j \in \mathbb{O}_{F,v}/\delta\mathbb{O}_{F,v}$, having components

$$\gamma_{j,\delta,v} = \begin{pmatrix} 1 & j \\ & 1 \end{pmatrix}\begin{pmatrix} & 1 \\ -1 & \end{pmatrix} = \frac{1}{\pi_v}\begin{pmatrix} \pi_v & j \\ & 1 \end{pmatrix}\begin{pmatrix} & 1 \\ -\pi_v & \end{pmatrix}$$

at places $v \mid \delta$ and $\gamma_{j,\delta,v} = 1$ everywhere else. From the second decomposition given just above, if f has weight 2, we obtain

$$a(\mathrm{Tr}_D(f), m) = \sum_{\delta|D} a(U(\delta)f^{(\delta)}, m) = \sum_{\delta|D} a(f^{\delta)}, m\delta) \tag{1.4.6}$$

where $f^{(\delta)}(g) = f(gW_\delta)$ with W_δ as in (1.4.2).

Remark 1.4.2. If D is prime to p, the various trace operators Tr_{NDp^r/Np^r} extend to a continuous operator $\mathrm{Tr}_{ND/N}$ on p-adic modular forms of tame level ND. Similarly, the operators $[m]$, $T(m)$ and W_m for m prime to Np extend to continuous operators on p-adic modular forms of tame level N.

Ordinary projector. Let L be a complete subfield of $\mathbb{C}_p$. Following Hida (see, e.g., [Hida 1991, §3]), we can define for each $\wp \mid p$ an idempotent

$$e_\wp = \lim_{n\to\infty} U_\wp^{n!} \colon \boldsymbol{S}_N(L) \to S_{N\wp}(L)$$

that is surjective onto $S_{N\wp}^{\wp\text{-ord}}(L)$, the subspace of $S_{N\wp}(L)$ spanned by $U_\wp$-eigenforms with unit eigenvalue.

Let $P = \prod_{\wp|p} \wp$. Then we similarly have a surjective idempotent

$$e = \prod_{\wp|p} e_\wp \colon \boldsymbol{S}_N(L) \to S_{NP}^{\mathrm{ord}}(L),$$

where $S_{NP}^{\mathrm{ord}}(L)$ is the subspace of $S_{NP}(L)$ spanned by simultaneous $U_\wp$-eigenforms with unit eigenvalue.

1.5. ***Fourier coefficients of old forms.*** As we will study modular forms through their Fourier coefficients, we give here a criterion for recognising the coefficients of certain old forms.[14] Let N and P be coprime ideals of $\mathbb{O}_F$. The space $S_{NP}^{N\text{-old}} \subset S_{NP}$ is the space spanned by forms $f = [d]f'$ for some $1 \neq d \mid N$ and some cuspform f'

[14] See [Zhang 2001a, §4.4.4].

of level $N'P$ with $N' \mid d^{-1}N$. In the case $P = 1$, we define the space of *newforms* of level dividing N to be orthogonal to the space of old forms for the Petersson inner product. We denote by $\boldsymbol{S}_N^{\mathrm{old}} \subset \boldsymbol{S}_N$ the closed subspace generated by the image of $S_{Np^\infty}^{N\text{-old}}$ in $\boldsymbol{S}_N$. (The coefficient ring will always be either a finite extension of $\mathbb{Q}_p$ or $\mathbb{C}_p$ as understood from context when not present explicitly in the notation.)

Let now $\mathcal{S}$ be the space of functions $f\colon \boldsymbol{N}_F \to \mathcal{A}$ modulo those for which there is an ideal M prime to p such that $f(n) = 0$ for all n prime to M. A function $f \in \mathcal{S}$ is called *multiplicative* if it satisfies[15] $f(mn) = f(m)f(n)$ for all $(m, n) = 1$. For h a multiplicative function, a function f is called an *h-derivative* if it satisfies $f(mn) = h(m)f(n) + h(n)f(m)$ for all $(m, n) = 1$.

Let σ_1 and r be the multiplicative elements of $\mathcal{S}$ defined by

$$\sigma_1(m) = \sum_{d|m} \boldsymbol{N}(d), \qquad r(m) = \sum_{d|m} \varepsilon_{E/F}(d)$$

(where E is a totally imaginary quadratic extension of F of discriminant prime to p).[16] Let $P = \prod_{\wp|p} \wp \subset \mathbb{O}_F$. We define a subspace $\mathcal{D}_N \subset \mathcal{S}$ to be generated by σ_1, r, σ_1-derivatives, r-derivatives and Fourier coefficients of forms in $S_{NP}^{N\text{-old}}$.

Lemma 1.5.1. *The q-expansion map $S_{NP}^{\mathrm{ord}}/S_{NP}^{N\text{-}old} \to \mathcal{S}/\mathcal{D}_N$ is injective.*

Proof. First notice that it is enough to show this when the coefficient ring is a number field L over which S_{NP}^{ord} is defined (it suffices for L to contain all the eigenvalues of the operators T_ℓ ($\ell \nmid Np$) and $U_\wp$ on $S_{NP}(L)$). By [Zhang 2001a, Proposition 4.5.1], the kernel of $S_{NP}(L)/S_{NP}^{N\text{-old}}(L) \to \mathcal{S}/\mathcal{D}_N$ is at most generated by $S_{NP}^{p\text{-old}}(L) = \sum_{\wp|p} S_{NP}^{\wp\text{-old}}(L)$, the space of forms that are old at some $\wp \mid p$. To conclude, it suffices to show that for each $\wp \mid p$ we have $I := S_{NP}^{\wp\text{-old}} \cap S_{NP}^{\wp\text{-ord}} = 0$. The intersection I is stable under the action of $\boldsymbol{T}_{NP}$, which decomposes it into spaces $I[f_i] \subset S_{NP}[f_i]$ corresponding to eigenforms f_i of level N' or $N'\wp$ for some $N' \mid NP\wp^{-1}$. If f_i has level $N'\wp$, then $S_{NP}[f_i]$ does not contain any nonzero $\wp$-oldforms. If f_i has level N' with $\wp \nmid N'$, then $S_{NP}^{\mathrm{ord}}[f_i]$ is either zero or the line spanned by the ordinary $\wp$-stabilisation of f_i, whereas $S_{NP}^{\wp\text{-old}}[f_i]$ is the line spanned by $[\wp]f_i$. We conclude that $I[f_i] = 0$ in all cases. □

Remark 1.5.2. The operators $U_\wp$ for $\wp \mid p$ extend to operators on $\mathcal{S}$ via $U_\wp f(m) = f(m\wp)$. The Hecke algebra $\boldsymbol{T}_{Np}$ acts on the image $\mathcal{S}_N$ of $\boldsymbol{S}_N$ in $\mathcal{S}/\mathcal{D}_N$.

1.6. ***The functional l_{f_α}.*** Recall from the introduction that we have fixed an ordinary primitive Hilbert modular newform f of level $K_0(N)$. If $\alpha_\wp$ is the unit root of

[15] This relation and the following are of course to be understood to hold in $\mathcal{S}$.

[16] We will see below that σ_1 and r are the Fourier coefficients of weight-1 Eisenstein series and theta series.

the $\wp$-th Hecke polynomial of f, $\beta_\wp$ is the other root and the operator $[\wp]$ is as in (1.4.1), then the *p-stabilisation* of f is

$$f_\alpha = \prod_{\wp|p}(1-\beta_\wp[\wp])\, f,$$

a form of level $K_0(N\prod_{\wp|p}\wp)$ satisfying $U_\wp f_\alpha = \alpha_\wp f_\alpha$ for all $\wp \mid p$.

We define a functional, first introduced by Hida, that plays the role of projection onto the f-component. Both sides of our main formula will be images of p-adic modular forms under this operator.

Let P be an ideal of $\mathbb{O}_F$ divisible exactly by the primes $\wp \mid p$. For a form $g \in M_2(K_0(NP))$ with $r \geq 1$, let

$$l_{f_\alpha}(g) = \frac{\langle W_{NP} f_\alpha^\rho, g\rangle}{\langle W_{NP} f_\alpha^\rho, f_\alpha\rangle}.$$

Let $L \subset \overline{\mathbb{Q}}_p$ be the extension of $\mathbb{Q}_p$ generated by $a(f,m)$ for all ideals m and $\alpha_\wp$ for $\wp \mid p$.

Lemma 1.6.1 (Hida). *The above formula defines a linear functional*

$$l_{f_\alpha} \colon M_2(K_0(Np^\infty), L) \to L$$

satisfying:

(1) *On $M_2(K_0(N), L)$, we have*

$$l_{f_\alpha} = \prod_{\wp|p}\left(1-\frac{\boldsymbol{N}\wp}{\alpha_\wp^2}\right)^{-1} \mathbb{1}_f$$

where $\mathbb{1}_f(g) = \langle f, g\rangle/\langle f, f\rangle$.

(2) *On $M_2(K_0(N\wp^r))$, we have, for each nonnegative $t \leq r-1$,*

$$l_{f_\alpha} \circ U_\wp^t = \alpha_\wp(f)^t l_{f_\alpha}.$$

(3) *If each $\iota_p(\alpha_\wp)$ is a p-adic unit, l_{f_α} admits a continuous extension to p-adic modular forms still denoted*

$$l_{f_\alpha} \colon \boldsymbol{M}_N(L) \to L.$$

Proof. See [Hida 1991, Lemma 9.3], where the well-definedness of the functional and its extension to p-adic modular forms are proved more generally for Hida families. For part (1), the computation is the same as in the case of elliptic modular forms: see [Perrin-Riou 1988] or [Hida 1985, §4]. □

Some quotient spaces. Let $\overline{\mathcal{S}} = \mathcal{S}/\mathcal{D}_N$. The ordinary projection operator e is not defined on all arithmetic functions; however, its kernel $\mathrm{Ker}(e)$ is a well-defined subspace of $\mathcal{S}$. We define

$$\overline{\mathcal{S}}^{\mathrm{ord}} := \mathcal{S}/\mathcal{D}_N + \mathrm{Ker}(e).$$

The quotient map $\overline{\mathcal{S}} \to \overline{\mathcal{S}}^{\mathrm{ord}}$ is clearly injective when restricted to the image of S_{NP}^{ord}, where $P = \prod_{\wp|p} \wp$. Then we denote by $\overline{\mathcal{S}}_N^{\mathrm{ord}}$ the image of S_{NP}^{ord} in either $\overline{\mathcal{S}}$ or $\overline{\mathcal{S}}^{\mathrm{ord}}$. It is also identified with the common image of S_{NP} and $\boldsymbol{S}_N$ in $\overline{\mathcal{S}}^{\mathrm{ord}}$. We denote by $\overline{\mathcal{S}}_N^{p\text{-adic}} \subset \overline{\mathcal{S}}$ the image of $\boldsymbol{S}_N$.

We obtain a commutative diagram (where L is as usual any sufficiently large finite extension of $\mathbb{Q}_p$):

$$\begin{array}{ccccc} \boldsymbol{S}_N(L) & \longrightarrow & \overline{\mathcal{S}}_N^{p\text{-adic}}(L) & \hookrightarrow & \overline{\mathcal{S}}^{\mathrm{ord}} \\ \downarrow{\scriptstyle e} & & \downarrow & & \\ S_{NP}^{\mathrm{ord}}(L)/S_{NP}^{N\text{-old}} & \xrightarrow{\sim} & \overline{\mathcal{S}}_N^{\mathrm{ord}}(L) & \xrightarrow{l_{f_\alpha}} & L \end{array} \tag{1.6.1}$$

where the right-hand vertical map is the restriction of the quotient $\overline{\mathcal{S}} \to \overline{\mathcal{S}}^{\mathrm{ord}}$ and the bottom horizontal map is an isomorphism by Lemma 1.5.1.

2. Theta measure

We construct a measure on the Galois group of the maximal abelian extension of E unramified outside p with values in p-adic theta series and compute its Fourier expansion.

2.1. ***Weil representation.*** We first define the Weil representation. See [Bump 1997, §4.8] for an introduction and [Waldspurger 1985] or [Yuan et al. 2013] for our conventions on the representation for similitude groups.

Local setting. Let $V = (V, q)$ be a quadratic space over a local field F of characteristic not 2 with a quadratic form q; we choose a nontrivial additive character $\boldsymbol{e}$ of F. For simplicity, we assume V has even dimension. For $u \in F^\times$, we denote by V_u the quadratic space (V, uq). We let $\boldsymbol{GL}_2(F) \times \boldsymbol{GO}(V)$ act on the space $\mathcal{S}(V \times F^\times)$ of Schwartz functions as follows (here $\nu\colon \boldsymbol{GO}(V) \to \boldsymbol{G}_m$ denotes the similitude character):

- $r(h)\phi(t, u) = \phi(h^{-1}t, \nu(h)u)$ for $h \in \boldsymbol{GO}(V)$,
- $r(n(x))\phi(t, u) = \boldsymbol{e}(xuq(t))\phi(t, u)$ for $n(x) = \left(\begin{smallmatrix} 1 & x \\ & 1 \end{smallmatrix}\right) \in \boldsymbol{GL}_2$,
- $r\left(\begin{smallmatrix} a & \\ & d \end{smallmatrix}\right)\phi(t, u) = \chi_V(a)|a/d|^{(\dim V)/4}\phi(at, d^{-1}a^{-1}u)$,
- $r(w)\phi(x, u) = \gamma(V_u)\hat{\phi}(x, u)$ for $w = \left(\begin{smallmatrix} & 1 \\ -1 & \end{smallmatrix}\right)$.

Here χ_V is the quadratic character associated with V, $\gamma(V_u)$ is a certain square root of $\chi(-1)$ and $\hat{\phi}$ denotes the Fourier transform in the first variable

$$\hat{\phi}(x,u) = \int_V \phi(y,u)\boldsymbol{e}(-u\langle x,y\rangle)\,dy$$

where $\langle\cdot,\cdot\rangle$ is the bilinear form associated with q and dy is the self-dual Haar measure.

Global setting. Given a quadratic space (V,q) over a global field F of characteristic not 2 (and a nontrivial additive character $\boldsymbol{e}\colon F\backslash \boldsymbol{A}_F \to \mathbb{C}^\times$), the Weil representation is the restricted tensor product r of the associated local Weil representations, with spherical functions $\phi_v(t,u) = \mathbb{1}_{\mathcal{V}_v\times\mathcal{O}_{F,v}^\times}(x,u)$ for some choice of lattices $\mathcal{V}_v \subset V(F_v)$.

The case of interest to us is the following: F is a totally real number field, $V=(E,\mathfrak{N})$ is given by a quadratic CM extension E/F with the norm form $\mathfrak{N}=N_{E/F}$ and the lattices $\mathcal{O}_{E,v}\subset E_v$ and the additive character $\boldsymbol{e}$ is the standard one. We denote $G=\boldsymbol{GL}_2$ and $H=\boldsymbol{GO}(V)$, two algebraic groups defined over F; we have $H\cong \mathrm{Res}_{E/F}\boldsymbol{G}_m$. In this case, we have

$$\chi_V = \varepsilon_{E/F} = \varepsilon,$$

where $\varepsilon_{E/F}$ is the quadratic character of $F_{\boldsymbol{A}}^\times$ associated with the extension E/F. The self-dual measure on E_v is the one giving $\mathcal{O}_{E,v}$ volume $|\mathcal{O}_{E,v}/\mathfrak{D}_v|^{-1/2}$ where $\mathfrak{D}_v$ is the relative different. Moreover, the constant γ can be explicitly described [Bushnell and Henniart 2006, §38.6, §30.4, §23.5]: in the case $v\mid\Delta_{E/F}$, which is the only one we will be using, such description is in terms of a local Gauss sum $\kappa(v)$:

$$\gamma(E_v,u\mathfrak{N}) = \varepsilon_v(u)\kappa(v) = \varepsilon_v(u)|\pi_v|^{1/2}\sum_{x\in(\mathcal{O}_{F,v}/\pi_v\mathcal{O}_{F,v})^\times}\varepsilon(x/\pi_v)\boldsymbol{e}_v(x/\pi_v). \quad (2.1.1)$$

Notice that our $\kappa(v)$ is the *inverse* of the quantity denoted by the same name in [Zhang 2001a, Proposition 3.5.2].

2.2. ***Theta series.*** We define the *theta kernel* to be

$$\theta_\phi(g,h) = \sum_{(t,u)\in V\times F^\times} r(g,h)\phi(t,u),$$

an automorphic form for the group $\boldsymbol{GL}_2(F)\backslash\boldsymbol{GL}_2(\boldsymbol{A}_F)\times\boldsymbol{GO}(V)\backslash\boldsymbol{GO}(V_{\boldsymbol{A}_F})$.

If $\mathcal{W}$ is an automorphic function for H that is trivial at infinity (which is the same thing as a linear combination of finite-order Hecke characters of E), we define the *theta series*[17]

$$\theta_\phi(\mathcal{W})(g) = \int_{H(F)\backslash H(\boldsymbol{A}_F)} \mathcal{W}(h^{-1})\theta_\phi(g,h)\,dh,$$

[17]The reason for taking $\mathcal{W}(h^{-1})$ rather than $\mathcal{W}(h)$ is that we want $\theta_\phi(\mathcal{W})$ to be the series classically denoted $\Theta(\mathcal{W})$ for a suitable choice of ϕ — this will be clear from the computations below.

which is an automorphic form on G. Here the measure dh is the product of the measure on $H(\boldsymbol{A}^\infty)$ that gives volume 1 to the compact $U_0 = \hat{\mathbb{O}}_E^\times$ and any fixed measure[18] on $H(\boldsymbol{A}_\infty)$.

Let us explain how to explicitly compute the integral in our situation. For each open compact subgroup $U \subset H(\boldsymbol{A}_F^\infty) = E_{\boldsymbol{A}^\infty}$, we have exact sequences

$$1 \to \mathbb{O}_{E,U}^\times \backslash U E_\infty^\times \to E^\times \backslash E_{\boldsymbol{A}}^\times \to E^\times U \backslash E_{\boldsymbol{A}^\infty}^\times \to 1$$

and

$$1 \to \mu(U) \backslash U E_\infty^1 \to \mathbb{O}_{E,U}^\times \backslash U E_\infty^\times \xrightarrow{\mathfrak{N}_\infty} N(\mathbb{O}_{E,U}^\times) \backslash F_\infty^+ \to 1.$$

The notation used is the following: $\mathbb{O}_{E,U}^\times = E^\times \cap U \supset \mu(U) =$ the subset of roots of unity, $\mathfrak{N}_\infty \colon E_\infty^\times \to F_\infty^+$ is the norm map at the infinite places and E_∞^1 is its kernel.

We can choose a splitting ι of the first sequence, for example

$$\iota \colon E^\times U \backslash E_{\boldsymbol{A}^\infty}^\times \cong E^\times U \backslash (E_{\boldsymbol{A}}^\times)^{1,\|} \hookrightarrow E^\times \backslash E_{\boldsymbol{A}}^\times,$$

where $(E_{\boldsymbol{A}}^\times)^{1,\|}$ denotes the set of idèles of adelic norm 1 with infinity component $h_\infty = (h, \dots, h)$ for some real number $h > 0$ and the isomorphism is the unique one that gives the identity once composed with projection onto the finite part.

We begin to expand the series, evaluating the integral as explained above and exploiting the fact that the action of $H(F_\infty) = E_\infty^\times$ on $\phi(t, u)$ factors through the norm. We take U to be small enough so that $\mathcal{W}$ and ϕ are invariant under U and denote

$$\bar{\phi}_v(t, u) = \int_{H(F_v)} r(h)\phi_v(t, u)\, dh \quad \text{if } v \mid \infty$$

and $\bar{\phi} = \prod_{v\nmid\infty} \phi_v \prod_{v\mid\infty} \bar{\phi}_v$. A specific choice of $\bar{\phi}_v$ will be made shortly; for the moment, we just say, and use in the following computation, that we will take $u \mapsto \bar{\phi}_v(t, u)$ to be supported on $\mathbb{R}^+$.

We have

$$\begin{aligned}\theta_\phi(\mathcal{W})(g) &= \int_{E^\times \backslash E_{\boldsymbol{A}}^\times} \mathcal{W}(h^{-1})\theta_\phi(g, h)\, dh \\ &= w_U^{-1} \int_U \int_{E_\infty^1} \int_{\mathfrak{N}(\mathbb{O}_{E,U}^\times)\backslash F_\infty^+} \int_{E^\times U \backslash E_{\boldsymbol{A}^\infty}^\times} \mathcal{W}(\iota(a)^{-1}) \\ &\qquad \cdot \sum_{(t,u)\in E\times F^\times} r(g, \iota(a)h)\phi(t, u)\, da\, dh.\end{aligned}$$

Here $w_U = |\mu(U)|$ and dh denotes the measure on $U \times E_\infty^1 \times F_\infty^+ = U \times H(F_\infty)$. We partially collapse the integral over $\mathfrak{N}(\mathbb{O}_{E,U}^\times) \backslash F_\infty^+$ and the sum over $u \in F^\times$ and

[18] There will be no ambiguity since later we will choose ϕ_∞ to again be any fixed Schwartz function whose integral over $H(\boldsymbol{A}_\infty)$ with respect to the chosen measure is a specified function $\bar{\phi}_\infty$.

use our choice of ϕ_∞ to get

$$= w_U^{-1}\,\mathrm{vol}(U)\int_{E^\times U\backslash E_{\mathbf{A}^\infty}^\times} \mathcal{W}(\iota(a)^{-1}) \sum_{u\in\mathfrak{N}(\mathbb{O}_{E,U}^\times)\backslash F^+}\sum_{t\in E} r(g,\iota(a))\bar{\phi}(t,u)\,da$$

$$= w^{-1}\frac{h}{h_U}\int_{E^\times U\backslash E_{\mathbf{A}^\infty}^\times} \mathcal{W}(\iota(a)^{-1})\nu_U \sum_{u\in\mathfrak{N}(\mathbb{O}_{E,U}^\times)\backslash F^+}\sum_{t\in E} r(g,\iota(a))\bar{\phi}(t,u)\,da. \quad (2.2.1)$$

Here in the last step, we have defined $\nu_U = [\mathfrak{N}(\mathbb{O}_E^\times) : \mathfrak{N}(\mathbb{O}_{E,U}^\times)]$ and computed $\mathrm{vol}(U) = \mathrm{vol}(U_0)(h/h_U)(w_U/w)\nu_U^{-1}$, where $U_0 = \hat{\mathbb{O}}_E^\times$, $h_U = |E^\times U\backslash E_{\mathbf{A}^\infty}^\times|$, $h = h_{U_0}$ and $w = w_{U_0}$. Recall that our measure satisfies $\mathrm{vol}(U_0) = 1$. The remaining integral is just a finite sum.

The sum over u is actually finite due to the integrality constraints imposed by ϕ at finite places.[19]

2.3. ***Theta measure.*** We define a measure with values in p-adic modular forms on the group

$$\mathcal{G}' = \mathrm{Gal}(E'_\infty/E) \cong \varprojlim \overline{E^\times U_{p^n}}\backslash E_{\mathbf{A}^\infty}^\times$$

where the overline denotes closure and E'_∞ is the maximal abelian extension of E unramified outside p, that is, the union of the ray class fields of E of p-power ray $U_{p^n} = \prod_v\{\text{units} \equiv 1 \bmod p^n\mathbb{O}_{E,v}\}$, and the isomorphism is given by class field theory. The topology is the profinite topology.

Recall that a *measure* on a topological space $\mathcal{G}$ with values in a p-adic Banach space $\boldsymbol{M}$ is a $\mathbb{C}_p$-linear functional

$$\mu\colon \mathcal{C}(\mathcal{G},\mathbb{C}_p)\to \boldsymbol{M}$$

on continuous $\mathbb{C}_p$-valued functions, which is continuous (equivalently, bounded) with respect to the supremum norm on $\mathcal{C}(\mathcal{G},\mathbb{C}_p)$. The linearity property will be called distributional property in what follows. The boundedness property will in each case at hand be verified on the set of p-adic characters of $\mathcal{G}$, which in our cases generates the whole of $\mathcal{C}(\mathcal{G},\mathbb{C}_p)$ (classically, the continuity of μ goes by the name of *abstract Kummer congruences* for μ).

When $\boldsymbol{M} = \boldsymbol{M}_0\otimes_{\mathbb{Q}_p}\mathbb{C}_p$ for a p-adic Banach space $\boldsymbol{M}_0$ over $\mathbb{Q}_p$, the measure μ is said to be *defined over* $\mathbb{Q}_p$ if $\mu(\mathcal{W})\in \boldsymbol{M}_0\otimes\mathbb{Q}_p(\mathcal{W})$ whenever the function $\mathcal{W}$ on $\mathcal{G}$ has values in $\mathbb{Q}_p(\mathcal{W})\subset\overline{\mathbb{Q}}_p\subset\mathbb{C}_p$.

[19] We will see this in more detail shortly. We are also using the definition of $\bar{\phi}_\infty$ in order to freely replace the sum over $u\in F^\times$ with a sum over $u\in F^+$ — in fact, a slight variation would be necessary when $\det g_\infty\notin F_\infty^+$, but this is a situation we won't encounter.

Definition 2.3.1. The *theta measure* $d\Theta$ on $\mathscr{G}'$ is defined by

$$\Theta(\mathscr{W}) = \int_{\mathscr{G}'} \mathscr{W}(\sigma)\, d\Theta(\sigma) := \theta_\phi(\mathscr{W}),$$

for any function $\mathscr{W}\colon \mathscr{G}' \to \overline{\mathbb{Q}}$ factoring through a finite quotient of $\mathscr{G}'$, where the function ϕ is chosen as follows:

- For $v \nmid p\infty$, $\phi_v(t,u) = \mathbb{1}_{\mathcal{O}_{E,v}}(t)\mathbb{1}_{d_{F_v}^{-1,\times}}(u)$.
- For $v \mid p$,
$$\phi_v(t,u) = [\mathcal{O}_{E,v}^\times : U_v'] \mathbb{1}_{U_v'}(t)\mathbb{1}_{d_{F_v}^{-1,\times}}(u),$$
where $U_v' \subset \mathcal{O}_{E,v}^\times$ is any small-enough compact set — that is, $U_v' \subset U_v$ if $\mathscr{W}$ is invariant under $U = \prod_v U_v$, and the definition does not depend on the choice of U_v. (In practice, we will choose $U_v' = U_v$ if U_v is maximal with respect to the property just mentioned.)
- For $v \mid \infty$, $\phi_v(t,u)$ is a Schwartz function such that
$$\int_{H(F_v)} r(h)\phi_v(t,u)\, dh = \bar{\phi}_v(t,u) = 1_{\mathbb{R}^+}(u)\exp(-2\pi u N(t)).$$
(See [Yuan et al. 2013, §4.1] for more details on this choice.)

In Corollary 2.4.2 below, we will show that this in fact defines a measure on $\mathscr{G}'$ with values in p-adic Hilbert modular forms of weight 1, tame level $\Delta_{E/F}$ and character ε.

2.4. ***Fourier expansion of the theta measure, I.*** We compute the Fourier expansion of the theta measure on $\mathscr{G}'$, carrying on the calculation started in Section 2.2.

In the case where $g = \left(\begin{smallmatrix} y & x \\ & 1 \end{smallmatrix}\right)$ with $y_\infty > 0$, the sum over (u,t) in (2.2.1) evaluates to

$$\varepsilon(y)|y|^{1/2} \sum_{u,t} \phi^\infty(a^{-1}yt, \mathfrak{N}(a)y^{-1}u)\boldsymbol{e}_\infty(iy_\infty u N(t))\boldsymbol{e}(xu\mathfrak{N}(t)). \tag{2.4.1}$$

Then we compute the sum of this expression over the finite quotient $\mathscr{G}'_U$ of $\mathscr{G}'$, with $\mathscr{G}'_U \cong E^\times U \backslash E_{\boldsymbol{A}^\infty}^\times$.

We assume $\mathscr{W}$ is a character so that $\mathscr{W}(a^{-1}) = \overline{\mathscr{W}}(a)$ where $\overline{\mathscr{W}} = \mathscr{W}^{-1}$.

First we precompute the product of all the constants appearing in the theta series of (2.2.1), including the one from ϕ — we take

$$\phi_v(t,u) = [\mathcal{O}_{E,v}^\times : U_v]\mathbb{1}_{U_v}(t)\mathbb{1}_{\mathcal{O}_F^\times}(u),$$

so

$$\begin{aligned} w\frac{h}{h_U}v_U[\mathcal{O}_{E,v}^\times : U_v] &= w[\mathcal{O}_E^\times \backslash \hat{\mathcal{O}}_{E,v}^\times : \mathcal{O}_{E,U}^\times \backslash U]^{-1}[\mathfrak{N}(\mathcal{O}_E^\times) : \mathfrak{N}(\mathcal{O}_{E,U}^\times)]^{-1}[\hat{\mathcal{O}}_E^\times : U] \\ &= w[\mu(\mathcal{O}_E) : \mu(U)] = w_U^{-1}. \end{aligned}$$

This computation together with (2.2.1) and (2.4.1) gives

$$\begin{aligned}\Theta(\mathcal{W}) &= \varepsilon(y)|y|^{1/2}w_U^{-1}\sum_{a\in E^\times U\backslash E_{\mathbf{A}^\infty}^\times}\overline{\mathcal{W}}(a)\sum_{t\in E,\,u\in\mathfrak{N}(\mathbb{O}_{E,U}^\times)\backslash F^+}\phi^{p\infty}(a^{-1}yt,\mathfrak{N}(a)y^{-1}u)\\ &\quad\cdot\mathbb{1}_{\mathbb{O}_{E,U,p}^\times}(a^{-1}yt)\mathbb{1}_{d_{F_p}^{-1},\times}(\mathfrak{N}(a)y^{-1}u)\boldsymbol{e}_\infty(iy_\infty u\mathfrak{N}(t))\boldsymbol{e}(xu\mathfrak{N}(t))\\ &= \varepsilon(y)\overline{\mathcal{W}}(y)|y|^{1/2}w_U^{-1}\sum_{a\in E^\times U\backslash E_{\mathbf{A}^\infty}^\times}\overline{\mathcal{W}}(a)\sum_{t\in E,\,u\in\mathfrak{N}(\mathbb{O}_{E,U}^\times)\backslash F^+}\mathbb{1}_{\widehat{\mathbb{O}_{E,U}}\cap\mathbb{O}_{E,U,p}^\times}(a^{-1}t)\\ &\quad\cdot\mathbb{1}[\mathfrak{N}(a)yu\mathbb{O}_F=d_F^{-1}]\boldsymbol{e}_\infty(iy_\infty u\mathfrak{N}(t))\boldsymbol{e}(xu\mathfrak{N}(t)),\end{aligned}$$

where we have made the change of variable $a\to ay^\infty$.

Now we make the substitution $u\mathfrak{N}(t)=\xi$ and observe that the contribution to the ξ-th term is equal to 0 if $(\xi y d_F,\,p)\neq 1$ and otherwise it equals $\overline{\mathcal{W}}(a)$ times the cardinality of the set

$$R_{a^{-1}}(\xi,\,y)=\left\{(t,u)\in\mathbb{O}_E\times F^+\;\middle|\;t\in U_p,\;u\mathfrak{N}(t)=\xi,\;\mathfrak{N}(t/a)\mathbb{O}_F=\xi y d_F\right\}/\mathfrak{N}(\mathbb{O}_{E,U}^\times),$$

which admits a surjection $\pi:\,(t,u)\mapsto a^{-1}t\mathbb{O}_E$ to the set $\boldsymbol{r}_{a^{-1}}(\xi y d_F)$ of ideals $\mathfrak{b}\subset\mathbb{O}_E$ in the U-class a^{-1}, whose norm is $\mathfrak{N}(\mathfrak{b})=\xi y d_F$. The fibres of π are in bijection with $\mathbb{O}_{E,U}^\times/\mathfrak{N}(\mathbb{O}_{E,U}^\times)$, which has cardinality w_U. We deduce the following description of the Fourier coefficients of $\Theta(\mathcal{W})$:

Proposition 2.4.1. *The series $\Theta(\mathcal{W})$ belongs to $S_1(K_1(\Delta(\mathcal{W})),\varepsilon\overline{\mathcal{W}}|_{F_{\mathbf{A}}^\times})$, where $\Delta(\mathcal{W})=\Delta\mathfrak{N}(\mathfrak{f}(\mathcal{W}))$. Its Fourier coefficients are given by*

$$a(\Theta(\mathcal{W}),m)=\sum_{\substack{\mathfrak{b}\subset\mathbb{O}_E\\ \mathfrak{N}(\mathfrak{b})=m}}\mathcal{W}(\mathfrak{b})=r_{\mathcal{W}}(m)$$

for $(m,\,p)=1$ and vanish for $(m,\,p)\neq 1$.

Corollary 2.4.2. *The functional Θ of Definition 2.3.1 is a measure on $\mathcal{G}'$ with values in $\boldsymbol{S}_1(K_1(\Delta),\varepsilon)$, defined over $\mathbb{Q}_p$.*

Proof. The distributional property is obvious from the construction or can be seen from the q-expansion given above, from which boundedness is also clear. See also [Hida and Tilouine 1993, Theorem 6.2], where a slightly different theta measure is constructed. □

Lemma 2.4.3. *Assume that $(D_E,\,D_F p)=1$. The theta series admits a functional equation*

$$W_{\Delta(\mathcal{W})}\Theta(\mathcal{W})=(-i)^{[F:\mathbb{Q}]}\mathcal{W}(d_F^{(p)})\overline{\mathcal{W}}(\mathfrak{D}_E)\tau(\overline{\mathcal{W}})\Theta(\overline{\mathcal{W}})$$

where $\mathfrak{D}_E$ is the relative different, $d_F^{(p)}$ is the prime-to-p factor of the different and $\tau(\overline{\mathcal{W}}) = \prod_{v|p} \tau(\overline{\mathcal{W}}_v)$ with

$$\tau(\overline{\mathcal{W}}_v) = |\pi_v|^{-c/2} \int_{E_v^\times} \overline{\mathcal{W}}_v(h_v) \boldsymbol{e}_v(-\operatorname{Tr}_{E_v/F_v}(h_v))\, dh_v$$

if the relative norm of the conductor of $\overline{\mathcal{W}}_v$ is $\pi_v^c \mathbb{O}_{F,v}$.

Proof. Let

$$\phi_{\mathcal{W}}(g,t,u) = \int_{H(F)\backslash H(\boldsymbol{A})} \mathcal{W}(h^{-1}) r(g,h)\phi(t,u)\, dh,$$
$$\phi'_{\mathcal{W}}(g,t,u) = \varepsilon\mathcal{W}(\pi_{\Delta(\mathcal{W})}) \int_{H(F)\backslash H(\boldsymbol{A})} \mathcal{W}(h^{-1}) r(g W_{\Delta(\mathcal{W})}, h)\phi(t,u)\, dh$$

for $(t,u) \in E_{\boldsymbol{A}} \times F_{\boldsymbol{A}}^\times$. The behaviour in g is through the Weil representation.

Then we have

$$W_{\Delta(\mathcal{W})}\Theta(\mathcal{W})(g) = \varepsilon\mathcal{W}(\det g) \sum_{(t,u)\in E\times F^\times} \phi'_{\mathcal{W}}(g,t,u),$$
$$\Theta(\overline{\mathcal{W}})(g) = \sum_{(t,u)\in E\times F^\times} \phi_{\overline{\mathcal{W}}}(g,t,u)$$

so that the lemma follows if we show that for all $(t,u) \in E_{\boldsymbol{A}} \times F_{\boldsymbol{A}}^\times$

$$\varepsilon\mathcal{W}(\det g)\phi'_{\mathcal{W}}(g,t,u) = (-i)^{[F:\mathbb{Q}]}\overline{\mathcal{W}}(\mathfrak{D}_E)\tau(\overline{\mathcal{W}})\varepsilon\mathcal{W}(u)\phi_{\overline{\mathcal{W}}}(g,\bar{t},u) \tag{2.4.2}$$

where $\bar{t}$ is the conjugate of t under the nontrivial automorphism of E over F. We write

$$\tilde{\tau}(\overline{\mathcal{W}}) = (-i)^{[F:\mathbb{Q}]}\mathcal{W}(d_F^{(p)})\overline{\mathcal{W}}(\mathfrak{D}_E)\tau(\overline{\mathcal{W}})$$

for short.

We claim that it suffices to prove (2.4.2) for $g = 1$. Indeed it is clear that this implies the same result for all $g \in \boldsymbol{SL}_2(\boldsymbol{A})$ by acting via the Weil representation on both sides (viewed as functions of (t,u)). Then it suffices to verify it for the elements of the form $d(y) = \left(\begin{smallmatrix} 1 & \\ & y \end{smallmatrix}\right)$:

$$\begin{aligned}\varepsilon(y)\mathcal{W}(y)r(d(y))\phi'_{\mathcal{W}}(1,t,u) &= \tilde{\tau}(\overline{\mathcal{W}})\varepsilon(y)\mathcal{W}(y)r(d(y))[\varepsilon\mathcal{W}(u)\phi_{\overline{\mathcal{W}}}(1,\bar{t},u)]\\ &= \tilde{\tau}(\overline{\mathcal{W}})\varepsilon\mathcal{W}(y)\varepsilon\mathcal{W}(y^{-1}u)r(d(y))\phi_{\overline{\mathcal{W}}}(1,\bar{t},u)\\ &= \tilde{\tau}(\overline{\mathcal{W}})\varepsilon(u)\mathcal{W}(u)\phi_{\overline{\mathcal{W}}}(d(y),\bar{t},u).\end{aligned}$$

We now prove (2.4.2) for $g = 1$, thus dropping g from the notation. We can write

$$\phi'_{\mathcal{W}}(t,u) = \int_{H(F)\backslash H(\boldsymbol{A}^{p\Delta})} {}^{\circ}\mathcal{W}(h_0^{-1}) r(1,h)\phi^{p\Delta}(t,u)\,dh_0 \cdot \prod_{v|p\Delta} {}^{\circ}\mathcal{W}(\pi_v^{c_v}) \int_{H(F_v)} {}^{\circ}\mathcal{W}(h_v^{-1}) r(W_{\pi_v^{c_v}},1)\phi(h_v^{-1}t, \nu(h_v)u)\,dh_v$$

where c_v is the appropriate exponent. We can rewrite this as

$$\phi'_{\mathcal{W}}(t,u) = \phi'^{\Delta p}_{\mathcal{W}}(t,u) \prod_{v|\Delta p} \phi'_{\mathcal{W},p}(t,u)$$

with obvious notation. A similar factorisation holds for $\phi_{\mathcal{W}}(t,u)$.

For $v \nmid \Delta p$, we have, by the explicit description of ϕ_v (dropping the subscripts v),

$$\begin{aligned} r(h)\phi(t,u) = \phi(h^{-1}t, \nu(h)u) &= \phi(\pi_{d_F} u\bar{h}\bar{t}, \nu(h)u) \\ &= \phi(\pi_{d_F} uh\bar{t}, \nu(h)^{-1}u^{-1}\pi_{d_F}^{-2}) = r((\pi_{d_F}uh)^{-1})\phi(\bar{t},u). \end{aligned}$$

A change of variable and integration over $H(F)\setminus H(\boldsymbol{A}^{\Delta p})$ then gives

$$\phi'^{\Delta p}_{\mathcal{W}}(t,u) = \varepsilon^{\Delta p}(ud_F)\mathcal{W}^{\Delta p}(ud_F)\phi^{\Delta p}_{\overline{\mathcal{W}}}(\bar{t},u). \tag{2.4.3}$$

For $v \mid \Delta$, we have by (2.5.1) below and the previous argument

$$\begin{aligned} \varepsilon(\pi) r(W_\pi, h)(\pi)\phi(t,u) &= \varepsilon(u)\kappa(v)\phi(h^{-1}t\pi_{\mathfrak{D}}, \pi^{-1}\nu(h)u) \\ &= \varepsilon(u)\kappa(v) r(u^{-1}\pi_{d_F^{-1}}h^{-1}\pi_{\mathfrak{D}})\phi(\bar{t},u) \end{aligned}$$

where $\pi_{\mathfrak{D}} \in \mathbb{O}_{E,v}^{\times}$ is a generator of the local relative different of E_v/F_v. After change of variable and integration, we obtain

$$\phi'_{\mathcal{W},v}(t,u) = \kappa(v)\varepsilon_v(u)\mathcal{W}_v(ud_F)\overline{\mathcal{W}}_v(\mathfrak{D})\phi_{\overline{\mathcal{W}},v}(\bar{t},u). \tag{2.4.4}$$

For $v \mid p$, we have

$$\begin{aligned} &{}^{\circ}\mathcal{W}(\pi^c)\int_{H(F_v)} \mathcal{W}(h^{-1}) r(h, w_{\pi^c})\phi(t,u)\,d^{\times}h \\ &\quad = |\pi|^{-c/2}\int_{E^{\times}}\int_{E} {}^{\circ}\overline{\mathcal{W}}(\pi^{-c}h)\boldsymbol{e}(-\pi^{-c}u\nu(h)\operatorname{Tr}(h^{-1}t\bar{\xi}))\phi(\xi, \pi^{-c}\nu(h)u)\,d\xi\,d^{\times}h \end{aligned}$$

Using the fact that $\phi(\xi,u)\,d\xi = \phi(\xi,u)\,d^{\times}\xi$ and a change of variables $\zeta = \pi^{-c}uh\xi\bar{t}$, this equals

$${}^{\circ}\mathcal{W}(u)\tau({}^{\circ}\overline{\mathcal{W}})\int_{E^{\times}} \mathcal{W}(\xi\bar{t})\phi(\xi, \nu(t\xi)u)\,d^{\times}\xi$$

after integration, where the new second argument in ϕ gives the condition for the integral in $d\zeta$ to be nonzero. We observe that $\phi(\xi) = \phi(\xi^{-1})$ so that with the new

variable $h' = \xi\bar{t}$, and reintroducing v in the notation, this can be rewritten as

$$\mathcal{W}_v(u)\tau(\overline{\mathcal{W}}_v)\int_{E_v^\times}\overline{\mathcal{W}}_v(h_v')^{-1}\phi(h'^{-1}\bar{t},\nu(h_v')u)\,d^\times h_v'$$

so that

$$\phi'_{\mathcal{W},v}(t,u) = \varepsilon_v(d_F)\varepsilon_v(u)\mathcal{W}_v(u)\tau(\overline{\mathcal{W}}_v)\phi_{\overline{\mathcal{W}},v}(\bar{t},u). \tag{2.4.5}$$

Putting together (2.4.3), (2.4.4) and (2.4.5) and using the formula $\prod_{v|\Delta}\kappa(v) = (-i)^{[F:\mathbb{Q}]}\varepsilon(d_F)$ from [Zhang 2001a, p. 127],[20] we obtain (2.4.2) as desired. □

2.5. ***Fourier expansion of the theta measure, II.*** For later use in computing the trace of the convolution of the theta measure with the Eisenstein measure (defined below), we need to consider the expansion of $\Theta(\mathcal{W})^{(\delta)}(g) = \Theta(\mathcal{W})(gW_\delta)$ for $g = \left(\begin{smallmatrix} y & x \\ & 1\end{smallmatrix}\right)$; for such a g, we have

$$\begin{pmatrix} y & x \\ & 1\end{pmatrix} W_\delta = \begin{pmatrix} 1 & x \\ & 1\end{pmatrix}\begin{pmatrix} y & \\ & \pi_\delta\end{pmatrix} w_\delta$$

where π_δ is an idèle with components π_v at $v \mid \delta$ and 1 everywhere else. Here π_v is a uniformiser chosen to satisfy $\varepsilon(\pi_v) = 1$.

The modular form $\Theta(\mathcal{W})^\delta$ can be expanded in the same way as in Section 2.4 except that for $v \mid \delta$ we need to replace $\phi_v(t,u) = \mathbb{1}_{\mathcal{O}_{E,v}}(t)\mathbb{1}_{d_F^{-1},\times}(u)$ by

$$\begin{aligned} W_\delta\phi_v(t,u) &= \varepsilon_v(\pi_v)\begin{pmatrix} 1 & \\ & \pi_v\end{pmatrix}\gamma(u)\widehat{\mathbb{1}_{\mathcal{O}_{E,v}}}(t)\mathbb{1}_{d_{F,v}^{-1},\times}(u) \\ &= \varepsilon_v(u)\kappa(v)\mathbb{1}_{\mathfrak{D}_v^{-1}}(t)\mathbb{1}_{d_F^{-1},\times}(\pi_\delta^{-1}u). \end{aligned} \tag{2.5.1}$$

Here recall that $\mathfrak{D}$ is the relative different of E/F and that w acts as Fourier transform in t with respect to the quadratic form associated with $u\mathfrak{N}$, with the normalising constant $\gamma(u) = \gamma(E_v, u\mathfrak{N})$ as described in (2.1.1).

The computation of the expansion can then be performed exactly as in Section 2.4. We omit the details but indicate that the relevant substitution is now $a \to \pi_\mathfrak{d} ay$, where $\mathfrak{d}$ is an ideal of $\mathcal{O}_E$ of norm δ and $\pi_\mathfrak{d} \in \widehat{\mathcal{O}_E}$ is a generator with components equal to 1 away from $\mathfrak{d}$.

Proposition 2.5.1. *The Whittaker–Fourier coefficients of the series $\Theta(\mathcal{W})^{(\delta)}$ are given by*

$$\tilde{a}(\Theta(\mathcal{W})^{(\delta)}, y) = \varepsilon\mathcal{W}(y)|y|^{1/2}\kappa(\delta)\mathcal{W}(\mathfrak{d})\varepsilon_\delta(y)r_\mathcal{W}(yd_F),$$

where $\kappa(\delta) = \prod_{v|\delta}\kappa(v)$.

[20] Recall that our $\kappa(v)$ are the inverses of the $\kappa(v)$ of [loc. cit.].

3. Eisenstein measure

In this section, we construct a measure (see Section 2.3) valued in Eisenstein series of weight 1 and compute its Fourier expansion.

3.1. ***Eisenstein series.*** Let k be a positive integer, M be an ideal of $\mathbb{O}_F$, and $\varphi\colon F_{\boldsymbol{A}}^\times/F^\times \to \mathbb{C}^\times$ be a finite-order character of conductor dividing M satisfying $\varphi_v(-1) = (-1)^k$ for $v \mid \infty$. Let

$$L^M(s,\varphi) = \sum_{(m,M)=1} \varphi(m)\boldsymbol{N}(m)^{-s}, \tag{3.1.1}$$

where the sum runs over all nonzero ideals of $\mathbb{O}_F$.

Let $B \subset \boldsymbol{GL}_2$ be the Borel subgroup of upper-triangular matrices; recall the notation from Section 1.1 and the Iwasawa decomposition (1.1.1); the decomposition is not unique, but the ideal of $\hat{\mathbb{O}}_F$ generated by the lower-left entry of the $K_0(1)$-component is well-defined.

For $s \in \mathbb{C}$, define a function $H_{k,s}(g,\varphi)$ on $\boldsymbol{GL}_2(\boldsymbol{A}_F)$ by

$$H_{k,s}(g = qur(\theta);\varphi) = \begin{cases} |y_1/y_2|^s \varphi(y_1 a)\boldsymbol{e}_\infty(k\theta) & \text{if } u = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in K_0(M), \\ 0 & \text{if } u \in K_0(1)\setminus K_0(M_0), \end{cases}$$

where $g = qur(\theta)$ with $q = \left(\begin{smallmatrix} y_1 & x \\ & y_2 \end{smallmatrix}\right) \in B(\boldsymbol{A}_F)$, $u \in K_0(1)$ and $r(\theta) \in K_\infty$.

We define two *Eisenstein series*

$$E_k^M(g,s;\varphi) = L^M(2s,\varphi) \sum_{\gamma \in B(F)\backslash \boldsymbol{GL}_2(F)} H_{k,s}(\gamma g;\varphi),$$

$$\widetilde{E}_k^M(g,s;\varphi) = W_M E_k^M(g,s;\varphi) = \varphi^{-1}(\det g\pi_M) E_k^M(g W_M, s;\varphi),$$

which are absolutely convergent for $\operatorname{Re} s > 1$ and continue analytically for all s to (nonholomorphic) automorphic forms of level M, parallel weight k and character φ (for E) and φ^{-1} (for $\widetilde{E}$). Here W_M is as in (1.4.3). The superscript M will be omitted from the notation when its value is clear from context.

3.2. ***Fourier expansion of the Eisenstein measure.*** We specialise to the case where k is odd, $M = \Delta P$ with $(\Delta, P) = 1$ and $\varphi = \varepsilon\phi$ with $\varepsilon = \varepsilon_{E/F}$ and ϕ a character of conductor dividing P, trivial at infinity (in particular, we have $\varphi_v(-1) = \varepsilon_v(-1)\phi_v(-1) = -1$ as required). We assume that Δ is squarefree. For $\delta \mid \Delta$, we compute[21] the Whittaker coefficients (see Section 1.2; we suppress φ, M and k from the notation) of $\widetilde{E}^{(\delta)}$:

$$c_s^\delta(\alpha, y) = D_F^{-1/2} \int_{\boldsymbol{A}_F/F} \widetilde{E}\left(\left(\begin{smallmatrix} y & x \\ & 1 \end{smallmatrix}\right) W_\delta, s\right)\boldsymbol{e}(-\alpha x)\,dx$$

[21] See [Zhang 2001a, §3.5, §6.2].

for $\alpha \in F$ and δ dividing Δ; since $c_s(\alpha, y) = c_s(1, \alpha y)$ for $\alpha \neq 0$, we can restrict to $\alpha = 0$ or 1. The choice of uniformisers π_v at $v \mid \delta$ implicit in the above formula is made so that $\varepsilon(\pi_v) = 1$ to save some notation.

Proposition 3.2.1. *In the case just described, the Whittaker coefficients $c_s^\delta(\alpha, y)$ of the Eisenstein series $\widetilde{E}_k^{(\delta)}(g, s; \varphi)$ are given by*

$$c_s^\delta(0, y) = \begin{cases} \dfrac{1}{D_F^{1/2} \boldsymbol{N}(\Delta P)^s} \varepsilon\phi(y)|y|^{1-s} V_{k,s}(0)^{[F:\mathbb{Q}]} L^{(P)}(2s-1, \varepsilon\phi) & \text{if } \delta = 1, \\ 0 & \text{if } \delta \neq 1, \end{cases}$$

$$c_s^\delta(1, y) = \begin{cases} \dfrac{\boldsymbol{N}(\delta)^{s-1/2}}{D_F^{1/2} \boldsymbol{N}(\Delta P)^s} \varepsilon\phi(y)|y|^{1-s} \kappa(\delta)\phi(\delta)\varepsilon_\delta(y) \\ \quad \cdot \phi_\delta(y^\infty d_F)|y\pi_\delta d_F|_\delta^{2s-1} \sigma_{k,s,\varepsilon\phi}(y) & \text{if } y d_F \text{ is integral}, \\ 0 & \text{otherwise}, \end{cases}$$

where $\kappa(\delta) = \prod_{v|\delta} \kappa(v)$ with $\kappa(v)$ as in (2.1.1) *and*

$$\sigma_{k,s,\varphi}(y) = \prod_{v \nmid \Delta M \infty} \sum_{n=0}^{v(yd_F)} \varphi_v(\pi_v)^n |\pi_v|^{n(2s-1)} \prod_{v|\infty} V_{k,s}(y_v)$$

with

$$V_{k,s}(y) = \int_{\mathbb{R}} \frac{e^{-2\pi i y x}}{(x^2+1)^{s-k/2}(x+i)^k}\, dx.$$

Proof. We use the Bruhat decomposition

$$\boldsymbol{GL}_2(F) = B(F) \coprod B(F) w N(F)$$

with $w = \left(\begin{smallmatrix} & -1 \\ 1 & \end{smallmatrix}\right)$ and the unipotent subgroup $N(F) \cong F$ via $N(F) \ni \left(\begin{smallmatrix} 1 & x \\ & 1 \end{smallmatrix}\right) \leftarrow\!\shortmid x \in F$ to get

$$\begin{aligned} \varepsilon\phi(y)\phi(\pi_{M/\delta}) c_s^\delta(\alpha, y) &= L(2s, \varphi) D_F^{-1/2} \int_{\boldsymbol{A}_F/F} H_s\left(\begin{pmatrix} y & x \\ & 1 \end{pmatrix} W_{M/\delta}\right) \boldsymbol{e}(-\alpha x)\, dx \\ &\quad + L(2s, \varphi) D_F^{-1/2} \int_{\boldsymbol{A}_F} H_s\left(w \begin{pmatrix} y & x \\ & 1 \end{pmatrix} W_{M/\delta}\right) \boldsymbol{e}(-\alpha x)\, dx. \end{aligned}$$

At any place $v \mid M/\delta$, we have the decomposition

$$\begin{pmatrix} y_v & x_v \\ & 1 \end{pmatrix} W_{M/\delta, v} = \begin{pmatrix} y_v & \pi_v x_v \\ & \pi_v \end{pmatrix} \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}$$

so that the first summand is always zero.

For the second integral, we use the identity

$$w \begin{pmatrix} y & x \\ & 1 \end{pmatrix} = \begin{pmatrix} 1 & \\ & y \end{pmatrix} \begin{pmatrix} & -1 \\ 1 & xy^{-1} \end{pmatrix}$$

and the substitution $x \to xy$ to get

$$\int_{\boldsymbol{A}_F} H_s\left(w\begin{pmatrix} y & x \\ & 1\end{pmatrix} W_{M/\delta}\right)\boldsymbol{e}(-\alpha x)\,dx = |y|^{1-s}\prod_v V_s^{M/\delta}(\alpha_v y_v),$$

where for $y \in F_v$

$$V_s^M(y) = \int_{F_v} H_s\left(\begin{pmatrix} & -1 \\ 1 & x\end{pmatrix} W_{M,v}\right)\boldsymbol{e}(-xy)\,dx. \tag{3.2.1}$$

Archimedean places. See [Zhang 2001a, Proposition 3.5.2].

Nonarchimedean places $v \nmid M/\delta$. If v is a finite place, we have $\left(\begin{smallmatrix} & -1 \\ 1 & x\end{smallmatrix}\right) \in \boldsymbol{GL}_2(\mathbb{O}_{F,v})$ if $x \in \mathbb{O}_{F,v}$, and otherwise we have the decomposition

$$\begin{pmatrix} & -1 \\ 1 & x\end{pmatrix} = \begin{pmatrix} x^{-1} & -1 \\ & x\end{pmatrix}\begin{pmatrix} 1 & \\ x^{-1} & 1\end{pmatrix}.$$

Therefore,

$$H_{s,v}\begin{pmatrix} & -1 \\ 1 & x\end{pmatrix} = \begin{cases} \bar{\varphi}_v(x)|x|^{-2s} & \text{if } v(x) \le -1, \\ 1 & \text{if } v \nmid M \text{ and } v(x) \ge 0, \\ 0 & \text{if } v \mid \delta \text{ and } v(x) \ge 0. \end{cases} \tag{3.2.2}$$

The case $v \nmid M$. We deduce that

$$\begin{aligned} V_s^{M/\delta}(y) &= \int_{\mathbb{O}_{F,v}} \boldsymbol{e}(-xy)\,dx + \sum_{n\ge 1}\int_{\mathbb{O}_{F,v}^\times} \bar{\varphi}_v(x\pi_v^{-n})|x\pi_v^{-n}|^{-2s}\boldsymbol{e}(-xy\pi_v^{-n})\,d(\pi_v^{-n}x) \\ &= \mathbb{1}[y \in d_F^{-1}] + \sum_{n\ge 1}\varphi_v(\pi_v)^n|\pi_v|^{n(2s-1)}\int_{\mathbb{O}_{F,v}^\times}\boldsymbol{e}(-xy\pi_v^{-n})\,dx. \end{aligned}$$

The integral evaluates to $1-|\pi_v|$ if $v(yd_F) \ge n$, to $-|\pi_v|$ if $v(yd_F) = n-1$ and to 0 otherwise. Therefore, we have $V_s^M(y) = 0$ unless $v(yd_F) \ge 0$, in which case if $y \ne 0$

$$\begin{aligned} V_s^{M/\delta}(y) &= 1 + (1-|\pi_v|)\sum_{n=1}^{v(yd_F)}(\varphi_v(\pi_v)|\pi_v|^{2s-1})^n - |\pi_v|(\varphi_v(\pi_v)|\pi_v|^{2s-1})^{v(yd_f)+1} \\ &= (1-\varphi_v(\pi_v)|\pi_v|^{2s})\sum_{n=0}^{v(yd_F)}\varphi_v(\pi_v)^n|\pi_v|^{n(2s-1)} \\ &= L_v(2s,\varphi)^{-1}\sum_{n=0}^{v(yd_F)}\varphi_v(\pi_v)^n|\pi_v|^{n(2s-1)}, \end{aligned}$$

whereas for $y = 0$ we have

$$\begin{aligned} V_s^{M/\delta}(0) &= 1 + (1 - |\pi_v|) \sum_{n=1}^{\infty} (\varphi_v(\pi_v)|\pi_v|^{2s-1})^n \\ &= 1 + (1 - |\pi_v|)(1 - \varphi_v(\pi_v)|\pi_v|^{2s-1})^{-1}(1 - \varphi_v(\pi_v)|\pi_v|^{2s}) \\ &= L_v(2s, \varphi)^{-1} L_v(2s - 1, \varphi). \end{aligned}$$

The case $v \mid \delta$. Again by (3.2.2), we find

$$V_s^{M/\delta}(y) = \sum_{n \geq 1} \int_{\mathbb{O}_{F,v}^\times} \bar{\varphi}_v(x\pi_v^{-n})|x\pi_v^{-n}|^{-(2s-1)} \boldsymbol{e}(-xy\pi_v^{-n})\, dx.$$

All the integrals vanish except the one with $n = v(yd_F) + 1$, which gives

$$\varepsilon_v(y\pi_v^n)\phi_v(y\pi_{d_F,v}\pi_v)|y\pi_{d_F,v}\pi_v|^{2s-1}|\pi_v|^{1/2}\kappa(v);$$

therefore, we have[22]

$$V_s^{M/\delta}(y) = \varepsilon_v(y)\phi_v(y\pi_{d_F,v}\pi_v)|y\pi_{d_F,v}\pi_v|^{2s-1}|\pi_v|^{1/2}\kappa(v)$$

if $y \neq 0$ and $v(yd_F) \geq 0$ and $V_s(y) = 0$ otherwise. In particular, we see that if $\delta \neq 1$ then $V_s(0) = c_s(0, y) = 0$.

Places $v \mid M/\delta$. For

$$w \begin{pmatrix} 1 & x \\ & 1 \end{pmatrix} \begin{pmatrix} & 1 \\ -\pi_v^{v(M)} & \end{pmatrix} = \begin{pmatrix} \pi_v^{v(M)} & \\ -x\pi_v^{v(M)} & 1 \end{pmatrix},$$

we have the decompositions

$$\begin{aligned} \begin{pmatrix} \pi_v^{v(M)} & \\ -x\pi_v^{v(M)} & 1 \end{pmatrix} &= \begin{pmatrix} -\pi_v^{v(M)} & \\ & 1 \end{pmatrix} \begin{pmatrix} -1 & \\ -x\pi_v^{v(M)} & 1 \end{pmatrix} \\ &= \begin{pmatrix} x^{-1} & -\pi_v^{v(M)} \\ & x\pi_v^{v(M)} \end{pmatrix} \begin{pmatrix} & 1 \\ -1 & x^{-1}\pi_v^{-v(M)} \end{pmatrix}; \end{aligned}$$

for $v(x) \geq 0$, we use the first one to find

$$H_s \begin{pmatrix} -\pi_v^{v(M)} & \\ x\pi_v^{v(M)} & -1 \end{pmatrix} = \varphi_v(\pi_v)^{v(M)}|\pi_v^{v(M)}|^s;$$

for $v(x) < 0$, the second decomposition shows that the integrand vanishes. We conclude that

$$V_s^{M/\delta}(y) = \begin{cases} \varphi_v(\pi_v)^{v(M)}|\pi_v^{v(M)}|^s & \text{if } v(yd_F) \geq 0, \\ 0 & \text{otherwise.} \end{cases}$$

The final formula follows from these computations. □

[22] Recall that we always choose π_v so that $\varepsilon_v(\pi_v) = 1$.

We specialise to the case $s = \frac{1}{2}$ and consider the rescaled holomorphic Eisenstein series:[23]

$$\boldsymbol{E}_{k,\varepsilon\phi}^{\Delta P}(g) = \frac{D_F^{1/2}\boldsymbol{N}(\Delta P)^{1/2}}{(-2\pi i)^{[F:\mathbb{Q}]}} E_k^{\Delta P}(g, \tfrac{1}{2}; \varepsilon\phi),$$

$$\widetilde{\boldsymbol{E}}_{k,\varepsilon\phi}^{\Delta P}(g) = \frac{D_F^{1/2}\boldsymbol{N}(\Delta P)^{1/2}}{(-2\pi i)^{[F:\mathbb{Q}]}} \widetilde{E}_k^{\Delta P}(g, \tfrac{1}{2}; \varepsilon\phi).$$

We further specialise to the case $k = 1$.

Corollary 3.2.2. *The Eisenstein series $\widetilde{\boldsymbol{E}}_{1,\varepsilon\phi}^{\Delta P}$ belongs to $M_1(K_1(\Delta P), \varepsilon\phi^{-1})$. The Whittaker–Fourier coefficients of $\widetilde{\boldsymbol{E}}_{\varepsilon\phi}^{(\delta)} = \widetilde{\boldsymbol{E}}_{1,\varepsilon\phi}^{\Delta P,(\delta)}$ for $\delta \mid \Delta$ are given by*

$$\tilde{a}^0(\widetilde{\boldsymbol{E}}_{\varepsilon\phi}^{(\delta)}, y) = \varepsilon\phi(y)|y|^{1/2}\frac{L^{(p)}(0, \varepsilon\phi)}{2^g}$$

if $\delta = 1$ and $\tilde{a}^0(\widetilde{\boldsymbol{E}}_{\varepsilon\phi}^{(\delta)}, y) = 0$ otherwise, and

$$c^\delta(y) = \tilde{a}(\widetilde{\boldsymbol{E}}_{\varepsilon\phi}^{(\delta)}, y) = \varepsilon\phi(y)|y|^{1/2}\kappa(\delta)\phi(\delta)\varepsilon_\delta\phi_\delta(y^\infty d_F)\sigma_{\varepsilon\phi}(y^\infty d_F),$$

where for any integral ideal m of $\mathbb{O}_F[\Delta^{-1}P^{-1}]$

$$\sigma_{\varepsilon\phi}(m) = \sum_{d|m} \varepsilon\phi(d),$$

the sum likewise running over integral ideals of $\mathbb{O}_F[\Delta^{-1}P^{-1}]$.

(If m is an integral ideal of $\mathbb{O}_F$ prime to P, then $\sigma_{\varepsilon\mathbb{1}}(m) = r(m)$.)

Proof. This follows from Proposition 3.2.1 together with the evaluation

$$V_{1,1/2}(t) = \begin{cases} 0 & \text{if } t < 0, \\ -\pi i & \text{if } t = 0, \\ -2\pi i e^{-2\pi t} & \text{if } t > 0, \end{cases}$$

which can be found in [Gross and Zagier 1986, Proposition IV.3.3 (a) and (d)] (for the case $t = 0$, this is deduced from (a) of [loc. cit.] using $\lim_{s\to 0}\Gamma(2s)/\Gamma(s) = \frac{1}{2}$). □

Definition 3.2.3. Let F'_∞ be the maximal abelian extension of F unramified outside p, and let $\mathcal{G}'_F = \mathrm{Gal}(F'_\infty/F)$. We define the *Eisenstein (pseudo)measure*[24] $\widetilde{\boldsymbol{E}}_\varepsilon$ on $\mathcal{G}'_F$ by

$$\widetilde{\boldsymbol{E}}_\varepsilon(\phi) = \widetilde{\boldsymbol{E}}_{\varepsilon\phi}^{\Delta P} = \frac{D_F^{1/2}\boldsymbol{N}(\Delta P)^{1/2}}{(-2\pi i)^g}\widetilde{E}_{\varepsilon\phi}^{\Delta P}$$

[23] Notice that these series do not depend on the ideal P but only on its support.

[24] We *do not* need to assume that Δ is squarefree when making the definition. See after the definition for the meaning of the term pseudomeasure.

for any character ϕ of $\mathcal{G}'_F$ of conductor dividing P (it does not depend on the choice of P once we require P to satisfy $v \mid P \leftrightarrow v \mid p$). We denote with the same name the distribution induced on the group $\mathcal{G}'$ of Section 2.3 by

$$\widetilde{\boldsymbol{E}}_\varepsilon(\mathcal{W}) = \widetilde{\boldsymbol{E}}_\varepsilon(\mathcal{W}|_{F_{\mathbb{A}}^\times}).$$

It has values in $\boldsymbol{M}_1(K_1(N\Delta), \varepsilon)$ and is defined over $\mathbb{Q}_p$.

To prove the soundness of the definition, it is easy to see that the nonzero Fourier coefficients interpolate to a measure on $\mathcal{G}'_F$, that is, an element of $\mathbb{Z}_p[\![\mathcal{G}'_F]\!]$. The L-values giving the constant term interpolate to the Deligne–Ribet p-adic L-function [1980]; it is a pseudomeasure in the sense of Serre [1978], that is, an element of the total quotient ring of $\mathbb{Z}_p[\![\mathcal{G}'_F]\!]$ with denominators of a particularly simple form.

4. The p-adic L-function

4.1. ***Rankin–Selberg convolution.*** Let f and g be modular forms of common level M, weights k_f and k_g and characters ψ_f and ψ_g, respectively. We define a normalised Dirichlet series

$$D^M(f, g, s) = L^M(2s - 1, \psi_f\psi_g) \sum_m a(f, m)a(g, m)\boldsymbol{N}m^{-s},$$

where the imprimitive L-function $L^M(s, \varphi)$ of a Hecke character φ of conductor dividing M is as in (3.1.1).

When f and g are primitive forms of level N_f and N_g (that is, normalised new eigenforms at those levels), for a prime $\wp \nmid N_f$, denote by $\gamma_\wp^{(1)}(f)$ and $\gamma_\wp^{(2)}(f)$ the two roots of the $\wp$-th Hecke polynomial of f

$$P_{\wp, f}(X) = X^2 - a(f, \wp)X + \psi_f(\wp)\boldsymbol{N}\wp^{k_f - 1}$$

and by $\gamma_\wp^{(1)}(g)$ and $\gamma_\wp^{(2)}(g)$ the analogous quantities for g. Then the degree-4 Rankin–Selberg L-function $L(f \times g, s)$ with unramified Euler factors at $\wp$ given by

$$\prod_{i,j=1}^{2} \left(1 - \gamma_\wp^{(i)}(f)\gamma_\wp^{(j)}(g)\boldsymbol{N}\wp^{-s}\right)^{-1}$$

equals the above Dirichlet series

$$L(f \times g, s) = D^{N_f N_g}(f, g, s)$$

if N_f and N_g are coprime.

Suppose now for simplicity that $k_f = 2$, $k_g = 1$ and f is a cusp form (not necessarily primitive). The Rankin–Selberg convolution method[25] gives

$$\langle f^\rho, gE_1^M(s;\psi_f\psi_g)\rangle_M = D_F^{s+1}\left[\frac{\Gamma(s+\frac{1}{2})}{(4\pi)^{s+1/2}}\right]^{[F:\mathbb{Q}]} D^M(f\times g, s+\tfrac{1}{2}), \quad (4.1.1)$$

where $\langle\cdot,\cdot\rangle_M$ is the Petersson inner product (1.1.2).

4.2. ***Convoluted measure and the p-adic L-function in the ordinary case.*** Consider the convolution pseudomeasure $\Theta * \widetilde{\boldsymbol{E}}_{\varepsilon,N}$ on $\mathcal{G}'$ defined by $\Theta * \widetilde{\boldsymbol{E}}_{\varepsilon,N}(\mathcal{W}) = \Theta(\mathcal{W})\widetilde{\boldsymbol{E}}_{\varepsilon,N}(\overline{\mathcal{W}})$ for any character $\mathcal{W}\colon \mathcal{G}' \to \mathbb{Z}_p^\times$, where $\widetilde{\boldsymbol{E}}_{\varepsilon,N} = [N]\widetilde{\boldsymbol{E}}_\varepsilon$. We deduce from it the (pseudo)measure

$$\Phi(\mathcal{W}) = \mathrm{Tr}_\Delta[\Theta * \widetilde{\boldsymbol{E}}_{\varepsilon,N}(\overline{\mathcal{W}})] = \mathrm{Tr}_\Delta[\Theta(\mathcal{W})\cdot[N]\widetilde{\boldsymbol{E}}_\varepsilon(\overline{\mathcal{W}})] \quad (4.2.1)$$

on $\mathcal{G}'$, which is a kind of p-adic kernel of the Rankin–Selberg L-function as will be made precise below. It is valued in $\boldsymbol{M}_2(K_0(N),\mathbb{C}_p)$. Notice that, while $\Phi(\mathcal{W})$, like $\widetilde{\boldsymbol{E}}_{\varepsilon,N}$, is not a measure, we can see that, for any $\wp \mid p$,

$$U_\wp\Phi(\mathcal{W})$$

is. Indeed its Fourier coefficients are the Fourier coefficients of $\Phi(\mathcal{W})$ at ideals m divisible by $\wp$ and hence sums of coefficients of the theta and Eisenstein series at pairs of ideals $(m_1 = nm, m_2 = (1-n)m)$ for some $n \in F$; since the coefficients of the theta series are zero at ideals m_1 divisible by $\wp$, only those pairs (m_1, m_2) with m_1 and m_2 both prime to $\wp$ contribute. In particular, the constant term of the Eisenstein series does not contribute to the Fourier expansion of $U_\wp\Phi$, which therefore belongs to $\mathbb{Z}_p[\![\mathcal{G}']\!]\otimes \boldsymbol{S}_2(K_0(N),\mathbb{C}_p)$.

Thanks to this discussion and the identity $l_{f_\alpha} = \alpha_\wp^{-1} l_{f_\alpha}\circ U_\wp$, the following definition makes sense:

Definition 4.2.1. The p-adic Rankin–Selberg L-function is an element of $\mathbb{O}_L[\![\mathcal{G}]\!]\otimes L$ that is defined by

$$L_p(f_E,\mathcal{W}) = D_F^{-2}H_p(f)l_{f_\alpha}(\Phi(\mathcal{W}))$$

for any character $\mathcal{W}\colon \mathcal{G}\to\mathbb{O}_L^\times$, where

$$H_p(f) = \prod_{\wp\mid p}\left(1-\frac{1}{\alpha_\wp(f)^2}\right)\left(1-\frac{\boldsymbol{N}\wp}{\alpha_\wp(f)^2}\right). \quad (4.2.2)$$

[25] See [Shimura 1978] or [Jacquet 1972, Chapter V] for general treatments; our setting and normalisations are the same as in [Zhang 2001a, Lemma 6.1.3] (where g is a specific form, but the same calculation works in general to prove (4.1.1)).

Functional equation. The p-adic L-function admits a functional equation; we prove it in the case of anticyclotomic characters, which is the only one we shall need.

Proposition 4.2.2. *Suppose $\mathcal{W}$ is an anticyclotomic character of $\mathcal{G}$, i.e., $\mathcal{W}|_{F_{\mathbf{A}}^\times} = 1$. Then there are functional equations for the p-adic L-function*

$$L_p(f_E)(\mathcal{W}) = (-1)^g \varepsilon(N) L_p(\mathcal{W}) \tag{4.2.3}$$

and for the analytic kernel

$$\Phi(\mathcal{W}) = (-1)^g \varepsilon(N) \Phi(\mathcal{W}). \tag{4.2.4}$$

In particular, if $\varepsilon(N) = (-1)^{g-1}$, we have

$$\Phi(\mathcal{W}) = L_p(f_E)(\mathcal{W}) = 0.$$

Proof. The functional equation for L_p is implied by the functional equation for Φ. We prove the latter by comparing the coefficients on both sides. From (4.5.1) below,[26] the coefficients of $\Phi(\mathcal{W})$ are given by

$$b(m) = \sum_{\delta|\Delta} \sum_{\substack{n \in F \\ 0<n<1}} \varepsilon_\delta((n-1)n) r_{\mathcal{W}^-}((1-n)m\delta) \sigma_{\varepsilon\mathbb{1}}(nm/N).$$

(We use the notation $\mathbb{1}$ for the character of ideals defined by $\mathbb{1}(m) = 1$ if $(m, p) = 1$ and $\mathbb{1}(m) = 0$ otherwise.) We rewrite this as $b(m) = \sum_{\delta,n} b_{\delta,n}(m)$ with, using $\varepsilon_\delta(x) = \varepsilon^\delta(x)$ for $x \in F^\times$ and writing in columns to highlight the factors,

$$\begin{aligned}
b_{\delta,n}(m) = \varepsilon_\delta(-1) &&= (-1)^g \varepsilon_{\Delta/\delta}(-1) \\
&\cdot \varepsilon_{\Delta/\delta}((1-n)m) \varepsilon_{\Delta/\delta}(nm) && \cdot \varepsilon_{\Delta/\delta}((1-n)m) \varepsilon_{\Delta/\delta}(nm) \\
&\cdot \varepsilon^\Delta((1-n)m) r_{\mathcal{W}}((1-n)m\delta) && \cdot r_{\mathcal{W}}((1-n)m\Delta/\delta) \\
&\cdot \varepsilon(N) && \cdot \varepsilon(N) \\
&\cdot \varepsilon^\Delta(nm/N) \sigma_{\varepsilon\mathbb{1}}(nm/N) && \cdot \sigma_{\varepsilon\mathbb{1}}(nm/N) \qquad = (-1)^g \varepsilon(N) b_{\Delta/\delta,n}.
\end{aligned}$$

Here we have used the following facts. In the first line, $\varepsilon_\Delta(-1) = \varepsilon_\infty(-1) = (-1)^g$. In the third line, we have that $r_{\mathcal{W}}(m) = 1$ if m is divisible only by ramified primes in E since in that case $m = \mathfrak{m}^2$ is a square and $\mathcal{W}(\mathfrak{m})^2 = \mathcal{W}(m) = 1$ — this implies $\mathcal{W}(\mathfrak{m}) = \pm 1$ and hence $\mathcal{W}(\mathfrak{m}) = 1$ since $\mathcal{W}$, which is a character of $\mathcal{G} \cong \mathbb{Z}_p^{1+g+\delta}$, has values in $1 + p\mathbb{Z}_p$. Finally, in the third and fifth lines, one can observe that, if $q = \sigma_{\varepsilon\mathbb{1}}$ or $q = r$, then $\varepsilon^\Delta(m) q(m) = q(m)$; indeed this is trivial if $\varepsilon^\Delta(m) = 1$ while both sides are zero if $\varepsilon^\Delta(m) = -1$. □

[26] Which does not use the present result. The formula (4.5.1) is stated in the case when the anticyclotomic part $\mathcal{W}^- = \mathbb{1}$, but the very same calculation gives the result in general.

