Comptage de courbes planes lisses

Marc Abboud et Seginus Mowlavi
Sous la direction de Margaret Bilu

Juin 2016

Résumé

Le théorème de Bertini affirme, sous une forme faible, que pour toute variété X quasi-projective lisse sur un corps algébriquement clos, il existe un hyperplan H tel que $H \cap X$ soit lisse. Il est alors naturel de se demander ce qu'il en est des corps finis : le résultat reste-t-il vrai ? Si ce n'est pas le cas, peut-on énoncer un résultat analogue ?

En 2004, Bjorn Poonen a répondu à ces deux questions avec [Poo04] : le théorème de Bertini énoncé ainsi est faux pour les corps finis, il est valide si au lieu de se restreindre à des hyperplans, on s'autorise des hypersurfaces de degré aussi grand que l'on veut. Ce nouvel énoncé est en fait une conséquence d'un théorème plus fort prouvé par Poonen, qui calcule la densité des hypersurfaces validant le théorème de Bertini au moyen de la fonction zêta de la variété considérée :

Théorème. *Soit X un sous-schéma quasiprojectif lisse de $\mathbb{P}^n$ de dimension $m \geq 0$ sur $\mathbb{F}_q$. Alors la fraction des $f \in \mathbb{F}_q[x_0, \ldots, x_n]$ homogènes de degré d tels que l'hypersurface* $\mathrm{Proj}(\mathbb{F}_q[x_0, \ldots, x_n]/(f))$ *intersecte X de manière lisse tend vers $\zeta_X(m+1)^{-1}$ lorsque d tend vers l'infini.*

La première partie de ce mémoire sera consacrée à l'établissement de notre cadre d'étude, à savoir les schémas. Dans un second temps, on définira la fonction zêta d'une variété sur un corps fini, avant de se plonger dans la démonstration du théorème de Bertini pour les corps finis. On s'intéressera tout d'abord au cas particulier du plan affine : le théorème compte alors les courbes lisses du plan. La démonstration de ce cas particulier met en jeu tous les ingrédients utilisés dans celle du théorème général tout en se formulant de manière élémentaire. Cela nous fournira ainsi une intuition de la preuve du cas général, qui nous permettra d'en exposer la plupart des étapes. Cependant, comme certaines étapes nécessitent des notions trop avancées, cette preuve ne sera ici pas complète. Par exemple, on ne considérera que des sous-variétés, pour lesquelles les intersections et la régularité sont plus simples à exprimer.

Table des matières

1 Généralités sur les spectres **3**
1.1 Spectre d'un anneau . . . 3
1.2 L'espace affine . . . 4
1.3 Irréductibilité . . . 5
1.4 Dimension . . . 6
1.5 Régularité d'une courbe plane en un point fermé . . . 8

2 Généralités sur les schémas **10**
2.1 Notion de faisceau . . . 10
2.2 Le faisceau structural sur spec A . . . 13
2.3 Notion de schéma . . . 15
2.4 L'exemple des Proj . . . 19
2.5 Sous-schémas . . . 21
2.6 L'espace projectif . . . 22
2.7 Dimension . . . 23
2.8 Régularité d'une hypersurface, espace tangent . . . 24
2.9 Notion d'$\mathcal{O}_X$-module . . . 25

3 La fonction zêta de Hasse-Weil **27**
3.1 Quelques préliminaires . . . 27
3.2 La fonction zêta de Hasse-Weil . . . 28
3.3 Quelques calculs et propriétés . . . 29

4 Le théorème de Bertini **30**
4.1 La méthode du crible . . . 30
4.2 Comptage des courbes lisses du plan affine . . . 31
4.3 Le théorème de Bertini sur un corps fini . . . 36

5 Applications **42**
5.1 Optimalité du théorème 4.10 . . . 43
5.2 Courbes remplissant l'espace, variétés évitant l'espace . . . 44
5.3 Singularités de dimension positive . . . 45

A Résultats d'algèbre **45**

Références **45**

1 Généralités sur les spectres

Cette partie est une étape nécessaire à l'introduction des schémas et des propriétés associées ; mais elle a surtout vocation à fournir un cadre élémentaire pour la section 4.2.

1.1 Spectre d'un anneau

Dans cette section, A désigne un anneau commutatif unitaire.

Définition 1.1. Le *spectre* de A est l'ensemble des idéaux premiers de A ; on le note $\mathrm{spec}(A)$.

Pour tout idéal premier $\mathfrak{p} \in \mathrm{spec}(A)$, le quotient $A/\mathfrak{p}$ est intègre ; on associe alors à $\mathfrak{p}$ le *corps résiduel* $k(\mathfrak{p}) := \mathrm{Frac}(A/\mathfrak{p})$.

Si I est un idéal de A, on définit $V(I) := \{\mathfrak{p} \in \mathrm{spec}(A) \mid I \subset \mathfrak{p}\}$. Pour un élément f de A, on fera souvent le raccourci $V(f)$ pour désigner $V((f))$.

On veut voir $\mathrm{spec}(A)$ comme un espace topologique. Notons déjà que $V((0)) = \mathrm{spec}(A)$ et $V(A) = \emptyset$. La proposition suivante montre qu'on peut définir une topologie sur $\mathrm{spec}(A)$ dont les $V(I)$ sont les fermés.

Proposition 1.2. *1. Si I_1 et I_2 sont des idéaux de A, alors $V(I_1) \cup V(I_2) = V(I_1 I_2) = V(I_1 \cap I_2)$.*

2. Si (I_i) est une famille d'idéaux de A, alors $\bigcap V(I_i) = V(\sum I_i)$

Définition 1.3. La *topologie de Zariski* est la topologie sur $\mathrm{spec}(A)$ dont les fermés sont les $V(I)$.

Exemple 1.4. 1. La notion de spectre a été construite comme généralisation des espaces topologiques rencontrés en géométrie algébrique classique. A ce titre, un exemple fondamental est $\mathrm{spec}(k[x_1, \ldots, x_n])$ qui correspond à l'espace k^n sur un corps k. Cet exemple sera étudié en détail dans la section suivante.

2. Le spectre de $\mathbb{Z}$ est l'ensemble des nombres premiers, auquel on ajoute (0). Les corps résiduels sont les $\mathbb{F}_p$ et $\mathbb{Q}$. Les fermés sont les parties finies ne contenant pas (0), ainsi que $\mathrm{spec}(\mathbb{Z})$ tout entier.

Notons que la topologie de *Zariski* n'est en général pas séparée : l'adhérence d'un point $\mathfrak{p} \in \mathrm{spec}(A)$ est $V(\mathfrak{p})$, qui est égal à $\{\mathfrak{p}\}$ si et seulement si $\mathfrak{p}$ est un idéal maximal.

Définition 1.5. Si f est un élément de A, l'ensemble $D(f) := \{\mathfrak{p} \in \mathrm{spec}(A) \mid f \notin \mathfrak{p}\}$ est un ouvert, appelé *ouvert principal*.

Proposition 1.6. *Les ouverts principaux forment une base de la topologie de Zariski.*

Démonstration. Soit $U = \mathrm{spec}(A) \setminus V(I)$ un ouvert. Si $\mathfrak{p}$ un point de U, l'idéal I n'est pas contenu dans $\mathfrak{p}$ donc il existe $f \in I \setminus \mathfrak{p}$. Un point $\mathfrak{q} \in \mathrm{spec}(A)$ contient f si et seulement s'il ne contient pas I, donc l'ouvert principal $D(f)$ est inclus dans U et contient $\mathfrak{p}$. □

Morphismes.

A un morphisme d'anneaux unitaires $\phi\colon A \to B$, on peut associer une fonction

$$f\colon \begin{array}{ccc} \operatorname{spec}(B) & \to & \operatorname{spec}(A) \\ \mathfrak{p} & \mapsto & \phi^{-1}(\mathfrak{p}) \end{array}$$

Elle est bien définie car $\phi^{-1}(\mathfrak{p})$ est un idéal premier de B lorsque $\mathfrak{p}$ est un idéal premier de A ; et elle est continue car $f^{-1}(V(I)) = V(B\phi(I))$ pour un idéal I de A.

Proposition 1.7. *1. Si $\phi\colon A \to B$ est un morphisme surjectif, alors l'application continue associée $f\colon \operatorname{spec}(B) \to \operatorname{spec}(A)$ est d'image $V(\ker\phi)$ et induit un homéomorphisme $\operatorname{spec}(B) \to V(\ker\phi)$.*

2. Soit S un système multiplicatif de A. Le morphisme naturel $\phi\colon A \to S^{-1}A$ induit un homéomorphisme $\operatorname{spec}(S^{-1}A) \to \{\mathfrak{p} \in \operatorname{spec}(A) \mid \mathfrak{p} \cap S = \emptyset\}$.

