Introduction aux conjectures de Weil
Cours de DEA

Bernard Le Stum[1]
Université de Rennes 1

Version du 6 novembre 2001

[1]lestum@univ-rennes1.fr

Table des matières

Chapitre 1

Enoncé des conjectures de Weil

Comme son nom l'indique, ce chapitre va être consacré à énoncer les conjectures de Weil. On garde une approche naïve et on introduit les notions géométriques nécessaires au fur et à mesure. On suppose connu l'essentiel des cinq premiéres sections du second chapitre du livre de Hartshorne. On étudiera de manière détaillée les notions de propreté et surtout de lissité pour des schémas quelconques. Ce n'est bien sûr pas nécessaire pour comprendre les conjectures de Weil, mais cela doit faire partie du bagage d'un géométre algébrique.

1.1 Systèmes d'équations polynomiales modulo p

Un invariant important d'un système d'équations est son nombre de solutions. Malheureusement, celui ci est en general infini. On obtient alors des invariants plus fins en recherchant le nombre de solutions modulo un entier donné. On va être plus précis.

Considérons un système d'équations polynomiales à coefficients dans $\mathbf{Z}$:

$$\left\{ \begin{array}{c} f_1(x_1, \ldots, x_n) = 0 \\ \vdots \\ f_r(x_1, \ldots, x_n) = 0 \end{array} \right.$$

Etant donné un nombre premier p, on peut chercher le nombre N de solutions de ce système modulo p.

Exercice 1.1 Que vaut N pour le système vide d'équations en n variables ?

Exercice 1.2 *Même question pour l'équations* $x_1 + \cdots + x_n = 0$ *?*

Exercice 1.3 *Même question pour le système d'équation en* 2 *variables*

$$\begin{cases} ax + by = 0 \\ cx + dy = 0 \end{cases} .$$

Exercice 1.4 *Même question pour l'équation en une variable* $x^2 + 1 = 0$.

Exercice 1.5 *Même question pour l'équation en* 2 *variables* $(ax + by)(cx + dy) = 0$.

Exercice 1.6 *Même question pour l'équation en* 2 *variables* $x^2 + y^2 = 0$.

Exercice 1.7 *Même question pour l'équation en* n^2 *variables*

$$\begin{vmatrix} x_{11} & \dots & x_{1n} \\ \vdots & \ddots & \vdots \\ x_{n1} & \dots & x_{nn} \end{vmatrix} = 0$$

Pour répondre à ces questions, on est amenés à travailler dans l'espace vectoriel $\mathbf{F}_p^n$. En fait, on s'interesse à un système d'équations

$$\begin{cases} f_1(x_1, \dots, x_n) = 0 \\ \qquad \vdots \\ f_r(x_1, \dots, x_n) = 0 \end{cases}$$

à coefficients dans le corps fini $\mathbf{F}_p$. Ces équations définissent un schéma affine X sur $\mathbf{F}_p$. Plus précisément, on considère l'idéal $I := (f_1, \dots, f_n)$ de $\mathbf{F}_p[t_1, \dots, t_n]$, on pose $A := \mathbf{F}_p[t_1, \dots, t_n]/I$ et $X := \operatorname{Spec} A$. Le nombre N est alors le nombre de points de X dont le corps résiduel est $\mathbf{F}_p$.

Avant d'aller plus loin, rappelons quelques résultats et notations.

1.2 Points à valeur dans un schéma

Afin de reformuler correctement notre problème dans le langage de la géométrie algébrique et de le généraliser, il est nécessaire d'introduire la notion de point à valeur dans un schéma.

Définition 1.2.1 *Si X et T sont deux S-schémas, on note $X(T)_S = Hom_S(T, X)$ l'ensemble des morphismes de S-schémas $T \to X$. Si S ou T est affine, on le remplace dans les natations par son anneau et on écrira $X(T) := X(T)_{\mathbf{Z}}$. On dit que $X(T)_S$ est l'ensemble des* points de X à valeur dans T*.*

On remarqueras que $T \mapsto X(T)_S$ est fonctoriel.

Exercice 1.8 Montrer que si $k := \mathbf{F}_p$ ou $k := \mathbf{Q}$, alors $X(T)_k = X(T)$. Montrer que c'est faux en général, pour un autre corps k.

Proposition 1.2.2 *i) Soient X, Y et T des S-schémas. Alors,*

$$(X \times_S Y)(T)_S = X(T)_S \times Y(T)_S.$$

ii) Soient X un S-schéma, $S' \to S$ un morphisme, T' un S'-schéma et $X' := X \times_S S'$. On a alors $X(T')_S = X'(T')_{S'}$.

Démonstration: Ces deux assertions résultent immédiatement de la propriété universelle du produit fibré. En fait, la première assertion est la définition. □

Définition 1.2.3 *Une* immersion $i : Y \hookrightarrow X$ *est la composée d'une immersion fermée $Y \to U$ et d'une immersion ouverte $U \to X$. On dit que $\mathcal{I} := \mathrm{Ker}(\mathcal{O}_X \to i_*\mathcal{O}_Y)$ est l'*idéal *de l'immersion.*

Les immersions se comportent bien par rapport aux opérations standards de la géométrie algébrique. C'est quelque chose que l'on peut vérifier en exercice.

Exercice 1.9 Montrer qu'une immersion peut s'écrire comme composé d'une immersion ouverte suivie d'une immersion fermée.

Exercice 1.10 Montrer que si $i : Y \hookrightarrow X$ et $j : Z \hookrightarrow Y$ sont deux immersions, alors $i \circ j$ aussi.

Exercice 1.11 Montrer que si $i : Y \hookrightarrow X$ est une immersion, alors pour tout morphisme $X' \to X$, le morphisme $Y' := Y \times_X X' \to X'$ déduit de i est une immersion.

Exercice 1.12 Soient $f : Y \to X$ et $g : Z \to Y$ deux morphismes avec $f \circ g$ une immersion. Montrer que g est une immersion.

Exercice 1.13 *Soient $i : Y \hookrightarrow X$ et $i' : Y' \hookrightarrow X'$ deux immersions de S-schémas. Montrer que $i \times i' : Y \times_S Y' \hookrightarrow X \times_S X'$ est une immersion.*

Exercice 1.14 *Soit $f : Y \to X$ un morphisme, $\{U_i\}$ un recouvrement ouvert de X et pour tout i, $V_i := f^{-1}(U_i)$. Si, pour tout i, le morphisme $V_i \to U_i$ induit par f est une immersion, alors f est une immersion.*

On peut aussi facilement caractériser, parmi les immersions, celles qui sont ouvertes.

Exercice 1.15 *Soit $i : Y \hookrightarrow X$ une immersion. Montrer que i est ouverte ssi $\mathcal{I} = 0$ ssi $i^{-1}(\mathcal{I}) = 0$.*

Proposition 1.2.4 *Si $i : Y \hookrightarrow X$ est une immersion de S-schémas, alors l'application canonique $Y(T)_S \to X(T)_S$ est injective. Son image est formée des s tels que $s(T) \subset i(Y)$ et s^* s'annule $s^{-1}(\mathcal{I})$ où $\mathcal{I}$ est l'idéal de Y dans X. La première condition est inutile si l'immersion est fermée et la seconde est inutile si l'immersion est ouverte.*

Démonstration: On se donne une application continue $s' : T \to Y$. En faire un morphisme, c'est se donner un morphisme d'anneaux $s'^* : s'^{-1}(\mathcal{O}_Y) \to \mathcal{O}_T$. Comme i est une immersion, on a une suite exacte

$$O \to i^{-1}(\mathcal{I}) \to i^{-1}(\mathcal{O}_X) \to \mathcal{O}_Y \to 0.$$

On pose $s := i \circ s'$. Comme s'^{-1} est exact, on a une suite exacte

$$O \to s^{-1}(\mathcal{I}) \to s^{-1}(\mathcal{O}_X) \to s'^{-1}(\mathcal{O}_Y) \to 0.$$

La donnée de s^* est donc équivalente à celle de l'application s et d'un morphisme d'anneaux $s^{-1}(\mathcal{O}_X) \to \mathcal{O}_T$ qui s'annule sur $s^{-1}(\mathcal{I})$. C'est ce que l'on voulait.

Clairement, si l'immersion est ouverte, $\mathcal{I} = 0$ et la seconde condition est bien sûr inutile. De même, si l'immersion est fermée et s^* s'annule $s^{-1}(\mathcal{I})$, on a automatiquement $s(T) \subset i(Y)$ car $s^{-1}(Y)$ est le sous-schéma fermé défini par l'image de $s^{-1}(\mathcal{I})$ dans $\mathcal{O}_T$. □

Proposition 1.2.5 *Si T est un S-schéma, alors l'application*

$$\mathbf{A}^n_S(T)_S \to \Gamma(T, \mathcal{O}_T)^n, s \mapsto (s_1, \ldots, s_n)$$

avec $s_i := s^*(t_i)$, est bijective (on note $t_1, \ldots, t_n$ les coordonnées sur l'espace affine). On identifiera par la suite ces deux ensembles.

Si R est un anneau et X un sous-schéma fermé de $\mathbf{A}^n_R$, défini par un idéal I, alors

$$X(T)_R = \{s \in \Gamma(T, \mathcal{O}_T)^n, \forall f \in I, f(s) = 0\}.$$

Démonstration: Pour la première assertion, il suffit en vertu de la proposition ci-dessus, de considérer le cas $n = 1$ et $S = \operatorname{Spec} \mathbf{Z}$. Notre application se réduit alors à la suite de bijections

$$\mathbf{A}^1(T) = Hom(T, \mathbf{A}^1) \tilde{\to} Hom(\mathbf{Z}[T], \Gamma(T, \mathcal{O}_T)) \tilde{\to} \Gamma(T, \mathcal{O}_T).$$

Pour la seconde assertion, on remarque que $s \in X(T)_R$ ssi s^* s'annule sur I et par définition, on a l'identité $s^*(f) = f(s_1, \ldots, s_n)$. $\square$

En fait, nous aurons essentiellement à considérer les points à valeur dans un corps.

Proposition 1.2.6 *Si X est un schéma et k un corps, alors $X(k)$ est en bijection avec les couples (x, i) ou x est un point de X et $i : k(x) \to k$ un homomorphime de corps.*

Démonstration: Un morphisme $s : \operatorname{Spec} k \to X$ est une application continue, donc déterminée par l'image x de l'unique point de $\operatorname{Spec} k$, munie d'un morphisme $s^{-1}(\mathcal{O}_X) \to \mathcal{O}_{\operatorname{Spec} k}$. Comme le foncteur $\Gamma(\operatorname{Spec} k, -)$ est une équivalence de catégories, ce morphisme correspond à un morphisme d'anneaux $\Gamma(\operatorname{Spec} k, s^{-1}(\mathcal{O}_X)) \to \Gamma(\operatorname{Spec} k, O_{\operatorname{Spec} k})$. On a bien sûr $\Gamma(\operatorname{Spec} k, \mathcal{O}_{\operatorname{Spec} k}) = k$, et par définition, $\Gamma(\operatorname{Spec} k, s^{-1}(\mathcal{O}_X)) = \mathcal{O}_{X,x}$. Par construction, on trouve un homomorphisme local $\mathcal{O}_{X,x} \to k$ qui se se factorise de manière unique par $k(x)$. $\square$

Exercice 1.16 Un morphisme bijectif $f : Y \to X$ induit-il une bijection $Y(k) \tilde{\to} X(k)$?

Corollaire 1.2.7 *Soit k un corps et X un k-schéma. Soit k' une extension de k. Alors, $X(k')_k$ est en bijection avec les couples (x, i) ou x est un point de X et $i : k(x) \to k'$ est un k-homomorphisme.*

Corollaire 1.2.8 *Si X est un k-schéma et $X = X_1 \cup X_2$ ou X_1 et X_2 sont deux sous-schémas disjoints, alors $X(k')_k = X_1(k')_k \cup X_2(k')_k$.*

Exercice 1.17 Si X est un S-schéma et $X = X_1 \cup X_2$ ou X_1 et X_2 sont deux sous-schémas disjoints, a-t-on toujours $X(T)_S = X_1(T)_S \cup X_2(T)_S$?

Exercice 1.18 Montrer que si k est un corps algébriquement clos et X un schéma localement de type fini sur k, alors $X(k)_k$ est en bijection avec l'ensemble $|X|$ des points fermés de X.

1.3 Points de schémas sur des corps finis

On revient à la situation du paragraphe 1.1 : $X := \operatorname{Spec} A$ avec $A := \mathbf{F}_p[t_1, \ldots, t_n]/I$ et $I := (f_1, \ldots, f_n)$.

Il résulte alors de la proposition 1.2.5 que $X(\mathbf{F}_p)$ est en bijection avec l'ensemble des solutions de

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \quad\vdots \\ f_r(x_1, \ldots, x_n) = 0 \end{cases}$$

dans $\mathbf{F}_p^n$. Notreproblème initial devient donc le calcul de $N := |X(\mathbf{F}_p)|$. En fait, on peut très bien avoir $N = 0$. Pour obtenir des informations sur X, il est nécessaire de calculer $N_r := |X(\mathbf{F}_{p^r})_{\mathbf{F}_p}|$.

Plus généralement, on fixe un nombre premier p, on choisit une puissance $q := p^f$ de p et on se donne un schéma (quasi-compact) X sur $\mathbf{F}_q$. On pose alors pour tout $r \in \mathbf{N}, N_r := N_r(X) := |X(\mathbf{F}_{q^r})_{\mathbf{F}_q}|$ et on écrira $N := N_1$.

Exercice 1.19 Montrer que si on pose $X_r := X \otimes_{\mathbf{F}_q} \mathbf{F}_{q^r}$ (vu comme $\mathbf{F}_{q^r}$-schéma, alors $N_r(X) = N(X_r)$.

Exercice 1.20 Montrer que si $\bar{\mathbf{F}}_q$ est une clôture algébrique de $\mathbf{F}_q$, alors $X(\mathbf{F}_{q^r})_{\mathbf{F}_q} \tilde{=} X(\bar{\mathbf{F}}_q)_{\mathbf{F}_q}^{F^r=1}$ ou $F : X \to X$ est le Frobenius de X (identité comme application et puissance q-ième sur les fonctions).

Exercice 1.21 Que vaut N_r pour $X = \mathbf{A}^n_{\mathbf{F}_q}$ (ou plus généralement pour une variété linéaire affine de dimension n) ?

Exercice 1.22 Même question pour $X = \operatorname{Spec} \mathbf{F}_{q^s}$ (ou plus généralement pour un schéma fini (1.4.1) sur $\mathbf{F}_q$) ?

Exercice 1.23 Même question pour l'union de deux droites dans le plan affine.

Exercice 1.24 Même question pour une conique affine ou projective.

Exercice 1.25 Même question pour le groupe linéaire $GL_{n\mathbf{F}_q}$: on rappelle que c'est l'ouvert de $\mathbf{A}^{n^2}_{\mathbf{F}_q}$ défini par

$$\begin{vmatrix} x_{11} & \dots & x_{1n} \\ \vdots & \ddots & \vdots \\ x_{n1} & \dots & x_{nn} \end{vmatrix} \neq 0.$$

Exercice 1.26 Même question pour $\mathbf{P}^n_{\mathbf{F}_q}$ (ou plus généralement pour une variété linéaire projective de dimension n).

Exercice 1.27 Même question pour la quadrique de Segre, c'est à dire la quadrique projective d'équation $xy = zt$ (on pourra montrer qu'elle est isomorphe à $\mathbf{P}^1 \times \mathbf{P}^1$).

On va maintenant introduire la première conjecture de Weil. Afin de faciliter l'intuition géométrique, on va se limiter dorénavant à des schémas ayant des propriétés raisonnables. On pose donc la définition suivante.

Définition 1.3.1 *Une* variété (algébrique) *sur un corps k est un schéma séparé de type fini sur k.*

Définition 1.3.2 *Un* entier algébrique *est un nombre algébrique dont le polynôme irréductible est (unitaire) à coefficient entiers. Un* nombre de Weil *de* poids $m \in \mathbf{Z}$ *relativement à q est un nombre algébrique dont toutes les valeurs absolues archimédiennes sont de la forme $q^{\frac{m}{2}}$.*

Exercice 1.28 Montrer que les entiers algébriques forment un anneau non noethérien.