4.3. ***Interpolation property.*** We manipulate the definition to show that the p-adic L-function $L_p(f_E)(\mathcal{W})$ of Definition 4.2.1 interpolates the special values of the complex Rankin–Selberg L-function $L(f_E, \mathcal{W}, s) = L(f \times \Theta(\mathcal{W}), s)$ defined in the introduction.

We will need a few technical lemmas.

Lemma 4.3.1. *Let P be an ideal of $\mathbb{O}_F$ such that $v \mid P$ if and only if $v \mid p$. We have*

$$\langle W_{NP} f_\alpha^\rho, f_\alpha \rangle_{NP} = \alpha_P(f)(-1)^g \tau(f) H_p(f) \langle f, f \rangle_N$$

with $H_p(f)$ as in (4.2.2) *and*

$$\alpha_P(f) = \prod_{\wp \mid p} \alpha_\wp(f)^{v_\wp(P)}.$$

Proof. When $P = P_0 := \prod_{\wp \mid p} \wp$, this is the direct generalisation of [Perrin-Riou 1988, Lemme 27], and it is proved in the same way. In general, we can write $P = P_0 P_1$, and then

$$W_{NP} f_\alpha^\rho = \boldsymbol{N}(P_1)[P_1] W_{NP_0} f_\alpha^\rho.$$

Observing that $[\wp]$ is the adjoint of $U_\wp$ for the Petersson inner product and that $\boldsymbol{N}(P_1) = [K_0(NP) : K_0(NP_0)]$, we deduce

$$\begin{aligned}\langle W_{NP} f_\alpha^\rho \rangle_{NP} &= [K_0(NP) : K_0(NP_0)] \langle W_{NP_0} f_\alpha^\rho, U(P_1) f_\alpha \rangle_{NP} \\ &= \alpha_{P_1} \langle W_{NP_0} f_\alpha^\rho, f_\alpha \rangle_{NP_0}.\end{aligned}$$

The lemma then follows from this and the special case $P = P_0$. □

For the next lemma, let M and N be coprime; then we define the space of *weakly N-old* forms of level NM to be the subspace of $M_k(K_1(MN))$ spanned by forms $f = [d] f'$ for some $d \mid N$ and some modular form f' of level $N'M$ with $N' \mid d^{-1}N$. (This is often simply called the space of N-old forms, but we have reserved that name for the span of forms $[d] f'$ as above with $d \neq 1$.)

Lemma 4.3.2. *For a character φ of conductor dividing M and an ideal N prime to M, let $E_\varphi^M = E_1^M(g, \frac{1}{2}; \varphi)$ and $\widetilde{E}_\varphi^M = W_M E_\varphi^M$. We have*

$$W_M[N] \widetilde{E}_\varphi^M = E_\varphi^{MN} + E^{\mathrm{old}}$$

where the form E^{old} is weakly old at N (in particular, E^{old} is orthogonal to newforms of exact level N and so is its product with any other form of level prime to N).

Proof. It is easy to see that $W_M[N] \widetilde{E}_\varphi^M = [N] E_\varphi^M$. Then we are reduced to showing

$$[N] E_\varphi^M = E_\varphi^{MN} + E^{\mathrm{old}}.$$

In fact, we have more generally and more precisely that

$$\boldsymbol{N}(N)^{s-}E_\varphi^M\left(g\begin{pmatrix}1 & \\ & \pi_M\end{pmatrix},s\right)=\sum_{d|N}\frac{\varphi(d)}{\boldsymbol{N}(d)^{2s}}E_\varphi^{MN/d}(g,s);$$

this is [Zhang 2001a, Lemma 6.1.4] with ε replaced by φ. The lemma then holds with

$$E^{\mathrm{old}}=\sum_{d|N,\,d\neq 1}\frac{\varphi(d)}{\boldsymbol{N}(d)}E_\varphi^{MN/d}. \qquad \square$$

Lemma 4.3.3. *With notation as in Section 4.1, we have*

$$D([\Delta]f,\Theta(\mathcal{W}),1)=\mathcal{W}(\mathfrak{D})D(f,\Theta(\mathcal{W}),1).$$

The proof is as in [Nekovář 1995, §I.5.9].

Theorem 4.3.4. *Let $\mathcal{W}\colon\mathcal{G}'\to\overline{\mathbb{Q}}^\times$ be a finite-order character of conductor $\mathfrak{f}$ divisible only by primes above p. Then we have*

$$L_p(f_E)(\mathcal{W})=\frac{\mathcal{W}(d_F^{(p)})\tau(\overline{\mathcal{W}})\boldsymbol{N}(\Delta(\mathcal{W}))^{1/2}V_p(f,\mathcal{W})\overline{\mathcal{W}}(\Delta)}{\alpha_{\mathfrak{N}(\mathfrak{f}(\mathcal{W}))}(f)\Omega_f}L(f_E,\overline{\mathcal{W}},1),$$

where $\Omega_f=(8\pi^2)^g\langle f,f\rangle_N$, $\tau(\overline{\mathcal{W}})$ is as in Lemma 2.4.3 and

$$V_p(f,\overline{\mathcal{W}})=\prod_{\wp|p}\prod_{\mathfrak{p}|\wp}\left(1-\frac{\overline{\mathcal{W}}(\mathfrak{p})}{\alpha_\wp(f)}\right). \tag{4.3.1}$$

Proof. Denote $P=\mathfrak{N}(\mathfrak{f}(\mathcal{W}))$, $\Delta(\mathcal{W})=\Delta P$ and $\phi=\mathcal{W}|_{\mathbb{A}_F^\times}$. We suppose that $\mathcal{W}$ is ramified at all places $v\mid p$ (in this case, we have $V_p(f,\mathcal{W})=1$). Then the result follows from the definition and the following calculation:

$$\begin{aligned}
l_{f_\alpha}(\Phi(\mathcal{W}))&=\frac{\langle W_{NP}f_\alpha^\rho,\mathrm{Tr}_\Delta[\Theta(\mathcal{W})\widetilde{\boldsymbol{E}}_{\varepsilon,N}(\overline{\mathcal{W}})]\rangle_{NP}}{\langle W_{NP}f_\alpha^\rho,f_\alpha\rangle_{NP}}\\
&\overset{\text{Lemma 4.3.1}}{=}\frac{\langle W_{N\Delta}f_\alpha^\rho,W_{\Delta(\mathcal{W})}\Theta(\mathcal{W})W_{\Delta(\mathcal{W})}\widetilde{\boldsymbol{E}}^{\Delta(\mathcal{W})}_{\varepsilon\phi^{-1},N}\rangle_{N\Delta(\mathcal{W})}}{\alpha_P(f)(-1)^g\tau(f)H_p(f)\Omega_f}\\
&\overset{\substack{\text{Lemma 4.3.2}\\ \text{Lemma 2.4.3}}}{=}\frac{(-i)^g\mathcal{W}(d_F^{(p)})\tau(\overline{\mathcal{W}})\overline{\mathcal{W}}(\mathfrak{D})D_E}{\alpha_P(f)(-1)^g\tau(f)H_p(f)\Omega_f}\langle W_N[\Delta]f_\alpha^\rho,\Theta(\overline{\mathcal{W}})\boldsymbol{E}^{N\Delta(\mathcal{W})}_{\varepsilon\phi^{-1}}\rangle_{N\Delta(\mathcal{W})}\\
&=\frac{(-i)^g\mathcal{W}(d_F^{(p)})\tau(\overline{\mathcal{W}})\overline{\mathcal{W}}(\mathfrak{D})}{\alpha_P(f)H_p(f)\Omega_f}\langle[\Delta]f_\alpha^\rho,\Theta(\overline{\mathcal{W}})\boldsymbol{E}^{N\Delta(\mathcal{W})\overline{\mathcal{W}}(\mathfrak{D})}_{\varepsilon\phi^{-1}}\rangle_{N\Delta(\mathcal{W})}\\
&\overset{(4.1.1)}{=}\frac{\mathcal{W}(d_F^{(p)})\tau(\overline{\mathcal{W}})D_F^2\boldsymbol{N}(\Delta(\mathcal{W}))^{1/2}}{\alpha_P(f)H_p(f)\Omega_f}D^{N\Delta(\mathcal{W})}([\Delta]f_\alpha,\Theta(\overline{\mathcal{W}}),1)\\
&\overset{\text{Lemma 4.3.3}}{=}\frac{\mathcal{W}(d_F^{(p)})\tau(\overline{\mathcal{W}})D_F^2\boldsymbol{N}(\Delta(\mathcal{W}))^{1/2}\overline{\mathcal{W}}(\Delta)}{\alpha_P(f)H_p(f)\Omega_f}L(f_E,\overline{\mathcal{W}},1),
\end{aligned}$$

where we have used various results from Section 1.4 and the fact that in our case $f^\rho = f$ as f has trivial character.

The previous calculation goes through in general with $\Delta(\mathcal{W})$ replaced by $\Delta(\mathcal{W})' = \mathrm{lcm}(\Delta(\mathcal{W}), \prod_{\wp|p} \wp)$; then one further needs to compare the imprimitive Dirichlet series $D^{\Delta(\mathcal{W})'}(f_\alpha, \Theta(\overline{\mathcal{W}}, 1))$ with the L-value $L(f_E, \overline{\mathcal{W}}, 1)$. This is done in the same way as in the case of elliptic modular forms [Perrin-Riou 1988, Lemme 2.3 (i), §4.4 (III)].[27] We omit the details since no new phenomena appear in our context and, strictly speaking, we do not need to use the precise form of the interpolation result except in the ramified case (which already determines $L_p(f_E)$ uniquely). □

4.4. ***Factorisation.*** The p-adic analogue of the standard L-function of f has been studied by several authors (Manin, Dabrowski, Dimitrov, etc.). Let $\mathcal{G}_F = \mathrm{Gal}(F_\infty/F)$ where F_∞ is the maximal $\mathbb{Z}_p$-extension of F unramified outside p.

Theorem 4.4.1. *There is a p-adic L-function $L_p(f) \in \mathbb{O}_L[\![\mathcal{G}'_F]\!] \otimes_{\mathbb{O}_L} L$ uniquely determined by the following property: for each finite-order character $\chi : \mathcal{G}_F \to \overline{\mathbb{Q}}^\times$ of conductor $\mathfrak{f}(\chi)$ divisible by all the primes $\wp \mid p$, we have*

$$L_p(f, \chi) = \chi(d_F^{(p)}) \frac{\tau(\overline{\chi}) \boldsymbol{N}(\mathfrak{f}(\chi))^{1/2}}{\alpha_{\mathfrak{f}(\chi)}} \frac{L(f, \overline{\chi}, 1)}{\Omega_f^+}$$

where $\Omega_f^+ \in \mathbb{C}^\times$ is a suitable period and $\tau(\overline{\chi}) = \prod_{v|p} \tau(\overline{\chi}_v)$ with

$$\tau(\overline{\chi}_v) = |\pi_v|^{-c/2} \int_{F_v^\times} \overline{\mathcal{W}}_v(x_v) \boldsymbol{e}_v(-x_v)\, dx_v$$

if $c = v(\mathfrak{f}(\chi))$.

Similarly, we have $L_{p,\varepsilon\alpha}(f_\varepsilon)$ and a period $\Omega_{f_\varepsilon}^+$ satisfying

$$L_{p,\varepsilon\alpha}(f_\varepsilon, \chi) = \chi(d_F^{(p)}) \frac{\tau(\overline{\chi}) \boldsymbol{N}(\mathfrak{f}(\chi))^{1/2}}{\varepsilon(\mathfrak{f}(\chi)) \alpha_{\mathfrak{f}(\chi)}} \frac{L(f_\varepsilon, \overline{\chi}, 1)}{\Omega_{f_\varepsilon}^+}$$

for ramified finite-order characters χ. (In fact, $\varepsilon(\mathfrak{f}(\chi) = 1$ under our assumptions).)

For the proof of the existence of $L_p(f)$, we refer to [Dimitrov 2013]: notice that our $L_p(f, \chi)$ equals $\chi(d_F^{(p)}) L_p(\pi_f, \chi^{-1})$ in [op. cit.], where moreover the notation $\tau(\chi_v)$ refers to *un*normalised Gauss sums. The definition and properties

[27] Notice that, as in [op. cit.], our $\Theta(\mathcal{W})$ is not the primitive theta series when $\mathcal{W}$ is unramified at some $\wp \mid p$; in general, we have

$$\Theta(\mathcal{W}) = \Big(\prod_{\mathfrak{p}|\wp|p} (1 - \boldsymbol{N}(\wp)^{1/2} \mathcal{W}(\mathfrak{p})[\wp]) \Big) \Theta(\mathcal{W})^{\mathrm{prim}}$$

if $\Theta(\mathcal{W})^{\mathrm{prim}}$ is the primitive theta series (i.e., the normalised newform in its representation). This replaces the second-to-last equation of [Perrin-Riou 1988, p. 21], whose $\Theta(\mathcal{W})$ and $\Theta(\mathcal{W}'')$ are our $\Theta(\mathcal{W})^{\mathrm{prim}}$ and $\Theta(\mathcal{W})$, respectively. The factor $V_p(f, \overline{\mathcal{W}})$ comes from the analogue of [Perrin-Riou 1988, Lemme 23].

of the period Ω_f^+ and of a related period Ω_f^- (both of which are a priori defined up to an $M_f^\times$-ambiguity) are given in Section 9 below; here we need $\Omega_f^+\Omega_f^- \sim \Omega_f$ and $\Omega_{f_\varepsilon}^+ \sim D_E^{-1/2}\Omega_f^-$, where $\sim$ denotes equality in $\mathbb{C}^\times/M_f^\times$. Then from the complex factorisation $L(f_E, \chi\circ\mathfrak{N}, s) = L(f,\chi,s)L(f_\varepsilon,\chi,s)$ and the interpolation properties satisfied by each factor, we obtain

$$L_p(f_E,\chi\circ\mathfrak{N}) = \chi(\Delta)^2\frac{\Omega_f^+\Omega_{f_\varepsilon}^+}{D_E^{-1/2}\Omega_f}L_p(f,\chi)L_p(f_\varepsilon,\chi), \tag{4.4.1}$$

where the period factor is in $M_f^\times$ (in particular, it is algebraic).

4.5. ***Fourier expansion of the analytic kernel.*** Consider the restriction of Φ to $\mathcal{G}$, the Galois group of the maximal $\mathbb{Z}_p$-extension of E unramified outside p. Any character $\mathcal{W}$ of $\mathcal{G}$ decomposes uniquely as $\mathcal{W} = \mathcal{W}^+\mathcal{W}^-$ with $(\mathcal{W}^+)^c = \mathcal{W}$ and $(\mathcal{W}^-)^c = \mathcal{W}^{-1}$ (we say that $\mathcal{W}^+$ is cyclotomic and $\mathcal{W}^-$ is anticyclotomic or dihedral). Since we are interested in the case $\varepsilon(N) = (-1)^{g-1}$ in which Φ is zero on the anticyclotomic characters, we study the restriction of Φ to the cyclotomic characters. We can write $\mathcal{W}^+ = \chi\circ\mathfrak{N}$ for a Hecke character $\chi\colon F^\times\backslash F_{\boldsymbol{A}}^\times \to 1+p\mathbb{Z}_p$, and we denote

$$\Theta_\chi = \Theta(\chi\circ\mathfrak{N}), \qquad \Phi_\chi = \Phi(\chi\circ\mathfrak{N}).$$

From now on, we assume that $(\Delta,2)=1$ and all primes $\wp \mid p$ are split in E.

Proposition 4.5.1. *The Fourier coefficients $b(m) = a_p(\Phi_\chi, m)$ of the p-adic modular form Φ_χ are given by*

$$b(m) = \sum_{\substack{n\in F\\ 0<n<1\\ n\in Nm^{-1}\Delta^{-1}}} \chi((1-n)m)\prod_{v\mid\Delta}\left[\mathbb{1}[v(nm)=0] + \varepsilon_v((n-1)n)\chi_v^{-2}(nm\wp_v/N)\right] \cdot r((1-n)m\Delta)\sigma_{\varepsilon\chi^{-2}}(nm/N).$$

Proof. By (1.4.6), the Fourier coefficient $b(m)$ of $\Phi_\chi = \mathrm{Tr}_\Delta[\Theta_\chi \widetilde{\boldsymbol{E}}_{\varepsilon\chi^2,N}]$ is given by

$$b(m) = \sum_{\delta\mid\Delta} b^\delta(m\delta)$$

with

$$\begin{aligned} b^\delta(m) = a(\Phi_\chi^{(\delta)}, m) &= |y|^{-1}\tilde{a}(\Phi_\chi^{(\delta)}, y)\\ &= |y|^{-1}\sum_{n\in F}\tilde{a}(\Theta_\chi^{(\delta)}, (1-n)y)\tilde{a}(\widetilde{\boldsymbol{E}}^{(\delta)}_{\varepsilon\chi^{-2},N}, ny)\\ &= |y|^{-1}\sum_{n\in F}\tilde{a}(\Theta_\chi^{(\delta)}, (1-n)y)\tilde{a}(\widetilde{\boldsymbol{E}}^{(\delta)}_{\varepsilon\chi^{-2}}, ny/\pi_N) \end{aligned}$$

if $y\in F_{\boldsymbol{A}}^\times$ satisfies $y_\infty > 0$ and $y^\infty d_F = m$.

Then by Proposition 2.5.1 and Corollary 3.2.2, we have[28]

$$b(m) = \sum_{\delta|\Delta} \sum_{\substack{n\in F\\ 0<n<1}} \varepsilon_\delta((n-1)n)\chi^{-1}(\delta)\chi((1-n)m\delta)\chi_\delta^{-2}(nm\delta/N) \cdot r((1-n)m\delta)\sigma_{\varepsilon\chi^{-2}}(nm/N). \quad (4.5.1)$$

We interchange the two sums and notice that the term corresponding to δ and n is nonzero only if $n \in Nm^{-1}\Delta^{-1}$ and $\delta_0 \mid \delta$, where

$$\delta_0 = \delta_0(n) = \prod_{\substack{v|\Delta\\ v(nm)=-1}} \wp_v$$

($\wp_v$ being the prime corresponding to v). Now for each n, we can rewrite the sum over δ (omitting the factor $\chi((1-n)m)$ and those on the second line of (4.5.1), which do not actually depend on δ) as

$$\varepsilon_{\delta_0}((n-1)n)\chi_{\delta_0}^{-2}(nm\delta_0/N) \sum_{\delta'|\Delta/\delta_0} \varepsilon_{\delta'}((n-1)n)\chi_{\delta'}^{-2}(nm\delta'/N)$$
$$= \prod_{v|\delta_0} \varepsilon_{\delta'}((n-1)n)\chi_v^{-2}(nm\wp_v) \prod_{v|\Delta/\delta_0} [1+\varepsilon_v((n-1)n)\chi_v^{-2}(nm\wp_v)].$$

The asserted formula follows. □

Remark 4.5.2. If $v(nm) = -1$, then $(n-1)\pi_m\pi_v \equiv n\pi_m\pi_v$ in $(\mathbb{O}_{F,v}/\pi_v\mathbb{O}_{F,v})^\times$ so that we actually have

$$\varepsilon_v((n-1)n) = \varepsilon_v((n-1)\pi_m\pi_v)\varepsilon_v(n\pi_m\pi_v) = 1.$$

We can now compute the Fourier coefficients of the analytic kernel giving the central derivative of the p-adic L-function in the cyclotomic direction. To this end, let

$$\nu\colon \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to 1 + p\mathbb{Z}_p \subset \mathbb{Q}_p^\times.$$

Since l_{f_α} is continuous, we have

$$\frac{d}{ds} L_p(f_E, \nu^s \circ \mathfrak{N}) = \frac{d}{ds} l_{f_\alpha}(\Phi(s)) = l_{f_\alpha}\left(\frac{d}{ds}\Phi(s)\right).$$

In particular, $L'_{p;\nu\circ\mathfrak{N}}(f_E, \mathbb{1}) = l_{f_\alpha}(\Phi'(0))$.

Let $\ell_F = \frac{d}{ds}\big|_{s=0}\nu^s\colon F^\times \setminus F_{\boldsymbol{A}^\infty}^\times \to \mathbb{Q}_p$ be the p-adic logarithm associated with ν.

Proposition 4.5.3. *Assume that* $\varepsilon(N) = (-1)^{g-1}$. *Then* $\Phi(0) = 0$ *and the Fourier coefficients* $b'(m)$ *of*

$$\Phi'_\nu = \Phi'(0) = \frac{d}{ds}\bigg|_{s=0} \Phi_{\nu^s}$$

[28] Recall that $\kappa(v)^2 = \varepsilon_v(-1)$.

are nonzero only for m integral and nonzero, in which case

$$b'(m) = \sum_v b'_v(m)$$

with the sum running over all finite places v of F and $b'_v(m)$ given for $\left(\prod_{\wp|p} \wp\right) \mid m$ by the following:

(1) *If $v = \wp$ is inert in E, then*

$$b'_v(m) = \sum_{\substack{n \in Nm^{-1}\Delta^{-1} \\ (p,nm)=1 \\ \varepsilon_v((n-1)n)=1\ \forall v|\Delta \\ 0<n<1}} 2^{\omega_\Delta(n)} r((1-n)m\Delta) r(nm\Delta/N\wp)(v(nm/N)+1)\ell_{F,v}(\pi_v),$$

where

$$\omega_\Delta(n) = \#\{v \mid (\Delta, nm\Delta)\}.$$

(2) *If $v = \wp \mid \Delta$ is ramified in E, then*

$$b'_v(m) = \sum_{\substack{n \in Nm^{-1}\Delta^{-1} \\ (p,nm)=1 \\ \varepsilon_v((n-1)n)=-1 \\ \varepsilon_w((n-1)n)=1\ \forall v\neq w|\Delta \\ 0<n<1}} 2^{\omega_\Delta(n)} r((1-n)m\Delta) r(nm\Delta/N)(v(nm)+1)\ell_{F,v}(\pi_v).$$

(3) *If v is split in E, then*

$$b'_v(m) = 0.$$

Proof. The vanishing of $\Phi(0) = \Phi_{\mathbb{1}}$ follows from the functional equation (4.2.4) and the sign assumption.

By Proposition 4.5.1, the Fourier coefficient $b_s(m)$ of $\Phi(s) = \Phi_{\nu^s}$ can be expressed as $b_s(m) = \sum_{n\in F} b_{n,s}(m)$ with

$$b_{n,s}(m) = \nu^s((1-n)m) r((1-n)m\Delta) \prod_{v\nmid p\infty} \sigma^n_{s,v}(m/N)$$

where, using Remark 4.5.2,

$$\sigma^n_{s,v}(m) = \begin{cases} \dfrac{1-\varepsilon(nm\wp)v(nm\wp)^{-2s}}{1-\varepsilon(\wp)v(\wp)^{-2s}} & \text{if } v = \wp \nmid \Delta, \\ 1+\varepsilon_v(n(n-1))v(nm\wp)^{-2s} & \text{if } v = \wp \mid \Delta \text{ and } v(nm) = 0, \\ v(nm\wp)^{-2s} & \text{if } v = \wp \mid \Delta \text{ and } v(nm) = -1. \end{cases}$$

Then $b'(m) = \sum_n b'_n(m) = \sum_n \sum_v b'_{n,v}(m)$ with $\sum_n b'_{n,v}(m) = b_v(m)$, and $b'_n(m)$ can be nonzero only if exactly one of the factors $\sigma^n_{s,v}$ vanishes at $s = 0$. If this happens for the place v_0, then the set over which n ranges accounts for the positivity and integrality conditions and the nonvanishing conditions at other places, whereas the condition $(p, nm) = 1$ results from observing that $\lim_{s\to 0} \nu^s(a) = \mathbb{1}[(p, a) = 1]$.

The values of $b'_{n,v}$ can then be determined in each case from the above expressions. For v ramified, this is straightforward. For $v = \wp$ inert, notice that if $v(nm/N)$ is odd then $r(nm\Delta/N\wp) = r((nm\Delta/N)^{(\wp)})$, where the superscript denotes prime-to-$\wp$ part, whereas if $v(nm/N)$ is even then $\sigma^n_{0,v}(m/N)$ does not vanish so (n, v) does not contribute to $b'(m)$ and indeed $r(nm/N\wp) = 0$. □

Part II. Heights

5. p-adic heights and Arakelov theory

By the work of many authors (Schneider, Perrin-Riou, Mazur and Tate, Coleman and Gross, Zarhin, Nekovář, etc.), there are p-adic height pairings on the Mordell–Weil group of an abelian variety defined over a number field. In this section, we first recall (Sections 5.1–5.2) a definition of the height pairing as a sum of local symbols following [Zarhin 1990; Nekovář 1993] and explain how it induces a pairing on degree-0 divisors on curves. In Sections 5.3–5.4, we explain how p-adic Arakelov theory allows us to extend the height pairing for curves to a pairing on divisors of any degree.

5.1. ***Local symbols.*** Let A be an abelian variety of dimension g over a local field E_v and $A^\vee$ its dual abelian variety, and let $V = V_pA = T_pA \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ be the rational Tate module of A, a continuous $\mathrm{Gal}(\bar{E}/E)$-representation.[29] Let $\ell_v \colon E_v^\times \to \mathbb{Q}_p$ be a homomorphism; we call ℓ a *local p-adic logarithm* and assume that it is ramified, that is, $\ell_v \colon E_v^\times \to \mathbb{Q}_p$ does not vanish identically on $\mathcal{O}_{E,v}^\times$. Let $D_{\mathrm{dR}}(V_v)$ be the filtered $\mathbb{Q}_p$-vector spaces attached to V_v by the theory of Fontaine. The comparison theorem identifies $D_{\mathrm{dR}}(V_v)$ with $H^1_{\mathrm{dR}}(A^\vee/E_v)$, equipped with the Hodge filtration; it is also identified with the filtered Dieudonné module of the special fibre of the p-divisible group of A (after an extension of scalars if E_v is ramified over $\mathbb{Q}_p$ [Fontaine 1982]). Let L be a finite extension of the coefficient field $\mathbb{Q}_p$, and if $v \mid p$, let $W_v \subset D_{\mathrm{dR}}(V_v) \otimes L$ be a splitting of the Hodge filtration, that is, a complementary subspace to $\Omega^1(A^\vee/E_v) \otimes L \subset D_{\mathrm{dR}}(V_v) \otimes L$, which is isotropic[30] for the cup product. When V_v is ordinary, there is a canonical choice for W_v, the "unit root" subspace (see, e.g., [Iovita 2000] for a nice discussion).

We proceed to define pairings, called *local Néron symbols*,[31]

$$\langle \cdot, \cdot \rangle_{v,W} \colon (\mathcal{D}_0(A)(E_v) \times Z_0(A)^0(E_v))_e \to L$$

[29] Nekovář [1993] defines height pairings for Galois representations in much greater generality than described here.

[30] The isotropy condition ensures that the resulting height pairing is symmetric [Nekovář 1993, Theorem 4.1.1 (4)]

[31] The notation is a bit abusive: the subscript W is meant to recall that the local pairing depends on the choice of W_v when $v \mid p$; when $v \nmid p$, it has no meaning. Although the symbol also depends on ℓ, we will usually omit it from the notation.

on the subset of pairs with disjoint supports in the product of the group $\mathcal{D}_0(A)(E_v)$ of divisors algebraically equivalent to 0 defined over E_v and the group $Z_0(A)^0(E_v)$ of 0-cycles of degree 0 defined over E_v.

Let $\mathscr{A}/\mathcal{O}_{E,v}$ and $\mathscr{A}^\vee/\mathcal{O}_{E,v}$ be the Néron models of A and $A^\vee$, and let $\mathscr{A}^0$ be the identity component of $\mathscr{A}$. The rational equivalence class $[D]$ of $D \in \mathcal{D}_0(A)(E_v)$ defines a point in $A^\vee(E_v) = \mathscr{A}^\vee(\mathcal{O}_{E,v}) = \mathrm{Ext}^1_{\mathrm{fppf}}(\mathscr{A}^0, \boldsymbol{G}_m)$ and hence an extension

$$1 \to \boldsymbol{G}_m \to \mathcal{Y}_{[D]} \to \mathscr{A}^0 \to 1$$

of abelian fppf sheaves on $\mathcal{O}_{E,v}$, and $\mathcal{Y}_{[D]}$ is represented by a smooth commutative group scheme. On the generic fibre, $\mathcal{Y}_{[D]} \otimes E_v$ can be identified with the complement Y_D of the zero section in the total space of the line bundle $\mathcal{O}(D)$ on A, and thus, the extension admits a section

$$s_D \colon A \setminus |D| \to Y_D,$$

which is canonical up to scaling.

Suppose we are given a morphism $\ell_{v,D,W}$ that makes the following diagram commute:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathcal{O}_{E,v}^\times \hat{\otimes} L & \longrightarrow & \mathcal{Y}_{[D]}(\mathcal{O}_{E,v}) \hat{\otimes} L & \longrightarrow & \mathscr{A}^0(\mathcal{O}_{E,v}) \hat{\otimes} L & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \| & & \\
0 & \longrightarrow & E_v^\times \hat{\otimes} L & \longrightarrow & Y_D(E_v) \hat{\otimes} L & \longrightarrow & A(E_v) \hat{\otimes} L & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \ell_v} & & \downarrow{\scriptstyle \ell_{v,D,W}} & & & & \\
 & & L & = & L & & & &
\end{array}$$

Then we can define the local pairing by

$$\langle D, z \rangle_{v,W} = \ell_{v,D,W}(s_D(z)), \tag{5.1.1}$$

where s_D is extended to the divisor z in the obvious way. Notice that, since z has degree 0, this is well-defined independently of the scaling ambiguity in s_D.

When $v \nmid p$, the logarithm ℓ_v vanishes on $\mathcal{O}_{E,v}^\times$ for topological reasons and we can uniquely extend it to an $\ell_{v,D}$ as in the above diagram by requiring its restriction to $\mathcal{Y}_{[D]}(\mathcal{O}_{E,v})$ to be trivial. When $v \mid p$, given the splitting W_v, one can construct a section

$$s_{v,D,W} \colon A(E_v) \hat{\otimes} L \to Y_D(E_v) \hat{\otimes} L$$

and define the extension $\ell_{v,D,W}$ by requiring it to be trivial on the image of $s_{v,D,W}$. The standard construction is explained, e.g., in [Kobayashi 2014, §3.2]. In the ordinary case, when W_v is chosen to be the unit root subspace, the crucial properties of the (canonical) local symbol are the last two in Proposition 5.1.2 below; in this case, the construction rests on the following result (see [Schneider 1985] or [Nekovář 1993, §6.9]):

Lemma 5.1.1. *Let $E_{v,\infty}$ be a totally ramified $\mathbb{Z}_p$-extension of E_v, and denote by $E_{v,n}$ its n-th layer. Let $e \in \mathrm{End}(A) \otimes \overline{\mathbb{Q}}$ be an idempotent. Assume that eV is ordinary as a Galois representation. Then the module of* universal norms

$$U(eA(E_v)) = \bigcap_n \mathrm{Im}[\mathrm{Tr}_{E_{v,n}/E_v} : eA(E_{v,n}) \to eA(E_v)]$$

has finite index in $eA(E_v)$.

Proposition 5.1.2. *The p-adic local symbol*

$$\langle \cdot, \cdot \rangle_v = \langle \cdot, \cdot \rangle_{v,W} : (\mathcal{D}_0(A)(E_v) \times Z_0(A)^0(E_v))_e \to L$$

defined by (5.1.1) *has the following properties* (*valid whenever they make sense*):

(1) *It is bilinear.*

(2) *If $h \in E_v(A)$ is a rational function, we have*

$$\langle (h), z \rangle_v = \ell_v(h(z))$$

where, if $z = \sum n_P P$, $h(z) = \prod h(P)^{n_P}$.

(3) *If $\phi : A \to A$ is a finite endomorphism, we have*

$$\langle \phi^* D, z \rangle_v = \langle D, \phi_* z \rangle_v.$$

(4) *For any $D \in \mathcal{D}_0(A)(E_v)$ and $x_0 \in A(E_v) \setminus |D|$ the map from $A(E_v) \setminus |D| \to L$ defined by*

$$x \mapsto \langle D, x - x_0 \rangle_v$$

is continuous.

(5) (compatibility) *Let E'_w/E_v be a finite extension. If $D \in \mathcal{D}_0(A)(E'_w)$ and $z \in Z_0(A)^0(E_v)$, we have*

$$\langle \mathrm{Tr}_{E'_w/E_v}(D'), z \rangle_v = \langle D', z \rangle_w$$

where $\langle \cdot, \cdot \rangle_w$ is the local pairing associated with $\ell_w = \ell_v \circ N_{E_w/E_v}$ and (if $v \mid p$) the splitting W_w is induced from W_v.

(6) (boundedness) *If $v \mid p$, let $E^\ell_{v,\infty} = \bigcup_n E^\ell_{v,n}$ be the ramified*[32] *$\mathbb{Z}_p$-extension of E_v determined by the isomorphism*

$$E_v^\times \supset \mathrm{Ker}(\ell_v) \cong \mathrm{Gal}(E^\ell_{v,\infty}/E) \subset \mathrm{Gal}(E_v^{\mathrm{ab}}/E)$$

induced from class field theory. In the ordinary situation of Lemma 5.1.1, if eW_v is the unit root subspace of eV, there is a nonzero constant $c \in \mathbb{Z}_p$ such that

$$\langle D, z \rangle_{v,n} \in c^{-1} \ell_w(E^{\ell,\times}_{v,n})$$

if $D \in e\mathcal{D}_0(A)(E_{v,n})$, $z \in eZ_0(A)^0(E_{v,n})$ and $\langle \cdot, \cdot \rangle_{v,n}$ is the local pairing associated with the extension $E^\ell_{v,n}/E_v$ as in (5).

If $v \nmid p$, the local symbol is characterised by properties (1)–(4).

[32] Recall that we choose ℓ_w to be ramified.

We refer to [Nekovář 1995, §II.1; Kobayashi 2013, §4.2] and references therein for the proof and more details on the construction. See also Proposition 5.4.1 below.

5.2. ***The p-adic height pairing.*** Let A be an abelian variety over a number field E. Let $\ell\colon E^\times \setminus E_{\boldsymbol{A}}^\times \to \mathbb{Q}_p$ be a homomorphism (which we call a *global p-adic logarithm*) whose restrictions $\ell_v = \ell|_{E_v^\times}$ are ramified for all $v \mid p$. Let W_v be Hodge splittings at the places $v \mid p$ as in Section 5.1. Then we can define a height pairing

$$\langle \cdot, \cdot \rangle\colon A^\vee(E) \times A(E) \to L$$

as the sum of local height pairings

$$\langle x, y \rangle = \sum_v \langle \tilde{x}, \tilde{y} \rangle_v,$$

where $\tilde{x}$ is a divisor on A whose class in $A^\vee(E) \cong \mathrm{Pic}^0(A)$ is x and $\tilde{y} = \sum n_P[P]$ is a 0-cycle of degree 0 on A with support disjoint from the support of $\tilde{x}$, which satisfies $\sum n_P P = y$. The result is independent of the choices of $\tilde{x}$ and $\tilde{y}$.

Let X be a (proper, smooth) curve over E of genus $g \geq 1$, together with a degree-1 divisor class defined over E inducing an embedding

$$\iota\colon X \hookrightarrow J(X)$$

into its Albanese variety $J(X)$.[33] Let $\mathrm{Div}(X)$ be the group of divisors on X, $\mathrm{Div}^0(X)$ the subgroup of degree-0 divisors and similarly $\mathrm{CH}(X) = \mathrm{Div}(X)/\sim$ and $\mathrm{CH}(X)_0 = \mathrm{Div}^0(X)/\sim$, the Chow group of 0-cycles modulo rational equivalence and its subgroup of degree-0 elements. Then, given a p-adic logarithm and Hodge splittings for $V_p J(X)$, we can define local and global pairings on degree-0 divisors on X (denoted with a subscript X) from the above pairings on $J(X)$ (here denoted with a subscript $J(X)$). Let D_1 and D_2 be divisors of degree 0 on X defined over E and with disjoint support. The morphism ι induces an isomorphism $\iota^*\colon \mathrm{Pic}^0 J(X) \cong \mathrm{Pic}^0(X)$; hence, we can pick an algebraically trivial divisor D_1' on $J(X)$ satisfying $D_1 = \iota^* D_1' + (h)$ for some rational function $h \in E(X)$. If D_1' is chosen so that its support is disjoint from the support of $\iota_* D_2$ and the support of (h) is disjoint from the support of D_2, we can define

$$\langle D_1, D_2 \rangle_{v,X} = -\langle D_1', \iota_* D_2 \rangle_{v,J(X)} - \ell_v(h(D_2))$$

and

$$\langle D_1, D_2 \rangle_X = \sum_v \langle D_1, D_2 \rangle_{v,X}.$$

[33] In our applications, we only have a rational divisor class, inducing a compatible system of maps $\iota_{E'}\colon X(E') \otimes \mathbb{Q} \to J(X)(E') \otimes \mathbb{Q}$ for E' a finite extension of E such that, for some integer n, $(n\iota_{E'})_{E'}$ is induced from an E-morphism. This causes no extra difficulties.

The latter pairing descends to a *height pairing* on divisor classes

$$\langle \cdot, \cdot \rangle \colon \mathrm{CH}(X)_0 \times \mathrm{CH}(X)_0 \to L.$$

There are various conventions in the literature for the normalisation of the signs of height pairings. Our choices are the same as those of [Kobayashi 2013, §4.3], whose discussion we have followed and to which we refer for a comparison with other authors' choices.

5.3. ***p*-adic Arakelov theory: local aspects.** Here and in Section 5.4, we summarise the main results of Besser [2005], who develops the p-adic analogue of classical Arakelov theory.

Metrised line bundles. Let X_v be a proper smooth variety over the finite extension E_v of $\mathbb{Q}_p$, and fix a ramified local p-adic logarithm $\ell_v \colon E_v^\times \to \mathbb{Q}_p$, which we extend to $\overline{\mathbb{Q}}_p^\times$ by $\ell_v|_{E_v'^\times} = \ell_v \circ N_{E_v'/E_v}$ for any finite extension E_v'/E_v.

A *metrised line bundle* $\widehat{\mathscr{L}} = (\mathscr{L}, \log_{\mathscr{L}})$ on X_v is a line bundle on X_v together with a choice of a *log function* $\log_{\mathscr{L}}$ on the total space of $\mathscr{L}$ minus the zero section (which will also be viewed as a function on the nonzero sections of $\mathscr{L}$). A log function is the analogue in the p-adic theory of the logarithm of a metric on the sections of a line bundle on a Riemann surface. It is a Coleman function having a certain analytic property[34] and the following algebraic property. If the p-adic logarithm ℓ_v factors as

$$\ell_v = t_v \circ \log_v \tag{5.3.1}$$

for some $\log_v \colon E_v^\times \to E_v$ and some $\mathbb{Q}_p$-linear $t_v \colon E_v \to \mathbb{Q}_p$, then for any nonzero section s of $\mathscr{L}_v$ and rational function $f \in E(X_v)$, we have

$$\log_{\mathscr{L},v}(fs) = \log_v(f) + \log_{\mathscr{L},v}(s). \tag{5.3.2}$$

Adding a constant to a log function produces a new log function; this operation is called *scaling*.

One can define a notion of $\bar{\partial}\partial$-operator on Coleman functions and attach to any log function $\log_{\mathscr{L}}$ on $\mathscr{L}$ its *curvature* $\bar{\partial}\partial \log_{\mathscr{L}} \in H^1_{\mathrm{dR}}(X_v) \otimes \Omega^1(X_v)$; its cup product is the first Chern class of $\mathscr{L}$.

Log functions on a pair of line bundles induce in the obvious way a log function on their tensor product and similarly for the dual of a line bundle. If $\pi \colon X_v \to Y_v$ is a morphism, then a log function on a line bundle on Y_v induces in the obvious way a log function on the pullback line bundle on X_v. If moreover π is a finite Galois cover with Galois group G and $\mathscr{L}$ is a line bundle on X_v with log function $\log_{\mathscr{L}}$

[34] For which we refer to [Besser 2005, Definition 4.1].

and associated curvature β, then the norm line bundle $N_\pi \mathscr{L}$ on Y_v with stalks

$$(N_\pi \mathscr{L})_y = \bigotimes_{x \mapsto y} \mathscr{L}_x^{\otimes e(x|y)}$$

has an obvious candidate log function $N_\pi \log_{\mathscr{L}}$ obtained by tensor product. A delicate point is that it is not automatic that the latter is a genuine log function (i.e., it satisfies the analytic property alluded to above); see [Besser 2005, Proposition 4.8] for a sufficient condition.

The canonical Green function. Now let X_v/E_v be a curve of genus $g \geq 1$ with good reduction above p. Choose a splitting $W_v \subset H^1_{\mathrm{dR}}(X_v) \otimes L$ of the Hodge filtration as in Section 5.1, which we use to identify $W_v \cong \Omega^1(X_v)^\vee$; we then define a canonical element

$$\mu_{X_v} = \frac{1}{g}\mathrm{id} \in \mathrm{End}\,\Omega^1(X_v) \cong W_v \otimes \Omega^1(X_v)$$

and similarly for the self-product $X_v \times X_v$ (denoting by π_1 and π_2 the projections)

$$\Phi = \begin{pmatrix} 1/g & -1 \\ -1 & 1/g \end{pmatrix} \in \mathrm{End}(\pi_1^*\Omega^1(X_v) \oplus \pi_2^*\Omega^1(X_v)) \hookrightarrow H^1_{\mathrm{dR}}(X_v \times X_v) \otimes \Omega^1(X_v \otimes X_v).$$

The first Chern class of Φ is the class of the diagonal $\Delta \subset X_v \times X_v$.

Let s_Δ denote the canonical section of the line bundle $\mathcal{O}(\Delta)$ on $X_v \times X_v$. Given any log function $\log_{\mathcal{O}(\Delta)}$ on $\mathcal{O}(\Delta)$ with curvature Φ, we can consider the function G on $X_v \times X_v$ given by

$$G(P, Q) = \log_{\mathcal{O}(\Delta)}(s_\Delta)(P, Q).$$

It is a Coleman function with singularities along Δ; we call G a *Green function* for X_v.

A Green function G induces a log function on any line bundle $\mathcal{O}(D)$ on X_v by

$$\log_{\mathcal{O}(D)}(s_D)(Q) = \sum n_i G(P_i, Q)$$

if $D = \sum n_i P_i$ and s_D is the canonical section of $\mathcal{O}(D)$. A log function $\log_{\mathscr{L}}$ on the line bundle $\mathscr{L}$ and the resulting metrised line bundle $(\mathscr{L}, \log_{\mathscr{L}})$ are called *admissible* with respect to G if, for one (equivalently, any) nonzero rational section s of $\mathscr{L}$, the difference $\log_{\mathscr{L}}(s) - \log_{\mathrm{div}(s)}$ is a constant. Such a constant is denoted by $\iota_{\log_{\mathscr{L}}}(s)$ or $\iota_{\log_v}(s)$ in the case of the trivial line bundle with the log function $\log_v$. It is the analogue of the integral of the norm of s. It follows easily from the definitions that any isomorphism of admissible metrised line bundles is an isometry up to scaling.

Let ω_{X_v} be the canonical sheaf on X_v. The canonical isomorphism $\omega_{X_v} \cong \Delta^*\mathcal{O}(-\Delta)$ gives another way to induce from G a log function $\log^G_{\omega_{X_v}}$ on ω_{X_v}, namely by pullback (and the resulting metrised line bundle has curvature $(2g-2)\mu_{X_v}$).

The requirement that this log function be admissible, together with a symmetry condition, leads to an almost unique choice of G.

Proposition 5.3.1 [Besser 2005, Theorem 5.10]. *There exists a unique-up-to-constant symmetric Green function G with associated curvature Φ such that $(\omega_{X_v}, \log^G_{\omega_{X_v}})$ is an admissible metrised line bundle with respect to G.*

In the following, we will arbitrarily fix the constant implied by the proposition. In our context, the canonical Green function thus determined is, in a suitable sense, defined over E_v [Besser 2005, Proposition 8.1].

5.4. ***p-adic Arakelov theory: global aspects.*** Let E be a number field with ring of integers $\mathcal{O}_E$. Let $\mathscr{X}/\mathcal{O}_E$ be an arithmetic surface with generic fibre X; that is, $\mathscr{X} \to \mathcal{O}_E$ is a proper regular relative curve and $\mathscr{X} \otimes_{\mathcal{O}_E} E = X$. We assume that $\mathscr{X}$ has *good reduction* at all places $v \mid p$, and denote $X_v = \mathscr{X} \otimes E_v$. Fix choices of a ramified p-adic logarithm ℓ and Hodge splittings W_v as in Section 5.3.

Arakelov line bundles and divisors. An *Arakelov line bundle* on $\mathscr{X}$ is a pair

$$\widehat{\mathscr{L}} = (\mathscr{L}, (\log_{\mathscr{L}_v})_{v|p})$$

consisting of a line bundle $\mathscr{L}$ on $\mathscr{X}$ together with admissible (with respect to the Green functions of Proposition 5.3.1) log functions $\log_{\mathscr{L}_v}$ on $\mathscr{L}_v = \mathscr{L}|_{X_v}$. We denote by $\mathrm{Pic}^{\mathrm{Ar}}(\mathscr{X})$ the group of isometry classes of Arakelov line bundles on $\mathscr{X}$.

The group $\mathrm{Div}^{\mathrm{Ar}}(\mathscr{X})$ of *Arakelov divisors* on $\mathscr{X}$ is the group of formal combinations

$$D = D_{\mathrm{fin}} + D_\infty$$

where D_{fin} is a divisor on $\mathscr{X}$ and $D_\infty = \sum_{v|p} \lambda_v X_v$ is a sum with coefficients $\lambda_v \in E_v$ of formal symbols X_v for each place $v \mid p$ of E. To an Arakelov line bundle $\widehat{\mathscr{L}}$ and a nonzero rational section s of $\mathscr{L}$, we associate the Arakelov divisor

$$\widehat{\mathrm{div}}(s) = (s)_{\mathrm{fin}} + (s)_\infty$$

where $(s)_{\mathrm{fin}}$ is the usual divisor of s and $(s)_\infty = \sum_{v|p} \iota_{\log_{\mathscr{L}_v}}(s_v) X_v$. The group $\mathrm{Prin}^{\mathrm{Ar}}(\mathscr{X})$ of *principal* Arakelov divisors on $\mathscr{X}$ is the group generated by the $\widehat{\mathrm{div}}(h)$ for $h \in E(\mathscr{X})^\times$. The Arakelov Chow group of $\mathscr{X}$ is

$$\mathrm{CH}^{\mathrm{Ar}}(\mathscr{X}) = \mathrm{Div}^{\mathrm{Ar}}(\mathscr{X}) / \mathrm{Prin}^{\mathrm{Ar}}(\mathscr{X}),$$

and we have an isomorphism

$$\mathrm{Pic}^{\mathrm{Ar}}(\mathscr{X}) \cong \mathrm{CH}^{\mathrm{Ar}}(\mathscr{X})$$

given by $\widehat{\mathscr{L}} \to [\widehat{\mathrm{div}}(s)]$ for any rational section s of $\mathscr{L}$.

The p-adic Arakelov pairing. Most important for us is the existence of a pairing on $\mathrm{CH}^{\mathrm{Ar}}(\mathscr{X})$, extending the p-adic height pairing of divisors of Section 5.2. Let $(\cdot,\cdot)_v$ denote the ($\mathbb{Z}$-valued) intersection pairing of cycles on $\mathscr{X}_v$ with disjoint support.

Proposition 5.4.1 [Besser 2005]. *Let $\mathscr{X}/\mathcal{O}_E$ be an arithmetic surface with good reduction above p. For any choice of ramified p-adic logarithm $\ell\colon E_{\boldsymbol{A}}^\times/E^\times \to \mathbb{Q}_p$ and Hodge splittings $(W_v)_{v|p}$ as above, there is a symmetric bilinear paring*[35]

$$\langle\cdot,\cdot\rangle^{\mathrm{Ar}}\colon \mathrm{CH}^{\mathrm{Ar}}(\mathscr{X})\times\mathrm{CH}^{\mathrm{Ar}}(\mathscr{X})\to L$$

satisfying:

(1) *If D_1 and D_2 are finite and of degree 0 on the generic fibre and one of them has degree 0 on each special fibre of $\mathscr{X}$, then*

$$\langle D_1, D_2\rangle^{\mathrm{Ar}} = \langle D_{1,E}, D_{2,E}\rangle,$$

where $D_{i,E}\in \mathrm{Div}^0(X)$ is the generic fibre of D_i and $\langle\cdot,\cdot\rangle$ denotes the height pairing of Proposition 5.1.2 associated with the same choices of ℓ and W_v.

(2) *If $D_{1,\mathrm{fin}}$ and $D_{2,\mathrm{fin}}$ have disjoint supports on the generic fibre, then*

$$\langle D_1, D_2\rangle^{\mathrm{Ar}} = \sum_v \langle D_1, D_2\rangle_v^{\mathrm{Ar}},$$

where the sum runs over all finite places of E, and the local Arakelov pairings are defined by

$$\langle D_1, D_2\rangle_v^{\mathrm{Ar}} = (D_1, D_2)_v \ell_v(\pi_v)$$

for $v\nmid p$ and below for $v\mid p$.

If moreover we are in the situation of (1), *then for each place v, we have*

$$\langle D_1, D_2\rangle_v^{\mathrm{Ar}} = \langle D_{1,E}, D_{2,E}\rangle_v.$$

(3) *In the situation of* (2), *if moreover $D_1 = \widehat{\mathrm{div}}(h)$ is the Arakelov divisor of a rational function h, then*

$$\langle D_1, D_2\rangle_v^{\mathrm{Ar}} = \ell_v(h(D_{2,\mathrm{fin}}))$$

for all places v.

For completeness, we give the description of the local pairing at $v\mid p$ of divisors with disjoint supports. If $\ell_v = t_v\circ\log_v$ as in (5.3.1) and G_v is the Green function on $X_v\times X_v$, we have $\langle D, X_w\rangle_v^{\mathrm{Ar}} = 0$ if $v\neq w$, $\langle X_v, X_v\rangle_v^{\mathrm{Ar}} = 0$, $\langle D, \lambda_v X_v\rangle_v^{\mathrm{Ar}} = (\deg D_E) t_v(\lambda_v)$ and, if D_1 and D_2 are finite divisors with images $D_{1,v} = \sum n_i P_i$ and $D_{2,v} = \sum m_j Q_j$ in X_v,

$$\langle D_1, D_2\rangle_v^{\mathrm{Ar}} = \sum_{i,j} n_i m_j t_v(G_v(P_i, Q_j)).$$

[35] The notation of [Besser 2005] is $D_1\cdot D_2$ for $\langle D_1, D_2\rangle^{\mathrm{Ar}}$.

In fact, in [Besser 2005], it is proved directly that the global Arakelov pairing and its local components at p coincide with the global and local height pairings of [Coleman and Gross 1989]. The latter coincide with the Zarhin–Nekovář pairings by [Besser 2004].

6. Heegner points on Shimura curves

In this section, we describe our Shimura curve and construct Heegner points on it, following [Zhang 2001a, §1–§2], to which we refer for the details (see also [Zhang 2001b, §5] and [Carayol 1986] for the original source of many results on Shimura curves). We go back to our usual notation, so F is a totally real number field of degree g, N is an ideal of $\mathbb{O}_F$, E is a CM extension of F of discriminant Δ coprime to $2Np$ and ε is its associated Hecke character.

6.1. ***Shimura curves.*** Let B be a quaternion algebra over F that is ramified at all but one infinite place. Then we can choose an isomorphism $B\otimes\mathbb{R}\cong M_2(\mathbb{R})\oplus \boldsymbol{H}^{g-1}$, where $\boldsymbol{H}$ is the division algebra of Hamilton quaternions. There is an action of $B^\times$ on $\mathfrak{H}^\pm=\mathbb{C}\setminus\mathbb{R}$ by Möbius transformations via the map $B^\times\to \boldsymbol{GL}_2(\mathbb{R})$ induced from the above isomorphism. For each open subgroup K of $\widehat{B}^\times=(B\otimes_F\widehat{F})^\times$ that is compact modulo $\widehat{F}^\times$, we then have a *Shimura curve*

$$M_K(\mathbb{C})=B^\times\setminus\mathfrak{H}^\pm\times\widehat{B}^\times/K,$$

where $\mathfrak{H}^\pm=\mathbb{C}\setminus\mathbb{R}$. Unlike modular curves, the curves M_K do not have a natural moduli interpretation. However, by [Carayol 1986], $M_K(\mathbb{C})$ has a finite map[36] to another (unitary) Shimura curve $M'_{K'}(\mathbb{C})$ that, if the level K' is small enough, has an interpretation as the moduli space of certain quaternionic abelian varieties. Namely, $M'_{K'}$ parametrises isomorphism classes of abelian varieties of dimension $4[F:\mathbb{Q}]$ with multiplication by the ring of integers $\mathbb{O}_{B'}$ of $B\otimes_F F'$ and some extra structure (a polarisation and a K'-level structure, compatible with the quaternionic multiplication) [Zhang 2001a, Proposition 1.1.5].

We will usually denote a point of $M'_{K'}$ simply by $[A]$, where A is the underlying abelian variety. If K' has maximal components at places dividing m, one can define a notion of an *admissible submodule* D of level m [Zhang 2001a, §1.4.3]: it is an $\mathbb{O}_{B'}$-submodules of $A[m]$ satisfying a certain condition, which ensures that the quotient A/D can be naturally endowed with the extra structure required by the functor $M'_{K'}$. We denote by $[A_D]$ the object whose underlying abelian variety is A/D, with the induced extra structure.

As a consequence of the moduli interpretation, the curve $M_K(\mathbb{C})$ has a canonical model M_K defined over F (it is connected but not, in general, geometrically

[36] That is an embedding if $K\supset\widehat{F}^\times$.

connected) and a proper regular integral model[37] $\mathcal{M}_K$ over $\mathbb{O}_F$; if v is a finite place where B is split, then $\mathcal{M}_K$ is smooth over $\mathbb{O}_{F,v}$ if K_v is a maximal compact subgroup of B_v and K^v is sufficiently small. We denote $\mathcal{M}_{K,v} = \mathcal{M}_K \otimes \mathbb{O}_{F,v}$.

Universal formal group and ordinary points. Assume that the level structure K is maximal at $\wp$. The curve $\mathcal{M}_{K,\wp}$ carries a universal $\wp$-divisible $\mathbb{O}_{B,\wp}$-module $\mathcal{G}$ obtained from the $\wp$-divisible group $\mathcal{A}[\wp^\infty]$ of the universal abelian scheme $\mathcal{A}$ over $\mathcal{M}'_{K',\wp}$. More precisely, choosing an auxiliary quadratic field F' that is split at $\wp$ and an isomorphism $j\colon \mathbb{O}_{F',\wp} \cong \mathbb{O}_{F,\wp} \oplus \mathbb{O}_{F,\wp}$, we have

$$\mathcal{G} = \mathcal{A}[\wp^\infty]^{(2)} = e_2 \mathcal{A}[\wp^\infty],$$

where e_2 is the idempotent in $\mathbb{O}_{F',\wp}$ corresponding to $(0, 1)$ under j.

Assume that B is split at $\wp$. Then we denote by $\mathcal{G}^1$ and $\mathcal{G}^2$ the images under the projectors corresponding to $\left(\begin{smallmatrix}1 & \\ & 0\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}0 & \\ & 1\end{smallmatrix}\right)$ under a fixed isomorphism $B \cong M_2(F_\wp)$; they are isomorphic via the element $\left(\begin{smallmatrix} & 1 \\ -1 & \end{smallmatrix}\right)$.

Let x be a geometric point of the special fibre $\mathcal{M}_{K,\wp}$. Then the $\mathcal{G}^i_x$ are divisible $\mathbb{O}_\wp$-modules of dimension 1 and height 2 and hence isomorphic to either

- the direct sum $\Sigma_1 \oplus F_\wp/\mathbb{O}_{F,\wp}$, where Σ_1 is the unique formal $\mathbb{O}_{F,\wp}$-module of height 1 — in this case, x is called *ordinary* — or
- the unique formal $\mathbb{O}_\wp$-module of dimension 1 and height 2 — in this case, x is called *supersingular*.

Let $M_K(\overline{\mathbb{Q}}_\wp)^{\mathrm{ord}} \subset M_K(\overline{\mathbb{Q}}_\wp)$ be the set of points with ordinary reduction. Then the Frobenius map $\mathrm{Frob}_\wp$ admits a lift

$$\varphi\colon M_K(\overline{F}_\wp)^{\mathrm{ord}} \to M_K(\overline{F}_\wp)^{\mathrm{ord}} \tag{6.1.1}$$

given in the moduli interpretation by $[A] \mapsto [A_{\mathrm{can}(A)}]$, where $\mathrm{can}(A)$ is the *canonical submodule* of A, that is, the sub-$\mathbb{O}_{F,\wp}$-module of $A[\wp]$ in the kernel of multiplication by $\wp$ in the formal group of A.

The order R and the curve X. Assume that $\varepsilon(N) = (-1)^{g-1}$. Then the quaternion algebra $\boldsymbol{B}$ over $\boldsymbol{A}_F$ ramified exactly at all the infinite places and the finite places $v \mid N$ such that $\varepsilon(v) = -1$ is *incoherent*; that is, it does not arise via extension of scalars from a quaternion algebra over F. On the other hand, for any embedding $\tau\colon F \hookrightarrow \mathbb{R}$, there is a *nearby* quaternion algebra $B(\tau)$ defined over F and ramified at τ and the places where $\boldsymbol{B}$ is ramified. Fix any embedding $\rho\colon E \to B(\tau)$, and let R be an order of $\widehat{B} = \widehat{B}(\tau)$ that contains $\rho(\mathbb{O}_E)$ and has discriminant N (this is constructed in [Zhang 2001a, §1.5.1]). Then the curve X over F of interest to us is the

[37] In the modular curve case $F = \mathbb{Q}$, $\varepsilon(v) = 1$ for all $v \mid N$, M_K and $\mathcal{M}_K$ are proper only after the addition of finitely many cusps. (We caution the reader that [Carayol 1986] uses the notation $\mathcal{M}_K$ to denote instead the set of geometrically connected components of M_K.)

(compactification of) the curve M_K defined above for the subgroup $K = \widehat{F}^\times \widehat{R}^\times \subset \widehat{B}$; that is, for each embedding $\tau : F \to \mathbb{C}$, we have

$$X(\mathbb{C}) = B(\tau)^\times \setminus \mathfrak{H}^\pm \times \widehat{B}^\times / \widehat{F}^\times \widehat{R}^\times \cup \{\text{cusps}\}. \tag{6.1.2}$$

The finite set of cusps is nonempty only in the classical case where $F = \mathbb{Q}$ and $\varepsilon(v) = 1$ for all $v \mid N$ so that $X = X_0(N)$. In what follows, we will not burden the notation with the details of this particular case, which poses no additional difficulties and is already treated in the original work of Perrin-Riou [1987].

We denote by $\mathscr{X}$ the canonical model of X over $\mathbb{O}_F$ and by $\mathscr{X}_v$ its base change to $\mathbb{O}_{F,v}$. We also denote by $J(X)$ the Albanese variety of X and by $\mathscr{J}_v$ its Néron model over $\mathbb{O}_{F,v}$.

Hecke correspondences. Let m be an ideal of $\mathbb{O}_F$ that is coprime to the ramification set of B. Let $\gamma_m \in \hat{\mathbb{O}}_B$ be an element with components 1 away from m and such that $\det \gamma_m$ generates m at the places dividing m. Then the Hecke operator $T(m)$ on X is defined by

$$T(m)[(z, g)] = \sum_{\gamma \in K \gamma_m K / K} [(z, g\gamma)]$$

under the complex description (6.1.2). When m divides N, we often denote the operator $T(m)$ by $U(m)$ or U_m.

Let $\boldsymbol{T}'_N$ be the algebra generated by the $T(m)$ for m prime to N. Then by [Zhang 2001a, Theorem 3.2.1], the algebra $\boldsymbol{T}'_N$ is a quotient of the Hecke algebra on Hilbert modular forms $\boldsymbol{T}_N$ (hence, the names $T(m)$ are justified). It acts by correspondences on $X \times X$, and taking Zariski closures of cycles on $\mathscr{X} \times \mathscr{X}$ extends the action to $\mathscr{X}$.

As in the classical case, the Hecke operators $T(m)$ admit a moduli interpretation, after base change to a suitable quadratic extension F' and passing to the curve X'. Namely we have

$$T(m)[A] = \sum_D [A_D],$$

where the sum runs over the admissible submodules of A of level m.

6.2. ***Heegner points.*** The curve X defined above has a distinguished collection of points defined over abelian extensions of E: we briefly describe it, referring the reader to [Zhang 2001a, §2] for more details.

A point y of X is called a *CM point* with multiplication by E if it can be represented by $(x_0, g) \in \mathfrak{H}^+ \times \widehat{B}^\times$ via (6.1.2), where $x_0 \in \mathfrak{H}^+$ is the unique point fixed by $E^\times$. The order

$$\mathrm{End}(y) = g \widehat{R} g^{-1} \cap \rho(E)$$

in $E = \rho(E)$ is defined independently of the choice of g, and

$$\mathrm{End}(y) = \mathbb{O}_E[c] = \mathbb{O}_F + c\mathbb{O}_E$$

for a unique ideal c of $\mathbb{O}_F$ called the *conductor* of y. We say that the point $y = [(x_0, g)]$ has the *positive orientation* if for every finite place v the morphism $t \mapsto g^{-1}\rho(t)g$ is $R_v^\times$-conjugate to ρ in $\mathrm{Hom}(\mathbb{O}_{E,v}, R_v)/R_v^\times$.[38] Let Y_c be the set of positively oriented CM points of conductor c. By the work of Shimura and Taniyama, it is a finite subscheme of X defined over E, and the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/E)$ is given by

$$\sigma[(x_0, g)] = [(x_0, \mathrm{rec}_E(\sigma)g)],$$

where $\mathrm{rec}_E\colon \mathrm{Gal}(\bar{E}/E) \to \mathrm{Gal}(\bar{E}/E)^{\mathrm{ab}} \xrightarrow{\sim} \overline{E^\times} \setminus \widehat{E}^\times$ is the reciprocity map of class field theory. If $y = [(x_0, g)]$ has conductor c, then the action factors through

$$\mathrm{Gal}(H[c]/E) \cong E^\times \setminus \widehat{E}^\times / \widehat{F}^\times \hat{\mathbb{O}}_E[c]^\times,$$

where $H[c]$ is the ring class field of E of conductor c; the action of this group on Y_c is simply transitive.

For each nonzero ideal c of $\mathbb{O}_F$, let $u(c) = [\mathbb{O}_E[c]^\times : \mathbb{O}_F^\times]$ and define the divisor

$$\eta_c = u(c)^{-1} \sum_{y \in Y_c} y. \tag{6.2.1}$$

Let $\eta = \eta_1$. By the above description of the Galois action on CM points, each divisor η_c is defined over E.

A *Heegner point* $y \in X(H)$ is a positively oriented CM point with conductor 1. We can use the embedding $\iota\colon X \to J(X) \otimes \mathbb{Q}$ to define the point

$$[z] = \iota(\eta) = [\eta] - h[\xi] \in J(X)(E) \otimes \mathbb{Q},$$

where h is a number such that $[z]$ has degree 0 in each geometrically connected component of X and $[\xi]$ is the Hodge class of the introduction (see below for more on the Hodge class).

Arakelov Heegner divisors. The Heegner divisor on X can be refined to an Arakelov divisor $\hat{z}$ having degree 0 on each irreducible component of each special fibre. On a suitable Shimura curve $\widetilde{X} \xrightarrow{\pi} X$ of deeper level away from $N\Delta_{E/F}$, we can give an explicit description of the pullback $\hat{\tilde{z}}$ of $\hat{z}$ and of the Hodge class as follows.

As outlined in Section 6.1, after base change to a suitable quadratic extension F' of F, we have an embedding $\widetilde{X} \hookrightarrow \widetilde{X}'$ of $\widetilde{X} = M_{\widetilde{K}}$ into the unitary Shimura curve $\widetilde{X}' = M'_{\widetilde{K}'}$ parametrising abelian varieties of dimension $4g$ with multiplication

[38] This set has two elements only if $v \mid N$ (the other element is called the negative orientation at v); otherwise, it has one element and the condition at v is empty. There is a group of Atkin–Lehner involutions acting transitively on orientation classes.

by $\mathbb{O}_{B'}$ and some extra structure. Then by the Kodaira–Spencer map, we have an isomorphism $\omega_{\widetilde{X}'} \cong \det \mathrm{Lie}\, \mathscr{A}^\vee|_{\widetilde{X}'}$, where $\mathscr{A} \to \widetilde{X}'$ is the universal abelian scheme and the determinant is that of an $\mathbb{O}_{F'}$-module of rank 4 (the structure of $\mathbb{O}_{F'}$-module coming from the multiplication by $\mathbb{O}_{B'}$ on $\mathscr{A}$). This gives a way[39] of extending the line bundle $\omega_{\widetilde{X}'}$ to the integral model $\widetilde{\mathscr{X}}'$ and to a line bundle $\mathscr{L}$ on $\widetilde{\mathscr{X}}$. For each finite place $v \mid p$, we endow $\mathscr{L}|_{\widetilde{X}_v}$ with the canonical log functions $\log_{\mathscr{L},v}$ coming from the description $\mathscr{L}|_{\widetilde{X}_v} = \omega_{\widetilde{X}_v}$ and a fixed choice of Hodge splittings on $\widetilde{X}$. We define $[\hat{\tilde{\xi}}] \in \mathrm{CH}^{\mathrm{Ar}}(\widetilde{\mathscr{X}}) \otimes \mathbb{Q}$ to be the class of $(\mathscr{L}, (\log_{\mathscr{L}})_{v|p})$ divided by its degree, $[\tilde{\xi}]$ to be its finite part and $\hat{\tilde{\xi}}$ to be any Arakelov divisor in its class.

Then the Arakelov Heegner divisor $\hat{\tilde{z}} \in \mathrm{Div}^{\mathrm{Ar}}(\mathscr{X} \otimes \mathbb{O}_E)$ is described by

$$\hat{\tilde{z}} = \hat{\tilde{\eta}} - h\hat{\tilde{\xi}} + Z, \tag{6.2.2}$$

where $\hat{\tilde{\eta}}$ is the Zariski closure in $\mathscr{X} \otimes \mathbb{O}_E$ of the pullback of η to $\widetilde{X}$ and Z is a finite vertical divisor uniquely determined by the requirement that $\hat{\tilde{z}}$ should have degree 0 on each irreducible component of each special fibre.

6.3. ***Hecke action on Heegner points.*** Recall from Section 1.5 the spaces of Fourier coefficients $\mathscr{D}_N \subset \mathscr{S}$, the arithmetic functions $\sigma_1, r \in \mathscr{D}_N$ and the space $\overline{\mathscr{S}} = \mathscr{S}/\mathscr{D}_N$. The action of Hecke operators on the Arakelov Heegner divisor is described as follows.

Proposition 6.3.1. *Let m be an ideal of $\mathbb{O}_F$ coprime to N. We have*:

(1) $T(m)\eta = \sum_{c|m} r(m/c)\eta_c$.

(2) *Let $\eta_c^0 = \sum_{\mathbb{O}_F \neq d|c} \eta_d$, and let $T^0(m)\eta = \sum_{c|m} \varepsilon(c)\eta^0_{m/c}$. Then η and $T^0(m)\eta$ have disjoint support, and if m is prime to $N\Delta$, then $T(m)\eta = T^0(m)\eta + r(m)\eta$.*

(3) $T(m)[\xi] = \sigma_1(m)[\xi]$, *and $m \mapsto T(m)\hat{\tilde{\xi}}$ is zero in $\overline{\mathscr{S}} \otimes \mathrm{Div}^{\mathrm{Ar}}(\widetilde{\mathscr{X}})$.*

(4) *The arithmetic function $m \mapsto T(m)Z$ is zero in $\overline{\mathscr{S}} \otimes \mathrm{Div}^{\mathrm{Ar}}(\mathscr{X})$.*

Proof. Parts (1), (2) and (4) are proved in [Zhang 2001a, §4]. For part (3), we switch to the curve $\widetilde{X}$. By definition, $[\hat{\tilde{\xi}}]$ is a multiple of the class of the Arekelov line bundle $\mathscr{L} = \det \mathrm{Lie}\, \mathscr{A}^\vee$ on $\widetilde{\mathscr{X}}$ with the canonical log functions on $\mathscr{L}_v \cong \omega_{\widetilde{X}_v}$, where $\mathscr{A} \to \mathscr{X}$ is the universal abelian scheme. We view $T(m)$ as a finite algebraic correspondence of degree $\sigma_1(m)$ induced by the subscheme $\widetilde{\mathscr{X}}_m \subset \widetilde{\mathscr{X}} \times \widetilde{\mathscr{X}}$ of pairs $(A, A/D)$ where D is an admissible submodule of A of level m. If $p_1, p_2 \colon \widetilde{\mathscr{X}}_m \to \widetilde{\mathscr{X}}$ are the two projections, then we have

$$T(m)\mathscr{L} = N_{p_1} p_2^* \mathscr{L},$$

[39] See [Zhang 2001a, §4.1.3, §1] for more details on this construction.

and the log functions $\log_{T(m)\mathscr{L}_v}$ on $T(m)\mathscr{L}|_{\widetilde{X}_v}$ are the ones induced by this description. (That these are genuine log functions — see the caveat in Section 5.3 — will be shown in the course of proving Proposition 6.3.1(3) below.)

Let $\pi : \mathscr{A}_1 \to \mathscr{A}_2$ be the universal isogeny over $\widetilde{\mathscr{X}}_m$. As $p_i^*\mathscr{L} = \det \mathrm{Lie}\, \mathscr{A}_i^\vee$, we have an induced map

$$\psi_m = N_{p_1}\pi^* \colon T(m)\mathscr{L} \to N_{p_1} p_1^*\mathscr{L} = \mathscr{L}^{\sigma_1(m)},$$

and [Zhang 2001a, §4.3] shows that $\psi_m(T(m)\mathscr{L}) = c_m \mathscr{L}^{\sigma_1(m)}$ where $c_m \subset \mathbb{O}_F$ is an ideal with divisor $[c_m]$ on $\operatorname{Spec} \mathbb{O}_F$ such that $m \to [c_m]$ is a σ_1-derivative (Section 1.5) and hence zero in $\overline{\mathscr{P}} \otimes \operatorname{Div}(\operatorname{Spec} \mathbb{O}_F) \subset \overline{\mathscr{P}} \otimes \operatorname{Div}^{\mathrm{Ar}}(\mathscr{X})$. In fact if the finite divisor $\hat{\xi}_{\mathrm{fin}} = \operatorname{div}(s)$ for a rational section s of $\mathscr{L}$, the same argument shows that $T(m)\hat{\xi}_{\mathrm{fin}} = \operatorname{div}(T(m)s) = \sigma_1(m)\operatorname{div}(s) + \operatorname{div}(c_m)$; hence, $m \mapsto \hat{\xi}_{\mathrm{fin}}$ is zero in $\overline{\mathscr{P}} \otimes \operatorname{Div}^{\mathrm{Ar}}(\mathscr{X})$.

We complete the proof by showing that, for each $v \mid p$, the difference of log functions

$$\psi_m^* \log_{\mathscr{L}_v^{\sigma_1(m)}} - \log_{T(m)\mathscr{L}_v} \tag{6.3.1}$$

on the line bundle $T(m)\mathscr{L}_v$ on $\widetilde{X}_v$ is a constant on the total space of $\mathscr{L}_v$, and it is a σ_1-derivative when viewed as a function of m. (In particular, this shows that $\log_{T(m)\mathscr{L}_v} = \sigma_1(m)\psi_m^* \log_{\mathscr{L}_v} + \text{constant}$ is a genuine log function.)