En particulier, chaque fermé $V(I)$ est homéomorphe à $\operatorname{spec}(A/I)$ et chaque ouvert principal $D(f)$ est homéomorphe à $\operatorname{spec}(A_f)$.

1.2 L'espace affine

Cette section est dédiée à l'étude d'un exemple fondamental de spectres et de l'intuition géométrique associée. On travaillera sur un corps k, et on note $A = k[x_1, \ldots, x_n]$ l'anneau des polynômes sur k.

Définition 1.8. L'*espace affine* de dimension n sur k est $\mathbb{A}^n_k := \operatorname{spec}(A) = \operatorname{spec}(k[x_1, \ldots, x_n])$.

Commençons par comprendre les points de l'espace affine, en particulier les points fermés (c'est-à-dire les idéaux maximaux).

Lemme 1.9. *Soit $\mathfrak{m}$ un idéal maximal de A. Alors $k(\mathfrak{m}) = A/\mathfrak{m}$ est une extension algébrique de k.*

Le *degré* du point associé est alors défini comme le degré de l'extension $k(\mathfrak{m})/k$.

Démonstration. A est de type fini sur k, donc $k(\mathfrak{m})$ aussi. D'après le le lemme de Noether (théorème A.2), il existe un entier d et une injection finie $k[t_1, \ldots, t_d] \hookrightarrow k(m)$, avec $t_1, \ldots, t_d$ algébriquement indépendants sur k.

Supposons par l'absurde que $d \geq 1$. Comme $\frac{1}{t_1} \in k(\mathfrak{m})$ est entier sur $k[t_1, \ldots, t_d]$, on peut écrire

$$\left(\frac{1}{t_1}\right)^n + \sum_{0 \leq i \leq n-1} Q_i \left(\frac{1}{t_i}\right)^i = 0 \quad , Q_i \in k[t_1, \ldots, t_d]$$

d'où

$$t_1 \cdot \left(- \sum_{0 \leq i \leq n-1} Q_i t_1^{n-1-i} \right) = 1$$

ce qui est impossible. Ainsi $d = 0$, donc $k(\mathfrak{m})$ est entier sur k. □

Corollaire 1.10. *Si $\bar{k}$ est une clôture algébrique de k, les points fermés P de $\mathbb{A}^n_k$ s'identifient avec les $a \in \bar{k}^n$ modulo l'action du groupe $\operatorname{Aut}_k \bar{k}$. Si un $a \in \bar{k}^n$ correspond à un point P, alors $\deg P = [k(a) : k]$.*

Démonstration. A un n-uplet $a \in \bar{k}^n$, on associe l'idéal maximal des polynômes qui s'annulent en a. Réciproquement, si l'on se donne un idéal maximal $\mathfrak{m}$, alors $k(\mathfrak{m})$ se réalise comme sous-corps de $\bar{k}$ d'après le lemme. Soit $a = (a_1, \ldots, a_n)$ tel que la surjection canonique $A \to A/\mathfrak{m} = k(\mathfrak{m})$ envoie X_i sur $a_i \in \bar{k}$; $\mathfrak{m}$ est alors l'idéal des polynômes s'annulant en a et $k(\mathfrak{m}) = k(a)$, ce qui donne le degré annoncé. Remarquons que le n-uplet $a \in \bar{k}^n$ dépend de l'inclusion de $k(\mathfrak{m})$ dans $\bar{k}$ qui n'est pas canonique. Par exemple, tout $b \in \bar{k}^n$ qui est l'image de a par un élément $\mathrm{Aut}_k \bar{k}$ convient ; et réciproquement, si b convient, alors on a un isomorphisme de $k(a)$ vers $k(b)$ qui se prolonge en un automorphisme de $\bar{k}$. □

Corollaire 1.11. *Pour $k = \mathbb{F}_q$, le nombre de points fermés de $\mathbb{A}^n_k$ de degré au plus d est majoré par* $\operatorname{card} \mathbb{F}^n_{q^d} = q^{nd}$.

Il est bon de voir les éléments de A comme des fonctions sur $\mathbb{A}^n_k = \mathrm{spec}(A)$: informellement, la valeur d'un polynôme f en un point $\mathfrak{p}$ est son image dans $k(\mathfrak{p})$. Dire que f s'annule en $\mathfrak{p}$ revient à dire que $f \in \mathfrak{p}$.

Ainsi, l'ouvert principal $D(f)$ est vu comme l'ensemble des points n'annulant pas f. Pour un idéal I de polynômes, $V(I)$ est l'ensemble des points annulant simultanément toute les fonctions de l'idéal : on retrouve la notion classique de variété algébrique.

En poursuivant l'analogie qui consiste à voir A comme l'anneau des fonctions sur $\mathrm{spec}(A)$, les anneaux A_f et A/I s'interprètent comme les anneaux de fonctions sur $D(f)$ et $V(I)$ respectivement. Notons que cette interprétation est pour le moment incohérente. En effet, le théorème A.3 montre que $V(I)$ et $V(\sqrt{I})$ sont le même espace topologique ; pourtant, les anneaux A/I et $A/\sqrt{I}$ sont a priori différents. Cette incohérence sera levée dans le cadre des schémas.

1.3 Irréductibilité

Définition 1.12. Un espace topologique X est *irréductible* lorsqu'il est non vide et qu'il ne peut pas s'écrire $X = F_1 \cup F_2$ avec F_1 et F_2 deux fermés stricts de X.

Proposition 1.13. *Un ouvert non vide d'un espace topologique irréductible est irréductible. Dans un espace topologique quelconque, l'adhérence d'une partie irréductible est irréductible.*

Démonstration. Si X est un espace topologique irréductible et U est un ouvert de X, alors $\overline{U} = X$ car $X = \overline{U} \cup (X \setminus U)$. Ainsi si U est contenu dans l'union de deux fermés de X, l'un d'eux est X. Maintenant si X est un espace quelconque et Y est une partie irréductible de X, alors si $\overline{Y}$ est contenu dans une union de deux fermés de X, l'un d'eux contient Y donc aussi $\overline{Y}$. □

Définition 1.14. Un point $\eta \in X$ est dit *générique* si $\overline{\eta} = X$.

Exemple 1.15. Un point $\mathfrak{p} \in \mathrm{spec}(A)$ est générique pour $V(\mathfrak{p})$.

Proposition 1.16. *Un espace topologique admettant un point générique est irréductible.*

Démonstration. Soient X un espace topologique et η un point générique de X. Supposons que $X = F_1 \cup F_2$ avec F_1, F_2 des fermés de X, alors si $\eta \in F_i$ $(i = 1, 2)$ on a $X = \overline{\eta} \subset F_i$. Donc $F_i = X$, ce qui prouve bien l'irréductibilité de X. □

Définition 1.17. Un anneau A est dit *réduit* si son nilradical $\sqrt{(0)}$ est réduit à 0. Pour tout anneau A, on définit $A_{\mathrm{red}} := A/\sqrt{(0)}$; c'est un anneau réduit.

Proposition 1.18. *Pour tout anneau A,* $\mathrm{spec}(A) = \mathrm{spec}(A_{\mathrm{red}})$. *De plus, ce spectre est irréductible si et seulement si A_{red} est intègre.*

Démonstration. Supposons que $\mathrm{spec}(A)$ est irréductible. Soient $f, g \in A$ tels que fg est nilpotent. Alors $\mathrm{spec}(A) = V(fg) = V(f) \cup V(g)$, donc $\mathrm{spec}(A) = V(f)$ (quitte à échanger f et g). Ceci veut dire que f est dans tous les idéaux premiers de A, donc est nilpotent d'après le théorème A.3.

Réciproquement, si A_{red} est intègre, alors (0) est dans $\mathrm{spec}(A_{\mathrm{red}})$ et en est un point générique. □

Les fermés irréductibles de $\mathrm{spec}(A)$ sont donc exactement les $V(\mathfrak{p}) = \overline{\{\mathfrak{p}\}}$ avec $\mathfrak{p} \in \mathrm{spec}(A)$. Ainsi, les points de $\mathrm{spec}(A)$ sont en bijection avec ses fermés irréductibles.

Définition 1.19. Un espace topologique X est dit *noethérien* si toute suite décroissante de fermés est stationnaire.

Remarque 1.20. Un anneau A est noethérien (en tant qu'anneau) si et seulement si $\mathrm{spec}(A)$ l'est (en tant qu'espace topologique). En particulier, l'espace affine $\mathbb{A}^n_k$ est noethérien.