Théorème 1.3.3 (Conj. de Weil, rationalité, version additive) *Soit X une variété algébrique sur $\mathbf{F}_q$. Alors, il existe des entiers algébriques α_i, β_j tels que pour tout r, on ait $N_r(X) = \sum \alpha_i^r - \sum \beta_j^r$.*

Cette conjecture faite par A. Weil en 1949 (voir [17]) fût démontrée par B. Dwork en 1960 (voir [4]).

Exercice 1.29 Vérifier cette conjecture pour une variété linéaire affine ou projective, pour une variété finie, pour une conique affine ou projective, pour le groupe linéaire et pour la quadrique de Segre.

Théorème 1.3.4 (Conj. de Weil, pureté, version additive) *Si X est de dimension d, les α_i et les β_j sont des nombres de Weil de poids $\in [0, 2d]$).*

Cette conjecture, énoncée par A. Weil, n'a été démontrée qu'en 1973 (voir [5]) pour les variétés projectives (1.4.4) et en 1984 (voir [6]) en toute généralité.

Exercice 1.30 Vérifier cette conjecture pour les variétés déja étudiées.

Afin d'énoncer la suite des conjectures de Weil, il est nécessaire de faire quelques compléments de géométrie algébrique. En effet, celles-ci s'appliquent essentiellement aux variétés *complètes non singulières* ou plutôt *propres et lisses* comme on dit maintenant. Comme ce cours est plus un tremplin qu'une fin en soi, nous allons définir ces notions en toute généralité.

1.4 Morphismes finis, projectifs, propres

Les propriétés que nous allons étudier maintenant sont les analogues des propriétés de compacité en géométrie complexe.

Définition 1.4.1 *Un morphisme $f : Y \to X$ est* affine *s'il existe un recouvrement de X par des ouverts affines U_i tel que pour tout i, $V_i := f^{-1}(U_i)$ soit affine. On dit que f est* fini *si de plus, il existe un tel recouvrement pour lequel $f_i : V_i \to U_i$ provient d'un homomorphisme fini $A_i \to B_i$. On dit aussi que Y est affine (resp. fini) sur X.*

Exercice 1.31 Un morphisme bijectif est il fini ?

Exercice 1.32 Montrer que si un schéma X sur un corps k est fini sur k, son ensemble sous-jacent est fini et tous les points sont fermés. La réciproque est-elle vraie ? Suffit-il que l'ensemble sous-jacent soit fini.

Exercice 1.33 Montrer que si X est localement de type fini sur un corps k, alors X est fini sur k ssi et si $|X|$ est un ensemble fini (utiliser le Nullstellensatz pour les anneaux locaux)

Lemme 1.4.2 *Soit X un schéma affine et $f : Y \to X$ un morphisme. Si f est affine, alors, Y est affine. Si f est fini, il provient d'un morphisme fini $A \to B$.*

Démonstration: Quitte à raffiner le recouverment, on peut supposer qu'il existe un nombre fini de $g_i \in A$ qui engendrent A comme idéal et tels que pour tout i, si on pose ou $U_i := D(g_i)$, alors $V_i := f^{-1}(U_i)$ est affine, disons $V_i = \operatorname{Spec} B_i$.

Montrons que Y est affine. Comme f se factorise par $\operatorname{Spec}\Gamma(Y,\mathcal{O}_Y)$, on peut supposer que $\Gamma(Y,\mathcal{O}_Y)=A$. Et il s'agit de montrer que f est l'identité. Comme f est quasi-compact et quasi-séparé, $f_*\mathcal{O}_Y$ est quasi-cohérent (on peut aussi le vérifier directement). Comme $\Gamma(Y,\mathcal{O}_Y)=A$, on en déduit que $f_*\mathcal{O}_Y=\mathcal{O}_X$. On a donc

$$\Gamma(V_i,\mathcal{O}_Y)=\Gamma(U_i,f_*\mathcal{O}_Y)=\Gamma(U_i,f_*\mathcal{O}_Y)=A_{g_i}$$

et il suit que f_i est l'identité. Il en va donc de même de f.

On sait donc que Y est affine, disons $Y=\operatorname{Spec}B$ et on suppose que B_i est fini sur A_{g_i}. On a alors $B_i=B_{g_i}$ qui est fini sur A_{g_i} et il faut montrer que B est fini sur A. Plus généralement, on se donne un A-module M et on suppose que les M_{g_i} sont de type fini sur les A_{g_i}. Il faut s'assurer que M est fini sur A. Ca se fait à la main. □

Proposition 1.4.3 *i) Une immersion fermée $Y\hookrightarrow X$ est finie.*

ii) Si $f:Y\to X$ et $g:Z\to Y$ sont, deux morphismes finis, alors $f\circ g$ est fini.

iii) Si X est fini sur S, alors pour tout changement de base $S'\to S$, $X':=X\times_S S'$ est fini sur S'.

iv) Soient $f:Y\to X$ un S-morphisme. Si Y est fini sur S, alors f est fini.

v) Soient $f:Y\to X$ et $f':Y'\to X'$ deux S-morphismes finis. Alors, $f\times f':Y\times_S Y'\to X\times_S X'$ est fini.

vi) Soit $f:Y\to X$ un morphisme, $\{U_i\}$ un recouvrement ouvert de X et pour tout i, $V_i:=f^{-1}(U_i)$. Si, pour tout i, le morphisme $V_i\to U_i$ induit par f est fini, alors f est fini.

Démonstration: Pour démontrer les trois premières assertions, on se ramène immédiatement, grâce au lemme, au cas ou tous les schémas sont affines. On retrouve des résultats classiques d'algèbre commutative : surjectif implique fini, transitivité de la finitude et stabilité par extension.

Les deux assertions suivantes résultent formellement des précédentes si on sait qu'un morphisme fini est séparé. Or cette question est locale sur la base, et tout morphisme de schémas affines est séparé.

Pour la dernière assertion, la nécessité de la condition résulte de l'assertion 3 et sa suffisance résulte du lemme. □

Exercice 1.34 Montrer que si $f:Y\to X$ est fini, alors, pour tout $x\in X$, $f^{-1}(x)$ est un ensemble fini. La réciproque est elle vraie ? Et si f est localement de type fini ?

Pour définir la notion de morphisme projectif, il est nécessaire de localiser la construction du Proj d'un anneau. On définit la notion de faisceau d'algèbres graduées de manière analogue à celle d'algèbre graduée.

Proposition et Définition 1.4.4 *Soit X un schéma et $\mathcal{B}$ une $\mathcal{O}_X$-algèbre graduée quasi-cohérente. Alors, il existe à isomorphisme près au dessus de X, un unique morphisme $f : Y \to X$ tel que l'on ait une famille compatible d'isomorphismes $f^{-1}(U) \tilde{\to} \operatorname{Proj}\Gamma(U, \mathcal{B})$ pour tout ouvert affine $U \subset X$. On dit que f est un morphisme* projectif *si $\mathcal{B}_1$ est de type fini et engendre $\mathcal{B}$. On dit aussi que Y est projectif sur X.*

Démonstration: Complétement standard. □

Avant d'énoncer le résultat suivant, on fait quelques rappels.

A tout module gradué M sur un anneau gradué A, on sait associer un faisceau $\mathcal{F}$ sur $X := Proj A$. En particulier, on peut considérer les faisceaux $\mathcal{O}_X(d)$ associés aux décalés $A(d)$. Remarquons aussi que si I est un idéal homogène de A, alors le faisceau associé à I n'est autre que est l'idéal qui définit l'immersion de $\operatorname{Proj} A/I$ dans X.

On a une construction dans l'autre sens qui à tout faisceau $\mathcal{F}$ sur X associe un A-module gradué : On pose $\mathcal{F}(d) := \mathcal{F} \otimes \mathcal{O}(d)$, $M_d := \Gamma(X, \mathcal{F}(d))$ et $M := \oplus M_d$. On peut montrer que si A est engendré comme A_0-algèbre par un nombre fini d'éléments de A_1 (on note A_d le sous-module des éléments de degré d) et si $\mathcal{F}$ est quasi-cohérent, alors $\mathcal{F}$ est bien le faisceau associé à M.

Proposition 1.4.5 *Soit A un anneau. Un A-schéma X est projectif ssi il existe une immersion fermée $X \hookrightarrow \mathbf{P}_A^N$.*

Démonstration: La condition est nécessaire : si $f_0, \ldots, f_N$ sont des générateurs de degré 1 de B, le morphisme surjectif d'algèbres graduées $A[T_0, \ldots, T_N] \to B, t_i \mapsto f_i$ nous fournit une immersion fermée $\operatorname{Proj} B \hookrightarrow \mathbf{P}_A^n$.

Il faut montrer que la condition est aussi suffisante. On note $\mathcal{I}$ le faisceau d'idéaux qui définit X dans $\mathbf{P}_A^N$ et I le module gradué correspondant. C'est clairement un idéal homogène de $A[T_0, \ldots, T_N]$. On pose alors $B := A/I$. Comme $\mathcal{I}$ est quasi-cohérent, le faiseau associé à I sur $\mathbf{P}_A^N$ est bien $\mathcal{I}$ et on a donc $X \tilde{=} \operatorname{Proj} B$. □

La projectivité n'est pas une notion de nature locale. Celle-ci, issue de la géométrie classique, est en fait un cas particulier de la notion de propreté, que nous allons étudier bientôt et qui se comporte bien mieux par rapport aux opérations standard de la géométrie algébrique. On peut tout de même démontrer pour les morphismes projectifs les résultats suivants qui sont donnés sous forme d'exercice.

Exercice 1.35 *Montrer que fini implique projectif.*

Exercice 1.36 *Montrer que si $f : Y \to X$ et $g : Z \to Y$ sont deux morphismes projectif et si X est quasi-compact et quasi-séparé, alors $f \circ g$ est projectif.*

Exercice 1.37 *Montrer que si X est projectif sur S et si $S' \to S$ est un changement de base, alors $X' := X \times_S S'$ est projectif sur S'.*

Exercice 1.38 *Montrer que si $f : Y \to X$ est un S-morphisme avec Y projectif et X séparé sur S, alors f est projectif.*

Exercice 1.39 *Montrer que si $f : Y \to X$ et $f' : Y' \to X'$ sont deux morphismes projectifs de S-schémas. Alors, $f \times f' : Y \times_S Y' \to X \times_S X'$ est projectif.*

Définition 1.4.6 *Un morphisme $f : Y \to X$ est* universellement fermé *si, pour tout morphisme $X' \to X$, le morphisme $Y \times_X X' \to X'$ déduit de f est une application fermée (l'image d'un fermé est fermé). On dit que f est* propre *si il est séparé, de type fini et universellement fermé.*

Exercice 1.40 *Montrer que $\mathbf{A}^1_S$ n'est pas propre sur S.*

Proposition 1.4.7 *i) Une immersion fermée $f : Y \hookrightarrow X$ est propre.*

ii) Si $f : Y \to X$ et $g : Z \to Y$ sont, deux morphismes propres, alors $f \circ g$ est propre.

iii) Si X est propre sur S et $S' \to S$ est un changement de base, alors $X' := X \times_S S'$ est propre sur S'.

iv) Si $f : Y \to X$ est un S-morphismes avec Y prore et X séparé, alors f est propre.

v) Soient $f : Y \to X$ et $f' : Y' \to X'$ deux morphismes propres de S-schémas. Alors, $f \times f' : Y \times_S Y' \to X \times_S X'$ est propre.

vi) Soit $f : Y \to X$ un morphisme, $\{U_i\}$ un recouvrement ouvert de X et pour tout i, $V_i := f^{-1}(U_i)$. Si, pour tout i, le morphisme induit par f, $V_i \to U_i$ est propre, alors f est propre.

Démonstration: Les assertions 4 et 5 sont conséquences formelles des 3 premières. On connait aussi tous ces résultats pour les morphismes séparés ou de type fini. Il reste donc à traiter la propriété d'être universellement fermé. Comme les morphismes qui sont des applications fermées vérifient les analogues des assertions 1, 2 et 6. On en déduit facilement qu'il en va de même des morphismes universellement fermés. Finalement, le fait d'étre une immersion fermée est clairement stable par extension de la base, d'où l'assertion 3. □

Proposition 1.4.8 *i) Un morphisme fini $f : Y \to X$ est propre.*

ii) Un morphisme projectif $f : Y \to X$ est propre.

Démonstration: Comme de tels morphismes sont séparés de type fini (vérifier !) et que la propriété d'être fini ou projectif est stable par extension, il suffit dans les deux cas de montrer que f est fermé. En localisant sur la base, on peut supposer que X est affine. De plus, comme une immersion fermée est propre, il suffit de montrer que l'image de f est fermée.

Pour les morphismes finis, il reste à vérifier que si B est une A-algèbre finie, alors l'image de $\operatorname{Spec} B$ dans $\operatorname{Spec} A$ est fermé. Quite à remplacer A par son image dans B, on peut supposer que $A \to B$ est injectif. On sait alors que $\operatorname{Spec} B \to \operatorname{Spec} A$ est surjectif (résultat classique d'algèbre comutative).

Pour les morphismes projectifs, il faut travailler un peu plus. On se donne un anneau gradué B, et on note B_n le sous-groupe des éléments de degré n. On écrit $A := B_0$ et on suppose que B est engendré comme A-algèbre par un nombre fini d'éléments de B_1. Il faut montrer que l'image du morphisme canonique $f : \operatorname{Proj} B \to \operatorname{Spec} A$ est fermé. Soit pour tout n, I_n l'annulateur de B_n et $I := \cup I_n$. On remarquera que I_n est une suite croissante. Nous allons montrer que $f(\operatorname{Proj} B) = V(I)$.

Pour $\mathfrak{p} \in \operatorname{Spec} A$, on a $f^{-1}(\mathfrak{p}) \tilde{=} \operatorname{Proj}(B \otimes_A k(\mathfrak{p}))$ (vérifier). Il suit que $f^{-1}(\mathfrak{p}) = \emptyset$ ssi $B_n \otimes_A k(\mathfrak{p}) = 0$ pour $n >> 0$ (crirère de nullité des Proj). Comme B_n est un module de type fini, le lemme de Nakayama nous dit que cette dernière condition est équivalente à $B_n \otimes_A A_{\mathfrak{p}} = 0$, ce qui signifie que $I_n \not\subset \mathfrak{p}$ pour $n >> 0$, ou encore que $I \not\subset \mathfrak{p}$. On voit donc que $\mathfrak{p} \in f(\operatorname{Proj} B)$ ssi $\mathfrak{p} \in V(I)$. □

Un morphisme propre n'est pas loin d'être projectif comme le montre l'exercice (difficile) suivant.

Exercice 1.41 Soit S un schéma quasi-compact et X un S-schéma propre et irréductible. Alors, il existe un ouvert dense U de X, un S-schéma projectif *et irréductible X' contenant U et un S-morphisme $f : X' \to X$ qui prolonge l'identité de U.*

1.5 Morphismes lisses, définitions

La seconde notion que nous voulons étudier est l'analogue des singularités en géométrie analytique complexe. Il est donc nécessaire avant tout de définir ce qu'on appelle une différentielle en géométrie algébrique. On peut déja introduire la notion de dérivation qui est très générale.

Définition 1.5.1 *Soient $\mathcal{R}$ est un faisceau d'anneaux sur un espace topologique X, $\mathcal{A}$ une $\mathcal{R}$-algèbre et $\mathcal{F}$ un $\mathcal{A}$-module. Une* $\mathcal{R}$-dérivation $D : \mathcal{A} \to \mathcal{F}$ *est un homomorphisme de $\mathcal{R}$-modules tel que pour toutes sections locales f, g de $\mathcal{A}$, on ait $D(fg) = fD(g) + gD(f)$. Leur ensemble se note* $\mathrm{Der}_{\mathcal{R}}(\mathcal{A}, \mathcal{F})$.

Exercice 1.42 Montrer que dans cette définition, au lieu de demander que D soit $\mathcal{R}$-linéaire, on peut demander que D soit additive et nulle sur $\mathcal{R}$.