It is enough to show this after pullback via p_1 on $\widetilde{X}_m$, where (denoting pulled-back objects with a prime) the map ψ_m' decomposes as

$$\psi_m' = \bigotimes_D \pi_D^* \colon \bigotimes_D \det \mathrm{Lie}(\mathscr{A}'/D)^\vee \to (\det \mathrm{Lie}\, \mathscr{A}'^\vee)^{\otimes \sigma_1(m)},$$

where the tensor product runs over admissible submodule schemes of level m of $\mathscr{A}'$ (since base change via p_1 splits the cover p_1, there are exactly $\sigma_1(m)$ of those). Now the difference (6.3.1) is the sum of the $\sigma_1(m)$ differences

$$(\pi_D^*)^* \log_{\mathscr{L}} - \log_{\mathscr{L}},$$

which are all the same since they are permuted by the Galois group of p_1. As π_D^* acts by multiplication by $(\deg \pi_D)^{1/2} = \boldsymbol{N}(m)^2$, by (5.3.2), each of these differences is $2\log_v \boldsymbol{N}(m)$ so that (6.3.1) equals

$$2\sigma_1(m)\log_v \boldsymbol{N}(m),$$

which is indeed a σ_1-derivative. □

7. Heights of Heegner points

Let Ψ be the modular form of level N with Fourier coefficients given by the p-adic height pairing $\langle z, T(m)z\rangle$ (it is a modular form because of Lemma 1.4.1 and the

fact that the quaternionic Hecke algebra $\boldsymbol{T}'_N$ is a quotient of $\boldsymbol{T}_N$, as explained at the end of Section 6.1). We will compute the heights of Heegner points, with the goal of showing (in Section 8) that $l_{f_\alpha}(\Phi')$ and $l_{f_\alpha}(\Psi)$ are equal up to the action of some Hecke operators. The main theorem will follow.

The strategy is close to that of Perrin-Riou. Namely, we separate the local contributions to Ψ from primes above p, writing $\Psi \sim \Psi_{\mathrm{fin}} + \Psi_p$; using the computations of [Zhang 2001a; 2001b], we find an explicit expression for Ψ_{fin}, which in Section 8 we will show to be "almost" equal to the expression for Φ', while the contribution of Ψ_p is shown to vanish. We circumvent the difficulties posed by the absence of cusps through the use of p-adic Arakelov theory.

It will be crucial to work in the quotient spaces $\overline{\mathcal{S}}$ and $\overline{\mathcal{S}}^{\mathrm{ord}}$ introduced in Section 1.6; for the convenience of the reader, we copy here the diagram (1.6.1) that summarises the relations among them.

$$\begin{array}{ccccc}
\boldsymbol{S}_N(L) & \longrightarrow & \overline{\mathcal{S}}_N^{p\text{-adic}}(L) & \hookrightarrow & \overline{\mathcal{S}}^{\mathrm{ord}} \\
\downarrow{\scriptstyle e} & & \downarrow & & \\
S_{NP}^{\mathrm{ord}}(L)/S_{NP}^{N\text{-old}} & \xrightarrow{\sim} & \overline{\mathcal{S}}_N^{\mathrm{ord}}(L) & \xrightarrow{l_{f_\alpha}} & L
\end{array}$$

We will abuse notation by using the same name for a modular form and its image in $\overline{\mathcal{S}}_N^{\mathrm{ord}}$.

The height pairings $\langle\,\cdot\,,\,\cdot\,\rangle$ (and the accompanying Arakelov pairings) on the base change of X to E that will be considered are the ones associated with a "cyclotomic" p-adic logarithm given by $\ell = \ell_F \circ \mathfrak{N}\colon E^\times \setminus E_{\boldsymbol{A}^\infty}^\times \to \mathbb{Q}_p$ for some[40]

$$\ell_F\colon F^\times \setminus F_{\boldsymbol{A}^\infty}^\times \to \mathbb{Q}_p$$

and with choices of Hodge splittings on $V_{v,L} = H^1_{\mathrm{dR}}(X_v/E_v) \otimes L$ $(v \mid p)$ such that, on $e_f V_{v,L} \cong e_f M_{\mathcal{J},L}$, the induced Hodge splitting is the unit root splitting.

As mentioned before, the Shimura curve X and its integral model $\mathcal{X}$ may not be fine enough for the needs of Arakelov and intersection theory, so we may need to pass to a Shimura curve $\widetilde{\mathcal{X}} \xrightarrow{\pi} \mathcal{X}$ of deeper level away from p and consider the pullbacks $\tilde{\eta}$ of the divisors η, etc. Then notation such as $\langle \hat{\eta}, T^0(m)\hat{\eta}\rangle^{\mathrm{Ar}}$ is to be properly understood as $\langle \hat{\tilde{\eta}}, T^0(m)\hat{\tilde{\eta}}\rangle^{\mathrm{Ar}}/\deg \pi$.

7.1. ***Local heights at places not dividing p.*** The next two results will be used to show the main identity.

Lemma 7.1.1. *In the space $\overline{\mathcal{S}}$ we have*

$$\langle z, T(m)z\rangle = \langle \hat{z}, T(m)\hat{z}\rangle^{\mathrm{Ar}} \sim \langle \hat{\eta}, T^0(m)\hat{\eta}\rangle^{\mathrm{Ar}}.$$

[40] In our application, we will take $\ell_F = \frac{d}{ds}\big|_{s=0} \nu^s$ for a character $\nu\colon \mathcal{G}_F \to 1 + p\mathbb{Z}_p$.

Proof. First observe that, by Lemma 1.4.1, the first member is a modular form of level N, so it does indeed belong to $\overline{\mathcal{S}}_N$. The first equality is a consequence of Proposition 5.4.1(1) and the construction of $\hat{z}$. The second part follows from expanding the second term for m prime to $N\Delta$ according to (6.2.2) and observing that the omitted terms are zero in $\overline{\mathcal{S}}$ by Proposition 6.3.1. □

We can therefore write

$$\Psi \sim \sum_w \Psi_w = \sum_v \Psi_v = \Psi_{\mathrm{fin}} + \Psi_p \tag{7.1.1}$$

in $\overline{\mathcal{S}}$, with the first sum running over the finite places w of E, the second sum running over the finite places v of F and

$$\Psi_w(m) = \langle \hat{\eta}, T^0(m)\hat{\eta}\rangle_w^{\mathrm{Ar}}, \qquad \Psi_v = \sum_{w|v} \Psi_w, \qquad \Psi_{\mathrm{fin}} = \sum_{v\nmid p} \Psi_v, \qquad \Psi_p = \sum_{v|p} \Psi_v.$$

(We are exploiting the fact that for m prime to $N\Delta$ the divisors $\hat{\eta}$ and $T^0(m)\hat{\eta}$ have disjoint supports so that we can apply Proposition 5.4.1(2).)

For each prime $\wp$ of F above p, we define an operator[41] on $\mathcal{S}$

$$\mathcal{R}_\wp = U_\wp - 1, \qquad \mathcal{R}_p = \prod_{\wp|p} \mathcal{R}_\wp.$$

We also define, for integers $\mu_\wp \geq 1$, operators

$$\mathcal{R}_\wp^{(\mu_\wp)} = U_\wp^{\mu_\wp} - 1, \qquad \mathcal{R}_p^{(\mu)} = \prod_{\wp|p} \mathcal{R}_\wp^{(\mu_\wp)}.$$

Proposition 7.1.2. *In the space $\overline{\mathcal{S}}$, we have*

$$\Psi_{\mathrm{fin}} \sim \sum_{v\nmid p} \Psi_v + h,$$

where h is a modular form that is killed by l_{f_α}; the sum runs over the finite places of F, and the summands are given by:

(1) *If $v = \wp$ is inert in E, then*

$$\Psi_v(m) = \sum_{\substack{n \in Nm^{-1}\Delta^{-1} \\ \varepsilon_v((n-1)n)=1\ \forall v|\Delta \\ 0<n<1}} 2^{\omega_\Delta(n)} r((1-n)m\Delta) r(nm\Delta/N\wp)(v(nm/N)+1)\ell_{F,v}(\pi_v).$$

[41] This is different from the operator bearing the same name in [Perrin-Riou 1987].

(2) *If $v = \wp \mid \Delta$ is ramified in E, then*

$$\Psi_v(m) = \sum_{\substack{n \in Nm^{-1}\Delta^{-1} \\ \varepsilon_v((n-1)n)=-1 \\ \varepsilon_w((n-1)n)=1\ \forall v \neq w \mid \Delta \\ 0<n<1}} 2^{\omega_\Delta(n)} r((1-n)m\Delta) r(nm\Delta/N)(v(nm)+1)\ell_v(\pi_v).$$

(3) *If v is split in E, then*

$$\Psi_v(m) = 0.$$

Proof. For m prime to $N\Delta$, we have $\Psi_{\text{fin}}(m) = \sum_{w \nmid p} \langle \hat{\eta}, T^0(m)\hat{\eta} \rangle_w^{\text{Ar}}$ (the sum running over all finite places w of E). By Proposition 5.4.1(2), up to the factor $\ell_{F,v}(\pi_v)$ (which equals $\ell_w(\pi_w)$ or its half for each place w of E above v), each term is given by an intersection multiplicity $(\hat{\eta}, T(m)\hat{\eta})_w$, which is computed by Zhang.

When $v(N) \leq 1$ for all v that are not split in E, the result is summarised in [Zhang 2001a, Proposition 5.4.8]; in this case, the values obtained there are equivalent to the asserted ones by [Zhang 2001a, Propositions 7.1.1 and 6.4.5], and there is no extra term h. In fact (and with no restriction on N), these values also appear as the local components ${}^{\mathbb{C}}\Phi'_v$ at finite places of a form ${}^{\mathbb{C}}\Phi'$ of level N, which is a kernel of the Rankin–Selberg convolution for the central derivative $L'(f_E, 1)$ of the complex L-function.

In general, [Zhang 2001b, Lemma 6.4.3] proves that[42]

$$\frac{\Psi_v}{\ell_{F,v}(\pi_v)} \sim \frac{{}^{\mathbb{C}}\Phi_v'^{\sharp}}{\log \boldsymbol{N}(\wp_v)} + {}_v h, \tag{7.1.2}$$

where ${}_v h$ is a modular form with zero projection onto the f-eigenspace (see the discussion at the very end of [Zhang 2001b]; the forms ${}_v h$ come from intersections at bad places) and ${}^{\mathbb{C}}\Phi'^{\sharp}$ is a form of level $N\Delta$ that is a kernel for the complex Rankin–Selberg convolution in level $N\Delta$ (in particular, it is modular and $\text{Tr}_\Delta({}^{\mathbb{C}}\Phi'^{\sharp}) = {}^{\mathbb{C}}\Phi' + h'$, where h' is a modular form of level N that is orthogonal to f). Applying the operator Tr_Δ in (7.1.2), we recover the asserted formula. □

7.2. *Local heights at p, I.* The following is the key result concerning the local heights at places dividing p. We assume that all primes $\wp$ of F dividing p are split in E.

Proposition 7.2.1. *The arithmetic function $\mathcal{R}_p^4 \Psi_p$ belongs to $\overline{\mathcal{S}}_N^{\text{ord}} \subset \overline{\mathcal{S}}^{\text{ord}}$, and*

$$l_{f_\alpha}(\mathcal{R}_p^4 \Psi_p) = 0.$$

[42] We are adapting the notation to our case. In [Zhang 2001b], the form f is denoted by ϕ and the functions ${}_v h$ are denoted by ${}_v f$.

The modularity assertion follows, as in [Nekovář 1995], by difference from the modularity of Ψ (hence of $\mathcal{R}_p^4\Psi$) and the modularity of $\mathcal{R}_p^4\Psi_{\mathrm{fin}}$ proved in Proposition 8.1.1 below.

The proof of the vanishing of the f_α-component will be completed in Section 7.3 using the results of the rest of this subsection.

We start by fixing for the rest of this section a prime $\wp$ of F dividing p. Fix an isomorphism $B_\wp = B \otimes_F F_\wp \cong M_2(F_\wp)$ identifying the local order $R_\wp$ with $M_2(\mathbb{O}_{F,\wp})$ and the field $E \subset B$ with the diagonal matrices in $M_2(F_\wp)$. Let the divisors η_c be as in (6.2.1), and denote

$$H_s = H[\wp^s], \qquad u_s = u(\wp^s).$$

Let $y_s \in X(H_s)$ be the CM point of conductor $\wp^s$ defined by

$$y_s = \left[\left(x_0, \iota_\wp \begin{pmatrix} \pi^s & 1 \\ & 1 \end{pmatrix}\right)\right],$$

where $\iota_\wp \colon \boldsymbol{GL}_2(F_\wp) \to \widehat{B}^\times$ is the natural inclusion and π is a uniformiser at $\wp$.

Fix a place w of H above $\wp$; we still denote by w the induced place on each H_s and by $\mathfrak{p}$ the prime of E lying below w. Since $\wp$ splits in E, by [Zhang 2001a, §2.2], the CM points $y_s = [A_s]$ are ordinary, and their canonical submodules with respect to the reduction modulo w are given by $A_s[\mathfrak{p}]$.

Proposition 7.2.2 (norm relations). *Let y_s be the system of CM points defined above.*

(1) *Let $m = m_0\wp^n$ be an ideal of F with m_0 prime to $\wp N$. We have*

$$[T(m\wp^{r+2}) - 2T(m\wp^{r+1}) + T(m\wp^r)](\eta) = u_{n+r+2}^{-1} T(m_0)\,\mathrm{Tr}_{H_{n+r+2}/E}(y_{n+r+2})$$

as divisors on X.

(2) *For all $s \geq 1$, we have*

$$T(\wp)y_s = \mathrm{Tr}_{H_{s+1,w}/H_{s,w}}(y_{s+1}) + y_{s-1}.$$

(3) *For all $s \geq 1$, we have*

$$\varphi(y_s) = y_{s-1},$$

where φ is the lift (6.1.1) *of Frobenius with respect to the reduction modulo w.*

Proof. By the multiplicativity of Hecke operators, it is enough to prove the statement of part (1) for $m_0 = 1$. A simple computation based on Proposition 6.3.1 shows that the left-hand side is equal to $\eta_{\wp^{n+r+2}}$. Since the Galois action of $\mathrm{Gal}(H_{n+r+2}/E)$ is simply transitive on $Y_{\wp^{n+r+2}}$, the right-hand side is also equal to $\eta_{\wp^{n+r+2}}$.

For part (2), use the notation $[g]$ to denote $[(x_0, \iota_\wp(g))]$. Then we have

$$T(\wp)y_s = \sum_{j\in\mathbb{O}_{F,\wp}/\wp}\left[\begin{pmatrix}\pi^s & 1\\ & 1\end{pmatrix}\begin{pmatrix}\pi & j\\ & 1\end{pmatrix}\right]+\left[\begin{pmatrix}\pi^s & 1\\ & 1\end{pmatrix}\begin{pmatrix}1 & \\ & \pi\end{pmatrix}\right].$$

The last term is identified as y_{s-1} after acting by the diagonal matrix $\pi^{-1}\mathrm{id}$ (whose action is trivial on X). On the other hand, by local class field theory and the description of the Galois action on CM points of Section 6.2, we have

$$\mathrm{Tr}_{H_{s+1,w}/H_{s,w}}(y_{s+1}) = \sum_{j\in\mathbb{O}_{F,\wp}/\wp}\left[\begin{pmatrix}1+j\pi^s & \\ & 1\end{pmatrix}\begin{pmatrix}\pi^{s+1} & 1\\ & 1\end{pmatrix}\right],$$

which is the same as the above sum in j.

For part (3), which in fact is not needed in what follows, we switch to the moduli description,[43] so $y_s = [A_s] = [A_{D_s}]$ for an increasing sequence of admissible submodules D_s of level $\wp^s$ (this follows from part (2), together with a variant for $s = 0$ that we omit, and the moduli description of Hecke correspondences). Now D_1 is different from $\mathrm{can}(A) = A[\mathfrak{p}]$ since $[A_{A[\mathfrak{p}]}]$ has conductor 1, and in fact each D_s does not contain $A[\mathfrak{p}]$ since if it did then $[A_s]$ would be in the support of $T(\wp)^{s-1}[A_{A[\mathfrak{p}]}]$, which is easily seen[44] to consist of CM points of conductor dividing $\wp^{s-1}$. It follows that the point $\varphi([A_s]) = [A_{D_s+\mathrm{can}(A_s)}] = [A_{D_s+A[\mathfrak{p}]}]$ is in the support of $T(\wp)[A_s]$, but it is not one of the Galois conjugates of y_{s+1} since as just seen it has lower conductor; by part (2), it must then be y_{s-1}. □

Lemma 7.2.3. *Let w a place of E dividing $\wp$, and let $h \in E_w(X)$ be a rational function whose reduction at w is defined and nonzero. Let $\mu = \mu_\wp$ be the order of the ideal $\mathfrak{p}_w$ in the relative class group of E/F. Then the arithmetic functions*

$$\mathcal{R}_\wp^2\mathcal{R}_\wp^{(\mu)}\langle\widehat{\mathrm{div}}(h), T^0(m)\hat{\eta}\rangle_w^{\mathrm{Ar}}, \qquad \mathcal{R}_\wp^3\langle\mathrm{div}(h), T(m)z\rangle_w$$

belong to the kernel of the $\wp$-partial ordinary projection $e_\wp$.

Proof. We show more precisely that

$$v(U_\wp^s\mathcal{R}_\wp^3\langle\widehat{\mathrm{div}}(h), T^0(m)\hat{\eta}\rangle_w^{\mathrm{Ar}}) \geq v(N\wp^s) - C \tag{7.2.1}$$

for a uniform constant C, where v is the p-adic valuation. We may assume m prime to $\wp N\Delta$.

For the second expression, under our assumptions, $T(m\wp^s)\eta = T^0(m\wp^s)\eta + r(m\wp^s)\eta - h\sigma_1(m\wp^s)\xi$, so the analogue of (7.2.1) holds with the same proof together

[43] As usual, after base change to a suitable quadratic extension F'.

[44] By the following observation: if y is a CM point of conductor c, then the support of $T(m)y$ consists of CM points of conductors dividing cm.

with the observation that $\mathscr{R}^2_{\wp} r(m) = 0$ and $v(\sigma_1(m\wp^s)) = v(\boldsymbol{N}\wp^s)$ [Perrin-Riou 1987, Lemme 5.4].

As $\mathscr{R}^2_{\wp} r(m) = 0$, Proposition 7.2.2(1) gives

$$U^s_{\wp}\mathscr{R}^2_{\wp}\eta = u^{-1}_{s+2}\,\mathrm{Tr}_{H_{s+2}/E}\, y_{s+2}$$

where $y_{s+2} \in Y_{\wp^{s+2}}$; we make a compatible choice of y_s such as the one described above Proposition 7.2.2.

For s large enough, the divisor of h is supported away from y_s and its conjugates. Then by Proposition 5.4.1(3), we have

$$\begin{aligned} U^s_{\wp}\mathscr{R}^2_{\wp}\langle \widehat{\mathrm{div}}(h), T^0(m)\hat{\eta}\rangle^{\mathrm{Ar}}_w &= u^{-1}_{s+2}\ell_w(h(T^0(m)y_{s+2})) \\ &= u^{-1}_{s+2}\sum_{w'|w}\ell_w(N_{H_{s+2,w'}/E_w}h(y_{s+2})), \end{aligned}$$

where w' runs over the places of H above w (which are identified with the places of H_{s+2} above w since H_{s+2}/H is totally ramified above $\wp$).

For any $w' \mid w$, we have

$$\begin{aligned} &\mathscr{R}^{(\mu)}_{\wp}\ell_w(N_{H_{s+2,w'}/E_w}h(y_{s+2})) \\ &\qquad = \ell_w \circ N_{H_{w'}/E_w}(N_{H_{s+2+\mu,w'}/H_{w'}}h(y_{s+2+\mu})/N_{H_{s+2,w'}/H_{w'}}h(y_{s+2})). \end{aligned}$$

Suppose that (for s large enough)

$$\begin{aligned} &\text{the } w'\text{-adic valuation of } N_{H_{s,w'}/H_{w'}}(h(y_s)) \text{ only} \\ &\text{depends on the residue class of } s \pmod{\mu}. \end{aligned} \tag{7.2.2}$$

Then each w'-summand in the expression of interest is the product of u^{-1}_{s+2} (which is eventually constant in s) and the p-adic logarithm of a unit that is a norm from an extension of E_w whose ramification degree is a constant multiple of $\boldsymbol{N}\wp^s$; hence, its p-adic valuation is also at least a constant multiple of the valuation of $\boldsymbol{N}\wp^s$, which proves the lemma.

It remains to prove (7.2.2). We have

$$w'(N_{H_{s,w'}/H_{w'}}(h(y_s))) = [H_{s,w'} : H_{w'}](\underline{(h)}, \underline{y_s}), \tag{7.2.3}$$

where the pairing in the right-hand side denotes the intersection multiplicity of the Zariski closures in the integral model. Now as in [Perrin-Riou 1987, Lemme 5.5], if π_s denotes a uniformiser of $H_{s,w'}$, we can show that we have

$$\underline{y_s} \equiv \underline{y_{s-\mu}} \bmod \pi_s, \qquad \underline{y_s} \not\equiv \underline{y_{s-\mu}} \bmod \pi_s^2. \tag{7.2.4}$$

In fact, we first check that the two points have the same reduction. By [Zhang 2001b, Lemma 5.4.2], the set of points in the special fibre $\mathscr{X} \times_{\mathscr{O}_{F,\wp}} \bar{\boldsymbol{F}}_{\wp}$ having CM

by E (and thus being ordinary as $\wp$ splits in E) is identified with

$$E^\times \setminus (N(F_v) \setminus \boldsymbol{GL}_2(F_\wp)) \times \boldsymbol{B}^{\wp\infty\times}/\widehat{F}^\times \widehat{R}^\times \tag{7.2.5}$$

(where N is the group of upper-triangular unipotent matrices) in such a way that the reduction map sends the CM point $[(x_0, g)] \in X(\mathbb{C})$ to the class of g. Then if $\sim$ denotes the equivalence relation in (7.2.5) and $t \in E^\times$ is a generator of the ideal $\mathfrak{p}_w^\mu a$ for some ideal a of $\mathbb{O}_F$ with adelic generator π_a, the reduction of y_s is the class of

$$\begin{aligned}\iota_\wp \begin{pmatrix} \pi^s & 1 \\ & 1 \end{pmatrix} &\sim \iota_\wp \begin{pmatrix} \pi^s & \\ & 1 \end{pmatrix} \sim \iota_\wp \left(\begin{pmatrix} \pi^\mu & \\ & 1 \end{pmatrix} \begin{pmatrix} \pi^{s-\mu} & \\ & 1 \end{pmatrix} \right) \\ &\sim t\iota_\wp \begin{pmatrix} \pi^{s-\mu} & \\ & 1 \end{pmatrix} (t^{\wp\infty})^{-1} \pi_a^{-1} \sim \iota_\wp \begin{pmatrix} \pi^{s-\mu} & \\ & 1 \end{pmatrix} \sim \iota_\wp \begin{pmatrix} \pi^{s-\mu} & \\ & 1 \end{pmatrix},\end{aligned}$$

which is the same as the reduction of $y_{s-\mu}$.

We can then verify the congruence relation (7.2.4) on the completed local ring $\hat{\mathbb{O}}_{\mathscr{X}/W(\bar{\boldsymbol{F}}_v),\bar{y}}$ of the common reduction $\bar{y}$; here W is the ring of integers in the completion of the maximal unramified extension of F_v. By [Carayol 1986, §5.5, Proposition], this is the universal deformation ring of the p-divisible module $\mathscr{G}^1_{\bar{y}}$ (with the notation of Section 6.1). As the point $\bar{y}$ is ordinary, such module is isomorphic to the product $F_\wp/\mathbb{O}_{F,\wp} \times \Sigma_1$, where Σ_1 is the Lubin–Tate formal $\mathbb{O}_{F,\wp}$-module of height 1. Now its lifting $\mathscr{G}^1_s = \mathscr{G}^1_{y_s}$ is defined precisely over the ring of integers of $H_{s,w'}$, and so it is a quasicanonical lifting of level s of its reduction $\mathscr{G}_{\bar{y}}$, in the sense of [Gross 1986]. Then by [Gross 1986, §6] (see also [Meusers 2007] for a detailed account), $\mathscr{G}^1_s$ is congruent to the canonical lifting modulo π_s but not modulo π_s^2, whereas $\mathscr{G}^1_{s-\mu}$ is congruent to the canonical lifting modulo $\pi_{s-\mu} = \pi_s^{N\wp^\mu}$; this implies (7.2.4). Then for each irreducible component $\underline{a}$ in the support of $(\underline{h})$, the sequence $[H_{s,w'} : H_{w'}](\underline{a}, \underline{y_s})$ stabilises to either 0 or 1 so that the expression (7.2.3) is indeed eventually constant along the arithmetic progression. □

Lemma 7.2.4. *For each divisor $D \in \mathrm{Div}^0(X)(E_v)$ or $\widehat{D} \in \mathrm{Div}^{\mathrm{Ar}}(X)$, the element of $\overline{\mathcal{F}}^{\mathrm{ord}}$ given by*

$$m \mapsto \mathcal{R}^2_\wp \mathcal{R}^{(\mu)}_\wp \langle D, T(m)z\rangle_w, \qquad m \mapsto \mathcal{R}^2_\wp \mathcal{R}^{(\mu)}_\wp \langle \widehat{D}, T^0(m)\hat{\eta}\rangle^{\mathrm{Ar}}_w$$

is well-defined independently of the choice of D in its class $[D]$ or $\widehat{D}$ in its class $[\widehat{D}]$, respectively; it will be denoted by

$$\mathcal{R}^2_\wp \mathcal{R}^{(\mu)}_\wp \langle [D], T(m)z\rangle_w, \qquad \mathcal{R}^2_\wp \mathcal{R}^{(\mu)}_\wp \langle [\widehat{D}], T^0(m)\hat{\eta}\rangle^{\mathrm{Ar}}_w.$$

If $\widehat{D} = D$, then the two elements coincide as elements of $\overline{\mathcal{F}}^{\mathrm{ord}}$; moreover, for the arithmetic function $\Psi_w \in \overline{\mathcal{F}}$ with $\Psi_w(m) = \langle \hat{\eta}, T^0(m)\hat{\eta}\rangle^{\mathrm{Ar}}_w$, we have

$$\mathcal{R}^2_\wp \mathcal{R}^{(\mu)}_\wp \Psi_w \sim \mathcal{R}^2_\wp \mathcal{R}^{(\mu)}_\wp \langle [z], T(m)z\rangle_w \tag{7.2.6}$$

in $\overline{\mathcal{F}}^{\mathrm{ord}}$.

Proof. The first part follows from Lemma 7.2.3. For the second part, we may argue as in the proof of Lemma 7.1.1: for example, in $\overline{\mathcal{S}}$, we have

$$\begin{aligned}\mathcal{R}_{\wp}^2\mathcal{R}_{\wp}^{(\mu)}\langle\hat{\eta}, T^0(m)\hat{\eta}\rangle_w^{\mathrm{Ar}} &\sim \mathcal{R}_{\wp}^2\mathcal{R}_{\wp}^{(\mu)}\langle\hat{\eta}+\widehat{\mathrm{div}}(h), T^0(m)\hat{\eta}\rangle_w^{\mathrm{Ar}}\\ &\sim \mathcal{R}_{\wp}^2\mathcal{R}_{\wp}^{(\mu)}\langle\hat{z}+\widehat{\mathrm{div}}(h), T(m)\hat{z}\rangle_w^{\mathrm{Ar}}\\ &= \mathcal{R}_{\wp}^2\mathcal{R}_{\wp}^{(\mu)}\langle z+\mathrm{div}(h), T(m)z\rangle_w. \qquad \square\end{aligned}$$

7.3. ***Local heights at p, II.*** Here we prove the vanishing statement for p-adic local symbols asserted in Proposition 7.2.1. In fact, we will show the equivalent statement

$$l_{f_\alpha}(\mathcal{R}_p^4\mathcal{R}_p^{(\mu)}\Psi_p) = \prod_{\wp\mid p}(\alpha_{\wp}^{\mu_\wp}-1)l_{f_\alpha}(\mathcal{R}_p^4\Psi_p) = 0,$$

where the integers $\mu=(\mu_\wp)_{\wp\mid p}$ are as in Lemma 7.2.3.

Let $e_f \in \boldsymbol{T}_{Np}\otimes M_f$ be the maximal idempotent satisfying $T(m)\circ e_f = a(f,m)e_f$ for all m prime to Np;[45] viewed as an endomorphism of $S_{N\prod_{\wp\mid p}\wp}$, it is the projector onto the subspace generated by f and $[\wp]f$ for all the primes $\wp$ of F dividing p. With $z_f = e_f[z]$, we have by (7.2.6)

$$e_f e\mathcal{R}_p^4\mathcal{R}_p^{(\mu)}\Psi_p = \mathcal{R}_p^4\mathcal{R}_p^{(\mu)}\langle z_f, T(m)z\rangle_p$$

in $\overline{\mathcal{S}}_N^{\mathrm{ord}}$, where the left-hand side makes sense by the modularity part of Proposition 7.2.1 and the right-hand side makes sense by Lemma 7.2.4. We also denote, for w a place of E above the F-prime $\wp\mid p$, and $i\geq 2$,

$$e_f e\mathcal{R}_{\wp}^i\mathcal{R}_{\wp}^{(\mu_\wp)}\Psi_w := \mathcal{R}_{\wp}^i\mathcal{R}_{\wp}^{(\mu_\wp)}\langle z_f, T(m)z\rangle_w, \tag{7.3.1}$$

where the right-hand side makes sense as an element of $\overline{\mathcal{S}}^{\mathrm{ord}}$ by Lemma 7.2.4. (As we have not shown that $\mathcal{R}_{\wp}^3\Psi_w$ is modular, the left-hand side is not otherwise defined.) Then by definition, we have

$$e_f e\mathcal{R}_p^4\mathcal{R}_p^{(\mu)}\Psi_p = \sum_{w\mid p} e_f e\mathcal{R}_p^4\mathcal{R}_p^{(\mu)}\Psi_w. \tag{7.3.2}$$

Now since $l_{f_\alpha} = l_{f_\alpha}\circ e_f = l_{f_\alpha}\circ e_f\circ e$, by (7.3.2), the desired result is implied by the following lemma for all $\wp\mid p$:

Lemma 7.3.1. *Suppose that f is ordinary at $\wp$. For each place w of E above $\wp\mid p$, the element $e_f\mathcal{R}_{\wp}^2\mathcal{R}_{\wp}^{(\mu_\wp)}\Psi_w$ is zero in $\overline{\mathcal{S}}^{\mathrm{ord}}$.*

Proof. The ordinarity assumption and Lemma 5.1.1 [Perrin-Riou 1987, Example 4.12] imply that z_f is "almost" a universal norm in the totally ramified $\mathbb{Z}_p$-extension $E_{w,\infty}^{\ell}$ of E_w: that is, after perhaps replacing z_f by an integer multiple,

[45] Recall that M_f is the number field generated by the Fourier coefficients $a(m, f)$.

for each layer $E^{\ell}_{w,n}$, we have

$$z_f = \mathrm{Tr}_n(z_n)$$

for some $z_n \in e_f J(X)(E^{\ell}_{v,n})$, where $\mathrm{Tr}_n = \mathrm{Tr}_{E^{\ell}_{w,n}/E_w}$. Then we have

$$e_f \mathcal{R}^2_{\wp} \mathcal{R}^{(\mu_\wp)}_{\wp} \Psi_w(m) = \mathcal{R}^2_{\wp} \mathcal{R}^{(\mu_\wp)}_{\wp} \langle \mathrm{Tr}_n(z_n), T(m) z \rangle_w = \mathcal{R}^2_{\wp} \mathcal{R}^{(\mu_\wp)}_{\wp} \langle z_n, T(m) z \rangle_{w,n},$$

where $\langle \cdot, \cdot \rangle_{w,n}$ is the local height pairing on $\mathrm{Div}^0(X)(E^{\ell}_{w,n})$ associated with the logarithm $\ell_{n,v} = \ell_w \circ N_{E^{\ell}_{w,n}/E_w}$. By Proposition 5.1.2(5)–(6), the right-hand side above has image in $c^{-1} \mathrm{Im}(\ell_n) \subset \mathbb{Z}_p$ for a uniform nonzero constant $c \in \mathbb{Z}_p$. As the extension $E^{\ell}_{w,n}/E_w$ has ramification degree p^n, we have for some nonzero $c' \in \mathbb{Z}_p$

$$e_f \mathcal{R}^2_{\wp} \mathcal{R}^{(\mu_\wp)}_{p} \Psi_v(m) \in c^{-1} \mathrm{Im}(\ell_n) \subset c'^{-1} p^n \mathbb{Z}_p$$

for all n; therefore, $e_f \mathcal{R}^2_{\wp} \mathcal{R}^{(\mu_\wp)}_{p} \Psi_w = 0$. □

Part III. Main theorem and consequences

8. Proof of the main theorem

In this section, we prove Theorem B.

8.1. ***Basic case.*** First we prove the formula when $\Delta_{E/F}$ is totally odd and each prime $\wp$ of F dividing p splits in E.

Let $\Psi_{\mathcal{W}} \in \overline{\mathcal{S}}_N$ denote the modular form with coefficients $\langle [z], T(m)[z] \rangle_{\mathcal{W}}$, where ${}^{\circ}\mathcal{W} = \nu \circ \mathfrak{N}$ and $\langle \cdot, \cdot \rangle_{\mathcal{W}}$ is the height pairing on $J(X)(E)$ associated with the p-adic logarithm $\ell_F \circ \mathfrak{N}$, with

$$\ell_F = \frac{d}{ds}\bigg|_{s=0} \nu^s \colon F^{\times} \backslash F^{\times}_{\boldsymbol{A}^\infty} \to \mathbb{Q}_p.$$

Recall that l_{f_α} is a continuous functional so that it commutes with limits and

$$L'_{p,\mathcal{W}}(f_E)(\mathbb{1}) = l_{f_\alpha}\left(\frac{d}{ds}\bigg|_{s=0} \Phi({}^{\circ}\mathcal{W}^s) \right) = l_{f_\alpha}(\Phi'_{\mathcal{W}}).$$

We compare the Fourier coefficients of $\Phi'_{\mathcal{W}}$ and $\Psi_{\mathcal{W}} = \Psi_{\mathcal{W},\mathrm{fin}} + \Psi_{\mathcal{W},p}$.

Proposition 8.1.1. *Suppose that all of the prime ideals $\wp$ of F dividing p are principal. Then we have*

$$\left(\prod_{\wp | p} U^4_{\wp} - U^2_{\wp} \right) \Phi'_{\mathcal{W}} \sim \left(\prod_{\wp | p} (U_{\wp} - 1)^4 \right) \Psi_{\mathcal{W},\mathrm{fin}}$$

in the quotient space $\overline{\mathcal{S}}^{\mathrm{ord}}_N / \mathrm{Ker}(l_{f_\alpha})$.

Proof. We prove that the identity holds in $\overline{\mathcal{F}}/(\mathcal{D}_N + \mathrm{Ker}(l_{f_\alpha}))$, where $\mathrm{Ker}(l_{f_\alpha})$ denotes the image in $\overline{\mathcal{F}}$ of classical modular form killed by l_{f_α}. Then since the left-hand side belongs to $\overline{\mathcal{F}}_N^{p\text{-adic}}$, so does the right-hand side (and after further quotienting by $\mathrm{Ker}(e)$, we descend to $\overline{\mathcal{F}}_N^{\mathrm{ord}}/\mathrm{Ker}(l_{f_\alpha})$).

The coefficients of $\Psi_{\mathrm{fin}} = \Psi_{\mathcal{W},\mathrm{fin}}$ are computed in Proposition 7.1.2. To lighten the notation, we write the explicit expression for $\Psi(m) = \sum_{v \text{ nonsplit}} \Psi_v(m)$ as

$$\Psi_v(m) = \sum_{\substack{n \in S_v([m]) \\ v_\wp(nm) \geq 0 \, \forall \wp \mid p}} c_v([nm]) r((1-n)m\Delta) r(nm\Delta/N\wp_v^{\varepsilon(v)}),$$

where the value $c_v([nm])$ only depends on the prime-to-p part of the fractional ideal nm and the set $S_v([m])$ only depends on v and the prime-to-p part of m; here $\varepsilon(v) = 1$ if v is inert and $\varepsilon(v) = 0$ if v is ramified.

The coefficients of Φ' are computed in Proposition 4.5.3. They look "almost" the same in that, up to the modular form h of Proposition 7.1.2, which is in $\mathrm{Ker}(l_{f_\alpha})$, we have, when m is divisible by every $\wp \mid p$,

$$\Phi'_{\mathcal{W}}(m) = \sum_{v \text{ nonsplit}} \Psi_v^{[p]}(m),$$

where for a product P of some of the primes $\wp \mid p$ we denote

$$\Psi_v^{[P]}(m) = \sum_{\substack{n \in S_v([m]) \\ v_\wp(nm) \geq 0 \, \forall \wp \mid p \\ v_\wp(nm) = 0 \, \forall \wp \mid P}} c_v([nm]) r((1-n)m\Delta) r(nm\Delta/N).$$

Then it is enough to show that, for each $v \nmid p$, each $\wp \mid p$ and each $\wp \nmid P$ with P as above, we have

$$(U_\wp^4 - U_\wp^2)\Psi_v^{[P\wp]} = (U_\wp - 1)^4 \Psi_v^{[P]}.$$

For the sake of notation, we write the computation when v is ramified in E and $P = \prod_{\wp' \neq \wp} \wp'$ (for more general P, one just needs more notation to keep track of $v_{\wp'}(nm)$ for the primes $\wp' \neq \wp$).

The right-hand side equals

$$\sum_{i=0}^{4} (-1)^i \binom{4}{i} \sum_{\substack{n_i \in S_v([m]) \\ v_{\wp'}(n_i m) = 0 \, \forall \wp' \neq \wp, \, \wp' \mid p \\ v_\wp(n_i m \wp^i) \geq 0}} c_v([n_i m]) r((1-n_i)m\wp^i\Delta) r(n_i m \wp^i \Delta/N). \tag{8.1.1}$$

From the relation $r(m_0\wp^t) = (t+1)r(m_0)$, valid for $\wp \nmid m_0$, we deduce the relations

$$\begin{aligned} 2r(m) &= r(m\wp) + r(m\wp^{-1}), \\ 2r(m) &= r(m\wp^2) + r(m\wp^{-2}) \quad \text{if } \wp \mid m, \\ 2r(m) &= r(m\wp^2) - r(m) \qquad \text{if } \wp \nmid m, \end{aligned}$$

where we recall that $r(m) = 0$ if m is not an integral ideal. Then we can pick a totally positive generator in F for the ideal $\wp$, which abusing notation we will still denote by $\wp$, and make the substitution $n_i = \wp^{t-i} n_0$ with $\wp^t \parallel n_i m \wp^i$ to write (8.1.1) as

$$\sum_{t \geq 0} \sum_{\substack{n_0 \in S_v(m) \\ v_{\wp'}(n_0 m) = 0 \, \forall \wp \mid p}} c_v([n_0 m]) r((n_0 m)^{(\wp)})(t+1) A_t,$$

where we recall that for an ideal m we denote $m^{(\wp)} = m \wp^{-v_\wp(m)}$ and

$$\begin{aligned} A_t = {} & r(m\Delta\wp^4(1 - n_0\wp^{t-4}))[t + 1 - 2t + 2(t-1)] \\ & + r(m\Delta\wp^2(1 - n_0\wp^{t-2}))\left[-2(t+2) + \begin{cases} 4(t+1) - 2t & \text{if } t \geq 1, \\ 3 & \text{if } t = 0 \end{cases}\right] \\ & + r(m\Delta(1 - n_0\wp^t))[t + 3 - 2(t+2) + t + 1]. \end{aligned}$$

The three expressions in square brackets vanish when $t > 0$ and yield, respectively, 1, 1 and 0 when $t = 0$. Substituting back $n_4 = \wp^{t-4} n_0$ in the first line and $n_2 = \wp^{t-2} n_0$ in the second line, we deduce that (8.1.1) equals

$$(U_\wp^4 - U_\wp^2) \Psi_v^{[P\wp]}$$

as desired.[46] □

Combining this proposition with Proposition 7.2.1, which says

$$l_{f_\alpha}\left(\prod_{\wp \mid p} (U_\wp - 1)^4 \Psi_{\mathcal{W}, p}\right) = 0,$$

we find for $\mathcal{W} = \nu \circ \mathfrak{N}$

$$\begin{aligned} D_F^2 \prod_\wp (\alpha_\wp^4 - \alpha_\wp^2) L'_{p,\mathcal{W}}(f_E, \mathbb{1}) &= \prod_\wp (\alpha_\wp^4 - \alpha_\wp^2)\left(1 - \frac{1}{\alpha_\wp^2}\right)\left(1 - \frac{\boldsymbol{N}\wp}{\alpha_\wp^2}\right) l_{f_\alpha}(\Phi'_{\mathcal{W}}) \\ &= \prod_\wp (\alpha_\wp - 1)^4 \left(1 - \frac{1}{\alpha_\wp^2}\right)\left(1 - \frac{\boldsymbol{N}\wp}{\alpha_\wp^2}\right) l_{f_\alpha}(\Psi_{\mathcal{W}}) \\ &= \prod_\wp (\alpha_\wp - 1)^4 \left(1 - \frac{1}{\alpha_\wp^2}\right) \langle z_f, z_f \rangle_{\mathcal{W}}. \end{aligned}$$

Here, besides the definition of $L_p(f_E)$ (Definition 4.2.1), we have used various properties of the functional l_{f_α} from Lemma 1.6.1 and the observation that the projection onto the f-component of the modular form $\Psi_{\mathcal{W}} \in S_2(K_0(N), \mathbb{Q}_p)$ is $\mathbb{1}_f(\Psi_{\mathcal{W}}) = \langle z_f, z_f \rangle_{\mathcal{W}}$.

This completes the proof of Theorem B when $(\Delta_{E/F}, 2) = 1$ and all primes $\wp \mid p$ split in E.

[46] See [Perrin-Riou 1987, proof of Proposition 3.20].

8.2. ***Reduction to the basic case.*** The general case, where E is only assumed to satisfy $(\Delta_{E/F}, Np) = 1$, can be reduced to the previous one under the assumption

$$L'_{p,\mathcal{W}}(f_E, \mathbb{1}) \neq 0$$

by the following argument due to [Kobayashi 2013, proof of Theorem 5.9] using the complex Gross–Zagier formula (which is known with no restrictions on Δ) and the factorisation $L_p(f_E, \chi \circ \mathfrak{N}) \sim L_p(f, \chi) L_p(f_\varepsilon, \chi)$.

By the factorisation, the orders of vanishing at the central point of the factors of $L_p(f_E, \nu^s \circ \mathfrak{N})$ will be 1 (say for $L_p(f)$) and 0 (say for $L_p(f_\varepsilon)$). Then, by the first part of Theorem C,[47] the orders of vanishing of $L(f, s)$ and $L(f_\varepsilon, s)$ at $s = 1$ will also be 1 and 0. Moreover, the Heegner point $z_{f,E'}$ attached to f and any E' also satisfying $L(f_{\varepsilon_{E'/F}}, 1) \neq 0$ is nontorsion, and in fact, its trace $z_{f,F} = \mathrm{Tr}_{E'/F}(z_{f,E'})$ is nontorsion and $z_{f,E'}$ is up to torsion a multiple of $z_{f,F}$ in $J(X)(E') \otimes \overline{\mathbb{Q}}$. Therefore, by the complex and p-adic Gross–Zagier formulas for a suitable E' satisfying the assumptions of Section 8.1 and $L(f_{\varepsilon_{E'/F}}, 1) \neq 0$, we have

$$L'_{p,\nu}(f, \mathbb{1}) = \prod_{\wp \mid p} \left(1 - \frac{1}{\alpha_\wp}\right)^2 \frac{L'(f, 1)}{\Omega_f^+ \langle z_{f,F}, z_{f,F} \rangle} \langle z_{f,F}, z_{f,F} \rangle_\nu,$$

where $\langle \cdot, \cdot \rangle_\nu$ is the p-adic height pairing on $J(X)(F)$ attached to ν and $\langle \cdot, \cdot \rangle$ is the Néron–Tate height (the ratio appearing above belongs to $M_f^\times$ by the Gross–Zagier formula). This allows us to conclude

$$\begin{aligned}
L'_{p,\mathcal{W}}(f_E, \mathbb{1}) &= \frac{\Omega_f^+ \Omega_{f_\varepsilon}^+}{D_E^{-1/2} \Omega_f} L'_{p,\nu}(f, \mathbb{1}) L_p(f_\varepsilon, \mathbb{1}) \\
&= D_E^{1/2} \prod_{\wp \mid p} \left(1 - \frac{1}{\alpha_\wp}\right)^2 \left(1 - \frac{\varepsilon(\wp)}{\alpha_\wp}\right)^2 \frac{L'(f, 1) L(f_\varepsilon, 1)}{\Omega_f \langle z_{f,F}, z_{f,F} \rangle} \langle z_{f,F}, z_{f,F} \rangle_\nu \\
&= D_F^{-2} \prod_{\wp \mid p} \left(1 - \frac{1}{\alpha_\wp}\right)^2 \left(1 - \frac{\varepsilon(\wp)}{\alpha_\wp}\right)^2 \frac{\langle z_{f,E}, z_{f,E} \rangle}{\langle z_{f,F}, z_{f,F} \rangle} \langle z_{f,F}, z_{f,F} \rangle_\nu \\
&= D_F^{-2} \prod_{\wp \mid p} \left(1 - \frac{1}{\alpha_\wp}\right)^2 \left(1 - \frac{\varepsilon(\wp)}{\alpha_\wp}\right)^2 \langle z_{f,E}, z_{f,E} \rangle_{\mathcal{W}}.
\end{aligned}$$

Remark 8.2.1. It is natural to conjecture that when $L'_{p,\mathcal{W}}(f_E, \mathbb{1}) = 0$ we should have $\langle z_f, z_f \rangle_{\mathcal{W}} = 0$. However, in this case, the above argument fails because, without knowledge of the nontriviality of the p-adic height pairing, the vanishing of $L_p(f_E, \mathcal{W}^s)$ to order ≥ 2 does not imply a similar high-order vanishing for $L(f_E, s)$.

[47] Which can be proved by using the p-adic Gross–Zagier formula attached to a field E' satisfying the assumptions of Section 8.1.

9. Periods and the Birch and Swinnerton-Dyer conjecture

As seen in the introduction, the application of our result to the Birch and Swinnerton-Dyer formula rests on a conjectural relation among the periods of f and the associated abelian variety A. Here we would like to briefly elaborate on this conjecture and its arithmetic consequences. (This section contains no new results or conjectures and is a very brief survey of work of Shimura and [Yoshida 1994].) We retain the notation of the introduction and set $M = M_f$ and $\dim A = [M : \mathbb{Q}] = d$.

9.1. ***Real periods.*** The conjecture on periods stated in the introduction can be refined to a conjecture on rationality rather than algebraicity. First we need to define the automorphic periods $\Omega^+_{f^\sigma}$ for $\sigma \in \mathrm{Hom}(M, \mathbb{C})$; they are naturally defined as elements of $\mathbb{C}^\times/M^\times$ (see [Raghuram and Tanabe 2011] for a modern exposition): one can choose them "covariantly" in the sense of [Yoshida 1994] in order to have $\prod_\sigma \Omega^+_{f^\sigma}$ defined up to $\mathbb{Q}^\times$ or define directly the product as follows. Let $\mathscr{H}_N = Z(\boldsymbol{A}) \setminus \boldsymbol{GL}_2(\boldsymbol{A})/K_0(N)K_\infty$ be the open Hilbert modular variety of level N. Then the perfect pairing of $\mathbb{Q}$-vector spaces

$$H_g(\mathscr{H}_N, \mathbb{Q})^+ \times S_2(K_0(N), \mathbb{Q}) \to \mathbb{C} \tag{9.1.1}$$

(where $+$ denotes the intersection of the $+1$-eigenspaces for the complex conjugations) decomposes under the diagonal action of $\boldsymbol{T}_N$ into $\mathbb{Q}$-rational blocks parametrised by the Galois-conjugacy classes of eigenforms. Then

$$\prod_\sigma \Omega^+_{f^\sigma} \in \mathbb{C}^\times/\mathbb{Q}^\times$$

is $(2\pi i)^{dg}$ times the discriminant of the pairing on the rational block corresponding to $\{f^\sigma\}_\sigma$. (The individual $\Omega^+_{f^\sigma} \in \mathbb{C}^\times/M^\times$ are defined as the discriminants of (9.1.1) on $\overline{\mathbb{Q}}$-rational $\boldsymbol{T}_N$-eigenblocks. One can similarly define periods $\Omega^-_{f^\sigma}$ by paring with $H_g(\mathscr{H}_N, \mathbb{Q})^-$, the -1-eigenspace for the complex conjugations.)

Conjecture 9.1.1. *We have*

$$\Omega_A \sim \prod_\sigma \Omega^+_{f^\sigma}$$

in $\mathbb{C}^\times/\mathbb{Q}^\times$.

The conjecture is originally due [Shimura 1988, especially §11] and was refined by [Yoshida 1994]. When A has complex multiplication, it has been proved by [Blasius 1986]. It is also known when $F = \mathbb{Q}$; before discussing that, let us translate it into a language closer to conjectures of Shimura.

For each $\tau\colon F \to \mathbb{R}$, let $f_{B(\tau)}$ be the Jacquet–Langlands transfer of f to a rational[48] form on the quaternion algebra $B(\tau)/F$ defined in the introduction (recall that $B(\tau)$ is ramified at all infinite places except τ), and let X be our Shimura curve. Then A is (up to isogeny) a quotient ϕ of $J(X)$, and for each embedding τ, we can write

$$\phi^*\omega_A = c_\tau \bigwedge_\sigma 2\pi i f^\sigma_{B(\tau)}(z)\, dz$$

as forms in $H^0(J(X)(\mathbb{C}_\tau), \Omega^d)$ for some $c_\tau \in F^\times$ (since both are generators of a rank-1 F-vector space); here z denotes the coordinate on the upper half-plane uniformising X. Then we have

$$\int_{A(\mathbb{R}_\tau)} |\omega_A|_\tau \sim \prod_\sigma \Omega^+_{f^\sigma_{B(\tau)}} \quad \text{in } \mathbb{C}^\times/F^\times,$$

where $\Omega^+_{f^\sigma_{B(\tau)}}$ is $2\pi i$ times the discriminant of the $f^\sigma_{B(\tau)}$-part of the analogue of the pairing (9.1.1) on $X(\mathbb{C}_\tau)$. When choices are made covariantly in τ, we then get $\Omega_A \sim \prod_{\sigma,\tau} \Omega^+_{f^\sigma_{B(\tau)}}$ in $\mathbb{C}^\times/\mathbb{Q}^\times$.

Our conjecture, decomposed into its σ-constituents, can then be rewritten as

$$\Omega^+_f \sim \prod_\tau \Omega^+_{f_{B(\tau)}} \quad \text{in } \mathbb{C}^\times/(MF)^\times. \tag{9.1.2}$$

In this form, this is a stronger version of Shimura's conjecture [1983] on the factorisation of periods of Hilbert modular forms up to algebraic factors in terms of P-invariants. The reader is referred to [Yoshida 1994] for a discussion of this point.

Notice that (9.1.2) is nontrivial even when $F = \mathbb{Q}$: it asserts that the periods of the transfers of f to any indefinite quaternion algebra have the same transcendental (or irrational) parts. However, in this case, the conjecture is known by [Shimura 1981] (for the algebraicity) and [Prasanna 2009] (for the rationality).

For general F, Shimura's conjecture on P-invariants is largely proved by [Yoshida 1995] under an assumption of nonvanishing of certain L-values.

Remark 9.1.2. It is clear that our conjecture implies that the Birch and Swinnerton-Dyer conjectural formula is true up to a nonzero rational factor when A has analytic M-rank 0. By the complex and p-adic Gross–Zagier formulas, the conjecture for f also implies the complex and p-adic Birch and Swinnerton-Dyer formulas, respectively, up to a rational factor when A has (p-adic) analytic M-rank 1.

9.2. ***Quadratic periods.*** We can formulate a conjecture analogous to Conjecture 9.1.1 for the periods of the base-changed abelian variety $A_E = A \times_{\operatorname{Spec} F} \operatorname{Spec} E$.

[48] For consistency with the case in which $B(\tau) = \boldsymbol{GL}_2(\mathbb{Q})$ and "rational" means "rational q-expansion coefficients", here $f_{B(\tau)}$ is considered F-rational for the structure $H^0(X/F, \Omega_{X/F}) \otimes (2\pi i)^{-1}\mathbb{Q} \subset H^0(X/F, \Omega_{X/F}) \otimes_{F,\tau} \mathbb{C}$ (where X is the Shimura curve defined in the introduction).

Conjecture 9.2.1. *We have*

$$\Omega_{A_E} \sim \prod_{\sigma} \Omega_{f^\sigma}$$

in $\mathbb{C}^\times/\mathbb{Q}^\times$.

Here the period of A_E is

$$\Omega_{A_E} = \prod_{\tau: E \to \mathbb{C}} \int_{A(\mathbb{C}_\tau)} |\omega_{A_E}|_\tau,$$

where for a differential form $\omega = h(z)\, dz_1 \wedge \cdots \wedge dz_k$ we have $|\omega|_\tau = |h(z)|_\tau^2\, dz_1 \wedge d\bar{z}_1 \wedge \cdots \wedge dz_k \wedge d\bar{z}_k$.

As above, this conjecture can be "decomposed" into

$$\Omega_f \sim \prod_{\tau} \Omega_{f_{B(\tau)}} \quad \text{in } \mathbb{C}^\times/(MF)^\times, \tag{9.2.1}$$

where $\Omega_{f_{B(\tau)}}$ is π^2 times the Pertersson inner product of $f_{B(\tau)}$. This is essentially Shimura's conjecture on Q-invariants [1983]. Up to algebraicity, it has been proved by [Harris 1993] under a local condition (a new proof of the same result should appear in forthcoming work of Ichino and Prasanna, yielding rationality and removing the local assumption). As $\Omega_f = \Omega_f^+ \Omega_f^-$,[49] the factorisation (9.2.1) is implied by (9.1.2) and its analogue for Ω_f^-; thus, Harris's result can be seen as evidence for the conjecture on real periods.

We take the opportunity to record an immediate consequence of the conjecture on quadratic periods and the Gross–Zagier formulas.

Theorem 9.2.2. *If A_E has complex or p-adic analytic M-rank ≤ 1, then the complex or p-adic Birch and Swinnerton-Dyer formula, respectively, for A_E is true up to a nonzero algebraic factor.*

List of symbols

Throughout this text, we use the following notation and assumptions, unless otherwise noted:

- F is a totally real field of degree g.
- $\boldsymbol{N}_F$ is the monoid of nonzero ideals of $\mathbb{O}_F$.
- $|\cdot|_v$ is the standard absolute value on F_v.
- $\boldsymbol{A} = \boldsymbol{A}_F$ is the adele ring of F; if $*$ is a place or a set of places or an ideal of F, the component at $*$ or away from $*$ of an adelic object x is denoted x_* or x^*, respectively. For example if $\phi = \prod_v \phi_v$ is a Hecke character and δ is an

[49] See, e.g., [Shimura 1978, Theorem 4.3 (II)], where the assumption on the weight can now be removed thanks to the work of Rohrlich.

ideal of $\mathbb{O}_F$, we write $\phi_\delta(y) = \prod_{v|\delta} \phi_v(y_v)$ and $|y|_\delta = \prod_{v|\delta} |y|_v$. We also use the notation

$$|m|_v = |\pi_m|_v, \qquad |m|_\delta = |\pi_m|_\delta, \qquad \phi_v(m) = \phi_v(\pi_m), \qquad \phi_\delta(m) = \phi_\delta(\pi_m)$$

if m is an ideal of $\mathbb{O}_F$ and ϕ is unramified at δ (here π_m satisfies $\pi_m \mathbb{O}_F = m$).

- $>$ denotes the partial order on $\boldsymbol{A}_F$ given by $x > 0$ if and only if x_∞ is totally positive.
- $R_{\boldsymbol{A}} = R \otimes_F \boldsymbol{A}$ if R is an F-algebra.
- $\boldsymbol{N}m$ is the absolute norm of an ideal m in a number field (the index of m in the ring of integers: it is a positive natural number).
- d_F is the different of F.
- π_N, for N an ideal of $\mathbb{O}_F$, is the idele with components $\pi_v^{v(N)}$ for $v \nmid \infty$ and 1 for $v \mid \infty$.
- $D_F = \boldsymbol{N} d_F$ is the discriminant of F.
- $m^\times = \{a \in F_{\boldsymbol{A}}^\times \mid a\mathbb{O}_F = m\}$ if m is any nonzero fractional ideal of F (this notation will be used with $m = d_F^{-1}$).
- E is a quadratic CM (that is, totally imaginary) extension of F.
- $\mathfrak{D} = \mathfrak{D}_{E/F}$ is the different of E/F.
- $\mathfrak{N} = N_{E/F}$ is the relative norm on E or any E-algebra.
- $\Delta = \Delta_{E/F} = \mathfrak{N}(\mathfrak{D})$ is the relative discriminant of E/F, and we assume
$$(\Delta_{E/F}, D_F Np) = 1;$$
in Sections 2.5, 4.5 and part of 3.2, we further assume that
$$(\Delta, 2) = 1$$
and in Sections 7.2, 7.3 and 8.1 that
$$(\Delta, 2) = 1 \text{ and all primes } \wp \text{ dividing } p \text{ are split in } E.$$
- $D_E = \boldsymbol{N}(\Delta)$ is the absolute discriminant of E.
- $U_F(N)$ is the subgroup of $\hat{\mathbb{O}}_F^\times = \prod_v \mathbb{O}_{F,v}^\times \subset F_{\boldsymbol{A}^\infty}^\times$ consisting of elements $x \equiv 1 \bmod N\hat{\mathbb{O}}_F$, if N is any ideal of $\mathbb{O}_F$.
- $\boldsymbol{e}_v(x) = \exp(-2\pi i \{\mathrm{Tr}_{F_v/\mathbb{Q}_p}(x)\}_p)$ for $v \mid p < \infty$ and $\{y\}_p$ the p-fractional part of $y \in \mathbb{Q}_p$ is the standard additive character of F_v, with conductor $d_{F,v}^{-1}$; for $v \mid \infty$, $\boldsymbol{e}_v(x) = \exp(2\pi i \,\mathrm{Tr}_{F_v/\mathbb{R}}(x))$.
- $\boldsymbol{e}(x) = \prod_v \boldsymbol{e}_v(x_v)$ is the standard additive character of $\boldsymbol{A}_F$.
- $\mathbb{1}_Y$ is the characteristic function of the set Y.
- If φ is any logical proposition, we define $\mathbb{1}[\varphi]$ to be 1 when φ is true and 0 when φ is false — e.g., $\mathbb{1}[x \in Y] = \mathbb{1}_Y(x)$.

Acknowledgements

The present paper grew out of my Columbia thesis. I am grateful to my advisor Professor Shou-Wu Zhang for suggesting this area of research and for his support and encouragement and to Amnon Besser, Shinichi Kobayashi, Luis Garcia Martinez, David Loeffler, Yifeng Liu, Giovanni Rosso, Eric Urban, Jeanine Van Order and Shou-Wu Zhang for useful conversations or correspondence.

This work builds upon the works of Perrin-Riou [1987] and Zhang [2001a; 2001b; 2004] — and, of course, Gross and Zagier [1986]. My debt to their ideas cannot be overstated and will be obvious to the reader.

Some revisions to the manuscript were done while the author was a postdoctoral fellow at MSRI funded under NSF grant 0932078000.

References

[Andreatta and Goren 2005] F. Andreatta and E. Z. Goren, *Hilbert modular forms: mod p and p-adic aspects*, Mem. Amer. Math. Soc. **819**, Amer. Math. Soc., Providence, RI, 2005. MR 2006f:11049 Zbl 1071.11023

[Bertrand 1984] D. Bertrand, "Propriétés arithmétiques de fonctions thêta à plusieurs variables", pp. 17–22 in *Number theory* (Noordwijkerhout, Netherlands, 1983), edited by H. Jager, Lecture Notes Math. **1068**, Springer, Berlin, 1984. MR 756080 Zbl 0546.14029

[Besser 2004] A. Besser, "The p-adic height pairings of Coleman–Gross and of Nekovář", pp. 13–25 in *Number theory* (Montreal, 2002), edited by H. Kisilevsky and E. Z. Goren, CRM Proc. Lecture Notes **36**, Amer. Math. Soc., Providence, RI, 2004. MR 2005f:11130 Zbl 1153.11316

[Besser 2005] A. Besser, "p-adic Arakelov theory", *J. Number Theory* **111**:2 (2005), 318–371. MR 2006j:14029 Zbl 1079.14033

[Blasius 1986] D. Blasius, "On the critical values of Hecke L-series", *Ann. Math.* (2) **124**:1 (1986), 23–63. MR 88i:11035 Zbl 0608.10029

[Bump 1997] D. Bump, *Automorphic forms and representations*, Cambridge Stud. Adv. Math. **55**, Cambridge Univ., 1997. MR 97k:11080 Zbl 0868.11022

[Bump et al. 1990] D. Bump, S. Friedberg, and J. Hoffstein, "Nonvanishing theorems for L-functions of modular forms and their derivatives", *Invent. Math.* **102**:3 (1990), 543–618. MR 92a:11058 Zbl 0721.11023

[Bushnell and Henniart 2006] C. J. Bushnell and G. Henniart, *The local Langlands conjecture for* GL(2), Grundlehren der math. Wissenschaften **335**, Springer, Berlin, 2006. MR 2007m:22013 Zbl 1100.11041

[Carayol 1986] H. Carayol, "Sur la mauvaise réduction des courbes de Shimura", *Compositio Math.* **59**:2 (1986), 151–230. MR 88a:11058 Zbl 0607.14021

[Casselman 1973] W. Casselman, "On some results of Atkin and Lehner", *Math. Ann.* **201**:4 (1973), 301–314. MR 49 #2558 Zbl 0239.10015

[Coleman and Gross 1989] R. F. Coleman and B. H. Gross, "p-adic heights on curves", pp. 73–81 in *Algebraic number theory* (Berkeley, CA, 1987), edited by J. Coates et al., Adv. Stud. Pure Math. **17**, Academic, Boston, 1989. MR 92d:11057 Zbl 0758.14009

[Deligne and Ribet 1980] P. Deligne and K. A. Ribet, "Values of abelian L-functions at negative integers over totally real fields", *Invent. Math.* **59**:3 (1980), 227–286. MR 81m:12019 Zbl 0434.12009

[Dimitrov 2013] M. Dimitrov, "Automorphic symbols, p-adic L-functions and ordinary cohomology of Hilbert modular varieties", *Amer. J. Math.* **135**:4 (2013), 1117–1155. MR 3086071 Zbl 06203659

[Disegni 2015] D. Disegni, "The p-adic Gross–Zagier formula on Shimura curves", preprint, 2015, Available at http://www.math.mcgill.ca/disegni/papers/pyzz-pst.pdf.

[Faltings 1983] G. Faltings, "Endlichkeitssätze für abelsche Varietäten über Zahlkörpern", *Invent. Math.* **73**:3 (1983), 349–366. MR 85g:11026a Zbl 0588.14026

[Fontaine 1982] J.-M. Fontaine, "Sur certains types de représentations p-adiques du groupe de Galois d'un corps local; construction d'un anneau de Barsotti–Tate", *Ann. Math.* (2) **115**:3 (1982), 529–577. MR 84d:14010 Zbl 0544.14016

[Freitas et al. 2015] N. Freitas, B. V. Le Hung, and S. Siksek, "Elliptic curves over real quadratic fields are modular", *Invent. Math.* **201**:1 (2015), 159–206. MR 3359051 Zbl 06468724

[Gross 1986] B. H. Gross, "On canonical and quasi-canonical liftings", *Invent. Math.* **84**:2 (1986), 321–326. MR 87g:14051 Zbl 0597.14044

[Gross and Zagier 1986] B. H. Gross and D. B. Zagier, "Heegner points and derivatives of L-series", *Invent. Math.* **84**:2 (1986), 225–320. MR 87j:11057 Zbl 0608.14019

[Harris 1993] M. Harris, "L-functions of 2×2 unitary groups and factorization of periods of Hilbert modular forms", *J. Amer. Math. Soc.* **6**:3 (1993), 637–719. MR 93m:11043 Zbl 0779.11023

[Hida 1985] H. Hida, "A p-adic measure attached to the zeta functions associated with two elliptic modular forms, I", *Invent. Math.* **79**:1 (1985), 159–195. MR 86m:11097 Zbl 0573.10020

[Hida 1991] H. Hida, "On p-adic L-functions of $\mathrm{GL}(2) \times \mathrm{GL}(2)$ over totally real fields", *Ann. Inst. Fourier* (*Grenoble*) **41**:2 (1991), 311–391. MR 93b:11052 Zbl 0725.11025

[Hida and Tilouine 1993] H. Hida and J. Tilouine, "Anti-cyclotomic Katz p-adic L-functions and congruence modules", *Ann. Sci. École Norm. Sup.* (4) **26**:2 (1993), 189–259. MR 93m:11044 Zbl 0778.11061

[Howard 2004] B. Howard, "Iwasawa theory of Heegner points on abelian varieties of GL_2 type", *Duke Math. J.* **124**:1 (2004), 1–45. MR 2005f:11117 Zbl 1068.11071

[Hsieh 2014] M.-L. Hsieh, "Eisenstein congruence on unitary groups and Iwasawa main conjectures for CM fields", *J. Amer. Math. Soc.* **27**:3 (2014), 753–862. MR 3194494 Zbl 06346502

[Iovita 2000] A. Iovita, "Formal sections and de Rham cohomology of semistable abelian varieties", *Israel J. Math.* **120**:B (2000), 429–447. MR 2002g:14026 Zbl 1045.14503

[Jacquet 1972] H. Jacquet, *Automorphic forms on* GL(2), part II, Lecture Notes Math. **278**, Springer, Berlin, 1972. MR 58 #27778 Zbl 0243.12005

[Kobayashi 2013] S. Kobayashi, "The p-adic Gross–Zagier formula for elliptic curves at supersingular primes", *Invent. Math.* **191**:3 (2013), 527–629. MR 3020170 Zbl 1300.11053

[Kobayashi 2014] S. Kobayashi, "The p-adic height pairing on abelian varieties at non-ordinary primes", pp. 265–290 in *Iwasawa theory 2012: state of the art and recent advances* (Heidelberg, 2012), edited by T. Bouganis and O. Venjakob, Contrib. Math. Comput. Sci. **7**, Springer, Berlin, 2014. Zbl 06455256

[Kolyvagin 1988] V. A. Kolyvagin, "Finiteness of $E(\mathbf{Q})$ and $Ш(E, \mathbf{Q})$ for a subclass of Weil curves", *Izv. Akad. Nauk SSSR Ser. Mat.* **52**:3 (1988), 522–540. In Russian; translated in *Math. USSR Izv.* **32**:3 (1989), 523–541. MR 89m:11056 Zbl 0662.14017

[Kolyvagin 1991] V. A. Kolyvagin, "On the structure of Shafarevich–Tate groups", pp. 94–121 in *Algebraic geometry* (Chicago, 1989), edited by S. Bloch et al., Lecture Notes Math. **1479**, Springer, Berlin, 1991. MR 94b:11055 Zbl 0753.14025

[Kolyvagin and Logachëv 1991] V. A. Kolyvagin and D. Y. Logachëv, "Finiteness of Ш over totally real fields", *Izv. Akad. Nauk SSSR Ser. Mat.* **55**:4 (1991), 851–876. In Russian; translated in *Math. USSR Izv.* **39**:1 (1992), 829–853. MR 93d:11063 Zbl 0791.14019

[Le Hung 2014] B. V. Le Hung, *Modularity of some elliptic curves over totally real fields*, Ph.D. thesis, Harvard University, 2014, Available at http://search.proquest.com/docview/1557761503. MR 3251352

[Manin 1976] Yu. I. Manin, "Non-Archimedean integration and p-adic Jacquet–Langlands L-functions", *Uspekhi Mat. Nauk* **31**:1 (1976), 5–54. In Russian; translated in *Russ. Math. Surv.* **31**:1 (1976), 5–57. MR 54 #5194 Zbl 0348.12016

[Meusers 2007] V. Meusers, "Canonical and quasi-canonical liftings in the split case", pp. 87–98 in *Argos seminar on intersections of modular correspondences* (Bonn, 2003–2004), Astérisque **312**, Société Math. France, Paris, 2007. MR 2008g:11101 Zbl 1223.14051

[Nekovář 1993] J. Nekovář, "On p-adic height pairings", pp. 127–202 in *Séminaire de Théorie des Nombres* (Paris, 1990–1991), edited by S. David, Progr. Math. **108**, Birkhäuser, Boston, 1993. MR 95j:11050 Zbl 0859.11038

[Nekovář 1995] J. Nekovář, "On the p-adic height of Heegner cycles", *Math. Ann.* **302**:4 (1995), 609–686. MR 96f:11073 Zbl 0841.11025

[Panchishkin 1988] A. A. Panchishkin, "Convolutions of Hilbert modular forms and their non-Archimedean analogues", *Mat. Sb.* (*N.S.*) **136**:4 (1988), 574–587. In Russian; translated in *Math. USSR Sb.* **64**:2 (1989), 571–584. MR 89k:11033 Zbl 0656.10021

[Perrin-Riou 1987] B. Perrin-Riou, "Points de Heegner et dérivées de fonctions L p-adiques", *Invent. Math.* **89**:3 (1987), 455–510. MR 89d:11034 Zbl 0645.14010

[Perrin-Riou 1988] B. Perrin-Riou, "Fonctions L p-adiques associées à une forme modulaire et à un corps quadratique imaginaire", *J. London Math. Soc.* (2) **38**:1 (1988), 1–32. MR 89m:11043 Zbl 0656.10019

[Prasanna 2009] K. Prasanna, "Arithmetic properties of the Shimura–Shintani–Waldspurger correspondence", *Invent. Math.* **176**:3 (2009), 521–600. MR 2011d:11102 Zbl 1213.11102

[Raghuram and Tanabe 2011] A. Raghuram and N. Tanabe, "Notes on the arithmetic of Hilbert modular forms", *J. Ramanujan Math. Soc.* **26**:3 (2011), 261–319. MR 2012m:11060 Zbl 1272.11069

[Schneider 1985] P. Schneider, "p-adic height pairings, II", *Invent. Math.* **79**:2 (1985), 329–374. MR 86j:11063 Zbl 0571.14021

[Serre 1978] J.-P. Serre, "Sur le résidu de la fonction zêta p-adique d'un corps de nombres", *C. R. Acad. Sci. Paris Sér. A* **287**:4 (1978), A183–A188. MR 58 #22024 Zbl 0393.12026

[Shimura 1978] G. Shimura, "The special values of the zeta functions associated with Hilbert modular forms", *Duke Math. J.* **45**:3 (1978), 637–679. MR 80a:10043 Zbl 0394.10015

[Shimura 1981] G. Shimura, "The periods of certain automorphic forms of arithmetic type", *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **28**:3 (1981), 605–632. MR 84f:10040 Zbl 0499.10027

[Shimura 1983] G. Shimura, "Algebraic relations between critical values of zeta functions and inner products", *Amer. J. Math.* **105**:1 (1983), 253–285. MR 84j:10038 Zbl 0518.10032

[Shimura 1988] G. Shimura, "On the critical values of certain Dirichlet series and the periods of automorphic forms", *Invent. Math.* **94**:2 (1988), 245–305. MR 90e:11069 Zbl 0656.10018

[Shnidman 2014] A. Shnidman, "p-adic heights of generalized Heegner cycles", preprint, 2014. arXiv 1407.0785v2

[Skinner and Urban 2014] C. Skinner and E. Urban, "The Iwasawa main conjectures for GL_2", *Invent. Math.* **195**:1 (2014), 1–277. MR 3148103 Zbl 1301.11074

[Urban 2014] E. Urban, "Nearly overconvergent modular forms", pp. 401–441 in *Iwasawa theory 2012: state of the art and recent advances* (Heidelberg, 2012), edited by T. Bouganis and O. Venjakob, Contrib. Math. Comput. Sci. **7**, Springer, Berlin, 2014. Zbl 06455261

[Waldspurger 1985] J.-L. Waldspurger, "Sur les valeurs de certaines fonctions L automorphes en leur centre de symétrie", *Compositio Math.* **54**:2 (1985), 173–242. MR 87g:11061b Zbl 0567.10021

[Wan 2013] X. Wan, "Iwasawa main conjecture for Hilbert modular forms", preprint, 2013, Available at http://www.math.columbia.edu/∼xw2295/Hilbert Modular Forms.pdf.