Proposition 1.21. *Dans un espace topologique noethérien X, tout fermé non vide peut s'écrire $Y = Y_1 \cup \ldots \cup Y_r$ avec les Y_i des fermés irréductibles tels que $\forall i \neq j, Y_i \not\subseteq Y_j$. Cette écriture est unique à permutation près.*

Les Y_i sont alors les *composantes irréductibles* de Y, c'est-à-dire les fermés irréductibles maximaux de Y.

Démonstration. Montrons tout d'abord l'existence d'une telle écriture de Y. Soit $\mathfrak{S}$ l'ensemble des fermés non vides de X qui *ne peuvent pas* s'écrire comme union finie de fermés irréductibles et supposons $\mathfrak{S}$ non vide. Comme X est noethérien, $\mathfrak{S}$ doit avoir un élément minimal. Si Y est un tel élément, alors Y n'est pas irréductible par définition de $\mathfrak{S}$ donc il s'écrit $Y = Y' \cup Y''$ avec Y' et Y'' des fermés stricts de Y. Par minimalité de Y, Y' et Y'' s'écrivent comme union finie de fermés irréductibles et donc Y aussi, ce qui est absurde. D'où l'existence d'une écriture de Y sous la forme $Y = Y_1 \cup \ldots \cup Y_r$. En enlevant quelques Y_i, on peut supposer $\forall i \neq j, Y_i \not\subseteq Y_j$.

Passons maintenant à l'unicité. Si $Y = Y'_1 \cup \ldots \cup Y'_s$, alors $Y'_1 = \cup_{i=1}^r (Y'_1 \cap Y_i)$. Comme Y'_1 est irréductible il existe i tel que $Y'_1 \subseteq Y_i$, on peut supposer $i = 1$. De la même manière on trouve j tel que $Y_1 \subseteq Y'_j$, ce qui donne $j = 1$ et donc $Y_1 = Y'_1$. En répétant cet algorithme on trouve finalement $s = r$ et $\forall i \in \{1, \ldots, r\}, Y_i = Y'_i$. □

Remarque 1.22. Un espace topologique X est toujours recouvert par ses composantes irréductibles (en particulier, elles existent). En effet, l'union d'une chaîne croissante de fermés irréductibles est irréductible, donc on peut appliquer le lemme de Zorn à l'ensemble des fermés irréductibles qui contiennent un point fixé x (cet ensemble est non vide car il contient $\overline{\{x\}}$).

1.4 Dimension

Définition 1.23. La *dimension* d'un espace topologique X est le plus grand entier $n \in \mathbb{N} \cup \{\infty\}$ tel qu'il existe une suite $Z_0 \subset Z_1 \subset \ldots \subset Z_n$ de fermés irréductibles distincts de X. On la note $\dim(X)$.

Proposition 1.24. *Pour tout sous-ensemble Y de X, on a* $\dim(Y) \leq \dim(X)$.

Démonstration. Soit $Z_0 \subset Z_1 \subset \ldots \subset Z_n$ une suite strictement croissante de fermés irréductibles de Y. On considère Z_i' l'adhérence de Z_i dans X ; les Z_i' sont donc des fermés irréductibles de X. Comme Z_i est fermé dans Y, $Z_i = Z_i' \cap Y$, donc la suite (Z_i') est strictement croissante. □

Proposition 1.25. *Si la dimension de X est finie, alors c'est le maximum des dimensions de ses composantes irréductibles.*

Démonstration. La dimension de X est évidemment supérieure à la dimension de chaque composante irréductible. Réciproquement, dans une suite maximale $Z_0 \subset Z_1 \subset \ldots \subset Z_n$ de fermés irréductibles distincts de X, le fermé Z_n est une composante irréductible de X de dimension $n = \dim(X)$. □

Proposition 1.26. *Si (U_i) est un recouvrement ouvert de X, alors la dimension de X est le supremum des dimensions des U_i.*

Démonstration. On sait que la dimension de chaque U_i est inférieure à celle de X. Donnons-nous maintenant une suite $Z_0 \subset Z_1 \subset \ldots \subset Z_n$ strictement croissante de fermés irréductibles. Soient x un point de Z_0 et U un ouvert du recouvrement qui contient x. Chacun des $U \cap Z_i$ est un fermé irréductible de U, et la suite $(U \cap Z_i)$ est strictement croissante (car $Z_i \setminus Z_{i-1}$ est un ouvert non vide de l'irréductible Z_i donc rencontre l'ouvert non vide $Z_i \cap U$ de Z_i). □

Définition 1.27. Soit A un anneau. La *hauteur* d'un idéal premier $\mathfrak{p}$ est le plus grand entier $n \in \mathbb{N} \cup \{\infty\}$ tel qu'il existe une suite $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_n = \mathfrak{p}$ d'idéaux premiers distincts. On la note $\mathrm{ht}(\mathfrak{p})$.

La *dimension de Krull* de A est le supremum des hauteurs de ses idéaux premiers. On la note $\dim(A)$.

Comme les fermés irréductibles de $\mathrm{spec}(A)$ sont les $V(\mathfrak{p})$ avec $\mathfrak{p}$ premier, les notions de dimension s'accordent bien :

Proposition 1.28. *Soit A un anneau. Alors* $\dim(A) = \dim(\mathrm{spec}(A))$.

Le théorème suivant, qu'on admettra, permet de calculer facilement des dimensions.

Théorème 1.29. *Soient k un corps et A un anneau intègre qui est une k-algèbre finiment engendrée. Alors*

$$\dim(A) = \mathrm{degtr}_k(\mathrm{Frac}(A))$$

Pour un idéal premier $\mathfrak{p}$ de A, on a

$$\mathrm{ht}(\mathfrak{p}) + \dim(A/\mathfrak{p}) = \dim(A)$$

Corollaire 1.30. *L'espace affine $\mathbb{A}_k^n$ est de dimension n.*

Définition 1.31. Une *courbe* (resp. *hypersurface*) de $\mathbb{A}_k^n$ est un fermé dont toutes les composantes irréductibles sont de dimension (resp. codimension) 1.

Lemme 1.32. *Dans un anneau factoriel, tout idéal premier de hauteur 1 est principal.*

Démonstration. Soient $\mathfrak{p}$ un tel idéal, et f un élément de $\mathfrak{p}$. Comme $\mathfrak{p}$ est premier, f a un facteur premier p dans $\mathfrak{p}$. Alors (p) est un idéal premier non nul contenu dans $\mathfrak{p}$, donc est égal à ce dernier. □

Proposition 1.33. *Les hypersurfaces de $\mathbb{A}_k^n$ sont données par les $V(f)$, avec f non constant.*

Démonstration. On rappelle que l'anneau $k[x_1, \ldots, x_n]$ est factoriel et noethérien. Si f est non constant, alors $V(f)$ est l'union d'un nombre fini de fermés $V(p)$ avec p des polynômes irréductibles ; cette union est la décomposition de $V(f)$ en composantes irréductibles, et chaque $V(p)$ est de codimension 1 d'après le théorème 1.29, donc $V(f)$ aussi. Réciproquement, soit $V(I)$ une hypersurface. Ecrivons sa décomposition en composantes irréductibles $V(I) = \bigcup V(\mathfrak{p})$; elle est finie et chaque $V(\mathfrak{p})$ est de codimension 1, donc chaque $\mathfrak{p}$ est de hauteur 1, c'est-à-dire qu'il s'écrit $\mathfrak{p} = (p)$ d'après le lemme précédent. Alors $V(I) = V(\prod p)$. □

1.5 Régularité d'une courbe plane en un point fermé

Les notions et résultats présentés ici seront surtout utilisés dans la section 4.2. Le cadre sera donc l'espace affine $\mathbb{A}_k^2$, où $k = \mathbb{F}_q$ est un corps fini de caractéristique p. D'après la section précédente, une courbe est un fermé $V(f)$, où f est un polynôme non nul ; on désignera dans la suite la courbe par f. De même, on confondra un point fermé $\mathfrak{m}_P \in \mathbb{A}_k^2$ avec un couple $P \in \bar{k}^2$ correspondant.

L'objectif est ici d'étudier sous quelles conditions une courbe f est lisse en un point fermé P, ainsi que de déterminer la densité des telles courbes.

Définition 1.34. Une courbe f est *lisse* (ou *régulière*) en un point P si elle ne passe pas par P, ou si $(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y})$ ne s'annule pas en P. Autrement dit, elle est lisse si le triplet $(f, \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y})$ ne s'annule pas en P. Elle est *singulière* en P si elle n'y est pas régulière.