Exercice 1.43 Montrer que si X est un schéma et $p : \mathbf{A}^1_X \to X$ le morphisme structural, il existe une unique $p^{-1}(\mathcal{O}_X)$-dérivation $D : \mathcal{O}_{\mathbf{A}^1_X} \to \mathcal{O}_{\mathbf{A}^1_X}$ telle que $D(t) = 1$. On écrira $D =: \partial/\partial t$.

On introduit maintenant de manière un peu brutale le module des différentielles. Etant donné un morphisme de schémas $p : X \to S$, on cherche à représenter le foncteur qui a un $\mathcal{O}_X$-module $\mathcal{F}$ associe $Der_{\mathcal{O}_S}(\mathcal{O}_X, \mathcal{F})$ (on devrait écrire $Der_{p^{-1}(\mathcal{O}_S)}(\mathcal{O}_X, \mathcal{F})$). En d'autres termes, on cherche un $\mathcal{O}_X$-module $\Omega_{X/S}$, muni d'une $\mathcal{O}_S$-dérivation $d : \mathcal{O}_X \to \Omega_{X/S}$, tel que pour tout $\mathcal{O}_X$-module $\mathcal{F}$, l'application $u \mapsto D := u \circ d$ soit une bijection

$$Hom_{\mathcal{O}_X}(\Omega_{X/S}, \mathcal{F}) \tilde{\to} Der_{\mathcal{O}_S}(\mathcal{O}_X, \mathcal{F}).$$

Définition 1.5.2 *Soit X un S-schéma, $\delta : X \hookrightarrow X \times_S X$ l'immersion diagonale et $\mathcal{I}$ l'idéal de cette immersion. Le* faisceau des différentielles *de X sur S est $\Omega_{X/S} := \delta^{-1}(\mathcal{I}/\mathcal{I}^2)$. Si $S =:$* $\operatorname{Spec} R$*, on écrit $\Omega_{X/R} := \Omega_{X/S}$; si de plus $X =: SpecA$, on écrit $\Omega_{A/R} := \Gamma(X, \Omega_{X/R})$.*

Proposition 1.5.3 *Soit X un S-schéma. Alors*

i) Le faisceau $\Omega_{X/S}$ est un $\mathcal{O}_X$-module quasi-cohérent.

ii) Soient $p_1, p_2 : X \times_S X \to X$ les projections. Alors,

$$\delta^{-1}(p_2^*) - \delta^{-1}(p_1^*) : \mathcal{O}_X \to \delta^{-1}(\mathcal{O}_{X\times_S X})$$

est à valeur dans $\delta^{-1}(\mathcal{I})$ et induit une $\mathcal{O}_S$-dérivation $d : \mathcal{O}_X \to \Omega_{X/S}$.

iii) Le couple $(\Omega_{X/S}, d)$ représente le foncteur $Der_{\mathcal{O}_S}(\mathcal{O}_X, -)$

Démonstration: Il est clair que $\mathcal{I}/\mathcal{I}^2$ est un $\mathcal{O}_{X\times_S X}$-module quasi-cohérent sur lequel $\mathcal{I}$ agit trivialement. En appliquant δ^{-1}, on voit que $\Omega_{X/S}$ a une structure naturelle de $\mathcal{O}_X$-module et que celui-ci est quasi-cohérent.

Comme $p_i \circ \delta = Id_X$, on voit que la composée de $\delta^{-1}(p_i^*)$ avec la surjection $\delta^* : \delta^{-1}(\mathcal{O}_{X\times_S X}) \to \mathcal{O}_X$ est l'identité. Il suit que $\delta^{-1}(p_2^*) - \delta^{-1}(p_1^*)$ est à valeur dans le noyau $\delta^{-1}(\mathcal{I})$ de δ^*.

On remarque ensuite que si f et g sont deux sections locales de $\mathcal{O}_X$, alors fdg est représenté par la section $p_1^*(f)(p_2^*(g) - p_1^*(g))$ de $\delta^{-1}(\mathcal{O}_{X\times_S X})$. De même, gdf est représenté par la section $p_2^*(g)(p_2^*(f) - p_1^*(f))$. En sommant, on trouve $p_2^*(fg) - p_1^*(fg)$ qui représente $d(fg)$. Et d est donc bien une dérivation.

On sait que, localement, $\delta^{-1}(\mathcal{O}_{X\times_S X})$ est engendré sur $\delta^{-1}(\mathcal{O}_S)$ par les sections de la forme $p_1^*(f)p_2^*(g) = p_1^*(fg) + p_1^*(f)(p_2^*(g) - p_1^*(g))$. On peut en déduire que $\delta^{-1}(\mathcal{I})$ est localement engendré comme idéal par les sections de la forme $p_2^*(g) - p_1^*(g)$ (vérifier) et donc que $\Omega_{X/S}$ est localement engendré par les sections de la forme dg. En d'autres termes, $\Omega_{X/S}$ est engendré par l'image de $\mathcal{O}_X$.

Ce résultat nous donne l'unicité de la dernière assertion. Pour l'existence, on se done une dérivation $D : \mathcal{O}_X \to \mathcal{F}$. On munit $\mathcal{O}_X \oplus \mathcal{F}$ de sa structure triviale d'algèbre (localement $(f, m)(g, n) = (fg, fn + gm)$). On considère $\delta^{-1}(\mathcal{O}_{X\times_S X})$ comme une $\mathcal{O}_X$-algèbre en utilisant p_1. Il existe alors un unique morphisme de $\mathcal{O}_X$-algèbre $\delta^{-1}(\mathcal{O}_{X\times_S X}) \to \mathcal{O}_X \oplus \mathcal{F}$, qui, composé à gauche avec p_2^* donne l'identité sur $\mathcal{O}_X$ et D dans $\mathcal{F}$ (localement $p_1^*(f)(p_2^*(g) \mapsto (fg, fD(g)))$. On vérifie aisément que celui-ci envoit $\delta^{-1}(\mathcal{I})$ dans $\mathcal{F}$ et donc $\delta^{-1}(\mathcal{I}^2)$ sur 0 (car $\mathcal{F}$ est un idéal de carré nul). Il induit donc un morphisme $\Omega_{X/S} \to \mathcal{F}$ qui factorise bien D par d. □

Avant de pouvoir calculer efficacement des modules de différentielles, il faut démontrer quelques résultats qui permettent de faire des dévissages géométriques.

Si $f : Y \to X$ est un S-morphisme, la propriété universelle nous donne un morphisme $\Omega_{Y/S} \to \Omega_{Y/X}$. De même, la propriété universelle nous fournit un morphisme $\Omega_{X/S} \to f_*(\Omega_{Y/S})$ et donc, par adjonction, un morphisme $f^* : f^*(\Omega_{X/S}) \to \Omega_{Y/S}$. Enfin, si $Y \hookrightarrow X$ est une S-immersion d'idéal $\mathcal{I}$, la restriction à $\mathcal{I}$ de la dérivation de $\mathcal{O}_X$ induit un morphisme $\mathcal{N}_{Y/X} := i^{-1}(\mathcal{I}/\mathcal{I}^2) \to i^*(\Omega_{X/S})$. On dit que $\mathcal{N}_{Y/X}$ est le *faisceau conormal* à l'immersion.

Proposition 1.5.4 *i) Soit $f : Y \to X$ un S-morphisme, alors la suite*

$$f^*(\Omega_{X/S}) \to \Omega_{Y/S} \to \Omega_{Y/X} \to 0$$

est exacte.

ii) Soit $i : Y \hookrightarrow X$ une S-immersion d'idéal $\mathcal{I}$, alors la suite

$$\mathcal{N}_{Y/X} \to i^*(\Omega_{X/S}) \to \Omega_{Y/S} \to 0$$

est exacte.

Démonstration: Rappelons que dans une catégorie abelienne, une suite $M' \to M \to M'' \to 0$ est exacte ssi pour tout objet N, la suite $0 \to \mathrm{Hom}(M'', N) \to \mathrm{Hom}(M, N) \to \mathrm{Hom}(M'', N)$ est exacte (pour la réciproque, faire $N := \mathrm{Coker}(M' \to M)$).

Dans le premier cas, il s'agit donc de montrer que, pour tout $\mathcal{O}_Y$-module $\mathcal{F}$ la suite

$$O \to \mathrm{Hom}(\Omega_{Y/X}, \mathcal{F}) \to \mathrm{Hom}(\Omega_{Y/S}, \mathcal{F}) \to \mathrm{Hom}(f^*(\Omega_{X/S}), \mathcal{F})$$

est exacte. Or cette suite se réécrit

$$0 \to \mathrm{Der}_{\mathcal{O}_X}(\mathcal{O}_Y, \mathcal{F}) \to \mathrm{Der}_{\mathcal{O}_S}(\mathcal{O}_Y, \mathcal{F}) \to \mathrm{Der}_{\mathcal{O}_S}(\mathcal{O}_X, f_*(\mathcal{F})).$$

Et notre assertion résulte immédiatement des définitions.

De même, dans le second cas, on utilise la suite d'injections

$$\mathrm{Hom}_{\mathcal{O}_Y}(\mathcal{N}_{Y/X}, \mathcal{F}) \hookrightarrow \mathrm{Hom}_{i^{-1}(\mathcal{O}_X)}(\mathcal{N}_{Y/X}, \mathcal{F})$$
$$= \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{I}/\mathcal{I}^2, i_*(\mathcal{F})) \hookrightarrow \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{I}, i_*(\mathcal{F}))$$

pour se ramener à l'exactitude de la suite

$$0 \to \mathrm{Der}_{\mathcal{O}_S}(\mathcal{O}_Y, \mathcal{F}) \to \mathrm{Der}_{\mathcal{O}_S}(\mathcal{O}_X, i_*(\mathcal{F})) \to \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{I}, i_*(\mathcal{F})),$$

qui est encore immédiate. □

Les autres résultats sur les différentielles sont laissés en exercice :

Exercice 1.44 Montrer que si X est un S-schéma et U un ouvert de X, alors $(\Omega_{X/S})_{|U} = \Omega_{U/S}$.

Exercice 1.45 Montrer que si X est un S-schéma et $f : X' \to X$ le morphisme déduit d'un changement de base $S' \to S$, alors $\Omega_{X'/S'} = f^*(\Omega_{X/S})$.

Exercice 1.46 Montrer que si X et Y sont deux S-schémas, alors $\Omega_{X\times_S Y/S} = p_X^*(\Omega_{X/S}) \oplus p_Y^*(\Omega_{Y/S})$.

Avec tout ca, on peut facilement calculer les modules des différentielles.

Exercice 1.47 Montrer que si $A = R[t_1, \ldots, t_n]$, alors $\Omega_{A/R}$ est un module libre sur les dt_i et que pour tout $f \in A$, on a $df = \sum_{1\leq i\leq n}(\partial f/\partial t_i)dt_i$.

Exercice 1.48 Montrer que si $A = R[t_1, \ldots, t_n]/(f_1, \ldots, f_r)$, alors $\Omega_{A/R}$ est le quotient du A-module libre sur les dt_i par les relations $\sum_{1\leq j\leq n}(\partial f_i/\partial t_j)dt_j = 0$.

Exercice 1.49 Montrer que si C est une conique iréductible réduite (c'est à dire intègre) affine ou projective sur un corps k, alors Ω_C (on devrait écrire $\Omega_{C/k}$) est localement libre. Et si la conique n'est pas réduite, ou pas intègre ?

Exercice 1.50 Soit C la courbe affine plane d'équation $y^2 = x^3$ sur un corps k de caractéristique $\neq 2$. Montrer que Ω_C n'est pas localement libre. Même chose pour l'équation $y^2 = x^3 - x^2$. Et pour l'équation $y^2 = x^3 - x$?

Exercice 1.51 Pour les courbes de l'exercice précédent, considérer la projection $p : C \to \mathbf{A}^1_k$ sur l'axe des x ou l'axe des y. Calculer $\Omega_{C/\mathbf{A}^1_k}$. La suite

$$0 \to p^*(\Omega_{\mathbf{A}^1_k}) \to \Omega_C \to \Omega_{C/\mathbf{A}^1_k} \to 0$$

est elle exacte à gauche aussi ?

Exercice 1.52 Montrer que si $X := \mathbf{P}^n_S$, alors $\Omega_{X/S}$ est un module localement libre de rang n (on peut aussi montrer l'existence d'une suite exacte

$$0 \to \Omega_{X/S} \to \mathcal{O}_X(-1)^{n+1} \to \mathcal{O}_X \to 0).$$

Exercice 1.53 Montrer que si k'/k est une extension algèbrique séparable, alors $\Omega_{k'/k} = 0$.

Exercice 1.54 Soit k un corps de caractéristique $p > 0$, $K := k(t)$ et $K' := K[X]/(X^p - t)$. Montrer que $\Omega_{K'/K} \neq 0$.

Pour aller plus loin, il va falloir mettre des conditions de finitudes. La notion adoptée est celle de morphisme localement de présentation finie, qui se définit de la même manière que celle de morphisme localement de type fini. Et sur des schémas localement noethériens, les deux notions coincident.

Définition 1.5.5 *Un morphisme $f : Y \to X$ est* localement de présentation finie *si il existe un recouvrement affine ouvert $\{U_i\}_{i\in I}$ de X et pour tout $i \in I$ un recouvrement affine $\{V_{ij}\}_{j\in J_i}$ de $f^{-1}(U_i)$ tel que, si on écrit $U_i =: \operatorname{Spec} A_i$ et $V_{ij} =: \operatorname{Spec} B_{ij}$, alors B_{ij} est une A_i-algèbre de présentation finie (quotient d'un anneau de polynôme par un idéal de type fini). Le morphisme est dit* de présentation finie *si, en plus, il est quasi-compact.*

Comme pour les morphisme localement de type fini, on démontre un certain nombre de propriétés. Celles-ci sont laissées en exercice.

Exercice 1.55 Montrer que si $f : Y \to X$ et $g : Z \to Y$ sont localement de présentation finie, alors $f \circ g$ aussi.

Exercice 1.56 Montrer que si X est localement de présentation finie sur S et $S' \to S$ est un changemnent de base, alors $X' := X \times_S S'$ est localement de présentation finie sur S'.

Exercice 1.57 Montrer que si $f : Y \to X$ est un S-morphisme avec X localement de type fini et Y localement de présentation finie sur S, alors f est localement de présentation finie.

Exercice 1.58 Montrer que si $f : Y \to X$ et $f' : Y' \to X'$ sont deux morphismes localement de présentation finie de S-schémas, alors $f \times f' : Y \times_S Y' \to X \times_S X'$ est localement de présentation finie.

Nous aurons aussi besoin plus tard du résultat suivant (laissé aussi en exercice) et qui peut servir dans les exercices précédents.

Exercice 1.59 Montrer que si X est un S-schéma localement de type fini, alors l'immersion diagonale $\delta : X \hookrightarrow X \times_S X$ est localement de présentation finie. Montrer qu'en fait l'idéal $\mathcal{I}$ de cette immersion est de type fini. En particulier, $\Omega_{X/S}$ est un $\mathcal{O}_X$-module de type fini.

On va maintenant définir la notion de morphisme lisse. Il faut avoir à l'esprit que la définition qui suit, très formelle, n'est pas très maniable en pratique. Il faudra travailler un peu pour obtenir des caractérisations plus fonctionnelles.

Définition 1.5.6 *Un morphisme localement de présentation finie $f : X \to S$ est* lisse *(resp.* étale*, resp.* non-ramifié*) si pour tout S-schéma affine T et tout sous-schéma fermé T' définit par un idéal de carré nul, l'application $X(T)_S \to X(T')_S$ est surjective (resp. bijective, resp. injective).*

Par récurence, on peut remplacer dans cette définition l'idéal de carré nul par n'importe quel idéal nilpotent. D'autre part, pour la définition des morphismes étales ou non-ramifiés, il n'est pas nécessaire de supposer T affine (comme on peut le voir par recollement).

Exercice 1.60 Montrer que $\mathbf{A}^n_S$ est lisse sur S.

Exercice 1.61 Montrer que l'union de deux droites sécantes dans le plan affine sur un corps n'est pas lisse.

On va illustrer cette notion par un exemple fondamental.