[Yoshida 1994] H. Yoshida, "On the zeta functions of Shimura varieties and periods of Hilbert modular forms", *Duke Math. J.* **75**:1 (1994), 121–191. MR 95d:11059 Zbl 0823.11018

[Yoshida 1995] H. Yoshida, "On a conjecture of Shimura concerning periods of Hilbert modular forms", *Amer. J. Math.* **117**:4 (1995), 1019–1038. MR 96d:11056 Zbl 0841.11024

[Yuan et al. 2013] X. Yuan, S.-W. Zhang, and W. Zhang, *The Gross–Zagier formula on Shimura curves*, vol. 184, Ann. Math. Stud., Princeton Univ., 2013. MR 3237437 Zbl 1272.11082

[Zarhin 1990] Y. G. Zarhin, "p-adic heights on abelian varieties", pp. 317–341 in *Séminaire de Théorie des Nombres* (Paris, 1987–1988), edited by C. Goldstein, Progr. Math. **81**, Birkhäuser, Boston, 1990. MR 91f:11043 Zbl 0707.14040

[Zhang 2001a] S. Zhang, "Heights of Heegner points on Shimura curves", *Ann. Math.* (2) **153**:1 (2001), 27–147. MR 2002g:11081 Zbl 1036.11029

[Zhang 2001b] S.-W. Zhang, "Gross–Zagier formula for GL_2", *Asian J. Math.* **5**:2 (2001), 183–290. MR 2003k:11101 Zbl 1111.11030

[Zhang 2004] S.-W. Zhang, "Gross–Zagier formula for GL(2), II", pp. 191–214 in *Heegner points and Rankin L-series* (Berkeley, CA, 2001), edited by H. Darmon and S.-W. Zhang, Math. Sci. Res. Inst. Publ. **49**, Cambridge Univ., 2004. MR 2005k:11121 Zbl 1126.11026

[Zhang 2014] W. Zhang, "Selmer groups and the indivisibility of Heegner points", *Camb. J. Math.* **2**:2 (2014), 191–253. MR 3295917 Zbl 06409349

Communicated by John Henry Coates
Received 2014-09-18 Revised 2015-04-27 Accepted 2015-06-11

daniel.disegni@mcgill.ca *Department of Mathematics and Statistics, McGill University, 805 Shebrooke Street West, Montreal, QC H3A 0B9, Canada*

msp

ALGEBRA AND NUMBER THEORY 9:7 (2015)
dx.doi.org/10.2140/ant.2015.9.1647

Calculabilité de la cohomologie étale modulo ℓ

David A. Madore et Fabrice Orgogozo

À Jean-Louis Colliot-Thélène, qui nous a beaucoup appris

Soient X un schéma algébrique sur un corps algébriquement clos et ℓ un nombre premier inversible sur X. D'après le théorème 1.1 de (SGA $4\frac{1}{2}$, Th. finitude), les groupes de cohomologie étale $\mathrm{H}^i(X, \mathbb{Z}/\ell\mathbb{Z})$ sont de dimension finie. Utilisant une variante ℓ-adique des bons voisinages d'Artin et des résultats élémentaires sur la cohomologie des pro-ℓ groupes, on exprime la cohomologie de X comme colimite bien contrôlée de celle de topos construits sur des $\mathrm{B}G$, où les G sont des ℓ-groupes finis calculables. On en déduit que les nombres de Betti modulo ℓ de X sont algorithmiquement calculables (au sens de Church–Turing). La première partie du texte est consacrée à la démonstration de ce fait et de quelques compléments naturels. Elle s'appuie sur les outils de la seconde partie, dédiée à la géométrie algébrique effective.

Let X be an algebraic scheme over an algebraically closed field and ℓ a prime number invertible on X. According to Theorem 1.1 of (SGA $4\frac{1}{2}$, Th. finitude), the étale cohomology groups $\mathrm{H}^i(X, \mathbb{Z}/\ell\mathbb{Z})$ are finite-dimensional. Using an ℓ-adic variant of Artin's good neighborhoods and elementary results on the cohomology of pro-ℓ groups, we express the cohomology of X as a well controlled colimit of that of toposes constructed on $\mathrm{B}G$ where the G are computable finite ℓ-groups. From this, we deduce that the Betti numbers modulo ℓ of X are algorithmically computable (in the sense of Church and Turing). The proof of this fact, along with certain related results, occupies the first part of this paper. This relies on the tools collected in the second part, which deals with computational algebraic geometry.

MSC2010 : primary 14F20; secondary 03D99, 12G05, 12Y05, 13P10, 14A20, 14F35, 18G30, 20E18, 55P20, 55T05.

Mots-clefs : cohomologie étale, cohomologie galoisienne, descente cohomologique, suite spectrale, schéma simplicial, groupe profini, espace d'Eilenberg–MacLane, voisinage d'Artin, champ algébrique, gerbe, géométrie algébrique effective, calculabilité, étale cohomology, Galois cohomology, cohomological descent, spectral sequence, simplicial scheme, profinite group, Eilenberg–MacLane space, Artin's neighborhood, stack, effective algebraic geometry, computability.

Introduction

L'objet principal de ce texte est de démontrer le théorème suivant, ainsi que la variante relative 0.9.

Théorème 0.1. *Il existe un algorithme calculant la cohomologie étale* $\mathrm{H}^i(X, \mathbb{F}_\ell)$ *à coefficients dans* $\mathbb{F}_\ell$ *d'un schéma algébrique* X *sur un corps algébriquement clos de caractéristique différente de* ℓ, *ainsi que l'application* $\mathrm{H}^i(X, \mathbb{F}_\ell) \to \mathrm{H}^i(Y, \mathbb{F}_\ell)$ *déduite par fonctorialité d'un morphisme* $Y \to X$.

Bien entendu, il faut préciser l'énoncé et notamment ce qu'on entend par « calculer » : nous rappelons dans la partie II les faits essentiels dont nous aurons besoin sur les corps calculables et la calculabilité des opérations algébriques. Calculer le groupe $\mathrm{H}^i(X, \mathbb{F}_\ell)$ signifie notamment en calculer la dimension, en fonction de i, ℓ et des équations de X, et calculer l'application $\mathrm{H}^i(X, \mathbb{F}_\ell) \to \mathrm{H}^i(Y, \mathbb{F}_\ell)$ signifie en calculer la matrice dans une base déterminée par l'algorithme. (Voir 0.4 ci-dessous et ¶ 9.1.2–9.1.3 pour des précisions.)

L'énoncé précédent répond notamment à la question posée en [Poonen, Testa et van Luijk 2015, hypothèse 7.4] et également considérée dans [Edixhoven et Couveignes 2011, chapitre 1 et chapitre 15, p. 401], où l'accent est mis sur la dépendance du temps d'exécution en ℓ.

En caractéristique nulle ce résultat est déjà connu : voir par exemple [Simpson 2008, corollaire 2.5] ou [Poonen, Testa et van Luijk 2015, §7.2], qui calcule aussi l'action galoisienne lorsque le schéma X est obtenu par extension des scalaires d'un corps de caractéristique nulle à une clôture algébrique. Pour une discussion du problème de la calculabilité des groupes d'homotopie ou d'homologie en topologie algébrique, voir par exemple [Sergeraert 1994].

0.2. Rappelons [Deligne 1980, 5.2.2] brièvement une définition *à la Čech* de ces groupes de cohomologie étale. Soit X une variété algébrique sur un corps algébriquement clos dénombrable de caractéristique $p \neq \ell$ (par exemple $\overline{\mathbb{F}_p}$). Il existe un système projectif, indexé par les entiers naturels α, de recouvrements étales $X_\alpha \twoheadrightarrow X$, cofinal au sens suivant : pour tout $U \twoheadrightarrow X$ étale, il existe une factorisation d'un $X_\alpha \twoheadrightarrow X$ à travers U. Notons $X_{\alpha\bullet}$ le cosquelette du morphisme $X_\alpha \to X$ c'est-à-dire le schéma simplicial $X_{\alpha n} := X_\alpha \times_X \cdots \times_X X_\alpha$ ($n+1$ facteurs). La cohomologie de Čech $\check{\mathrm{H}}^i(X_{\alpha\bullet}, \mathbb{Z}/\ell\mathbb{Z})$ est, par définition, celle de l'ensemble simplicial $\pi_0(X_{\alpha\bullet})$. (Pour tout ensemble simplicial, on peut considérer le $\mathbb{Z}/\ell\mathbb{Z}$-module cosimplicial naturellement associé puis le complexe dont les dérivations sont les sommes alternées des faces (cf. [SGA 4_2 1972, V, §1.0 et §2.3 ; Milne 1980, III, §2]).) Si X est quasi-projective, il résulte de [Artin 1971, corollaire 4.2] que le groupe $\mathrm{H}^i(X, \mathbb{Z}/\ell\mathbb{Z})$ est isomorphe à la colimite des $\check{\mathrm{H}}^i(X_{\alpha\bullet}, \mathbb{Z}/\ell\mathbb{Z})$. Le problème auquel on est immédiatement confronté est que, donnés k, les $X_\alpha \to X$ et ℓ, il n'est *a priori* pas évident de calculer deux entiers $\alpha \leq \beta$ tels que $\mathrm{H}^i(X, \mathbb{Z}/\ell\mathbb{Z}) = \mathrm{Im}\big(\check{\mathrm{H}}^i(X_{\alpha\bullet}, \mathbb{Z}/\ell\mathbb{Z}) \to \check{\mathrm{H}}^i(X_{\beta\bullet}, \mathbb{Z}/\ell\mathbb{Z})\big)$ (ces entiers existent car le système inductif $\check{\mathrm{H}}^i(X_{\alpha\bullet}, \mathbb{Z}/\ell\mathbb{Z})$ de groupes abéliens finis, ayant une colimite finie, est « essentiellement constant » au sens de la section 5 ; voir notamment 5.1).

0.3. ***Stratégie.*** Inspirés par des travaux de Michael Artin [SGA 4_3 1973, XI] et Gerd Faltings [1988, §2], nous nous ramenons au cas où l'on peut se restreindre dans la description précédente à des *revêtements* étales $X_\alpha \to X$ galoisiens de groupe un ℓ-groupe. Nous montrons alors que le système inductif $\check{\mathrm{H}}^i(X_{\alpha\bullet}, \mathbb{Z}/\ell\mathbb{Z})$ — il s'agit maintenant de cohomologie de ℓ-groupes — est « explicitement » essentiellement constant. La technique utilisée pour résoudre (ou plutôt ignorer) les divers problèmes d'extension que l'on rencontre est semblable à celle de [Schön 1991, chapitres I–II] (également connue, indépendamment de [Schön 1991], de Ofer Gabber). La réduction à des espaces « $K(\pi, 1)$ » n'est possible que localement pour la topologie de la descente cohomologique universelle : si X n'est pas lisse,

on utilise un théorème de résolution des singularités de A. Johan de Jong. (En particulier, la *topologie des altérations* est suffisamment fine pour notre propos.)

Les ingrédients essentiels de la démonstration, présentés en §1–8, sont résumés en §10 qui récapitule l'algorithme de calcul des nombres de Betti.

0.4. Cette approche permet également de résoudre le problème posé à la fin de 0.2. On montre en effet que l'on peut obtenir pour chaque i des cocycles (hyper-Čech) pour une base de $\mathrm{H}^i(X, \mathbb{Z}/\ell\mathbb{Z})$ et, pour tout autre hyperrecouvrement $X_\bullet \to X$ pour la topologie des altérations, le moyen de développer l'image dans cette base d'un cocycle (hyper-Čech) par le morphisme $\check{\mathrm{H}}^i(X_\bullet, \mathbb{Z}/\ell\mathbb{Z}) \to \mathrm{H}^i(X, \mathbb{Z}/\ell\mathbb{Z})$ (voir 8.3). Comme nous le fait remarquer Pierre Deligne, il n'est pas difficile d'en déduire un calcul de $\mathrm{R}\Gamma(X, \mathbb{Z}/\ell\mathbb{Z})$ (voir 8.4).

Remarque 0.5. Dans l'énoncé du théorème 0.1, le schéma X est supposé décrit explicitement, c'est-à-dire par des équations le définissant (ou définissant un atlas d'ouverts affines : cf. §16 pour les détails). Il est donc tentant de se demander quelles constructions naturelles, par exemple solutions de problèmes universels, peuvent être ainsi décrites explicitement par des équations. Cette question fait l'objet d'une vaste littérature ; signalons simplement ici les articles [Anderson 2002] (jacobienne ; voir aussi [Mumford 1975]) et [Haiman et Sturmfels 2004] (schéma de Hilbert). Bien entendu, nous utiliserons d'autres résultats de ce type au cours de la démonstration ; cf. par exemple ¶ 15.5, où l'on « calcule » la normalisation.

Signalons maintenant quelques améliorations du théorème 0.1. D'autres améliorations et compléments, ainsi que quelques questions, figurent dans la section 11.

0.6. Notons tout d'abord que la cas de la cohomologie à support compact, et plus généralement de la cohomologie relative (c'est-à-dire modulo un fermé), en résulte formellement ; cf. ¶ 11.2. Nous avons énoncé 0.1 avec des coefficients dans $\mathbb{Z}/\ell\mathbb{Z}$ pour plus de simplicité, mais nous traiterons plus généralement le cas de la cohomologie à valeurs dans $\mathbb{Z}/\ell^n\mathbb{Z}$ (ou même à valeurs dans un faisceau constructible sur un tel anneau ; voir 0.9 *infra*).

0.7. ***Stratifications.*** En analysant plus précisément le formalisme de calculabilité sur les éléments d'un corps arbitraire, comme nous le présentons dans un texte complémentaire au présent article ([Madore et Orgogozo 2014] ; ou cf. [Bürgisser, Clausen et Shokrollahi 1997, proposition 4.27]), il n'est guère difficile de montrer que les résultats énoncés ci-dessus, interprétés dans un modèle de calcul différent où ils restent encore valables, entraînent automatiquement la calculabilité de stratifications associées aux objets calculés. Plus exactement, on peut montrer les affirmations suivantes, où ℓ est un nombre premier *fixé*, inversible sur les schémas considérés :

- si les équations de X comportent des indéterminées, on peut calculer les équations des parties constructibles de l'espace (affine) de ces indéterminées correspondant

à une stratification par la dimension : autrement dit, donnés ℓ et n et un morphisme de type fini $\mathscr{X} \to \mathbb{A}^r_k$ (où k est un corps algébriquement clos calculable, cf. 12.1), on peut calculer une partition de $\mathbb{A}^r_k$ en un nombre fini de parties constructibles sur chacune desquelles $\mathrm{H}^i(X, \mathbb{Z}/\ell^n\mathbb{Z})$ (où X désigne une fibre en un point géométrique de la partie) a un type d'isomorphisme [1] donné, qu'on peut calculer ; il en va de même, par exemple, du type de $\mathrm{H}^i(X, \mathbb{Z}/\ell^n\mathbb{Z}) \to \mathrm{H}^i(Y, \mathbb{Z}/\ell^n\mathbb{Z})$ (pour un morphisme $\mathscr{X} \to \mathscr{Y}$ sur $\mathbb{A}^r_k$) ;

- si X est un schéma de type fini sur un ouvert de $\operatorname{Spec}\mathbb{Z}$, on peut calculer, en fonction de ℓ et n (et de la description de X), un p_0 tel que le type de $\mathrm{H}^i(X_p, \mathbb{Z}/\ell^n\mathbb{Z})$ ne dépende pas de p lorsque $p \geq p_0$, où X_p désigne une fibre géométrique au-dessus de p ; il en va de même du type de $\mathrm{H}^i(X_p, \mathbb{Z}/\ell^n\mathbb{Z}) \to \mathrm{H}^i(Y_p, \mathbb{Z}/\ell^n\mathbb{Z})$;
- variante de l'affirmation précédente : donné un morphisme de type fini $\mathscr{X} \to \mathbb{A}^r_{\mathbb{Z}[1/\ell]}$, on peut calculer une partition de $\mathbb{A}^r_{\mathbb{Z}[1/\ell]}$ en un nombre fini de parties constructibles sur chacune desquelles $\mathrm{H}^i(X, \mathbb{Z}/\ell^n\mathbb{Z})$ a un type d'isomorphisme fixé, où X désigne une fibre en un point géométrique de la partie.

Notons que l'*existence* d'une stratification (resp. d'un nombre premier p_0) comme ci-dessus est conséquence des résultats généraux de constructibilité et commutation aux changements de base. Les démonstrations de [Orgogozo 2013] (resp. [Katz et Laumon 1985, théorème 3.3.2]), de nature géométrique, devraient fournir une stratification (resp. un nombre premier p_0) explicite qui convienne pour *chaque* nombre premier ℓ inversible sur les schémas considérés.

Comme l'observe Olivier Wittenberg [Poonen, Testa et van Luijk 2015, proposition 8.3], le théorème 0.1 (étendu au cas des coefficients $\mathbb{Z}/\ell^n\mathbb{Z}$) a le corollaire suivant.

Corollaire 0.8. *Il existe un algorithme calculant la structure de la partie de torsion du groupe de cohomologie ℓ-adique $\mathrm{H}^i(X, \mathbb{Z}_\ell)$ d'une variété* propre et lisse *X sur un corps algébriquement clos de caractéristique différente de ℓ.*

(Le rang des $\mathrm{H}^i(X, \mathbb{Z}_\ell)$ se calcule, dans le cas d'une variété sur un corps fini, en comptant les points de celles-ci et en utilisant une borne a priori, et dans le cas général en se ramenant au cas des corps finis : cf. [Poonen, Testa et van Luijk 2015].) Par contre, hormis dans le cas propre et lisse, permettant d'utiliser des arguments de poids, on ne sait malheureusement rien dire de la cohomologie *ℓ-adique* (cf. 11.5).

On déduira du théorème 0.1 le résultat suivant (voir 11.4).

Théorème 0.9. *Soit $f : X \to S$ un morphisme de schémas algébriques sur un corps algébriquement clos k. Pour tout faisceau abélien $\mathscr{F}$ constructible sur X, de torsion*

1. Par « type d'isomorphisme » d'un ℓ-groupe abélien fini V, nous entendons ici bien sûr des $d_1 \leq \cdots \leq d_s$ tels que $V \simeq (\mathbb{Z}/\ell^{d_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/\ell^{d_s}\mathbb{Z})$; et par type d'isomorphisme d'un morphisme entre deux tels groupes, la donnée d'une matrice à équivalence près.

inversible sur k, et tout entier $i \geq 0$, on peut explicitement calculer le faisceau $\mathrm{R}^i f_\star \mathscr{F}$, fonctoriellement en $\mathscr{F}$.

Il en résulte formellement que l'on peut calculer $\mathrm{R}^i f_! \mathscr{F}$: appliquer le théorème à une compactification de f et au prolongement par zéro correspondant de $\mathscr{F}$.

(Idéalement, on aimerait plutôt déduire 0.1 du théorème 0.9, démontré par dévissage.)

0.10. ***Remarques sur la notion d'algorithme.*** La « calculabilité » dans le titre de cet article, et le mot « algorithme calculant » dans l'énoncé du théorème 0.1 doivent se comprendre au sens (standard) de Church–Turing, c'est-à-dire le fait que les fonctions annoncées soient (générales) récursives, autrement dit calculables par un ordinateur idéalisé, par exemple une machine de Turing ou une machine à registres : cf. [Odifreddi 1989, définition I.1.7 et théorèmes I.4.3 et I.7.9]. Voir 12.1 sur la manière dont la machine doit manipuler les éléments du corps de base.

Soulignons que le fait de travailler avec des fonctions générales récursives nous permet d'effectuer des « recherches non bornées » (ce qu'on appelle aussi utiliser l'« opérateur μ de Kleene ») : si pour chaque m il existe n vérifiant une certaine propriété $\boldsymbol{P}(m,n)$ elle-même calculable, alors la fonction $\mu_n \boldsymbol{P}$ qui à m associe le plus petit n vérifiant $\boldsymbol{P}(m,n)$ est calculable (l'idée étant qu'on parcourt les n jusqu'à en trouver un qui vérifie la propriété recherchée).

Nous utiliserons notamment librement ce résultat pour construire des objets géométriques : dès lors qu'un théorème garantit l'existence d'un objet géométrique (schéma, morphisme de schémas,...) possédant une propriété *algorithmiquement testable*, on peut calculer algorithmiquement un tel objet, simplement en énumérant toutes les équations possibles pour les objets géométriques en question et en testant la propriété souhaitée jusqu'à en trouver un qui vérifie la condition voulue (cf. 12.8 pour plus de détails).

Pour une discussion sur la question de savoir dans quelle mesure on pourrait se passer de ce procédé, et si les fonctions dont on affirme la calculabilité seraient en fait *primitivement* récursives, voir ¶ 11.6 plus bas.

0.11. ***Leitfaden.*** Des efforts ont été faits pour rendre la lecture des deux parties largement indépendante chacune de l'autre. L'ordre logique est de commencer par la partie II, mais le lecteur prêt à admettre la calculabilité des opérations classiques de la géométrie algébrique (ainsi que la représentation algorithmique des objets) pourra se contenter de lire la partie I. Inversement, la partie II peut servir de présentation autonome de certains résultats de géométrie algébrique effective.

Par ailleurs, le lecteur souhaitant démontrer les affirmations énoncées en 0.7 doit commencer par la lecture du texte complémentaire [Madore et Orgogozo 2014], et ensuite interpréter la notion de calculabilité utilisée tout au long du présent article comme faisant référence à la notion universelle introduite dans ce complément.

I. Cohomologie étale

1. $K(\pi, 1)$ pro-ℓ

Les résultats de cette section, essentiellement dus à Ofer Gabber,[2] permettent d'établir une variante (1.4.7) de [Friedlander 1982, théorème 11.7] (dont l'énoncé est rappelé en 1.3.3). Ceux qui préfèrent admettre les résultats de cette section pourront se contenter de lire les définitions 1.3.1 à 1.3.4 et 1.4.4, ainsi que les propositions 1.4.7 et 1.4.12.

Il est fort probable que les hypothèses nœthériennes faites dans cette section sur les schémas puissent être remplacées par des hypothèses de finitude plus faibles (cohérence, ouverture des composantes connexes).

1.1. *Champs ℓ-monodromiques : définitions.*

1.1.1. Soit $\mathscr{C}$ un champ en groupoïdes sur un schéma localement nœthérien S, muni de la topologie étale [Giraud 1971, II.1.2.1.3]. Rappelons que l'on note $\pi_0(\mathscr{C})$ le faisceau associé au préfaisceau

$$U/S \mapsto \{\text{classes d'isomorphie d'objets de } \mathscr{C}(U)\}$$

— c'est aussi le faisceau des *sous-gerbes maximales* (= strictement pleines ; [Giraud 1971, III.2.1.3]) de $\mathscr{C}$ — et, pour chaque section locale $c_U \in \mathrm{Ob}\,\mathscr{C}(U)$, où U/S est un ouvert étale, $\pi_1(\mathscr{C}, c_U)$ le faisceau en groupes $\underline{\mathrm{Aut}}(c_U)$ sur U. Le champ $\mathscr{C}$ est dit *constructible* si le faisceau $\pi_0(\mathscr{C})$ et les divers $\pi_1(\mathscr{C}, c)$ sont constructibles. Dans [SGA 1 2003, XIII, §0], un tel champ est dit 1-constructible. (Comparer avec [Giraud 1971, VII.2.2.1] et [Orgogozo 2003, §2].)

1.1.2. Un *lien* sur S est une section cartésienne (sur S) du champ associé au préchamp des faisceaux de groupes *à automorphisme intérieur près* [Giraud 1971, IV.1.1] ; un tel objet peut être représenté par un triplet constitué d'un recouvrement étale S' de S, d'un faisceau en groupes G' sur S' et d'un isomorphisme extérieur $\phi \in \mathsf{Isomex}(p_1^\star G', p_2^\star G')$, où $p_1, p_2 : S' \times_S S' \rightrightarrows S'$ sont les deux projections, satisfaisant la condition de cocycle usuelle [Deligne et al. 1982, II, appendice].

1.1.3. À tout champ localement connexe-non vide (*gerbe*) $\mathscr{G}$ sur S, est associé un lien $\mathscr{L}$; si $c_{S'} \in \mathrm{Ob}\,\mathscr{G}(S')$ pour S' couvrant S, on peut prendre $G' = \pi_1(\mathscr{G}, c_{S'})$ dans la description précédente : le lien « est » le faisceau des groupes d'automorphismes de sections locales, à conjugaison près. On dit que $\mathscr{G}$ est *lié* par le lien $\mathscr{L}$ ou encore que $\mathscr{G}$ est une $\mathscr{L}$-gerbe.

Si $\mathscr{G}$ est le champ $\mathsf{B}G$ des torseurs sous un S-faisceau en groupes G, son lien est celui naturellement associé à G, représenté par le triplet $(S' = S, G' = G, \phi = \mathrm{Id})$.

2. Les auteurs sont bien entendu seuls responsables des éventuelles imprécisions ou erreurs dans l'exposition.

Le faisceau des automorphismes de ce lien est le faisceau des automorphismes *extérieurs* de G et l'ensemble des classes d'isomorphie de liens *localement* représentés par le S-schéma en groupes G est naturellement isomorphe à $\mathrm{H}^1(S, \mathsf{Autex}(G))$.

1.1.4. Soit $\mathscr{L}$ un lien sur S. L'ensemble $\mathrm{H}^2(S, \mathscr{L})$ des classes d'équivalences de gerbes liées par $\mathscr{L}$ est naturellement muni d'une action libre et transitive du groupe de cohomologie $\mathrm{H}^2(S, Z(\mathscr{L}))$, où $Z(\mathscr{L})$ désigne le *centre* du lien $\mathscr{L}$. (Voir [Deligne et al. 1982, loc. cit.] et [Giraud 1971, IV, 1.5.3, 3.1.1 et 3.3.3].)

Définition 1.1.5. Soit ℓ un nombre premier. Un objet sur S du type suivant est dit *ℓ-monodromique* s'il satisfait l'une des conditions suivantes :

- un faisceau d'*ensembles* F : s'il est localement constant, constructible, et si pour tout point géométrique s de S, le groupe de monodromie, image de $\pi_1(S, s)$ dans $\mathsf{Aut}(F_s)$, est un ℓ-groupe ;
- un faisceau de *groupes* G : s'il est ℓ-monodromique en tant que faisceau d'ensembles et si ses fibres sont des ℓ-groupes (finis) ;
- un lien $\mathscr{L}$: s'il est *localement* représenté par un ℓ-groupe fini (constant) G et si, sur chaque composante connexe, le $\mathsf{Autex}(\mathsf{G})$-torseur $\mathsf{Isom}_{\mathrm{liens}}(\mathscr{L}, \mathrm{lien}(\mathsf{G}))$ est ℓ-monodromique, où $\mathrm{lien}(\mathsf{G})$ désigne (abusivement) le lien du champ des G-torseurs ;
- un champ $\mathscr{C}$: si le faisceau d'ensembles $\pi_0(\mathscr{C})$ est ℓ-monodromique et si, sur le revêtement correspondant de S, les sous-gerbes maximales sont à liens ℓ-monodromiques.

Nous dirons également qu'un morphisme Y/X est un *ℓ-revêtement* s'il est fini étale galoisien d'ordre une puissance de ℓ.

1.1.6. *Mise en garde.* Un faisceau ℓ-monodromique provient par image inverse du topos $S_{\ell\text{ét}}$ considéré en 1.4.3 mais il n'en est pas de nécessairement de même d'un champ ℓ-monodromique quelconque ; cela reflète le fait qu'une classe dans $\mathrm{H}^2(S, \mathbb{Z}/\ell\mathbb{Z})$ n'est pas nécessairement tuée par un revêtement galoisien d'ordre une puissance de ℓ (cf. 1.1.4).

Remarque 1.1.7. Les faisceaux ℓ-monodromiques sont également utilisés en [Orgogozo 2003, 4.6], où l'on démontre la locale constance générique du type d'homotopie étale pro-ℓ des fibres d'un morphisme de type fini.

1.2. *Champs ℓ-monodromiques : sorites.*

1.2.1. Un faisceau abélien extension (resp. un sous-quotient) de faisceaux abéliens ℓ-monodromiques est également ℓ-monodromique. La lissité (locale constance et constructibilité) résulte de [SGA 4_3 1973, IX, 2.1(ii) et 2.6(ii)]. Que la monodromie d'une extension soit un ℓ-groupe est conséquence immédiate du fait qu'un élément

unipotent de $\mathrm{GL}_n(\mathbb{Z}/\ell^r\mathbb{Z})$ est de ℓ-torsion, c'est-à-dire annulé par une *puissance* de ℓ.

Réciproquement, tout faisceau abélien ℓ-monodromique est extension successive du faisceau constant $\mathbb{Z}/\ell\mathbb{Z}$.

1.2.2. Un faisceau en groupes G est ℓ-monodromique si et seulement si son lien est ℓ-monodromique. (Cette dernière propriété est tautologiquement équivalente au fait que la gerbe $\mathsf{B}G$ des G-torseurs soit ℓ-monodromique.) Pour vérifier ce fait, on peut supposer S connexe, et en choisir un point géométrique s. Les deux derniers termes de la suite exacte

$$1 \to G_s/Z(G_s) \to \mathsf{Aut}(G_s) \to \mathsf{Autex}(G_s) \to 1$$

reçoivent le groupe $\pi_1(S, s)$. Le noyau $G_s/Z(G_s)$ étant un ℓ-groupe, l'image de $\pi_1(S, s)$ dans $\mathsf{Aut}(G_s)$ est un ℓ-groupe si et seulement si l'image de $\pi_1(S, s)$ dans $\mathsf{Autex}(G_s)$ l'est.

1.2.3. *Gerbe quotient.* Par *sous-groupe normal* d'une gerbe $\mathcal{G}$ sur S nous entendons la donnée pour chaque section locale $\sigma \in \mathrm{Ob}\,\mathcal{G}(U)$ d'un sous-faisceau en groupes distingués $N_\sigma \trianglelefteq \underline{\mathsf{Aut}}(\sigma) = \pi_1(\mathcal{G}, \sigma)$ et ceci de façon compatible aux restrictions et aux isomorphismes entre sections locales. La *gerbe quotient* de $\mathcal{G}$ par $N = (N_\sigma)_\sigma$ est, par définition, le champ associé à la catégorie fibrée $\mathcal{G}'$ ayant mêmes objets que $\mathcal{G}$ mais dont les homomorphismes sont les faisceaux quotients $\underline{\mathsf{Hom}}_{\mathcal{G}'}(\sigma, \tau) := \underline{\mathsf{Hom}}_{\mathcal{G}}(\sigma, \tau)/N_\sigma$. On la note $\mathcal{G}/N$. Le morphisme $\mathcal{G} \to \mathcal{G}/N$ est conservatif et couvrant, c'est-à-dire localement surjectif sur les objets et les flèches.

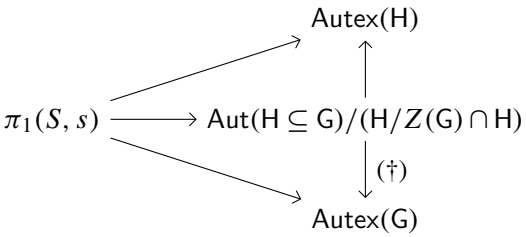
Cette construction s'applique en particulier aux centres $Z_\sigma = Z(\underline{\mathsf{Aut}}(\sigma))$ des faisceaux d'automorphismes locaux. Ici, Z_σ ne « dépend pas » du choix de la section locale et se descend donc à S : il existe un faisceau en groupes abéliens Z et, pour chaque section locale $\sigma \in \mathrm{Ob}\,\mathcal{G}(U)$, un isomorphisme $Z(U) \xrightarrow{\sim} Z_\sigma$ commutant aux restrictions et aux isomorphismes entre sections locales. Lorsque $\mathcal{G}$ est une gerbe des G-torseurs, où G est un faisceau en groupes, la gerbe quotient ainsi obtenue est équivalente à celle des G'-torseurs, où G' est le quotient de G par son centre.

Si σ est une section globale de la gerbe quotient $\mathcal{G}/Z$, la gerbe $\mathcal{H}(\sigma)$ des relèvements de σ à $\mathcal{G}$ [Giraud 1971, IV.2.5.1, 2.5.4] est naturellement une Z-gerbe (cf. [Giraud 1971, 2.5.6.(ii)]). Rappelons que $\mathcal{H}(\sigma)$ est triviale si et seulement si la section σ se relève à $\mathcal{G}$.

Lemme 1.2.4. *Soit $\iota : \mathcal{H} \hookrightarrow \mathcal{G}$ un morphisme fidèle entre gerbes constructibles localement constantes sur un schéma localement nœthérien S. Si $\mathcal{G}$ est ℓ-monodromique, il en est de même de $\mathcal{H}$.*

Démonstration. Supposons S connexe, comme il est loisible de le faire, et choisissons en un point géométrique s. Pour chaque section locale h de $\mathcal{H}$, le morphisme ι induit une injection $\underline{\mathsf{Aut}}_{\mathcal{H}}(h) \hookrightarrow \underline{\mathsf{Aut}}_{\mathcal{G}}(\iota h)$. Il en résulte que, localement, le morphisme

$\mathrm{lien}(\iota) : \mathrm{lien}(\mathscr{H}) \to \mathrm{lien}(\mathscr{G})$ est représenté par une injection de groupes finis $\mathsf{H} \subseteq \mathsf{G}$ et que l'action du groupe fondamental $\pi_1(S, s)$ sur les liens de $\mathscr{H}$ et $\mathscr{G}$ se factorise à travers le morphisme horizontal ci-dessous :



où $\mathsf{Aut}(\mathsf{H} \subseteq \mathsf{G})$ désigne le groupe des automorphismes de G préservant globalement H. Bien entendu, G étant un ℓ-groupe, il en est de même de H. Notons d'autre part que le noyau de la flèche (†) est un ℓ-groupe : c'est un quotient du normalisateur de H dans G. Il en résulte que l'image du morphisme horizontal est un ℓ-groupe, car $\mathscr{G}$ est supposé ℓ-monodromique. Partant, il en est de même de l'image du morphisme $\pi_1(S, s) \to \mathsf{Autex}(\mathsf{H})$. CQFD. □

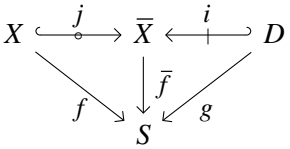
Lemme 1.2.5. *Soient ℓ un nombre premier, G un ℓ-groupe fini et $\mathscr{G}$ une gerbe ℓ-monodromique sur un topos S, localement isomorphe à $\mathsf{B}\mathsf{G}$. Si $\mathrm{H}^2(S, \mathbb{Z}/\ell\mathbb{Z}) = 0$, alors la gerbe $\mathscr{G}$ est triviale : elle a une section globale.*

En d'autres termes, $\mathscr{G}$ est une gerbe de torseurs sous un *faisceau* en groupes, localement isomorphe à G.

Démonstration. Soit $\mathscr{G}'$ la gerbe quotient de $\mathscr{G}$ par son centre Z (cf. 1.2.3). Cette gerbe est localement isomorphe à $\mathsf{B}\mathsf{G}'$, où G' est le quotient de G par son centre (non trivial, à moins que G ne le soit). Par récurrence sur l'ordre du groupe, elle a une section globale. La Z-gerbe $\mathscr{K}$ de ses relèvements à $\mathscr{G}$ (cf. *loc. cit.*) a une classe dans $\mathrm{H}^2(S, Z)$ (1.1.4), nécessairement nulle par hypothèse (utiliser 1.2.1). Il en résulte que la gerbe $\mathscr{K}$ est triviale et, par conséquent, que la section globale de $\mathscr{G}'$ considérée se relève à la gerbe $\mathscr{G}$, qui est donc également triviale. □

1.3. ***Courbes et polycourbes ℓ-élémentaires.*** Rappelons les définitions [SGA 4_3 1973, XI.3.1 et XI.3.2].

1.3.1. On appelle *courbe élémentaire* sur S un morphisme de schémas $f : X \to S$ qui peut être plongé dans un diagramme commutatif



satisfaisant aux conditions suivantes :

(i) j est une immersion ouverte et $X = \overline{X} - D$;

(ii) $\overline{f}$ est une courbe (relative) projective lisse, à fibres géométriquement connexes ;

(iii) g est un revêtement étale à fibres non vides.

Donnés un morphisme projectif $\overline{f}$ et une immersion fermée i, les conditions (i)-(iii) sont algorithmiquement testables : pour la lissité de $\overline{f}$ et g, utiliser 17.2 ; pour la connexité géométrique (resp. non vacuité) des fibres de $\overline{f}$ (resp. de g), on peut supposer que S est un corps en localisant en ses points maximaux (calculables par 15.2), car le faisceau $\overline{f}_\star \underline{2}$ (resp. $g_\star \underline{2}$) est lisse, et utiliser 16.6.

(Notons que si S est *normal* intègre — comme il serait loisible de le supposer pour notre propos — on pourrait également utiliser la connexité géométrique des fibres d'un morphisme propre $Y \to S$ dont la fibre générique est géométriquement connexe.)

1.3.2. On appelle *polycourbe élémentaire* sur S un morphisme de schémas $X \to S$ admettant une factorisation en courbes élémentaires. (Lorsque cela ne semble pas prêter à confusion, on s'autorise à confondre X avec le morphisme $X \to S$.) Notre terminologie, inspirée des courbes et polycourbes *hyperboliques* de [Mochizuki 1999], nous semble plus explicite que les « fibrations élémentaires » et « bons voisinages » de [SGA 4_3 1973, XI]. (Voir aussi [ÉGA V, IV.20 ou V.5 (« Sections hyperplanes et projections coniques ») §13 (« Morphismes élémentaires et théorème de M. Artin »)], où un tel morphisme est dit « polyélémentaire ».)

1.3.3. Soient X un schéma algébrique sur un corps parfait infini k et x un point fermé en lequel $X \to \mathrm{Spec}(k)$ est *lisse*. D'après [SGA 4_3 1973, XI.3.3], il existe un voisinage ouvert de Zariski U de x qui est une polycourbe élémentaire sur k. (Si $k = \mathbb{C}$, l'espace topologique $U(\mathbb{C})$ est un $K(\pi, 1)$ et toute classe de cohomologie en degré > 0 est tuée par un revêtement fini étale $U' \to U$ [SGA 4_3 1973, XI.4.6].) On a le raffinement suivant [Friedlander 1982, théorème 11.7] : il existe un voisinage *étale* de x qui est un « $K(\pi, 1)$ pro-ℓ » (au sens expliqué en ¶ 1.4), où π est un pro-ℓ-groupe extension itérée de pro-ℓ-groupes libres de type fini. Dans cette section et la suivante, on donne une démonstration alternative de ce résultat, amélioré par la possibilité d'utiliser le théorème de résolution des singularités de A. J. de Jong.

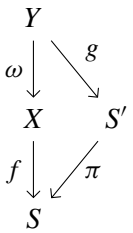
1.3.4. Soit ℓ un nombre premier. Une courbe élémentaire $f : X \to S$ est dite *ℓ-élémentaire* si le faisceau $\mathrm{R}^1 f_\star \mathbb{Z}/\ell\mathbb{Z}$ est ℓ-monodromique (1.1.5). Lorsque ℓ est inversible sur les schémas considérés, ce qui est systématiquement le cas dans cet article, les faisceaux $\mathrm{R}^i f_\star \mathbb{Z}/\ell\mathbb{Z}$ sont automatiquement localement constants constructibles, de formation commutant aux changements de base (cf. [SGA 1 2003, XIII.2.9] pour $i \leq 1$, et [SGA $4\frac{1}{2}$ 1977, Th. finitude, appendice, 1.3.3] pour $i \geq 0$ arbitraire) ; l'hypothèse précédente porte donc sur la *monodromie* de $\mathrm{R}^1 f_\star \mathbb{Z}/\ell\mathbb{Z}$: si S est connexe et $\bar{s}$ en est un point géométrique, on demande que l'image de $\pi_1(S, \bar{s})$

dans $\mathrm{GL}(\mathrm{H}^1(X_{\bar{s}}, \mathbb{Z}/\ell\mathbb{Z}))$ soit un ℓ-groupe. Une *polycourbe* f est dite ℓ-élémentaire si elle admet une factorisation en courbes qui sont ℓ-élémentaires ; nous déduirons de la proposition 1.3.7 ci-dessous que $\mathrm{R}^1 f_\star \mathbb{Z}/\ell\mathbb{Z}$ est alors ℓ-monodromique.

Avant d'énoncer la proposition principale de cette section, commençons par deux lemmes.

Lemme 1.3.5. *Soient X/S une courbe élémentaire* (*resp. ℓ-élémentaire*), *ℓ un nombre premier inversible sur S et Y/X un ℓ-revêtement connexe. Alors, le morphisme $Y \to S$ se factorise à travers un ℓ-revêtement $S' \to S$ en une courbe élémentaire* (*resp. ℓ-élémentaire*) *$Y \to S'$.*

Démonstration. Commençons par l'énoncé non respé. Soit $\overline{X}/S$ une compactification comme en 1.3.1. Par modération et le lemme d'Abhyaṁkar relatif [SGA 1 2003, XIII.5.5], il existe — *localement* sur $\overline{X}$ pour la topologie étale — un prolongement de Y/X en un morphisme de Kummer généralisé relativement à $D \subseteq \overline{X}$ [Grothendieck et Murre 1971, 1.3.9.c]. Celui-ci est unique à isomorphisme unique près et sa source est lisse sur S. Si, en coordonnées locales, $D = V(t)$ et $Y \to X$ est $t = f(y)$, le diviseur E d'équation f/f' est étale sur S. (Si $f(y) = y^n$, avec n inversible sur S, le diviseur E est d'équation y, comme attendu.) [3] Par unicité (forte), on peut recoller ces morphismes construits étale-localement en un morphisme fini et plat $\overline{Y} \to \overline{X}$, prolongeant $Y \to X$, tel que $\overline{Y} \to S$ soit une courbe propre et lisse et $E = \overline{Y} - Y$ soit un diviseur fini étale sur S, à fibres non vides. (Cf. par exemple [Illusie, Laszlo et Orgogozo 2014, IX.2.1] pour une approche log-géométrique, lorsque S est un schéma régulier, cas suffisant dans cet article.) Les fibres de $\overline{Y} \to S$ ne sont pas nécessairement géométriquement connexes mais sa factorisation de Stein répond à la question. (Rappelons que d'après [ÉGA III_2 1963, 7.8.10], la factorisation de Stein d'un morphisme propre et réduit est un revêtement *étale*.)



Montrons maintenant que si $f : X \to S$ est ℓ-élémentaire, il en est de même de $g : Y \to S'$. L'égalité $\pi_\star \mathrm{R}^1 g_\star \mathbb{Z}/\ell\mathbb{Z} = \mathrm{R}^1(f\omega)_\star \mathbb{Z}/\ell\mathbb{Z}$, où π (resp. ω) est le ℓ-revêtement $S' \to S$ (resp. $Y \to X$) nous ramène à montrer que le faisceau $\mathrm{R}^1(f\omega)_\star \mathbb{Z}/\ell\mathbb{Z}$ est ℓ-monodromique car un faisceau $\mathscr{L}$ sur S' est ℓ-monodromique si $\pi_\star \mathscr{L}$ l'est. (Utiliser

3. Notons que si S est réduit, ce qui est suffisant pour nos applications, cela revient à prendre l'image inverse réduite de D.

la surjectivité de la coünité $\pi^\star\pi_\star\mathscr{L} \to \mathscr{L}$.) Enfin, le faisceau $\omega_\star\mathbb{Z}/\ell\mathbb{Z}$ étant abélien ℓ-monodromique, il est extension successive du faisceau constant $\mathbb{Z}/\ell\mathbb{Z}$ et, par conséquent, son image directe par $\mathrm{R}^1 f_\star$ est extension successive de sous-quotients du faisceau $\mathrm{R}^1 f_\star\mathbb{Z}/\ell\mathbb{Z}$, qui est ℓ-monodromique par hypothèse. □

Lemme 1.3.6. *Soient $X \to S$ une courbe élémentaire, ℓ un nombre premier inversible sur S et $\mathscr{C}$ un champ en groupoïdes sur X. Si S est* strictement local *et si $\mathscr{C}$ est ℓ-monodromique, il existe un ℓ-revêtement étale $X' \to X$ tel que $\mathscr{C}' = (X' \to X)^\star\mathscr{C}$ soit isomorphe à un coproduit (fini) de champs de torseurs sous des ℓ-groupes finis.*

Ceci nous permettra de ramener — *étale-localement sur S* — l'étude des champs ℓ-monodromiques à celle des champs de torseurs sous un ℓ-groupe fini.

Démonstration. D'après le lemme précédent (1.3.5) et l'hypothèse sur le champ $\mathscr{C}$, on peut supposer $\pi_0(\mathscr{C})$ constant. Quitte à remplacer $\mathscr{C}$ par une sous-gerbe maximale, on peut supposer que c'est une gerbe. Il suffit de montrer qu'elle a une section : elle sera alors isomorphe à une gerbe ℓ-monodromique de torseurs et l'on pourra conclure par 1.2.2. L'existence d'une section résulte de 1.2.5 et du fait que, par modération et commutation aux changements de base, les groupes $\mathrm{H}^2(X', \mathbb{Z}/\ell\mathbb{Z})$ sont nuls pour tout ℓ-revêtement X' de X. (Rappelons que S est *strictement local*.) □

Proposition 1.3.7. *Soient S un schéma localement nœthérien sur lequel un nombre premier ℓ est inversible et $f : X \to S$ une courbe ℓ-élémentaire. Alors, pour tout champ ℓ-monodromique $\mathscr{C}$ sur X, le champ image directe $f_\star\mathscr{C}$ est également ℓ-monodromique. De plus, la formation de cette image directe commute aux changements de base $S' \to S$.*

Démonstration. La commutation aux changements de base et la lissité reviennent à montrer que si S est strictement local de point fermé s et $\bar\eta$ est un point générique géométrique, les morphismes $\mathscr{C}(X) \to \mathscr{C}(X_s)$ et $\mathscr{C}(X) \to \mathscr{C}(X_{\bar\eta})$ sont des équivalences. Par descente (finie étale) et les deux lemmes précédents (1.3.5, 1.3.6), on se ramène au cas particulier où $\mathscr{C}$ est une gerbe de torseurs sous un ℓ-groupe fini : cela résulte alors des théorèmes bien connus de spécialisation du groupe fondamental (modéré). La constructibilité de l'image directe est également déjà connue [SGA 1 2003, XIII, §2] et résulte d'ailleurs de la démonstration ci-dessous.

Commençons par montrer que pour tout champ $\mathscr{C}$ comme dans l'énoncé, le faisceau $\pi_0(f_\star\mathscr{C})$ est ℓ-monodromique en traitant tout d'abord le cas d'un *faisceau* (c'est-à-dire d'un champ en catégories discrètes). Par passage à la limite, il suffit de montrer que si S est un schéma (non nécessairement nœthérien) n'admettant pas de revêtement connexe d'ordre ℓ (c'est-à-dire : le topos $S_{\ell\text{ét}}$ défini en 1.4.3 est *local*) et s est un point géométrique de S, alors le morphisme $\pi_1^{\text{pro-}\ell}(X \times_S S_{(s)}) \to \pi_1^{\text{pro-}\ell}(X)$ est *surjectif*. (Voir par exemple [Szamuely 2009, chapitre 5] pour une théorie du

groupe fondamental pour les schémas non nécessairement localement nœthériens.) Comme il s'agit de pro-ℓ groupes, cela est équivalent à montrer que la flèche induite par application du foncteur $\mathrm{H}^1(-, \mathbb{Z}/\ell\mathbb{Z})$ à $X \times_S S_{(s)} \to X$ est injective (cf. [Serre 1994, I, §4.2, proposition 23]). Or, on a la suite exacte (Leray)

$$0 \to \mathrm{H}^1(S, f_\star\mathbb{Z}/\ell\mathbb{Z}) \to \mathrm{H}^1(X, \mathbb{Z}/\ell\mathbb{Z}) \to \mathrm{H}^0(S, \mathrm{R}^1 f_\star\mathbb{Z}/\ell\mathbb{Z}),$$

où : $f_\star\mathbb{Z}/\ell\mathbb{Z} = \mathbb{Z}/\ell\mathbb{Z}$ (par connexité des fibres géométriques), $\mathrm{H}^1(S, \mathbb{Z}/\ell\mathbb{Z}) = 0$ (par hypothèse sur S), et $\mathrm{R}^1 f_\star\mathbb{Z}/\ell\mathbb{Z}$ est constant sur S (par hypothèse sur f) de sorte que $\mathrm{H}^0(S, \mathrm{R}^1 f_\star\mathbb{Z}/\ell\mathbb{Z}) = \mathrm{H}^1(X \times_S S_{(s)}, \mathbb{Z}/\ell\mathbb{Z})$. Supposons maintenant que $\mathscr{C}$ est un champ ℓ-monodromique quelconque et montrons que $\pi_0(f_\star\mathscr{C})$ est ℓ-monodromique. D'après ce qui précède, on peut supposer — quitte à remplacer S par un ℓ-revêtement — le faisceau $f_\star\pi_0(\mathscr{C})$ *constant* puis que le champ $\mathscr{C}$ est une *gerbe* (ℓ-monodromique), notée $\mathscr{G}$ dorénavant. Soit $\mathscr{G}'$ son quotient par le centre Z de $\mathscr{G}$ (1.2.3) et posons $\mathscr{L} := \pi_0(f_\star\mathscr{G})$ et $\mathscr{L}' := \pi_0(f_\star\mathscr{G}')$. Le faisceau en groupes abéliens $\mathrm{R}^1 f_\star Z$ agit sur le morphisme (localement constant) canonique $\mathscr{L} \to \mathscr{L}'$ et l'action est transitive sur les fibres : $(\mathrm{R}^1 f_\star Z)\backslash\mathscr{L} \to \mathscr{L}'$ est injective. (Ceci est l'analogue du fait bien connu (voir [Giraud 1971, III, 3.4.5] ou [Serre 1994, I, §5.7]) que si $1 \to Z \to G \to G' \to 1$ est une extension centrale de groupes sur un topos E, le groupe abélien $\mathrm{H}^1(E, Z)$ agit sur $\mathrm{H}^1(E, G)$ par produit contracté, c'est-à-dire par

$$[T] \cdot [P] = [T \overset{Z}{\wedge} P],$$

et l'application $\mathrm{H}^1(E, Z)\backslash\mathrm{H}^1(E, G) \to \mathrm{H}^1(E, G')$, de source le quotient à gauche de $\mathrm{H}^1(E, G)$ par $\mathrm{H}^1(E, Z)$, est *injective*.) Le morphisme f étant ℓ-monodromique, on peut supposer $\mathrm{R}^1 f_\star Z$ constant ; par récurrence, on peut supposer qu'il en est de même de $\mathscr{L}'$. La conclusion résulte alors formellement de l'observation suivante : si un ℓ-groupe abélien fini C agit fidèlement et transitivement sur les fibres d'un morphisme $\mathscr{L} \to \mathscr{L}'$ de faisceaux lisses à but constant, le faisceau $\mathscr{L}$ est ℓ-monodromique. En effet, l'action de la monodromie sur $\mathscr{L}$ se factorise à travers C. Ceci achève la démonstration du fait que $\pi_0(f_\star\mathscr{C})$ est ℓ-monodromique lorsque f est une courbe ℓ-élémentaire et $\mathscr{C}$ est ℓ-monodromique.

Supposons dorénavant le faisceau $\mathscr{L} = \pi_0(f_\star\mathscr{C})$ trivial et considérons une sous-gerbe maximale $\mathscr{G}$ de $f_\star\mathscr{C}$. Il nous faut montrer que son lien est ℓ-monodromique (1.1.5) ; on va utiliser le lemme 1.2.4. On vérifie en effet que le morphisme $f^\star\mathscr{G} \to \mathscr{C}$ déduit par adjonction de l'inclusion $\mathscr{G} \hookrightarrow f_\star\mathscr{C}$ est fidèle : par commutation des images directes au passage aux fibres, on se ramène à observer que si G est un faisceau localement constant sur X et x un point géométrique d'une fibre géométrique X_s, le morphisme $G(X_s) \to G_x$ est injectif. (On utilise la connexité des fibres géométriques du morphisme $f : X \to S$.) D'après *loc. cit.*, il en résulte que la gerbe $f^\star\mathscr{G}$ est ℓ-monodromique. Pour démontrer que le lien de $\mathscr{G}$ est ℓ-monodromique, on est donc ramené à vérifier qu'un faisceau $\mathscr{F}$ sur S est ℓ-monodromique si $f^\star\mathscr{F}$ l'est.

La constructibilité résulte de la surjectivité de f, cf. p. ex. [SGA 4_3 1973, IX.2.8], et la lissité n'est guère plus difficile. Que $\mathscr{F}$ soit ℓ-monodromique résulte, dans le cas où les schémas sont connexes, de la surjectivité du morphisme $\pi_1(X) \to \pi_1(S)$ rappelée en 1.4.7 (premier paragraphe). □

1.4. *Schémas $K(\pi, 1)$.*

1.4.1. Commençons par rappeler quelques résultats de [Abbes et Gros 2011, §9]. Pour chaque schéma X, on note $X_{\text{ét}}$ le topos étale, $X_{f\text{ét}}$ le topos *fini étale* (autrement dit, le topos associé à la sous-catégorie pleine des X-schémas étales finis munie de la topologie étale) et $\rho : X_{\text{ét}} \to X_{f\text{ét}}$ le morphisme évident [ibid., §9.2]. Lorsque X est *cohérent*, le morphisme ρ est un morphisme cohérent entre topos cohérents [ibid., 9.11, 9.13]. Si l'on suppose de plus l'espace topologique quotient $\pi_0(X) = \operatorname{Spec}\operatorname{Idem}(X)$ discret (autrement dit : les composantes connexes de X ouvertes), le morphisme d'adjonction $\mathrm{Id} \to \mathrm{R}\rho_\star\rho^\star$ induit un isomorphisme en degrés 0 et 1, comme on peut le vérifier par passage aux fibres, c'est-à-dire en supposant X simplement connexe (ou encore : $X_{f\text{ét}}$ local). On dit [ibid., 9.20] que le schéma X est un $K(\pi, 1)$ s'il satisfait la condition d'acyclicité suivante : pour tout entier $n \geq 1$ inversible sur X et tout faisceau $\mathscr{L}_f$ de $\mathbb{Z}/n\mathbb{Z}$-modules sur $X_{f\text{ét}}$, le morphisme d'adjonction $\mathscr{L}_f \to \mathrm{R}\rho_\star\rho^\star\mathscr{L}_f$ est un isomorphisme.

1.4.2. *Traduction dans le cas connexe.* Si X est connexe, le choix d'un point géométrique x de X identifie le topos $X_{f\text{ét}}$ au topos $\mathrm{B}\pi_1(X, x)$ des $\pi_1(X, x)$-ensembles continus (cf. [ibid., §9.7]). En particulier, la cohomologie de $X_{f\text{ét}}$ n'est autre que la cohomologie (« galoisienne ») du groupe profini $\pi_1(X, x)$ [ibid., 9.7.6]. Si X est un $K(\pi, 1)$, alors pour tout chaque entier n inversible sur X et chaque faisceau étale $\mathscr{L}$ de $\mathbb{Z}/n\mathbb{Z}$-modules localement constant constructible sur X, la flèche canonique $\mathrm{R}\Gamma(\pi_1(X, x), \mathscr{L}_x) \to \mathrm{R}\Gamma(X, \mathscr{L})$ est un isomorphisme. La réciproque est vraie lorsque X est cohérent et ceci est encore équivalent au fait qu'un revêtement universel $\widetilde{X}$ de X n'a pas de cohomologie à valeur dans $\mathbb{Z}/n\mathbb{Z}$ en degré ≥ 1 (ou, de façon équivalente, > 1).

1.4.3. *Variante pro-ℓ.* Soit ℓ un nombre premier inversible sur un schéma cohérent X à composantes connexes ouvertes et considérons la sous-catégorie pleine des X-schémas finis étales dont la monodromie (en tant que faisceau d'ensembles représenté) est, sur chaque composante connexe, un ℓ-groupe, autrement dit, dont le groupe de Galois sur X d'une clôture galoisienne est un ℓ-groupe. Munie de la topologie étale, cette catégorie donne lieu à un site, dont on note $X_{\ell\text{ét}}$ le topos associé, naturellement équipé d'un morphisme $\rho_\ell : X_{\text{ét}} \to X_{\ell\text{ét}}$. Par construction, la cohomologie de $X_{\ell\text{ét}}$ est, dans le cas où X est connexe, la cohomologie du groupe fondamental pro-ℓ de X (pointé en un point géométrique).

1.4.4. Un schéma X comme ci-dessus est un $K(\pi, 1)$ *pro-ℓ* si pour tout faisceau

abélien de ℓ-torsion [SGA 4_3 1973, IX.1.1] $\mathscr{L}_\ell$ sur $X_{\ell\text{ét}}$, l'unité d'adjonction $\mathscr{L}_\ell \to \mathrm{R}\rho_{\ell\star}\rho_\ell^\star\mathscr{L}_\ell$ est un isomorphisme. En conséquence, si x est un point géométrique de X, supposé connexe, et $\mathscr{L}$ est un faisceau abélien ℓ-monodromique (donc constructible) sur X, on a $\mathrm{R}\Gamma(\pi_1^{\text{pro-}\ell}(X,x),\mathscr{L}_x) \xrightarrow{\sim} \mathrm{R}\Gamma(X,\mathscr{L})$ et, réciproquement, ceci caractérise les $K(\pi,1)$ pro-ℓ.

1.4.5. *Mise en garde.* Notons qu'avec nos définitions, un schéma $K(\pi,1)$ n'est pas nécessairement un $K(\pi,1)$ pro-ℓ : le noyau du morphisme de pro-ℓ-complétion (« sous-groupe ℓ-résiduel ») d'un groupe profini n'est en général pas pro-ℓ' et, *a fortiori*, pas nécessairement acyclique pour les coefficients de ℓ-torsion.

1.4.6. *Exemple.* Toute courbe affine lisse C sur un corps algébriquement clos est un $K(\pi,1)$ pro-ℓ pour chaque nombre premier ℓ. En effet, ni la courbe (affine), ni le pro-ℓ groupe fondamental (libre, cf. p. ex. [Wingberg 1984, théorème 1.1] lorsque ℓ est inversible sur C) n'ont de cohomologie en degré > 1. (On utilise également le fait général que l'unité d'adjonction $\mathrm{Id} \to \mathrm{R}\rho_{\ell\star}\rho_\ell^\star$ est un isomorphisme en degré ≤ 1 pour les faisceaux de ℓ-torsion.)

Proposition 1.4.7. *Soient ℓ un nombre premier inversible sur un corps algébriquement clos k et X une polycourbe ℓ-élémentaire sur* $\mathrm{Spec}(k)$. *Alors, le schéma X est un $K(\pi,1)$ pro-ℓ (cf. 1.4.4), et le pro-ℓ complété du groupe fondamental de chaque composante connexe de X est extension itérée de pro-ℓ groupes libres de type fini.*

Démonstration. Soit $f : X \to Y$ une polycourbe ℓ-élémentaire, où Y est une courbe affine connexe lisse sur corps algébriquement clos de caractéristique $\neq \ell$. On note $\bar\eta$ un point générique géométrique de Y et on souhaite tout d'abord montrer que la suite de pro-ℓ groupes

$$1 \to \pi_1^{\text{pro-}\ell}(X_{\bar\eta}) \to \pi_1^{\text{pro-}\ell}(X) \to \pi_1^{\text{pro-}\ell}(Y) \to 1 \qquad (\dagger)$$

est *exacte*. (On omet ici la notation de points bases.) L'exactitude à droite résulte de la surjection $\pi_1(X) \twoheadrightarrow \pi_1(Y)$ [SGA 1 2003, XIII.4.1]. Soit G un ℓ-groupe fini. Rappelons (cf. par exemple [SGA 4_3 1973, XII, §1]) que l'on a une suite exacte d'ensembles pointés :

$$1 \to \mathrm{H}^1(Y, f_\star\mathsf{G}) \to \mathrm{H}^1(X,\mathsf{G}) \to \mathrm{H}^0(Y, \mathrm{R}^1 f_\star\mathsf{G}),$$

analogue non abélien de la suite exacte de bas degré usuelle (Leray). Ici, on a l'égalité $f_\star\mathsf{G} = \mathsf{G}$ et le faisceau $\mathrm{R}^1 f_\star\mathsf{G}$ est localement constant de fibre en $\bar\eta$ isomorphe à $\mathrm{H}^1(X_{\bar\eta},\mathsf{G})$ de sorte que le noyau de la flèche (d'ensembles pointés) $\mathrm{H}^1(X,\mathsf{G}) \to \mathrm{H}^1(X_{\bar\eta},\mathsf{G})$ est l'image de $\mathrm{H}^1(Y,\mathsf{G})$: $(\dagger)$ est exacte au centre (voir p. ex. [SGA 1 2003, V, §6] pour la traduction en terme de groupes fondamentaux).

Notons $\mathscr{C}$ le champ sur Y image directe par f du champ des G-torseurs sur X. Rappelons [Giraud 1971, V.3.1.6] l'interprétation champêtre de la suite exacte

d'ensembles pointés précédente. Le terme de droite s'identifie à l'ensemble des sous-gerbes maximales de $\mathscr{C}$: à une classe $c \in \mathrm{H}^0(Y, \mathrm{R}^1 f_\star \mathsf{G})$ est associée la gerbe $D(c)$ sur Y dont la fibre en $V \to Y$ est la catégorie des G-torseurs sur $U = X \times_Y V$ dont la classe dans $\mathrm{H}^1(U, \mathsf{G})$ s'envoie sur la restriction $c_{|V} \in \mathrm{H}^0(V, \mathrm{R}^1 f_\star \mathsf{G})$. La gerbe $D(c)$ est triviale si et seulement si c est l'image d'une classe $[T] \in \mathrm{H}^1(X, \mathsf{G})$ et, dans ce cas, $D(c)$ est équivalente au champ des $f_\star \mathsf{Aut}(T)$-torseurs sur Y. D'après 1.3.7, il existe un ℓ-revêtement étale de $Y' \to Y$ tel que le faisceau $\pi_0(\mathscr{C}')$ des sous-gerbes maximales de $\mathscr{C}' = (Y' \to Y)^\star \mathscr{C}$ soit fini constant et que chacune des sous-gerbes maximales soient *localement* liées par le lien d'un ℓ-groupe constant. (On utilise la commutation au changement de base de la formation de l'image directe $f_\star \mathsf{BG}$.) D'après 1.2.5, ces sous-gerbes maximales, sur la *courbe affine* Y', sont triviales. Il en résulte que le foncteur de restriction $\mathscr{C}'(Y') = \mathscr{C}(Y') \to \mathscr{C}(\bar\eta)$ est essentiellement surjectif : tout G-torseur sur $X_{\bar\eta}$ s'obtient par restriction à partir d'un G-torseur sur $X' = X \times_Y Y'$. Ceci suffit pour achever la démonstration de l'exactitude de (†) (cf. [SGA 1 2003, V.6.8 et XIII.4.3]). On utilise le fait qu'une clôture galoisienne *sur* X d'un G-torseur sur X' est un revêtement d'ordre une puissance de ℓ : si $\mathsf{H}'' \trianglelefteq \mathsf{H}' \trianglelefteq \mathsf{H}$ sont des groupes finis avec $[\mathsf{H} : \mathsf{H}']$ et $[\mathsf{H}' : \mathsf{H}'']$ des puissances d'un nombre premier ℓ, le sous-groupe $\bigcap_{h \in \mathsf{H}/\mathsf{H}''} h\mathsf{H}''h^{-1}$ est d'indice une puissance de ℓ dans H.

Pour montrer que X est un $K(\pi, 1)$ pro-ℓ, commençons par constater que si $\mathscr{F}$ est un faisceau abélien ℓ-monodromique, et f une polycourbe ℓ-élémentaire, les faisceaux $\mathrm{R}^j f_\star \mathscr{F}$ sont ℓ-monodromiques. La stabilité par extension des faisceaux abéliens ℓ-monodromiques (1.2.1) nous permet en effet de nous ramener, par récurrence, au cas où f est une courbe ℓ-élémentaire, auquel cas cela résulte de la proposition 1.3.7. La conclusion résulte alors de la suite exacte d'homotopie précédente, de l'égalité

$$\mathrm{R}\Gamma(X, \mathscr{F}) = \mathrm{R}\Gamma(Y, \mathrm{R} f_\star \mathscr{F}),$$

de l'isomorphisme

$$\mathrm{R}\Gamma(\pi_1^{\text{pro-}\ell}(Y, \bar\eta), (\mathrm{R} f_\star \mathscr{F})_{\bar\eta}) \xrightarrow{\sim} \mathrm{R}\Gamma(Y, \mathrm{R} f_\star \mathscr{F})$$

(cf. 1.4.6) et enfin de l'isomorphisme

$$(\mathrm{R} f_\star \mathscr{F})_{\bar\eta} = \mathrm{R}\Gamma(X_{\bar\eta}, \mathscr{F}) \xleftarrow{\sim} \mathrm{R}\Gamma(\pi_1^{\text{pro-}\ell}(X_{\bar\eta}), \mathscr{F}),$$

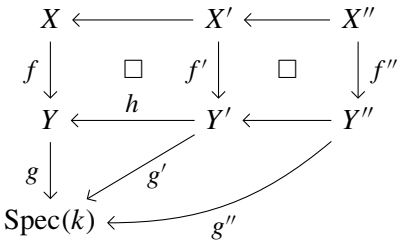
obtenu par récurrence sur la dimension relative. □

1.4.8. Avant d'énoncer le résultat d'abondance des $K(\pi, 1)$ pro-ℓ ci-dessous, rappelons que P. Deligne a défini dans [Deligne 1974, §5.3.5] la topologie de la descente cohomologique universelle [SGA 4_2 1972, V$^{\text{bis}}$, §3.3] ; pour une introduction pédagogique à cette notion, le lecteur pourra se référer à [Conrad 2003]. Nous appellerons *topologie des altérations* la topologie définie par la prétopologie engendrée par les

recouvrements étales et les altérations (= morphisme propre et surjectif induisant un morphisme fini au-dessus d'un ouvert partout dense et envoyant tout point maximal sur un point maximal). La topologie de la descente cohomologique universelle est plus fine que la topologie des altérations.

Proposition 1.4.9. *Soit ℓ un nombre premier inversible sur un corps algébriquement clos k.* Localement pour la topologie des altérations, *tout k-schéma algébrique est une polycourbe ℓ-élémentaire* (*et en particulier*, *d'après 1.4.7*, *localement un $K(\pi, 1)$ pro-ℓ*). *De plus*, *si le schéma est supposé lisse*, *c'est même vrai localement pour la topologie* étale.

Démonstration. Soit X un schéma comme dans l'énoncé, que l'on peut supposer intègre. D'après [de Jong 1996, 4.1], il est localement (par une altération) *lisse* sur k. D'après [SGA 4_3 1973, XI.3.3] (rappelé en 1.3.3), on peut donc supposer que le k-schéma lisse connexe X est une polycourbe élémentaire. Factorisons $X \to \mathrm{Spec}(k)$ à travers une courbe élémentaire $f : X \to Y$. Il existe un revêtement étale $h : Y' \to Y$ trivialisant $\mathrm{R}^1 f_\star \mathbb{Z}/\ell\mathbb{Z}$, c'est-à-dire tel que le faisceau $h^\star \mathrm{R}^1 f_\star \mathbb{Z}/\ell\mathbb{Z} = \mathrm{R}^1 f'_\star \mathbb{Z}/\ell\mathbb{Z}$ soit trivial (i.e., constant) donc, en particulier, ℓ-monodromique. Un tel revêtement est calculable : quitte à se placer au-dessus du point générique du schéma normal Y, ceci est expliqué en §2. (Le cas considéré ici est celui, plus facile, d'une courbe ; cf. 2.4 et 2.7.) Étant obtenu par changement de base de f, le morphisme f' est une courbe élémentaire, et même ℓ-élémentaire par construction. Par récurrence sur la dimension du schéma considéré, on peut supposer qu'il existe, localement pour la topologie étale au voisinage de chaque point, un morphisme $Y'' \to Y'$ tel que le morphisme g'' du diagramme commutatif ci-dessous soit une polycourbe ℓ-élémentaire. Le schéma X'' obtenu par changement de base convient.



□

1.4.10. Notons que l'utilisation du théorème de A. J. de Jong fait perdre l'éventuelle primitive récursivité de notre algorithme (puisqu'on utilise ce théorème en énumérant tous les morphismes sur X jusqu'à trouver une altération qui en résolve les singularités, sans aucune borne sur le temps d'exécution autre que le fait que cette énumération terminera, cf. 11.6 et 12.8). Il est probable que, dans le cas lisse, on puisse préserver l'éventuelle primitive récursivité de notre algorithme par une analyse précise de [SGA 4_3 1973, XI, §2–3].

1.4.11. Si k est algébrique séparable sur un corps ${}_0k$ et X/k obtenu par extension des scalaires d'un ${}_0k$-schéma algébrique ${}_0X$, tout recouvrement $\{Y_\alpha \to X\}$ par des polycourbes ℓ-élémentaires est dominé par un recouvrement du même type *défini sur* ${}_0k$.[4] En effet, si $Y_\alpha \to X$ se descend en un morphisme de ${}_1k$-schémas algébriques ${}_1Y_\alpha \to {}_1X$, où ${}_1k/{}_0k$ est étale, il suffit de considérer le ${}_0k$-morphisme composé ${}_1Y_\alpha \to {}_0X$. Le schéma ${}_1Y_\alpha \otimes_{{}_0k} k$ est isomorphe à $Y_\alpha \otimes_k ({}_1k \otimes_{{}_0k} k)$; c'est un coproduit de polycourbes ℓ-élémentaires, fini surjectif au-dessus de Y_α.

Nous utiliserons la proposition précédente sous la forme suivante (cf. [SGA 4_2 1972, V$^{\text{bis}}$.5.1] ou bien [Deligne 1974, 5.3.3.1 et §6.2]).

Corollaire 1.4.12. *Soient ℓ un nombre premier inversible sur un corps algébriquement clos k et X un k-schéma algébrique. Alors, il existe un X-schéma simplicial $X_\bullet$ tel que chaque X_i soit un coproduit fini de polycourbes ℓ-élémentaires et tel que la flèche d'adjonction* $\mathrm{R}\Gamma(X_{\text{ét}}, \mathbb{Z}/\ell\mathbb{Z}) \to \mathrm{R}\Gamma(\mathrm{Tot}\, X_{\bullet\text{ét}}, \mathbb{Z}/\ell\mathbb{Z})$ *soit un isomorphisme. De plus* :

- *un morphisme $Y \to X$ de k-schémas algébriques peut être coiffé par un morphisme simplicial $Y_\bullet \to X_\bullet$ du type précédent* ;
- *si k est algébrique séparable sur ${}_0k$ et X/k obtenu par extension des scalaires d'un ${}_0k$-schéma algébrique ${}_0X$, on peut supposer pour tout entier r que la flèche $X_{\bullet\leq r} \to X$ provient par extension des scalaires d'une flèche ${}_0X_{\bullet\leq r} \to {}_0X$.*

Le dernier point résulte de l'observation 1.4.11 et de la construction des hyperrecouvrements rappelée ci-dessous, effectuée sur ${}_0k$. Pour la définition du *topos total* $\mathrm{Tot}\, X_{\bullet\text{ét}}$, voir les références citées en §4. (Voir également 4.1.1 pour une variante « n-approchée ».) Pour la définition d'un *hyperrecouvrement*, voir par exemple [SGA 4_2 1972, V.7.3.1.1] ou bien [Deligne 1974, 5.3.5] (ou, de nouveau, [Conrad 2003] pour une approche pédagogique).

1.4.13. Par la suite, nous utiliserons implicitement le fait que les objets et les flèches ci-dessus sont calculables en tout étage : la construction décrite en [SGA 4_2 1972, V$^{\text{bis}}$.5.1.3] (voir aussi [Deligne 1974, proposition 6.2.4]) ne fait intervenir que des limites et coproduits finis et explicites de schémas, que l'on « améliore » en utilisant 1.4.9. Traitons le problème de la construction d'une flèche $Y_\bullet \to X_\bullet$ plus en détail ; le cas de $X_\bullet$ en est un cas particulier. Par produit fibré, il suffit de montrer le lemme suivant.

Lemme. *Tout hyperrecouvrement $X_\bullet$ de X peut être dominé par un hyperrecouvrement $X'_\bullet$ à composantes des coproduits de polycourbes ℓ-élémentaires, calculables en tout étage.*

4. Les indices sont mis à gauche pour éviter la confusion avec les indices simpliciaux utilisés ci-dessous.

Ici, « hyperrecouvrement » = « hyperrecouvrement pour la topologie des altérations ».

Démonstration. Fixons un entier $r \geq 0$ et supposons donné un morphisme simplicial (r-tronqué) $X'_{\bullet\leq r} \to \mathrm{sq}_r X_\bullet$, où $X'_{\bullet\leq r}$ est scindé à composantes des coproduits de polycourbes ℓ-élémentaires. D'après 1.4.9, on peut « couvrir » le produit fibré de X_{r+1} et $\mathrm{cosq}_r(X'_{\bullet\leq r})_{r+1}$ au-dessus de $\mathrm{cosq}_r(\mathrm{sq}_r X_\bullet)_{r+1}$ par un coproduit de polycourbes ℓ-élémentaires, noté N. Pour le calcul du cosquelette, on utilise la formule :

$$\mathrm{cosq}_r(Z)_s = \lim_{\substack{k\leq r \\ [k]\to[s]}} Z_k$$

(la limite étant comprise dans la catégorie des X-schémas, et calculable d'après 16.3). D'après [SGA 4_2 1972, V$^{\mathrm{bis}}$.5.1.3], il existe un schéma simplicial $r+1$-tronqué scindé (calculable) $X'_{\bullet\leq r+1}$ prolongeant $X'_{\bullet\leq r}$, s'envoyant sur $\mathrm{sq}_{r+1}(X_\bullet)$, tel que X'_{r+1} soit un coproduit de N et de composantes scindées de $X'_{\bullet\leq r}$; c'est donc un coproduit de polycourbes ℓ-élémentaires. □

2. Calculabilité du H^1

L'objectif de cette section est de démontrer le théorème suivant.