Remarque 1.35. Quelques remarques à propos de l'amalgame entre la courbe $V(f)$ et f :

- Il est abusif : en effet $V(f) = V(f^2)$, mais $f \neq f^2$.
- La définition de la régularité provient de la géométrie réelle ; cependant elle est très peu satisfaisante dans la mesure où elle repose sur f et non sur $V(f)$. Elle est d'autant moins satisfaisante qu'elle ne produit pas toujours les mêmes résultats pour des f correspondant à la même courbe : par exemple si f s'annule en P, alors f^2 est toujours singulière au sens de cette définition mais f peut quand même être régulière.

On se permettra néanmoins de faire dans cette partie l'abus de considérer f au lieu de $V(f)$: le point de vue des schémas (qui sera développé dans la partie suivante) effacera ce problème et fournira une définition intrinsèque (et plus générale) de la régularité.

On montre dans cette section que l'ensemble des courbes singulières en P est $\mathfrak{m}_P^2$. Pour cela, introduisons l'espace cotangent :

Définition 1.36. L'*espace cotangent* en un point P est $\mathfrak{m}_P/\mathfrak{m}_P^2$.

Il peut être muni d'une structure de $k(P)$-espace vectoriel de la manière suivante : si $f \in \mathfrak{m}_P/\mathfrak{m}_P^2$ et $\alpha \in k(P) = k[x,y]/\mathfrak{m}_P$, on choisit des représentants $\widetilde{f} \in \mathfrak{m}_P$ et $\widetilde{\alpha} \in k[x,y]$, et on pose $\alpha \cdot f$ comme étant l'image de $\widetilde{\alpha}\widetilde{f}$ dans $\mathfrak{m}_P^2$. On vérifie que cette définition est correcte (ne dépend pas du représentant, et fournit bien une structure d'espace vectoriel).

Si $f \in \mathfrak{m}_P/\mathfrak{m}_P^2$ et $\widetilde{f} \in \mathfrak{m}_P$ en est un représentant, on vérifie que $\frac{\partial \widetilde{f}}{\partial x}(P)$ et $\frac{\partial \widetilde{f}}{\partial y}(P)$ ne dépendent pas du choix de $\widetilde{f}$. Cela définit ainsi une application

$$\phi\colon \begin{array}{ccc} {}^{m_P}\!/_{m_P^2} & \to & k(P)^2 \\ f & \mapsto & (\frac{\partial \widetilde{f}}{\partial x}(P), \frac{\partial \widetilde{f}}{\partial y}(P)) \end{array}$$

La proposition suivante donne alors la caractérisation désirée de la régularité.

Proposition 1.37. *L'application ϕ est un isomorphisme de $k(P)$-espaces vectoriels.*

Démonstration. — ϕ est un morphisme : vérification immédiate.

— ϕ est surjective : notons $P = (a, b) \in k(P)^2$. Soit π_a le polynôme minimal de a sur k. Supposons, par l'absurde, que $\pi_a'(a) = 0$. Alors $\pi_a \mid \pi_a'$, donc $\pi_a' = 0$. Ainsi, $\pi_a(x)$ s'écrit $\sum a_i x^{ip}$. Comme k est un corps fini, chaque a_i a une racine p-ième dans k, notée b_i ; il vient alors $\pi_a(x) = (\sum b_i x^i)^p$, ce qui est impossible par irréductibilité. Ainsi, $\pi_a'(a) = \alpha \neq 0$, et de même $\pi_b'(b) = \beta \neq 0$. On a donc une base de $k(P)^2$ formée par $\phi(\pi_a(x)) = (\alpha, 0)$ et $\phi(\pi_b(y)) = (0, \beta)$.

— ϕ est un isomorphisme : un système de générateurs de l'idéal $\mathfrak{m}_P$ donne aussi un système de générateurs de l'espace vectoriel $\mathfrak{m}_P/\mathfrak{m}_P^2$; il nous suffit donc de montrer que $\mathfrak{m}_P$ est engendré par deux éléments. Il s'avère en fait que l'un de ces deux générateurs peut être $\pi_a(x)$, c'est à dire que $\mathfrak{m}_P/(\pi_a(x))$ est un idéal principal de $k[x, y]/(\pi_a(x))$; en effet cet anneau est principal, car c'est $(k[x]/(\pi_a(x))[y]$, et $k[x]/(\pi_a(x))$ est un corps.

□

Remarque 1.38. Cette proposition admet en fait plusieurs degrés de généralité supplémentaires :

1. On peut remplacer $k = \mathbb{F}_q$ par un corps de caractéristique nulle quelconque (par exemple $\mathbb{R}$), ou même n'importe quel corps parfait.
2. En dimension n, on a un isomorphisme analogue entre $\mathfrak{m}_P/\mathfrak{m}_P^2$ et $k(P)^n$; la preuve s'écrit de la même manière (pour montrer que $\mathfrak{m}_P$ est engendré par n éléments, le cas $n = 2$ s'étend en une récurrence sur n). La régularité d'une hypersurface se définit donc de façon totalement analogue à celle des courbes du plan (sous les mêmes réserves que celles exprimées à la remarque 1.35).
3. En caractéristique nulle, les quotients suivants $\mathfrak{m}_P^i/\mathfrak{m}_P^{i+1}$ peuvent se comprendre de la même manière (suivant le point précédent, on se place en dimension n : $\mathfrak{m}_P$ est un idéal maximal de $k[x_1, \ldots, x_n]$). Comme pour $i = 1$, on vérifie que $\mathfrak{m}_P^i/\mathfrak{m}_P^{i+1}$ est un $k(P)$-espace vectoriel, et que le morphisme suivant est bien défini :

$$\phi\colon \begin{array}{ccc} {}^{m_P^i}\!/_{m_P^{i+1}} & \to & k(P)^{l(i,n)} \\ f & \mapsto & \left(\frac{\partial^{|\alpha|} f}{\partial x^\alpha}(P)\right)_{|\alpha|=i} \end{array}$$

où α est un n-uplet de somme i et $l(i, n)$ est le nombre de tels n-uplets (qui est aussi la dimension de l'espace des polynômes homogènes de degré i).

On prouve alors que ϕ est un isomorphisme suivant le même plan. Pour la surjectivité, on considère, pour un n-uplet α fixé, l'élément de $\mathfrak{m}_P^i/\mathfrak{m}_P^{i+1}$ correspondant au polynôme $\pi_1(x_1)^{\alpha_1} \ldots \pi_n(x_n)^{\alpha_n}$, où π_j est le polynôme minimal de a_j (en écrivant $P = (a_1, \ldots, a_n)$). Pour en déduire la bijectivité, il suffit alors de montrer que $\mathfrak{m}_P^i/\mathfrak{m}_P^{i+1}$ est de dimension au plus $l(i, n)$. Or on sait déjà que $\mathfrak{m}_P$ est engendré (en tant qu'idéal) par n éléments $u_1, \ldots, u_n$; il en découle que les $u_1^{\alpha_1} \ldots u_n^{\alpha_n}$ engendrent $\mathfrak{m}_P^i/\mathfrak{m}_P^{i+1}$.

Corollaire 1.39. *La densité des courbes lisses en P est* $(\operatorname{card} k[x,y]/\mathfrak{m}_P^2)^{-1} = q^{-3\deg(P)}$.

Démonstration. $\mathfrak{m}_P/\mathfrak{m}_P^2$ est un idéal de $k[x,y]/\mathfrak{m}_P^2$ et l'anneau quotient associé est $\frac{k[x,y]}{\mathfrak{m}_P^2}/\frac{\mathfrak{m}_P}{\mathfrak{m}_P^2}$, qui est isomorphe à $k[x,y]/\mathfrak{m}_P = k(P)$. D'après la proposition, on a alors

$$\operatorname{card}\frac{k[x,y]}{\mathfrak{m}_P^2} = \operatorname{card} k(P)\cdot\operatorname{card}\frac{\mathfrak{m}_P}{\mathfrak{m}_P^2} = \operatorname{card} k(P)^3 = q^{3\deg(P)}$$

□

2 Généralités sur les schémas

Cette partie présente quelques notions et propriétés de base associées aux schémas. Elle est en grande partie inspirée de [Har10].

2.1 Notion de faisceau

On introduit ici la notion de faisceau nécessaire à la définition des schémas.

Définition 2.1. Soit X un espace topologique. Un *préfaisceau* $\mathcal{F}$ de groupes abéliens est la donnée pour tout ouvert U de X d'un groupe abélien $\mathcal{F}(U)$ et pour tout ouvert $V \subseteq U$ d'un morphisme $\rho_V^U : \mathcal{F}(U) \to \mathcal{F}(V)$ (que l'on appelle application de restriction), vérifiant les conditions suivantes :

(i) $\mathcal{F}(\emptyset) = \{0\}$ et $\rho_U^U = \mathrm{id}_U$.