Proposition 1.5.7 *Une extension de corps k'/k est finie séparable ssi le morphisme correspondant est étale.*

Démonstration: On se done donc une k-algèbre R, un idéal de carré nul I dans R et un k-morphisme $k' \to R/I$. Par le théorème de l'élément primitif, on peut écrire $k' = k[\alpha]$ et on choisit $a \in R$, tel que l'image de α dans R/I soit $a \mod I$. On veut montrer que notre morphisme se relève en un morphisme $k' \to R$. Un tel morphisme est déterminé par l'image de α et c'est un relèvement ssi cette image est de la forme $a + \epsilon$ avec $\epsilon \in I$. Si P est le polynôme minimal de α, on veut donc montrer qu'il existe un unique $\epsilon \in I$ tel que $P(a + \epsilon) = 0$. Et on sait que $P(a) = 0 \mod I$. Comme $I^2 = 0$, on a $P(a + \epsilon) = P(a) + \epsilon P'(a)$. Et puisque l'extension est séparable, $P'(a) \neq 0$. □

Pour bien comprendre la lissité, il est nécessaire de développer des critères plus efficaces. C'est l'objet du paragraphe suivant.

1.6 Morphismes lisses, propriétés

La dernière assertion de la proposition suivante, qui va nous demander un peu de travail (dans le cas lisse), est fondamentale pour comprendre la lissité.

Proposition 1.6.1 *i) Une immersion localement de présentation finie (resp. une immersion ouverte) est non-ramifiée (resp. étale).*

ii) Si $f : Y \to X$ et $g : Z \to Y$ sont, deux morphismes lisses (resp, non-ramifiés, resp. étales), alors $f \circ g$ est lisse (resp, non-ramifié, resp. étale).

iii) Si X est lisse (resp. non-ramifié, resp. étale) sur S et si $S' \to S$ est un changement de base, alors $X' := X \times_S S'$ est lisse (resp, non-ramifié, resp. étale) sur S'.

iv) Soit $f : Y \to X$ un S-morphisme avec Y non-ramifié et X localement de type fini sur S. Alors, f est non-ramifié.

v) Soient $f : Y \to X$ et $f' : Y' \to X'$ deux morphismes lisses (resp, non-ramifiés, resp. étales) de S-schémas. Alors, $f \times f' : Y \times_S Y' \to X \times_S X'$ est lisse (resp, non-ramifié, resp. étale).

vi) Soit $f : Y \to X$ un morphisme, $\{U_i\}$ un recouvrement ouvert de X et pour tout i, $\{V_{ij}\}$ un recouvrement de $f^{-1}(U_i)$. Si, pour tout i, j, le morphisme $V_{ij} \to U_i$ induit par f est lisse (resp, non-ramifié, resp. étale), alors f est lisse (resp, non-ramifié, resp. étale). Et réciproquement.

Démonstration: La quatrième et la cinquième assertion sont conséquences formelles des trois premières. Et celles ci sont conséquences immédiates des définitions (vérifier !). Il reste à démontrer la dernière assertion. La réciproque est immédiate en remarquant que si T' est un sous-schéma de T défini par un idéal nilpotent, il a même espace sous-jacent que T.

On se donne donc un X-schéma affine T et un sous-schéma T' défini par un idéal de carré nul. On se donne un X-point s' de Y à valeur dans T' et on note W'_{ij} l'image inverse de V_{ij} dans T'. Le point s' induit un U_i-point s'_{ij} de V_{ij}. On note W_{ij} le sous-schéma ouvert de T qui a même espace sous-jacent que W'_{ij}. Par construction, c'est un U_i-schéma.

On suppose d'abord que les morphismes $V_{ij} \to U_i$ sont non-ramifiés et on suppose que s' se relève en un point s de T à valeur dans Y. On veut montrer que s est unique. La question est locale sur Y et on conclut facilement.

On suppose maintenant que les morphismes $V_{ij} \to U_i$ sont lisses. Alors, les s'_{ij} se relèvent en des points s_{ij} de W_{ij} à valeurs dans V_{ij}. Il faut montrer que s' se relève en un point de T. C'est l'objet de la seconde partie du lemme suivant. □

Lemme 1.6.2 *Soit X un S-schéma, T un S-schéma, T' un sous-schéma de T défini par un idéal $\mathcal{I}$ de carré nul et s' un S-point de X à valeur dans T'. Alors,* *i) L'ensemble $\mathcal{E}(T) := \{s \in X(T)_S, s_{|T'} = s'\}$ est naturellement muni d'une action simplement transitive de $\mathcal{G}(T) := Hom_{\mathcal{O}_{T'}}(s'^*\Omega_{X/S}, \mathcal{I})$.*

ii) Si s' se relève localement sur T en un S-point de T et si T est affine, alors s' se relève globalement sur T.

Démonstration: Remarquons tout d'abord que comme $\mathcal{I}$ est un idéal de carré nul, c'est de manière évidente un $\mathcal{O}_{T'}$-module. En particulier, $s'_*\mathcal{I}$ est un $\mathcal{O}_X$-module. Remarquons aussi que si s est un relèvement de s', alors $s_* = s'_*$.

Soient s_1 et s_2 deux relèvement de s', alors $s_2^* - s_1^* : \mathcal{O}_X \to s'_*\mathcal{O}_T$ est à valeur dans $s'_*\mathcal{I}$ et fournit donc un morphisme $D : \mathcal{O}_X \to s'_*\mathcal{I}$. On peut vérifier que D est une S-dérivation. Réciproquement, si on se donne un relèvement s de s' et une S-dérivation $D : \mathcal{O}_X \to s'_*\mathcal{I}$, on obtient un autre relévement en substituant $s^* + D$ à s^*.

On voit donc que $\mathcal{E}(T)$ est muni d'une action simplement transitive de

$$Der_S(\mathcal{O}_X, s'_*\mathcal{I}) = Hom_{\mathcal{O}_X}(\Omega_{X/S}, s'_*\mathcal{I}) = Hom_{\mathcal{O}_{T'}}(s'^*\Omega_{X/S}, \mathcal{I}) = \mathcal{G}(T).$$

Bien sûr, dans cette construction, on peut substituer à T n'importe quel ouvert W de T et les différentes constructions sont compatibles. On définit ainsi un faisceau d'ensembles $\mathcal{E}$ sur T qui est muni d'une action simplement transitive du groupe $\mathcal{G} := \mathcal{H}om_{\mathcal{O}_{T'}}(s^*\Omega_{X/S}, \mathcal{I})$ (on appelle ça un *pseudo-torseur*).

Dire que s' se relève localement sur T en un S-point de T signifie qu'il existe un recouvrement ouvert $\{W_i\}$ de T tel que pour tout i, on ait $\mathcal{E}(W_i) \neq \emptyset$ (on dit alors que $\mathcal{E}$ est un *torseur* sous $\mathcal{G}$). Chosissons alors pour tout i un relevement s_i de s' sur W_i. Pour chaque couple (i,j), il existe alors un unique $D_{ij} \in \mathcal{G}(W_i \cap W_j)$ tel que $s^*_{j|W_i} - s^*_{i|W_j} = D_{ij}$ et ceux ci satisfont la *condition de cocycle* $D_{ij|W_k} + D_{jk|W_i} = D_{ik|W_j}$. Comme $\mathcal{G}$ est quasi-cohérent et qu'on a supposé T affine, il résulte de la proposition suivante qu'il existe une famille $\{D_i\}$ avec $D_i \in \mathcal{G}(W_i)$ tels que pour tout i,j, on ait $D_{j|W_i} - D_{i|W_j} = D_{ij}$. On remplace alors, pour tout i, s_i^* par $s_i^* + D_i$. On obtient $s_{j|W_i} = s_{i|W_j}$ et les s_i se recollent pour donner le s tant attendu.

Remarquons pour finir que, pour démontrer ce lemme, on peut remplacer le recouvrement par un recouvrement plus fin. En particulier, on peut supposer que s' se relève sur un recouvrement affine standard $T = W_1 \cup \cdots \cup W_n$ avec $W_i = D(f_i)$. De plus, par récurrence, on peut supposer que ce recouvrement est réduit à deux ouverts : En effet, on peut écrire $\sum_{1 \leq i \leq n} h_i f_i = 0$. On pose $f := 1 - h_1 f_1$ et $W := D(f)$. Alors, $T = W_1 \cup W$

est un recouvrement standard et $W = (W_2 \cap W) \cup \cdots \cup (W \cap W_n)$ aussi. $\square$

Ce que nous venons de voir dans la démonstration de ce lemme se généralise. Dans ce qui suit, les détails sont laissés en exercice. Si on se donne un faisceau de groupes $\mathcal{G}$ sur un espace topologique X, une *action* de $\mathcal{G}$ sur un faisceau d'ensemble $\mathcal{E}$ est un morphisme de groupes $\mathcal{G} \to \mathcal{E}nd(\mathcal{E})$. On dit ausi que $\mathcal{E}$ est un $\mathcal{G}$-ensemble. Les $\mathcal{G}$-ensembles forment de manière évidente une catégorie. On dit que le $\mathcal{G}$-ensemble $\mathcal{E}$ est un *pseudo-torseur* si pour tout ouvert $U \in X$, l'action induite de $\mathcal{G}(U)$ sur $\mathcal{E}(U)$ est simplement transitive. On dit que c'est un *torseur* si, en plus, il existe un recouvrement $\mathcal{U} := \{U_i\}$ de X tel que, pour tout i, on ait $E(U_i) \neq \emptyset$. On dit alors que $\mathcal{E}$ se *trivialise* sur $\mathcal{U}$.

Un *1-cocycle* associé au recouvrement $\mathcal{U}$ est une famille de $g_{ij} \in \mathcal{G}(U_i \cap U_j)$ tel que $g_{ij|U_k} g_{jk|U_i} = g_{ik|U_j}$. Ceux-ci forment de manière évidente un groupe $Z^1(\mathcal{U}, \mathcal{G})$. A une trivialisation sur $\mathcal{U}$ du torseur $\mathcal{E}$, on associe un 1-cocycle comme dans la démonstration du lemme.

On dit qu'un 1-cocycle est est un *1-cobord* s'il existe une famille $\{g_i\}$ avec $g_i \in \mathcal{G}(W_i)$ tels que pour tout i, j, on ait $g_{j|W_i} g_{i|W_j}^{-1} = g_{ij}$. Ceux-ci forment un sous-groupe $B^1(\mathcal{U}, \mathcal{G})$ du groupe des 1-cocycles. On note $H^1(\mathcal{U}, \mathcal{G}) = Z^1(\mathcal{U}, \mathcal{G})/B^1(\mathcal{U}, \mathcal{G})$. On obtient ainsi une bijection entre les classes d'isomorphie de torseurs trivialisés sur $\mathcal{U}$ et l'ensemble $H^1(\mathcal{U}, \mathcal{G})$. En passant à la limite, on obtient même une bijection entre les classes d'isomorphie de torseurs sous $\mathcal{G}$ et l'ensemble $\check{H}^1(X, \mathcal{G}) := \varinjlim H^1(\mathcal{U}, \mathcal{G})$.

Avec ces notations, le résultat dont nous avons besoin est le suivant.

Proposition 1.6.3 *Soit $\mathcal{F}$ un faisceau quasi-cohérent sur un schéma affine X. Soit $\mathcal{U}$ un recouvrement ouvert de X. Alors $H^1(\mathcal{U}, \mathcal{G}) = 0$.*

Démonstration: On peut se ramener à un recouvrement standard par deux ouverts. Cette réduction est laissée en exercice car, comme remarqué à la fin de la démonstration du lemme, c'est le seul cas dont nous avons besoin.

On se donne donc un anneau A, un A-module M et $f, g \in A$ premiers entre eux (qui engendrent l'idéal unité de A). On se donne $m \in M_{fg}$. On peut écrire $m = \frac{m'}{(fg)^r}$ avec $m' \in A$ et $r \in \mathbf{N}$. Comme f et g sont premiers entre eux, il en va de même de f^r et g^r et on peut donc écrire $hg^r - kf^r = 1$ dans A. On a alors $m = (hg^r - kf^r)m = h\frac{m'}{f^r} - k\frac{m'}{g^r}$. $\square$

La propriété suivante dont la démonstration est formelle (et ne nécessite pas le résultat que nous venons de démontrer) est laissés en exercice.

Exercice 1.62 Montrer que si $f : Y \to X$ est un S-morphisme avec X non-ramifié sur S et Y lisse (resp. étale, non-ramifié) sur S, alors f est lisse (resp. étale, non-ramifié).

Proposition 1.6.4 *Soit $f : Y \to X$ un morphsime localement de présentation finie. Alors, les conditions suivantes sont équivalentes*

i) Le morphisme f est non-ramifié.

ii) On a $\Omega_{Y/X} = 0$.

iii) L'immersion diagonale $\delta : Y \hookrightarrow Y \times_X Y$ est ouverte.

Démonstration: La seconde condition implique bien grâce au lemme 1.6.2 i) que f est non-ramifié.

D'autre part, comme l'ideal $\mathcal{I}$ de l'immersion diagonale est de type fini, on voit que $\Omega_{Y/X} = 0$ ssi $i^{-1}(\mathcal{I}) = 0$, c'est à dire ssi δ est une immersion ouverte.

Pour conclure, il suffit de montrer que montrer que si f est non-ramifié, alors $\Omega_{Y/X} = 0$. On sait que δ induit un isomorphisme de Y sur un sous-schéma T' de $Y \times_X Y$. Soit Δ le sous-schéma fermé de $Y \times_X Y$ défini par $\mathcal{I}^2$ et T l'ouvert de Δ ayant même espace sous-jacent que T'. Les deux projections $p_1, p_2 : Y \times_X Y \to Y$ induisent des morphismes $s_1, s_2 : T \to Y$ qui relèvent s. Par construction, l'idéal $\bar{I}$ engendré par les $s_2^*(f) - s_1^*(f)$ est l'idéal de T' dans T. Si f est non-ramifié, alors $s_1 = s_2$ et donc $\bar{I} = 0$. Il suit que $T = T'$ et donc que $\Omega_{Y/X} = 0$. $\square$

Exercice 1.63 0n considére la courbe affine plane C d'équation $y^2 = x^3$ sur un corps k de caractéristique $\neq 2$. La projection p sur l'axe des x ou des y est il un morphisme non-ramifié ? Même question pour les coubes d'équation $y^2 = x^3 - x^2$ où $y^2 = x^3 - x$.

On a l'habitude de dire qu'un morphisme $f : Y \to X$ est lisse (étale, non-ramifié) en un point $y \in Y$ s'il l'est sur un voisinage de y. Dans le cas non-ramifié, cet abus est justifié par la proposition suivante.

Proposition 1.6.5 *Soit $f : Y \to X$ un morphisme localement de présentation finie, $y \in Y$ et $x := f(y)$. Alors, les condition suivantes sont équivalentes :*

i) Le morphisme f est non-ramifié au voisinage de y.

ii) Le schéma $f^{-1}(x)$ est non-ramifé sur $k(x)$ au voisinage de y.

Démonstration: Par changement de base, la première condition implique la seconde. Pour montrer la réciproque, on note $i : f^{-1}(x) \hookrightarrow Y$ et

$i_y : \operatorname{Spec} k(y) \hookrightarrow f^{-1}(x)$ les morphismes d'inclusion. On a

$$\begin{aligned}\Omega_{Y/X,y} \otimes_{\mathcal{O}_{Y,y}} k(y) &= \Gamma(\operatorname{Spec} k(y), (i \circ i_y)^* \Omega_{Y/X}) \\ &= \Gamma(\operatorname{Spec} k(y), i_y^* \Omega_{f^{-1}(y)/k(y)}) = 0.\end{aligned}$$

Or on sait que $\Omega_{Y/X}$ est de type fini. Par Nakayama, on obtient que $\Omega_{Y/X,y} = 0$ et donc que $\Omega_{Y/X}$ est nul au vosinage de y. □

On peut donc voir si un morphisme est non-ramifié en étudiant cette notion pour les shémas sur un corps. Dans ce cas, on a une description explicite. Nous aurons besoin d'un résultat d'algèbre commutative.