Théorème 2.1. *Soient X un schéma* normal, *de type fini sur un corps algébriquement clos k, et G un groupe fini constant d'ordre une puissance d'un nombre premier ℓ inversible sur X. Alors, on peut calculer* $\mathrm{H}^1(X, G)$, *c'est-à-dire produire une liste de représentants des classes d'isomorphie de G-torseurs sur X.*

2.2. Il suffit de trouver une extension finie galoisienne du corps des fractions K de X qui domine tous ces G-torseurs, ou encore une extension les trivialisant tous. En effet, si L/K est une telle extension, de groupe de Galois π, l'ensemble $\mathrm{H}^1(X, G)$ est naturellement un sous-ensemble de l'ensemble fini $\mathrm{H}^1(L/K, G) = \mathsf{Hom}(\pi, G)/G$ des classes d'isomorphie de G-torseurs sur K trivialisés par L/K. Si $\phi \in \mathsf{Hom}(\pi, G)$, on peut construire explicitement le G-torseur $A_\phi = \mathsf{Hom}_{\pi\text{-}\mathsf{Ens}}(G, L)$ sur K correspondant par la théorie de Galois–Grothendieck, et tout G-torseur sur X est obtenu par normalisation de X dans un tel A_ϕ (voir 15.5 pour la calculabilité de la normalisation). Parmi ces X-schémas, en nombre fini, il faut vérifier quels sont ceux qui sont étales et galoisiens de groupe G sur X (cf. 17.2 et 17.3).

2.3. ***Réduction au cas abélien.*** Notons Z le centre (non trivial) du ℓ-groupe fini G. La suite exacte

$$1 \to Z \to G \to G/Z \to 1$$

induit [Giraud 1971, V.2.3] une suite exacte d'*ensembles pointés*

$$\mathrm{H}^1(X, Z) \to \mathrm{H}^1(X, G) \to \mathrm{H}^1(X, G/Z).$$

Supposons, par récurrence, que l'on sache trouver une extension L du corps des fonctions de X trivialisant les G/Z-torseurs. Soit X_L le normalisé de X dans L. L'image inverse sur X_L de chaque G-torseur sur X provient d'un Z-torseur sur X_L. (On utilise le fait que la restriction au point générique induit une injection sur les H^1 car les schémas considérés sont normaux.) Ceci nous ramène au cas particulier où G est un ℓ-groupe abélien et, finalement, au cas où $G = \mathbb{Z}/\ell\mathbb{Z}$, ce qu'on supposera maintenant.

2.4. *Cas d'une courbe.*

2.4.1. Si X est une *courbe* lisse sur le corps algébriquement clos k, le cardinal de $\mathrm{H}^1(X, \mathbb{Z}/\ell\mathbb{Z})$ est connu. On peut donc effectivement produire tous les $\mathbb{Z}/\ell\mathbb{Z}$-torseurs sur X en un temps fini.

Remarque 2.4.2. Signalons comment l'on pourrait se ramener au cas d'une courbe projective (lisse). Si $\overline{X}$ est la complétion projective de X et $\overline{X} - X = \{c_1, \ldots, c_r\}$ sont les points à l'infini, il existe (Riemann–Roch) une fonction $f \in K^\times$ s'annulant exactement en ces points. Notons $L = K(\sqrt[\ell]{f})$. D'après le lemme d'Abhyaṁkar, le tiré en arrière d'un $\mathbb{Z}/\ell\mathbb{Z}$-torseur sur X au normalisé X_L de X dans L s'étend à la complétion projective $\overline{X}_L$. Pour trouver f, on note qu'il existe un entier n explicite tel que, pour chaque $i \in \{1, \ldots, r\}$, il existe une fonction $f_i \in \mathscr{L}((n+1)c_i) - \mathscr{L}(nc_i)$, que l'on peut calculer algorithmiquement, cf. [Hess 2002] ; la fonction $f = \sum_i f_i$ convient. (Une variante de cet argument est également possible lorsque X est un k-schéma algébrique normal, quitte à l'altérer pour en faire le complémentaire d'un diviseur à croisements normaux dans un k-schéma projectif lisse (de Jong).)

Signalons pour terminer que si X est une courbe projective lisse, on sait [Serre 1975, chapitre VI, n°12] que tout revêtement connexe de groupe $\mathbb{Z}/\ell\mathbb{Z}$ est induit par une isogénie de la jacobienne de X (que l'on peut construire explicitement ; cf. p. ex. [Anderson 2002]). Ceci fournit une approche différente de 2.4.1 pour la détermination effective de $\mathrm{H}^1(X, \mathbb{Z}/\ell\mathbb{Z})$, qui peut probablement être rendue primitivement récursive.

2.5. ***Fibration en courbes.*** [5] Supposons dorénavant le schéma X de dimension $d \geq 2$ et démontrons 2.1 par récurrence sur l'entier d. On peut supposer le schéma X intègre et, quitte à le modifier — c'est-à-dire le remplacer par un X-schéma propre et birationnel —, on peut également supposer qu'il existe un k-schéma de type fini intègre S de dimension $d-1$ et un morphisme $X \to S$ faisant de X une courbe relative sur S à fibre générique lisse et géométriquement connexe. (cf. p. ex. [de Jong 1996, 4.11–12].) Il résulte de ce qui précède — appliqué à la courbe $X_{\bar{\eta}}$ où $\bar{\eta}$ est un point générique géométrique de S — qu'il existe un S-schéma étale S' intègre

5. Cette méthode nous a été suggérée par Ofer Gabber.

de point générique η' et un revêtement $Y' \to X_{S'}$ tel que si T est un G-torseur sur X et T' le torseur obtenu par le changement de base $Y' \to X$, la fibre générique géométrique $T'_{\bar{\eta}'}$ est le G-torseur trivial. Quitte à changer les notations, on peut supposer $S = S'$ et $X = Y'$.

(Du point de vue algorithmique, signalons que l'on peut déterminer η par 15.2 et que les corps $\kappa(\eta)$ et $\kappa(\bar{\eta})$ conservent les bonnes propriétés de calculabilité que l'on peut imposer à k par 12.5.)

2.6. Quitte à remplacer S par un ouvert étale, on peut supposer que le morphisme $X \to S$ est une *courbe élémentaire*. Vérifions que, sous cette hypothèse, tout G-torseur T sur X à fibre générique géométrique triviale provient de S : ceci nous permettra de conclure, par récurrence, car $\dim(S) = d - 1 < d$. Supposons, comme il a été fait ci-dessus, que G est le groupe abélien $\mathbb{Z}/\ell\mathbb{Z}$, et notons f le morphisme $X \to S$. Considérons la suite exacte

$$0 \to \mathrm{H}^1(S, f_\star \mathbb{Z}/\ell\mathbb{Z}) \to \mathrm{H}^1(X, \mathbb{Z}/\ell\mathbb{Z}) \to \mathrm{H}^0(S, \mathrm{R}^1 f_\star \mathbb{Z}/\ell\mathbb{Z}).$$

Comme rappelé en 1.3.4, le morphisme d'adjonction $\mathbb{Z}/\ell\mathbb{Z} \to f_\star \mathbb{Z}/\ell\mathbb{Z}$ est un isomorphisme, le faisceau $\mathrm{R}^1 f_\star \mathbb{Z}/\ell\mathbb{Z}$ est lisse sur S et la fibre générique géométrique de $\mathrm{R}^1 f_\star \mathbb{Z}/\ell\mathbb{Z}$ est isomorphe à $\mathrm{H}^1(X_{\bar{\eta}}, \mathbb{Z}/\ell\mathbb{Z})$. Il en résulte que la flèche $\mathrm{H}^0(S, \mathrm{R}^1 f_\star \mathbb{Z}/\ell\mathbb{Z}) \to \mathrm{H}^1(X_{\bar{\eta}}, \mathbb{Z}/\ell\mathbb{Z})$ est une injection et, par conséquent, que tout $\mathbb{Z}/\ell\mathbb{Z}$-torseur sur X trivialisé par $X_{\bar{\eta}}$ provient de S. (Voir aussi 1.3.7 et 1.4.7.) Ceci achève la démonstration du théorème 2.1.

Remarque 2.7. Supposons X obtenu par extension algébrique des scalaires à partir d'un schéma X_0 sur k_0 et $T^{(1)}, \ldots, T^{(N)}$ des représentants des classes d'isomorphie de G-torseurs sur X. Il existe une sous-extension étale k_1/k_0 de k, calculable (16.11), telle que les G-torseurs précédents soient définis sur k_1, c'est-à-dire que chaque $T^{(i)}$ soit X-isomorphe à $T_1^{(i)} \times_{X_1} X$, où $X_1 = X_0 \times_{k_0} k_1$ et $T_1^{(i)}$ est un G-torseur sur X_1. Dans ce cas, l'action naturelle de $\mathsf{Aut}(k/k_0)$ sur $\mathrm{H}^1(X, G)$ se factorise à travers une action explicite du quotient fini $\mathrm{Gal}(k_1/k_0)$: si (plus généralement) $g \in \mathsf{Aut}_{k_0}(X_1)$, l'action (à droite) de g sur $[T_1] \in \mathrm{H}^1(X_1, G)$ est donnée par $[T_1] \cdot g = [T_1 \times_{X_1, g} X_1]$.

3. Série ℓ-centrale descendante et groupe fondamental

3.1. *Une filtration.*

3.1.1. Soient ℓ un nombre premier et G un pro-ℓ groupe. Pour tout sous-groupe H de G, notons $F(H)$ l'adhérence du sous-groupe $H^\ell \cdot (H, G)$ de G, où (X, Y) désigne le sous-groupe engendré par les commutateurs $x^{-1}y^{-1}xy$ pour x dans X et y dans Y : autrement dit, il s'agit du sous-groupe fermé de G engendré par les puissances ℓ-ièmes des éléments de H et des commutateurs de ces éléments avec ceux de G. Rappelons ([Dixon et al. 1999, 1.15] ou [Neukirch, Schmidt et Wingberg

2000, définition 3.8.1]) que la *série ℓ-centrale descendante* de G est la filtration définie de la façon suivante : $G^{[1]} = G$, et $G^{[n+1]} = F(G^{[n]})$. Ces sous-groupes sont caractéristiques dans G et on note $G^{(n)}$ le quotient $G/G^{[n]}$. En particulier, $G^{[2]}$ est le sous-groupe de Frattini $\Phi(G)$ de G ([Serre 1978–79, §3.6] ou [Rotman 1995, théorème 5.48(ii)]) et le $\mathbb{F}_\ell$-espace vectoriel $G^{(2)}$ est naturellement le dual de $\mathsf{Hom}_{\mathrm{cont}}(G, \mathbb{Z}/\ell\mathbb{Z})$.

Pour des raisons typographiques, nous noterons parfois F^nG pour $G^{[n]}$, notamment en §6.

Remarques 3.1.2. On vérifie sans peine que $G^{[n+1]}$ est le plus petit sous-groupe fermé normal de G contenu dans $G^{[n]}$ tel que $G^{[n]}/G^{[n+1]}$ soit ℓ-élémentaire abélien et contenu dans le centre de $G/G^{[n+1]}$.

Pour notre propos, nous avons une certaine liberté dans le choix de la filtration : on aurait aussi bien pu considérer, par exemple, la filtration de Frattini itérée Φ^nG, où $\Phi(H) = \overline{H^\ell(H, H)} \subseteq F(H)$. À ce sujet, signalons que la filtration de Frattini itérée Φ^nG et la filtration ℓ-centrale descendante F^nG définie ci-dessus sont équivalentes au sens où il existe une fonction $\tau(d, n)$ (explicitement calculable, et même, primitivement récursive) telle que $F^{\tau(d,n)}G \subseteq \Phi^nG \subseteq F^nG$ si G a d générateurs (comme pro-ℓ-groupe). (Esquisse de démonstration : l'inclusion $\Phi^nG \subseteq F^nG$ est évidente. L'inclusion $F^{\tau(d,n)}G \subseteq \Phi^nG$ se montre en combinant le (i) du lemme 6.1 ci-dessous avec un l'analogue du (ii) pour la filtration Φ^nG. Cet analogue du (ii) revient à majorer l'ordre de L/Φ^nL où L est le pro-ℓ-groupe libre à d générateurs : ceci peut se faire par récurrence sur n en utilisant le fait que $\#(L/\Phi L) = \ell^d$ et le théorème de l'indice de Schreier [Lubotzky et Segal 2003, proposition 16.4.5] pour calculer le nombre de générateurs de Φ^nL.)

Signalons également que si G est topologiquement de type fini, le passage à l'adhérence est superflu, les sous-groupes considérés étant déjà fermés, tant pour F que pour Φ [Dixon et al. 1999, corollaire 1.20].

3.2. *Revêtements et topos associés.*

3.2.1. Soient X un schéma *connexe*, séparé de type fini sur un corps algébriquement clos k, x un point géométrique, ℓ un nombre premier inversible sur k et π_X le groupe fondamental pro-ℓ de (X, x). Ce groupe est topologiquement de type fini, par finitude de $\mathrm{H}^1(X, \mathbb{F}_\ell) = \mathsf{Hom}(\pi_X, \mathbb{F}_\ell)$, si bien que le morphisme canonique $\pi_X \to \lim_n \pi_X^{(n)}$ est un isomorphisme (voir par exemple [Neukirch, Schmidt et Wingberg 2000, 3.8.2], ou [Dixon et al. 1999, proposition 1.16 (iii)]).

Pour chaque entier $n \geq 1$, notons $X^{[n]} \to X$ un revêtement étale de X correspondant au sous-groupe d'indice fini $\pi_X^{[n]}$ de π_X ; nous dirons que c'est un *revêtement ℓ-étale n-approché universel* de X. On note $X_{\ell\text{ét}}^{(n)}$, voire simplement $X^{(n)}$, le *topos* des faisceaux sur $X_{\ell\text{ét}}$ trivialisés par le revêtement étale $X^{[n]} \to X$. Le morphisme

naturel $X_{\ell\text{ét}} \to X^{(n)}_{\ell\text{ét}}$ s'identifie au morphisme de topos $\mathrm{B}\pi_X \to \mathrm{B}\pi^{(n)}_X$ déduit de la surjection $\pi_X \twoheadrightarrow \pi^{(n)}_X$: l'image inverse est le foncteur des $\pi^{(n)}_X$-ensembles vers les π_X-ensembles continus (obtenu par composition) et l'image directe est le foncteur « invariants sous $\pi^{[n]}_X$ » ; cf. p. ex. [SGA 4_1 1972, IV.4.5.1]. (On laisse le soin au lecteur de définir $X^{(n)}_{\ell\text{ét}}$ sous des hypothèses plus générales ; nous n'en aurons pas usage.) Par construction, pour chaque $n \geq 2$, le topos $X^{(n)}_{\ell\text{ét}}$ est ponctuel si et seulement si π_X est trivial, c'est-à-dire si X ne possède pas de revêtement étale connexe d'ordre ℓ.

3.2.2. *Mutatis mutandis*, les définitions précédentes s'étendent au cas d'un schéma (algébrique sur un corps algébriquement clos) *non nécessairement connexe*. Pour définir $X^{[n]}$, on écrit X comme coproduit de ses composantes connexes (ouvertes) et l'on procède de manière évidente : si $X = \coprod_{c\in\pi_0(X)} X_c$, on pose

$$X^{[n]} := \coprod_{c\in\pi_0(X)} X_c^{[n]}.$$

La définition du topos $X^{(n)}$ est inchangée et celle du groupe $\pi^{(n)}_X$ devrait être remplacée par la définition d'un *groupoïde* $\Pi^{(n)}_X$.

Notons que $X^{(1)}_{\ell\text{ét}}$ est le topos discret des faisceaux sur l'ensemble (fini) $\pi_0(X)$.

3.2.3. Donnons une description alternative de $X^{(n)}$. Commençons par observer qu'il est équivalent au topos des faisceaux sur le site *ℓ-étale n-approché* de X dont les objets sont les $U \to X$ finis étales qui sont, composante connexe par composante connexe, quotients d'un revêtement ℓ-étale n-approché universel de X ; une famille est couvrante si son image recouvre X. Fixons un revêtement ℓ-étale n-approché universel $X^{[n]}$ de X, et notons $\Pi_{X^{[n]}/X}$ le groupoïde totalement discontinu (au sens de [Gabriel et Zisman 1967, 6.1.4]) dont les objets sont les $c \in \pi_0(X)$, de groupe d'automorphismes $\mathrm{Aut}_{X_c}(X_c^{[n]})$. Le foncteur $\mathcal{F} \mapsto \mathcal{F}(X^{[n]})$ induit une équivalence entre le topos $X^{(n)}$ et le topos des préfaisceaux sur $\Pi_{X^{[n]}/X}$. Les foncteurs $\mathcal{F} \mapsto \mathcal{F}(X_c^{[n]})$ sont des *points* du topos $X^{(n)}$. (Noter qu'un schéma $X_c^{[n]}$ n'est pas nécessairement local au sens de la topologie ℓ-étale n-approchée considérée.)

3.2.4. Nous dirons qu'un faisceau d'ensembles constructible $\mathcal{F}$ sur $X^{(n)}$ (resp. un morphisme $\mathcal{F} \to \mathcal{G}$) est *calculable* (en fonction des données) s'il en est ainsi du X-schéma ℓ-étale n-approché $X^{\mathcal{F}}$ (resp. du morphisme $X^{\mathcal{F}} \to X^{\mathcal{G}}$) qui le représente (ce schéma ou morphisme étant lui-même décrit au sens de la section 16) ; si le faisceau $\mathcal{F}$ est abélien, on demande de plus que les X-morphismes $+ : X^{\mathcal{F}} \times_X X^{\mathcal{F}} \to X^{\mathcal{F}}$ (addition), $[-1] : X^{\mathcal{F}} \to X^{\mathcal{F}}$ (opposé) et $e : X \to X^{\mathcal{F}}$ (neutre) soient calculables. L'ensemble des sections sur un ouvert ℓ-étale n-approché donné U d'un faisceau calculable $\mathcal{F}$, ainsi que les flèches de fonctorialité, sont calculables : il suffit de calculer l'ensemble des sections du morphisme fini étale de schémas $X^{\mathcal{F}} \to X$

au-dessus de U, et les flèches induites ; cf. 17.3. Réciproquement, l'action de la monodromie sur $\mathscr{F}(X^{[n]})$ permet de reconstruire $X^{\mathscr{F}}$.

3.2.5. Il résulte immédiatement de ce qui précède que l'on peut calculer le noyau d'un morphisme calculable $\mathscr{F} \to \mathscr{G}$ de faisceaux constructibles abéliens. Il en est de même du conoyau : il est représenté par le plus grand quotient X' de $X^{\mathscr{G}}$ tel que le morphisme de schémas en groupes $X^{\mathscr{F}} \to X'$ se factorise à travers la section nulle $X \to X'$.

3.2.6. Nous dirons qu'un faisceau d'ensembles constructible $\mathscr{F}$ sur $X^{(n)}$ est *induit* s'il est isomorphe à un faisceau image directe étale $\pi_{\text{ét}\star}E$, où π est le morphisme (fini étale) $X^{[n]} \to X$ et E est un faisceau constant constructible sur chaque composante connexe. Tout faisceau d'ensemble constructible $\mathscr{F}$ sur $X^{(n)}$ est sous-objet d'un faisceau induit : l'unité $\mathscr{F} \to \pi_{\text{ét}\star}\pi^{\star}_{\text{ét}}\mathscr{F}$ est un monomorphisme. Si $\mathscr{F}$ est *calculable*, il en est de même de l'injection précédente.

Rappelons que l'image inverse d'un faisceau représentable est représentée par le produit fibré évident et que si $\mathscr{G}$ est un faisceau d'ensembles constructible sur un schéma X', représenté par un X'-schéma Y', le faisceau étale image directe $f_{\text{ét}\star}\mathscr{G}$ par un morphisme *fini étale* $f : X' \to X$ est représenté par même schéma Y', vu sur X. On utilise ici l'égalité $f_{\text{ét}\star} = f_{\text{ét}!}$ et la description de ce dernier foncteur faite par exemple en [SGA 4_1 1972, IV.11.3.1].

3.3. *Calculabilité de* $X^{[n]}$.

3.3.1. Soient k un corps algébriquement clos et X un k-schéma algébrique *normal*, non nécessairement connexe. Comme précédemment, on a fixé un nombre premier ℓ inversible sur k. On se propose de montrer que l'on peut calculer un revêtement ℓ-étale n-approché universel $X^{[n]}$ de X. Une décomposition de X en composantes connexes étant calculable (cf. 16.6), on suppose dorénavant le schéma X connexe. Observons maintenant qu'une fois calculé $X^{[n]} \to X$, on peut en déduire $\pi_X^{(n)}$ qui est isomorphe au groupe d'automorphismes $\mathsf{Aut}_X(X^{[n]})$, lui-même en bijection avec $\pi_0(X^{[n]} \times_X X^{[n]})$ par son action sur la composante connexe diagonale (cf. 17.3 ou 16.6). Réciproquement, si $\pi_X^{(n)}$ — ou même simplement son cardinal — est connu, on peut construire $X^{[n]}$, au pire par recherche non bornée (12.8) d'un revêtement étale ayant le bon groupe de Galois. Ci-dessous, nous allons donc nous contenter de calculer le groupe $\pi_X^{(n)}$ dans le cas où X est normal connexe (en fait, il n'est pas difficile de se convaincre qu'on construit bien $X^{[n]}$).

Remarque 3.3.2. Par « calcul » d'un groupe fini, on entend la détermination du cardinal et d'une table de multiplication du groupe. (En particulier, on peut en déterminer des générateurs — par exemple, le groupe tout entier — et, pour tout ensemble fini de générateurs, une présentation finie associée.)

3.3.3. $n = 2$. Comme signalé ci-dessus, le groupe abélien $\pi_X^{(2)}$ est isomorphe au dual du $\mathbb{F}_\ell$-espace vectoriel de dimension finie $\mathrm{H}^1(X, \mathbb{F}_\ell)$. D'après le théorème 2.1, on peut calculer le rang de cet espace vectoriel. En particulier, si π_X est un pro-ℓ-groupe libre de type fini, on peut calculer son rang (nombre minimal de progénérateurs).

3.3.4. *Récurrence sur n.* On suppose que l'on sait calculer le groupe $\pi_X^{(n)}$ et par conséquent un revêtement ℓ-étale n-approché universel $X^{[n]} \to X$. Considérons maintenant un revêtement ℓ-étale 2-approché universel $X^{[n][2]}$ de $X^{[n]}$. C'est également un revêtement galoisien de X car le sous-groupe de Frattini $\Phi(\pi_X^{[n]})$ est caractéristique dans π_X donc distingué. Notons G le groupe de Galois de $X^{[n][2]}$ sur X, que l'on peut calculer : c'est le groupe d'automorphismes d'un X-schéma explicite. Abstraitement, il est isomorphe à $\pi_X/\Phi(\pi_X^{[n]})$; le groupe $\pi_X^{(n+1)} = \pi_X/\pi_X^{[n+1]}$ — que l'on cherche à calculer — en est donc un quotient. Plus précisément, par fonctorialité [Dixon et al. 1999, proposition 1.16 (i)], $\pi_X^{(n+1)} = G^{(n+1)}$. Ceci permet de conclure.

3.4. ***Fonctorialité.*** De même que l'on ne peut associer à un espace topologique (connexe localement simplement connexe) un revêtement universel de façon fonctorielle, on ne peut espérer choisir $X^{[n]}$ fonctoriellement en X. Tout comme $X \rightsquigarrow X_{\text{ét}}$ (cf. p. ex. [SGA 4_2 1972, VII.1.4]), la construction $X \rightsquigarrow X_{\ell\text{ét}}^{(n)}$ définit seulement un *pseudo*-foncteur ([SGA 1 2003, VI, §8] ou [Borceux 1994, 7.5.1]) covariant de la catégorie des schémas vers la 2-catégorie des topos.

3.4.1. Soit $f : (X, x) \to (Y, y)$ un morphisme de schémas pointés, entre k-schémas algébriques, où k est un corps algébriquement clos sur lequel un nombre premier ℓ fixé est inversible. (On ne suppose pas que le morphisme f est un k-morphisme.) Soient $n \geq 1$ un entier et $X^{[n]}$ (resp. $Y^{[n]}$) un revêtement ℓ-étale n-approché universel de X (resp. Y). Il résulte de la théorie des revêtements et de la fonctorialité de $G \mapsto G^{(n)}$ qu'il existe un morphisme $f^{[n]} : X^{[n]} \to Y^{[n]}$ au-dessus de $f : X \to Y$, c'est-à-dire rendant commutatif le diagramme suivant :

$$\begin{array}{ccc} X^{[n]} & \overset{f^{[n]}}{\dashrightarrow} & Y^{[n]} \\ \downarrow & & \downarrow \\ X & \xrightarrow[f]{} & Y \end{array}$$

Si X et Y sont connexes, ce morphisme $f^{[n]}$ est unique à translation près par $\mathrm{Aut}_Y(Y^{[n]})$. Si f est un k-morphisme explicite entre schémas normaux, on peut le calculer.

Rigidification : choisissons des points géométriques $x^{[n]} \to X^{[n]}$ et $y^{[n]} \to Y^{[n]}$ au-dessus de x et y respectivement. Alors, il existe un *unique* morphisme pointé

$f^{[n]}_{xy} : (X^{[n]\circ}, x^{[n]}) \to (Y^{[n]\circ}, y^{[n]})$ au-dessus de f, où le terme de gauche d'une paire (Z°, z) désigne la composante connexe de Z contenant z.

3.4.2. *Version simpliciale.* Soit $X_\bullet$ un k-schéma algébrique simplicial tronqué — c'est-à-dire un foncteur d'une catégorie $\mathbf{\Delta}_{\leq r}$ [6] ($r \in \mathbb{N}$) vers les k-schémas algébriques — et $P_\bullet \to X_\bullet$ un morphisme simplicial (tronqué), tel que chaque P_i soit coproduit fini de points géométriques. Il existe pour chaque i un relèvement de $P_i \to X_i$ à un revêtement ℓ-étale n-approché universel $X_i^{[n]}$ de X_i. Notons $X_{P_i}^{[n]\circ}$ le coproduit $\coprod_{p_i \in P_i} X_{p_i}^{[n]\circ}$, où $X_{p_i}^{[n]\circ}$ désigne la composante connexe de $X_i^{[n]}$ contenant l'image de p_i. D'après le paragraphe précédent, les $X_{P_i}^{[n]\circ}$ s'organisent *de façon unique* en un schéma simplicial $X_{P_\bullet}^{[n]\circ}$ de telle sorte que $P_\bullet \to X_{P_\bullet}^{[n]\circ}$ soit une factorisation simpliciale de $P_\bullet \to X_\bullet$.

En d'autres termes, quitte à introduire des « multiplicités », on peut relever simplicialement les points géométriques d'un schéma à un revêtement ℓ-étale n-approché universel.

4. Cohomologie ℓ-étale n-approchée d'un schéma simplicial

On vérifie ici le fait — énoncé en 4.3.1 et intuitivement évident compte tenu de ce qui précède (3.3) — que l'on sait calculer la cohomologie des topos obtenus à partir d'un schéma simplicial tronqué par application du pseudo-foncteur $S \rightsquigarrow S^{(n)}$ (cf. ¶ 3.4). Il est logiquement possible, et peut-être préférable, de ne lire cette section qu'après la section 8. Pour un raccourci, cf. 4.2.3.

4.1. ***Généralités.*** Nous renvoyons le lecteur à [Illusie 1972, VI, §5.1 et §6.2] ou [SGA 4_2 1972, VI, §7] pour les détails, et [Deligne 1974, §5.1] pour un résumé (qui est le point de départ de la théorie) dans le cas des espaces topologiques.

4.1.1. *Cohomologie d'un topos simplicial.* Soient $X_\bullet$ un k-schéma algébrique simplicial et n un entier ≥ 1. Notons $X_\bullet^{(n)}$ le topos simplicial (c'est-à-dire fibré sur $\mathbf{\Delta}$) qui s'en déduit par application du pseudo-foncteur $S \rightsquigarrow S^{(n)}$ et $\mathrm{Tot}\, X_\bullet^{(n)}$ le topos total associé, noté $\mathrm{Top} X_\bullet^{(n)}$ dans [Illusie 1972, VI, §5.1]. On peut voir un objet $\mathscr{F}_\bullet$ de $\mathrm{Tot}\, X_\bullet^{(n)}$ comme la donnée pour chaque ouvert U d'un X_i (ouvert : objet du site ℓ-étale n-approché défini en 3.2.3) d'un ensemble $\mathscr{F}_\bullet(U) = \mathscr{F}_i(U)$, fonctoriellement en un sens que nous ne répétons pas ([Illusie 1972, VI, §5.2] ou [Deligne 1974, 5.1.7] ; essentiellement, la fonctorialité est « cosimpliciale en i et faisceautique en U »).

Rappelons par contre un procédé de calcul de la cohomologie de $\mathrm{Tot}\, X_\bullet^{(n)}$ à valeurs dans un faisceau abélien $\mathscr{F}_\bullet$. Le cas du H^0 (sections globales) est particulièrement

6. C'est la catégorie des ensembles $\{0, \ldots, s\} \subseteq \mathbb{N}$, où $s \leq r$, munis des applications croissantes ; elle est notée $(\Delta)_r$ dans [Deligne 1974, 5.1.1].

simple : c'est

$$\lim_{i\in\mathbf{\Delta}} \Gamma(X_i^{(n)}, \mathscr{F}_i) = \mathrm{Ker}\big(\Gamma(X_0^{(n)}, \mathscr{F}_0) \rightrightarrows \Gamma(X_1^{(n)}, \mathscr{F}_1)\big).$$

Soit $u_\bullet : P_\bullet \to X_\bullet^{(n)}$ un morphisme simplicial tel que pour chaque étage i, le topos P_i soit discret (c'est-à-dire coproduit de topos ponctuels) et le morphisme $u_i : P_i \to X_i^{(n)}$ d'image inverse conservative. Notons $\mathscr{F}_i^\bullet = (\mathscr{F}_i^j)$ la résolution flasque (« de Godement ») du faisceau $\mathscr{F}_i$ associée. Le système des $\Gamma(X_i^{(n)}, \mathscr{F}_i^j)$ est cosimplicial en i et différentiel gradué en j ; il fournit un complexe double, la différentielle en i étant la somme alternée usuelle. La cohomologie cherchée est celle du complexe simple associé :

$$\mathrm{R}\Gamma(\mathrm{Tot}\, X_\bullet^{(n)}, \mathscr{F}_\bullet) \simeq \mathrm{Tot}\, \Gamma(X_i^{(n)}, \mathscr{F}_i^j).$$

Le terme $\Gamma(X_i^{(n)}, \mathscr{F}_i^j)$ de droite n'est autre que l'ensemble des sections globales de $\mathscr{F}_i^j$, vu comme faisceau étale sur le schéma X_i.

On en déduit notamment que $\tau_{<r}\mathrm{R}\Gamma(\mathrm{Tot}\, X_\bullet^{(n)}, \mathscr{F}_\bullet)$ ne dépend que du schéma simplicial tronqué $X_{\bullet\leq r}$ et de la restriction de $\mathscr{F}_\bullet$ correspondante. Bien que cela ne soit pas absolument nécessaire pour les résultats de cet article, nous précisons en 4.1.2 ci-dessous cette observation.

4.1.2. *Variante tronquée* (cf. [Gabber 2001]). Pour tout $r \in \mathbb{N} \cup \{+\infty\}$ et tout faisceau abélien $F_{\bullet\leq r}$ sur $\mathbf{\Delta}_{\leq r}^{\mathsf{op}}$ (c'est-à-dire : groupe abélien cosimplicial tronqué $\mathbf{\Delta}_{\leq r} \to \mathsf{Ab}$), les sections globales dérivées $\mathrm{R}\Gamma(\mathbf{\Delta}_{\leq r}^{\mathsf{op}}, F_{\bullet\leq r})$ sont calculées par le complexe normalisé $NF_{\bullet\leq r} \in \mathrm{Ob}\, C^{[0,r]}(\mathsf{Ab})$ de la correspondance de Dold–Kan. Pour une définition de ce complexe dans un contexte non tronqué, cf. par exemple [Dold et Puppe 1961, §3]. Les sections globales dérivées d'un *complexe* (de groupes abéliens cosimpliciaux tronqués) se calculent en prenant le *complexe simple* obtenu par ce procédé. Si $X_{\bullet\leq r}$ est un k-schéma algébrique tronqué et $\mathscr{F}_{\bullet\leq r}$ est un faisceau sur $\mathrm{Tot}\, X_{\bullet\leq r}^{(n)}$, on en déduit en poussant par $X_{\bullet\leq r}^{(n)} \to \mathbf{\Delta}_{\leq r}$ que pour toute résolution $\mathscr{F}_{\bullet\leq r}^\bullet$ à $\mathscr{F}_{i\leq r}^j$ acycliques sur $X_i^{(n)}$, on a

$$\mathrm{R}\Gamma(\mathrm{Tot}\, X_{\bullet\leq r}^{(n)}, \mathscr{F}_{\bullet\leq r}) = \mathrm{Tot}\, N_i\Gamma(X_{i\leq r}^{(n)}, \mathscr{F}_i^j),$$

où, pour chaque j, on note $N_i\Gamma(X_{i\leq r}^{(n)}, \mathscr{F}_i^j)$ le complexe normalisé déduit du groupe cosimplicial tronqué $i \mapsto \Gamma(X_{i\leq r}^{(n)}, \mathscr{F}_i^j)$. Ceci est compatible avec la description non « normalisée » du paragraphe précédent par le théorème d'Eilenberg–Mac Lane, [Dold et Puppe 1961, 3.22].

Si $X_\bullet$ (resp. $\mathscr{F}_\bullet$) est une extension de $X_{\bullet\leq r}$ (resp. de $\mathscr{F}_{\bullet\leq r}$) en un k-schéma simplicial non tronqué (resp. en un faisceau sur $\mathrm{Tot}\, X_\bullet^{(n)}$), on a donc un triangle distingué

$$(\text{complexe dans } D^{>r}(\mathbb{Z})) \to \mathrm{R}\Gamma(\mathrm{Tot}\, X_\bullet^{(n)}, \mathscr{F}_\bullet) \to \mathrm{R}\Gamma(\mathrm{Tot}\, X_{\bullet\leq r}^{(n)}, \mathscr{F}_{\bullet\leq r}) \overset{+1}{\to}$$

de sorte qu'en particulier la flèche

$$\mathrm{H}^d(\mathrm{Tot}\, X^{(n)}_\bullet, \mathscr{F}_\bullet) \to \mathrm{H}^d(\mathrm{Tot}\, X^{(n)}_{\bullet\leq r}, \mathscr{F}_{\bullet\leq r})$$

est un isomorphisme pour $d < r$ et injective pour $d = r$.

4.2. ***Résolution de Godement explicite.*** Montrons maintenant que les considérations précédentes permettent de calculer les $\mathrm{H}^i(\mathrm{Tot}\, X^{(n)}_{\bullet\leq r}, \mathscr{F}_{\bullet\leq r})$ lorsque les objets sont donnés explicitement.

4.2.1. On reprend les notations de 4.1.1 et l'on suppose chacun des étages X_i de $X_{\bullet\leq r}$ *normaux*, afin de pouvoir appliquer les résultats de 3.3. Observons tout d'abord que, si P est un point géométrique d'un des X_i (obtenu par exemple par le procédé décrit en 16.10), l'ensemble de ses images par toutes les composées de morphismes de bord et de dégénérescence est fini, de cardinal borné par celui de l'ensemble de toutes les applications croissantes $\{0, \ldots, m\} \to \{0, \ldots, n\}$ avec $m, n \leq r$. On peut donc choisir un ensemble *fini* $\{P_j\}$ de points géométriques formant un morphisme simplicial $P_{\bullet\leq r} \to X_{\bullet\leq r}$ et tel que chaque composante connexe de chacun des X_i contienne au moins un des P_j. Comme expliqué en 3.4.2, on peut relever $P_{\bullet\leq r}$ en un morphisme de schémas simpliciaux $P_{\bullet\leq r} \to X^{[n]\circ}_{P_{\bullet\leq r}}$, qui nous permet de calculer les images directes et inverses par le morphisme de topos simpliciaux $u_{\bullet\leq r} : P_{\bullet\leq r} \to X^{(n)}_{\bullet\leq r}$, où l'on voit maintenant (abusivement) les P_i comme des topos discrets. Le calcul de l'image inverse $u_i^\star\mathscr{F}$ d'un faisceau $\mathscr{F}$ sur $X^{(n)}_i$ est évident : sa fibre en p_i est $\mathscr{F}(X^{[n]\circ}_{p_i})$. L'image directe $u_{i\star}E$, pour la topologie ℓ-étale n-approchée, est le faisceau induit (3.2.6) image directe usuelle (= étale) par le morphisme fini étale $X^{[n]\circ}_{P_i} \to X_i$ du faisceau constant sur chaque composante connexe correspondant à E. Donné E, ce faisceau est calculable, étant représenté par un coproduit explicite $X^{[n]\circ}_{P_i,E}$ de copies de $X^{[n]\circ}_{p_i}$. De plus, on peut calculer les X-morphismes (addition, neutre, opposé) faisant de $X^{[n]\circ}_{P_i,E}$ un X-schéma en groupes fini.

4.2.2. Pour tout faisceau $\mathscr{F}_{\bullet\leq r} \in \mathrm{Ob}\,\mathrm{Tot}\, X^{(n)}_{\bullet\leq r}$, le morphisme d'adjonction $\mathscr{F}_{\bullet\leq r} \to \mathscr{G}_{\bullet\leq r} := u_{\bullet\leq r\star}u^\star_{\bullet\leq r}\mathscr{F}_{\bullet\leq r}$ est le début de la résolution flasque de Godement considérée ci-dessus. Supposons $\mathscr{F}_{\bullet\leq r}$ calculable, c'est-à-dire représentable par un schéma simplicial tronqué en groupes abéliens finis $X^{\mathscr{F}}_{\bullet\leq r}$ au-dessus de $X_{\bullet\leq r}$ qui est calculable (cf. 3.2.4). Comme expliqué ci-dessus, le faisceau $\mathscr{G}_{\bullet\leq r}$ — induit étage par étage — est également calculable, ainsi que la flèche $\mathscr{F}_{\bullet\leq r} \to \mathscr{G}_{\bullet\leq r}$. D'après 3.2.5, le conoyau de cette flèche est calculable : on a montré que, donné $\mathscr{F}_{\bullet\leq r}$ — et les données auxiliaires, non canoniques, $P_{\bullet\leq r}$, etc. — on peut calculer une résolution « de Godement » $\mathscr{C}^{(n)}_P(\mathscr{F}_{\bullet\leq r})$ jusqu'à des degrés arbitrairement grands.

4.2.3. *Variante par recherche non bornée.* Si l'on s'autorise à être moins explicite (et perdre l'éventuelle primitive récursivité), on peut procéder plus simplement, c'est-à-dire sans avoir recourt aux schémas simpliciaux $P_{\bullet\leq r}$ et $X^{[n]\circ}_{P_{\bullet\leq r}}$. Fixons

comme ci-dessus un corps k, un nombre premier ℓ, un schéma simplicial tronqué $X_{\bullet\leq r}$, un anneau Λ, et deux entiers n et d. Il existe une résolution tronquée par un complexe d'induits $\mathscr{F}_i^j$ (cosimplicial en $i \leq r$, différentiel gradué en $j \leq d$) du faisceau constant de valeur Λ sur $X_{\bullet\leq r}$. Cette résolution tronquée est, par hypothèse, acyclique étage par étage et calcule la cohomologie tronquée : $\tau_{<d}\mathrm{R}\Gamma(\mathrm{Tot}\, X^{(n)}_{\bullet\leq r}, \Lambda) = \tau_{j<d}\,\mathrm{Tot}\, N_i\Gamma(X_i, \mathscr{F}_i^j)$. Pour calculer la cohomologie de $\mathrm{Tot}\, X^{(n)}_{\bullet\leq r}$ à valeurs dans Λ en degrés strictement inférieurs à d, il suffit donc de parcourir les morphismes $\Lambda \to \mathscr{F}_\bullet^\bullet$, où $\mathscr{F}_i^j$ est un complexe tronqué d'induits, et, si c'est une résolution tronquée (c'est-à-dire acyclique en degrés $\leq d$) — fait que l'on sait vérifier (cf. 3.2.5) —, de calculer le terme de droite correspondant. On peut procéder de même pour calculer les flèches de fonctorialité en n et en $X_{\bullet\leq r}$.

Remarque 4.2.4. Ce qui précède peut être vu comme une variante du fait bien connu que l'on sait calculer en chaque degré la cohomologie d'un groupe fini agissant sur un Λ-module explicite (voir par exemple la définition donnée en [Serre 1994, I, §2.2]). Sur le problème de la détermination de l'*algèbre* de cohomologie $\mathrm{H}^\star(G, \Lambda)$ d'un groupe fini G, voir par exemple [Carlson 2001]. (D'après le théorème de Venkov–Evens [Evens 1991, 7.4.6], c'est une Λ-algèbre de type fini.)

4.2.5. La construction précédente d'un résolution de Godement est fonctorielle en n en un sens évident : une fois choisi $P_{\bullet\leq r} \to X^{[n]\circ}_{P_{\bullet\leq r}}$ comme ci-dessus, on a pour tout $m \leq n$ un choix naturel de $P_{\bullet\leq r} \to X^{[m]\circ}_{P_{\bullet\leq r}}$, qui permet de calculer — jusqu'à des degrés arbitrairement grands — la flèche $\rho_m^\star \mathscr{C}_P^{(m)}(\mathscr{F}_{\bullet\leq r}) \to \rho_n^\star \mathscr{C}_P^{(n)}(\mathscr{F}_{\bullet\leq r})$, où $\rho_?$ est le morphisme de topos $\mathrm{Tot}\, X_{\bullet\leq r} \to \mathrm{Tot}\, X^{(?)}_{\bullet\leq r}$.

4.2.6. Soit maintenant $f_{\bullet\leq r} : X_{\bullet\leq r} \to Y_{\bullet\leq r}$ un morphisme de k-schémas normaux simpliciaux tronqués. Expliquons brièvement comment calculer la flèche induite sur la cohomologie des topos totaux ℓ-étales n-approchés. On commence par produire une flèche simpliciale de points conservatifs $P^X_{\bullet\leq r} \to P^Y_{\bullet\leq r}$ au-dessus de $X_{\bullet\leq r} \to Y_{\bullet\leq r}$, que l'on relève arbitrairement aux schémas $X_i^{[n]}$ et $Y_i^{[n]}$, puis on construit l'unique morphisme simplicial $X^{[n]}_{P^X_{\bullet\leq r}} \to Y^{[n]}_{P^Y_{\bullet\leq r}}$ au-dessus de $X_{\bullet\leq r} \to Y_{\bullet\leq r}$ les respectant. On peut alors calculer un morphisme de résolution de Godement $\mathscr{C}^{(n)}_{P^Y}(\mathscr{F}_{\bullet\leq r}) \to \mathscr{C}^{(n)}_{P^X}(\mathscr{F}_{\bullet\leq r})$ au-dessus du morphisme de topos $\mathrm{Top}X^{(n)}_{\bullet\leq r} \to \mathrm{Top}Y^{(n)}_{\bullet\leq r}$.

4.3. Pour référence ultérieure, résumons les rappels et observations précédentes sous la forme suivante.

Proposition 4.3.1. *Soient k un corps algébriquement clos, ℓ un nombre premier inversible sur k, $r \geq 0$ un entier et $X_{\bullet\leq r}$ un k-schéma algébrique normal simplicial tronqué. Pour tout ℓ-groupe abélien fini Λ et tout triplet d'entiers $d \geq 0$, $n \geq m \geq 1$, on peut calculer le complexe $\tau_{\leq d}\mathrm{R}\Gamma(\mathrm{Tot}\, X^{(n)}_{\bullet\leq r}, \Lambda)$ et la flèche*

$$\tau_{\leq d}\mathrm{R}\Gamma(\mathrm{Tot}\, X^{(m)}_{\bullet\leq r}, \Lambda) \to \tau_{\leq d}\mathrm{R}\Gamma(\mathrm{Tot}\, X^{(n)}_{\bullet\leq r}, \Lambda).$$

De plus, donné un morphisme $X_{\bullet\leq r} \to Y_{\bullet\leq r}$ de k-schémas algébriques normaux simpliciaux tronqués, on peut calculer la flèche

$$\tau_{\leq d}\mathrm{R}\Gamma(\mathrm{Tot}\, Y^{(n)}_{\bullet\leq r}, \Lambda) \to \tau_{\leq d}\mathrm{R}\Gamma(\mathrm{Tot}\, X^{(n)}_{\bullet\leq r}, \Lambda).$$

Par « calcul » d'un complexe ou d'une flèche, on entend par là que l'on peut trouver des représentants explicites au sens de 13.3.

Remarque 4.3.2. Considérant le cas particulier $m = 1$, on voit que l'on peut calculer les flèches

$$\tau_{\leq d}\check{\mathrm{R}}\Gamma(X_{\bullet\leq r}, \Lambda) \to \tau_{\leq d}\mathrm{R}\Gamma(\mathrm{Tot}\, X^{(n)}_{\bullet\leq r}, \Lambda),$$

où le terme de gauche est le tronqué du complexe associé au Λ-module cosimplicial tronqué des $\Gamma(X_i, \Lambda)$. Cela résulte du fait que $X^{(1)}_{\bullet\leq r} = \pi_0(X_{\bullet\leq r})$ (voir 3.2.2).

5. Systèmes essentiellement constants

5.1. Soit $\mathscr{A}$ une catégorie abélienne satisfaisant les conditions AB3 et AB5 [Grothendieck 1957, I] — qui garantissent l'existence et l'exactitude des colimites filtrantes — et $A_\bullet = (A_i)$ un système inductif de $\mathscr{A}$ indexé par $\mathbb{N}$. Notons A_∞ la colimite de $A_\bullet$ et, pour chaque $j \leq k$ dans $\mathbb{N} \cup \{\infty\}$, posons $A(j,k) := \mathrm{Im}(A_j \to A_k)$. Si $j^- \leq j \leq k \leq k^+$, on a naturellement des flèches $A(j^-,k) \hookrightarrow A(j,k) \twoheadrightarrow A(j,k^+)$. Si A_∞ est *nœthérien*, il existe un j tel que $A(j,\infty) = A_\infty$; si de plus A_j est nœthérien, il existe un $k \geq j$ tel que $A(j,k) \xrightarrow{\sim} A(j,\infty) = A_\infty$.

Définition 5.2. Soient $\mathscr{A}$ une catégorie abélienne, i_0 un entier, et $c : \mathbb{N}_{\geq i_0} \to \mathbb{N} \times \mathbb{N}$ une fonction. On dit qu'un système inductif $A_\bullet = (A_i)$ de $\mathscr{A}$, indexé par $\mathbb{N}_{\geq i_0}$, est *c-essentiellement constant* si la colimite $A_\infty = \mathrm{colim}_i\, A_i$ est représentable dans $\mathscr{A}$ et si pour chaque $i \in \mathbb{N}_{\geq i_0}$, tel que $c(i) = (j,k)$, l'inégalité $i \leq j \leq k$ est satisfaite et la flèche canonique $A(j,k) \to A_\infty$ est un *isomorphisme*.

5.3. Variante : soient $N \geq i_0$ deux entiers et $\phi : \mathbb{N}_{\geq i_0} \to \mathbb{N}$ une fonction telle que $\phi(j) \geq j$ pour tout $j \in \mathbb{N}_{\geq i_0}$. On dit qu'un système inductif $A_{\bullet\geq i_0}$ est (N,ϕ)-*essentiellement constant* si :

(i) pour chaque j, le système inductif $A(j,k)_{k\geq\phi(j)}$, à flèches de transition *a priori* épimorphiques, est constant ;

(ii) le système inductif $A(j,\phi(j))_{j\geq N}$, à flèches de transition *a priori* monomorphiques, est constant.

Explicitement : (i) $\mathrm{Ker}(A_j \to A_{\phi(j)}) \xrightarrow{\sim} \mathrm{Ker}(A_j \to A_k)$ pour $k \geq \phi(j)$ et (ii) $\mathrm{Im}(A_N \to A_{\phi(j)}) \xrightarrow{\sim} \mathrm{Im}(A_j \to A_{\phi(j)})$ pour $j \geq N$.

Nous laissons le soin au lecteur de vérifier que, donné c, on peut calculer une paire (N,ϕ) telle que tout système inductif c-essentiellement constant soit (N,ϕ)-essentiellement et que, réciproquement, donnée (N,ϕ), on peut calculer un c.

5.4. Il résulte des observations précédentes que si $A_\bullet$ est un système inductif constitué d'objets nœthériens et à colimite nœthérienne, il existe une telle fonction. Nous dirons, de façon un peu vague, qu'un système inductif est *explicitement essentiellement constant* s'il est (N, φ)-essentiellement constant pour un entier N et une fonction φ *calculables* en fonction des données. Cette notion apparaît, avec un but semblable, dans [Schön 1991], puis [Rubio et Sergeraert 2002, §2.1], où un tel système inductif est appelé « module de Schön ». Voir également [Grothendieck 1956, p. 3]. [7]

5.5. Notons qu'un tel système inductif est essentiellement constant au sens usuel : il appartient à l'image essentielle du plongement de $\mathscr{A}$ dans la catégorie abélienne (cf. p. ex. [Kashiwara et Schapira 2006, 8.6.5(i)]) des ind-objets $\mathrm{Ind}(\mathscr{A})$. La proposition clef suivante est le pendant « explicite », du fait que la catégorie $\mathscr{A}$ est naturellement une sous-catégorie *épaisse* de $\mathrm{Ind}(\mathscr{A})$ (cf. p. ex. [Kashiwara et Schapira 2006, 8.6.11]).

Proposition 5.6. *Soit* $0 \to A'_\bullet \to A_\bullet \to A''_\bullet \to 0$ *une suite exacte de systèmes inductifs. Si deux des trois termes sont explicitement essentiellement constants, il en est de même du troisième.*

Cette proposition est élémentaire et bien connue (cf. [Schön 1991, lemme 5, p. 4] ou [Rubio et Sergeraert 2002, théorème 2.3]). Pour la commodité du lecteur, nous en donnons une démonstration, dans le cas d'une catégorie de modules pour simplifier l'exposition.

Démonstration. Supposons d'abord que (A_n) et (A''_n) soient respectivement (N, ϕ)- et (N'', ϕ'')-essentiellement constants. La première condition de 5.3 est vérifiée de (A'_n) pour la fonction ϕ : en effet, un élément de A'_n qui s'annule dans A'_m pour $m \geq \phi(n)$ s'annule en particulier dans A_m (d'après la même condition sur (A_n)) donc s'annule dans $A_{\phi(n)}$ donc dans $A'_{\phi(n)}$. Soit maintenant $N' = \phi''(N)$ (qui est supérieur ou égal à N) : si x appartient à A'_n, son image dans $A'_{\phi(n)}$ vue dans $A_{\phi(n)}$ est l'image d'un élément y de A_N (d'après la deuxième condition sur le système (A_n)) : l'image de ce y dans A''_N s'annule dans $A''_{\phi(n)}$, c'est-à-dire appartient à $\mathrm{Ker}(A''_N \to A''_{\phi(n)})$, et la première condition sur (A''_n) entraîne que cette image s'annule dans $A''_{N'}$, donc l'image de y dans $A_{N'}$ provient d'un élément de $A'_{N'}$, qui par construction a la même image dans $A'_{\phi(n)}$ que l'élément x qu'on s'était fixé. On a donc montré que le système (A'_n) était (N', ϕ)-essentiellement constant (pour $N' = \phi''(N)$).

Supposons maintenant que (A_n) et (A'_n) soient respectivement (N, ϕ)- et (N', ϕ')-essentiellement constants. Soit $z \in A''_n$ avec $n \geq N'$, et soit $m \geq n$ tel que l'image de z s'annule dans A''_m : alors, si y est un relèvement quelconque de z à A_n, l'image

7. Nous remercions Luc Illusie de nous avoir communiqué cette référence.

de y dans A''_m s'annule, donc l'image de y dans A_m provient d'un $x \in A'_m$; puisque (A'_n) est essentiellement constant, il existe $x_0 \in A'_n$ tel que x_0 et x aient même image dans $A'_{\phi'(m)}$; alors $y' := y - x_0$ (vu comme élément de A_n) a une image nulle dans $A_{\phi'(m)}$: donc l'image de y' dans $A_{\phi(n)}$ est déjà nulle (d'après la première condition sur (A_n)), mais ceci implique que l'image de z dans $A''_{\phi(n)}$ est nulle. Ceci montre la première condition pour (A''_n), pour la fonction ϕ'' égale à $\max(\phi, N')$. S'agissant de la seconde condition, si $z \in A''_n$ et si y en est un relèvement quelconque à A_n, il existe un $\tilde{y}$ dans A_N tel que y et $\tilde{y}$ aient la même image dans $A_{\phi''(n)}$, et alors l'image $\tilde{z}$ de $\tilde{y}$ dans A''_N a la même image que z dans $A''_{\phi''(n)}$. On a donc montré que le système (A''_n) était (N, ϕ'')-essentiellement constant (pour $\phi'' = \max(\phi, N')$).

Enfin, supposons que (A'_n) et (A''_n) soient respectivement (N', ϕ')- et (N'', ϕ'')-essentiellement constants. Soit $y \in A_n$ qui s'annule dans A_m pour $m \geq n$: alors en particulier son image dans A''_m s'annule, donc elle s'annule déjà dans $A''_{\phi''(n)}$ (d'après la première propriété sur (A''_n)) ; donc l'image de y dans $A_{\phi(n)}$ provient d'un élément x de $A'_{\phi''(n)}$; si $m \geq \phi''(n)$, l'image de x dans A'_m s'annule et s'annule donc déjà (d'après la première propriété sur (A'_n)) dans $A'_{\phi'(\phi''(n))}$. Ceci montre la première condition sur (A_n) pour la fonction $\phi\colon n \mapsto \phi'(\phi''(n))$. Enfin, soit $y \in A_n$: son image dans A''_n a la même image dans $A''_{\phi''(n)}$ qu'un certain élément $\tilde{z} \in A''_{N''}$, donc si $\tilde{y}$ est un relèvement quelconque de $\tilde{z}$ à $A_{N''}$, les éléments y et $\tilde{y}$ (de A_n et $A_{N''}$ respectivement) ont même image dans $A_{\phi''(n)}$, donc la différence entre ces images provient d'un élément $x \in A'_{\phi''(n)}$; ce dernier a la même image dans $A'_{\phi(n)} = A'_{\phi'(\phi''(n))}$ qu'un certain élément $\tilde{x} \in A'_{N'}$: si on appelle N le maximum de N' et N'' alors la somme des images de $\tilde{x}$ et $\tilde{y}$ dans $A_{\phi(n)}$ est la même que celle de y. On a donc montré que le système (A_n) était (N, ϕ)-essentiellement constant pour $\phi = \phi' \circ \phi''$ et $N = \max(N', N'')$. □

5.7. Soient $\mathscr{A}$ une catégorie abélienne, et $(\mathrm{E}^{\star,\star}_{r,\lambda})_{\lambda\in\mathbb{N}}$ un système inductif (indexé par λ) de suites spectrales ($r \geq r_0$) d'objets de $\mathscr{A}$, supposées dans le premier quadrant, dont on note, pour chaque indice λ, l'aboutissement $\mathrm{E}^{\star}_{\lambda}$. (Suivant p. ex. [ÉGA III$_1$ 1961, **0**, §11.1], on considère que cet objet filtré de $\mathscr{A}$ fait partie de la donnée.)

Corollaire 5.8. *Soit m un entier tel que les systèmes inductifs $(\mathrm{E}^{p,q}_{r_0,\lambda})_\lambda$ soient explicitement essentiellement constants pour chaque paire d'entiers p, q d'entiers tels que $p+q \leq 2m+1$. Alors, pour chaque $0 \leq d \leq m$, le système inductif $(\mathrm{E}^{d}_{\lambda})_\lambda$ est explicitement essentiellement constant.*

Démonstration. Pour chaque indice λ, le calcul de $\mathrm{E}^{p,q}_{r,\lambda}$ ne fait intervenir que des flèches entre sous-quotients de $\mathrm{E}^{p',q'}_{r_0,\lambda}$ avec $p'+q' \leq p+q+(r-r_0)$. Comme d'autre part $\mathrm{E}^{p,q}_{\infty,\lambda} = \mathrm{E}^{p,q}_{r,\lambda}$ si $r > p+q+1$, il résulte de la proposition précédente (5.6) que les systèmes inductifs $(\mathrm{E}^{p,q}_{\infty})_\lambda$ pour $p+q < m$ sont explicitement essentiellement constants. Enfin, comme pour chaque $0 \leq d \leq m$ l'aboutissement E^{d}_{λ} est une

extension itérée de ces $\mathrm{E}_{\infty,\lambda}^{p,q}$ la conclusion résulte d'une nouvelle application de *loc. cit.* □

Proposition 5.9. *Soient $A_\bullet \to B_\bullet$ un morphisme de systèmes inductifs et $\tau : \mathbb{N} \to \mathbb{N}$ une fonction strictement croissante. Supposons qu'il existe un diagramme commutatif*

$$\begin{array}{ccc} A_\bullet & \longrightarrow & B_\bullet \\ \downarrow & \overset{h_\bullet}{\swarrow} & \downarrow \\ A_{\tau(\bullet)} & \longrightarrow & B_{\tau(\bullet)} \end{array}$$

Alors, si $B_\bullet$ est (N, ϕ)-essentiellement constant, le système inductif $A_\bullet$ est $(\tau N, \tau\phi)$-essentiellement constant. En particulier, lorsque τ est calculable, le système inductif $A_\bullet$ est explicitement *essentiellement constant si $B_\bullet$ l'est.*

Démonstration. Soit j un entier. Remplaçons, dans le carré commutatif de l'énoncé, le système inductif $A_\bullet$ (resp. $B_\bullet$, etc.) par le système $A'_\bullet := A(j, \bullet \geq \phi(j))$ — à morphismes de transition épimorphiques — (resp. $B'_\bullet := B(j, \bullet \geq \phi(j))$ — constant par hypothèse —, etc.). La commutativité du diagramme montre alors que $h'_\bullet$ est un isomorphisme ; le système inductif $(A'_k)_{k \geq \phi(j)}$ est donc constant pour $k \geq \tau\phi(j)$. Posons $\psi = \tau\phi$. Le même argument, appliqué à $A''_\bullet := A(j, \psi(j))_j$, etc. montre que ce système est constant pour $j \geq \tau(N)$. (On utilise le fait que B est (N, ψ)-essentiellement constant car $\psi \geq \phi$.) □

6. Approximation d'un pro-ℓ-groupe par ses quotients finis

Pour π un ℓ-groupe fini, on rappelle qu'on a défini en §3 la filtration ℓ-centrale descendante par $F^1\pi = \pi$ et $F^{n+1}\pi = (F^n\pi)^\ell \cdot (\pi, F^n\pi)$ (groupe topologiquement engendré).

Lemme 6.1. *Il existe deux fonctions calculables φ_ℓ et ψ_ℓ telles que :*

(i) *si π est un ℓ-groupe fini d'ordre $\leq n$ alors $F^{\varphi_\ell(n)}\pi = 1$, et*

(ii) *si π est un ℓ-groupe fini à d générateurs tel que $F^n\pi = 1$, alors $\#\pi \leq \psi_\ell(d, n)$.*

Il résulte de la démonstration que $\ell^{(d+1)^n}$ convient pour $\psi_\ell(d, n)$, et que 1 plus la valuation ℓ-adique de n convient pour $\varphi_\ell(n)$.

Démonstration. Pour ce qui est de φ : pour chaque ℓ-groupe fini il existe un r tel que $F^r\pi = 1$ (cf. [Neukirch, Schmidt et Wingberg 2000, proposition 3.8.2]) ; or comme $F^{i+1}\pi$ est défini en fonction de π et de $F^i\pi$, deux termes consécutifs de la suite $F^i\pi$ ne peuvent pas être égaux sauf à ce que cette suite stationne, et on vient de dire que ceci ne se produit que pour $F^i\pi = 1$: il en résulte que la valuation ℓ-adique de l'ordre de $F^i\pi$ doit décroître strictement jusqu'à atteindre 0, donc la valuation ℓ-adique de n (plus 1, puisque la filtration $F^i\pi$ est numérotée à partir de 1) convient pour $\varphi_\ell(n)$.

Pour ce qui est de ψ : d'après [Lubotzky et Segal 2003, théorème 3.5.1], si L est le pro-ℓ-groupe libre sur $d \geq 2$ générateurs et N un sous-groupe distingué ouvert de L d'indice $\ell^s > 1$, si on note $N' = N^\ell \cdot (N, L)$, on a $(N : N') \leq \ell^{(d-1)s+1}$, de sorte que $(L : N') \leq \ell^{ds+1} \leq \ell^{(d+1)s}$; en appliquant ceci à $N = F^r L$ et par récurrence sur r on en déduit $(L : F^r L) \leq \ell^{(d+1)^r}$ (on vérifie immédiatement que cette inégalité fonctionne encore pour $d = 1$ et $r = 1, 2$). Par conséquent, si π est un ℓ-groupe fini à d générateurs tel que $F^n\pi = 1$, en considérant $L \twoheadrightarrow \pi$ la surjection donnée par ces d générateurs, on a une surjection $L/F^n L \twoheadrightarrow \pi$, donc $\#\pi \leq \ell^{(d+1)^n}$. □

6.2. Il résulte de ce lemme que pour chaque ℓ et chaque d, on peut calculer (au sens de 3.3.2) le ℓ-groupe fini $L^{(n)}$ quotient du pro-ℓ groupe libre L à d générateurs : parmi les groupes π comme en (ii) ci-dessus, c'est celui ayant le plus gros cardinal. (Notons qu'ici, il est *a priori* trivial de déterminer une présentation finie de $L^{(n)}$: c'est le quotient du pro-ℓ-groupe libre L par $L^{[n]}$. Par Frattini, le nombre minimal de générateurs de $L^{(n)}$ est d ; par Golod–Šafarevič [Serre 1994, I, §4.4], le nombre de relations entre ces générateurs est $> \frac{1}{4}d^2$.) En conséquence, on peut — pour chaque entier n — déterminer explicitement le système projectif tronqué $L^{(\bullet \leq n)}$ et un système compatible de d générateurs.

Proposition 6.3 (lemme d'Artin–Rees–Frattini effectif). *Il existe une fonction τ_ℓ calculable telle que, si $1 \to \pi' \to \pi \to \pi'' \to 1$ est une suite exacte courte de pro-ℓ-groupes, où π', π'' ont respectivement d', d'' générateurs, on a $F^{\tau_\ell(d',d'',n)}\pi \cap \pi' \subseteq F^n\pi' \subseteq F^n\pi \cap \pi'$ pour tout n.*

Démonstration. Il est évident que $F^n\pi' \subseteq F^n\pi \cap \pi'$. On souhaite montrer que, réciproquement, $F^n\pi' \supseteq F^{\tau(n)}\pi \cap \pi'$ pour une certaine fonction τ explicitement calculable (dépendant du nombre d', d'' de générateurs de π', π'', mais pas d'autres données).

Expliquons pourquoi on peut supposer que π'' est libre (en tant que pro-ℓ-groupe) : il existe en tout cas un morphisme surjectif $L \twoheadrightarrow \pi''$ où L est le pro-ℓ-groupe libre sur d'' générateurs ; et quitte à relever à π les images par ce morphisme de chacun des générateurs, on peut le factoriser comme la composée d'un morphisme $s : L \to \pi$ et de la surjection donnée $\pi \twoheadrightarrow \pi''$. Soit $\hat{\pi} = \pi \times_{\pi''} L$ l'ensemble des éléments de $\pi \times L$ dont les deux composantes ont même image dans π'' (la première projection est donc un morphisme surjectif $\hat{\pi} \twoheadrightarrow \pi$ qui se restreint à l'identité sur π') : ce $\hat{\pi}$, qui s'inscrit dans une suite exacte $1 \to \pi' \to \hat{\pi} \to L \to 1$, se décrit aussi comme le produit semidirect $\hat{\pi} = \pi' \rtimes_* L$ par l'action de L sur π' donnée par $z * x = s(z)\, x\, s(z)^{-1}$. Si on a montré la conclusion voulue pour la suite exacte $1 \to \pi' \to \hat{\pi} \to L \to 1$, la même vaut encore pour $1 \to \pi' \to \pi \to \pi'' \to 1$ (puisque l'image de $F^N\hat{\pi}$ dans π est contenue dans, et même égale à, $F^N\pi$).

On peut donc bien supposer que π'' est libre, et qu'il existe une section $s\colon \pi'' \to \pi$, qui fait de π le produit semidirect $\pi = \pi' \rtimes_* \pi''$ où $*$ désigne l'action de π'' sur π' définie par $z * x = s(z)\, x\, s(z)^{-1}$.

Fixons n. On veut montrer qu'il existe N tel que $F^n\pi' \supseteq F^N\pi \cap \pi'$, et expliquer pourquoi N se calcule sous la forme $\tau(d', d'', n)$ en fonction de d', d'' et n.

L'action de π'' sur π' stabilise $F^n\pi'$, donc définit une action sur $\pi'/F^n\pi'$, et on a $(\pi/F^n\pi') = (\pi'/F^n\pi') \rtimes_* \pi''$ pour cette action quotient.

Comme $\pi'/F^n\pi'$ est fini, $\mathrm{Aut}(\pi'/F^n\pi')$ est lui-même fini, et comme $\pi'' \to \mathrm{Aut}(\pi'/F^n\pi')$ (donné par $*$) est continu, et que les $F^m\pi''$ forment un système fondamental de voisinages de l'unité dans π'', il existe m tel que $F^m\pi''$ agisse trivialement sur $\pi'/F^n\pi'$ (cf. [Neukirch, Schmidt et Wingberg 2000, proposition 3.8.2]). On peut être plus précis : on a $\#(\pi'/F^n\pi') \leq \psi(d', n)$ avec les notations du lemme, donc $\#\mathrm{Aut}(\pi'/F^n\pi') \leq \psi(d', n)!$, donc $\varphi(\psi(d', n)!)$ convient (en considérant l'image de π'' dans $\mathrm{Aut}(\pi'/F^n\pi')$) — ce qui nous importe est qu'un m qui convient puisse être calculé en fonction de d' et n.

L'action de π'' sur $\pi'/F^n\pi'$ passe donc au quotient par $F^m\pi''$, c'est-à-dire définit une action de $\pi''/F^m\pi''$ sur $\pi'/F^n\pi'$, et on a $(\pi/F^n\pi')/s(F^m\pi'') = (\pi'/F^n\pi') \rtimes_* (\pi''/F^m\pi'')$ pour cette action quotientée.

Notons $\bar\pi$ ce ℓ-groupe fini $\pi/((F^n\pi') \cdot s(F^m\pi'')) = (\pi'/F^n\pi') \rtimes_* (\pi''/F^m\pi'')$. Son ordre est majoré par $\psi(d', n) \times \psi(d'', m)$ (et rappelons que $m = \varphi(\psi(d', n)!)$ convient).

Il existe alors $N \geq n, m$ tel que $F^N\bar\pi = 1$: précisément, $\varphi(\psi(d', n) \times \psi(d'', m))$ convient pour N. On a alors $F^N\pi \subseteq (F^n\pi') \cdot s(F^m\pi'')$, donc $F^N\pi \cap \pi' \subseteq F^n\pi'$, ce qu'on voulait démontrer. □

Corollaire 6.4. *On reprend les hypothèses et les notations de la proposition. Soient* $\widetilde{\pi}'^{(n)} = \pi'/(\pi' \cap \pi^{[n]})$ *le noyau de la surjection naturelle* $\pi^{(n)} \twoheadrightarrow \pi''^{(n)}$ *et* Λ *un groupe abélien. Pour tout entier* j, *si le système inductif* $\mathrm{H}^j(\pi'^{(n)}, \Lambda)$ *est explicitement essentiellement constant, il en est de même de* $\mathrm{H}^j(\widetilde{\pi}'^{(n)}, \Lambda)$. (*La fonction explicitant ce fait fait intervenir uniquement* d', d'' *et celle explicitant le fait que* $\mathrm{H}^j(\pi'^{(n)}, \Lambda)$ *est essentiellement constant.*)

Démonstration. Cela résulte de la proposition précédente, réécrite sous la forme d'un diagramme commutatif (pour chaque n)

$$\begin{array}{ccc} \widetilde{\pi}'^{(n)} & \twoheadleftarrow & \pi'^{(n)} \\ \uparrow & \nearrow & \uparrow \\ \widetilde{\pi}'^{(\tau n)} & \twoheadleftarrow & \pi'^{(\tau n)} \end{array}$$

et de 5.9. □

Proposition 6.5. *Soient L un pro-ℓ-groupe libre à d générateurs topologiques, $n_0 \geq 1$ un entier, Λ un ℓ-groupe abélien fini et V un Λ-module de type fini muni d'une action explicite de $L^{(n_0)}$. Pour tout entier i, le système inductif $\mathrm{H}^i(L^{(n)}, V)$, $n \geq n_0$, est explicitement essentiellement constant.*

Par « action explicite », on entend la donnée d'une présentation explicite (13.3) de V et de d éléments de $\mathsf{Aut}(V)$ (13.4) satisfaisant des relations explicites décrivant $L^{(n_0)}$ (cf. 6.2). Le module V est naturellement muni, pour chaque $n \geq n_0$, de l'action de $L^{(n)}$ déduite de la surjection $L^{(n)} \twoheadrightarrow L^{(n_0)}$.

Démonstration. Distinguons trois cas :

$i = 0$. Le système inductif $\mathrm{H}^0(L^{(n)}, V)$ étant *constant*, il est (n_0, Id)-essentiellement constant (5.3).

$i = 1$. Rappelons (cf. p. ex. [Serre 1994, I, §2.6(b)]) que les flèches $\mathrm{H}^1(L^{(n)}, V) \to \mathrm{H}^1(L^{(n+1)}, V)$ sont *injectives*, de sorte que la propriété 5.3 (i) est satisfaite pour $\phi = \mathrm{Id}$. (Notons que V est fixe par $L^{[n]}/L^{[n+1]}$.) Il reste à trouver $N \geq n_0$ tel que la flèche (injective) $\mathrm{H}^1(L^{(N)}, V) \to \mathrm{H}^1(L, V)$ soit un isomorphisme ou, de façon équivalente, tel que l'on ait l'égalité $\#\mathrm{H}^1(L^{(N)}, V) = \#\mathrm{H}^1(L, V)$. La conclusion résulte du fait que ces cardinaux sont calculables. Pour le terme de gauche c'est clair : on sait calculer le système projectif $L^{(n)}$; pour le terme de droite, rappelons [Ogg 1962, p. 188] que l'on a une suite exacte

$$0 \to \mathrm{H}^0(L, V) \to V \to V^d \to \mathrm{H}^1(L, V) \to 0$$

si bien que l'on a l'égalité (formule « d'Euler–Poincaré », due à Ogg et Šafarevič) $\#\mathrm{H}^1(L, V) = (\#V)^{d-1} \times \#\mathrm{H}^0(L, V)$.

$i \geq 2$. La colimite $\mathrm{H}^i(L, V)$ étant nulle (cf. [Serre 1994, I, §3.4]), il suffit de trouver $\phi : \mathbb{N} \to \mathbb{N}$ telle que $\mathrm{H}^i(L^{(n)}, V) \to \mathrm{H}^i(L^{(\phi(n))}, V)$ soit nulle pour chaque $n \geq n_0$ et de poser, par exemple, $N = n_0$. Une telle fonction ϕ existe et est calculable car les objets et les flèches le sont. □

Remarque 6.6. Bien que cela ne soit pas nécessaire — sauf pour ne pas perdre la primitive récursivité — signalons que l'on peut être plus précis. Avec les notations de l'énoncé, on a pour chaque $N \geq n \geq n_0$ un morphisme de la suite exacte

$$0 \to \mathrm{H}^1(L^{(n)}, V) \to \mathrm{H}^1(L, V) \to \mathrm{H}^1(L^{[n]}, V)$$

vers la suite exacte

$$0 \to \mathrm{H}^1(L^{(N)}, V) \to \mathrm{H}^1(L, V) \to \mathrm{H}^1(L^{[N]}, V),$$

où $L^{[n]}$ (resp. $L^{[N]}$) agit trivialement sur V et les flèches sont les flèches de fonctorialité évidentes. Par chasse au diagramme, l'injection $\mathrm{H}^1(L^{(N)}, V) \hookrightarrow \mathrm{H}^1(L, V)$

est un isomorphisme si la flèche « verticale » $\mathrm{H}^1(L^{[n]}, V) \to \mathrm{H}^1(L^{[N]}, V)$ est nulle. Il suffit pour cela que l'on ait l'inclusion $L^{[N]} \subseteq L^{[n][2]}$. À n fixé, un tel N peut être obtenu à partir de la suite exacte

$$1 \to L^{[n]} \to L \to L^{(n)} \to 1$$

par application de la proposition 6.3 et de l'estimation du rang du groupe libre $L^{[n]}$ par la formule de l'indice de Schreier ([Serre 1977, I, §3.4] ou [Rotman 1995, théorème 11.45]). Considérons maintenant le cas $i \geq 2$. La suite spectrale de Hochschild–Serre associée à la suite exacte précédente dégénère en E_3, car $\mathrm{H}^j(L^{[n]}, V)$ est nul pour $j > 1$. Comme l'aboutissement est nul — pour la même raison — en degré cohomologique > 1, la flèche

$$d_2 : \mathrm{H}^{i-2}(L^{(n)}, \mathrm{H}^1(L^{[n]}, V)) \to \mathrm{H}^i(L^{(n)}, V)$$

est surjective pour chaque $i \geq 2$. Ceci est bien entendu valable pour chaque $N \geq n$. Il en résulte que pour tuer la flèche $\mathrm{H}^i(L^{(n)}, V) \to \mathrm{H}^i(L^{(N)}, V)$, il suffit de tuer $\mathrm{H}^1(L^{[n]}, V) \to \mathrm{H}^1(L^{[N]}, V)$. C'est ce que l'on a fait ci-dessus.