(ii) Pour tous ouverts U, V, W tels que $W \subseteq V \subseteq U$: $\rho_W^U = \rho_W^V \circ \rho_V^U$

On définit de même un préfaisceau d'anneaux commutatifs, d'algèbres sur un corps ou un anneau fixé. Un élément $s \in \mathcal{F}(U)$ s'appelle une *section* de $\mathcal{F}$ sur U. Les exemples de faisceaux les plus immédiats sont donnés par des algèbres de fonctions (par exemple, le préfaisceau des fonctions continues) ; c'est pour cela qu'on appelle les ρ_V^U des applications de restriction, et on notera donc $s_{|V} = \rho_V^U(s)$.

Définition 2.2. On dit qu'un préfaisceau $\mathcal{F}$ est un *faisceau* si les deux conditions de recollement suivantes sont vérifiées :

(i) (Unicité) Si U est un ouvert de X et (U_i) un recouvrement ouvert de U, alors pour toute section $s \in \mathcal{F}(U)$ vérifiant $s_{|U_i} = 0$ pour tout i, on a $s = 0$.

(ii) (Existence) Avec les notations ci-dessus, si des $s_i \in \mathcal{F}(U_i)$ sont donnés avec la propriété que pour tout i, j : $(s_i)_{|U_i \cap U_j} = (s_j)_{|U_i \cap U_j}$, alors il existe un unique $s \in \mathcal{F}(U)$ tel que pour tout i, $s_{|U_i} = s_i$.

Remarque 2.3. La condition d'unicité dans (ii) est impliqué par (i).

Un faisceau est donc un préfaisceau avec la propriété que pour définir une fonction globalement, il suffit de la définir localement.

Exemple 2.4. Si X est un espace topologique, on a le faisceau des fonctions continues vers $\mathbb{R}$: $\mathcal{F}(U)$ est l'ensemble des fonctions continues de U vers $\mathbb{R}$. Les applications de restrictions sont évidentes.

En revanche, le préfaisceau des applications constantes n'est pas un faisceau. Le faisceau correspondant (cela a un sens précis, qu'on ne détaille pas ici) est celui des applications localement constantes.

Définition 2.5. Soit $(I, <)$ un ensemble ordonné. On dit que I est *filtrant* si et seulement si

$$\forall i, j \in I, \exists k \in I, i \leq k \text{ et } j \leq k$$

Soit I un ensemble ordonné filtrant. On se donne $(E_i, f_j^i)_{i \leq j, (i,j) \in I^2}$ avec E_i des anneaux et $f_j^i : E_i \to E_j$ des morphismes avec les propriétés :

(i) $\forall i \in I, f_i^i = \mathrm{id}$.

(ii) $\forall (i, j, k) \in I^3, i \leq k \leq j \Rightarrow f_j^i = f_j^k \circ f_k^i$.

Alors on définit la *limite inductive* de (E_i, f_j^i) comme étant

$$\varinjlim_{E_i} := \bigsqcup E_i / \sim$$

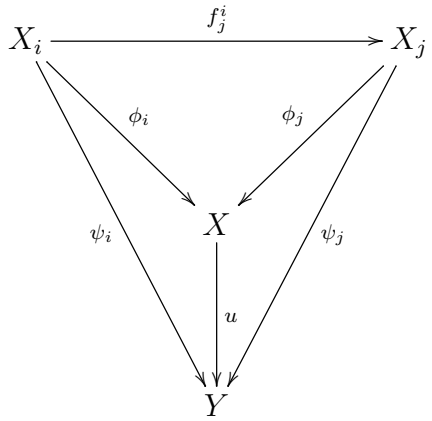
avec $\sim$ la relation d'équivalence suivante :

$$(i, x) \sim (j, y) \Leftrightarrow \exists k \in I, k \geq i, k \geq j, f_k^i(x) = f_k^j(x)$$

C'est aussi un anneau, intègre si chaque E_i l'est. C'est un corps si chaque E_i en est un.

On peut aussi définir la limite inductive sous forme de problème universel :

Proposition 2.6. *Soit (X_i, f_j^i) un système inductif, la limite inductive E est munie de morphismes $\phi_i : X_i \to X$ avec la propriété de compatibilité suivante : $\forall i \leq j, \phi_i = \phi_j \circ f_j^i$. De plus, la donnée de (X, ϕ_i) est universelle au sens suivant : Si Y est muni de morphismes ψ_i vérifiant les mêmes propriétés de compatibilité que les ϕ_i, alors il existe un unique morphisme $u : X \to Y$, tel que le diagramme suivant :*



soit commutatif, pour tout $i \leq j$.

Définition 2.7. Soit $\mathcal{F}$ un préfaisceau sur X et $x \in X$. On définit la *tige* $\mathcal{F}_x$ de $\mathcal{F}$ en x comme la limite inductive des $\mathcal{F}(U)$ pour U ouvert contenant x.

On peut donc voir un élément de $\mathcal{F}_x$ comme une paire (U, s) avec U un voisinage ouvert de x et $s \in \mathcal{F}(U)$, où on identifie deux paires (U, s) et (V, t) s'il existe W un voisinage ouvert de x inclus dans $U \cap V$ tel que $s_{|W} = t_{|W}$.

Remarque 2.8. Supposons qu'on indice tous les ouverts contenant x par un ensemble I, notons les $(U_i)_{i \in I}$. Ici l'ordre sur I est donné par $i < j \Leftrightarrow U_j \subset U_i$, I est alors bien filtrant car si i, j sont dans I, soit k l'indice de I tel que $U_k = U_i \cap U_j$ (U_k est non vide car $x \in U_i \cap U_j$), on a $i \leq k$ et $j \leq k$.

Remarque 2.9.

1. Si $\mathcal{B}$ est une base d'ouverts de X stable par intersection finie, pour définir un faisceau $\mathcal{F}$ sur X, il suffit de définir $\mathcal{F}(U)$ pour U dans $\mathcal{B}$ et de définir les morphismes de restrictions ρ_V^U pour U, V dans $\mathcal{B}$, en respectant les conditions de compatibilité et de recollement. Ensuite, pour définir $\mathcal{F}(U)$ pour U un ouvert quelconque, il suffit de le recouvrir par des ouverts $U_i \in \mathcal{B}$ et de prendre pour $\mathcal{F}(U)$ l'ensemble des familles $(s_i)_i \in \prod_i \mathcal{F}(U_i)$ telles que $(s_i)_{|U_i \cap U_j} = (s_j)_{|U_i \cap U_j}$ pour tout i, j, les applications de restrictions sont alors évidentes.

   On vérifie que cette construction ne dépend pas du recouvrement choisi grâce à la propriété d'unicité du recollement.
2. Si $\mathcal{F}$ est un faisceau sur X, on peut le restreindre en un faisceau sur tout ouvert U de X.
3. Si $\mathcal{F}$ est un faisceau, on peut restreindre toute section $s \in \mathcal{F}(U)$ en $s_x \in \mathcal{F}_x$ pour tout x dans U. Alors deux sections s et t coïncident sur U si et seulement si pour tout $x \in U$ $s_x = t_x$. On voit apparaître ici l'analogie avec les fonctions mentionnée précédemment. On voit $s \in \mathcal{F}(U)$ comme une fonction sur U ainsi : si $x \in U$, on pose $s(x) = s_x$ l'image de s dans la tige $\mathcal{F}_x$.

Définition 2.10. Soit X un espace topologique. Un *morphisme de faisceaux* $\phi : \mathcal{F} \to \mathcal{G}$ est une famille de morphismes $\phi_U : \mathcal{F}(U) \to \mathcal{G}(U)$ satisfaisant la condition de compatibilité suivante : pour tout ouvert U, V de X tels que $V \subseteq U$, le diagramme suivant :

$$\begin{array}{ccc} \mathcal{F}(U) & \xrightarrow{\phi_U} & \mathcal{G}(U) \\ \downarrow & & \downarrow \\ \mathcal{F}(V) & \xrightarrow{\phi_V} & \mathcal{G}(V) \end{array}$$

est commutatif, les flèches verticales étant les restrictions.

Remarque 2.11. Un morphisme de faisceaux $\phi : \mathcal{F} \to \mathcal{G}$ induit un morphisme sur les tiges $\mathcal{F}_x \to \mathcal{G}_x$.

Enfin, on va définir la notion d'image directe d'un faisceau ce qui nous permettra de changer d'espace :

Définition 2.12. Soit $f : X \to Y$ une application continue entre espaces topologiques. Pour tout faisceau $\mathcal{F}$ sur X, on définit l'*image directe* $f_*\mathcal{F}$ par :

$$f_*\mathcal{F}(V) = \mathcal{F}(f^{-1}(V))$$

pour tout V ouvert de Y. C'est un faisceau sur Y.