Définition 1.6.6 *Soient k un corps, $\bar{k}$ une clôture algébrique de k et A une k-algèbre. On dit que A est* séparable *sur k si le radical de Jacobson de $\bar{A} := A \otimes_k \bar{k}$ est nul.*

En d'autres termes, si on pose $\bar{X} = \operatorname{Spec} \bar{A}$, cela signifie que l'application canonique $\bar{A} \to \bar{k}^{|\bar{X}|}, f \to \{f(x)\}_{x \in \bar{X}}$ est injective. Le résultat dont nous aurons besoin est laissé en exercice.

Exercice 1.64 Soient k un corps et A une k-algèbre de type fini. Montrer que A est finie séparable ssi A est isomorphe à un produit fini d'extension finies séparables de k.

Proposition 1.6.7 *Un schéma X sur un corps k est non-ramifié ssi c'est une somme disjointe de spectres d'extensions finies séparables de k. En particulier, il est étale.*

Démonstration: Comme une extension finie séparable de corps fournit bien un morphisme étale (exercice), la condition est suffisante et la dernière assertion est vérifiée. Pour montrer que la condition est nécessaire, on peut supposer que $X = \operatorname{Spec} A$ affine et et il s'agit de montrer A est finie séparable. On peut donc prendre k algébriquement clos.

Si x est un point fermé de X, on lui associe un morphisme $i : \operatorname{Spec} k \hookrightarrow X$. En faisont le produit avec l'identité, on en déduit un morphisme $s : X = X \otimes_k k \to X \times_k X$ (localement, $y \mapsto (x, y)$). On a donc un diagramme cartésien

$$\begin{array}{ccc} X & \hookrightarrow & X \times_k X \\ \uparrow & & \uparrow \\ \operatorname{Spec} k & \hookrightarrow & X \end{array}$$

et comme δ est une immersion ouverte, il en va de même de i. Il suit que x est ouvert (et fermé) dans X. On voit donc que l'ensemble $|X|$ des points fermés de X est un ouvert discret de X. Comme X est affine de type fini sur k, il est noetherien et $|X|$, qui est ouvert, est donc quasi-compact. Comme c'est un ensemble discret, il est fini. Et X étant de type fini sur k, c'est un schéma fini sur k, somme disjointe de ses points. Enfin, comme la question est locale, on peut supposer X réduit à un point x. L'immersion diagonale est alors bijective. Comme c'est une immersion ouverte, c'est un isomorphisme. Il suit que $X = \operatorname{Spec} k$. □

A ce point, on a vraiment une vision claire de la notion de morphisme non-ramifié : c'est un morphisme dont les fibres sont des unions disjointes d'extensions séparables. On va s'attaquer maintenant aux deux autres notions. On montre d'abord un résultat classique sur les morphismes lisses.

Proposition 1.6.8 *i) Si $f : Y \to X$ est un morphisme lisse, alors $\Omega_{Y/X}$ est localement libre.*

ii) Soit $f : Y \to X$ un S-morphisme lisse, alors la suite

$$0 \to f^*(\Omega_{X/S}) \to \Omega_{Y/S} \to \Omega_{Y/X} \to 0$$

est exacte et localement scindée.

iii) Soit $i : Y \hookrightarrow X$ une S-immersion. Si Y est lisse sur S, la suite

$$0 \to \mathcal{N}_{Y/X} \to i^*(\Omega_{X/S}) \to \Omega_{Y/S} \to 0$$

est exacte et localement scindée.

Démonstration: Montrons la première assertion. La question est locale. On peut donc supposer que f provient d'un morphisme d'anneaux $A \to B$. Pour montrer que $\Omega_{B/A}$ est projectif, on se donne un homomorphisme surjectif de B-modules $M \to N$. Il faut montrer que $\operatorname{Hom}_B(\Omega_{B/A}, M) \to \operatorname{Hom}_B(\Omega_{B/A}, N)$ est surjectif, c'est à dire que $\operatorname{Der}_A(B, M) \to \operatorname{Der}_A(B, N)$ est surjectif. On se donne donc une A-dérivation $D : B \to N$ que l'on étend en un morphisme de A-algèbres $\phi : B \to B \oplus N$. On considère alors le morphisme surjectif de A-algèbres $B \oplus M \to B \oplus N$. Son noyau est contenu dans M qui est un idéal de carré nul. Comme B est lisse sur A, le morphisme ϕ se relève en un morphisme $\psi : B \to B \oplus N$. On compose avec la projection sur M pour obtenir une dérivation qui relève D (vérifier).

De même, pour montrer la seconde assertion, on se ramène à montrer que si $A \to B$ est un morphisme lisse de R-algèbres et M un B-module, l'application $\operatorname{Der}_R(B, M) \to \operatorname{Der}_R(A, M)$ est surjective. Une R-dérivation $D : A \to M$ permet de munir $B \oplus M$ d'une structure de A-algèbre et comme B est lisse sur A, l'identité se relève en un morphisme de B-algèbres $B \to B \oplus M$ qui fournit un relèvement de D.

Pour la dernière assertion, la technique est identique. □

En fait, la dernière assertion de la proposition précédente posséde une réciproque.

Proposition 1.6.9 *Soit $i : Y \hookrightarrow X$ une S-immersion dans un schéma lisse, d'idéal $\mathcal{I}$. Alors, Y est lisse sur S ssi la suite*

$$0 \to \mathcal{N}_{Y/X} \to i^*(\Omega_{X/S}) \to \Omega_{Y/S} \to 0$$

est exacte et localement scindée.

Démonstration: On sait que la condition est nécessaire. On se donne un S-schéma affine T et un sous-schéma fermé T' défini par un idéal $\mathcal{J}$ de carré nul. Soit $s' \in Y(T')_S$. Comme X est lisse, $i \circ s'$ se relève en $s \in X(T)_S$. On sait que $s \in Y(T)_S$ ssi s^* est nul sur $s^{-1}(\mathcal{I})$. En fait, s^* induit un morphisme de $s'^{-1}\mathcal{O}_Y$-modules $s'^{-1}\mathcal{N}_{Y/X} = s^{-1}(\mathcal{I}/\mathcal{I}^2) \to \mathcal{J}$. Celui-ci correspond à un un morphisme de $\mathcal{O}_T$-modules $\delta : s'^*\mathcal{N}_{Y/X} \to \mathcal{J}$ et on a $s \in Y(T)_S$ ssi $\delta = 0$.

On va reformuler ça : soient E_Y et E_X les ensembles de points qui prolongent à T, s' et $i \circ s'$, respectivement, et $H = \mathrm{Hom}_{\mathcal{O}_T}(s'^*\mathcal{N}_{Y/X}, \mathcal{J})$. On a donc une application $E_X \to H$ dont la fibre en 0 est E_Y. Notons $G_Y := \mathrm{Hom}_{\mathcal{O}_T}(s'^*\Omega_{Y/S}, \mathcal{J})$ et $G_X := \mathrm{Hom}_{\mathcal{O}_T}(s'^*i^*(\Omega_{X/S}), \mathcal{J})$. Il résulte de nos hypothèses que l'on a une suite exacte

$$0 \to G_Y \to G_X \to H \to 0.$$

Les ensembles E_X, E_Y et H etant munis d'une action simplement transitive de G_X, G_Y et H et nos constructions étant compatibles à ces actions, la conclusion est formelle (vérifier). □

Nous allons maintenant établir le critère jacobien. On va introduire un peu de vocabulaire.

Définition 1.6.10 *Soit X un S-schéma lisse. On dit que des sections globales $t_1, \ldots, t_n$ de $\mathcal{O}_X$ sont des* coordonnées *sur X/S si $dt_1, \ldots, dt_n$ forment une base de $\Omega_{X/S}$. Si f est une section globale de $\mathcal{O}_X$, on écrit $df =: \sum \partial f/\partial t_i dt_i$.*

Définition 1.6.11 *Soit X un S-schéma et $x \in X$. Une* présentation *de X au voisinage de x au dessus de S est la donnée d'une immersion $i : U \hookrightarrow Z$*

d'un voisinage ouvert de x dans un S-schéma lisse, de coordonnées $t_1, \ldots, t_n$ sur Z et de générateurs $f_1, \ldots, f_r$ de l'idéal $\mathcal{I}$ de i sur Z. On dit alors que $J := [\partial f_i/\partial t_j]$ est la matrice jacobienne *associée à cette présentation. Enfin, on dit que la présentation est* minimale *en x si $f_1, \ldots, f_r$ est un système minimal de générateurs de $\mathcal{I}$ au voisinage de x (c'est à dire dans $\mathcal{O}_{Z,x}$.*

En pratique, on prend pour U un voisinage affine $\operatorname{Spec} A$ de x au dessus d'un ouvert $\operatorname{Spec} R$ de S, on écrit $A =: R[t_1, \ldots, t_n]/(f_1, \ldots, f_r)$ et on prend $Z := \mathbf{A}^n_R$.

Nous aurons aussi besoin des notations suivantes. Si $\mathcal{F}$ est un faisceau sur un schéma X et s une section de $\mathcal{F}$ sur un voisinage de x, on notera $s(x)$ l'image de s dans $\mathcal{F} \otimes k(x) := \mathcal{F}_x \otimes_{\mathcal{O}_{X,x}} k(x)$.

Proposition 1.6.12 *(Critère jacobien) Soit X un S-schéma muni d'une présentation au voisinage d'un point x. Alors, la jacobienne évaluée en x, $J(x)$, est de rang maximal ssi X est lisse sur S en x et la présentation est minimale en x.*

Démonstration: On se donne donc une immersion $i : U \hookrightarrow Z$ d'un voisinage ouvert U de x dans un S-schéma lisse, des générateurs $f_1, \ldots, f_r$ de l'idéal $\mathcal{I}$ de i et une base de la forme $dt_1, \ldots, dt_n$ de $\Omega_{Z/S}$. Dire que $J(x)$ est de rang maximal signifie que $df_1(x), \ldots, df_r(x)$ sont linéairement indépendants dans $\Omega_{Z/S} \otimes k(x)$. Quitte à faire un changement de coordonnées, cela signifie encore que

$$df_1(x), \ldots, df_r(x), dt_{r+1}(x), \ldots dt_n(x)$$

forment une base de $\Omega_{Z/S} \otimes k(x)$. Par Nakayama, et quitte à rétrécir Z, cela veut dire que $df_1, \ldots, df_r, dt_{r+1}, \ldots dt_n$ forment une base de $\Omega_{Z/S}$.

En d'autres termes, notre condition signifie que

$$0 \to \mathcal{N}_{Z/U} \to i^*(\Omega_{Z/S}) \to \Omega_{U/S} \to 0$$

est exacte et scindée et que les images de $f_1, \ldots, f_r$ dans $\mathcal{N}_{Z/U}$ forment une base.

On traduit une dernière fois notre hypothèse. La première partie signifie que X est lisse en x. Et la seconde partie nous dit que les $f_1, \ldots, f_r$ forment un système minimal de générateurs de $\mathcal{I}$ au voisinage de x (appliquer Nakayama à $\mathcal{I}_x$ dans $\mathcal{O}_{Z,x}$). $\square$

Exercice 1.65 Soit R un anneau et H une hypersurface de $\mathbf{A}^n_R$ définie par un polynôme (non-constant) f. Montrer que H est lisse en x sur R ssi il existe i tel que $(\partial f/\partial t_i)(x) \neq 0$.

Exercice 1.66 Soit k un corps de caractéristique $p > 0$ et V l'hypersurface diagonale d'équation $\sum_{i=0}^{n} X_i^d = 0$ dans $\mathbf{P}_k^n$. A quelle condition V est elle lisse ?

Exercice 1.67 Soit C une cubique projective irréductible et réduite sur un corps algébriquement clos de caractéristique > 3. Montrer que si C n'est pas lisse, alors C est isomorphe à la courbe d'équation $y^2z = x^3$ où à la courbe d'équation $y^2z = x^3 - x^2z$.

Exercice 1.68 Avec les hypothèses de la proposition, montrer que $J(x)$ est carrée inversible ssi X est étale sur S en x et la présentation est minimale en x.

La seconde assertion de la propostion 1.6.8 possède aussi une réciproque.

Proposition 1.6.13 *Soit $f : Y \to X$ un S-morphisme entre schémas lisses. Alors f est lisse ssi la suite*

$$0 \to f^*(\Omega_{X/S}) \to \Omega_{Y/S} \to \Omega_{Y/X} \to 0$$

est exacte et localement scindée. En particulier, f est étale ssi

$$f^*(\Omega_{X/S}) \tilde{\to} \Omega_{Y/S}.$$

Démonstration: On sait que la condition est nécéssaire. Montrons qu'elle est suffisante. On peut factoriser f en une immersion $i : Y \hookrightarrow Z$ suivie d'un morphisme lisse $p : Z \to X$ (prendre par exemple l'immersion diagonale et la projection). Par hypothèse, on a une suite exacte localement scindée

$$(*) 0 \to f^*(\Omega_{X/S}) \to \Omega_{Y/S} \to \Omega_{Y/X} \to 0.$$

Mais comme Z aussi est lisse sur S, on a une suite exacte localement scindée

$$0 \to p^*(\Omega_{Y/S}) \to \Omega_{Z/S} \to \Omega_{Z/Y} \to 0$$

et en prenant l'image invers par i, on obtient une suite exacte localement scindée

$$(**) 0 \to f^*(\Omega_{Y/S}) \to i^*\Omega_{Z/S} \to i^*\Omega_{Z/Y} \to 0.$$

On a bien sûr un morphisme de suites exacte de $(**)$ dans $(*)$. Comme X est lisse sur S, la suite

$$0 \to \mathcal{N}_{Z/X} \to i^*(\Omega_{Z/S}) \to \Omega_{X/S} \to 0$$

est exacte localement scindée. Il suit que la suite

$$0 \to \mathcal{N}_{Z/X} \to i^*(\Omega_{Z/Y}) \to \Omega_{X/Y} \to 0$$

l'est aussi. Cela signifie bien que f est lisse.

La seconde assertion résulte du fait que f est étale ssi f est non-ramifié, et que f est non-ramifié ssi $\Omega_{X/Y} = 0$. □

On peut raffiner un peu ce résultat :

Exercice 1.69 Avec les hypothèses de la proposition précédente, montrer que f est lisse (resp. étale) en y ssi $f^*(\Omega_{X/S}) \otimes k(y) \to \Omega_{Y/S} \otimes k(y)$ est injectif (resp. bijectif).

De notre proposition, on déduit une autre description de la notion de coordonnées locales.

Corollaire 1.6.14 *Soit X un S-schéma et $t_1, \ldots, t_n \in \Gamma(X, \mathcal{O}_X)$. Dire que le morphisme correspondant $t : X \to \mathbf{A}^n_S$ est étale signifie que X est lisse et que $t_1, \ldots, t_n$ forment un système de coordonnées locales sur X.*

On peut définir la notion de topologie sur une catégorie. Il s'agit de se donner des morphismes, qui correspondent aux ouverts, et des familles de morphimes qui correspondent aux recouvrements. L'exemple fondamental est celui de la catégorie des espaces topologiques. Un ouvert est une aplication $U \to X$ qui induit un homéomorphisme entre U et son image dans X. Un recouvrement est une famille d'ouverts $\{U_i \to X\}_{i \in I}$ qui est surjective (tout point de X est dans l'image de l'un des U_i.

On peut faire la même chose avec la catégorie de schémas sur une base S : les ouverts sont les immersions ouvertes et les recouvrements sont les familles surjectives d'immersions ouvertes. Idem avec la catégorie des variétés holomorphes (ou plus généralement, des espaces analytiques) sur $\mathbf{C}$. Dans ce cas, on dispose du théorème d'inversion locale qui dit qu'un morphisme est un isomorphisme local ssi il induit un isomorphisme sur les différentielles. De même, une variété est holomorphe ssi elle est localement isomorphe à $\mathbf{C}^n$. L'analogue pour la topologie de Zariski est faux (une courbe elliptique n'est pas localement isomorphe à une droite). Il est donc nécessaire de remplacer la topologie de Zariski par une topologie plus riche. On prend la topologie étale. Les ouverts sont les morphismes étales et les recouvrements sont les familles surjectives. On vient alors de voir le théoréme d'inversion locale qui dit qu'un morphisme entre deux schémas lisses est étale en un point ssi il induit un isomorphisme sur les modules de différentielles au voisinage de ce point. On peut aussi montrer qu'un S-schéma X est lisse ssi il est localement isomorphe pour la topologie étale à $\mathbf{A}^n_S$. C'est une conséquence du théorème des fonctions implicites que lon va déduire, comme dans le cas classique, du théorème d'inversion locale.