Remarque 6.7. Il serait intéressant de calculer la plus petite fonction ϕ telle que les flèches $\mathrm{H}^i(L^{(n)}, \mathbb{Z}/\ell\mathbb{Z}) \to \mathrm{H}^i(L^{(\phi(d,i,n))}, \mathbb{Z}/\ell\mathbb{Z})$ soient nulles. (Lorsque $d = 1$ — cas d'un pro-ℓ-groupe abélien libre — la fonction $n \mapsto n+1$ convient.) Nous ignorons la réponse à cette question, mais nous indiquons un argument, duquel nous sommes redevables à Jean-Pierre Serre, qui montre que si $i = 2$ et si $L^{[n]}$ désigne maintenant la filtration de Frattini itérée $\Phi^n L$ plutôt que la filtration $F^n L$ considérée ci-dessus (cf. 3.1.2 à ce sujet), et bien sûr $L^{(n)} = L/\Phi^n L$, alors la fonction $n \mapsto n+1$ convient. Autrement dit, la flèche $\mathrm{H}^i(L^{(n)}, \mathbb{Z}/\ell\mathbb{Z}) \to \mathrm{H}^i(L^{(n+1)}, \mathbb{Z}/\ell\mathbb{Z})$ est nulle.

En comparant les suites spectrales de Hochschild–Serre associées aux suites exactes $1 \to L^{[n]} \to L \to L^{(n)} \to 1$ et $1 \to L^{[n]}/L^{[n+1]} \to L^{(n+1)} \to L^{(n)} \to 1$, le morphisme évident de la seconde suite spectrale vers la première donne :

$$\begin{array}{ccccc}
\mathrm{H}^0(L^{(n)}, \mathrm{H}^1(L^{[n]}/L^{[n+1]}, \mathbb{Z}/\ell\mathbb{Z})) & \longrightarrow & \mathrm{H}^2(L^{(n)}, \mathbb{Z}/\ell\mathbb{Z}) & \longrightarrow & \mathrm{H}^2(L^{(n+1)}, \mathbb{Z}/\ell\mathbb{Z}) \\
\downarrow & & \| & & \downarrow \\
\mathrm{H}^0(L^{(n)}, \mathrm{H}^1(L^{[n]}, \mathbb{Z}/\ell\mathbb{Z})) & \longrightarrow & \mathrm{H}^2(L^{(n)}, \mathbb{Z}/\ell\mathbb{Z}) & \longrightarrow & \mathrm{H}^2(L, \mathbb{Z}/\ell\mathbb{Z}) = 0
\end{array}$$

Or la flèche canonique de $\mathrm{H}^1(L^{[n]}/L^{[n+1]}, \mathbb{Z}/\ell\mathbb{Z}) = \mathsf{Hom}(L^{[n]}/L^{[n+1]}, \mathbb{Z}/\ell\mathbb{Z})$ vers

$$\mathrm{H}^1(L^{[n]}, \mathbb{Z}/\ell\mathbb{Z}) = \mathsf{Hom}(L^{[n]}, \mathbb{Z}/\ell\mathbb{Z})$$

est un isomorphisme puisque nous avons pris la filtration où $L^{[n+1]}$ est le Frattini de $L^{[n]}$. Comme tout élément de $\mathrm{H}^2(L^{(n)}, \mathbb{Z}/\ell\mathbb{Z})$ se relève à $\mathrm{H}^0(L^{(n)}, \mathrm{H}^1(L^{[n]}, \mathbb{Z}/\ell\mathbb{Z}))$, on en conclut que son image dans $\mathrm{H}^2(L^{(n+1)}, \mathbb{Z}/\ell\mathbb{Z})$ est nulle.

7. Calcul de la cohomologie d'une polycourbe ℓ-élémentaire

7.1. Soit X une polycourbe ℓ-élémentaire sur $\mathrm{Spec}(k)$, où k est un corps algébriquement clos, que l'on peut supposer factorisée en courbes ℓ-élémentaires ($X = X_m \to X_{m-1} \to \cdots \to X_1 \to \mathrm{Spec}\, k$ où $\dim X_i = i$). D'après 1.4.7, c'est un $K(\pi, 1)$ pro-ℓ, où π est le pro-ℓ complété du groupe fondamental de X, qui est extension itérée de pro-ℓ groupes libres de type fini. En particulier, pour chaque ℓ-groupe abélien fini Λ et chaque entier $d \geq 0$ le groupe $\mathrm{H}^d(X, \Lambda)$ est canoniquement isomorphe à $\mathrm{H}^d(\pi, \Lambda)$ qui s'identifie, d'après l'égalité $\pi = \lim_n \pi^{(n)}$ (3.2.1) et [Serre 1994, I, §2.2, proposition 8], à la colimite des $\mathrm{H}^d(\pi^{(n)}, \Lambda)$.

L'objectif de cette section est de montrer que l'on peut déterminer une paire (N_d, ϕ_d) telle que ce système inductif $\mathrm{H}^d(\pi^{(n)}, \Lambda)$, $n \geq 0$, soit (N_d, ϕ_d)-essentiellement constant au sens de 5.3.

7.2. ***Dévissage.*** On raisonne par récurrence sur la dimension m de X. Par hypothèse (cf. 1.4.7, démonstration), le groupe π s'insère dans une suite exacte

$$1 \to \pi' \to \pi \to \pi'' \to 1,$$

où π'' est un pro-ℓ groupe libre (non abélien) et π' est une extension itérée de tels groupes. Cette suite exacte est d'*origine géométrique*, c'est-à-dire déduite de morphismes calculables de schémas (normaux connexes) comme ci-dessous, par application du foncteur « groupe fondamental pro-ℓ ».

$$\begin{array}{cccc} \pi & X & \longleftarrow & X_{\bar\eta} \quad \pi' \\ & \downarrow & & \downarrow \\ [\text{pro-}\ell\text{-libre}]\ \pi'' & Y & \longleftarrow & \bar\eta \\ & \downarrow & & \\ & k & & \end{array}$$

(où $Y = X_1$ est une courbe ℓ-élémentaire et $\bar\eta$ un point générique géométrique de celle-ci ; soulignons que $X_{\bar\eta} \to \bar\eta$ est encore une polycourbe ℓ-élémentaire, cette fois de dimension $m-1$). Notons que l'on peut calculer le nombre de pro-générateurs (3.3.3) de π'' et π', qui apparaissent dans le lemme d'Artin–Rees–Frattini effectif 6.3. (Pour π', on peut procéder par récurrence ou bien utiliser la calculabilité du H^1.)

Fixons j. D'après 3.3 et 3.4.1, on peut calculer pour chaque $n \geq 1$ la suite exacte $1 \to \widetilde{\pi}'^{(n)} \to \pi^{(n)} \to \pi''^{(n)} \to 1$ (de groupes finis) considérée en 6.4 et, en particulier, calculer $\widetilde{\pi}'^{(n)} = \pi'/(\pi' \cap \pi^{[n]})$. L'hypothèse de récurrence permet d'affirmer que le système inductif $\mathrm{H}^j(\pi'^{(n)}, \Lambda)$ est explicitement essentiellement constant. D'après *loc. cit.*, il en est de même de $V_n := \mathrm{H}^j(\widetilde{\pi}'^{(n)}, \Lambda)$. (Comme rappelé en 4.2.4, on sait calculer chacun de ces différents groupes de cohomologie.)

7.3. ***Cas d'une courbe.*** Soit $V = \operatorname{colim}_n V_n$; c'est un Λ-module de type fini. Il résulte du caractère explicitement essentiellement constant de la colimite que l'on peut calculer V ainsi que l'action induite d'un quotient explicite $\pi''^{(n_0)}$ de π''. Fixons i. D'après 6.5, on peut calculer un couple (M, ψ) tel que le système $\mathrm{H}^i(\pi''^{(n)}, V)$, $n \geq n_0$, soit (M, ψ)-essentiellement constant. On veut montrer que, quitte à changer M et ψ, il en est de même du système inductif $\mathrm{H}^i(\pi''^{(n)}, V_n)$. Par hypothèse, il existe un entier $N \geq n_0$ et une fonction strictement croissante $\phi : \mathbb{N} \to \mathbb{N}$ tels que $(V_n)_n$ soit (N, ϕ)-essentiellement constant ; en particulier, le morphisme $(V_n)_{n\geq N} \to (V_{\phi(n)})_{n\geq N}$ se factorise à travers le morphisme $(V_n)_n \to (V)_n$, où $(V)_n$ est le système inductif constant de valeur V. Passant à la cohomologie, on en déduit un diagramme commutatif

$$\begin{array}{ccc} \mathrm{H}^i(\pi''^{(\bullet)}, V_\bullet) & \longrightarrow & \mathrm{H}^i(\pi''^{(\bullet)}, V) \\ \downarrow & \overset{h_\bullet}{\swarrow} & \downarrow \\ \mathrm{H}^i(\pi''^{(\phi(\bullet))}, V_{\phi(\bullet)}) & \longrightarrow & \mathrm{H}^i(\pi''^{(\phi(\bullet))}, V) \end{array}$$

D'après 5.9, le système inductif $\mathrm{H}^i(\pi''^{(\bullet)}, V_\bullet)$ est $(\phi M, \phi\psi)$-essentiellement constant.

7.4. ***Suite spectrale de Hochschild–Serre.*** Revenons maintenant au calcul de la cohomologie du schéma X. On a

$$\mathrm{R}\Gamma(X, \Lambda) = \mathrm{R}\Gamma(\pi, \Lambda) = \mathrm{R}\Gamma\big(\pi'', \mathrm{R}\Gamma(\pi', \Lambda)\big),$$

que l'on approche par

$$\mathrm{R}\Gamma(\pi^{(n)}, \Lambda) = \mathrm{R}\Gamma\big(\pi''^{(n)}, \mathrm{R}\Gamma(\widetilde{\pi}'^{(n)}, \Lambda)\big).$$

D'après [Serre 1994, I, §2.6], on a pour chaque entier $\lambda \geq 1$ une suite spectrale

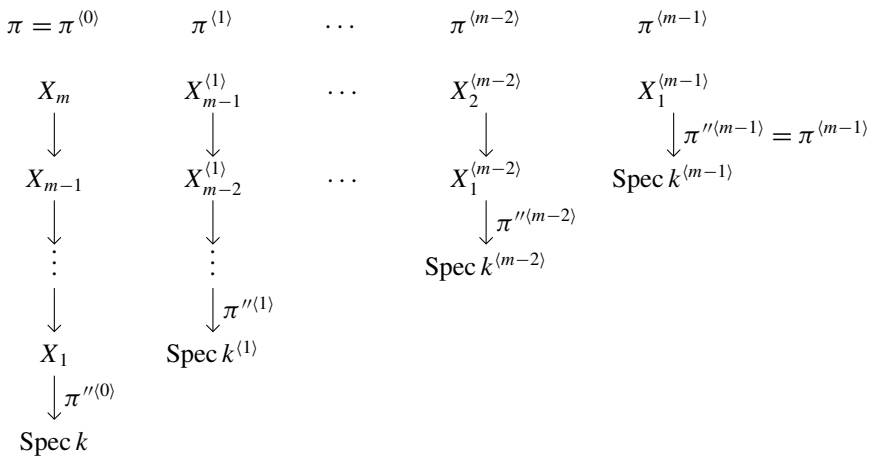
$$\mathrm{E}_{2,\lambda}^{i,j} = \mathrm{H}^i\big(\pi''^{(\lambda)}, \mathrm{H}^j(\widetilde{\pi}'^{(\lambda)}, \Lambda)\big) \implies \mathrm{H}^{i+j}(\pi^{(\lambda)}, \Lambda).$$

Il résulte de 5.8 et de ce qui précède que pour chaque entier $d \geq 0$ on peut calculer (N_d, ϕ_d) tels que le système inductif $\mathrm{H}^d(\pi^{(\bullet)}, \Lambda)$ soit (N_d, ϕ_d)-essentiellement constant. En particulier, on peut trouver deux entiers $\alpha \leq \beta$ tels que

$$\mathrm{H}^d(\pi, \Lambda) = \mathrm{Im}\big(\mathrm{H}^d(\pi^{(\alpha)}, \Lambda) \to \mathrm{H}^d(\pi^{(\beta)}, \Lambda)\big).$$

Ces objets sont donc algorithmiquement calculables.

7.5. ***Synthèse.*** Résumons la situation de cette section sous la forme du diagramme suivant avec des notations légèrement différentes pour expliciter la récurrence :



Si $X = X_m \to X_{m-1} \to \cdots \to X_1 \to \operatorname{Spec} k$ est la polycourbe ℓ-élémentaire de départ, on appelle $X_{m-i}^{\langle i\rangle} \to X_{m-i-1}^{\langle i\rangle} \to \cdots \to X_1^{\langle i\rangle} \to \operatorname{Spec} k^{\langle i\rangle}$ sa fibre au-dessus d'un point générique géométrique de X_i, et $\pi^{\langle i\rangle}$ le groupe fondamental pro-ℓ de cette fibre $X_{m-i}^{\langle i\rangle}$, ainsi que $\pi''^{\langle i\rangle}$ celui de $X_1^{\langle i\rangle}$. Les $\pi''^{\langle i\rangle}$ sont des groupes pro-ℓ-libres dont on peut calculer le nombre de générateurs ; les $\pi^{\langle i\rangle}$ s'inscrivent dans des suites exactes $1 \to \pi^{\langle i+1\rangle} \to \pi^{\langle i\rangle} \to \pi''^{\langle i\rangle} \to 1$, permettant de calculer leur nombre de générateurs, et des fonctions explicitant le fait que les $\mathrm{H}^d(\pi^{\langle i\rangle}, \Lambda)$ sont essentiellement constants.

8. Descente

8.1. Soient k un corps algébriquement clos, X un k-schéma algébrique (supposé décrit comme en 16.2), et ℓ un nombre premier inversible sur k. D'après 1.4.12, il existe un X-schéma simplicial $X_\bullet$ calculant la cohomologie étale de X à coefficients dans le ℓ-groupe abélien fini Λ, et dont les constituants sont des coproduits de polycourbes ℓ-élémentaires. Par descente cohomologique et 1.4.4, les flèches ci-dessous sont des isomorphismes :

$$\mathrm{R}\Gamma(X_{\text{ét}}, \Lambda) \xrightarrow{\sim} \mathrm{R}\Gamma(\operatorname{Tot} X_{\bullet\text{ét}}, \Lambda) \xleftarrow{\sim} \mathrm{R}\Gamma(\operatorname{Tot} X_{\bullet\ell\text{ét}}, \Lambda),$$

où $\operatorname{Tot} X_{\bullet\text{ét}}$ (resp. $\operatorname{Tot} X_{\bullet\ell\text{ét}}$) désigne le topos total associé au système simplicial des topos $X_{i\text{ét}}$ (resp. $X_{i\ell\text{ét}}$), $i \geq 0$. Le second isomorphisme résulte du fait que les images directes entre topos simpliciaux se calculent étage par étage, si bien que l'adjonction est un isomorphisme si elle l'est sur chaque étage (cf. [Deligne 1974, 5.2.5] ou [Illusie 1972, VI.5.8.1 (iii)]).

8.2. Fixons un entier $d \geq 0$ puis un entier $r > d$. D'après les observations précédentes et 1.4.13, il existe un X-schéma simplicial $X_\bullet$, à tronqué (= squelette) $X_{\bullet\leq r}$ calculable, tel que $\mathrm{H}^d(X_{\text{ét}}, \Lambda) = \mathrm{H}^d(\operatorname{Tot} X_{\bullet\ell\text{ét}}, \Lambda)$ et tel que les X_i soient des

coproduits finis de k-polycourbes ℓ-élémentaires.

Pour alléger les notations, on omet dorénavant les indices « $_{\ell\text{ét}}$ » et « $_{\text{ét}}$ ».

Pour chaque entier $\lambda \geq 2$, on a une suite spectrale [Illusie 1972, VI.6.2.3.2]

$$\mathrm{E}_{1,\lambda}^{i,j} = \mathrm{H}^j(X_i^{(\lambda)}, \Lambda) \implies \mathrm{H}^{i+j}(\mathrm{Tot}\, X_\bullet^{(\lambda)}, \Lambda),$$

où les topos $X_i^{(\lambda)}$ sont comme définis en 3.2. Il résulte donc de l'exactitude des colimites filtrantes [ÉGA III$_1$ 1961, 0.11.1.8] et des isomorphismes

$$\mathrm{colim}_\lambda\, \mathrm{H}^j(X_i^{(\lambda)}, \Lambda) \xrightarrow{\sim} \mathrm{H}^j(X_i, \Lambda),$$

que la cohomologie de $\mathrm{Tot}\, X_\bullet$ est colimite de la cohomologie des $\mathrm{Tot}\, X_\bullet^{(\lambda)}$. D'autre part, d'après les résultats de §7 (cas d'une polycourbe ℓ-élémentaire), on peut calculer (N_1, ϕ_1) tels que les systèmes inductifs $(\mathrm{E}_{1,\lambda}^{i,j})_\lambda$ soient (N_1, ϕ_1)-essentiellement constants pour chaque $i, j \geq 0$ tels que $i + j \leq 2d + 1$. Il en résulte (5.8) que l'on peut calculer (N_∞, ϕ_∞) tels que le système inductif $\mathrm{H}^d(\mathrm{Tot}\, X_\bullet^{(\lambda)}, \Lambda)$ soit (N_∞, ϕ_∞)-essentiellement constants ; en particulier, on peut calculer deux entiers $\mu \leq \nu$ tels que l'on ait

$$\mathrm{H}^d(X, \Lambda) = \mathrm{Im}\big(\mathrm{H}^d(\mathrm{Tot}\, X_\bullet^{(\mu)}, \Lambda) \to \mathrm{H}^d(\mathrm{Tot}\, X_\bullet^{(\nu)}, \Lambda)\big).$$

Comme expliqué en 4.1.2, on a $\mathrm{H}^d(\mathrm{Tot}\, X_\bullet^{(\mu)}, \Lambda) \xrightarrow{\sim} \mathrm{H}^d(\mathrm{Tot}\, X_{\bullet\leq r}^{(\mu)}, \Lambda)$, et de même pour ν. Que l'on puisse trouver une présentation explicite (13.3) de $\mathrm{H}^d(X, \Lambda)$ résulte alors de la proposition 4.3.1.

8.3. *Hyper-Čech.*

8.3.1. Soit $X'_\bullet \to X$ un hyperrecouvrement pour la topologie des altérations. Vérifions que l'on peut calculer les morphismes $\check{\mathrm{H}}^d(X'_\bullet, \Lambda) \to \mathrm{H}^d(X, \Lambda)$, comme annoncé en 0.4.

D'après le lemme 1.4.13, on peut calculer (en tout étage) un hyperrecouvrement $X_\bullet \to X$ comme ci-dessus, se factorisant à travers un morphisme $X_\bullet \to X'_\bullet$. Fixons $d \geq 0$. On sait que la flèche $\check{\mathrm{H}}^d(X'_\bullet, \Lambda) \to \mathrm{H}^d(X, \Lambda)$ est la composée des flèches $\check{\mathrm{H}}^d(X'_\bullet, \Lambda) \to \check{\mathrm{H}}^d(X_\bullet, \Lambda)$ et $\check{\mathrm{H}}^d(X_\bullet, \Lambda) \to \mathrm{H}^d(X, \Lambda)$, la première étant trivialement calculable pour des schémas simpliciaux donnés (par calculabilité fonctorielle du π_0). On est donc ramené au cas particulier où $X'_\bullet = X_\bullet$. La conclusion résulte alors d'une part du fait que, comme observé en 4.3.2, on a $\check{\mathrm{H}}^d(X_\bullet, \Lambda) = \mathrm{H}^d(\mathrm{Tot}\, X_{\bullet\leq r}^{(1)}, \Lambda)$ pour $r > d$ et, d'autre part, de la calculabilité des flèches $\mathrm{H}^d(\mathrm{Tot}\, X_{\bullet\leq r}^{(\mu)}, \Lambda) \to \mathrm{H}^d(\mathrm{Tot}\, X_{\bullet\leq r}^{(\nu)}, \Lambda)$ pour $\mu \leq \nu \leq \infty$.

8.3.2. Il résulte de ce qui précède que, donnés deux hyperrecouvrements $X'_\bullet \to X_\bullet$ de X pour la topologie des altérations, on sait vérifier si la flèche $\check{\mathrm{H}}^d(X_\bullet, \Lambda) \to \mathrm{H}^d(X, \Lambda)$ identifie la cohomologie de X au quotient de $\check{\mathrm{H}}^d(X_\bullet, \Lambda)$ par le noyau (calculable) de $\check{\mathrm{H}}^d(X_\bullet, \Lambda) \to \check{\mathrm{H}}^d(X'_\bullet, \Lambda)$. (D'autre part, on sait qu'il existe deux tels

hyperrecouvrements.) En particulier, si les $X_{\alpha\bullet}$ sont comme en 0.2, le système inductif $\check{\mathrm{H}}^d(X_{\alpha\bullet}, \Lambda)$ est explicitement essentiellement constant (mais le « explicitement » utilise une recherche non bornée).

Remarque 8.3.3. Notons que si $V \to U$ est un morphisme de k-schémas algébriques se factorisant à travers un revêtement ℓ-étale n-approché universel $U^{[n]}$ de U, le morphisme de topos $V^{(n)} \to U^{(n)}$ se factorise à travers $V^{(n)} \to V^{(1)}$, dont le but est naturellement équivalent au topos discret des faisceaux sur $\pi_0(V)$. D'autre part, pour chaque $X_\bullet$ comme en 8.2 et chaque entier $n \geq 1$, on devrait sans aucun doute pouvoir fabriquer en utilisant les techniques usuelles de construction d'hyperrecouvrements (cf. 1.4.13 et 4.2.1) — donc, en particulier, sans nouvelle recherche non bornée — un hyperrecouvrement $\tilde{X}_\bullet$ de X au-dessus de $X_\bullet$ tel que les $\tilde{X}_i \to X_i$ se factorisent par un revêtement n-approché universel de X_i. Que $\mathrm{R}\Gamma(X_\bullet^{(n)}, \Lambda) \to \mathrm{R}\Gamma(X, \Lambda)$ se factorise à travers $\check{\mathrm{R}}\Gamma(\tilde{X}_\bullet, \Lambda) \to \mathrm{R}\Gamma(X, \Lambda)$ entraîne que l'on peut obtenir (sans nouvelle recherche non bornée) des cocycles hyper-Čech pour une base des $\mathrm{H}^i(X, \Lambda)$.

8.4. *Calcul de* $\mathbf{R\Gamma(X, \Lambda)}$.

8.4.1. Soient X et Λ comme ci-dessus et $X_{\alpha\bullet}$ un système projectif (indexé par les entiers)[8] d'hyperrecouvrements de X tel que pour chaque entier i, on ait l'égalité $\mathrm{colim}_\alpha \check{\mathrm{H}}^i(X_{\alpha\bullet}, \Lambda) \xrightarrow{\sim} \mathrm{H}^i(X, \Lambda)$, ou encore un quasi-isomorphisme $\mathrm{hocolim}_\alpha \check{\mathrm{R}}\Gamma(X_{\alpha\bullet}, \Lambda) \xrightarrow{\sim} \mathrm{R}\Gamma(X, \Lambda)$, où $\check{\mathrm{R}}\Gamma(X_{\alpha\bullet}, \Lambda)$ est le complexe de Čech déduit du Λ-module cosimplicial $\Gamma(X_{\alpha\bullet}, \Lambda)$. (Rappelons que dans une catégorie abélienne satisfaisant la condition AB5 de Grothendieck, la cohomologie d'une colimite homotopique est la colimite des groupes de cohomologie.) Le complexe $\mathrm{R}\Gamma(X, \Lambda)$ appartenant à $\mathrm{D}_c^b(\Lambda)$, il résulte du lemme classique [SGA $4\frac{1}{2}$ 1977, Rapport, 4.7] qu'il existe un complexe $\mathcal{K}$ de Λ-modules de type fini, concentré en degrés $[0, 2\dim(X)]$ et, pour α suffisamment grand, un morphisme de (vrais) complexes $\mathcal{K} \to \check{\mathrm{R}}\Gamma(X_{\alpha\bullet}, \Lambda)$ tel que la flèche composée $\mathcal{K} \to \mathrm{R}\Gamma(X, \Lambda)$ soit un quasi-isomorphisme. Pour calculer un tel $\mathcal{K}$, il suffit de parcourir les morphismes $\mathcal{K} \to \check{\mathrm{R}}\Gamma(X_{\alpha\bullet}, \Lambda)$ et de s'arrêter lorsqu'on en a trouvé un induisant le quasi-isomorphisme recherché (en degré $0 \leq i \leq 2\dim(X)$). C'est possible car on sait calculer les flèches $\check{\mathrm{H}}^i(X_{\alpha\bullet}, \Lambda) \to \mathrm{H}^i(X, \Lambda)$.

8.4.2. La remarque précédente devrait même permettre de calculer $\mathrm{R}\Gamma(X, \Lambda)$ sans plus de recherches non bornées que celles faites jusqu'à 8.2.

8. Lorsque k est dénombrable, ce qui suffit pour notre propos, l'existence d'un tel système projectif est élémentaire (voir [Deligne 1980, 5.2.2], cité en 0.2). Pour k quelconque, on peut améliorer le résultat classique selon lequel la catégorie des hyperrecouvrements *à homotopie près* est cofiltrante (cf. p. ex. [Artin et Mazur 1969, 8.13]) en la « rigidifiant » ([Friedlander 1982, §4] ; comparer avec 3.4.2). D'après O. Gabber (communication personnelle) on a des résultats semblables pour des sites généraux, sans hypothèse de finitude (ni, notamment, d'existence de suffisamment de points).

9. Fonctorialité

9.1. *Fonctorialité sur* Spec(k).

9.1.1. Soient k un corps algébriquement clos, $f : Y \to X$ un morphisme de k-schémas algébriques (supposé décrit comme en 16.2), et Λ un ℓ-groupe abélien fini, avec ℓ inversible sur k. D'après 1.4.12, il existe un morphisme simplicial $Y_\bullet \to X_\bullet$ au-dessus de f, calculable jusqu'à des étages arbitrairement élevés (et dépendant de ℓ mais pas de Λ), donnant lieu à un diagramme commutatif

$$\begin{array}{ccccccc}
\mathrm{R}\Gamma(\mathrm{Tot}\, X_{\bullet \ell\text{ét}}, \Lambda) & \xrightarrow{\sim} & \mathrm{R}\Gamma(\mathrm{Tot}\, X_{\bullet\text{ét}}, \Lambda) & \longrightarrow & \mathrm{R}\Gamma(\mathrm{Tot}\, Y_{\bullet\text{ét}}, \Lambda) & \xleftarrow{\sim} & \mathrm{R}\Gamma(\mathrm{Tot}\, Y_{\bullet \ell\text{ét}}, \Lambda) \\
 & & \uparrow\sim & & \uparrow\sim & & \\
 & & \mathrm{R}\Gamma(X, \Lambda) & \longrightarrow & \mathrm{R}\Gamma(Y, \Lambda) & &
\end{array}$$

D'après ce qui précède (§8), il existe deux entiers explicites $\mu \leq \nu$ tels que pour chaque $d \leq 2\max\{\dim(X), \dim(Y)\} < r$, on ait

$$\mathrm{H}^d(Z, \Lambda) = \mathrm{Im}\big(\mathrm{H}^d(\mathrm{Tot}\, Z^{(\mu)}_{\bullet \leq r}, \Lambda) \to \mathrm{H}^d(\mathrm{Tot}\, Z^{(\nu)}_{\bullet \leq r}, \Lambda)\big)$$

pour $Z = X$ ou Y. Le morphisme $\mathrm{H}^d(\mathrm{Tot}\, X^{(\nu)}_{\bullet \leq r}, \Lambda) \to \mathrm{H}^d(\mathrm{Tot}\, Y^{(\nu)}_{\bullet \leq r}, \Lambda)$ étant calculable (cf. 4.2.6), on peut trouver une présentation explicite du morphisme $\mathrm{H}^d(f, \Lambda) : \mathrm{H}^d(X, \Lambda) \to \mathrm{H}^d(Y, \Lambda)$ (au sens de 13.3). Si Λ est le corps $\mathbb{Z}/\ell\mathbb{Z}$, cela revient bien entendu à calculer le rang de $\mathrm{H}^d(f, \mathbb{Z}/\ell\mathbb{Z})$.

Notons que l'on pourrait bien entendu utiliser la présentation tirée de 8.3, pour obtenir le même résultat (voir aussi 9.2).

9.1.2. *Amélioration.* Vérifions maintenant que pour toute collection finie $f_1, \ldots, f_r$ de k-morphismes explicites $Y \to X$, on peut calculer des présentations explicites des $\mathrm{H}^d(f_i, \Lambda)$ relativement à de *mêmes* présentations explicites de $\mathrm{H}^d(X, \Lambda)$ et $\mathrm{H}^d(Y, \Lambda)$. Il résulte en effet de 1.4.12 et 1.4.13 qu'il existe pour chaque $\alpha \in \{1, \ldots, r\}$ un morphisme $Y_{\alpha\bullet} \to X_\bullet$ comme en *loc. cit.* au-dessus de f_α. En considérant le produit fibré des $Y_{\alpha\bullet}$ au-dessus de Y et en réappliquant la construction de *loc. cit.*, on en déduit qu'il existe un diagramme commutatif

$$\begin{array}{ccc}
Y_\bullet & \begin{array}{c} \xrightarrow{f_{1\bullet}} \\ \vdots \\ \xrightarrow[f_{r\bullet}]{} \end{array} & X_\bullet \\
\downarrow & & \downarrow \\
Y & \begin{array}{c} \xrightarrow{f_1} \\ \vdots \\ \xrightarrow[f_r]{} \end{array} & X
\end{array}$$

où les flèches verticales *ne dépendent pas de l'indice* $\alpha \in \{1, \ldots, r\}$. La conclusion en résulte aussitôt.

(En particulier, donnés deux morphismes $f, g : Y \to X$, on peut décider si $\mathrm{H}^d(g, \Lambda) = \mathrm{H}^d(f, \Lambda)$.)

Notons que si $Y = X$, on peut supposer que les Λ-modules explicites $\mathrm{H}^d(X, \Lambda)$ et $\mathrm{H}^d(Y, \Lambda)$ sont *égaux*. Pour s'en convaincre, il suffit par exemple de rajouter l'identité $Y \to X$ aux morphismes $f_1, \ldots, f_r$ et de composer avec l'inverse de l'isomorphisme $\mathrm{H}^d(X, \Lambda) \to \mathrm{H}^d(Y, \Lambda)$ qui s'en déduit.

On peut reformuler la fonctorialité établie sous la forme suivante.

9.1.3. Soit $\mathcal{G}$ un graphe fini orienté avec arêtes multiples possibles. Supposons donné un étiquetage de $\mathcal{G}$ par la catégorie des k-schémas algébriques, c'est-à-dire un étiquetage de ses sommets par des k-schémas algébriques et un étiquetage des arêtes par des k-morphismes (entre les schémas correspondants). On peut calculer un étiquetage du graphe opposé $\mathcal{G}^{\mathrm{op}}$ par la catégorie des Λ-modules finis, déduit du précédent par application du foncteur $\mathrm{H}^d(-, \Lambda)$.

On peut déduire cet énoncé du précédent en considérant le coproduit

$$X = \mathrm{Spec}(k) \amalg \coprod_s X_s,$$

où X_s parcourt les étiquettes des sommets s de $\mathcal{G}$, et les endomorphismes $X \to X$ envoyant chaque $X_{s'}$, sauf un X_s, sur $\mathrm{Spec}(k)$ et déterminé par l'étiquette d'une arête sur ce dernier X_s.

9.2. *Action galoisienne.*

9.2.1. Soient ${}_0k$ un corps (calculable et disposant d'un algorithme de factorisation et d'une p-base finie explicite : cf. 12.7) et ${}_0X$ un ${}_0k$-schéma algébrique explicite. Fixons une clôture algébrique k de ${}_0k$ et notons X le k-schéma obtenu par extension des scalaires. Nous allons montrer que l'on peut calculer une extension finie galoisienne ${}_1k/{}_0k$ telle que l'action du groupe de Galois de ${}_0k$ sur $\mathrm{H}^*(X, \Lambda)$ se factorise à travers $\Gamma = \mathrm{Gal}({}_1k/{}_0k)$ et calculer la représentation du groupe fini correspondante. Toute extension étale de la clôture parfaite de ${}_0k$ dans k se descendant explicitement à ${}_0k$, on peut supposer le corps ${}_0k$ parfait (12.5(v)).

9.2.2. Fixons d. Comme on l'a vu en 8.3, il existe un hyperrecouvrement tronqué pour la topologie des altérations $X_{\bullet \leq r} \to X$ tel que $\check{\mathrm{H}}^d(X_{\bullet \leq r}, \Lambda) \to \mathrm{H}^d(X, \Lambda)$ soit *surjective* ; par cofinalité (observée en 1.4.11), il existe un tel hyperrecouvrement *défini sur* ${}_0k$. La calculabilité de l'action du groupe de Galois sur $\mathrm{H}^d(X, \Lambda)$ se déduit donc de celle de l'action sur $\check{\mathrm{H}}^d(X_{\bullet \leq r}, \Lambda)$ et de la calculabilité de la flèche. Plus précisément, si $c \in \mathrm{H}^d(X, \Lambda)$ est l'image d'une d-chaîne $z \in \mathrm{H}^0(X_d, \Lambda)$, la classe de cohomologie $\gamma \cdot c$, où $\gamma \in \mathrm{Gal}(k/{}_0k)$, est l'image de la d-chaîne $\gamma \cdot z$ déduite de l'action du groupe de Galois sur $\pi_0(X_d) = \pi_0({}_0X_d \otimes_{{}_0k} k)$.

Notons que l'hyperrecouvrement tronqué $X_{\bullet\leq r} \to X$ est défini sur une sous-extension galoisienne finie ${}_1k/{}_0k$, et l'action précédente se factorise à travers le quotient fini $\Gamma = \mathrm{Gal}({}_1k/{}_0k)$. Ce dernier est calculable car ${}_0k$ est un corps calculable avec un algorithme de factorisation [Fried et Jarden 2008, 19.3.2].

10. Structure de l'algorithme et exemple simple

10.1. ***Structure générale.*** Récapitulons brièvement comment les différents éléments qui ont été présentés s'emboîtent pour fournir, en principe, un algorithme permettant de calculer $\mathrm{H}^d(X, \Lambda)$ pour X un schéma algébrique sur un corps algébriquement clos de caractéristique différente de ℓ et Λ un ℓ-groupe abélien fini.

Dans un premier temps, on calcule, jusqu'à un certain niveau r, un hyperrecouvrement $X_\bullet$ de X tel qu'explicité en 1.4.12. Plus exactement, on calcule $X_0 \to X$ qui recouvre X et dont les composantes sont des polycourbes ℓ-élémentaires (et en particulier, des $K(\pi, 1)$ pro-ℓ) : ceci se fait au moyen de la proposition 1.4.9 (compte tenu des remarques qui suivent au sujet de la constructivité) ; puis de même $X_1 \to X_0 \times_X X_0$ et ainsi de suite comme expliqué en 1.4.13. Cette construction des X_i doit être menée pour $i \leq r$ avec r qui dépend uniquement du degré en lequel on veut calculer la cohomologie (comme expliqué en 4.1.2, en fait $r = d + 1$ suffit).

D'après les résultats de la section 3, et s'appuyant sur la calculabilité du nombre de $\mathbb{Z}/\ell\mathbb{Z}$-torseurs établie en 2.1, on sait calculer, pour chaque niveau d'approximation fini $\lambda \geq 1$, et pour tout k-schéma algébrique normal Y, un revêtement ℓ-étale λ-approché universel $Y^{[\lambda]}$, ainsi que le groupe de Galois correspondant $\pi_Y^{[\lambda]}$ si Y est connexe.

D'après §4, on sait calculer, pour chaque niveau d'approximation fini $\lambda \geq 1$, le groupe $\mathrm{H}^d(\mathrm{Tot}\, X_\bullet^{(\lambda)}, \Lambda)$ (isomorphe à $\mathrm{H}^d(\mathrm{Tot}\, X_{\bullet\leq r}^{(\lambda)}, \Lambda)$ puisque r a été choisi assez grand), et même la flèche $\mathrm{H}^d(\mathrm{Tot}\, X_\bullet^{(\mu)}, \Lambda) \to \mathrm{H}^d(\mathrm{Tot}\, X_\bullet^{(\nu)}, \Lambda)$ pour deux entiers $\mu \leq \nu$.

Il s'agit donc de calculer de tels entiers pour que l'image de cette flèche soit le groupe $\mathrm{H}^d(X, \Lambda)$ recherché. Comme expliqué en §8, ceci résulte de 5.8 appliqué à la suite spectrale $\mathrm{E}_{1,\lambda}^{i,j} = \mathrm{H}^j(X_i^{(\lambda)}, \Lambda) \Rightarrow \mathrm{H}^{i+j}(\mathrm{Tot}\, X_\bullet^{(\lambda)}, \Lambda)$, une fois connus des fonctions explicitant, pour chaque i et j, le fait que $\mathrm{H}^j(X_i^{(\lambda)}, \Lambda)$ est essentiellement constant. De telles bornes sont obtenues en §7.

10.2. ***Esquisse d'exemple.*** Pour illustrer la manière dont l'algorithme s'exécuterait, nous esquissons le calcul de $\mathrm{H}^i(\mathbb{P}^1_k, \mathbb{Z}/\ell\mathbb{Z})$ pour les petits i en en suivant les différentes étapes. (Le cas encore plus simple d'une courbe *affine* lisse X consiste essentiellement à calculer $X^{[\lambda]}$ par 3.3 pour des petites valeurs de λ et à appliquer la proposition 6.5 : de toute façon, on est ramené à §2.)

Notons $U = \mathbb{P}^1_k \setminus \{\infty\}$ et $U' = \mathbb{P}^1_k \setminus \{0\}$ deux ouverts de Zariski qui recouvrent $\mathbb{P}^1_k$ et

dont on note $V := U \times_{\mathbb{P}^1_k} U'$ l'intersection. Soit $X_0 := U \amalg U' \to \mathbb{P}^1_k$, vu comme un $\mathbb{P}^1_k$-schéma simplicial 0-tronqué ; son cosquelette est donné par $X_p = X_0 \times_{\mathbb{P}^1_k} \cdots \times_{\mathbb{P}^1_k} X_0$ (avec $p+1$ facteurs), qui est le coproduit $U \amalg V \amalg \cdots \amalg V \amalg U'$ de U, U' et $2^{p+1} - 2$ copies de V qu'on imaginera étiquetés par les 2^{p+1} mots binaires w de longueur $p+1$, et pour $0 \leq i \leq p+1$, le morphisme $X_{\delta_{p,i}} \colon X_{p+1} \to X_p$ envoie par le morphisme évident la composante $X_{p+1,w}$ étiquetée w sur celle $X_{p,w'}$ étiquetée par le mot w' égal à w privé de son i-ième bit. Il s'agit manifestement d'un hyperrecouvrement. Comme U, U', V sont des (poly)courbes ℓ-élémentaires sur $\operatorname{Spec} k$, il est possible que la recherche de courbes élémentaires effectuée par l'algorithme retourne cet hyperrecouvrement.

Examinons maintenant comment se déroulerait le calcul de la cohomologie de $\operatorname{Tot} X_\bullet^{(\lambda+1)}$ (en fonction d'un entier $\lambda + 1 \geq 1$) à valeurs dans le faisceau constant $\mathbb{Z}/\ell\mathbb{Z}$. Comme $V = \mathbb{G}_{\mathrm{m}}$, le topos $V^{(\lambda+1)}$ est le topos des $\mathbb{Z}/\ell^\lambda\mathbb{Z}$-ensembles, tandis que $U^{(\lambda+1)}$ et $U'^{(\lambda+1)}$ sont, bien sûr, celui des ensembles. (Et pour un λ donné, l'algorithme est capable d'effectuer ce calcul en suivant 3.3.) Un faisceau abélien de $\operatorname{Tot} X_\bullet^{(\lambda+1)}$ est donc (cf. 4.1.1) la donnée pour chaque mot binaire w de longueur $p+1$ (pour $p \geq 0$) d'un groupe abélien $A_{p,w}$, muni d'une action de $\mathbb{Z}/\ell^\lambda\mathbb{Z}$ sauf si w est l'un des mots $00\cdots0$ ou $11\cdots1$, ainsi que de morphismes $A_{p,w} \to A_{p+1,w'}$ pour chaque mot w' obtenu en insérant un bit dans w, vérifiant les compatibilités évidentes. Si comme topos discret utilisé en §4 on prend $P_\bullet = X_\bullet^{(1)}$, alors un faisceau abélien de $\operatorname{Tot} P_\bullet$ correspond à de telles données sans l'action de $\mathbb{Z}/\ell^\lambda\mathbb{Z}$: à un tel objet est associé un complexe de différentielle

$$\bigoplus_{w \in \{0,1\}^{p+1}} A_{p,w} \to \bigoplus_{w \in \{0,1\}^{p+2}} A_{p+1,w} \qquad (\dagger)$$

somme alternée des morphismes $A_{p,w} \to A_{p+1,w'}$.

Les foncteurs $u^\star$ associant à un $\mathbb{Z}/\ell^\lambda\mathbb{Z}$-ensemble son ensemble sous-jacent, et $u_\star$ son adjoint à droite $X \mapsto \mathsf{Hom}_{\mathsf{Ens}}(\mathbb{Z}/\ell^\lambda\mathbb{Z}, X)$, définissent pour tout $\mathbb{Z}/\ell^\lambda\mathbb{Z}$-module une résolution de Godement, analogue (et quasi-isomorphe) à l'une des résolutions habituelles définissant la cohomologie des groupes (par exemple [Serre 1994, I, §2.2] ou [Neukirch, Schmidt et Wingberg 2000, I, §2]). Ces foncteurs forment un morphisme $\operatorname{Tot} P_\bullet \to \operatorname{Tot} X_\bullet^{(\lambda+1)}$. À partir du faisceau constant $A_{p,w} = \mathbb{Z}/\ell\mathbb{Z}$, l'algorithme (4.2) va donc calculer, en bas degrés, le complexe double dont les colonnes sont sommes de copies de la résolution qu'on vient de dire (et pour $w = 00\cdots0$, $11\cdots1$, de la résolution triviale), et dont les différentielles horizontales sont données par (†). Le calcul du $\mathrm{H}^i(\operatorname{Tot} X_\bullet^{(\lambda+1)}, \mathbb{Z}/\ell\mathbb{Z})$ est alors donné par la cohomologie du complexe simple associé à ce complexe double.

On peut prédire quel sera le résultat de ce calcul en utilisant la suite spectrale de descente décrite en 8.2 (et qui est la « première » suite spectrale associée au complexe double décrit ci-dessus) : il est facile de se convaincre que cette suite

spectrale dégénère en E_2, les seuls termes non nuls étant $E_2^{0,0} = \mathbb{Z}/\ell\mathbb{Z}$ et $E_2^{1,q} = H^q(\mathbb{Z}/\ell^\lambda\mathbb{Z}, \mathbb{Z}/\ell\mathbb{Z})$ si $q \geq 2$. Ainsi, $H^n(\mathrm{Tot}\, X_\bullet^{(\lambda+1)}, \mathbb{Z}/\ell\mathbb{Z})$ vaut $\mathbb{Z}/\ell\mathbb{Z}$ si $n = 0$, 0 si $n = 1$, et $H^{n-1}(\mathbb{Z}/\ell^\lambda\mathbb{Z}, \mathbb{Z}/\ell\mathbb{Z})$ si $n \geq 2$ (c'est-à-dire $\mathbb{Z}/\ell\mathbb{Z}$ dès que $\lambda \geq 1$). Pour $\lambda \leq \mu$, les flèches $H^n(\mathrm{Tot}\, X_\bullet^{(\lambda+1)}, \mathbb{Z}/\ell\mathbb{Z}) \to H^n(\mathrm{Tot}\, X_\bullet^{(\mu+1)}, \mathbb{Z}/\ell\mathbb{Z})$ correspondent bien aux morphismes fonctoriels (d'inflation) $H^{n-1}(\mathbb{Z}/\ell^\lambda\mathbb{Z}, \mathbb{Z}/\ell\mathbb{Z}) \to H^{n-1}(\mathbb{Z}/\ell^\mu\mathbb{Z}, \mathbb{Z}/\ell\mathbb{Z})$, et grâce à 6.5–6.7 on sait que cette flèche sera un isomorphisme pour $n \leq 2$ et nulle pour $n \geq 3$ dès que $1 \leq \lambda < \mu$. Muni de cette borne, l'algorithme calcule $H^n(\mathbb{P}^1_k, \mathbb{Z}/\ell\mathbb{Z})$ comme l'image de $H^n(\mathrm{Tot}\, X_\bullet^{(2)}, \mathbb{Z}/\ell\mathbb{Z}) \to H^n(\mathrm{Tot}\, X_\bullet^{(3)}, \mathbb{Z}/\ell\mathbb{Z})$, ce qui donne bien le résultat attendu.

Soulignons sur cet exemple le fait suivant : si on remplace les coefficients $\mathbb{Z}/\ell\mathbb{Z}$ par le groupe $\boldsymbol{\mu}_\ell$ des racines ℓ-ièmes de l'unité (qui lui est non canoniquement isomorphe) et le groupe $\mathbb{Z}/\ell^\lambda\mathbb{Z}$ par le groupe $\boldsymbol{\mu}_{\ell^\lambda}$ (de nouveau non canoniquement isomorphe) des automorphismes du revêtement étale $\mathbb{G}_\mathrm{m} \to \mathbb{G}_\mathrm{m}$ donné par $z \mapsto z^{\ell^\lambda}$, on se convainc aisément que le calcul ne dépend plus d'aucun choix arbitraire (même si la description ci-dessus en utilise), et on voit donc $H^2(\mathbb{P}^1_k, \boldsymbol{\mu}_\ell)$ comme $H^1(\boldsymbol{\mu}_{\ell^\lambda}, \boldsymbol{\mu}_\ell)$ (l'action de $\boldsymbol{\mu}_{\ell^\lambda}$ étant triviale), lui-même isomorphe à $\mathrm{Hom}(\boldsymbol{\mu}_{\ell^\lambda}, \boldsymbol{\mu}_\ell) = \mathbb{Z}/\ell\mathbb{Z}$ sans faire de choix arbitraire.

11. Compléments

On considère ici quelques résultats qui sont des prolongements naturels de notre théorème principal et on énonce en 11.5 quelques questions, dont certaines sont probablement hors de portée. Cette section se termine (11.6) par quelques précisions métamathématiques sur la nature des algorithmes que l'on espère pouvoir obtenir.

Ci-dessous k est un corps algébriquement clos et Λ un anneau commutatif fini de cardinal inversible sur k.

11.1. ***Cohomologie d'un schéma simplicial.*** Soit $X_\bullet$ un k-schéma algébrique simplicial. D'après [Deligne 1974, §6.4] et les résultats de §1.4, il existe un hyperrecouvrement $X_{\bullet\bullet} \to X_\bullet$ par des polycourbes ℓ-élémentaires tel que $H^*(X_\bullet, \Lambda) = H^*(X_{\bullet\bullet}, \Lambda)$. On peut donc procéder comme dans le cas non simplicial pour calculer le terme de gauche en tout degré donné à l'avance. Noter qu'il n'est pas absolument nécessaire d'utiliser une variante bisimpliciale de arguments précédents : d'après le théorème de Cartier–Eilenberg–Zilber ([Deligne 1974, 6.4.2.2] ou [Illusie 1971, I, §1.2]), on a $R\Gamma(X_{\bullet\bullet}, \Lambda) = R\Gamma(\delta X_{\bullet\bullet}, \Lambda)$, où $\delta X_{\bullet\bullet}$ est le schéma simplicial *diagonal* déduit de $X_{\bullet\bullet}$. Le même argument est valable si l'on veut calculer la cohomologie de $X_\bullet$ à valeurs dans un faisceau à composantes localement constantes (étage par étage).

Tout espace algébrique (au sens d'Artin) étant localement pour la topologie étale un schéma, on peut probablement utiliser le résultat précédent pour en calculer la cohomologie étale.

11.2. ***Cohomologie relative.*** On présente ici deux constructions de la cohomologie relative d'un morphisme $Y \to X$: la première (simpliciale) est valable en toute généralité, la seconde (11.2.5) s'applique uniquement à la cohomologie relativement à un sous-schéma fermé.

Rappelons que la cohomologie relative s'inscrit dans un triangle distingué

$$\mathrm{R}\Gamma(X/Y, \Lambda) \to \mathrm{R}\Gamma(X, \Lambda) \to \mathrm{R}\Gamma(Y, \Lambda) \xrightarrow{+1} .$$

Lorsque Λ est un corps, la calculabilité de la dimension du groupe de cohomologie relative $\mathrm{H}^i(X/Y, \Lambda)$ résulte donc immédiatement du théorème 0.1 : c'est une extension de $\mathrm{Ker}\big(\mathrm{H}^i(X, \Lambda) \to \mathrm{H}^i(Y, \Lambda)\big)$ par $\mathrm{Im}\big(\mathrm{H}^{i-1}(X, \Lambda) \to \mathrm{H}^{i-1}(Y, \Lambda)\big)$.

11.2.1. *Cône d'un morphisme simplicial.* Soit $f_\bullet : Y_\bullet \to X_\bullet$ un morphisme de topos simpliciaux (dont on notera $\mathrm{Tot}\, f_\bullet : \mathrm{Tot}\, Y_\bullet \to \mathrm{Tot}\, X_\bullet$ le morphisme entre les topos totaux, cf. 4.1.1) ; on pourra penser au cas d'un morphisme déduit, par passage aux topos étales, d'un morphisme de k-schémas algébriques simpliciaux. Notons $Cf_\bullet$ son *cône* : $Cf_n = X_n \amalg Y_{<n}$, où $Y_{<n} = \coprod_{-1 \le i < n} Y_i$ et, conformément à l'usage, Y_{-1} est le topos final e. Explicitons le morphisme de fonctorialité $Cf_\phi : Cf_m \to Cf_n$ déduit d'une application croissante $\phi : [n] = \{0, \dots, n\} \to [m] = \{0, \dots, m\}$. Sur le facteur X_m, c'est le morphisme composé $X_m \to X_n \hookrightarrow Cf_n$, la première flèche étant X_ϕ. Soit maintenant $-1 \le \mu < m$ et considérons l'application $\phi_\mu : [\nu] \to [\mu]$ déduite de ϕ par changement de base $[\mu] \hookrightarrow [m]$. Sur le facteur Y_μ, le morphisme Cf_ϕ est le morphisme composé $Y_\mu \to Y_\nu \hookrightarrow Cf_n$, la première flèche étant Y_{ϕ_μ} si $\nu < n$, et $Y_\mu \to Y_\nu \to X_\nu \hookrightarrow Cf_n$, où $Y_\nu \to X_\nu$ est f_ν, si $\nu = n$. Par exemple, le morphisme face $d_i : Cf_{n+1} \to Cf_n$, déduit de l'unique injection croissante $[n] \to [n+1]$ d'image ne contenant pas i, est induit par les identités $Y_j \to Y_j$ pour $j < i$ (composée avec $Y_n \to X_n$ si $j = n$) et les faces $d_i : Y_l \to Y_{l-1}$ pour $i \le l \le n$ et $d_i : X_{n+1} \to X_n$.

Soit $\phi_\bullet : \mathscr{F}_\bullet \to \mathscr{G}_\bullet$ un $f_\bullet$-morphisme entre faisceaux abéliens $\mathscr{F}_\bullet$ sur $\mathrm{Tot}\, X_\bullet$ et $\mathscr{G}_\bullet$ sur $\mathrm{Tot}\, Y_\bullet$, c'est-à-dire un morphisme $f_\bullet^\star \mathscr{F}_\bullet \to \mathscr{G}_\bullet$, objet du topos flèche $\mathrm{Fl}(\mathrm{Tot}\, f_\bullet)$. Les coproduits et les flèches du paragraphe précédent, calculés dans la catégorie des paires $(X, \mathscr{F})$ — cf. [Deligne 1974, 6.3.1.b], en remplaçant « *espace topologique* » par « *topos* »[9] —, permettent de définir un faisceau *abélien* simplicial sur $\mathrm{Tot}\, Cf_\bullet$, cône de $\phi_\bullet$, que nous notons $C\phi_\bullet$. (Notons que l'objet final de cette catégorie de paires est le faisceau nul sur e.)

11.2.2. La cohomologie relative de $\mathrm{Tot}\, X_\bullet$ modulo $\mathrm{Tot}\, Y_\bullet$ est un cas particulier de celle définie, pour tout morphisme $S \to T$ de topos, en [Illusie 1971, III, §4] (voir aussi [Deligne 1980, §4.3.4]). On la note $\mathrm{R}\Gamma(\mathrm{Tot}\, X_\bullet / \mathrm{Tot}\, Y_\bullet, \phi_\bullet)$; ce n'est en général *pas* la cohomologie de $\mathrm{Fl}(\mathrm{Tot}\, f_\bullet)$ à valeurs dans $\phi_\bullet$. (Cette dernière étant isomorphe à $\mathrm{R}\Gamma(\mathrm{Tot}\, X_\bullet, \mathscr{F}_\bullet)$ d'après [Illusie 1971, III.4.2].) Implicite en [Deligne

9. Voir aussi [SGA 4_2 1972, $\mathrm{V}^{\mathrm{bis}}$.4.3.0].

1974, §6.3] est la formule suivante :

$$\mathrm{R}\Gamma(\mathrm{Tot}\, X_\bullet/\mathrm{Tot}\, Y_\bullet, \phi_\bullet) = \mathrm{R}\Gamma(\mathrm{Tot}\, Cf_\bullet, C\phi_\bullet). \qquad (\star)$$

En degré cohomologique nul, cette formule résulte immédiatement de la description explicite de d_0 et d_1, et du fait que le terme de gauche est $\mathrm{Ker}(\mathrm{H}^0(\mathrm{Tot}\, X_\bullet, \mathscr{F}_\bullet) \to \mathrm{H}^0(\mathrm{Tot}\, Y_\bullet, \mathscr{G}_\bullet))$. (On pourra aussi comparer à [Anderson 1987, §1], où le cas des *ensembles* simpliciaux et des coefficients constants est considéré.)

11.2.3. Justifions brièvement ($\star$). Notons $\mathscr{R}$ le topos $\mathrm{Fl}(\mathrm{Tot}\, f_\bullet)$ et $\mathscr{C}$ le topos $\mathrm{Tot}\, Cf_\bullet$. Il n'y a pas de morphisme naturel $\mathscr{C} \to \mathscr{R}$ — comme on le voit par exemple en considérant l'unique endomorphisme du topos simplicial vide — mais un morphisme $a : \mathscr{C}^\times \to \mathscr{R}$, où $\mathscr{C}^\times$ est le *sous-topos ouvert* de $\mathscr{C}$, défini par la condition : $i^\star = \varnothing$, où $i : \mathrm{Fl}(e_\bullet) \to \mathscr{C}$ est le morphisme évident. Le morphisme image inverse $a^\star$ est la variante ensembliste du cône d'un morphisme de faisceau abélien considérée en 11.2.1 : sur chaque $Y_{-1} = e$, on considère le faisceau initial (= vide). Notant $j : \mathscr{C}^\times \hookrightarrow \mathscr{C}$, on vérifie sans peine l'égalité $C\phi_\bullet = j_! a^\star \phi_\bullet$ pour tout faisceau abélien sur $\mathscr{R}$. La formule ($\star$) résulte alors, par dérivation et exactitude de $j_! a^\star$, de la formule en degré cohomologique nul.

11.2.4. Soient $f : Y \to X$ un morphisme de k-schémas algébriques et $f_\bullet : Y_\bullet \to X_\bullet$ le morphisme induit entre les schémas simpliciaux constants. Il résulte de ce qui précède et de 11.1 que l'on peut calculer le groupe de cohomologie étale $\mathrm{H}^i(X/Y, \Lambda)$: c'est $\mathrm{H}^i(Cf_\bullet, C\Lambda_\bullet)$. Ceci s'applique en particulier au calcul de la cohomologie à support compact : si X est *propre* sur k, la cohomologie de X/F — où F est un fermé de X — est la cohomologie à support compact de $U = X - F$:

$$\mathrm{H}^i_c(U, \Lambda) = \mathrm{H}^i(X/F, \Lambda).$$

11.2.5. Esquissons une autre approche du calcul de la cohomologie de X relative à un fermé F. Notons $Z = X \amalg_F X$ la somme amalgamée (pincement) de deux copies de X le long de F ; si $X = \mathrm{Spec}(A)$ et $F = \mathrm{Spec}(A/I)$, le schéma Z est le spectre du sous-anneau $B = \{(a_1, a_2) \in A^2 : a_1 \equiv a_2 \bmod I\}$ de A^2. Voir [Ferrand 2003, §5 et §7, notamment le théorème 7.1] pour une discussion de l'existence de coproduits sous des hypothèses bien plus générales et 16.4 pour une approche effective.

Notons i_1 et i_2 les deux immersions fermées canoniques de X dans Z, et i l'immersion fermée de F dans Z. Considérons les morphismes d'adjonctions $\rho_\alpha : i_{\alpha\star}\Lambda \to i_\star\Lambda$ (pour $\alpha \in \{1, 2\}$) et δ le morphisme « différence » $(i_\star\Lambda)^2 \to i_\star\Lambda$, $(a_1, a_2) \mapsto a_1 - a_2$. Le complexe concentré en degrés $[0, 1]$

$$[i_{1\star}\Lambda \oplus i_{2\star}\Lambda \xrightarrow{\delta\circ(\rho_1,\rho_2)} i_\star\Lambda]$$

calcule la cohomologie $\mathrm{R}\Gamma(Z, \Lambda)$ de Z (« Mayer–Vietoris »). Or, il est *isomorphe*

au complexe

$$[i_{1\star}\Lambda \oplus i_{2\star}\Lambda \xrightarrow{0\oplus\rho_2} i_\star\Lambda]$$

dont la cohomologie est la somme directe $\mathrm{R}\Gamma(X, \Lambda) \oplus \mathrm{R}\Gamma(X/F, \Lambda)$. La cohomologie de X/F se déduit donc fonctoriellement de la cohomologie (usuelle) de X et de celle de $Z = X \amalg_F X$.

(Notons que la rétraction $Z = X \amalg_F X \to X = X \amalg_X X$ des deux inclusions $X \rightrightarrows Z$ induit la décomposition en somme directe ci-dessus.)

11.3. *Structure d'algèbre graduée.*

11.3.1. Soient X et Y deux k-schémas de type fini, Λ comme au début de la section 11 et i, j deux entiers. Comme expliqué en 8.3, on peut notamment construire deux hyperrecouvrements (étales) $X_\bullet \to X$ et $Y_\bullet \to Y$ tels que les flèches $\check{\mathrm{H}}^i(X_\bullet, \Lambda) \to \mathrm{H}^i(X, \Lambda)$ et $\check{\mathrm{H}}^j(Y_\bullet, \Lambda) \to \mathrm{H}^j(Y, \Lambda)$ soient *surjectives*. Utilisant la formule de Künneth triviale $\pi_0(X_\bullet \times_k Y_\bullet) = \pi_0(X_\bullet) \times \pi_0(Y_\bullet)$ et l'existence d'un homotopisme d'Eilenberg–Zilber *explicite* [Mac Lane 1963, VIII, théorèmes 8.1 et 8.8]

$$\mathsf{Hom}(\pi_0(X_\bullet), \Lambda) \otimes \mathsf{Hom}(\pi_0(Y_\bullet), \Lambda) \to \mathsf{Hom}(\pi_0(X_\bullet \times_k Y_\bullet), \Lambda),$$

on en déduit un morphisme

$$\check{\mathrm{H}}^i(X_\bullet, \Lambda) \otimes \check{\mathrm{H}}^j(Y_\bullet, \Lambda) \to \check{\mathrm{H}}^{i+j}(X_\bullet \times_k Y_\bullet, \Lambda)$$

relevant le morphisme de Künneth $\mathrm{H}^i(X, \Lambda) \otimes \mathrm{H}^j(Y, \Lambda) \to \mathrm{H}^{i+j}(X \times_k Y, \Lambda)$ ([Milne 1980, V.1.19] ; comparer avec [Deligne 1974, 8.1.25]). Ce dernier est donc calculable compte tenu de ce qui précède. (On utilise le fait que la flèche naturelle $\check{\mathrm{H}}^{i+j}(X_\bullet \times_k Y_\bullet, \Lambda) \to \mathrm{H}^{i+j}(X \times_k Y, \Lambda)$ l'est.)

11.3.2. Lorsque $X = Y$, on en déduit la structure de Λ-algèbre graduée commutative sur $\mathrm{H}^*(X, \Lambda)$ par composition avec la flèche de fonctorialité $\mathrm{H}^*(X \times_k X, \Lambda) \to \mathrm{H}^*(X, \Lambda)$ induite par la diagonale $X \to X \times_k X$: on peut donc calculer le produit

$$\mathrm{H}^*(X, \Lambda) \otimes \mathrm{H}^*(X, \Lambda) \to \mathrm{H}^*(X, \Lambda), \quad c_1 \otimes c_2 \mapsto c_1 \smile c_2.$$

11.3.3. Le résultat précédent a une application immédiate aux cycles algébriques. Supposons dorénavant X propre, lisse, connexe de dimension d_X, et fixons un isomorphisme $t_X : \mathrm{H}^{2d_X}(X, \Lambda) \xrightarrow{\sim} \Lambda$. Par la dualité de Poincaré, toute forme linéaire $\phi : \mathrm{H}^i(X, \Lambda) \to \Lambda$ est de la forme $b \mapsto t_X(a_\phi \smile b)$ pour une unique classe $a_\phi \in \mathrm{H}^{2d_X - i}(X, \Lambda)$, que l'on peut calculer. En particulier, tout morphisme $Z \to X$ de source une variété propre lisse connexe de dimension d_Z induit une classe $c_Z \in \mathrm{H}^{2(d_X - d_Z)}(X, \Lambda)$, correspondant à la forme linéaire composée $\mathrm{H}^{2d_Z}(X, \Lambda) \to \mathrm{H}^{2d_Z}(Z, \Lambda) \xrightarrow{\sim} \Lambda$, où le dernier morphisme est un morphisme trace pour Z.

La classe de cycle c_Z est ainsi définie à multiplication par un élément de $\Lambda^\times$ près (lié au choix arbitraire de traces pour X et Z), ambiguïté que l'on devrait pouvoir lever. Ceci nous permet cependant de répondre à la question : la classe d'un cycle algébrique lisse de X est-elle triviale ?

11.4. ***Images directes.*** On montre que pour tout morphisme $f : X \to S$ entre k-schémas algébriques, tout faisceau constructible $\mathscr{F}$ de Λ-modules sur X et tout entier i, on peut calculer le faisceau $\mathrm{R}^i f_\star \mathscr{F}$, fonctoriellement en $\mathscr{F}$.

11.4.1. Il conviendrait de donner une description explicite de la catégorie des faisceaux constructibles sur un schéma (explicite) X et de vérifier que quelques opérations usuelles (noyau, conoyau, etc.) sont bien calculables. Signalons simplement que différentes approches sont possibles : stratifications et flèches de recollement (cf. [SGA 4_1 1972, IV.9.3]), description des générateurs ou cogénérateurs usuels [SGA 4_3 1973, IX 2.9(ii) et 2.14(ii)], espaces algébriques ([Artin 1973, chapitre VII], ou [Milne 1980, chapitre V, §1]). Cette dernière est probablement la plus économique.

11.4.2. *Effaçabilité et dévissages.* Soient S un schéma nœthérien et $f : X \to S$ un morphisme de type fini. D'après une variante de [SGA $4\frac{1}{2}$ 1977, Arcata, IV.3.5], les foncteurs $\mathrm{R}^i f_\star$ pour $i > 0$ sont *effaçables* dans la catégorie des faisceaux constructibles sur X : pour chaque faisceau (abélien) constructible $\mathscr{F}$ sur X, il existe un plongement de $\mathscr{F}$ dans un faisceau *constructible* $\widetilde{\mathscr{F}}$ tel que le morphisme $\mathrm{R}^i f_\star \mathscr{F} \to \mathrm{R}^i f_\star \widetilde{\mathscr{F}}$ soit nul. De plus, il est formel de vérifier que tout morphisme $\mathscr{F}_1 \to \mathscr{F}_2$ de faisceaux constructibles s'insère dans un diagramme

$$\begin{array}{ccc} \mathscr{F}_1 & \longrightarrow & \mathscr{F}_2 \\ \downarrow & & \downarrow \\ \widetilde{\mathscr{F}}_1 & \longrightarrow & \widetilde{\mathscr{F}}_2 \end{array}$$

où $\widetilde{\mathscr{F}}_1$ et $\widetilde{\mathscr{F}}_2$ effacent respectivement $\mathrm{R}^i f_\star \mathscr{F}_1$ et $\mathrm{R}^i f_\star \mathscr{F}_2$.

Fixons un entier $n > 1$ et supposons que l'on sache calculer, fonctoriellement en $\mathscr{F}$, les $\mathrm{R}^i f_\star \mathscr{F}$ pour chaque entier $i < n$, et chaque faisceau constructible $\mathscr{F}$ de Λ-modules sur X. Considérons un faisceau constructible $\mathscr{F}$ sur X et $\mathscr{F} \hookrightarrow \widetilde{\mathscr{F}}$ un monomorphisme effaçant $\mathrm{R}^n f_\star \mathscr{F}$. Notant $\mathscr{G}$ le faisceau quotient $\widetilde{\mathscr{F}}/\mathscr{F}$, on a la suite exacte $\mathrm{R}^{n-1} f_\star \widetilde{\mathscr{F}} \to \mathrm{R}^{n-1} f_\star \mathscr{G} \to \mathrm{R}^n f_\star \mathscr{F} \to 0$. La calculabilité (fonctorielle) de $\mathrm{R}^n f_\star \mathscr{F}$ se ramène donc à la détermination explicite d'un monomorphisme $\mathscr{F} \hookrightarrow \widetilde{\mathscr{F}}$ comme ci-dessus. La possibilité de plonger tout Λ-faisceau constructible dans l'image directe par un morphisme fini d'un faisceau constant sur chaque composante connexe nous ramène au problème suivant : trouver un morphisme fini surjectif $\pi : X' \to X$ tel que la flèche de fonctorialité $\mathrm{R}^n f_\star \Lambda \to \mathrm{R}^n f'_\star \Lambda$ (déduite de l'unité de l'adjonction $\pi^\star \dashv \pi_\star$) soit nulle, où $f' = f \circ \pi'$.

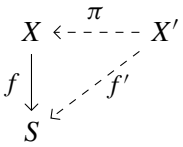
11.4.3. *Cas d'un morphisme propre.* (Par la suite, S est de type fini sur k algébriquement clos.) Quitte à énumérer les morphismes π (pour faire une recherche non bornée : cf. 12.8), on se ramène au problème de *tester* la nullité d'une flèche comme ci-dessus. Or, on peut calculer une stratification explicite $S = \bigcup_\iota S_\iota$ (réunion disjointe) telle que les faisceaux $\mathrm{R}^n f_\star \Lambda$ et $\mathrm{R}^n f'_\star \Lambda$ ci-dessus soient lisses sur les S_ι ; c'est un corollaire immédiat des démonstrations « géométriques » de la constructibilité des images directes. (Voir [Orgogozo 2013] pour des variantes sur ce thème.) Tester si $\mathrm{R}^n f_\star \Lambda \to \mathrm{R}^n f'_\star \Lambda$ est nulle revient donc à tester si sa fibre l'est en tout point géométrique $\bar{\eta}$ localisé en un point maximal η des S_ι. Lorsque f est *propre* (ou simplement cohomologiquement propre pour les faisceaux de torsion), cette fibre n'est autre que la flèche de fonctorialité

$$\mathrm{H}^n(X_{\bar{\eta}}, \Lambda) \to \mathrm{H}^n(X'_{\bar{\eta}}, \Lambda).$$

D'après le théorème 0.1, on peut décider si une telle flèche est nulle ou non ; la conclusion résulte alors du fait que les points maximaux η sont en nombre fini.

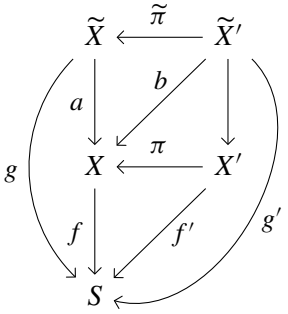
Ceci démontre le théorème 0.9 dans le cas particulier où f est *propre*, ou bien lorsque $S = \mathrm{Spec}(k)$.

11.4.4. Notons que l'on peut améliorer légèrement le résultat d'effaçabilité précédent : donné $f : X \to S$ propre (et Λ), on peut calculer $X' \to X$ fini surjectif



tel que le morphisme $\mathrm{R}^{\geq 1} f_\star \Lambda \to \mathrm{R}^{\geq 1} f'_\star \Lambda$ soit nul, où l'on note $\mathrm{R}^{\geq 1} = \tau_{\geq 1}\mathrm{R}$ pour simplifier. Il suffit d'itérer suffisamment la construction (cf. par exemple [Bhatt 2012, §2]).

Déduisons de cette observation que, si f n'est plus nécessairement propre (mais toujours de type fini), l'existence d'un morphisme *fini* surjectif $\pi : X' \to X$ tel que les $\mathrm{R}^i f_\star \Lambda \to \mathrm{R}^i f'_\star \Lambda$ soient nuls pour $i > 0$ se déduit de l'existence d'une *altération a* effaçant la cohomologie. Supposons en effet que l'on ait un diagramme commutatif



où :

- a est une altération effaçant la cohomologie de f : la flèche de fonctorialité $\mathrm{R}^i f_\star\Lambda \to \mathrm{R}^i g_\star\Lambda$ est nulle pour chaque $i > 0$;
- $\widetilde{\pi}$ est un morphisme fini surjectif effaçant la cohomologie du morphisme *propre* a : la flèche de fonctorialité $\mathrm{R}^{\geq 1}a_\star\Lambda \to \mathrm{R}^{\geq 1}b_\star\Lambda$ est nulle ;
- $\widetilde{X}' \to X' \to X$ est la *factorisation de Stein* de b ; en particulier, π est *fini* surjectif.

(D'après ce qui précède, donné a, on sait *calculer* un tel diagramme.) Il résulte de la seconde hypothèse que l'on a une factorisation diagonale du carré commutatif ci-dessous

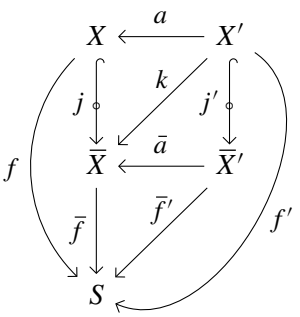
$$\begin{array}{ccc} \Lambda & \longrightarrow & \mathrm{R}^0 b_\star\Lambda = \pi_\star\Lambda \\ \downarrow & \nearrow & \downarrow \\ \mathrm{R}a_\star\Lambda & \longrightarrow & \mathrm{R}b_\star\Lambda \end{array}$$

où l'égalité du coin supérieur droit est conséquence de la troisième hypothèse. Fixons $n > 0$ et appliquons le foncteur $\mathrm{R}^n f_\star$. Le carré précédent devient

$$\begin{array}{ccc} \mathrm{R}^n f_\star\Lambda & \longrightarrow & \mathrm{R}^n f'_\star\Lambda \\ 0 \downarrow & \nearrow & \downarrow \\ \mathrm{R}^n g_\star\Lambda & \longrightarrow & \mathrm{R}^n g'_\star\Lambda \end{array}$$

La nullité de la flèche verticale de gauche correspond à la première hypothèse. La flèche horizontale supérieure est donc nulle. CQFD.