Remarque 2.13. La tige en $f(x)$ de $f_*\mathcal{F}$ n'est pas en général $\mathcal{F}_x$. En revanche, il y a un morphisme canonique ϕ_x de $(f_*\mathcal{F})_x$ vers $\mathcal{F}_x$ donné par $\phi_x(s, V) = (s, f^{-1}(V))$. En effet, si s est une section de $\mathcal{F}$ sur $f^{-1}(V)$ avec $f(x) \in V$, alors par continuité de f, il existe un ouvert U de X qui contient x, tel que $f(U) \subset V$, c'est à dire $U \subset f^{-1}(V)$, on peut donc restreindre s à U.

2.2 Le faisceau structural sur spec A

Définition 2.14. Soit A un anneau commutatif.

- Soit S une partie de A, on dit que S est un système multiplicatif si $1 \in S$ et $\forall x, y \in S, xy \in S$.
- On définit le localisé de A par rapport au système multiplicatif S, noté $S^{-1}A$, l'espace $A \times S$ que l'on quotiente par la relation d'équivalence :

$$(a, s) \sim (a', s') \Leftrightarrow \exists t \in S, t(as' - a's) = 0.$$

On note alors a/s la classe d'équivalence de (a, s) et on obtient un anneau avec les opérations usuelles :

$$\frac{a}{s} + \frac{a'}{s'} = \frac{as' + a's}{ss'} \text{ et } \frac{a}{s} \times \frac{a'}{s'} = \frac{aa'}{ss'}$$

Le but de cette section est de construire un faisceau d'anneaux $\mathcal{O}_X$ sur l'espace topologique $X = \text{spec}\, A$, tel que pour tout $\mathfrak{p} \in \text{spec}\, A$, la tige de $\mathcal{O}_X$ en $\mathfrak{p}$ soit $A_\mathfrak{p}$ qui est le localisé de A par rapport à la partie multiplicative $A \setminus \mathfrak{p}$, ce sera donc un anneau local avec pour seul idéal maximal $\mathfrak{p}A_\mathfrak{p}$ car on a inversé tous les éléments qui ne sont pas dans $\mathfrak{p}$. On veut aussi que pour tout $f \in A$, la restriction du faisceau $\mathcal{O}_X$ à $D(f)$ soit isomorphe à $\mathcal{O}_Y$ avec $Y = \text{spec}\, A_f$, où A_f est le localisé de A par rapport à la partie multiplicative $\{1, f, f^2, \ldots\}$. Cette idée est assez intuitive car on veut voir $\mathcal{O}_X(U)$ comme étant l'anneau des fonctions régulières sur U, ainsi si $U = D(f)$, on définit pour tout $\mathfrak{p} \in U$, $(a/f^n)(\mathfrak{p}) = a/f^n \mod \mathfrak{p}$. Il est donc nécessaire que f ne s'annule pas en $\mathfrak{p}$, c'est à dire $f \notin \mathfrak{p}$. On aura en particulier $H^0(X, \mathcal{O}_X) := \mathcal{O}_X(X) = A$. On dit que $H^0(X, \mathcal{O}_X)$ est l'anneau des fonctions régulières sur X.

On va d'abord définir $\mathcal{O}_X(D(f))$ et les applications de restriction $\mathcal{O}_X(D(f)) \to \mathcal{O}_X(D(g))$ lorsque $D(g) \subseteq D(f)$. On pose $\mathcal{O}_X(D(f)) = A_f$. Si $D(g) \subset D(f)$, cela implique que pour tout $\mathfrak{p} \in \text{spec}\, A$, $f \in \mathfrak{p} \Rightarrow g \in \mathfrak{p}$, donc $g \in \sqrt{(f)}$ d'après le théorème A.3. Donc il existe $m > 0$ et $b \in A$ tels que $g^m = fb$, ainsi, f est inversible dans A_g et on obtient un morphisme $A_f \to A_g$ canonique par définition de la localisation (cela revient à envoyer af^{-n} sur $ab^n g^{-mn}$). De plus, c'est un isomorphisme si $D(f) = D(g)$. On a donc bien défini $\mathcal{O}_X(U)$ et les restrictions $\mathcal{O}_X(U) \to \mathcal{O}_X(V)$ pour U, V des ouverts principaux de spec A.

Maintenant d'après la partie 1, les ouverts principaux forment une base de topologie $\mathcal{B}$ de spec A, et cette base est stable par intersection finie, étant donné que $D(f) \cap D(g) = D(fg)$. D'après la remarque 2.9, il suffit de montrer le lemme suivant :

Lemme 2.15. *Soit (U_i) un recouvrement de $U \in \mathcal{B}$ par des ouverts principaux. Alors si on se donne des $s_i \in O_X(U_i)$ avec $(s_i)_{|U_i \cap U_j} = (s_j)_{|U_i \cap U_j}$ pour tout i, j, il existe une unique section $s \in \mathcal{O}_X(U)$ telle que $s_{|U_i} = s_i$ pour tout i.*

Démonstration. Il suffit de montrer le cas $U = \text{spec}\, A$, quitte à remplacer A par un localisé A_f. On pose $U_i = D(f_i)$, l'hypothèse $U = \bigcup U_i$ se traduit par :

$$V(\sum_i (f_i)) = \bigcap_i V(f_i) = \emptyset,$$

c'est à dire que l'idéal engendré par les f_i est A tout entier. On écrit alors $1 \in \sum_{i \in F}(f_i)$ avec F une partie finie. Notons que pour tout entier $k \geq 1$: $U = \bigcup_{i \in F} D(f_i) = \bigcup_{i \in F} D(f_i^k)$ et donc $1 \in \sum_{i \in F}(f_i^k)$.

On commence par montrer l'unicité, soit $s \in A$ tel que pour tout $i \in F$, $s_{|U_i} = 0$ dans A_{f_i}. Cela signifie que l'image de s dans A_{f_i} est nulle donc comme F est une partie finie, il existe un entier $m > 0$ tel que pour tout $i \in F$, $f_i^m s = 0$. Mais d'après la remarque précédente $1 \in \sum_{i\in F}(f_i^m)$, donc $s \in \sum_{i\in F}(sf_i^m) = \{0\}$.

Passons maintenant à l'existence, supposons donnés des s_i dans $\mathcal{O}_X(U_i) = A_{f_i}$ vérifiant la condition de recollement. On peut trouver $m > 0$ tel que $s_i = b_i f_i^{-m}$ pour tout i dans F, avec les b_i dans A. La condition de recollement donne que s_i et s_j ont la même image dans $A_{f_i f_j}$, on peut donc trouver $r > 0$ tel que

$$(b_i f_j^m - b_j f_i^m)(f_i f_j)^r = 0 \tag{1}$$

pour tout i, j dans F. D'après le début de la preuve, on peut écrire $1 = \sum_{j\in F} a_j f_j^{m+r}$ avec $a_j \in A$. On cherche tout d'abord $s \in A$ tel que pour tout i, l'image de $sf_i^m - b_i$ soit nulle dans A_{f_i}. Pour $i \in F$, on a :

$$(sf_i^m - b_i) = sf_i^m - \sum_{j\in F} a_j f_j^{m+r} b_i$$

Posons

$$s = \sum_{j\in F} a_j b_j f_j^r$$

alors

$$(sf_i^m - b_i) = \sum_{j\in F} a_j f_j^r (b_j f_i^m - b_i f_j^m)$$

et la relation (1) donne que pour tout i dans F, $(sf_i^m - b_i)f_i^r = 0$. Donc l'image de $(sf_i^m - b_i)$ est nulle dans A_{f_i}, ce qui montre que $s_{|U_i} = s_i$ dès que $i \in F$.

Maintenant soit j quelconque, les restrictions de $s_{|U_j}$ et s_j à $U_i \cap U_j$ sont les mêmes pour tout i dans F : en effet la première est aussi la restriction de $s_{|U_i} = s_i$ à $U_i \cap U_j$. Ceci implique $s_j = s_{|U_j}$ à cause de l'unicité vue plus haut car chaque U_j est recouvert par les $U_i \cap U_j$ pour i dans F. □

Cette démonstration montre aussi que :

Lemme 2.16. *L'espace topologique* spec A *est quasi-compact*

Démonstration. En effet, on a vu dans la démonstration précédente que de tout recouvrement (U_i) par des ouverts principaux, on pouvait extraire un sous-recouvrement fini $(U_i)_{i\in F}$. □

Le faisceau $\mathcal{O}_X$ sur $X = \operatorname{spec} A$ s'appelle le *faisceau structural* de X. On peut notamment noter qu'il nous est maintenant possible de distinguer spec k, spec L et spec $k[t]/t^2$ avec k, L des corps : les spectres sont tous constitués d'un seul élément mais les faisceaux structuraux sont différents.