Proposition 1.6.15 *Un schéma X est lisse sur S en $x \in X$ ssi il existe un voisinage ouvert U de x et un morphisme étale $U \to \mathbf{A}^n_S$ au dessus de S.*

Démonstration: Il s'agit de montrer que si X est lisse sur S en $x \in X$, on peut trouver un système de coordonnées locales au voisinage de x. Or ceci est clair car on peut supposer $\Omega_{X/S}$ libre et on sait qu'il est engendré par l'image de $\mathcal{O}_X$. □

Une autre notion fondamentale que nous n'aurons pas le temps d'étudier est celle de platitude. La section suivante liste définitions et les premiers résultats.

1.7 Quelques mots sur la platitude

La notion de morphisme plat est une notion plus faible que celle de morphisme lisse (pour les morphismes localement de présentation finie) qui permet de ramener certains problemes a un calcul sur les fibres.

Définition 1.7.1 *Soit $f : Y \to X$ un morphisme de schémas. Soit $y \in Y$ et $x := f(y)$, alors f est* plat *en y si $\mathcal{O}_{Y,y}$ est plat sur $\mathcal{O}_{X,x}$. Le morphisme f est* plat *s'il est plat en tout point de Y.*

Exercice 1.70 Montrer que $\operatorname{Spec} A \to \operatorname{Spec} B$ *est plat ssi $A \to B$ est plat.*

Exercice 1.71 Montrer qu'une immersion ouverte est un morphisme plat.

Exercice 1.72 Montrer que si $f : Y \to X$ et $g : Z \to Y$ sont deux morphismes plats, alors $f \circ g$ est plat.

Exercice 1.73 Montrer que si X est plat sur S et si $S' \to S$ est un changement de base, alors $X' := X \times_S S'$ est plat sur S'.

Exercice 1.74 Montrer que si $f : Y \to X$ et $f' : Y' \to X'$ sont deux morphismes plats de S-schémas, alors $f \times f' : Y \times_S Y' \to X \times_S X'$ est plat.

Exercice 1.75 Montrer que si $f : Y \to X$ un morphisme, $\{U_i\}$ un recouvrement ouvert de X et pour tout i, $\{V_{ij}\}$ un recouvrement de $f^{-1}(U_i)$ tels que les morphismes $V_{ij} \to U_i$ induits par f sont plats, alors f est plat. Et réciproquement.

Voici par exemple une application de cette notion.

Proposition 1.7.2 *Soit $f : Y \to X$ un morphisme localement de présentation finie, $y \in Y$ et $x := f(y)$. Alors, f est lisse en y si f est plat en y et $f^{-1}(y)$ est lisse sur $k(x)$.*

Démonstration: Non rédigé. □

On en a fini avec ces notions. On va revenir maintenant aux conjectures de Weil.

1.8 Approche naïve des conjectures de Weil

On revient à notre problème. Et on rapelle tout d'abord la première conjecture de Weil.

Théorème 1.8.1 (Conj. de Weil, rationalité, version additive) *Soit X une variété algébrique sur $\mathbf{F}_q$. Alors, il existe des entiers algébriques α_i, β_j tels que pour tout r, on ait $N_r(X) = \sum \alpha_i^r - \sum \beta_j^r$.*

On va regarder de plus près le cas propre et lisse. Dans ce cas, on a déja une précision sur le résultat de pureté.

Théorème 1.8.2 (Conj. de Weil, pureté, version additive) *Si X est de dimension d, les entiers algébriques α_i et β_j sont des nombres de Weil de poids $\in [0, 2d]$. Si X est propre et lisse, les poids sont pairs pour les α_i et impairs pour les β_j.*

Exercice 1.76 Vérifier cette conjecture pour une variété linéaire projective, pour la quadrique de Segre et pour un schéma fini étale.

On peut aussi regarder maintenant l'équation fonctionnelle. On rappelle que X est de *pure* dimension d si toutes les composantes connexes ont dimension d.

Théorème 1.8.3 (Conj. de Weil, éq. fonct., version additive) *Si X est propre et lisse de pure dimnension d, alors, l'application $\gamma \mapsto q^d/\gamma$ induit une permutations des α_i et une permutation des β_j.*

Ce résultat est dû à Grothendieck ([10]) et date de 1965.

Exercice 1.77 Vérifier cette conjecture pour une variété linéaire projective, pour la quadrique de Segre et pour un schéma fini étale.

Pour aller au dela, il est nécessaire d'avoir une meilleure formulation de ces conjectures. Celle ci passe par le formalisme des fonctions zéta.

Chapitre 2

Etude des conjectures de Weil

Dans ce chapitre, on va reformuler les conjectures de Weil en termes de fonctions zéta et démontrer ces conjectures pour les hypersurfaces diagonales.

2.1 Fonctions zétas arithmétiques

En théorie analytique des nombres, les *séries de Dirichlet* jouent un rôle très important. Ce sont les fonctions complexes d'une variable complexe qui admettent un développement en série de la forme

$$f(s) = \sum_{n=1}^{\infty} a_n n^{-s}.$$

On reviendra plus tard sur ces fonctions. Pour l'instant, on va donner une approche algébrique de cette notion. Les propriétés, faciles à démontrer seront laissées en exercice.

Soit R un anneau. Une *fonction arithmétique* à valeur dans R est un élément de $\mathcal{A} := R^{\mathbf{N}^*}$. On peut donc le voir comme une fonction $f : \mathbf{N}^* \to R$ ou comme une suite (a_n) d'éléments de R indexée par N^*. Le *produit de convolution* est défini par $(a_n) * (b_n) =: (c_n)$ avec $c_n := \sum_{ij=n} a_i b_j$. On peut généraliser cette notion en remplacant $\mathbf{N}$ par le monoïde les idéaux d'un anneau de Dedekind. Nous ne le ferons pas car nous n'en aurons pas besoin.

Exercice 2.1 Montrer que $\mathcal{A}$ est une R-algèbre commutative unitaire. Montrer que les inversibles sont les (a_n) avec $a_1 \in R^*$.

Pour faire le lien avec les séries de Dedekind, note n^{-s} l'élément de $\mathcal{A}$ tel que $a_n = 1$ et $a_m = 0$ pour $m \neq n$. Cette notation est justifée par le résultat qui suit.

Exercice 2.2 Montrer que $n^{-s}m^{-s} = (nm)^{-s}$.

On peut aussi montrer que $\mathcal{A}$ est une algèbre de séries formelles.

Exercice 2.3 Soit P *l'ensemble des nombres premiers* $A := R[[\{t_p\}_{p\in P}]]$. *Montrer qu'il existe un unique isomorphisme d'anneaux* $A \to \mathcal{A}$ *tel que* $t_p \to p^{-s}$ *(on pourra remarquer que, par définition* $A = R^{\mathbf{N}[P]}$ *où* $\mathbf{N}[P]$ *est le monoïde engendré par* P*, et utiliser la bijection* $\mathbf{N}^* \tilde{=} \mathbf{N}[P]$ *correspondant à la décomposition des entiers non-nuls en facteurs premiers).*

On munit R de la topologie discrète et $\mathcal{A}$ de la topologie produit.

Exercice 2.4 Montrer que $\mathcal{A}$ *est une* R*-algèbre linéairement topologisée (les opérations sont continues et il exite un système fondamental (dénombrable) de voisinages de zéro formé d'idéaux* I_n*).*

Exercice 2.5 Montrer que $\mathcal{A}$ *est séparé et complet (on peut prendre pour distance* $d(f,g) = e^{-n}$ *ou* n *est le plus grand entier tel que* $g - f \in I_n$*). Montrer en fait que* $\mathcal{A} = \varprojlim \mathcal{A}/I_n$.

Exercice 2.6 Montrer que l'isomorphisme $A \to \mathcal{A}$ *est un homéomorphisme.*

On voit immédiatement que tout élément de $\mathcal{A}$ s'écrit de manière unique sous la forme $\sum_{n=1}^{\infty} a_n n^{-s}$. C'est pourquoi on appelle aussi $\mathcal{A}$ l'algèbre des *séries formelles de Dirichlet* à coefficients dans R.

On revient à nos moutons de la géométrie algébrique.

Proposition 2.1.1 *Soit* X *un schéma localement de type fini sur* $\mathbf{Z}$ *et* $x \in X$. *Alors,* $x \in |X|$ *ssi* $k(x)$ *est fini.*

Démonstration: Comme tout anneau integre fini est un corps, la condition est clairement suffisante. Pour montrer la réciproque, on peut supposer que X est affine, puis que $X = \mathbf{A}^n_{\mathbf{Z}}$. On se donne donc un homomorphisme surjectif $\mathbf{Z}[t_1, \ldots, t_n] \to k$ et il faut montrer que k est fini.

Supposons tout d'abord que k est de caractéristique nulle. Il résulte du Nullstellensatz que k est une extension finie de $\mathbf{Q}$, c'est à dire un corps de nombres. Soit $\mathcal{O}$ l'anneau des entiers de k. Alors, on peut écrire les images des t_i dans k sous la forme α_i/γ avec $\alpha_i, \gamma \in \mathcal{O}$. On a donc $k = \mathcal{O}_\gamma$. Donc, si p est un nombre premier, on peut écire $\frac{1}{p} = \frac{\alpha}{\gamma}$ et on en déduit que $N(\gamma) = N(\alpha)p^d$ si bien que p divise $N(\gamma)$. On a donc $N(\gamma) = 0$ et $\gamma = 0$. Contradiction.

On voit donc que k est de caractéristique $p > 0$. On a alors un morphisme surjectif $\mathbf{F}_p[t_1, \ldots, t_n] \to k$ et il résulte du Nullstellensatz que k est une extension finie de F_p et donc fini. $\square$

On se donne donc un schéma de type fini X sur $\mathbf{Z}$. Si $x \in |X|$, on pose $N(x) = |k(x)|$.

Exercice 2.7 Montrer que pour tout entier n, il existe un nombre fini de $x \in |X|$ tels que $N(x) \leq n$.

Exercice 2.8 Montrer que pour tout $x \in |X|$, $1 - N(x)^{-s}$ est une série de Dirichlet inversible et que le produit

$$\prod_{x \in |X|} \frac{1}{1 - N(x)^{-s}}$$

converge dans l'anneau des séries de Dirichlet (sur $\mathbf{Z}$).

Définition 2.1.2 *Avec les notations précédentes, la fonction zéta de X est la série de Dirichlet*

$$\zeta(X, s) := \prod_{x \in |X|} \frac{1}{1 - N(x)^{-s}}.$$

On rappelle que la fonction zéta de Riemann est la série formelle de Dirichlet définie par $\zeta(s) := \sum_{n=1}^{\infty} n^{-s}$.

Exercice 2.9 Montrer que $\zeta(\mathbf{A}^n_{\mathbf{Z}}, s) = \zeta(s - n)$.

Exercice 2.10 Montrer que si on écrit X comme union disjointe de sous-schémas X_i, alors $\zeta(X, s) = \prod_i \zeta(X_i, s)$.

Exercice 2.11 Exprimer $\zeta(\mathbf{P}^n_{\mathbf{Z}}, s)$ à l'aide de la fonction zéta de Riemann.

On va considérer maintenant le cas des variétés algébriques sur un corps fini.

2.2 Fonctions zéta géométriques

Si X est un schéma de type fini sur $\mathbf{F}_q$ et si $x \in |X|$, on pose $\deg x := [k(x) : \mathbf{F}_q]$.

On rappelle que si R est un anneau, alors $R[[t]] := R^{\mathbf{N}}$ comme R-module topologique et que $t := (0, 1, 0, 0, \ldots)$. On en fait une R-algèbre en définissant la multiplication comme d'habitude (comme pour les polynômes). C'est une R-algèbre linéairement topologisee separée et complète. En fait, les puissances de l'idéal (t) forment une base de voisinage de 0. Dans la catégorie des R-algèbres topologiques, on a $R[[t]] = \varprojlim R[t]/t^n$ ou les quotients sont munis de la topologie discrète.

Lemme 2.2.1 *Si X est un schéma de type fini sur $\mathbf{F}_q$, le produit*

$$\prod_{x \in |X|} \frac{1}{1 - t^{\deg x}}$$

converge dans $\mathbf{Z}[[t]]$.

Démonstration: Effectivement, comme X est de type fini, on a $1 - t^{\deg x} = 1 \mod t^N$ pour presque tout x. □

Définition 2.2.2 *Si X est un schéma de type fini sur $\mathbf{F}_q$, la* fonction zéta géométrique *de X est*

$$\mathrm{Z}(X, t) := \prod_{x \in |X|} \frac{1}{1 - t^{\deg x}}.$$

Remarquons qu'alors, $\zeta(X, s) = \mathrm{Z}(X, q^{-s})$. En particulier, pour étudier les fonctions zéta arithmétiques de schémas définis sur un corps fini, il suffit de considérer les fonctions zéta géométriques. On a une formule plus générale, laissée en exercice, qui était d'ailleurs la définition originale de la fonction zéta arithmétique.

Exercice 2.12 Soit X un schéma de type fini sur $\mathbf{Z}$, P l'ensemble des nombres premiers et pour tout $p \in P$, $X_p := X \otimes_{\mathbf{Z}} \mathbf{F}_p$. Montrer que

$$\zeta(X, s) = \prod_{p \in P} \mathrm{Z}(X_p, p^{-s}).$$

Exercice 2.13 Montrer que si on écrit X comme union disjointe de sous-schémas X_i, alors $\mathrm{Z}(X, s) = \prod_i \mathrm{Z}(X_i, s)$.

Proposition 2.2.3 *Si X est un schéma de type fini sur $\mathbf{F}_q$, on a*

$$\mathrm{Z}(X,t) = \exp(\sum_{r=1}^{\infty} N_r \frac{t^r}{r})$$

avec $N_r = |X(\mathbf{F}_{q^r})_{\mathbf{F}_q}|$.

Démonstration: On va d'abord donner une autre description de N_r. On a une application évidente $X(\mathbf{F}_q^r) \to |X|$. Son image est formée des $x \in |X|$ tels que $deg x|r$. De plus, la fibre en x de cette application est munie d'une action simplement transitive de $\mathrm{Gal}(k(x)/\mathbf{F}_q)$. Il suit que

$$N_r = \sum_{\deg x|r} deg x.$$

Notre assertion résulte alors du lemme qui suit. □

Lemme 2.2.4 *Si X est un schéma de type fini sur $\mathbf{F}_q$ et $\lambda : |X| \to R$ une application dans un anneau R, on a*

$$\prod_{x\in|X|} \frac{1}{1-\lambda(x)t^{\deg x}} = \exp(\sum_{r=1}^{\infty} S_r \frac{t^r}{r})$$

avec $S_r = \sum_{\deg x|r} \lambda(x)^{\frac{r}{\deg x}} \deg x$.

Démonstration: Comme nos deux série prennent la même valeur 1 en 0, il suffit de considérer les dérivées logarithmiques. D'un coté, on trouve

$$\sum_{x\in|X|} \frac{\lambda(x)t^{\deg x-1}\deg x}{1-\lambda(x)t^{\deg x}} = \sum_{x\in|X|}\sum_{k=1}^{\infty} \lambda(x)^k t^{k\deg x-1}\deg x$$

$$= \sum_{r=1}^{\infty}\sum_{deg x|r} \lambda(x)^{\frac{r}{\deg x}} t^{r-1}\deg x = \sum_{r=1}^{\infty} S_r t^{r-1}$$

qui est bien la dérivée de $\sum_{r=1}^{\infty} S_r \frac{t^r}{r}$. □

Exercice 2.14 Calculer $\mathrm{Z}(X,t)$ pour une variété linéaire affine ou projective, pour une variété finie, pour une conique affine ou projective, pour le groupe linéaire et pour la quadrique de Segre.

On peut enfin énoncer les conjectures de Weil sous leur forme multiplicative.