11.4.5. Les observations précédentes et le théorème de résolution des singularités [de Jong 1996, 4.1] ramènent le calcul d'un morphisme fini surjectif effaçant la cohomologie d'un morphisme (non nécessairement propre) $f : X \to S$ au cas particulier où : X est le complémentaire d'un diviseur à croisements normaux stricts D dans un schéma projectif lisse $\overline{X}$ sur k, et où l'on s'autorise à effacer par une *altération* a. Le cas propre étant déjà connu, il suffit de montrer que l'on peut calculer un diagramme commutatif



où $\bar{a}$ est une altération et le carré commutatif ci-dessous

$$\begin{array}{ccc} \mathrm{R}^n \bar{f}_\star \Lambda & \longrightarrow & \mathrm{R}^n \bar{f}'_\star \Lambda \\ \downarrow & \nearrow & \downarrow \\ \mathrm{R}^n f_\star \Lambda & \longrightarrow & \mathrm{R}^n f'_\star \Lambda \end{array}$$

se factorise diagonalement comme indiqué. En effet, le cas propre appliqué au morphisme $\bar{f}'$ permet de construire une altération (et même un morphisme fini surjectif) $\overline{X}'' \to \overline{X}'$ effaçant $\mathrm{R}^n \bar{f}'_\star \Lambda$; la conclusion est alors immédiate.

Comme au paragraphe précédent (11.4.4), il suffit de montrer que l'on peut calculer une altération $\bar{a}$ effaçant $\mathrm{R}^{\geq 1} j_\star \Lambda$, c'est-à-dire telle que le morphisme $\mathrm{R}^{\geq 1} j_\star \Lambda \to \mathrm{R}^{\geq 1} k_\star \Lambda$ soit nul. En effet, on a sous cette hypothèse un diagramme commutatif et une factorisation

$$\begin{array}{ccccc} \Lambda & \longrightarrow & k_\star \Lambda = \bar{a}_\star \Lambda & \longrightarrow & \mathrm{R}\bar{a}_\star \Lambda \\ \downarrow & \nearrow & & & \downarrow \\ \mathrm{R} j_\star \Lambda & & \longrightarrow & & \mathrm{R} k_\star \Lambda \end{array}$$

induisant après application du foncteur $\mathrm{R}^n \bar{f}_\star$ le diagramme commutatif

$$\begin{array}{ccccc} \mathrm{R}^n \bar{f}_\star \Lambda & \longrightarrow & \mathrm{R}^n \bar{f}_\star (\bar{a}_\star \Lambda) & \longrightarrow & \mathrm{R}^n \bar{f}_\star (\mathrm{R}\bar{a}_\star \Lambda) = \mathrm{R}^n \bar{f}'_\star \Lambda \\ \downarrow & \nearrow & & & \downarrow \\ \mathrm{R}^n f_\star \Lambda & & \longrightarrow & & \mathrm{R}^n f'_\star \Lambda \end{array}$$

désiré. Pour effacer $\mathrm{R}^{\geq 1} j_\star \Lambda$, il suffit — par itération, cf. 11.4.4, premier paragraphe — de savoir effacer chaque $\mathrm{R}^i j_\star \Lambda$ pour $i > 0$ (en nombre fini). Pour tout entier $N > 0$, il existe un morphisme fini surjectif $\overline{X}' \to \overline{X}$ tel que, Zariski-localement sur $\overline{X}$, le tiré en arrière du diviseur $D = \overline{X} - X$ soit une puissance N-ième dans $\overline{X}'$. En effet, il est possible de trouver, Zariski-localement, une extension finie du corps des fractions de $\overline{X}$ telle que la clôture intégrale de $\overline{X}$ convienne (cf. [Deligne 1980, §1.7.9]) ; il suffit alors de considérer la clôture intégrale de $\overline{X}$ dans une extension composée. Vérifions que $\overline{X}' \to \overline{X}$ efface les $\mathrm{R}^i j_\star \Lambda$. Soit d un point géométrique de D, $U = X \times_{\overline{X}} \overline{X}_{(d)}$ le complémentaire de $D_{(d)}$ dans le schéma régulier strictement local $\overline{X}_{(d)}$ et V l'ouvert correspondant dans $\overline{X}'_{(d)} = \overline{X}_{(d)} \times_{\overline{X}} \overline{X}'$. La fibre en d de $\mathrm{R}^i j_\star \Lambda \to \mathrm{R}^i k_\star \Lambda$ s'identifie à l'application de fonctorialité $\mathrm{H}^i(U, \Lambda) \to \mathrm{H}^i(V, \Lambda)$. Cette dernière est nulle par construction et pureté lorsque $N \cdot \Lambda = \{0\}$. Notons que l'on peut bien itérer cette construction car, quitte à altérer (ce qui est licite comme on l'a vu), on peut supposer que $\overline{X}'$ est régulier et que l'ouvert X' image inverse de X est le complémentaire d'un diviseur à croisements normaux stricts. Ceci achève la démonstration du théorème 0.9.

11.5. ***Questions.*** Nous terminons en suggérant quelques questions, de difficulté variée, qui nous paraissent être un prolongement naturel de ce travail, et que nous n'avons pas eu la patience ou le courage d'aborder.

11.5.1. Calculer $\mathrm{H}^i(X, \mathcal{K})$, voire $\mathrm{R}\Gamma(X, \mathcal{K})$, pour $\mathcal{K}$ un complexe borné constructible de Λ-modules. Variante relative : étendre le théorème 0.9 au calcul de $\mathrm{R}f_\star\mathcal{K}$.

11.5.2. (Théorème de changement de base propre effectif.) Donnés $X \to S$ un morphisme *propre* et $s \in S$, construire un voisinage étale U de s tel que tout élément de $\mathrm{H}^*(X_s, \Lambda)$ se relève à X_U.

11.5.3. Calculer les cycles proches $\Psi_f(\Lambda)$ d'un morphisme $f : X \to S = \mathrm{Spec}(k[t]_{(t)})$.

11.5.4. Calculer les nombres de Betti ℓ-adiques dans le cas non nécessairement propre et lisse. [10]

11.6. ***Primitive récursivité, ou existence de bornes algorithmiques.*** Comme nous l'avons signalé en 0.10 (voir aussi 12.8 pour une explication plus détaillée), la notion de « calculabilité » que nous avons utilisée est la notion classique de calculabilité au sens de Church–Turing, qui permet notamment d'effectuer des « recherches non bornées », c'est-à-dire énumérer des objets (toujours ramenables aux entiers naturels) jusqu'à en trouver un, si on sait qu'il existe, vérifiant une propriété algorithmiquement testable. L'utilisation de ce procédé, sans aucune borne *a priori* sur la longueur des recherches en question, fait perdre tout contrôle sur la complexité de nos algorithmes.

Il nous semble cependant plausible que de telles bornes puissent être trouvées. Plus exactement, nous pensons que les fonctions calculées algorithmiquement dans le présent article sont au moins *primitivement récursives*, c'est-à-dire calculables par un algorithme dont toutes les boucles peuvent être bornées *a priori* au sens où on doit avoir calculé un majorant sur le nombre d'exécutions de toute boucle avant d'entrer dans celle-ci : cf. [Odifreddi 1989, définition I.1.6 et proposition I.5.8]. Ceci interdit l'utilisation des « recherches non bornées » et correspond à la façon la plus naturelle de les interdire. [11] (Pour rendre plus parlante la notion de fonction primitivement récursive, on peut décrire un langage de programmation qui ne permet

10. Ce problème nous semble actuellement hors de portée.

11. Il n'est malheureusement pas possible de dire que toute fonction intuitivement calculable sans recherche non bornée est primitivement récursive, car il existe différentes sortes de récursion garantissant la terminaison qui ne peuvent pas s'exprimer sous forme primitivement récursive : la fonction d'Ackermann en est un exemple ; on pourra consulter [Odifreddi 1999, VIII.9, notamment les définitions VIII.9.1 et VIII.9.3] pour des notions plus générales. De toute manière, l'argument général du problème de l'arrêt (i.e., un principe diagonal) ne permet pas qu'on puisse formaliser la notion intuitive de « fonction calculable sans recherche non bornée » (donc en particulier, terminant toujours).

pas d'appels récursifs de fonctions et dans lequel toutes les boucles sont des boucles bornées par la valeur d'une variable à l'entrée de la boucle : tel est le langage « BlooP » décrit dans [Hofstadter 1979, chapitre XIII], qu'on pourra consulter pour une description agréable à lire de la différence entre fonctions primitivement récursives et générales récursives, ces dernières y étant définies par le langage « FlooP ».) Par ailleurs, les fonctions primitivement récursives sont une « classe de complexité » car une fonction primitivement récursive est une fonction qui peut être calculée algorithmiquement avec une complexité (en espace ou en temps) elle-même donnée par une fonction primitivement récursive : cf. [Odifreddi 1999, VIII.8.8].

Les fonctions que nous calculons sont peut-être même « élémentaires » (ou « élémentairement récursives ») au sens de Kalmár, c'est-à-dire de temps d'exécution borné par une tour d'exponentielles, cf. [ibid., définition VIII.7.1] ; de nouveau, il revient au même de dire qu'elle est calculable algorithmiquement avec une complexité elle-même élémentaire (cf. [ibid., théorème VIII.7.6]).

Cette supposition est motivée, entre autres, par un slogan proposé par certains logiciens, cf. [Friedman 1999, conjecture 1] ou [Avigad 2003, « grand conjecture » p. 258], selon lequel tout théorème mathématique « ordinaire », [12] qui peut s'énoncer dans le langage de l'arithmétique, est en fait prouvable dans des systèmes formels faibles de l'arithmétique ; or, dès que ces systèmes prouvent qu'un algorithme termine, ils prouvent en fait qu'il appartient à une classe de complexité bien comprise. On pense notamment au système PRA, « Primitive Recursive Arithmetic » (défini par exemple en [Simpson 2009, IX, §3]) et qui démontre la terminaison précisément des fonctions primitivement récursives (cf. [Hájek et Pudlák 1998, corollaire IV.3.7]), et au système EA, « Elementary [function] Arithmetic », défini en [Avigad 2003, §2], et qui démontre la terminaison des fonctions Kalmár-élémentaires (cf. [Avigad 2003, théorème 2.2 et remarque qui suit]). Si notre théorème (affirmant qu'un certain algorithme termine en calculant la cohomologie étale) est démontrable dans ces systèmes faibles, c'est que l'algorithme est primitivement récursif voire Kalmár-élémentaire.

Pour s'en convaincre, il faudrait chercher à reprendre tous les résultats d'existence utilisés ici pour faire apparaître une borne explicite sur les objets construits (de manière à placer les algorithmes dans une des hiérarchies décrites dans [Odifreddi 1999, chapitre VIII]). Nous n'avons pas eu le courage de mener cet exercice, mais nous avons au moins cherché à limiter les appels aux « recherches non bornées » (notamment en 6.6, ou encore 15.5 pour le calcul de la normalisation). Il reste que nous n'avons pas réussi à l'éviter dans la construction d'un hyperrecouvrement

12. Il va de soi que l'affirmation est fausse sans le qualificatif « ordinaire », et que celui-ci ne peut pas être défini rigoureusement. Voir [Smoryński 1985] (ainsi que les autres articles de cet auteur dans le même recueil [Harrington et al. 1985]) pour un aperçu généraliste de ces questions, ou bien l'introduction de [Friedman 2011] pour une présentation plus systématique.

d'un schéma X par des polycourbes ℓ-élémentaires (proposition 1.4.9 et suite) : s'il est probable que, dans le cas où X est lisse on puisse sans trop de mal construire explicitement les polycourbes en question en suivant la démonstration de [SGA 4_3 1973, XI, §2–3], le cas général nécessiterait aussi de revoir les résultats de [de Jong 1996] sous un angle algorithmique.

II. Algèbre commutative et géométrie algébrique effectives

L'objet de cette partie est de vérifier la calculabilité des propriétés et opérations algébriques et géométriques utilisées dans la première partie. Certains des résultats rassemblés ici, bien que connus, nous ont semblé difficiles à trouver dans la littérature, ou bien formulés dans un langage différent du nôtre, si bien que nous avons préféré, pour la commodité du lecteur, redémontrer certains faits, ou rappeler la manière dont ils se démontrent. (Ceci devrait en outre faciliter le travail de vérification du lecteur qui a commencé sa lecture par le texte [Madore et Orgogozo 2014] et qui souhaite vérifier que tout ce que nous utilisons est calculable dans le modèle de calcul qui y est exposé.)

12. Corps et extensions de corps

Définition 12.1. On appelle *corps calculable* la donnée d'une partie calculable (= récursive) $\mathfrak{K}$ de $\mathbb{N}$, d'une relation d'équivalence calculable $\equiv$ sur $\mathfrak{K}$, d'éléments $0_\mathfrak{K}$ et $1_\mathfrak{K}$ de $\mathfrak{K}$, et de fonctions calculables $(+)_\mathfrak{K}\colon \mathfrak{K}\times\mathfrak{K}\to\mathfrak{K}$ et $(-)_\mathfrak{K}\colon \mathfrak{K}\to\mathfrak{K}$ et $(\times)_\mathfrak{K}\colon \mathfrak{K}\times\mathfrak{K}\to\mathfrak{K}$ et $({}^{-1})_\mathfrak{K}\colon \{z\in\mathfrak{K}\colon z\not\equiv 0_\mathfrak{K}\}\to\mathfrak{K}$, telles que ces opérations passent au quotient par $\equiv$ et définissent sur $\mathfrak{K}/\equiv$ une structure de corps. On notera généralement $K=(\mathfrak{K}/\equiv)$ et on dira abusivement que K « est » un corps calculable pour sous-entendre qu'on s'est donné une structure de corps calculable dont K est le quotient ; s'il faut désambiguïser, on pourra dire que $\mathfrak{K}$ est l'ensemble d'*étiquettes* [13] qui servent à décrire les éléments de K.

Une *extension calculable* $\mathfrak{K}\to\mathfrak{L}$ de corps calculables est la donnée d'une fonction calculable $f\colon\mathfrak{K}\to\mathfrak{L}$ telle que $x\equiv_\mathfrak{K} y$ implique $f(x)\equiv_\mathfrak{L} f(y)$ et que l'application $K\to L$ définie par passage au quotient soit une extension (un morphisme) de corps. (On dira aussi que K est un sous-corps calculable de L.) Si de plus K est une partie récursive de L, c'est-à-dire s'il existe une fonction calculable qui, donné $y\in\mathfrak{L}$, décide s'il existe x tel que $f(x)\equiv_\mathfrak{L} y$ (et, cf. 12.8, on peut alors supposer [14] qu'elle calcule ce x), alors on dit que K est un sous-corps calculable *reconnaissable* de L (ou que L est une extension calculable reconnaissable de K).

13. Une autre terminologie possible serait d'appeler $\mathfrak{K}$ un « corps calculé » et K un « corps calculable ».

14. Ce serait la bonne définition à prendre si on voulait remplacer la notion de calculabilité par celle de fonction primitivement récursive.

On dit qu'un corps calculable K admet un *algorithme de factorisation* lorsqu'il existe un algorithme qui, donné un polynôme à coefficients dans K en une variable, calcule sa factorisation [15] en polynômes irréductibles.

Remarques 12.2. **(0)** Nous renvoyons notamment à [Fröhlich et Shepherdson 1956] et [Stoltenberg-Hansen et Tucker 1999] pour des généralités sur les corps calculables. Il existe différentes variantes autour de la définition, essentiellement sans importance dans le cadre dans lequel nous nous plaçons (par exemple, quitte à n'utiliser que le plus petit élément — pour l'ordre de $\mathfrak{K}$ en tant que partie de $\mathbb{N}$ — de chaque classe d'équivalence, on peut omettre la relation d'équivalence et demander directement que $\mathfrak{K}$ soit une partie récursive de $\mathbb{N}$ munie d'opérations qui en font un corps) ; celle proposée ci-dessus (équivalente à celle de [Stoltenberg-Hansen et Tucker 1999, 2.1.5]), nous semble la plus naturelle et celle qui se transpose le plus agréablement, par exemple, au cas où on remplacerait les fonctions récursives par des fonctions seulement primitivement récursives (cf. [Jacobsson et Stoltenberg-Hansen 1985, §1]).

Il est notamment utile de rappeler les faits suivants.

(1) Si K est un corps calculable, alors $K(T)$ (où T est une indéterminée), ainsi que $K[X]/(f)$ (où $f \in K[X]$ est un polynôme irréductible) sont des extensions calculables et reconnaissables de K. (C'est-à-dire qu'il y a une façon standard de faire de $K(T)$ ou de $K[X]/(f)$ des corps calculables et de l'extension une extension calculable reconnaissable, et c'est de cette structure qu'on parlera toujours ; par exemple, un élément de $K[X]/(f)$, si $d = \deg f$, est décrit comme un d-uplet $(c_0, \ldots, c_{d-1})$ d'éléments de K, ou plus précisément de l'ensemble $\mathfrak{K}$ d'étiquettes des éléments de K, représentant la classe modulo f du polynôme $\sum c_i X^i$, l'addition se faisant terme à terme et la multiplication se faisant en terminant par le reste de la division euclidienne par f, laquelle est évidemment calculable.)

(2) Si K est un corps calculable, alors « la » clôture algébrique de K est une extension calculable de K ([Rabin 1960, théorème 7] ; cf. [Stoltenberg-Hansen et Tucker 1999, corollaire 3.1.11]), mais non reconnaissable en général (cf. le point suivant). **(3)** L'existence d'un algorithme de factorisation pour un corps calculable K équivaut à l'existence d'un algorithme qui décide si un polynôme admet une racine, ou encore à l'existence d'un algorithme qui reconnaît si un élément de la clôture algébrique de K (calculable comme on vient de le dire en (2)) appartient à K ([Rabin 1960, théorème 8] : cf. aussi [Stoltenberg-Hansen et Tucker 1999, proposition 3.2.2] et [Miller 2010, théorème 2.5(2)]). Bien entendu, **(4)** tout corps calculable algébriquement clos admet un algorithme de factorisation.

15. Plus exactement : donné une suite d'étiquettes représentant les coefficients d'un polynôme (en une variable) à factoriser, renvoie des suites d'étiquettes représentant les coefficients de ses facteurs irréductibles.

De plus, **(5)** si K est un corps calculable admettant un algorithme de factorisation, alors c'est aussi le cas de $K(T)$ (où T est une indéterminée) et de $K[X]/(f)$ si $f \in K[X]$ est un polynôme irréductible *séparable* (cf. [Stoltenberg-Hansen et Tucker 1999, théorèmes 3.2.3 et 3.2.4] ; et **(6)** la nécessité de l'hypothèse « séparable » pour le point précédent est montrée dans [Fröhlich et Shepherdson 1956, théorème 7.12]).

(7) Si K est un corps *parfait* calculable admettant un algorithme de factorisation (notamment si K est un corps calculable algébriquement clos), et si $K(x_1, \dots, x_n)$ est une extension de type fini de K, puisqu'on peut extraire de $x_1, \dots, x_n$ une base de transcendance séparante [Matsumura 1989, remarque précédant le théorème 26.3], le point (5) montre que le corps calculable $K(x_1, \dots, x_n)$ admet lui aussi un algorithme de factorisation (cf. [Stoltenberg-Hansen et Tucker 1999, 3.2.6] ; ou bien [Lecerf 2013, théorème 4 de l'introduction] lorsque K est un corps premier).

En lien avec ce fait, rappelons que si un corps calculable admet un algorithme de factorisation (des polynômes en une variable), il en admet automatiquement un pour les polynômes en un nombre fini quelconque de variables : [Fried et Jarden 2008, lemme 19.1.3].

12.3. On rappelle (voir notamment [Bourbaki 1981, V, §13] ou [ÉGA IV_1 1964, **0**, §21] ou encore [Fried et Jarden 2008, §2.7]) qu'une *p-base* (resp. une famille *p-libre*) finie d'un corps K de caractéristique $p > 0$ (sous-entendu : sur K^p) est une famille $b_1, \dots, b_r \in K$ tels que les produits $b_1^{i_1} \cdots b_r^{i_r}$ pour $0 \leq i_u < p$ forment une base (resp. une famille libre) du K^p-espace vectoriel K ; il existe une p-base finie de K si et seulement si K est de degré fini sur K^p, auquel cas ce degré vaut p^r où r est le cardinal de la p-base : on appelle r le *p-rang* ou *exposant d'imperfection* de K (sous-entendu : sur K^p).

Proposition 12.4. *Soit K un corps calculable de caractéristique $p > 0$ et de p-rang fini. Il revient au même de se donner* :

(i) *le p-rang r de K et un algorithme décidant si des éléments $a_1, \dots, a_s$ de K sont linéairement indépendants sur K^p* ;

(ii) *le p-rang r de K et un algorithme décidant si des éléments $a_1, \dots, a_s$ de K sont p-libres* ;

(iii) *une p-base $b_1, \dots, b_r$ de K* ;

(iv) *une p-base $b_1, \dots, b_r$ de K et un algorithme exprimant un élément x de K sous la forme $\sum_{\underline{i}} \xi_{\underline{i}}^p b_1^{i_1} \cdots b_r^{i_r}$ où $\xi_{\underline{i}} \in K$ pour $\underline{i} = (i_1, \dots, i_r)$ vérifiant $0 \leq i_u < p$ pour tout u.*

« Il revient au même de se donner » signifie qu'on peut exprimer n'importe laquelle de ses données en fonction de n'importe quelle autre de façon algorithmique et uniforme — c'est-à-dire par un algorithme indépendant de K et des autres données.

(On pourra comparer ces équivalences avec [Richman 1981, théorème 1] qui en est l'analogue dans le cadre de l'algèbre constructive.)

On dira qu'on a sur un corps calculable une *p-base finie explicite* en référence à n'importe laquelle de ces données.

Démonstration. Il est évident que connaître (i) permet de connaître (ii) (tester la p-liberté revient, par définition de ce terme, à tester l'indépendance linéaire de certaines puissances). Connaissant (ii), on peut connaître (iii) en énumérant les éléments de K et en ajoutant ceux qui sont p-libres avec les précédents jusqu'à atteindre le p-rang de K. Connaissant (iii) on obtient (iv) en énumérant toutes les écritures possibles de x sur la p-base jusqu'à en obtenir une qui convient. Enfin, connaissant (iv), on a un isomorphisme explicite de K^p-espaces vectoriels entre K et $(K^p)^{\oplus p^r}$ (somme de p^r copies de K^p), ce qui permet donc facilement de tester l'indépendance linéaire d'une famille (il s'agit simplement de calculer des déterminants). □

Comme on l'a souligné en 12.2(5–6), si K est un corps calculable admettant un algorithme de factorisation, ces propriétés valent pour $L := K[X]/(f)$ (avec $f \in K[X]$ irréductible) lorsque f est séparable, mais pas nécessairement dans le cas général. Si on fait l'hypothèse qu'on dispose sur K d'une p-base finie explicite, cette difficulté n'existe plus :

Lemme 12.4.1. *Soit K un corps calculable pour lequel on dispose d'un algorithme de factorisation et d'une p-base finie explicite. Soit $a \in K$ n'appartenant pas à K^p. Alors sur le corps $L := K(\sqrt[p]{a})$ (extension calculable reconnaissable de K comme rappelé en 12.2*(1)*), on dispose d'un algorithme de factorisation et d'une p-base finie explicite.*

Démonstration. Puisque $a \notin K^p$ (autrement dit, le singleton a est p-libre), d'après 12.4(ii), on peut explicitement construire une p-base de K contenant l'élément a (comme dans la démonstration du fait que (ii) permet de trouver (iii), en partant de a), disons $a, b_2, \ldots, b_r$. Alors $a^{1/p}, b_2, \ldots, b_r$ constitue une p-base explicite de L.

Pour montrer que L dispose d'un algorithme de factorisation, d'après [Fröhlich et Shepherdson 1956, 7.3] ou son amélioration citée dans [Stoltenberg-Hansen et Tucker 1999, 3.2.5], il suffit de montrer qu'on peut décider si un élément de L est une puissance p-ième : or d'après 12.4(iv) on sait l'écrire sur la p-base $a^{1/p}, b_2, \ldots, b_r$, et il suffit de vérifier que seul le coefficient devant 1 est non nul dans cette écriture. □

Le résultat suivant a pour objet de convaincre que tous les corps que nous serons amenés à considérer sont calculables avec un algorithme de factorisation :

Proposition 12.5. *Soit K un corps calculable pour lequel on dispose d'un algorithme de factorisation et (si K est de caractéristique $p > 0$) d'une p-base finie explicite. Soit L l'extension de K définie par l'une des opérations suivantes* :

(i) *l'ajout d'un transcendant* : $L = K(T)$ *où T est une indéterminée*,

(ii) *l'ajout d'un élément algébrique* : $L = K[X]/(f)$ *où $f \in K[X]$ est irréductible (non supposé séparable), donné*,

(iii) *le passage à la*[16] *clôture algébrique $L = K^{\mathrm{alg}}$ de K*,

(iv) *le passage à la clôture séparable $L = K^{\mathrm{sép}}$ de K*,

(v) (*dans le cas où K est de caractéristique $p > 0$*) *le passage à la clôture parfaite $L = K^{1/p^\infty}$ de K*,

alors L est une extension calculable reconnaissable de K, et on dispose d'un algorithme de factorisation et d'une p-base finie explicite pour L.

Plus précisément, on va esquisser des algorithmes explicites qui, donnés des algorithmes qui calculent les opérations sur K et la factorisation des polynômes de $K[X]$ et une p-base finie explicite de K, et donnés le cas où on se place, et le polynôme f dans le cas (ii), présentent L comme une extension calculable reconnaissable de K, permettent de factoriser les polynômes de $L[X]$, et fournissent une p-base de L.

(On pourra comparer avec [Mines et Richman 1982, théorème 3.9], analogue de (ii) ci-dessus mais dans le cadre de l'algèbre constructive.)

Démonstration. Traitons chacun des cas séparément.

(i) Le corps $L = K(T)$ est une extension calculable reconnaissable de K comme on l'a rappelé en 12.2(1), et dispose d'un algorithme de factorisation d'après 12.2(5). En ajoutant T à la p-base de K on obtient une p-base de L (cf. [Fried et Jarden 2008, lemme 2.7.2 et sa démonstration]).

Pour le cas (ii), on peut distinguer le cas où f est séparable et celui où il est purement inséparable : en effet, il est algorithmique d'écrire un polynôme irréductible $f \in K[X]$ sous la forme $h(X^{p^e})$ avec h irréductible et séparable, ce qui ramène l'extension $K[X]/(f)$ aux deux extensions $E := K[X]/(h)$ avec h séparable puis $L = E[X]/(X^{p^e} - a)$ avec a la classe de X modulo h. Par ailleurs, pour les extensions purement inséparables, on peut encore se ramener au cas où le polynôme est de la forme $X^p - a$ (quitte à écrire une racine (p^e)-ième comme extractions successives de racines p-ièmes).

16. On conviendra que, s'agissant d'un corps calculable, « la » clôture algébrique désigne celle qui est construite explicitement par l'algorithme de Rabin : cf. 12.2(2) ; et de même « la » clôture séparable désigne la clôture séparable dans cette clôture algébrique.

Dans le cas (ii) avec f séparable, le corps L est une extension calculable reconnaissable de K comme on l'a rappelé en 12.2(1), et dispose d'un algorithme de factorisation d'après 12.2(5). Une p-base de K est encore une p-base de L (cf. [Fried et Jarden 2008, lemme 2.7.3]).

Dans le cas (ii) avec f de la forme $X^p - a$ a été traité en 12.4.1.

(iii) La clôture algébrique L de K est une extension calculable de K comme on l'a rappelé en 12.2(2), et dispose d'un algorithme de factorisation (12.2(4)). La p-base vide convient pour L. De plus, comme K était supposé disposer d'un algorithme de factorisation, on peut reconnaître K dans L d'après 12.2(3).

(iv) La clôture séparable L de K se voit comme un sous-corps de la clôture algébrique : pour reconnaître si un élément de cette dernière appartient à L, il suffit de calculer son polynôme minimal sur K (quitte à énumérer tous les polynômes de $K[X]$ jusqu'à en trouver un qui annule l'élément considéré, [17] cf. 12.8, puis le factoriser) et vérifier s'il est séparable. On dispose d'un algorithme de factorisation puisque, d'après 12.2(3), il suffit pour cela de savoir identifier un élément de L dans la clôture algébrique commune de K et L, et on vient d'expliquer que c'est possible. Enfin, une p-base de K est encore une p-base de L (cf. [Fried et Jarden 2008, lemme 2.7.3]).

(v) Si K est un corps calculable (sans autre hypothèse pour l'instant), alors on peut construire $L = K^{1/p^\infty}$ extension calculable de K explicitement selon sa définition : on définit $\mathfrak{L}$ comme l'ensemble des couples (e, a) où $e \in \mathbb{N}$ et a est un élément de K : ce couple représente alors la racine (p^e)-ième de a dans L, et on peut définir $(e, a) \equiv_{\mathfrak{L}} (e', a')$ (disons pour $e' \geq e$) lorsque $a^{p^{e'-e}} = a'$ dans K, ce qui est bien une relation calculable. Pour ajouter ou multiplier (e, a) et (e', a') (disons pour $e' \geq e$), on remplace (e, a) par $(e', a^{p^{e'-e}})$ et on effectue l'opération entre $a^{p^{e'-e}}$ et a', qui est calculable.

Avec l'hypothèse supplémentaire que K dispose d'un algorithme de factorisation, on peut tester si un élément de K a sa racine p-ième dans K (et le cas échéant la calculer) : on peut donc considérer uniquement les couples $(e, a) \in \mathfrak{L}$ « canoniques », définis comme ceux pour lesquels $a \notin K^p$ si $e > 0$, convertir un couple $(e, a) \in \mathfrak{L}$ quelconque en un couple « canonique », et on voit alors clairement que L est une extension calculable reconnaissable de K (c'est d'ailleurs essentiellement ce qui est fait dans [Steel 2005, §2.1]).

Pour montrer que L dispose d'un algorithme de factorisation, il suffit clairement de montrer qu'on peut factoriser dans L les polynômes f de $K[X]$ (quitte à appliquer l'isomorphisme entre K^{1/p^e} et K pour un e assez grand) : comme K a un algorithme de factorisation, on peut évidemment supposer f irréductible dans $K[X]$, et l'écrire

17. Il va de soi que sur une description réellement explicite de la clôture algébrique on n'aurait pas besoin de faire quelque chose d'aussi absurde !

sous la forme $h(X^{p^e})$ avec $h \in K[X]$ irréductible séparable : ceci se réécrit $(h_1(X))^{p^e}$ avec h_1 le polynôme de $L[X]$ dont les coefficients sont les racines (p^e)-ièmes de ceux de h ; en utilisant de nouveau l'isomorphisme entre K^{1/p^e} et K il est clair que h_1 est irréductible dans $L[X]$, et on a la factorisation voulue. Enfin, la p-base vide convient pour L. □

Remarque 12.6. L'énoncé ci-dessus considère des extensions algébriques du type $L = K[X]/(f)$ avec f irréductible (i.e., (f) maximal dans $K[X]$). Il n'y aura pas de difficulté, dès qu'on saura manipuler les idéaux d'une algèbre de polynômes à plusieurs variables (§13), à y exprimer des extensions du type $L = K[Z_1, \dots, Z_d]/\mathfrak{m}$ avec $\mathfrak{m}$ un idéal maximal de $K[Z_1, \dots, Z_d]$ comme une tour d'extensions monogènes. Il suffit en effet d'utiliser un algorithme d'élimination, cf. [Eisenbud 1995, §15.10.4], pour calculer les intersections $\mathfrak{m} \cap K[Z_1, \dots, Z_i]$, qui définissent autant d'extensions de corps $K_i \subseteq K_{i+1}$ avec $K_i = K[Z_1, \dots, Z_i]/(\mathfrak{m} \cap K[Z_1, \dots, Z_i])$, algébriques engendrées par un seul élément dont on connaît le polynôme minimal, et $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_d = L$.

Plus généralement, si $\mathfrak{p}$ est un idéal premier de $K[Z_1, \dots, Z_d]$, l'extension $L := \mathrm{Frac}(K[Z_1, \dots, Z_d]/\mathfrak{p})$ de K se ramène également explicitement à des extensions comme envisagées ci-dessus : en effet, il suffit de considérer un ensemble maximal E de variables Z_i telles que $\mathfrak{p} \cap K[E] = \{0\}$ (de nouveau calculable par élimination), si bien que $K(E) = \mathrm{Frac}(K[E])$ est une extension transcendante pure de K et que L en est une extension algébrique du type considéré au paragraphe précédent (on peut aussi invoquer le lemme de normalisation de Noether [Eisenbud 1995, théorème 13.3] ou [Serre 1965, III(D)2, théorème 2], mais ce n'est pas nécessaire ici car on a recherche simplement la finitude générique, c'est-à-dire la finitude de l'extension de corps).

Convention 12.7. On fera souvent l'abus de langage consistant à écrire qu'une certaine opération algébrique ou géométrique est calculable sans autre précision sur le corps k dans lequel vivent les données : sauf mention du contraire, il faut en fait comprendre : pour tout corps k *calculable, disposant d'un algorithme de factorisation* (cf. 12.2) *et une p-base finie explicite* (12.4), l'opération en question est calculable. Lorsque k est algébriquement clos, bien entendu, seule l'hypothèse « calculable » est utile (cf. 12.2(4)) ; par ailleurs, d'après le résultat qu'on vient de montrer, les corps que nous sommes amenés à manipuler vérifient toujours les hypothèses qui viennent d'être dites.

(Dans le langage de l'algèbre constructive, l'analogue de nos hypothèses « calculable, disposant d'un algorithme de factorisation et une p-base finie explicite » serait les corps « discrets pleinement factoriels » : voir [Mines, Richman et Ruitenburg 1988, théorème VII.3.3].)

Remarque 12.8. Le fait de considérer des fonctions récursives (générales, par opposition par exemple aux fonctions primitivement récursives) signifie que si $\boldsymbol{P}(m,n)$ est une propriété calculable (des entiers naturels) et que pour chaque m il existe n vérifiant $\boldsymbol{P}(m,n)$, alors la fonction $\mu_n \boldsymbol{P}$ qui à m associe le plus petit n vérifiant $\boldsymbol{P}(m,n)$ est calculable (il s'agit de l'« opérateur μ de Kleene », cf. par exemple [Odifreddi 1989, définitions I.1.5 et I.1.7]). Concrètement, cela signifie que les fonctions calculables (= récursives, donc) peuvent effectuer des « recherches non bornées » dans les entiers naturels, c'est-à-dire parcourir tous les n jusqu'à en trouver un qui vérifie la propriété $\boldsymbol{P}(m,n)$ demandée, même si on ne dispose d'aucune borne de complexité sur le temps qu'une telle recherche pourra prendre (on demande simplement qu'elle termine pour tout m si on veut que la fonction soit totale).

Comme les corps calculables (12.1) sont étiquetés par les entiers naturels, cette notion de « recherche non bornée » s'applique aussi bien à eux. C'est la raison pour laquelle, dans la définition d'un corps calculable, on pourrait par exemple se passer d'imposer que la fonction $(^{-1})_{\mathfrak{K}} \colon \{z \in \mathfrak{K} \colon z \not\equiv 0_{\mathfrak{K}}\} \to \mathfrak{K}$ soit calculable (elle l'est automatiquement puisque pour calculer x^{-1} on peut parcourir tous les $y \in \mathfrak{K}$ jusqu'à en trouver un qui vérifie $x \times_{\mathfrak{K}} y \equiv_{\mathfrak{K}} 1_{\mathfrak{K}}$).

Une fois définis les schémas et autres objets géométriques en 16, on pourra effectuer de même ce type de « recherches non bornées » sur l'ensemble des schémas, morphismes de schémas, ou tout autre objet géométrique du même type : il s'agira d'énumérer toutes les données susceptibles de décrire, par exemple, un schéma, et pour chacune d'elles de tester si elle vérifie la propriété $\boldsymbol{P}$ considérée. Ainsi, il découle du théorème de A. J. de Jong sur la résolution des singularités par altérations [de Jong 1996, 4.1], et du fait que cette propriété soit algorithmiquement testable, qu'on peut en fait calculer une telle résolution ! Il va de soi que cette façon de procéder fait perdre toute utilisabilité pratique à nos algorithmes — et comme observé en 11.6 on *devrait* pouvoir s'en passer.

Sous-remarque : On pourrait même être un peu plus général dans les recherches par test non bornées : il n'est pas nécessaire que la propriété $\boldsymbol{P}(m,n)$ soit décidable (= calculable, = récursive), il suffit qu'elle soit semi-décidable (= récursivement énumérable), autrement dit qu'il existe une machine de Turing qui termine en répondant « vrai » lorsque $\boldsymbol{P}(m,n)$ est vrai, sans imposer qu'elle termine quand $\boldsymbol{P}(m,n)$ n'est pas vrai — on peut alors calculer *un* n vérifiant $\boldsymbol{P}(m,n)$ (pas nécessairement le plus petit) en lançant en parallèle la vérification de tous les $\boldsymbol{P}(m,n)$ jusqu'à ce que l'une d'entre elles termine.

13. Modules de type fini sur une k-algèbre de type fini

Soit $S = k[Z_1, \ldots, Z_d]$ où k est un corps calculable (nous n'utiliserons pas ici l'ensemble des hypothèses 12.7 puisque nous n'aurons jamais affaire à des

factorisations de polynômes : la simple calculabilité de k suffit). Le but de cette section est de montrer qu'on peut manipuler algorithmiquement les S-modules de type fini, et, plus généralement, les modules de type fini sur une algèbre quotient de S.

13.1. ***Algorithmes fondamentaux.*** Un morphisme $\varphi\colon S^m \to S^n$ de S-modules est représenté par une matrice $n \times m$ d'éléments de S. On sait (par exemple en utilisant des bases de Gröbner) répondre algorithmiquement aux deux questions fondamentales suivantes :

— *(Test d'appartenance à un sous-module.)* Donné $\varphi\colon S^m \to S^n$ et un élément $y \in S^n$, décider si y appartient à l'image M de φ et, le cas échéant, en calculer un antécédent. (Ou, de façon équivalente : donnés $x_1, \ldots, x_m \in S^n$ et $y \in S^n$, décider si y peut être écrit comme combinaison linéaire de $x_1, \ldots, x_m$ et, le cas échéant, en trouver les coefficients. Pour le faire, on peut calculer une base de Gröbner du sous-module M engendré par $x_1, \ldots, x_m$, cf. [Eisenbud 1995, algorithmes 15.7 et 15.9], [Decker et Lossen 2006, problème 2.16] ou [Becker et Weispfenning 1993, lemme 6.7 et discussion qui suit], cette base de Gröbner étant elle-même écrite comme combinaison des x_i, et ceci permet de décider si un élément y appartient à M et, le cas échéant, l'écrire comme combinaison des élément de la base, donc des $x_1, \ldots, x_m$.)

— *(Calcul de syzygies.)* Donné $\varphi\colon S^m \to S^n$, calculer un ensemble de générateurs du noyau de φ (ou, si on préfère, donnés des éléments $x_1, \ldots, x_m$ de S^n, calculer un système de générateurs des syzygies entre eux, cf. [Eisenbud 1995, algorithme 15.10] ou [Becker et Weispfenning 1993, théorème 6.4]).

(De façon alternative, on pourra se référer à [Mines, Richman et Ruitenburg 1988, VIII.1.5 combiné à III.2.6] ou bien [Lombardi et Quitté 2011, VII.1.10] pour une présentation de ces faits en algèbre constructive et sans utiliser de bases de Gröbner.)

Soulignons que les algorithmes en question n'utilisent que des opérations rationnelles et des tests d'égalité dans le corps k.

13.2. ***Noyaux, conoyaux et images sur les anneaux de polynômes.*** Une *présentation explicite* d'un S-module M de type fini est la donnée d'un morphisme $\varphi\colon G \to F$, où F, G sont deux S-modules libres de type fini, tel que $M = \operatorname{Coker}\varphi$ (concrètement, φ est fourni sous la forme d'une matrice $n \times m$ d'éléments de S où m et n sont les rangs de G et F respectivement).

Une *présentation explicite* d'un morphisme $\alpha\colon P \to Q$ de S-modules, où

$$P = \operatorname{Coker}(G_P \xrightarrow{\varphi_P} F_P) \quad \text{et} \quad Q = \operatorname{Coker}(G_Q \xrightarrow{\varphi_Q} F_Q) \qquad (\ddagger)$$

sont deux S-modules explicitement présentés comme ci-dessus, est la donnée d'un morphisme $\alpha_F : F_P \to F_Q$ tel que α se déduise de α_F par passage au quotient (autrement dit, tel qu'il existe $\alpha_G : G_P \to G_Q$ vérifiant $\alpha_F \varphi_P = \varphi_Q \alpha_G$).

Dans le contexte ci-dessus, donnés les conoyaux P et Q de $G_P \xrightarrow{\varphi_P} F_P$ et $G_Q \xrightarrow{\varphi_Q} F_Q$, on sait tester si un $\alpha_F : F_P \to F_Q$ est la présentation explicite d'un morphisme $\alpha : P \to Q$; et de plus, on sait calculer algorithmiquement l'image, le conoyau, et le noyau, d'un morphisme explicitement présenté : les algorithmes à cet effet sont bien connus, mais nous les rappelons brièvement ci-dessous pour la commodité du lecteur.

- Pour tester si $\alpha_F : F_P \to F_Q$ passe au quotient et définit (une présentation explicite d')un morphisme $\alpha : P \to Q$ (où P et Q sont encore donnés par (‡)), il s'agit, grâce à l'algorithme de test d'appartenance évoqué en 13.1, de tester si les éléments images de la base de G_P par $\alpha_F \varphi_P$ sont dans l'image de φ_Q : cf. [Decker et Lossen 2006, problème 4.1 et début de §4.2].
- Donné $\alpha : L \to F$ un morphisme entre S-modules libres de type fini, on sait calculer une présentation explicite de $\operatorname{Im}\alpha$ (sous la forme $\operatorname{Im}\alpha = \operatorname{Coker}(H \to L)$). En effet, ceci revient exactement à calculer des générateurs des syzygies entre les images par α des éléments de la base de L (c'est-à-dire, des colonnes de la matrice décrivant α), algorithme déjà évoqué en 13.1 comme calcul de syzygies.
- Si $\alpha : L \to Q$ est un morphisme de S-modules, où L est toujours libre mais cette fois Q est défini par une présentation explicite $Q = \operatorname{Coker}(G_Q \xrightarrow{\varphi_Q} F_Q)$, le morphisme α étant explicitement présenté par la donnée de $\alpha_F : L \to F_Q$, alors on peut encore calculer une présentation explicite de $\operatorname{Im}\alpha$. En effet, il est isomorphe à $(\operatorname{Im}\alpha_F + \operatorname{Im}\varphi_Q)/\operatorname{Im}\varphi_Q$, or $\operatorname{Im}\alpha_F + \operatorname{Im}\varphi_Q$ est l'image du morphisme $L \oplus G_Q \xrightarrow{(\alpha_F, \varphi_Q)} F_Q$ de modules libres, cas traité par le paragraphe précédent, et si $H \to L \oplus G_Q$ est la présentation de cette image, alors $H \to L$ définit la présentation de $\operatorname{Im}\alpha$ recherchée (cf. [Decker et Lossen 2006, problème 4.2]).
- Donné un morphisme $\alpha : P \to Q$ explicitement présenté entre modules explicitement présentés $P = \operatorname{Coker}(G_P \xrightarrow{\varphi_P} F_P)$ et $Q = \operatorname{Coker}(G_Q \xrightarrow{\varphi_Q} F_Q)$, il est facile de calculer une présentation explicite de $\operatorname{Coker}\alpha$, à savoir $\operatorname{Coker}\alpha = \operatorname{Coker}(F_P \oplus G_Q \xrightarrow{(\alpha_F, \varphi_Q)} F_Q)$ (cf. [Decker et Lossen 2006, §4.2.1]). Mais on peut également calculer une présentation de $\operatorname{Im}\alpha$ sous la forme $\operatorname{Coker}(H \to F_P)$ avec H libre (en effet, il s'agit de $\operatorname{Im}(F_P \to Q)$, cas qu'on a traité au paragraphe précédent), et aussi de $\operatorname{Ker}\alpha$ (il s'agit de l'image de $H \to P$, de nouveau le cas qu'on a traité). (cf. [Decker et Lossen 2006, problème 4.3] ou [Eisenbud 1995, proposition 15.32].)

On notera bien évidemment qu'on obtient non seulement une présentation explicite de l'image ou du noyau d'un morphisme explicitement présenté $\alpha : P \to Q$, mais

aussi une présentation explicite de l'inclusion canonique $\operatorname{Im}\alpha \to Q$ ou $\operatorname{Ker}\alpha \to P$. Ceci permettra aisément de se convaincre, par exemple, qu'on peut calculer des sommes ou intersections de sous-modules.

13.3. ***Modules sur les algèbres de type fini quelconques.*** Si $R = S/I$ est une algèbre de type fini sur un corps k où $S = k[Z_1, \dots, Z_d]$ et I l'idéal engendré par $h_1, \dots, h_r \in S$, un R-module n'est autre qu'un S-module annulé par I. On peut appeler *R-module explicitement présenté* le conoyau d'un morphisme $\varphi\colon R^m \to R^n$ (décrit par une matrice $n \times m$ d'éléments de R) ou, de façon équivalente, comme le conoyau d'un morphisme $\tilde{\varphi}\colon S^m \to S^n$ tel que $h_j e_i$ soit dans l'image de $\tilde{\varphi}$ pour tout $1 \leq j \leq r$ et tout $1 \leq i \leq n$ (en notant $e_1, \dots, e_n$ la base canonique de S^n) : ce critère est algorithmiquement testable, et on passe de façon évidente d'une description à l'autre (dans un sens en reprenant la matrice de $\tilde{\varphi}$ comme matrice de φ, et dans l'autre en relevant de façon quelconque la matrice de φ et en ajoutant des colonnes $h_j e_i$). Les morphismes de R-modules sont simplement des morphismes de S-modules qui s'avèrent être des R-modules, et ce qui précède montre qu'on sait calculer l'image, le conoyau et le noyau d'un morphisme explicitement présenté de R-modules.

Notons par ailleurs que pour manipuler des *sous-modules* d'un module explicitement présenté, on peut représenter ceux-ci comme l'image d'un morphisme (ou, ce qui revient au même, par un ensemble d'éléments engendrant le sous-module) ou comme le noyau d'un morphisme : on a vu qu'on peut passer d'une représentation à l'autre. Dès lors, il est clair qu'on peut calculer des sommes ou intersections de sous-modules, de tester l'inclusion ou l'égalité entre deux sous-modules (tout se ramène facilement à tester la nullité d'un sous-module, ce qui est facile si on le décrit comme engendré par certains éléments).

(En particulier, on sait tester l'inclusion et l'égalité d'idéaux.)

13.4. ***Produits tensoriels et* Hom *de modules ; transporteurs et annulateurs.*** On continue de noter $R = S/I$ une k-algèbre de type fini où $S = k[Z_1, \dots, Z_d]$.

Si

$$P = \operatorname{Coker}(G_P \xrightarrow{\varphi_P} F_P) \quad \text{et} \quad Q = \operatorname{Coker}(G_Q \xrightarrow{\varphi_Q} F_Q)$$

sont deux R-modules explicitement présentés, on peut calculer une présentation explicite de $P \otimes_R Q$, à savoir $P \otimes Q = \operatorname{Coker}((G_P \otimes F_Q) \oplus (F_P \otimes G_Q) \to F_P \otimes F_Q)$ où les produits tensoriels de modules libres sont triviaux à calculer et la flèche est $(\varphi_P \otimes \mathrm{Id}) \oplus (\mathrm{Id} \otimes \varphi_Q)$.

De même, grâce au fait qu'on sait calculer les noyaux, on peut calculer une présentation explicite du module $\mathsf{Hom}_R(P, Q) = \operatorname{Ker}(\mathsf{Hom}_R(F_P, Q) \to \mathsf{Hom}_R(G_P, Q))$ où $\mathsf{Hom}_R(F_P, Q)$ admet la présentation explicite évidente $\operatorname{Coker}(\mathsf{Hom}_R(F_P, G_Q) \to \mathsf{Hom}_R(F_P, F_Q))$ et de même pour $\mathsf{Hom}_R(G_P, Q)$, et où la flèche entre eux est

donnée par le morphisme $\mathrm{Hom}_R(F_P, F_Q) \to \mathrm{Hom}_R(G_P, F_Q)$ de composition à gauche par φ_P.

Si N, N' sont des sous-modules d'un module M explicitement présenté, on peut calculer l'idéal « transporteur » $(N : N') := \{f \in R : fN' \subseteq N\}$ (c'est-à-dire, en calculer des générateurs) : en effet, on peut le voir comme le noyau du morphisme $R \to \mathrm{Hom}_R(N', M/N)$. De même, si J est un idéal de R et N un sous-module de M, on peut calculer le sous-module $(N : J) := \{x \in M : Jx \subseteq N\}$ de M (car on peut le voir comme noyau de $M \to \mathrm{Hom}_R(J, M/N)$). (Comparer [Eisenbud 1995, exercice 15.41].)

En particulier, on sait calculer l'idéal annulateur $(0 : M)$ d'un module M explicitement présenté.

13.5. Tor *et* Ext. On continue de noter $R = S/I$ une k-algèbre de type fini où $S = k[Z_1, \ldots, Z_d]$.

Si M est un R-module défini par une présentation explicite $M = \mathrm{Coker}(G \to F)$, on peut aisément calculer le tronqué à un ordre quelconque d'une résolution libre de M : en effet, il suffit de poser $F_0 = F$ et $F_1 = G$ et récursivement construire le noyau de $F_{i+1} \to F_i$ comme l'image d'un morphisme $F_{i+2} \to F_{i+1}$ de modules libres (par l'algorithme de syzygies de 13.1 si on est sur l'algèbre de polynômes S, ou par les techniques générales présentées ci-dessus).

Si F_i est une résolution libre d'un R-module P explicitement présenté, et si Q est un R-module explicitement présenté, en calculant le complexe $F_i \otimes_R Q$, puis l'homologie de celui-ci, on peut calculer $\mathrm{Tor}_i^R(P, Q)$ pour i arbitraire (mais fixé). De même, en calculant la cohomologie du complexe $\mathrm{Hom}_R(F_i, Q)$ on calcule $\mathrm{Ext}_R^i(P, Q)$ pour i arbitraire (mais fixé).

13.6. *Présentation d'une algèbre finie comme module.* Soit A un anneau quelconque. Une A-algèbre de présentation finie en tant que A-module est, en particulier, de présentation finie en tant que A-algèbre : la proposition facile suivante explicite ce fait (on pourra comparer avec [de Jong 1998, §3], ou [Lombardi et Quitté 2011, exercice IV.15] dans le cas libre) :

Proposition 13.6.1. *Soit A un anneau et B une A-algèbre engendrée comme A-module par les éléments $1, x_1, \ldots, x_n$ dont le module des syzygies (c'est-à-dire le sous-A-module N de A^{n+1} formé des $(c_0, \ldots, c_n) \in A^{n+1}$ tels que $c_0 + c_1x_1 + \cdots + c_nx_n = 0 \in B$) soit de type fini engendré par $y_1, \ldots, y_m$.*

Soit $\Phi\colon A[T_1, \ldots, T_n] \to B$ le morphisme de A-algèbres envoyant T_i sur x_i et J son noyau (c'est-à-dire l'idéal des relations algébriques entre $x_1, \ldots, x_n$). On considère chaque y_i comme un élément de J en identifiant $(c_0, \ldots, c_n) \in A^{n+1}$ au polynôme $c_0 + c_1T_1 + \cdots + c_nT_n$ de degré 1. De plus, pour chaque $1 \le i, j \le n$, écrivons $x_ix_j = b_0^{(i,j)} + b_1^{(i,j)}x_1 + \cdots + b_n^{(i,j)}x_n$ pour certains $b_u^{(i,j)} \in A$, et soit

$q_{i,j} = b_0^{(i,j)} + b_1^{(i,j)} T_1 + \cdots + b_n^{(i,j)} T_n - T_i T_j$, *polynôme de degré* 2 *appartenant à* J (*relation quadratique*).

Alors J *est engendré, en tant qu'idéal de* $A[T_1, \ldots, T_n]$, *par les* y_i *et par les* $q_{i,j}$.

Démonstration. Soit J' l'idéal de $A[T_1, \ldots, T_n]$ engendré par les y_i et par les $q_{i,j}$. Fixons un ordre total quelconque sur les monômes en $T_1, \ldots, T_n$ qui raffine l'ordre partiel donné par le degré total (par exemple, l'ordre lexicographique gradué) : il s'agit donc d'un bon ordre sur les monômes. Soit z un élément de J n'appartenant pas à J' et dont le monôme initial (c'est-à-dire, le plus grand monôme intervenant dans z avec un coefficient non nul) soit le plus petit possible. Si z est de degré ≥ 2, ce monôme initial est divisible par un $T_i T_j$, disons $z = aT_i T_j e + u$ où $a \in A$, où e est un monôme et où u ne fait intervenir que des monômes plus petits que $T_i T_j e$: alors $z' := z + aeq_{i,j}$ est congru à z modulo J', donc appartient à J mais non à J', et son monôme initial est strictement plus petit que celui de z, une contradiction. Si z est de degré ≤ 1, alors z appartient à N donc z est engendré par $y_1, \ldots, y_m$, de nouveau une contradiction. □

13.6.2. En particulier, si $R = S/I$ est une algèbre de présentation finie sur un corps k et si B est un R-module explicitement présenté, et si on dispose sur B d'une multiplication décrite, par exemple, sous forme de tous les produits $x_i x_j$ pour x_i, x_j parcourant le système de générateurs donné par la présentation de B comme R-module, alors on peut calculer une présentation de B comme R-algèbre, et donc comme k-algèbre.

Ceci s'applique notamment pour montrer que si J est un idéal de R, on peut calculer une présentation de $\mathsf{End}_R(J)$ en tant que R-algèbre ou en tant que k-algèbre.

14. Algèbres de type fini sur un corps : description algorithmique

Comme dans la section précédente, k est ici un corps calculable (nous n'utiliserons pas ici l'ensemble des hypothèses 12.7 puisque nous n'aurons jamais affaire à des factorisations de polynômes : la simple calculabilité de k suffit).

14.1. ***Algèbres de type fini sur k.*** Une algèbre de type fini sur un corps k sera représentée comme un quotient $A = k[X_1, \ldots, X_m]/I$ d'une algèbre de polynômes, c'est-à-dire par la donnée d'un ensemble (fini !) de générateurs de I. Un élément de R sera représenté par un polynôme dans $k[X_1, \ldots, X_m]$ qui le relève : on peut ainsi calculer algorithmiquement les sommes et produits dans A, et le fait de pouvoir tester l'appartenance à I permet de tester la nullité, donc l'égalité, d'éléments de A. Remarquons aussi qu'on sait tester l'inversibilité (un $f \in R$ est inversible si et seulement si, pour n'importe quel $\tilde{f} \in k[X_1, \ldots, X_m]$ le relevant, l'idéal $I + (\tilde{f})$ obtenu en adjoignant $\tilde{f}$ aux générateurs décrivant I, est égal à l'idéal unité de $k[X_1, \ldots, X_m]$, chose qu'on sait tester).

14.2. ***Morphismes entre algèbres de type fini.*** Si $A = k[X_1, \ldots, X_m]/I$ et $B = k[Y_1, \ldots, Y_n]/J$ sont deux algèbres de type fini sur k comme ci-dessus, on représentera un morphisme de k-algèbres $A \to B$ comme la donnée de m éléments $h_1, \ldots, h_m$ de Y tels que $f_i(h_1, \ldots, h_m) = 0$ pour tout i si $f_1, \ldots, f_r$ sont les générateurs choisis pour représenter I (cette condition est évidemment testable algorithmiquement).

Dans ces conditions, on peut aussi présenter B comme A-algèbre de la manière suivante : $B = A[Y_1, \ldots, Y_n]/\tilde{J}$, où $\tilde{J}$ est l'idéal $J + (x_i - h_i)$ décrit en adjoignant aux générateurs décrivant J les relations supplémentaires identifiant l'image x_i de X_i dans A avec l'élément h_i de B (ou plus exactement, n'importe quel polynôme dans $k[Y_1, \ldots, Y_n]$ le relevant). Et réciproquement, donnée une présentation $B = A[Y_1, \ldots, Y_n]/J$ où J est décrit par des générateurs, on peut écrire $B = k[X_1, \ldots, X_m, Y_1, \ldots, Y_n]/\hat{J}$ où $\hat{J}$ est l'idéal obtenu en relevant les générateurs décrivant J et en y adjoignant ceux de I ; et le morphisme $A \to B$ est alors évident. On pourra donc librement choisir entre la représentation d'un morphisme entre k-algèbres de type fini et celle d'une algèbre sur une autre algèbre.

Dans les conditions ci-dessus, on peut tester algorithmiquement si le morphisme $A \to B$ est *surjectif*. En effet, sur la description où $A = k[X_1, \ldots, X_m]/I$ et $B = k[X_1, \ldots, X_m, Y_1, \ldots, Y_n]/\hat{J}$, il s'agit de tester, pour chaque Y_i, si Y_i est congru modulo $\hat{J}$ à un élément de $k[X_1, \ldots, X_m]$, or ceci peut se faire testant, au moyen d'une base de Gröbner, si chaque Y_i appartient à l'idéal initial (cf. [Eisenbud 1995, §15.2]) de $\hat{J}$ pour un ordre monomial pour lequel Y_i est supérieur à tout monôme en les $X_1, \ldots, X_m$. (En effet, si pour chaque $i \in \{1, \ldots, n\}$ il existe $u_i \in k[X_1, \ldots, X_m]$ tel que $Y_i - u_i \in \hat{J}$ alors pour un tel ordre monomial le terme initial de $Y_i - u_i$, à savoir Y_i d'après l'hypothèse faite sur l'ordre monomial, appartient à l'idéal initial de $\hat{J}$; et réciproquement, si chaque Y_i appartient à l'idéal initial de $\hat{J}$, disons que $Y_1 < \cdots < Y_n$, alors chaque Y_i est congru modulo $\hat{J}$ a un polynôme en $X_1, \ldots, X_m, Y_1, \ldots, Y_{i-1}$, donc en les $X_1, \ldots, X_m$.)

On peut aussi tester algorithmiquement si le morphisme $A \to B$ est *injectif* ou même calculer son noyau (un idéal de A, qu'on peut représenter comme l'image d'un idéal de $k[X_1, \ldots, X_m]$). En effet, si $A = k[X_1, \ldots, X_m]/I$ et $B = k[X_1, \ldots, X_m, Y_1, \ldots, Y_n]/\hat{J}$ où $I \subseteq \hat{J}$, le noyau du morphisme $A \to B$ est (l'image modulo I de) l'intersection $\hat{J} \cap k[X_1, \ldots, X_m]$, laquelle se calcule par un algorithme d'élimination (cf. [Eisenbud 1995, §15.10.4]). Ceci permet naturellement de calculer aussi une présentation de l'image $\operatorname{Im}\varphi \simeq A/\operatorname{Ker}\varphi$ d'un morphisme $\varphi\colon A \to B$ (il n'y a pas redondance avec le paragraphe précédent, car cette présentation de l'image ne permet pas trivialement de savoir si elle est B tout entier sauf, justement, à utiliser ce qui précède).

Lemme 14.3. *Soit $\varphi\colon A \to B$ un morphisme de k-algèbres (où, ici, k est un anneau quelconque). Pour $f \in A$, on note comme d'habitude $A[1/f]$ la k-algèbre*

$A[T]/(Tf-1)$ localisée de A en inversant f (et $B[1/f] = B \otimes_A A[1/f]$). Alors l'ensemble des $f \in A$ tels que le morphisme $A[1/f] \to B[1/f]$ déduit de φ soit injectif (*resp. soit surjectif*, *resp. soit un isomorphisme*) *est un idéal de A.*

Démonstration. Soient $N = \operatorname{Ker}\varphi$ et $Q = \operatorname{Coker}\varphi$, vus comme A-modules. La suite exacte $0 \to N \to A \to B \to Q \to 0$, tensorisée par le A-module plat $A[1/f]$, donne $0 \to N[1/f] \to A[1/f] \to B[1/f] \to Q[1/f] \to 0$: on voit donc que l'ensemble des f tels que $A[1/f] \to B[1/f]$ soit injective (resp. surjective, resp. bijective) est l'ensemble des f tels que $N[1/f] = 0$ (resp. $Q[1/f] = 0$, resp. $N[1/f] = 0$ et $Q[1/f] = 0$). Or si M est un A-module, dire de $f \in A$ que $M[1/f] = 0$ signifie que chaque élément de M est annulé par une puissance de f (pouvant dépendre de l'élément), c'est-à-dire que f est dans l'intersection des radicaux des annulateurs de tous les éléments $z \in M$ — sous cette forme, il est clair que l'ensemble des f en question est bien un idéal de A. □

Proposition 14.4. *Dans les conditions du lemme ci-dessus* (*mais en reprenant pour k un corps calculable*), *si A et B sont des k-algèbres de type fini décrites par une présentation, alors on peut algorithmiquement calculer les idéaux indiqués par le lemme qui précède, à condition de savoir calculer le radical d'un idéal de A* (*ce qui sera possible d'après 15.2 au prix des hypothèses 12.7 sur le corps k*).

Démonstration. On note comme précédemment $N = \operatorname{Ker}\varphi$ et $Q = \operatorname{Coker}\varphi$, vus comme, respectivement, un idéal de A et un A-module (qui n'est pas, en général, de type fini). Par ailleurs, on suppose

$$A = k[X_1, \ldots, X_m]/I \quad \text{et} \quad B = k[X_1, \ldots, X_m, Y_1, \ldots, Y_n]/\hat{J},$$

où $I \subseteq \hat{J}$.

On a déjà expliqué qu'on peut calculer l'idéal $\hat{J} \cap k[X_1, \ldots, X_m]$ de $k[X_1, \ldots, X_m]$ par un algorithme d'élimination : les générateurs ainsi obtenus, lus modulo I, engendrent N, et fournissent donc une description de celui-ci comme idéal de A, ou en particulier, comme A-module de type fini. L'idéal des $f \in A$ tels que $A[1/f] \to B[1/f]$ soit injectif, soit $N[1/f] = 0$, est le radical de l'annulateur de N, qu'on peut calculer d'après 13.4 et l'hypothèse faite sur la calculabilité du radical.

Pour calculer l'idéal des $f \in A$ tels que $A[1/f] \to B[1/f]$ soit surjectif, on peut supposer que $A \xrightarrow{\varphi} B$ est injectif (quitte à quotienter par N, qu'on sait calculer, pour remplacer A par l'image de φ), autrement dit que $I = \hat{J} \cap k[X_1, \ldots, X_m]$. Nous ferons donc cette hypothèse.

Pour chaque variable Y_i, dont on note y_i l'image dans B, on peut calculer l'idéal formé des $f \in A$ tels qu'il existe $r \geq 0$ pour lequel $f^r y_i \in A$: en effet, il s'agit du radical de l'idéal $(A : y_i)$ des $f \in A$ tels que $f y_i \in A$, et ce dernier est calculable en travaillant dans le sous-A-module de type fini de B engendré par 1 et y_i (dont les relations sont connues : c'est l'intersection de $\hat{J}$ avec $k[X_1, \ldots, X_m, Y_i]$). On peut

donc aussi calculer l'intersection de ces n idéaux, c'est-à-dire l'ensemble des $f \in A$ tels que pour chaque i il existe $r \geq 0$ vérifiant $f^r y_i \in A$. Mais il est clair que cet idéal est aussi l'idéal des $f \in A$ tels que pour chaque $h \in B$ il existe $r \geq 0$ vérifiant $f^r h \in A$: c'est bien l'idéal des $f \in A$ tels que $A[1/f] \to B[1/f]$ soit surjectif. □

Vu au niveau du morphisme de schémas $\operatorname{Spec} B \to \operatorname{Spec} A$, l'idéal des f tels que $A[1/f] \to B[1/f]$ soit injectif définit le plus grand ouvert au-dessus duquel $\operatorname{Spec} B \to \operatorname{Spec} A$ est schématiquement dominant, tandis que l'idéal des f tels que $A[1/f] \to B[1/f]$ soit surjectif définit le plus grand ouvert au-dessus duquel $\operatorname{Spec} B \to \operatorname{Spec} A$ est une immersion fermée.

Nous tirons le lemme suivant de [Petersen 2010] :

Lemme 14.5. *Soit $\varphi : A \to B$ un morphisme de k-algèbres* (*où*, *ici*, *k est un anneau quelconque*) : *le morphisme* $\operatorname{Spec} B \to \operatorname{Spec} A$ *est une immersion ouverte si et seulement si l'idéal engendré dans B par l'idéal P des $f \in A$ tels que $A[1/f] \to B[1/f]$ soit un isomorphisme*, *est l'idéal unité de B. De plus*, *si c'est le cas*, *l'image de cette immersion est l'ouvert complémentaire du fermé de* $\operatorname{Spec} A$ *défini par l'idéal P.*

Démonstration. Si $\operatorname{Spec} B \to \operatorname{Spec} A$ est une immersion ouverte, son image dans $\operatorname{Spec} A$ est la réunion d'ouverts principaux $D(f_i)$ pour certains $f_i \in A$ (qui *a priori* pourraient ne pas être en nombre fini), pour chacun d'entre eux $A[1/f_i] \to B[1/f_i]$ est un isomorphisme puisque le morphisme de schémas correspondant en est un, et comme les $D(f_i)$ recouvrent $\operatorname{Spec} B$, les images des f_i dans B engendrent l'idéal unité de B.

Réciproquement, supposons donnés un certain nombre (que cette fois on peut d'emblée supposer fini) de f_i dans A qui engendrent l'idéal unité de B et tels que les $A[1/f_i] \to B[1/f_i]$ soient des isomorphismes : alors le morphisme $\operatorname{Spec} B \to \operatorname{Spec} A$ est un isomorphisme au-dessus de chacun des ouverts principaux $D(f_i)$ de $\operatorname{Spec} A$, et leurs images réciproques recouvrent $\operatorname{Spec} B$: il s'agit donc d'un isomorphisme de $\operatorname{Spec} B$ sur l'ouvert réunion des $D(f_i)$ dans A. Cet ouvert est bien le complémentaire du fermé défini par les f_i. □

En particulier, si A et B sont des k-algèbres de type fini décrites par une présentation, alors on peut algorithmiquement tester si φ définit une immersion ouverte $\operatorname{Spec} B \to \operatorname{Spec} A$.

14.6. ***Morphismes finis.*** Soit

$$A = k[X_1, \ldots, X_m]/I \quad \text{et} \quad B = k[X_1, \ldots, X_m, Y_1, \ldots, Y_n]/\hat{J}$$

avec $I \subseteq \hat{J}$ (comme en 14.2) la présentation d'un morphisme $A \to B$ entre k-algèbres de type fini. Alors on peut tester algorithmiquement si ce morphisme est *fini* (c'est-à-dire si B est un A-module de type fini). En effet, c'est le cas si et

seulement si les images modulo $\hat{J}$ de chacun des Y_i sont entières sur A, ce qui d'une part permet de se ramener au cas où ($n = 1$, c'est-à-dire) $B = k[X_1, \ldots, X_m, Y]/\hat{J}$, et d'autre part c'est le cas si et seulement si $\hat{J}$ contient un polynôme dont le monôme initial, pour un ordre monomial pour lequel Y est supérieur à tout monôme en les $X_1, \ldots, X_m$, est une puissance de Y. Autrement dit, sous ces hypothèses, c'est le cas lorsque l'idéal initial de $\hat{J}$ (pour un tel ordre ; c'est-à-dire l'idéal engendré par les monômes initiaux des éléments de $\hat{J}$) contient une puissance de Y. Or les monômes initiaux de la base de Gröbner de $\hat{J}$ (pour l'ordre considéré) engendrent son idéal initial : il s'agit donc simplement de tester si la base contient un élément dont le monôme initial est une puissance de Y.

Notons qu'on a alors une présentation explicite de B comme un A-module de type fini, dont les générateurs sont les monômes sur les Y_i. Dans le cas où $n = 1$, il suffit d'aller jusqu'à la puissance donnée par le degré de l'équation entière satisfaite par Y, moins 1).

15. Algèbre commutative effective

Dans cette section (en fait, à partir de 15.2) et dans la suite de cette partie, même si elles ne sont pas partout indispensables, nous ferons implicitement les hypothèses 12.7 sur le corps k auquel on a affaire.

15.1. ***Fonction de Hilbert et dimension.*** Soit $S = k[Z_1, \ldots, Z_d]$ où k est un corps, que nous voyons comme une k-algèbre *graduée* (par le degré total). Si $M = \mathrm{Coker}(G \to F)$ est un S-module gradué explicitement présenté (c'est-à-dire que F et G sont des modules libres de type fini gradués, i.e. des sommes directes finies de $S[n_i]$ où $S[n_i]$ désigne l'algèbre S où le degré est décalé de n_i ; et où la flèche $G \to F$ qui décrit M est homogène de degré 0), alors on sait algorithmiquement calculer la fonction de Hilbert de M (qui à n associe la dimension sur k de l'espace vectoriel des éléments de M homogènes de degré n) : c'est-à-dire que non seulement on sait calculer sa valeur en chaque degré n donné, mais on sait aussi calculer un rang à partir duquel cette fonction est un polynôme, et quel est ce polynôme. (Pour ce fait, nous renvoyons à [Eisenbud 1995, théorème 15.26] et [Cox, Little et O'Shea 2007, chapitre 9, §2–3].)

Dans ce même contexte, on sait calculer une résolution libre graduée *finie* de M (c'est-à-dire de la forme $0 \to F_r \to \cdots \to F_2 \to F_1 \to F_0 \to 0$ avec F_i libre de type fini gradué et les flèches homogènes de degré 0) : cf. [Eisenbud 1995, corollaire 15.11]. (Ce calcul ne fait pas appel à des recherches non bornées : notamment, la longueur r de la résolution est majorée par le nombre d de variables.)

Si $S = R/I$ où I est un idéal homogène de R, la fonction de Hilbert d'un S-module gradué M est celle du R-module gradué sous-jacent à M. (En revanche, il n'existe pas en général de résolution libre finie de M comme S-module.)

15.2. ***Décomposition primaire.*** Dans cette section, où on se penche sur la calculabilité d'une décomposition primaire d'un idéal I (dans un anneau de polynômes), on entend par ce terme le calcul de couples $(M_i, \mathfrak{p}_i)$ d'idéaux (du même anneau) tels que $I = \bigcap_i M_i$, l'intersection étant irredondante, avec $\mathfrak{p}_i$ des idéaux premiers deux à deux distincts et M_i (pour chaque i) un idéal $\mathfrak{p}_i$-primaire. Nous cherchons donc à la fois à calculer les M_i (qui ne sont pas uniques) et les $\mathfrak{p}_i$ (qui le sont). Remarquons en particulier que la décomposition primaire recouvre le calcul du radical d'un idéal (intersection des $\mathfrak{p}_i$), et permet de tester si un idéal est radical, ou s'il est premier.

15.2.1. *Dimension zéro.* Soit k un corps (dont, conformément à la convention 12.7, on suppose qu'il est calculable et dispose d'un algorithme de factorisation et une p-base finie explicite). Alors, si I est un idéal de $k[Z_1, \ldots, Z_d]$ de dimension 0 (voir la section suivante pour le cas plus général), on peut algorithmiquement calculer le radical, et plus généralement une décomposition primaire, de I : pour cela, on renvoie soit à [Gianni, Trager et Zacharias 1988, §6], ou bien, pour une présentation peut-être plus simple, à [Becker et Weispfenning 1993, théorème 8.22] combiné à [Steel 2005] pour lever les difficultés liées à l'inséparabilité (cette dernière référence se place dans un cas plus restreint, mais il est aisé de voir que ces hypothèses additionnelles ne servent que pour obtenir celle que nous avons faite de factorisation dans les extensions finies).

15.2.2. *Dimension arbitraire.* Soit k un corps (dont, comme dans le paragraphe précédent, et conformément à la convention 12.7, on suppose qu'il est calculable et dispose d'un algorithme de factorisation et une p-base finie explicite). Alors, si I est un idéal de $k[Z_1, \ldots, Z_d]$, on peut algorithmiquement calculer une décomposition primaire de I en ramenant ce problème à celui de la dimension 0 : on renvoie pour cela à [Gianni, Trager et Zacharias 1988, §8 et §9] et [Becker et Weispfenning 1993, théorème 8.101] (cf. aussi [Steel 2005, §5.3]).

(On pourra remarquer au passage que l'algorithme IDEALDIV2 décrit en [Becker et Weispfenning 1993, p. 268], est primitivement récursif.)

15.3. ***Algèbre de Rees et gradué associé.*** Soit R une k-algèbre de type fini, disons $R = S/I$ où $S = k[Z_1, \ldots, Z_d]$ est un anneau de polynômes, et soit J un idéal de R engendré par des éléments $f_1, \ldots, f_r \in R$.

L'*algèbre de Rees* associée à cette situation est la sous-algèbre $R[Jt] = R \oplus Jt \oplus J^2t^2 \oplus \cdots$ de l'algèbre $R[t]$ des polynômes en une indéterminée t sur R formée des polynômes dont le coefficient de degré i appartient à J^i. On peut calculer une présentation de $R[Jt]$ comme R-algèbre, donc aussi comme k-algèbre, de la manière suivante. Soit L l'idéal de $S[T_1, \ldots, T_r]$ défini comme l'intersection de ce dernier avec l'idéal de $S[T_1, \ldots, T_r, t]$ engendré par I et par les $T_i - f_i t$: alors on sait calculer L par un algorithme d'élimination (cf. [Eisenbud 1995, §15.10.4]).