Proposition 2.17. *Soit $X = \operatorname{spec} A$ et $\mathfrak{p} \in X$, la tige $\mathcal{O}_{X,\mathfrak{p}}$ du faisceau structural en $\mathfrak{p}$ est isomorphe à $A_{\mathfrak{p}}$.*

Démonstration. L'ouvert $D(f)$ contient $\mathfrak{p}$ si et seulement si $f \notin \mathfrak{p}$. Il faut donc montrer que le morphisme canonique

$$\phi : \varinjlim_{f \notin \mathfrak{p}} A_f \to A_{\mathfrak{p}}$$

est un isomorphisme.

Explicitons tout d'abord ce morphisme. On a pour tout $f \notin \mathfrak{p}$ une inclusion $\iota_f : A_f \hookrightarrow A_{\mathfrak{p}}$. Ensuite, on note si $D(g) \subset D(f)$, $\rho_g^f : A_f \to A_g$ l'application de restriction. On montre alors que pour tout $f \notin \mathfrak{p}$, $\iota_f = \iota_g \circ \rho_g^f$. En effet, comme $D(g) \subset D(f)$, on a $g \in \sqrt{(f)}$, donc on peut trouver $n \geq 1$ et $b \in A$ tels que $g^n = fb$, on a alors $\rho_g^f(f^{-k}) = b^k/g^{nk}$ et le résultat suit. Donc par la proposition 2.6, ϕ est bien défini et on peut calculer ses valeurs : pour tout $f \notin \mathfrak{p}$ et $a \in A$, $\phi(af^{-N}, D(f)) = \iota_f(af^{-N}) = af^{-N}$. La compatibilité des fonctions ι_f, ι_g et ρ_g^f permet de montrer que la valeur trouvée à l'arrivée ne dépend pas du choix du représentant $(af^{-N}, D(f))$ dans la limite inductive.

On voit donc que la surjectivité de ϕ est directe. Soit $f \notin \mathfrak{p}$, $a \in A$ et $N \in \mathbb{N}$, alors af^{-N} a pour antécédent la classe de $(af^{-N}, D(f))$ dans la limite inductive.

Montrons l'injectivité de ϕ : Si af^{-N} a une image nulle dans $A_{\mathfrak{p}}$, il existe $g \notin \mathfrak{p}$ tel que $ag = 0$ ce qui implique que l'image de af^{-N} dans A_{fg} est nulle, donc par définition elle est aussi nulle dans la limite inductive des A_f pour $f \notin \mathfrak{p}$. □

Remarque 2.18. On aurait aussi pu définir le faisceau $\mathcal{O}_X$ sur $X = \operatorname{spec}(A)$ en prenant pour $\mathcal{O}_X(U)$ les fonctions $s : U \to \amalg_{\mathfrak{p} \in U} A_{\mathfrak{p}}$ vérifiant : pour tout $\mathfrak{p}$ de U, $s(\mathfrak{p}) \in A_{\mathfrak{p}}$, et au voisinage de tout $\mathfrak{p}$ de U, s provient d'un élément de A_f pour un certain f (c'est à dire qu'il existe un voisinage principal $V = D(f) \cap U$ contenant $\mathfrak{p}$ et un élément $a \in A_f$ tels que pour tout $\mathfrak{q} \in V$, $s(\mathfrak{q}) = a$).

2.3 Notion de schéma

Définition 2.19. Un *espace annelé* est la donnée d'un couple $(X, \mathcal{O}_X)$ avec X un espace topologique et $\mathcal{O}_X$ un faisceau d'anneaux sur X (appelé *faisceau structural de* X tel que pour tout x dans X, $\mathcal{O}_{X,x}$ est un anneau local. Si on note $\mathcal{M}_x$ l'idéal maximal de $\mathcal{O}_{X,x}$ alors $\mathcal{O}_{X,x}/\mathcal{M}_x$ est appelé le *corps résiduel* de x.

D'après la partie précédente, spec A muni de son faisceau structural est un espace annelé. La définition du corps résiduel correspond bien à celle donnée dans le cadre des spectres, en vertu de la propriété suivante : si $\mathfrak{p} \in \operatorname{spec}(A)$ est un idéal premier de A, alors $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ est canoniquement isomorphe à $\operatorname{Frac}(A/\mathfrak{p})$.

Exemple 2.20.

1. Sur spec $\mathbb{Z}$, la tige du point générique (0) est $\mathbb{Q}$ et celle de (p) est l'anneau des entiers p-adiques $\mathbb{Z}_p$. Les corps résiduels sont donc $\mathbb{Q}$ et $\mathbb{Q}_p$ respectivement.
2. Sur $A_k^1 = \operatorname{spec}(k[t])$, le corps résiduel du point générique est $k(t)$. Celui de (P) pour P un polynôme irréductible est $k[t]/(P)$. C'est une extension finie de k.
3. De manière plus générale, si A est un anneau, alors le corps résiduel de $\mathfrak{p} \in \operatorname{spec} A$ est $\operatorname{Frac}(A/\mathfrak{p})$. Si A est intègre le corps résiduel du point générique (0) est $\operatorname{Frac} A$.

Un schéma va être un espace annelé qui va ressembler localement au spectre d'un anneau. Pour arriver à cette définition, il nous faut d'abord définir la notion de morphisme entre espaces annelés.

Définition 2.21. Soit $\phi : A \to B$ un morphisme entre anneaux locaux. ϕ est *local* si l'image de l'idéal maximal de A est contenue dans celui de B. C'est équivalent à demander que la préimage de l'idéal maximal de B soit l'idéal maximal de A.

Définition 2.22. Un *morphisme d'espaces annelés* $(X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ est la donnée d'une paire $(f, f^\sharp)$ où $f : X \to Y$ est une application continue et $f^\sharp : \mathcal{O}_Y \to f_*\mathcal{O}_X$ un morphisme de faisceaux sur Y, tels que pour tout x dans X, le morphisme induit

$$f_x^\sharp : \mathcal{O}_{Y,y} \to \mathcal{O}_{X,x}$$

soit local, avec $y = f(x)$

Remarque 2.23. D'après la remarque 2.13, $f_x^\sharp$ est défini de manière canonique.

On définit aussi la composée de deux morphismes d'espaces annelés et la notion d'isomorphisme d'espace annelé de manière claire.

Définition 2.24. Un *schéma affine* est un espace annelé qui est isomorphe à $\operatorname{spec} A$ muni de son faisceau structural pour un certain anneau A.

Remarque 2.25. On a vu qu'un morphisme d'anneaux $\widetilde{f}\colon A \to B$ induit une fonction continue $f\colon Y = \operatorname{spec}(B) \to X = \operatorname{spec}(A)$. On peut en faire un morphisme d'espaces annelés en définissant $f^\sharp$ de la manière suivante. Si U est un ouvert de X, à chaque élément $s \in \mathcal{O}_X(U) \subset \prod_{\mathfrak{p}\in U} A_\mathfrak{p}$, on associe $f^\sharp(s) \in f_\star\mathcal{O}_Y(U) \subset \prod_{\mathfrak{q}\in f^{-1}(U)} B_q$ défini par $f^\sharp(s)_\mathfrak{q} = \widetilde{f}(s_{f(\mathfrak{q})})$ où on étend le morphisme $\widetilde{f}\colon A \to B$ au localisé $\widetilde{f}\colon A_{f(\mathfrak{q})} \to B_\mathfrak{q}$ de manière naturelle. Ceci définit bien un morphisme $f^\sharp$. Vérifions à présent qu'il est local. En chaque point $\mathfrak{q} \in \operatorname{spec}(A)$ d'image $\mathfrak{p} = f(\mathfrak{q}) = \widetilde{f}^{-1}(\mathfrak{q})$, le morphisme induit $f_\mathfrak{q}^\sharp\colon A_\mathfrak{p} \to B_\mathfrak{q}$ est l'extension naturelle de $\widetilde{f}$, et elle envoie $\mathfrak{p}$ sur $\widetilde{f}(\mathfrak{p}) \subset \mathfrak{q}$, donc elle envoie $\mathfrak{p}A_\mathfrak{p}$ dans $\mathfrak{q}B_\mathfrak{q}$.

On peut montrer que chaque morphisme d'espaces annelés de $\operatorname{spec}(B)$ vers $\operatorname{spec}(A)$ (munis des faisceaux structuraux) provient d'un morphisme d'anneaux de A vers B de cette manière. Il y a donc une bijection entre les deux types de morphismes, qui d'ailleurs respecte la composition. Ceci explique pourquoi la définition de morphisme d'espaces annelés impose que les morphismes sur les tiges soient locaux.