Théorème 2.2.5 (Conjectures de Weil) *Soit X une variété algébrique de dimension d sur $\mathbf{F}_q$. Alors,*

i) (rationalité) $\mathrm{Z}(X,t)$ est une fonction rationnelle à coefficients dans $\mathbf{Q}$.

ii) (pureté) Ses zéros et ses pôles sont des nombres de Weil de poids $\in [-2d, 0]$. Si X est propre et lisse, les poids des zéros sont impairs et ceux des pôles sont pairs.

iii) (équation fonctionnelle) Si X est propre et lisse de pure dimension d, alors

$$\mathrm{Z}(X, \frac{1}{q^d t}) = \pm q^{dE/2} t^E \, \mathrm{Z}(X,t)$$

avec $E \in \mathbf{Z}$.

La première assertion nous dit que $\mathrm{Z}(X,t) \in (1+t\mathbf{Z}[[t]]) \cap \mathbf{Q}(t) \subset \mathbf{Q}[[t]]$.

Exercice 2.15 Vérifier ces conjectures pour les variétés habituelles.

Exercice 2.16 Montrer que ces conjectures sont équivalentes à leurs versions additives.

On appelle polynôme de Weil de poids m tout $P \in \mathbf{Z}[t]$ qui peut s'écrire $P = \prod_{i=1}^{B}(1-\alpha_i t)$ avec $|\alpha_i| = q^{\frac{m}{2}}$.

Exercice 2.17 Montrer que les racines d'un polynôme de Weil de poids m sont des nombres de Weil de poids $-m$

La seconde assertion du théorème nous dit donc que $\mathrm{Z}(X,t)$ est un quotient de produits de polynômes de Weil de poids $\in [0, 2d]$. On va se concentrer maintenant sur le cas propre et lisse.

Théorème 2.2.6 (Conjectures de Weil, suite) *Si X est propre et lisse de dimension d, on peut écrire*

$$\mathrm{Z}(X,t) = \prod_{i=0}^{2d} P_i(t)^{(-1)^{i+1}}$$

ou P_i est un polynôme de Weil de poids i.

Si X est de pure dimension d, alors pour tout i, on a $P_{2d-i}(t) = C_i t^{B_i} P_i(\frac{1}{q^d t})$ avec $C_i \in \mathbf{Z}$ et $B_i \in \mathbf{N}$.

Exercice 2.18 Montrer que l'on a nécessairement $C_i C_{2d-i} = q^{dB_i}$ et $B_{2d-i} = B_i$.

Exercice 2.19 Montrer que, dans le cas $i = d$, la dernière assertion résulte de la première.

Exercice 2.20 Montrer que cette conjecture est équivalente à la précédente dans le cas propre et lisse et que $E = \sum_{i=0}^{2d}(-1)^i B_i$.

Exercice 2.21 Vérifier cette conjecture pour $\mathbf{P}^n$, pour la quadrique de Segre et pour une variété finie étale (calculer dans ce cas les polynômes P_i ansi que les C_i, B_i et E).

Notre problème de départ était l'étude modulo p d'un système d'équations à coefficients entiers. Ceci nous conduit à l'étude d'une variété X en caractéristique p. Mais un tel système permet aussi de définir une variété V en caractéristque nulle. La dernière partie des conjectures de Weil prédit l'allure de la fonction zéta de X à partir de la géométrie de V.

Nous allons voir ci-dessous comment on peut associer à une variété V propre et lisse sur $\mathbf{C}$, une variété différentable compacte V^{an}. Pour une telle variété, on peut considérer les groupes de cohomologie $H^i(V^{an}, \mathbf{Z})$. Admettant ceci pour l'instant, on peut énoncer la dernière partie des conjectures de Weil.

Théorème 2.2.7 (Conjectures de Weil, fin) *Soit R un anneau muni d'un morphisme surjectif $R \to \mathbf{F}_q$ et d'un morphisme injectif $R \hookrightarrow \mathbf{C}$. Soit $\mathcal{X}$ un R-schéma propre et lisse tel que $X := \mathcal{X} \otimes_R \mathbf{F}_q$ et $V := \mathcal{X} \otimes_R \mathbf{C}$. On a alors pour tout i, $B_i = \operatorname{rang} H^i(V^{an}, \mathbf{Z})$.*

Exercice 2.22 Vérifier cette conjecture dans les cas habituels (on rappelle que $\operatorname{rang} H^i(P_{\mathbf{C}}^{n,an}, \mathbf{Z}) = 1$ si $i = 2j$ avec $0 \leq j \leq n$ et 0 sinon).

On va maintenant expliquer la construction de la variété analytique associée à une variété algébrique.

2.3 Analytique vs algébrique

On définit un espace analytique sur $\mathbf{C}$ comme un espace localement annelé $(V, \mathcal{O}_V)$ qui est localement de la forme suivante : Il existe $f_1, \ldots, f_n$ holomorphes sur une boule ouverte $B := B(0,1) \subset \mathbf{C}^n$ tel que $X = \{x \in B, \forall i, f_i(x) = 0\}$ et $\mathcal{O}_X = i^{-1}(\mathcal{O}_B/(f_1, \ldots, f_n))$ ou $i : X \hookrightarrow B$ est l'inclusion et $\mathcal{O}_B$ est le faisceau des fonctions holomorphes sur B.

Si X est un schéma localement de type fini sur $\mathbf{C}$, on considère l'ensemble $X^{an} = |X|$. Si $X = \mathbf{A}^n_{\mathbf{C}}$, on a une bijection évidente $X^{an} \tilde{=} X(\mathbf{C}) \tilde{=} \mathbf{C}^n$ qui munit X^{an} d'une structure d'espace analytique. Si X est affine, on peut supposer que $X \subset \mathbf{A}^n_{\mathbf{C}}$ et $X^{an} \subset \mathbf{C}^n$ est muni d'une structure d'espace analytique (qui dépend de la structure de schéma de X). En général, X peut être recouvert par des ouverts affines U_i et il suit que X^{an} est recouvert par les U_i^{an} et est donc aussi muni d'une topologie qui en fait un espace analytique.

Exercice 2.23 Montrer que si X est un schéma localement de type fini, la topologie de X^{an} ne dépend pas des choix et que l'inclusion $X^{an} \hookrightarrow X$ est continue.

On peut définir la topologie de X^{an} d'une autre manière. Si $f \in \Gamma(X, \mathcal{O}_X)$, on peut considérer $f^{an} : X^{an} \to \mathbf{C}$ définie par $f^{an}(x) = f(x) \in k(x) = \mathbf{C}$.

Exercice 2.24 Montrer que la topologie de X^{an} est la topologie la moins fine rendant continues les fonctions f^{an} avec $f \in \Gamma(U, \mathcal{O}_X)$, lorsque U parcourt les ouverts (de Zariski) de X.

On fait de l'inclusion $X^{an} \hookrightarrow X$ un morphisme d'espace annelés comme suit. La question est locale et on peut donc supposer X affine. On se ramène facilement au cas $X = \mathbf{A}^n_{\mathbf{C}}$. Or, on a un morphisme évident $\mathbf{C}[t_1, \ldots, t_n] \to \Gamma(\mathbf{C}^n, \mathcal{O}_{\mathbf{C}^n})$ qui induit bien l'inclusion $\mathbf{C}^n \hookrightarrow \mathbf{A}^n_{\mathbf{C}}$ (en général, un morphisme d'espace localement annelés $X \to \operatorname{Spec} A$ est déterminé par le morphisme d'anneaux $A \to \Gamma(X, \mathcal{O}_X)$).

On peut verifier que notre construction est correcte et fonctorielle. Plus précisément, on démontre le résultat suivant laissé en exercice.

Exercice 2.25 Montrer que si X est un schéma localement de type fini, le morphisme d'espace localement annelé $X^{an} \hookrightarrow X$ est bien défini et qu'il représente le foncteur $V \to \operatorname{Hom}_{loc.ann.}(V, X)$ sur la catégorie des espaces analytiques.

Si on veut être plus terre à terre, ce résultat dit que si on se donne un morphisme d'espaces localement annelés $V \to X$, il se factorise de manière unique en un morphisme d'espaces analytiques $V \to X^{an}$ suivi de $X^{an} \hookrightarrow X$. En particulier, la construction $X \mapsto X^{an}$ est fonctorielle.

Exercice 2.26 Montrer que X est connexe ssi X^{an} est connexe.

Exercice 2.27 Montrer que X est séparé ssi X^{an} est séparé.

Exercice 2.28 Montrer que X est propre ssi X^{an} est compact (difficile).

Exercice 2.29 Montrer que X est lisse ssi X^{an} est une variété holomorphe.

Exercice 2.30 Montrer que $f : Y \to X$ est fini ssi $f^{an} : Y^{an} \to X^{an}$ est propre à fibres finies (difficile).

Exercice 2.31 Montrer que $f : Y \to X$ est étale ssi $f^{an} : Y^{an} \to X^{an}$ est un homéomorphisme local.

Il y a des resultats plus difficiles à démontrer. Par exemple, tout sous espace analytique compact de $\mathbf{P}^{n,an}_{\mathbf{C}}$ est de la forme X^{an} (Chow). Si X et Y sont deux variétés projectives, tout morphisme $Y^{an} \to X^{an}$ est de la forme f^{an} pour un unique $f : Y \to X$ (Serre). Encore plus dur : toute variété holomorphe compacte de dimension (complexe) 1 est de la forme C^{an} ou C est une courbe projective (lisse) (Riemman). De plus en plus dur, si X est lisse et si V est une variété holomorphe, alors tout morphisme $V \to X^{an}$ propre à fibres finies est de la forme f^{an} avec $f : Y \to X$ (et donc en particuler, $V \tilde{=} Y^{an}$).

2.4 Sommes de gauss

Définition 2.4.1 *Un* caractère *d'un groupe G est un morphisme de groupes $G \to \mathbf{C}^*$. Un* caractére additif *(resp.* multiplicatif*) d'un corps k est un caractère du groupe additif k (resp. du groupe multiplicatif k^*). On prolongera un caractère multiplicatif χ en 0 par $\chi(0) = 0$.*

Exercice 2.32 Montrer que les caractères additifs continus (resp. continus bornés) de $\mathbf{R}$ sont les $\psi(t) = e^{2i\pi\alpha t}$ avec $\alpha \in \mathbf{C}$ (resp. $\alpha \in \mathbf{R}$).

Exercice 2.33 Montrer que si G est un groupe fini et χ un caractère de G alors $\chi(g)$ est une racine de l'unité ; en particulier $|\chi(g)| = 1$ et $\chi(g)^{-1} = \bar{\chi}(g)$.

Exercice 2.34 Montrer que si G est un groupe commutatif fini, les caractères de G forment un groupe isomorphe (non canoniquement) à G.

Lemme 2.4.2 *Si χ est un caractère non-trivial d'un groupe commutatif fini G, alors $\sum_{g\in G} \chi(g) = 0$*

Démonstration: On a toujours

$$\sum_{g\in G}\chi(g)=\sum_{g\in G}\chi(gh)=\sum_{g\in G}\chi(g)\chi(h)=\chi(h)\sum_{g\in G}\chi(g).$$

Et il suffit alors de prendre h tel que $\chi(h)\neq 1$. □

Si on muni $\mathbf{R}$ du caractère additif $\psi(t):=e^{-2i\pi t}$, et si $f\in L^1(\mathbf{R},\mathbf{C})$, la transformée de Fourier de f est définie par $\hat{f}(x):=\int_{\mathbf{R}}\psi(tx)f(t)dt$. Cette remarque justifie la définition suivante.

Définition 2.4.3 *Soit k un corps fini muni d'un caractère additif non-trivial ψ et $f:k\to\mathbf{C}$ une fonction quelconque. La* transformée de Fourier *de f est la fonction $\hat{f}(x)=\sum_{t\in k}\psi(tx)f(t)$. La* somme de Gauss *associée à un caractère multiplicatif χ est $g_\chi:=\hat{\chi}(1)$.*

Lemme 2.4.4 *Soit χ un caractère multiplicatif non trivial d'un corps fini k à q éléments. Alors,*

i) on a $\hat{\chi}(x)=\bar{\chi}(x)g_\chi$.

ii) on a $|g_\chi|=\sqrt{q}$.

Démonstration: On attaque la première assertion. Tout d'abord, pour $x=0$, on retrouve $\sum_{t\in k}\chi(t)=0$ comme dans le lemme. Si $x\neq 0$, alors

$$\sum_{t\in k}\psi(tx)\chi(t)=\sum_{t\in k}\psi(t)\chi(x^{-1}t)=\chi(x^{-1})\sum_{t\in k}\psi(t)\chi(t)=\bar{\chi}(x)g_\chi.$$

La seconde assertion, maintenant : on a

$$|g_\chi|^2=g_\chi\bar{g}_\chi=\sum_{x\in k}\bar{\psi}(x)\bar{\chi}(x)g_\chi=\sum_{t,x\in k}\psi(-x)\psi(tx)\chi(t)$$

$$=\sum_{t,x\in k}\psi(t(x-1))\chi(t)=\sum_{t\in k}(\sum_{x\in k}\psi(x(t-1)))\chi(t).$$

On a d'une part $\sum_{x\in k}\psi(0)\chi(1)=\sum_{x\in k}1=q$, et d'autre part,

$$\sum_{t\neq 1}(\sum_{x\in k}\psi(t(x-1)))\chi(t)=0$$

car pour $t\neq 1$, on a $\sum_{x\in k}\psi(x(t-1)))=\sum_{t\in k}\psi(t)=0$. □

On va maintenant étudier le comportement des sommes de Gauss par rapport aux extensions de k. Nous aurons besoin du résultat suivant, laissé en exercice.

Exercice 2.35 Soient E un ensemble, $M := \mathbf{N}[E]$ et R un anneau. Soient $d : M \to \mathbf{N}$ et $\lambda : M \to R^*$ deux morphismes de monoïdes. Montrer que dans $R[[t]]$, on a

$$\prod_{e \in E} \frac{1}{1 - \lambda(e)t^{d(e)}} = \sum_{m \in M} \lambda(m)t^{d(m)}.$$

Nous aurons aussi besoin du lemme suivant. On fixe un caractère additif non trivial ψ et un caractère multiplicatif χ d'un corps fini k. Si $F := X^n - a_1X^{n-1} + \cdots + (-1)^n a_n$ est un polynôme unitaire de degré n, on pose $\lambda(F) := \psi(a_1)\chi(a_n)$.

Lemme 2.4.5 *i) On a $\lambda(FG) = \lambda(F)\lambda(G)$.*

ii) On a $\sum_{degF=d} \lambda(F) = 0$ si $d > 1$ et $\sum_{degF=1} \lambda(F) = g_\chi$.

Démonstration: On a $F := X^n - a_1X^{n-1} + \cdots + (-1)^n a_n$ et $G := X^m - b_1X^{n-1} + \cdots + (-1)^m b_m$ si bien que $FG := X^{n+m} - (a_1 + b_1)X^{n+m-1} + \cdots + (-1)^{n+m} a_n b_m$. On a donc

$$\lambda(FG) := \psi(a_1 + b_1)\chi(a_n b_m) = \psi(a_1)\psi(b_1)\chi(a_n)\chi(b_m) = \lambda(F)\lambda(G).$$

Pour la seconde assertion, comme les polynômes unitaires de degré n sont en bijection avec k^n, on voit que, pour $d > 1$, on a

$$\sum_{degF=d} \lambda(F) = \sum_{a \in k^n} \psi(a_1)\chi(a_n) = q^{n-2} \sum_{a_1 \in k} \psi(a_1) \sum_{a_n \in k} \chi(a_n) = 0.$$

Et bien sûr, $\sum_{degF=1} \lambda(F) = \sum_{a \in k} \psi(a)\chi(a) = g_\chi$. □

Si k'/k est une extension algébrique, on dispose de la trace $Tr : k' \to k$ et de la norme $N : k'^* \to k^*$ qui sont des homomorphismes de groupes (si $a \in k'$, alors $Tr(a)$ est la trace de la multiplication sur k' vue comme k-endomorphisme de k' et $N(a)$ est son déterminant). De même, on définit le polynôme caractéristique de a comme étant le polynôme caractéristique de la multiplication par a dans k'.