Or $R[Jt]$ est isomorphe au quotient $S[T_1, \dots, T_r]/L$, l'isomorphisme envoyant $a \in R$ sur la classe modulo L de n'importe quel $\hat{a} \in S$ qui le représente (remarquer que L contient I), et $f_{u_1} \cdots f_{u_i} t^i \in J^i t^i$ sur la classe de $T_{u_1} \cdots T_{u_i}$ modulo L. (Cf. [Vasconcelos 2005, proposition 1.5].)

Le quotient de l'algèbre de Rees $R[Jt]$ par l'idéal J de R définit l'*algèbre graduée associée* à J dans R, soit $\mathrm{gr}_J(R) = (R/J) \oplus (J/J^2)t \oplus (J^2/J^3)t^2 \oplus \cdots$ (les t^i, qui servent simplement à étiqueter les degrés, sont souvent omis de cette description). D'après ce qui précède, on peut aussi en calculer une présentation comme (R/J)-algèbre ou comme k-algèbre, à savoir $S[T_1, \dots, T_r]/(L + (f_1, \dots, f_r))$.

Expliquons comment ceci s'adapte au cas d'un R-module M explicitement présenté (cf. 13.3) pour obtenir une présentation explicite de $M[Jt] = M \oplus JMt \oplus J^2Mt^2 \oplus \cdots$ comme module sur l'algèbre de Rees $R[Jt]$, ainsi donc que du gradué $\mathrm{gr}_J(M) = (M/JM) \oplus (JM/J^2M)t \oplus \cdots$ comme module sur $\mathrm{gr}_J(R)$. À partir d'une présentation $M = S^n/Q$ de M comme S-module (où $Q \subseteq S^n$ contient I^n), on définit encore le $S[T_1, \dots, T_r]$-module L — tel que $M[Jt]$ soit isomorphe à $S[T_1, \dots, T_r]^n/L$ — comme l'intersection de $S[T_1, \dots, T_r]^n$ avec le sous-$S[T_1, \dots, T_r, t]$-module de $S[T_1, \dots, T_r, t]^n$ engendré par Q et les produits de $T_i - f_i t$ par les éléments de la base canonique de $S[T_1, \dots, T_r, t]^n$. On peut calculer une présentation de L car la théorie de l'élimination fonctionne encore pour les sous-modules des modules libres de type fini sur les anneaux de polynômes [Eisenbud 1995, remarque suivant la proposition 15.29 et exercice 15.37].

15.4. ***Calculs de longueurs et de multiplicités.*** Soit comme dans la section précédente (15.3) R une k-algèbre de type fini, et soit maintenant $\mathfrak{p}$ un idéal *premier* de R. (On rappelle que grâce à 15.2 on sait tester si un idéal de R est premier.) Remarquons que le corps $\kappa_\mathfrak{p} := R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} = \mathrm{Frac}(R/\mathfrak{p})$ est calculable, et on a même les propriétés (12.7) d'admettre un algorithme de factorisation et une p-base finie explicite en vertu de 12.5 et des remarques 12.6. Si M est un R-module explicitement présenté, on a obtenu ci-dessus une présentation explicite de $\mathrm{gr}_\mathfrak{p} R$ comme algèbre de type fini sur $R/\mathfrak{p}$ et de $\mathrm{gr}_\mathfrak{p} M$ comme module sur $\mathrm{gr}_\mathfrak{p} R$: ceci donne donc également une présentation explicite de $\mathrm{gr}_\mathfrak{p} R_\mathfrak{p}$ comme algèbre de type fini sur $\kappa_\mathfrak{p}$ et de $\mathrm{gr}_\mathfrak{p} M_\mathfrak{p}$ comme module sur cette algèbre de type fini. D'après 15.1, on peut calculer la fonction de Hilbert de $\mathrm{gr}_\mathfrak{p} M_\mathfrak{p}$, c'est-à-dire la fonction $\dim_{\kappa_\mathfrak{p}} \mathfrak{p}^i M_\mathfrak{p}/\mathfrak{p}^{i+1} M_\mathfrak{p}$ (« calculer » au sens où on peut à la fois calculer le polynôme avec lequel cette fonction coïncide pour i assez grand, et expliciter une borne à partir de laquelle elle coïncide avec lui).

En particulier, on sait calculer la *multiplicité* $\mathrm{mult}_{R_\mathfrak{p}}(\mathfrak{p}, M_\mathfrak{p})$ de $\mathfrak{p}$ dans $M_\mathfrak{p}$ (cf. [Serre 1965, V(A)2] et [Eisenbud 1995, remarque suivant le corollaire 12.5]).

Expliquons comment, dans le cas où $\mathfrak{a}$ est seulement supposé être un idéal $\mathfrak{p}$-primaire de R (avec $\mathfrak{p}$ un idéal premier), on peut *majorer* la multiplicité $\mathrm{mult}_{R_\mathfrak{p}}(\mathfrak{a}, M_\mathfrak{p})$

(nous n'aurons pas besoin d'un calcul exact). En calculant la fonction de Hilbert de $\mathrm{gr}_{\mathfrak{p}} R/\mathfrak{a}$, on calcule (sans effectuer de recherche non bornée) un r assez grand pour que $\mathfrak{p}^r \subseteq \mathfrak{a}$, ce qui entraîne $\mathfrak{p}^{ri} M \subseteq \mathfrak{a}^i M$ pour tout i : la longueur sur $R_{\mathfrak{p}}$ de $M_{\mathfrak{p}}/\mathfrak{a}^i M_{\mathfrak{p}}$ est donc majorée par celle de $M_{\mathfrak{p}}/\mathfrak{p}^{ri} M_{\mathfrak{p}}$, or les paragraphes précédents montrent qu'on sait calculer la longueur sur $R_{\mathfrak{p}}$ de $\mathfrak{p}^j M_{\mathfrak{p}}/\mathfrak{p}^{j+1} M_{\mathfrak{p}}$ (qui est la dimension de ce $\kappa_{\mathfrak{p}}$-espace vectoriel), donc de $M_{\mathfrak{p}}/\mathfrak{p}^j M_{\mathfrak{p}}$.

15.5. *Normalisation.*

15.5.1. Soient A un anneau nœthérien réduit, K son anneau total des fractions et $\widetilde{A}$ le normalisé de A dans K. La détermination constructive de $\widetilde{A}$ est un problème classique, qui fait l'objet d'une littérature abondante : citons notamment les articles [Stolzenberg 1968], [de Jong 1998], [Singh et Swanson 2009] (en caractéristique positive uniquement) et les livres [Vasconcelos 2005, chapitre 6 ; Huneke et Swanson 2006, chapitre 15]. Pour la commodité du lecteur, nous rappelons ici brièvement un argument (tiré de [de Jong 1998]). Soit I un idéal de A contenant un élément i non diviseur de zéro et posons $A' = \mathrm{End}_A(I)$. Le morphisme évident $A \to A'$ est entier ; il est injectif, de même que le morphisme $A' \to K$, $\phi \mapsto \phi(i)i^{-1}$, qui est indépendant du choix de i. Notons que la structure d'anneau de A' est facilement explicitable, d'abord comme A-module puis comme anneau ; cf. 13.4 et 13.6.2 ou bien [de Jong 1998, §3]. Il résulte de ce qui précède que si A est normal, le morphisme $A \to A'$ est un isomorphisme. On a la réciproque suivante, moyennant des hypothèses supplémentaires.

Proposition 15.5.2 (Grauert–Remmert). *Soient k un corps* parfait *et*

$$A = k[x_1, \ldots, x_n]/(f_1, \ldots, f_r)$$

un anneau intègre de normalisé $\widetilde{A}$ dans son corps des fractions. Notons I le radical de l'idéal de Fitting $J = \mathrm{Fitt}_d(\Omega^1_{A/k})$ engendré par l'image dans A des déterminants des sous-matrices jacobiennes de taille $n-d$. Alors :

(i) *l'idéal J est non nul et inclus dans l'idéal conducteur $\mathfrak{c} := \mathrm{Ann}_A(\widetilde{A}/A)$;*

(ii) *le morphisme $A \to \mathrm{End}_A(I)$ est un isomorphisme si et seulement si A est normal.*

Pour (i), voir par exemple [Singh et Swanson 2009, remarque 1.5], où il est implicitement fait usage du théorème de normalisation de Noether « génériquement étale » [Eisenbud 1995, corollaire 16.18 ; Zariski et Samuel 1975, V, §3, théorème 8]. (Voir aussi [Huneke et Swanson 2006, exercice 12.12].) Pour (ii), voir par exemple [Grauert et Remmert 1984, VI, §5],

L'anneau A étant japonais, la suite croissante $A \subseteq A' \subseteq A'' \subseteq \cdots$ obtenue en itérant la construction $A \mapsto \mathrm{End}_I(A)$, pour $I = \sqrt{\mathrm{Fitt}(\Omega^1_{A/k})}$, est stationnaire. D'après (ii), sa limite est le normalisé $\widetilde{A}$ que l'on souhaite calculer.

15.5.3. La méthode précédente ne dit rien sur le nombre d'opérations à faire : on s'arrête simplement lorsque le morphisme d'inclusion d'un terme dans le suivant est un isomorphisme, condition que l'on sait tester (14.2). L'existence de bornes *a priori*, mais non calculables, est connue [van den Dries et Schmidt 1984, §3] mais inutile ici. On se propose ici de montrer que l'on peut contrôler cette terminaison par un calcul de multiplicité et ainsi calculer la normalisation sans faire de recherche non bornée.

Rappelons [Serre 1965, IV, théorème 11] qu'un anneau est normal si et seulement si il est R_1, c'est-à-dire régulier en codimension 1, et satisfait la condition S_2 de Serre [ÉGA IV$_2$ 1965, 5.7.2].

La condition S_2 est facile à satisfaire : si P est une sous-k-algèbre de polynômes de A telle que $P \to A$ soit fini, et que l'on note $D(-) = \mathrm{Hom}_P(-, P)$, le bidual $B = D(D(A))$ est S_2 et est la S_2-ification de A, c'est-à-dire que $A \to B$ est la plus petite extension finie contenue dans l'anneau total des fractions de A qui soit S_2. Voir [Vasconcelos 2005, proposition 6.21 ; Huneke et Swanson 2006, démonstration du théorème 15.3.3 et exercices 15.9 et 15.12]. (La multiplication sur B utilisée ici provient de son plongement dans le corps des fractions de A ; mais elle peut aussi se définir de façon intrinsèque : si $\xi, \eta \in D(D(A))$ sont vues comme des formes P-linéaires sur $D(A)$, leur produit est la forme P-linéaire sur $D(A)$ qui à $\varphi \in D(A)$ associe $\eta(x \mapsto \xi(y \mapsto \varphi(xy)))$ — cette multiplication du bidual, appelée « multiplication d'Arens » par les analystes dans le contexte des algèbres de Banach, cf. [Palmer 1974], n'est pas commutative en général, mais il est facile de se convaincre qu'elle l'est, et qu'elle coïncide bien avec la restriction de la multiplication sur $\mathrm{Frac}(A)$, dans le cas où on s'est placé, cf. [Madore 2014].) Voir aussi [ÉGA IV$_2$ 1965, §5.10] et [Achar et Sage 2009] pour une présentation intrinsèque de S_2-ification. Or P est calculable en utilisant une démonstration explicite du lemme de normalisation de Noether ([Eisenbud 1995, théorème 13.3 en utilisant le lemme 13.2(a)] ou [Serre 1965, III(D)2, théorème 2]), on sait décrire explicitement A comme un P-module de type fini d'après la remarque faite en 14.6, on peut en déduire la structure de B comme P-module d'après 13.4, et bien sûr comme algèbre (13.6.1, puisque la multiplication sur $D(D(A))$ est calculable).

D'autre part, si A est R_1, il en est de même de B (en fait, $A \to DD(A)$ est un isomorphisme en codimension 1 ; cf. [Huneke et Swanson 2006, exercice 15.11]).

Ceci nous ramène donc à normaliser (= régulariser) en codimension 1. D'après la proposition précédente (i), on peut trouver un élément non nul f dans le conducteur $\mathfrak{c}$. Notons $\mathfrak{p} \in \mathrm{Spec}(A)$ un point maximal (de codimension 1) de $V(f)$, calculé par décomposition primaire de f. Soit B le localisé de A en $\mathfrak{p}$ et notons $\widetilde{B}$ le normalisé de B. La longueur de toute chaîne strictement croissante $B \subsetneq B' \subsetneq \cdots \subsetneq \widetilde{B}$ est majorée par l'entier $\mathrm{long}_B(\widetilde{B}/B)$ lui-même inférieur ou égal à $\mathrm{long}_B(\widetilde{B}/\mathfrak{c})$. Rappelons que ce dernier est égal à la multiplicité $\mathrm{mult}(\mathfrak{c}, B)$ de $\mathfrak{c}$ dans B, à son tour inférieur ou égal à $\mathrm{mult}((f), B)$, que l'on sait majorer (cf. 15.4). Ceci montre

que l'on a peut calculer une borne sur le nombre d'étapes pour rendre A régulier en codimension 1. [18]

Justifions brièvement l'égalité $\mathrm{long}_B(\widetilde{B}/\mathfrak{c}) = \mathrm{mult}(\mathfrak{c}, B)$. Soit $n \geq 1$ un entier ; on a $\mathrm{long}_B(\widetilde{B}/\mathfrak{c}^n) = \sum_{\mathfrak{q}}[\kappa(\mathfrak{q}) : \kappa(\mathfrak{p})] \cdot \mathrm{long}_{\widetilde{B}_\mathfrak{q}}(\widetilde{B}_\mathfrak{q}/\mathfrak{c}^n)$, où $\mathfrak{q}$ parcourt le spectre maximal (fini) de l'anneau de Dedekind semi-local $\widetilde{B}$. Par régularité des anneaux $\widetilde{B}_\mathfrak{q}$ et nouvelle application de cette formule (pour $n = 1$), on obtient l'égalité $\mathrm{long}_B(\widetilde{B}/\mathfrak{c}^n) = n \cdot \mathrm{long}_B(\widetilde{B}/\mathfrak{c})$ d'où $\mathrm{mult}(\mathfrak{c}, \widetilde{B}) = \mathrm{long}_B(\widetilde{B}/\mathfrak{c})$. Comme d'autre part $\mathrm{long}_B(\widetilde{B}/B)$ est finie, on a $\mathrm{mult}(\mathfrak{c}, \widetilde{B}) = \mathrm{mult}(\mathfrak{c}, B)$.

15.6. ***Lissité et étalitude.*** Soient A un anneau, $P = A[X_1, \ldots, X_n]$ un anneau de polynômes sur A et B le quotient de P par un idéal de type fini I. Considérons le B-module $\mathrm{Ext}^1_B(\mathbb{L}_{B/A}, I/I^2)$, où $\mathbb{L}_{B/A}$ est le complexe cotangent. D'après [Illusie 1971, III.1.2.9.1], ce module est naturellement isomorphe au quotient $\mathrm{End}_B(I/I^2)/d^\star\mathrm{Hom}_P(\Omega^1_{P/A}, I/I^2)$, où d désigne la dérivation $I/I^2 \to \Omega^1_{P/A} \otimes_P B$. On peut donc en déterminer la structure (cf. 13.4). Notons $H_A(P, I)$ son idéal annulateur en tant que P-module ; d'après une variante du critère jacobien [Gabber et Ramero 2003, 5.4.2], le lieu lisse (à la source) du morphisme $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ est l'ouvert complémentaire du fermé Σ défini par l'idéal image de $H_A(P, I)$ dans B. (Un avantage de cette description est que, contrairement à la description plus classique du lieu singulier par un idéal de Fitting du B-module $\Omega^1_{B/A}$ (cf. 15.5), elle ne fait pas d'hypothèse d'équidimensionalité ou de platitude.) On trouve en [Gabber et Ramero 2003, §5.4.5] et [Elkik 1973, §0.2] une variante moins intrinsèque mais plus explicite qui, donnés des générateurs $\{f_1, \ldots, f_r\}$ de I, produit — par dérivation de ces générateurs et opérations élémentaires sur les idéaux de P (cf. 13.2 et 13.3) — un idéal contenu dans $H_A(P, I)$ et définissant également le fermé Σ.

Il résulte de ce qui précède que l'on peut tester si le morphisme de présentation finie $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ est *lisse*, par exemple lorsque A est une algèbre de type fini sur un corps. Pour vérifier s'il est *étale*, il suffit de vérifier si les fibres au-dessus des points maximaux de $\mathrm{Spec}(A)$ (c'est-à-dire les points génériques des composantes irréductibles, calculables d'après 15.2) sont vides ou de dimension nulle.

15.7. ***Présentation d'un pincement.***

Définition 15.7.1. Soit A un anneau et I un idéal de A. On définit une A-algèbre B en munissant le A-module $A \oplus I$ de la multiplication donnée par $(a, u) \cdot (b, v) = (ab, av + bu + uv)$. On dit que B est la A-algèbre obtenue par *pincement de A le long de I*.

Remarquons que B peut aussi se voir comme la A-algèbre $A \times_{A/I} A$ — en identifiant le couple (a, u) de $A \oplus I$ à $(a, a + u)$ de $A \times_{A/I} A$ — ou comme la

18. Cette technique nous a été suggérée par O. Gabber.

A-algèbre obtenue en ajoutant une unité à l'idéal I vu comme une A-algèbre-non-unitaire.

Proposition 15.7.2. *Soient k un corps, $A = k[t_1, \dots, t_d]/(u_1, \dots, u_q)$ une k-algèbre de type fini explicitement présentée et I l'idéal de A engendré par des éléments $x_1, \dots, x_r$ de A, images d'éléments $\hat{x}_1, \dots, \hat{x}_r$ de $k[t_1, \dots, t_d]$. Alors on peut trouver algorithmiquement une présentation explicite de l'algèbre $B = A \oplus I$ obtenue par pincement de A le long de I (cf. 15.7.1).*

Démonstration. Le A-module B est engendré par $1, x_1, \dots, x_r$. D'après 13.3, on sait trouver algorithmiquement des générateurs $y_1, \dots, y_s$ des relations linéaires entre les $x_1, \dots, x_r$ (donc entre les $1, x_1, \dots, x_r$). Quitte à écrire chaque $x_i x_j$ comme combinaison de $x_1, \dots, x_r$, on trouve également des relations quadratiques $q_{i,j}$ telles que définies en 13.6.1, qui assure alors que les relations y_i et les $q_{i,j}$ définissent l'algèbre B comme un quotient de $A[t'_1, \dots, t'_r]$, donc, quitte à prendre leur relèvement et y ajouter les $u_1, \dots, u_q$, comme un quotient de $k[t_1, \dots, t_d, t'_1, \dots, t'_r]$. □

16. Schémas de type fini sur un corps : description algorithmique

On rappelle que les hypothèses 12.7 sont implicitement faites sur le corps k. Par ailleurs, nous ne parlerons ici que de schémas de type fini sur k, omettant fréquemment les mots « de type fini ».

16.1. ***Schémas affines et quasi-affines, morphismes entre iceux.*** On représentera un *schéma affine* (sous-entendu : de type fini) X sur un corps k par une algèbre de type fini R dont il est le spectre, cette algèbre R étant elle-même représentée comme un quotient $k[Z_1, \dots, Z_d]/I$ d'une algèbre de polynômes, c'est-à-dire par la donnée d'un ensemble (fini !) de générateurs de I, équations de X dans l'espace affine $\mathbb{A}^d_k$. Remarquons qu'on peut tester algorithmiquement si un tel schéma est vide (il s'agit exactement de tester si I est l'idéal unité).

On représentera un morphisme $X \to Y$ de k-schémas affines, où $X = \mathrm{Spec}(R)$ et $Y = \mathrm{Spec}(S)$ sont les spectres de deux k-algèbres de type fini R, S, comme un morphisme $S \to R$ de k-algèbres (cf. 14.2).

On représentera un schéma *quasi-affine*, c'est-à-dire un ouvert U d'un schéma affine X, au moyen d'un fermé dont il est le complémentaire (décrit par des équations f_i de ce fermé : ceci revient à écrire U comme la réunion des ouverts principaux $D(f_i)$). Remarquons que, à l'intérieur d'un schéma affine X fixé, on sait tester l'inclusion ou l'égalité entre des ouverts (cela revient à tester l'inclusion entre les radicaux des idéaux définissant les fermés : cf. 15.2 pour le calcul du radical).

Un morphisme d'un schéma affine X vers un schéma quasi-affine V ouvert complémentaire de Z dans un schéma affine Y sera décrit comme un morphisme $X \to Y$ qui se factorise par V : ce fait est testable algorithmiquement en testant

si l'image réciproque de Z par $X \to Y$ est vide (c'est-à-dire si l'algèbre produit tensoriel de celles de X et Z au-dessus de celle de Y est nulle).

Un morphisme d'un schéma quasi-affine U ouvert d'un schéma affine X, vers un schéma quasi-affine V, sera décrit comme une collection de morphismes $U_i \to V$ qui coïncident sur $U_i \cap U_j$, où les U_i sont les ouverts affines principaux recouvrant U (c'est-à-dire les $D(f_i)$ avec f_i parcourant des équations d'un fermé dont U est le complémentaire dans X : on sait écrire des équations de $D(f_i)$ comme schéma affine en le considérant comme une hypersurface d'équation $Tf_i - 1$ au-dessus de X, où T est une nouvelle indéterminée ; et on peut représenter l'ouvert affine $U_i \cap U_j$ comme $D(f_i f_j)$). De nouveau, on peut calculer la composée de tels morphismes entre schémas quasi-affines, et tester l'égalité de deux d'entre eux (même si le quasi-affine U de départ n'est pas représenté par le même recouvrement par des $D(f_i)$: il suffit de prendre un raffinement commun entre deux recouvrements, ce qui est facile).

16.2. ***Description des schémas et de leurs morphismes.*** On représentera un *schéma* (sous-entendu : de type fini) X sur un corps k par la donnée d'un nombre fini de schémas affines U_i et, pour chacun, d'un recouvrement $V_{ii'}$ par des ouverts quasi-affines (les variables i et i' parcourent ici le même ensemble fini) et, pour chaque paire i, i', d'un morphisme $\varphi_{ii'} : V_{ii'} \to V_{i'i}$ vérifiant la condition de compatibilité que ($V_{ii} = U_i$ et $\varphi_{ii} = \mathrm{Id}_{U_i}$ et que) $\varphi_{i_2 i_3} \circ \varphi_{i_1 i_2}$ et $\varphi_{i_1 i_2}$ coïncident là où tous deux sont définis (en particulier, les $\varphi_{ii'}$ sont des isomorphismes). Toutes ces conditions sont bien testables algorithmiquement, et le schéma X défini est alors le recollement des U_i en identifiant l'ouvert $V_{ii'}$ de U_i avec l'ouvert $V_{i'i}$ de $U_{i'}$ au moyen de $\varphi_{ii'}$. On dit aussi que les U_i (avec les autres données les accompagnant) constituent un *atlas* affine de X. Un *raffinement* d'un tel atlas est un atlas obtenu en remplaçant chaque U_i par un recouvrement de celui-ci par des ouverts affines principaux U_{ij} (ici le j parcourt un ensemble fini qui peut dépendre de i), avec les données évidemment déduites de ce recouvrement.

On représentera un morphisme de schémas $X \to Y$, décrits par des atlas U_i pour X et V_j pour Y, en se donnant un raffinement U_{ij} de l'atlas initial de X et des morphismes $U_{ij} \to V_j$ de schémas affines, qui se recollent aux intersections décrites par l'atlas.

Notons qu'on peut algorithmiquement calculer la composée de morphismes de schémas ainsi décrits, et par ailleurs que, donnés deux morphismes $X \to Y$ entre les deux mêmes schémas décrits par les *mêmes* atlas, on peut tester leur égalité (ceci se fait en prenant un raffinement commun aux deux atlas de X qui décrivent les morphismes à comparer, ce qu'on peut faire puisqu'il s'agit de raffiner des recouvrements de mêmes schémas affines U_i).

Remarquons aussi que si dans la définition d'un schéma on ne suppose plus les U_i affines mais que ce sont des schémas plus généraux (autrement dit, si on cherche

à recoller un atlas formé de schémas non nécessairement affines), on peut encore se ramener algorithmiquement à la situation où ils sont affines (quitte à remplacer chaque schéma U_i par un atlas affine qui le décrit).

Nous ne prétendons pas qu'il soit possible de tester l'égalité (l'isomorphisme) de deux schémas décrits par des atlas (ceci sera néanmoins possible dans le cas étale : cf. 17.3 ci-dessous). Remarquons à ce sujet que dans la suite si nous écrivons par exemple « si Z est affine » il faut comprendre « si on s'est donné une description de Z comme schéma affine » et pas « si on s'est donné une description de Z comme un schéma général, et qu'il s'avère que Z est affine [chose qu'on ne sait pas tester] » : ceci ne devrait pas prêter à confusion.

En fait, à ce stade de la description, nous ne savons même pas encore tester si un morphisme *donné* entre schémas est un isomorphisme (ceci, en revanche, sera bien décidable : cf. 16.5).

16.3. ***Produits fibrés de schémas.*** Donnés X, Y, Z trois schémas (i.e., k-schémas de type fini) décrits comme précédemment, et donnés $X \to Z$ et $Y \to Z$ deux morphismes, on peut algorithmiquement calculer le produit fibré $X \times_Z Y$. En effet, si X, Y, Z sont affines (disons $X = \operatorname{Spec} R$, $Y = \operatorname{Spec} S$ et $Z = \operatorname{Spec} A$), il s'agit de calculer un produit tensoriel de k-algèbres de type fini, or on a vu en 14.2 qu'on pouvait calculer des présentations finies de R et S comme A-algèbres, auquel cas leur produit tensoriel se calcule simplement en réunissant les générateurs et les relations. La démonstration dans le cas général suit celle de [ÉGA I 1960, 3.2.6] : si Z est toujours supposé affine mais que X, Y ne le sont plus, on obtient un atlas de $X \times_Z Y$ comme en [ÉGA I 1960, 3.2.6.3], en prenant les $U_i \times_Z V_j$ pour U_i parcourant un atlas de X et V_j de Y ; si Z n'est plus supposé affine, étant donné un atlas W_i de Z, la donnée même des morphismes $X \to Z$ et $Y \to Z$ fournit des atlas de X et Y appropriés à les représenter, c'est-à-dire par des $U_i \to W_i$ où U_i est un ouvert de X (non nécessairement affine, mais réunion d'ouverts affines) et $V_i \to W_i$ de même, on peut donc calculer les produits fibrés $U_i \times_{W_i} V_i$ comme on vient de le dire, et les recoller à leur tour.

Dans le cas où $X = Y$, en recollant les morphismes $R \otimes_A R \to R$ (de multiplication, qui ne posent pas de difficulté à décrire algorithmiquement), on obtient une description de la diagonale $X \to X \times_Z X$ d'un morphisme $X \to Z$ quelconque.

16.4. ***Pincement (cas non nécessairement affine).*** On renvoie à [Ferrand 2003] pour la question générale de l'existence des pincements dans la catégorie des schémas, dont on tire notamment (théorème 7.1(B)) le fait que la somme amalgamée (= « pincement ») $X \amalg_F X$ est représentable dans la catégorie des schémas lorsque X est un schéma et F un sous-schéma fermé de X, et plus exactement, représentée par la même somme amalgamée dans la catégorie des espaces annelés.

On a vu en 15.7.2 comment calculer algorithmiquement ce pincement si X est un schéma affine de type fini sur un corps k (si $X = \operatorname{Spec} A$ et $F = \operatorname{Spec}(A/I)$ avec I un idéal de A, alors $X \amalg_F X = \operatorname{Spec}(A \oplus I)$ où $A \oplus I$ est muni de la structure d'algèbre décrite en 15.7.1). Remarquons par ailleurs que la construction est fonctorielle : si $\varphi\colon A \to A'$ est un morphisme d'algèbres et $I' = \varphi(I)\,A'$ l'idéal engendré dans A' par l'image de l'idéal I de A, alors $(A \oplus I) \to (A' \oplus I')$ défini par $(a, u) \mapsto (\varphi(a), \varphi(u))$ est bien un morphisme d'algèbres.

Si X est un schéma de type fini sur k et U un ouvert affine de X, alors d'après [Ferrand 2003, lemme 4.4] $U \amalg_V U$ est un ouvert de $X \amalg_F X$, où V désigne l'ouvert $F \cap U$ de F : ces ouverts sont calculables algorithmiquement d'après ce qu'on vient de dire (il est clair que $F \cap U$ est calculable, au besoin d'après 16.3), ils recouvrent $X \amalg_F X$, et si U, U' sont deux ouverts affines de X, l'ouvert quasi-affine $(U \amalg_V U) \cap (U' \amalg_{V'} U') = (U \cap U') \amalg_{V \cap V'} (U \cap U')$ se décrit comme réunion des $U'' \amalg_{V''} U''$ pour $U'' \subseteq U \cap U'$ et s'envoie vers $U \amalg_V U$ et $U' \amalg_{V'} U'$ par les morphismes de fonctorialité (cf. ci-dessus). Ceci fournit donc une description de $X \amalg_F X$ au sens de 16.2.

16.5. ***Immersions ouvertes et isomorphismes de schémas.*** Donné un schéma X décrit par un atlas d'ouverts affines $U_i = \operatorname{Spec} R_i$ (dont on notera $V_{ij} = U_i \cap U_j$ les intersections deux à deux que l'atlas identifie) et un schéma Y que nous supposons dans un premier temps affine $Y = \operatorname{Spec} S$, on peut tester algorithmiquement si un morphisme $X \to Y$ est une immersion ouverte : en effet, pour ceci, il faut et il suffit que chacun des $U_i \to Y$ soient des immersions ouvertes, et que l'intersection (dans Y) des images de U_i et U_j coïncide avec V_{ij} en tant qu'ouvert de U_i ; or d'après 14.5 on sait tester si $U_i \to Y$ est une immersion ouverte, on peut calculer $U_i \cap U_j$ dans Y comme $\operatorname{Spec}(R_i \otimes_S R_j)$, et tester si l'ouvert en question de $U_i = \operatorname{Spec} R_i$ coïncide bien avec V_{ij}.

Le cas où le schéma Y cible n'est plus supposé affine ne pose pas de difficulté : le morphisme est décrit dans des atlas adaptés, et il est une immersion ouverte si et seulement si sa restriction à chaque carte de la cible est une immersion ouverte.

On peut également tester algorithmiquement si un morphisme $X \to Y$ de schémas est un isomorphisme et, le cas échéant, calculer sa réciproque. En effet, en considérant d'abord le cas où Y est affine, ceci se fait en testant d'abord s'il s'agit d'une immersion ouverte comme décrit par le pénultième paragraphe dont nous reprenons les notations, puis, si c'est bien le cas, en vérifiant que les U_i recouvrent Y, ce qui se fait en calculant (toujours par 14.5) un fermé complémentaire de U_i dans Y, ce qui permet de tester si l'intersection de ces fermés est vide (les équations qui les décrivent engendrent l'idéal unité de S) ; le cas échéant, les ouverts principaux dont les U_i sont écrits comme réunion forment un atlas de Y pour lequel l'écriture de l'isomorphisme réciproque est claire. Le cas où Y n'est pas affine ne présente pas

de difficulté nouvelle (il s'agit, de nouveau, d'être un isomorphisme en restriction à chaque carte de la cible).

16.6. ***Réduit, composantes irréductibles, composantes connexes.*** On peut tester algorithmiquement si un schéma est réduit, ou bien calculer son réduit : en effet, X est réduit si et seulement si chacun des ouverts affines constituant un atlas de X l'est, ce qui ramène à tester si une k-algèbre de type fini est réduite, donc si un idéal d'un anneau de polynômes est radical (cf. 15.2) ; et réduire X se fait en réduisant chaque carte d'un atlas de X (les morphismes de recollement passent au réduit grâce à la fonctorialité de celui-ci).

De même, on peut tester algorithmiquement si un schéma est irréductible, ou bien calculer ses composantes irréductibles.

Enfin, en testant parmi les composantes irréductibles celles dont l'intersection est vide (on a déjà observé ci-dessus qu'on pouvait tester si un schéma est vide), on peut calculer algorithmiquement les composantes connexes d'un schéma.

16.7. ***Image fermée, immersions fermées.*** Si $X \to Y$ est un morphisme de schémas, on peut en calculer algorithmiquement l'image fermée schématique (c'est-à-dire, [ÉGA I 1960, 9.5], le plus petit sous-schéma fermé Y' de Y par lequel le morphisme $X \to Y$ se factorise, et bien sûr on cherche aussi à calculer la factorisation en question) : en effet, si on suppose d'abord que $Y = \operatorname{Spec} S$ est affine, et si X est décrit par un atlas d'ouverts affines $U_i = \operatorname{Spec} R_i$, alors $Y' = \operatorname{Spec}(S/N)$ où N est l'intersection des noyaux de tous les $S \to R_i$ décrivant le morphisme (cf. [ÉGA I 1960, 9.5.2]). Si Y n'est plus supposé affine, de nouveau, il suffit d'effectuer cette construction localement.

Grâce à cette construction, on peut tester si un morphisme de schémas $X \to Y$ est une immersion fermée : en effet, cela revient à tester si la factorisation $X \to Y'$, où Y' est l'image fermée schématique décrite ci-dessus, est un isomorphisme, et on a vu comment tester ce fait.

On peut également tester si un morphisme de schémas est dominant (c'est-à-dire d'image dense), puisque cela signifie précisément que son réduit est schématiquement dominant (c'est-à-dire que son image fermée schématique, définie ci-dessus, est toute la cible).

16.8. ***Image d'un morphisme, surjectivité.*** Si $X \to Y$ est un morphisme de schémas, on peut tester algorithmiquement s'il est surjectif, ou même calculer son image (une partie constructible de Y, décrite comme combinaison booléenne de fermés de Y). En effet, cette image est caractérisée par l'ensemble de ses points à valeurs dans la clôture algébrique de k (on rappelle que nous ne considérons ici que des schémas de type fini sur k ; cf. [ÉGA I 1971, proposition 7.1.8 et sa démonstration]), or pour k algébriquement clos il est algorithmique de calculer l'image d'une partie

constructible de k^n par la projection sur un sous-ensemble de ses coordonnées [Fried et Jarden 2008, théorème 9.3.1], ce qui suffit à calculer l'image de $X(k)$ par f comme la projection du graphe de f.

16.9. ***Morphismes et schémas séparés, radiciels.*** On peut tester si un morphisme de schémas est séparé, resp. radiciel, en testant si sa diagonale (qu'on sait calculer d'après 16.3) est une immersion fermée [ÉGA I 1960, 5.4.1], resp. une surjection [ÉGA IV$_1$ 1964, 1.8.7.1], ce qu'on sait tester d'après 16.7, resp. 16.8.

16.10. ***Détection de points.*** Expliquons brièvement pourquoi, donné un schéma X non vide sur k, on peut algorithmiquement en expliciter un point géométrique, c'est-à-dire un point sur « la » clôture algébrique de k. Comme il suffit de trouver un point d'un ouvert affine de X, on peut évidemment supposer que X est affine. Le cas où X est un fermé de la droite affine $\mathbb{A}^1_k$ est trivial (s'il est décrit comme l'ensemble $\{f = 0\}$ des zéros d'un polynôme f, on considère une racine de f dans la clôture algébrique de k), et le cas où X est un ouvert de $\mathbb{A}^1_k$ ne l'est pas moins (si l'ouvert en question est d'écrit comme $\{f \neq 0\}$, on peut considérer le fermé $\{f = 1\}$ qui y est contenu, se ramenant ainsi au cas précédent). Dans le cas général, on procède par récurrence sur la dimension de l'espace affine dans lequel X est inclus : si π est la projection sur une coordonnée, alors $\pi(X)$ est calculable d'après 16.8, on peut trouver un point géométrique de $\pi(X) \subseteq \mathbb{A}^1_k$ d'après ce qui vient d'être dit, et on est ramené au même problème dans la fibre de π au-dessus de ce point.

16.11. ***Passage à la limite.*** Soient k_0 un corps, X_0 un k_0-schéma séparé de type fini et k/k_0 une extension algébrique (non nécessairement finie). On note X le produit fibré $X_0 \times_{k_0} k$ et on suppose donné un morphisme de type fini $f : T \to X$. Alors, on peut construire une extension *finie* k_1/k_0 et un morphisme $f_1 : T_1 \to X_1 = X_0 \times_{k_0} k_1$ induisant le morphisme f par changement de base : il suffit de considérer le sous-corps de k engendré des coefficients définissant f. Si f est étale, on peut supposer qu'il en est de même de k_1/k_0 (par invariance topologique du site étale).

17. Géométrie algébrique effective

On rappelle que les hypothèses 12.7 sont implicitement faites sur le corps k, et que les schémas sur k sont supposés de type fini.

17.1. ***Dimension.*** Grâce au calcul de la fonction de Hilbert (cf. 15.1), il est possible de calculer la dimension d'un schéma (cf. [Cox, Little et O'Shea 2007, §9.3]), ou la dimension de ses composantes connexes et irréductibles.

17.2. ***Lissité et étalitude.*** Les propriétés d'être lisse ou étale étant locales, le fait de pouvoir tester cette propriété sur un morphisme d'algèbres (15.6) permet de tester si un morphisme de schémas est lisse, resp. étale.

17.3. ***Sections et isomorphismes de morphismes étales.*** On peut décider algorithmiquement si un morphisme étale séparé $X \to S$ admet une section. En effet, d'après [ÉGA IV$_4$ 1967, 17.4.9] (ou bien [Milne 1980, corollaire I.3.12]), c'est le cas si et seulement si sa restriction à une réunion de composantes connexes de X est un isomorphisme.

Par conséquent, on peut aussi décider si deux morphismes étales finis $X \to S$ et $Y \to S$ sont S-isomorphes. Pour s'en convaincre, constatons d'abord qu'on peut calculer le morphisme $\underline{\mathrm{Isom}}_S(X, Y) \to S$ où $\underline{\mathrm{Isom}}$ est le schéma paramétrant les S-isomorphismes $X \to Y$: ses équations s'écrivent explicitement en fonction de celles de X et Y. Plus exactement, on peut décrire $\underline{\mathrm{Isom}}_S(X, Y)$ comme le fermé des $(u, v) \in \underline{\mathrm{Hom}}_S(X, Y) \times_S \underline{\mathrm{Hom}}_S(Y, X)$ défini par les équations $v \circ u = \mathrm{Id}_X$ et $u \circ v = \mathrm{Id}_Y$, où $\underline{\mathrm{Hom}}_S(X, Y)$ (aussi noté $\mathfrak{R}_{X/S}(Y \times_S X)$, où $\mathfrak{R}$ désigne la restriction à la Weil) est le schéma paramétrant les morphismes $X \to Y$: voir [Bosch, Lütkebohmert et Raynaud 1990, §7.6, notamment théorème 4], dont la démonstration fournit une description explicite de ce schéma (cf. aussi [Debarre 2001, chapitre 2]). Comme $\underline{\mathrm{Isom}}_S(X, Y) \to S$ est lui-même étale fini quand X et Y le sont, et que savoir si X et Y sont isomorphes sur S revient à savoir s'il a une section, ce qui nous ramène à la question précédente.

17.4. ***Proj.*** Soient r un entier, k un corps et S l'algèbre graduée de polynômes $k[x_0, \ldots, x_r]$, où les variables x_i sont de degré 1. On va montrer que pour chaque un S-module gradué de type fini M, on peut calculer le k-module de type fini $\mathrm{H}^0(\mathbb{P}^r_k, \mathcal{M})$, où $\mathcal{M}$ désigne le faisceau quasi-cohérent naturellement associé à M [ÉGA II 1961, 2.5]. Rappelons [Serre 1955, chapitre III, §4, ¶ 69, corollaire 2], que l'on a $\mathrm{H}^0(\mathbb{P}^r_k, \mathcal{M}) = \mathrm{colim}_\nu \mathrm{Hom}_S((x_0^\nu, \ldots, x_r^\nu), M)_0$. (L'indice 0 indique que l'on ne considère que les morphismes de degré nul.) Étant donné une résolution libre (de type fini) $L_\bullet$ de M — que l'on peut déduire d'une présentation de M comme conoyau d'un morphisme $L_1 \to L_0$ entre S-modules gradués libres de type fini —, il résulte de [Serre 1955, chapitre III, §3, ¶ 63, proposition 3(a)] que l'on a égalité $\mathrm{H}^0(\mathbb{P}^r_k, \mathcal{M}) = \mathrm{Hom}_S((x_0^\nu, \ldots, x_r^\nu), M)_0$ dès que $\nu + r$ est supérieur à chaque entier n tel que $S(-n)$ apparaisse comme facteur direct des L_i. Rappelons qu'un S-module gradué libre est somme directe de modules $S(n)$, où $n \in \mathbb{Z}$ et $S(n)$ est le S-module S muni de la graduation $S(n)_i = S_{n+i}$. (Un tel ν est aussi lié à la « régularité », au sens de Mumford–Castelnuovo, de M, cf. [Bayer et Mumford 1993, définition 3.2].)

Pour le calcul d'une résolution libre, cf. 15.1.

17.5. ***Application.*** Soient k un corps et $X = V(I) \subseteq \mathbb{P}^r_k$ un schéma projectif. Il résulte de ce qui précède (et des résultats de la section 13) que l'on peut calculer $\mathrm{H}^0(X, \mathcal{O}_X) = \mathrm{H}^0(\mathbb{P}^r_k, \mathcal{O}_{\mathbb{P}^r_k}/I)$. En particulier, on peut vérifier si la flèche naturelle $k \to \mathrm{H}^0(X, \mathcal{O}_X)$ est un isomorphisme : ceci fournit une approche alternative à 16.6 pour le calcul des composantes connexes géométriques d'une variété projective.

La même approche, en remplaçant k par une k-algèbre A de type fini (qu'on peut supposer être une algèbre de polynômes) permettrait de calculer la factorisation de Stein d'un morphisme projectif $f\colon Y \to \operatorname{Spec} A$ en calculant la A-algèbre $f_\star \mathcal{O}_Y$: on pourrait en déduire la même chose pour $f\colon Y \to X$ sur une base non nécessairement affine.

Remerciements

Nous remercions chaleureusement Ofer Gabber auquel nous sommes redevables de plusieurs arguments importants et pour ses suggestions particulièrement utiles. À divers titres nous remercions également Pierre Deligne, Luc Illusie, Jean Lannes, Grégoire Lecerf, Henri Lombardi, Ronald van Luijk, Jean-Pierre Serre, Lenny Taelman, et Olivier Wittenberg. Le second auteur sait également gré à Ahmed Abbes et Weizhe Zheng (郑维喆) de leurs invitations, respectivement à l'IHÉS et au centre Morningside (晨兴数学中心).

Bibliographie

[Abbes et Gros 2011] A. Abbes et M. Gros, "Topos co-évanescents et généralisations", prépublication, 2011. arXiv 1107.2380v3

[Achar et Sage 2009] P. N. Achar et D. S. Sage, "Perverse coherent sheaves and the geometry of special pieces in the unipotent variety", *Adv. Math.* **220**:4 (2009), 1265–1296. MR 2010a:20093 Zbl 1168.20018

[Anderson 1987] G. W. Anderson, "Torsion points on Fermat Jacobians, roots of circular units and relative singular homology", *Duke Math. J.* **54**:2 (1987), 501–561. MR 89g:14012

[Anderson 2002] G. W. Anderson, "Abeliants and their application to an elementary construction of Jacobians", *Adv. Math.* **172**:2 (2002), 169–205. MR 2004c:14056 Zbl 1065.14035

[Artin 1971] M. Artin, "On the joins of Hensel rings", *Advances in Math.* **7** (1971), 282–296. MR 44 #6690 Zbl 0242.13021

[Artin 1973] M. Artin, *Théorèmes de représentabilité pour les espaces algébriques*, Séminaire de Mathématiques Supérieures **44**, Presses de l'Université de Montréal, 1973. MR 53 #10794 Zbl 0323.14001

[Artin et Mazur 1969] M. Artin et B. Mazur, *Etale homotopy*, Lecture Notes in Mathematics **100**, Springer, Berlin, 1969. MR 39 #6883 Zbl 0182.26001

[Avigad 2003] J. Avigad, "Number theory and elementary arithmetic", *Philos. Math.* (3) **11**:3 (2003), 257–284. MR 2004g:03099 Zbl 1050.03005

[Bayer et Mumford 1993] D. Bayer et D. Mumford, "What can be computed in algebraic geometry ?", pp. 1–48 dans *Computational algebraic geometry and commutative algebra* (Cortona, 1991), édité par D. Eisenbud et L. Robbiano, Symposia Mathematica **34**, Cambridge Univ. Press, New York, 1993. MR 95d:13032 Zbl 0846.13017

[Becker et Weispfenning 1993] T. Becker et V. Weispfenning, *Gröbner bases: a computational approach to commutative algebra*, Graduate Texts in Mathematics **141**, Springer, New York, 1993. MR 95e:13018 Zbl 0772.13010

[Bhatt 2012] B. Bhatt, "Derived splinters in positive characteristic", *Compos. Math.* **148**:6 (2012), 1757–1786. MR 2999303 Zbl 1291.14036

[Borceux 1994] F. Borceux, *Handbook of categorical algebra, I: Basic category theory*, Encyclopedia of Mathematics and its Applications **50**, Cambridge Univ. Press, 1994. MR 96g:18001a Zbl 0803.18001

[Bosch, Lütkebohmert et Raynaud 1990] S. Bosch, W. Lütkebohmert et M. Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) **21**, Springer, Berlin, 1990. MR 91i:14034 Zbl 0705.14001

[Bourbaki 1981] N. Bourbaki, *Éléments de mathématique: Algèbre, chapitres 4 à 7*, Deuxième éd., Masson, Paris, 1981. MR 84d:00002 Zbl 1139.12001

[Bürgisser, Clausen et Shokrollahi 1997] P. Bürgisser, M. Clausen et M. A. Shokrollahi, *Algebraic complexity theory*, Grundlehren der Mathematischen Wissenschaften **315**, Springer, Berlin, 1997. MR 99c:68002 Zbl 1087.68568

[Carlson 2001] J. F. Carlson, "Calculating group cohomology: tests for completion", *J. Symbolic Comput.* **31**:1-2 (2001), 229–242. MR 2002c:20083 Zbl 0979.20047

[Conrad 2003] B. Conrad, "Cohomological Descent", notes, 2003, voir http://math.stanford.edu/~conrad/papers/hypercover.pdf.

[Cox, Little et O'Shea 2007] D. Cox, J. Little et D. O'Shea, *Ideals, varieties, and algorithms*, Troisième éd., Springer, New York, 2007. MR 2007h:13036 Zbl 1118.13001

[Debarre 2001] O. Debarre, *Higher-dimensional algebraic geometry*, Springer, New York, 2001. MR 2002g:14001 Zbl 0978.14001

[Decker et Lossen 2006] W. Decker et C. Lossen, *Computing in algebraic geometry*, Algorithms and Computation in Mathematics **16**, Springer, Berlin, 2006. MR 2007b:14129 Zbl 1095.14001

[Deligne 1974] P. Deligne, "Théorie de Hodge, III", *Inst. Hautes Études Sci. Publ. Math.* 44 (1974), 5–77. MR 58 #16653b Zbl 0237.14003

[Deligne 1980] P. Deligne, "La conjecture de Weil, II", *Inst. Hautes Études Sci. Publ. Math.* 52 (1980), 137–252. MR 83c:14017 Zbl 0456.14014

[Deligne et al. 1982] P. Deligne, J. S. Milne, A. Ogus et K.-y. Shih, *Hodge cycles, motives, and Shimura varieties*, Lecture Notes in Mathematics **900**, Springer, Berlin-New York, 1982. MR 84m:14046 Zbl 0465.00010

[Dixon et al. 1999] J. D. Dixon, M. P. F. du Sautoy, A. Mann et D. Segal, *Analytic pro-p groups*, Deuxième éd., Cambridge Studies in Advanced Mathematics **61**, Cambridge Univ. Press, 1999. MR 2000m:20039 Zbl 0934.20001

[Dold et Puppe 1961] A. Dold et D. Puppe, "Homologie nicht-additiver Funktoren: anwendungen", *Ann. Inst. Fourier Grenoble* **11** (1961), 201–312. MR 27 #186 Zbl 0098.36005

[van den Dries et Schmidt 1984] L. van den Dries et K. Schmidt, "Bounds in the theory of polynomial rings over fields: a nonstandard approach", *Invent. Math.* **76**:1 (1984), 77–91. MR 85i:12016 Zbl 0539.13011

[Edixhoven et Couveignes 2011] B. Edixhoven et J.-M. Couveignes (éditeurs), *Computational aspects of modular forms and Galois representations*, Annals of Mathematics Studies **176**, Princeton Univ. Press, 2011. MR 2849700 Zbl 1216.11004

[ÉGA I 1960] A. Grothendieck, "Éléments de géométrie algébrique, I: Le langage des schémas", *Inst. Hautes Études Sci. Publ. Math.* **4** (1960), 5–228. Rédigés avec la collaboration de Jean Dieudonné. MR 29 #1207 Zbl 0118.36206

[ÉGA I 1971] A. Grothendieck et J. A. Dieudonné, *Éléments de géométrie algébrique, I*, Grundlehren der Mathematischen Wissenschaften **166**, Springer, Berlin, 1971. MR 3075000 Zbl 0203.23301

[ÉGA II 1961] A. Grothendieck, "Éléments de géométrie algébrique, II: Étude globale élémentaire de quelques classes de morphismes", *Inst. Hautes Études Sci. Publ. Math.* **8** (1961), 5–222. Rédigés avec la collaboration de Jean Dieudonné. MR 0163909 Zbl 0118.36206

[ÉGA III$_1$ 1961] A. Grothendieck, "Éléments de géométrie algébrique, III: Étude cohomologique des faisceaux cohérents, I", *Inst. Hautes Études Sci. Publ. Math.* **11** (1961), 5–167. Rédigés avec la collaboration de Jean Dieudonné. MR 0163910 Zbl 0118.36206

[ÉGA III$_2$ 1963] A. Grothendieck, "Éléments de géométrie algébrique, III: Étude cohomologique des faisceaux cohérents, II", *Inst. Hautes Études Sci. Publ. Math.* **17** (1963), 5–91. Rédigés avec la collaboration de Jean Dieudonné. MR 0163911 Zbl 0122.16102

[ÉGA IV$_1$ 1964] A. Grothendieck, "Éléments de géométrie algébrique, IV: Étude locale des schémas et des morphismes de schémas, I", *Inst. Hautes Études Sci. Publ. Math.* **20** (1964), 5–259. Rédigés avec la collaboration de Jean Dieudonné. MR 173675 Zbl 0136.15901

[ÉGA IV$_2$ 1965] A. Grothendieck, "Éléments de géométrie algébrique, IV: Étude locale des schémas et des morphismes de schémas, II", *Inst. Hautes Études Sci. Publ. Math.* **24** (1965), 5–231. Rédigés avec la collaboration de Jean Dieudonné. MR 0199181 Zbl 0135.39701

[ÉGA IV$_4$ 1967] A. Grothendieck, "Éléments de géométrie algébrique, IV: Étude locale des schémas et des morphismes de schémas, IV", *Inst. Hautes Études Sci. Publ. Math.* **32** (1967), 5–361. Rédigés avec la collaboration de Jean Dieudonné. MR 0238860 Zbl 153.22301

[ÉGA V] A. Grothendieck, "Pré-notes ÉGA V", 197?, voir http://www.jmilne.org/math/Documents/EGA-V.pdf.

[Eisenbud 1995] D. Eisenbud, *Commutative algebra*, Graduate Texts in Mathematics **150**, Springer, New York, 1995. MR 97a:13001 Zbl 0819.13001

[Elkik 1973] R. Elkik, "Solutions d'équations à coefficients dans un anneau hensélien", *Ann. Sci. École Norm. Sup.* (4) **6** (1973), 553–603. MR 49 #10692 Zbl 0327.14001

[Evens 1991] L. Evens, *The cohomology of groups*, Clarendon Press, Oxford Univ. Press, New York, 1991. MR 93i:20059 Zbl 0742.20050

[Faltings 1988] G. Faltings, "p-adic Hodge theory", *J. Amer. Math. Soc.* **1**:1 (1988), 255–299. MR 89g:14008 Zbl 0764.14012

[Ferrand 2003] D. Ferrand, "Conducteur, descente et pincement", *Bull. Soc. Math. France* **131**:4 (2003), 553–585. MR 2005a:13016 Zbl 1058.14003

[Fried et Jarden 2008] M. D. Fried et M. Jarden, *Field arithmetic*, Troisième éd., Ergebnisse der Mathematik und ihrer Grenzgebiete (3) **11**, Springer, Berlin, 2008. MR 2009j:12007 Zbl 1145.12001

[Friedlander 1982] E. M. Friedlander, *Étale homotopy of simplicial schemes*, Annals of Mathematics Studies **104**, Princeton Univ. Press, 1982. MR 84h:55012 Zbl 0538.55001

[Friedman 1999] H. Friedman, "Foundations of mathematics: grand conjectures", courriel à la liste de diffusion *Foundations of Mathematics*, 16 avril 1999, voir http://cs.nyu.edu/pipermail/fom/1999-April/003014.html.

[Friedman 2011] H. Friedman, "Boolean relation theory and incompleteness", prépublication, 2011, voir http://u.osu.edu/friedman.8/files/2014/01/0EntireBook061311-wh0yjy.pdf. À paraître dans Lecture Notes in Logic, Cambridge Univ. Press.

[Fröhlich et Shepherdson 1956] A. Fröhlich et J. C. Shepherdson, "Effective procedures in field theory", *Philos. Trans. Roy. Soc. London. Ser. A.* **248** (1956), 407–432. MR 17,570d Zbl 0070.03502

[Gabber 2001] O. Gabber, Lettre à F. Orgogozo, 28 décembre 2001.

[Gabber et Ramero 2003] O. Gabber et L. Ramero, *Almost ring theory*, Lecture Notes in Mathematics **1800**, Springer, Berlin, 2003. MR 2004k:13027 Zbl 1045.13002

[Gabriel et Zisman 1967] P. Gabriel et M. Zisman, *Calculus of fractions and homotopy theory*, Ergebnisse der Mathematik und ihrer Grenzgebiete **35**, Springer, New York, 1967. MR 35 #1019 Zbl 0186.56802

[Gianni, Trager et Zacharias 1988] P. Gianni, B. Trager et G. Zacharias, "Gröbner bases and primary decomposition of polynomial ideals", *J. Symbolic Comput.* **6**:2-3 (1988), 149–167. MR 90f:68091 Zbl 0667.13008

[Giraud 1971] J. Giraud, *Cohomologie non abélienne*, Grundlehren der mathematischen Wissenschaften **179**, Springer, Berlin-New York, 1971. MR 49 #8992 Zbl 0226.14011

[Grauert et Remmert 1984] H. Grauert et R. Remmert, *Coherent analytic sheaves*, Grundlehren der Mathematischen Wissenschaften **265**, Springer, Berlin, 1984. MR 86a:32001 Zbl 0537.32001

[Grothendieck 1956] A. Grothendieck, "Théorèmes de finitude pour la cohomologie des faisceaux", *Bull. Soc. Math. France* **84** (1956), 1–7. MR 18,327c Zbl 0071.17403

[Grothendieck 1957] A. Grothendieck, "Sur quelques points d'algèbre homologique", *Tôhoku Math. J.* (2) **9** (1957), 119–221. MR 21 #1328 Zbl 0118.26104

[Grothendieck et Murre 1971] A. Grothendieck et J. P. Murre, *The tame fundamental group of a formal neighbourhood of a divisor with normal crossings on a scheme*, Lecture Notes in Mathematics **208**, Springer, Berlin-New York, 1971. MR 47 #5000 Zbl 0216.33001

[Haiman et Sturmfels 2004] M. Haiman et B. Sturmfels, "Multigraded Hilbert schemes", *J. Algebraic Geom.* **13**:4 (2004), 725–769. MR 2005d:14006 Zbl 1072.14007

[Hájek et Pudlák 1998] P. Hájek et P. Pudlák, *Metamathematics of first-order arithmetic*, Springer, Berlin, 1998. MR 2000m:03003 Zbl 0889.03053

[Harrington et al. 1985] L. A. Harrington, M. D. Morley, A. Ščedrov et S. G. Simpson (éditeurs), *Harvey Friedman's research on the foundations of mathematics*, Stud. Logic Found. Math. **117**, North-Holland, Amsterdam, 1985. MR 87b:03004 Zbl 0588.03001

[Hess 2002] F. Hess, "Computing Riemann–Roch spaces in algebraic function fields and related topics", *J. Symbolic Comput.* **33**:4 (2002), 425–445. MR 2003j:14032 Zbl 1058.14071

[Hofstadter 1979] D. R. Hofstadter, *Gödel, Escher, Bach: an eternal golden braid*, Basic Books, New York, 1979. MR 80j:03009 Zbl 1014.03005

[Huneke et Swanson 2006] C. Huneke et I. Swanson, *Integral closure of ideals, rings, and modules*, London Math. Soc. Lecture Note Series **336**, Cambridge Univ. Press, 2006. MR 2008m:13013 Zbl 1117.13001

[Illusie 1971] L. Illusie, *Complexe cotangent et déformations, I*, Lecture Notes in Mathematics **239**, Springer, Berlin-New York, 1971. MR 58 #10886a Zbl 0224.13014

[Illusie 1972] L. Illusie, *Complexe cotangent et déformations, II*, Lecture Notes in Mathematics **283**, Springer, Berlin-New York, 1972. MR 58 #10886b Zbl 0238.13017

[Illusie, Laszlo et Orgogozo 2014] L. Illusie, Y. Laszlo et F. Orgogozo, *Travaux de Gabber sur l'uniformisation locale et la cohomologie étale des schémas quasi-excellents* (Séminaire à l'École polytechnique 2006–2008), Astérisque **363–364**, Société mathématique de France, Paris, 2014. Avec la collaboration de Frédéric Déglise, Alban Moreau, Vincent Pilloni, Michel Raynaud, Joël Riou, Benoît Stroh, Michael Temkin et Weizhe Zheng. MR 3329778 Zbl 1297.14003

[Jacobsson et Stoltenberg-Hansen 1985] C. Jacobsson et V. Stoltenberg-Hansen, "Poincaré–Betti series are primitive recursive", *J. London Math. Soc.* (2) **31**:1 (1985), 1–9. MR 87e:03103 Zbl 0584.03032

[de Jong 1996] A. J. de Jong, "Smoothness, semi-stability and alterations", *Inst. Hautes Études Sci. Publ. Math.* 83 (1996), 51–93. MR 98e:14011 Zbl 0916.14005

[de Jong 1998] T. de Jong, "An algorithm for computing the integral closure", *J. Symbolic Comput.* **26**:3 (1998), 273–277. MR 99d:13007 Zbl 0932.13021

[Kashiwara et Schapira 2006] M. Kashiwara et P. Schapira, *Categories and sheaves*, Grundlehren der Mathematischen Wissenschaften **332**, Springer, Berlin, 2006. MR 2006k:18001 Zbl 1118.18001

[Katz et Laumon 1985] N. M. Katz et G. Laumon, "Transformation de Fourier et majoration de sommes exponentielles", *Inst. Hautes Études Sci. Publ. Math.* 62 (1985), 361–418. MR 87i:14017 Zbl 0603.14015

[Lecerf 2013] G. Lecerf, "Factorisation des polynômes à plusieurs variables", *Les cours du CIRM* **3**:1 (2013), exposé no. 2.

[Lombardi et Quitté 2011] H. Lombardi et C. Quitté, *Algèbre commutative: méthodes constructives*, Calvage et Mounet, Paris, 2011. Zbl 1242.13002

[Lubotzky et Segal 2003] A. Lubotzky et D. Segal, *Subgroup growth*, Progress in Mathematics **212**, Birkhäuser, Basel, 2003. MR 2004k:20055 Zbl 1071.20033

[Mac Lane 1963] S. Mac Lane, *Homology*, Grundlehren der Mathematischen Wissenschaften **114**, Springer, Berlin, 1963. MR 28 #122 Zbl 0133.26502

[Madore 2014] D. Madore, "Commutative algebras whose bidual is commutative", question sur MathOverflow, 2014, voir http://mathoverflow.net/q/156091.

[Madore et Orgogozo 2014] D. Madore et F. Orgogozo, "Un modèle de calcul universel sur les éléments des corps" (titre provisoire), prépublication, 2014. Partie III de arXiv 1304.5376v3

[Matsumura 1989] H. Matsumura, *Commutative ring theory*, Deuxième éd., Cambridge Studies in Advanced Mathematics **8**, Cambridge Univ. Press, 1989. MR 90i:13001 Zbl 0666.13002

[Miller 2010] R. Miller, "Is it harder to factor a polynomial or to find a root?", *Trans. Amer. Math. Soc.* **362**:10 (2010), 5261–5281. MR 2011e:12003 Zbl 1215.12005

[Milne 1980] J. S. Milne, *Étale cohomology*, Princeton Mathematical Series **33**, Princeton Univ. Press, 1980. MR 81j:14002 Zbl 0433.14012

[Mines et Richman 1982] R. Mines et F. Richman, "Separability and factoring polynomials", *Rocky Mountain J. Math.* **12**:1 (1982), 43–54. MR 84e:03075 Zbl 0499.12019

[Mines, Richman et Ruitenburg 1988] R. Mines, F. Richman et W. Ruitenburg, *A course in constructive algebra*, Springer, New York, 1988. MR 89d:03066 Zbl 0725.03044

[Mochizuki 1999] S. Mochizuki, "Extending families of curves over log regular schemes", *J. Reine Angew. Math.* **511** (1999), 43–71. MR 2000f:14041 Zbl 0933.14012

[Mumford 1975] D. Mumford, *Curves and their Jacobians*, University of Michigan Press, Ann Arbor, MI, 1975. MR 54 #7451 Zbl 0316.14010

[Neukirch, Schmidt et Wingberg 2000] J. Neukirch, A. Schmidt et K. Wingberg, *Cohomology of number fields*, Grundlehren der Mathematischen Wissenschaften **323**, Springer, Berlin, 2000. MR 2000j:11168 Zbl 0948.11001

[Odifreddi 1989] P. Odifreddi, *Classical recursion theory*, Studies in Logic and the Foundations of Mathematics **125**, North-Holland, Amsterdam, 1989. MR 90d:03072 Zbl 0661.03029

[Odifreddi 1999] P. G. Odifreddi, *Classical recursion theory, II*, Studies in Logic and the Foundations of Mathematics **143**, North-Holland, Amsterdam, 1999. MR 2001b:03040 Zbl 0931.03057

[Ogg 1962] A. P. Ogg, "Cohomology of abelian varieties over function fields", *Ann. of Math.* (2) **76** (1962), 185–212. MR 27 #5758 Zbl 0121.38002

[Orgogozo 2003] F. Orgogozo, "Altérations et groupe fondamental premier à p", *Bull. Soc. Math. France* **131**:1 (2003), 123–147. MR 2004e:14034 Zbl 1083.14506

[Orgogozo 2013] F. Orgogozo, "Sur les propriétés d'uniformité des images directes en cohomologie étale", prépublication, 2013, voir http://fabrice.orgogozo.perso.math.cnrs.fr/articles/uniformite.pdf.

[Palmer 1974] T. W. Palmer, "Arens multiplication and a characterization of w^*-algebras", *Proc. Amer. Math. Soc.* **44** (1974), 81–87. MR 49 #5872 Zbl 0284.46041

[Petersen 2010] D. Petersen, "Ring-theoretic characterization of open affines?", réponse à une question sur MathOverflow, 2010, voir http://mathoverflow.net/a/20790/17064.

[Poonen, Testa et van Luijk 2015] B. Poonen, D. Testa et R. van Luijk, "Computing Néron–Severi groups and cycle class groups", *Compos. Math.* **151**:4 (2015), 713–734. MR 3334893 Zbl 06437570

[Rabin 1960] M. O. Rabin, "Computable algebra, general theory and theory of computable fields", *Trans. Amer. Math. Soc.* **95** (1960), 341–360. MR 22 #4639 Zbl 0156.01201

[Richman 1981] F. Richman, "Seidenberg's condition P", pp. 1–11 dans *Constructive mathematics* (Las Cruces, NM, 1980), édité par F. Richman, Lecture Notes in Mathematics **873**, Springer, Berlin-New York, 1981. MR 84k:12017 Zbl 0461.03016

[Rotman 1995] J. J. Rotman, *An introduction to the theory of groups*, Quatrième éd., Graduate Texts in Mathematics **148**, Springer, New York, 1995. MR 95m:20001 Zbl 0810.20001

[Rubio et Sergeraert 2002] J. Rubio et F. Sergeraert, "Constructive algebraic topology", *Bull. Sci. Math.* **126**:5 (2002), 389–412. MR 2003g:55001 Zbl 1007.55019

[Schön 1991] R. Schön, *Effective algebraic topology*, vol. 92, Mem. Amer. Math. Soc. **451**, Amer. Math. Soc., Providence, RI, 1991. MR 92h:55002 Zbl 0731.55015

[Sergeraert 1994] F. Sergeraert, "The computability problem in algebraic topology", *Adv. Math.* **104**:1 (1994), 1–29. MR 95c:55017 Zbl 0823.55011

[Serre 1955] J.-P. Serre, "Faisceaux algébriques cohérents", *Ann. of Math.* (2) **61** (1955), 197–278. MR 16,953c Zbl 0067.16201

[Serre 1965] J.-P. Serre, *Algèbre locale: multiplicités*, Deuxième éd., Lecture Notes in Mathematics **11**, Springer, Berlin-New York, 1965. MR 34 #1352 Zbl 0142.28603

[Serre 1975] J.-P. Serre, *Groupes algébriques et corps de classes*, Deuxième éd., Actualités Scientifiques et Industrielles **1264**, Hermann, Paris, 1975. MR 57 #6032 Zbl 0318.14004

[Serre 1977] J.-P. Serre, *Arbres, amalgames,* SL_2, Astérisque **46**, Société Mathématique de France, Paris, 1977. MR 57 #16426 Zbl 0369.20013

[Serre 1978–79] J.-P. Serre, "Groupes finis", notes d'un cours à l'ÉNSJF, 1978–79. arXiv 0503154v6

[Serre 1994] J.-P. Serre, *Cohomologie galoisienne*, Cinquième éd., Lecture Notes in Mathematics **5**, Springer, Berlin, 1994. MR 96b:12010 Zbl 0812.12002

[SGA 1 2003] A. Grothendieck, *Revêtements étales et groupe fondamental* (Séminaire de Géométrie Algébrique du Bois Marie 1960–1961), Documents Mathématiques (Paris) **3**, Société Mathématique de France, Paris, 2003. MR 2017446 Zbl 1039.14001

[SGA 4_1 1972] M. Artin, A. Grothendieck et J. L. Verdier, *Théorie des topos et cohomologie étale des schémas, Tome 1: Théorie des topos, Exposés I–IV* (Séminaire de Géométrie Algébrique du Bois Marie 1963–1964), Lecture Notes in Mathematics **269**, Springer, Berlin, 1972. MR 50 #7130 Zbl 0234.00007

[SGA 4_2 1972] M. Artin, A. Grothendieck et J. L. Verdier, *Théorie des topos et cohomologie étale des schémas, Tome 2: Exposés V–VIII* (Séminaire de Géométrie Algébrique du Bois Marie 1963–1964), Lecture Notes in Mathematics **270**, Springer, Berlin, 1972. MR 50 #7131 Zbl 0237.00012

[SGA 4_3 1973] M. Artin, A. Grothendieck et J. L. Verdier, *Théorie des topos et cohomologie étale des schémas, Tome 3: Exposés IX–XIX* (Séminaire de Géométrie Algébrique du Bois Marie 1963–1964), Lecture Notes in Mathematics **305**, Springer, Berlin, 1973. MR 50 #7132 Zbl 0245.00002

[SGA $4\frac{1}{2}$ 1977] P. Deligne, *Cohomologie étale* (Séminaire de Géométrie Algébrique du Bois Marie), Lecture Notes in Mathematics **569**, Springer, Berlin, 1977. Avec la collaboration de J.-F. Boutot, A. Grothendieck, L. Illusie et J.-L. Verdier. MR 57 #3132 Zbl 0349.14008

[Simpson 2008] C. Simpson, "Algebraic cycles from a computational point of view", *Theoret. Comput. Sci.* **392**:1-3 (2008), 128–140. MR 2008m:14021 Zbl 1134.14005

[Simpson 2009] S. G. Simpson, *Subsystems of second order arithmetic*, Deuxième éd., Cambridge Univ. Press, Association for Symbolic Logic, Poughkeepsie, NY, 2009. MR 2010e:03073 Zbl 1181.03001

[Singh et Swanson 2009] A. K. Singh et I. Swanson, "An algorithm for computing the integral closure", *Algebra Number Theory* **3**:5 (2009), 587–595. MR 2011b:13022 Zbl 1180.13010

[Smoryński 1985] C. Smoryński, "The varieties of arboreal experience [*Math. Intelligencer* **4**:4 (1982), 182–189]", pp. 381–397 dans *Harvey Friedman's research on the foundations of mathematics*, édité par L. A. Harrington et al., Stud. Logic Found. Math. **117**, North-Holland, Amsterdam, 1985. MR 835269 Zbl 0588.03001

[Steel 2005] A. Steel, "Conquering inseparability: primary decomposition and multivariate factorization over algebraic function fields of positive characteristic", *J. Symbolic Comput.* **40**:3 (2005), 1053–1075. MR 2006f:13023 Zbl 1120.13026

[Stoltenberg-Hansen et Tucker 1999] V. Stoltenberg-Hansen et J. V. Tucker, "Computable rings and fields", pp. 363–447 dans *Handbook of computability theory*, édité par E. R. Griffor, Stud. Logic Found. Math. **140**, North-Holland, Amsterdam, 1999. MR 2000g:03100 Zbl 0944.03040

[Stolzenberg 1968] G. Stolzenberg, "Constructive normalization of an algebraic variety", *Bull. Amer. Math. Soc.* **74** (1968), 595–599. MR 37 #201 Zbl 0164.04202

[Szamuely 2009] T. Szamuely, *Galois groups and fundamental groups*, Cambridge Studies in Advanced Mathematics **117**, Cambridge Univ. Press, 2009. MR 2011b:14064 Zbl 1189.14002

[Vasconcelos 2005] W. Vasconcelos, *Integral closure*, Springer, Berlin, 2005. MR 2006m:13007 Zbl 1082.13006

[Wingberg 1984] K. Wingberg, "Ein Analogon zur Fundamentalgruppe einer Riemannschen Fläche im Zahlkörperfall", *Invent. Math.* **77**:3 (1984), 557–584. MR 86e:11104 Zbl 0563.12008

[Zariski et Samuel 1975] O. Zariski et P. Samuel, *Commutative algebra, I*, Graduate Texts in Mathematics **28**, Springer, Berlin, 1975. MR 52 #5641 Zbl 0313.13001

Communicated by Bjorn Poonen
Received 2014-10-16 Revised 2015-04-16 Accepted 2015-04-28

david+math@madore.org *INFRES/CNRS LTCI, Institut Mines-Télécom, Télécom ParisTech, 75013 Paris, France*

fabrice.orgogozo+math@normalesup.org
Centre de mathématiques Laurent Schwartz, CNRS, École polytechnique, 91128 Palaiseau, France

Guidelines for Authors

Authors may submit manuscripts in PDF format on-line at the Submission page at the ANT website.

Originality. Submission of a manuscript acknowledges that the manuscript is original and and is not, in whole or in part, published or under consideration for publication elsewhere. It is understood also that the manuscript will not be submitted elsewhere while under consideration for publication in this journal.

Language. Articles in *ANT* are usually in English, but articles written in other languages are welcome.

Length There is no a priori limit on the length of an *ANT* article, but *ANT* considers long articles only if the significance-to-length ratio is appropriate. Very long manuscripts might be more suitable elsewhere as a memoir instead of a journal article.

Required items. A brief abstract of about 150 words or less must be included. It should be self-contained and not make any reference to the bibliography. If the article is not in English, two versions of the abstract must be included, one in the language of the article and one in English. Also required are keywords and subject classifications for the article, and, for each author, postal address, affiliation (if appropriate), and email address.

Format. Authors are encouraged to use LaTeX but submissions in other varieties of TeX, and exceptionally in other formats, are acceptable. Initial uploads should be in PDF format; after the refereeing process we will ask you to submit all source material.

References. Bibliographical references should be complete, including article titles and page ranges. All references in the bibliography should be cited in the text. The use of BibTeX is preferred but not required. Tags will be converted to the house format, however, for submission you may use the format of your choice. Links will be provided to all literature with known web locations and authors are encouraged to provide their own links in addition to those supplied in the editorial process.

Figures. Figures must be of publication quality. After acceptance, you will need to submit the original source files in vector graphics format for all diagrams in your manuscript: vector EPS or vector PDF files are the most useful.

Most drawing and graphing packages (Mathematica, Adobe Illustrator, Corel Draw, MATLAB, etc.) allow the user to save files in one of these formats. Make sure that what you are saving is vector graphics and not a bitmap. If you need help, please write to graphics@msp.org with details about how your graphics were generated.

White space. Forced line breaks or page breaks should not be inserted in the document. There is no point in your trying to optimize line and page breaks in the original manuscript. The manuscript will be reformatted to use the journal's preferred fonts and layout.

Proofs. Page proofs will be made available to authors (or to the designated corresponding author) at a Web site in PDF format. Failure to acknowledge the receipt of proofs or to return corrections within the requested deadline may cause publication to be postponed.

Algebra & Number Theory

Volume 9 No. 7 2015

1937-0652(2015)9:7;1-2