Si ψ (resp. χ) un caractère additif (resp. multiplicatif) de k, on note $\psi' := \psi \circ Tr$ et $\chi' := \chi \circ N$. Si $k = \mathbf{F}_q$ et $k' = \mathbf{F}_{q^r}$, on écrit plutôt ψ_r, χ_r. On pose alors $g_{\chi_r} := \sum_{t \in k'} \psi_r(t)\chi_r(t)$.

Proposition 2.4.6 (Davenport-Hasse) *Soit ψ un caractère additif non trivial de $\mathbf{F}_q$ et χ un caractère multiplicatif. On a alors pour tout r,*

$$g_{\chi_r} = (-1)^{r-1} g_\chi^r.$$

Démonstration: Soit M le monoïde des polynômes unitaires à coefficients dans $\mathbf{F}_q$. Si $E = |\mathbf{A}^1_{\mathbf{F}_q}|$, on a une bijection évidente entre M et $\mathbf{N}[E]$, donnée par $k(x) = \mathbf{F}_q[T]/F$ (F est le polynôme minimal de x). On écrira $\lambda(x) := \lambda(F)$.

Soit $a \in \mathbf{F}_{q^r}$, F son polynnôme minimal et x le point de $\mathbf{A}^1_{\mathbf{F}_q}$ correspondant. Le polynôme caractéristique de a sur $\mathbf{F}_{q^r}$ est donc $F^{\frac{r}{\deg x}}$ et il suit que $\psi_r(a)\chi_r(a) = \lambda(x)^{\frac{r}{\deg x}}$. On en déduit que $g_{\chi_r} = \sum_{\deg x | r} \lambda(x)^{\frac{r}{\deg x}} \deg x$.

On dispose de l'identité suivante dans $\mathbf{C}[[t]]$ (voir exercice) :

$$\prod_{x \in E} \frac{1}{1 - \lambda(x) t^{\deg x}} = \sum_{F \in M} \lambda(F) t^{\deg F}.$$

D'après le lemme précédent, le second membre vaut $1 + g_\chi t$. D'autre part, il résute du lemme 2.2.4 que le premier membre vaut $\exp(\sum_{r=1}^\infty g_{\chi_r} \frac{t^r}{r})$. On a donc bien $g_{\chi_r} = (-1)^{r-1} g_\chi^r$ comme annoncé. □

2.5 Sommes de Jacobi

Dans cette section, pour alléger l'écriture, si X est un schéma sur k, on écrit $X(k) := X(k)_k$.

Définition 2.5.1 *Soient $\chi_1, \dots, \chi_n$ des caractères multiplicatifs d'un corps fini k. La* somme de Jacobi *associée à ces caractères est*

$$j(\chi_1, \dots, \chi_n) := \sum_{x \in H(k)} \chi_1(x_1) \cdots \chi_n(x_n)$$

où H l'hyperplan d'équation $\sum_{i=1}^n X_i = 0$ dans $\mathbf{A}^n_k$.

Pour calculer les sommes de jacobi, nous aurons besoin du lemme suivant.

Lemme 2.5.2 *Soient $a_1, \dots, a_n \in k$ et ψ un caractère additif. On écrit $q := |k|$. Alors, $\sum_{x \in H(k)} \psi(\sum_{i=1}^n a_i x_i) = q^{n-1}$ si $a_1 = \cdots = a_n$ et 0 sinon.*

Démonstration: Pour $c \in k$, soit V_c la variété linéaire affine (ou vide) d'équations $\sum_{i=1}^n X_i = 0$ et $\sum_{i=1}^n a_i X_i = c$. On pose $N_c := |V_c(k)|$. On a alors

$$\sum_{x \in H(k)} \psi(\sum_{i=1}^n a_i x_i) = \sum_{c \in k} N_c \psi(c).$$

Si les a_i ne sont pas tous égaux, alors, pour tout c, V_c est une variété linéaire affine de dimension $n-2$ et on a donc $\sum_{c \in k} N_c \psi(c) = q^{n-2} \sum_{c \in k} \psi(c) = 0$.

Supposons maintenant que $a_1 = \cdots = a_n$. On a alors $V_0 = H$ et $V_c = \emptyset$ si $c \neq 0$. Il suit que $\sum_{c \in k} N_c \psi(c) = N_0 \psi(0) = q^{n-1}$. □

Proposition 2.5.3 *Soient $\chi_1, \ldots, \chi_n$ des caractères multiplicatifs de k et $j := j(\chi_1, \ldots, \chi_n)$. Si $\prod_{i=1}^n \chi_i \neq 1$, alors $j = 0$. Si $\prod_{i=1}^n \chi_i = 1$ mais pour tout i, $\chi_i \neq 1$, alors*

$$j = \frac{q-1}{q} \prod_{i=1}^n g_{\chi_i}$$

où $q := |k|$.

Démonstration: Dans le premier cas, on peut trouver $t \in k^*$ tel que $\alpha := \prod_{i=1}^n \chi_i(t) \neq 1$. L'application $x \mapsto tx$ étant une bijection de $H(k)$ sur lui même, on a

$$j = \sum_{x \in H(k)} \chi_1(tx_1) \cdots \chi_n(tx_n) = \prod_{i=1}^n \chi_i(t) \sum_{x \in H(k)} \chi_1(x_1) \cdots \chi_n(x_n) = \alpha j$$

et donc $j = 0$.

On suppose maintenant que $\prod_{i=1}^n \chi_i = 1$ et que pour tout i, on a $\chi_i \neq 1$. On calcule en utilisant le premier résultat de 2.4.4 et le lemme précédent,

$$\bar{j} \prod_{i=1}^n g_{\chi_i} = \sum_{x \in H(k)} \prod_{i=1}^n g_{\chi_i} \bar{\chi}_i(x_i) = \sum_{x \in H(k)} \prod_{i=1}^n \sum_{t \in k} \psi(tx_i) \chi_i(t)$$

$$= \sum_{x \in H(k)} \sum_{t \in k^n} \prod_{i=1}^n \psi(t_i x_i) \chi_i(t_i) = \sum_{t \in k^n} \sum_{x \in H(k)} \psi(\sum_{i=1}^n t_i x_i) \prod_{i=1}^n \chi_i(t_i)$$

$$= \sum_{t \in k} q^{n-1} \prod_{i=1}^n \chi_i(t) = (q-1) q^{n-1}$$

car $\prod_{i=1}^n \chi_i = 1$ (ne pas oublier que $1(0) = 0$). On en déduit que

$$j = (q-1) q^{n-1} \prod_{i=1}^n \frac{g_{\chi_i}}{q} = \frac{q-1}{q} \prod_{i=1}^n g_{\chi_i}$$

□

2.6 Hypersurfaces diagonales

Le premier cas non-trivial pour lequel André Weil a démontré ses conjectures est celui des hypersurfaces diagonales. Il s'agit des hypersurfaces projectives sur un corps k à q éléments ayant une équation de la forme $\sum a_i X_i^d = 0$ avec $(q,d) = 1$. Nous allons nous limiter pour des raisons techniques aux hypersurfaces diagonales (dites de Fermat) d'équation $\sum X_i^d = 0$ avec $q \equiv 1 \mod d$.

Théorème 2.6.1 *Soient $q, d \in \mathbf{N}$ tel que $q \equiv 1 \mod d$, k un corps à q éléments et V l'hypersurface d'équation $\sum_{i=0}^n X_i^d = 0$ dans $\mathbf{P}_k^n$. Alors,*

$$\mathrm{Z}(V,t) = \mathrm{Z}(\mathbf{P}_k^{n-1},t)P(t)^{(-1)^n}$$

où P est un polynôme de Weil de poids $n-1$.

Démonstration: Si K est un corps, on note $\mu_d(K)$ le groupe des racines d-ièmes de l'unité dans K et $(K^*)^d$ le groupe des puissances d-ièmes. On a donc une suite exacte

$$0 \to \mu_d(K) \to K^* \to (K*)^d \to 0.$$

Comme $d|(q-1)$, $X^d - 1|X^{q-1} - 1$ et donc $|\mu_d(k)| = d$. Il suit que $|(k^*)^d| = \frac{q-1}{d}$. D'autre part, comme $\mu_d(\mathbf{C})$ est cyclique d'ordre d, que k^* est cyclique d'ordre $q-1$, et que $d|(q-1)$, il existe un homomorphisme surjectif χ de $k*$ sur $\mu_d(\mathbf{C})$. On a alors $\operatorname{Ker}\chi = (k^*)^d$. En effet, l'inclusion réciproque est immédiate et les deux groupes ont même ordre.

On vérifie maintenant que le nombre de solutions de l'équation $X^d = a$ dans k est $1 + \chi(a) + \cdots + \chi(a)^{d-1} = \sum_{m=0}^{d-1} \chi(a)^m$ (attention, on fait la covention que $0^0 = 1$, et on a donc $\chi(0)^0 = 0^0 = 1 \neq 0 = \chi^0(0)$). En fait, trois cas se présentent. Tout d'abord, si $a = 0$, on trouve bien 1 de chaque coté. Ensuite, si $a \notin (k^*)^d$, alors $\chi(a) \neq 1$ et on trouve bien 0 des deux cotés. Enfin, si $a \in (k^*)^d$, alors $\chi(a) = 1$ et on trouve d des deux cotés car si $a \neq 0$, l'ensemble des solutions est muni d'une action simplement transitive de $\mu_d(k)$.

On note maintenant C le cône affine de V, c'est à dire l'hypersurface d'équation $\sum_{i=0}^n X_i^d = 0$ dans dans $\mathbf{A}_k^{n+1}$ et H l'hyperplan d'équation $\sum_{i=0}^n X_i = 0$ dans dans $\mathbf{A}_k^{n+1}$. On peut considérer le morphisme $p : C \to H$ donné par la puissance d-ième sur les coordonnées.

Dans la suite on utilise les notations standard pour les multiindex : $(m_1, \ldots, m_n) \leq (m'_1, \ldots, m'_n)$ signifie que pour tout i, on a $m_i \leq m'_i$ et on pose $|m| = m_1 + \cdots + m_n$.

On a $N(C) = \sum_{x\in H(k)} N(p^{-1}(x))$ et par ce qui précède

$$N(p^{-1}(x)) = \prod_{i=0}^{n}\sum_{m=0}^{d-1}\chi(x_i)^m = \sum_{m=0}^{d-1}\prod_{i=0}^{n}\chi(x_i)^{m_i}$$

et il suit que

$$N(C) = \sum_{m=0}^{d-1}\sum_{x\in H(k)}\prod_{i=0}^{n}\chi(x_i)^{m_i}.$$

Si $m \geq 1$, on a

$$\sum_{x\in H(k)}\prod_{i=0}^{n}\chi(x_i)^{m_i} = \sum_{x\in H(k)}\prod_{i=0}^{n}\chi^{m_i}(x_i) = j(\chi^{m_0},\ldots,\chi^{m_n}).$$

On sait que cette somme est nulle si $\prod_{i=0}^{n}\chi^{m_i} \neq 1$, c'est à dire si d ne divise pas $|m|$. Sinon, elle vaut $\frac{q-1}{q}\prod_{i=0}^{n} g_{\chi^{m_i}}$.

Si l'un des m_i, disons $m_1 = 0$, alors

$$\sum_{x\in H(k)}\prod_{i=0}^{n}\chi(x_i)^{m_i} = \sum_{x\in k^n}\prod_{i=1}^{n}\chi(x_i)^{m_i} = \prod_{i=1}^{n}\sum_{x\in k}\chi(x)^{m_i}.$$

Notre somme est donc nulle à moins que $m = 0$. Dans ce dernier cas, on trouve q^n.

Si on pose

$$A := \{m \in \mathbf{N}^{n+1}, 1 \leq m \leq d-1 \text{ et } d||m|\}$$

on voit donc que

$$N(C) = q^n + \frac{q-1}{q}\sum_{m\in A}\prod_{i=0}^{n} g_{\chi^{m_i}}.$$

On en déduit que $N(V) = \frac{N(C)-1}{q-1} = \frac{q^n-1}{q-1} + \frac{1}{q}\sum_{m\in A}\prod_{i=0}^{n} g_{\chi^{m_i}}$ et donc, finalement,

$$N(V) = N(\mathbf{P}_k^{n-1}) + (-1)^{n-1}\sum_{m\in A}\alpha_m$$

avec

$$\alpha_m = \frac{1}{q}\prod_{i=0}^{n} -g_{\chi^{m_i}} = \frac{(-1)^{n-1}}{q-1} j(\chi^{m_1},\ldots,\chi^{m_n}).$$

Grâce au théorème de Davenport-Hasse, on voit que

$$\alpha_m^r = \frac{1}{q^r}\prod_{i=0}^{n}(-1)^r g_{\chi^{m_i}}^r = \frac{1}{q^r}\prod_{i=0}^{n} -g_{\chi_r^{m_i}}$$

et on a donc

$$N_r(V) = N_r(\mathbf{P}_k^{n-1}) + (-1)^{n-1}\sum_{m\in A}\alpha_m^r.$$

On en déduit que

$$\mathrm{Z}(V,t) = \mathrm{Z}(\mathbf{P}_k^{n-1},t)P(t)^{(-1)^n}$$

avec $P = \prod_{m\in A}(1-\alpha_m t)$ qui est un polynome de Weil de poids $n-1$ puisque

$$|\alpha_m| = \frac{1}{q}\prod_{i=0}^{n}|g_{\chi^{m_i}}| = \frac{\sqrt{q}^{n}+1}{q} = \sqrt{q}^{n-1}.$$

□

Exercice 2.36 Montrer que V satisfait les conjectures de Weil (on laissera tomber la dernière partie qui nécessite le calcul de la cohomologie de l'hypersurface d'équation $\sum_{i=0}^{n} X_i^d = 0$ dans $\mathbf{P}^n(\mathbf{C})$).

Bibliographie

[1] M.F. Atiyah, I.G. Mac Donald, *Introduction to commutative Algebra.* Addison-Wesley, Reading, Mass (1969).

[2] A. Blanchard, *Initiation à la théorie analytique des nombres premiers.* Dunod, Paris (1969).

[3] Sigfried Bosh, Werner Lütkebohmert, Michel Raynaud, *Neron Models*, Ergebnisse der Mathematic und ihrer Grenzgebiete, 3 Folge, Band 21, Springer-Verlag (1990).

[4] Bernard Dwork, On the rationality of the zeta function of an algebraic variety, Amer. J. Maths. 82 (1960), 631–648.

[5] Pierre Deligne, La conjecture Weil I, Publ. Math. IHES 43 (1974), 273–307.

[6] Pierre Deligne, La conjeture de Weil II, Publ. Math. Inst. Hautes Etudes Sci. 52 (1981) 313-428.

[7] Jean Dieudonné, Alexander Grothendieck, *EGA 1 : Le langage des schémas.* Springer, Heildelberg (1971).

[8] Jean Dieudonné, Alexander Grothendieck, EGA 2 : Etude globale élémentaire de quelques classes de morphismes, Publ. Math. IHES 8 (1961).

[9] Jean Dieudonné, Alexander Grothendieck, EGA 4, tome 4 : Etude locale des schémas et des morphismes de schémas, Publ. Math. IHES 32 (1967).

[10] Alexander Grothendieck, formule de Lefschetz et rationnalité des fonctions L, Séminare Bourbaki 279 (1965).

[11] Robin Hartshorne, *Algebraic Geometry.* Springer, Heidelberg (1979).

[12] Steven L. Kleiman, Algebraic cycles and the Weil conjectures, in *Dix exposés sur la cohomologie des schémas*, North-Holland, Amsterdam (1968), 359–386.

[13] J.S. Milne, *Etale Cohomology*. Princeton University Press, Princeton NJ (1980).

[14] Paul Monsky, *p-adic Analysis and Zeta Functions*. Cours donné à Kyoto University (1969).

[15] Oscar Zariski, Pierre Samuel, *Commutative Algebra, Volume II*. Springer, Heidelberg (1979).

[16] Jean-Pierre Serre, Zeta and L functions, in *Arithmetical Algebraic Geometry* (Schilling, ed), Harper & Row, New-York (1965), 82–92.

[17] André Weil, Number of solutions of equations over finite fields, Bull. Amer. Math. Soc. 55 (1949), 497-508.