On est maintenant en mesure de définir la notion de schéma :

Définition 2.26. Un *schéma* est un espace annelé $(X, \mathcal{O}_X)$ admettant un recouvrement ouvert U_i tel que chaque U_i muni de la restriction de $\mathcal{O}_X$ soit un schéma affine. On notera souvent $H^0(X, \mathcal{O}_X)$ l'anneau des sections globales $\mathcal{O}_X(X)$.

Un *morphisme de schémas* est alors un morphisme entre les espaces annelés correspondants.

Les schémas affines fournissent évidemment des exemples de schémas. Une autre classe de schémas sera définie dans la section suivante.

Remarque 2.27. Un morphisme de schémas $f : X \to Y$ induit des morphismes locaux entre les anneaux locaux $\mathcal{O}_{X,x}$ et $\mathcal{O}_{Y,y}$ pour chaque $x \in X$ et $y = f(x)$ et donc un morphisme entre les corps résiduels $k(x) \hookrightarrow k(y)$.

Définition 2.28. On dit qu'un schéma X est réduit si pour tout x dans X, $\mathcal{O}_{X,x}$ est réduit (c'est à dire qu'il n'admet pas d'élément nilpotent non nul).

Proposition 2.29. *Soit X un schéma. Alors X est* réduit *si et seulement si pour tout U ouvert de X, $\mathcal{O}_X(U)$ est réduit.*

Démonstration. Supposons que pour tout U ouvert de X, $\mathcal{O}_X(U)$ est réduit. Soit $x \in X$; alors x est inclus dans un ouvert affine $U = \operatorname{spec} A$ avec A réduit. Si $\mathfrak{p}$ est l'idéal premier de A correspondant à x, il faut montrer que $\mathcal{O}_{X,x} = A_{\mathfrak{p}}$ est réduit. Or, si f/g est nilpotent, il existe $h \notin \mathfrak{p}$ et $m \geq 1$ tels que $hf^m = 0$, ainsi on a $(hf)^m = 0$ et donc $hf = 0$ car A est réduit. Ainsi, f/g est nulle dans $A_{\mathfrak{p}}$.

Réciproquement, supposons X réduit. Soit U un ouvert de X et $f \in \mathcal{O}_X(U)$ nilpotent. Alors pour tout x dans X, l'image f_x de f dans la tige $\mathcal{O}_{X,x}$ est nilpotente donc nulle. Comme $\mathcal{O}_X$ est un faisceau, f est nulle. □

Remarque 2.30. Si A est un anneau, on sait que le quotient A_{red} de A par son nilradical est réduit. On a une surjection canonique $A \twoheadrightarrow A_{\mathrm{red}}$ qui donne un homéomorphisme sur son image $\operatorname{spec} A_{\mathrm{red}} \to \operatorname{spec} A$. Les schémas $\operatorname{spec} A_{\mathrm{red}}$ et $\operatorname{spec} A$ ont le même espace topologique sous-jacent. On peut généraliser cette construction : pour tout schéma X, on construit un schéma X_{red}, équipé d'un homéomorphisme sur son image $X_{\mathrm{red}} \to X$, qui possède le même espace topologique sous-jacent que X. On prend comme faisceau le quotient de $\mathcal{O}_X$ par $\mathcal{N}$ où $\mathcal{N}$ est le faisceau défini par $U \mapsto \mathcal{N}(U)$ où $\mathcal{N}(U)$ est l'ensemble des $s \in \mathcal{O}_X(U)$ telle que s_x est nilpotent pour tout $x \in U$.

Définition 2.31. On dit qu'un schéma X est *intègre* s'il est irréductible et réduit.

On admettra les deux propositions suivantes (pour la démonstration, on pourra se reporter à [Har10]).

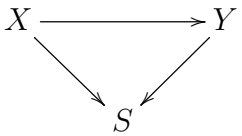
Proposition 2.32. *Soit $X = \operatorname{spec} A$ un schéma affine, alors X est intègre si et seulement si A est intègre.*

Si X est un schéma quelconque non vide, X est intègre si et seulement si $\mathcal{O}_X(U)$ est intègre pour tout ouvert U de X non vide.

Proposition 2.33. *Soit X un schéma irréductible. Alors l'espace topologique X contient un unique point générique η. Si de plus X est intègre, l'anneau $\mathcal{O}_{X,\eta}$ est un corps, appelé corps des fonctions de X, qui est le corps des fractions de $\mathcal{O}_X(U)$ pour tout ouvert affine non vide U de X.*

Points d'un schéma

Définition 2.34. Soit S un schéma fixé. Un *S-schéma* (ou schéma sur S) est un schéma X, muni d'un morphisme $X \to S$. Un morphisme de S-schémas est un morphisme $X \to Y$ qui est compatible avec les morphismes $X \to S$ et $Y \to S$, c'est à dire qu'on a le diagramme commutatif suivant :



Quand X, Y sont des S-schémas, on notera $\hom_S(X, Y)$ tous les morphismes de S-schémas entre X et Y.

Remarque 2.35. Quand $S = \mathrm{spec}(A)$ est affine, on abrègera souvent « $\mathrm{spec}(A)$-schéma » en « A-schéma ». Si X est un A-schéma, le morphisme $A = H^0(\mathrm{spec}(A), \mathcal{O}_{\mathrm{spec}(A)}) \to H^0(X, \mathcal{O}_X)$ se prolonge en des morphismes $A \to \mathcal{O}_X(U)$ pour tous ouverts U de X, ce qui fait de $\mathcal{O}_X$ un faisceau de A-algèbres.

Réciproquement, soit X un schéma tel que $\mathcal{O}_X$ soit un faisceau de A-algèbres. On a alors, pour chaque ouvert $U \subset X$ et chaque point $x \in X$, des morphismes $\phi_U \colon A \to \mathcal{O}_X(U)$ et $\phi_x \colon A \to \mathcal{O}_{X,x}$. Posons $f(x) = \phi_x^{-1}(\mathcal{M}_x)$: c'est un idéal premier de A, donc f définit une application de X dans $\mathrm{spec}(A)$. Notons que $f(x)$ est l'ensemble des éléments de A dont l'image dans $\mathcal{O}_{X,x}$ n'est pas inversible. Si a est un élément de A, alors $f^{-1}(D(a))$ est l'ensemble des $x \in X$ tels que $\phi_x(a)$ est inversible. C'est donc l'ensemble des $x \in X$ tels qu'il existe un ouvert $U \subset X$ contenant x et pour lequel $\phi_U(a)$ est inversible. L'image réciproque $f^{-1}(D(a))$ est alors l'union des tels ouverts U, donc est ouverte. On a donc montré la continuité de f, et même plus : $f^{-1}(D(a))$ est recouvert par des ouverts U_i comme précédemment. On a donc, pour chaque i, un $b_i \in U_i$ qui est l'inverse de $\phi_{U_i}(a)$. La restriction de b_i à $U_i \cap U_j$ est l'inverse de $\phi_{U_i \cap U_j}(a)$, donc elle coincide avec la restriction de b_j à cet ouvert. Ainsi on a $b \in U$ dont la restriction à chaque U_i est b_i ; et la restriction de $b\phi_U(a)$ à chaque U_i est 1, donc c'est 1. Ainsi $\phi_U(a)$ est inversible, donc ϕ_U s'étend en un morphisme $f^\sharp_{D(a)} \colon A_a \to \mathcal{O}_X(f^{-1}(D(a)))$. On construit donc un morphisme de faisceaux $f^\sharp$, qui avec f donne un morphisme de schémas $X \to \mathrm{spec}(A)$.

Définition 2.36. Soit k un corps. Un *schéma de type fini* sur k est un k-schéma qui admet un recouvrement *fini* par des ouverts affines $U_i = \mathrm{spec}\, A_i$, avec A_i des k-algèbres de type fini.

Définition 2.37. Le *degré* d'un point fermé x d'un schéma X de type fini sur k est le degré de l'extension $k(x)/k$. C'est un nombre fini d'après 1.10.

Proposition 2.38. *Soient X un schéma de type fini sur un corps fini k et d un entier naturel. Alors le nombre de points de x de degré au plus d est fini, majoré par s^d avec s un nombre ne dépendant que de X.*

Démonstration. Comme X est recouvert par un nombre fini d'ouverts affines, on peut supposer que X lui-même est un $\mathrm{spec}\, A$ avec A une k-algèbre de type fini. Le résultat découle alors de 1.11. □

Définition 2.39. Soient A un anneau et X un A-schéma. Soit B une A-algèbre. Un *B-point* de X est un élément de $\hom_{\mathrm{spec}\, A}(\mathrm{spec}\, B, X)$. On notera alors $X(B)$ l'ensemble des B-points de X (A étant sous-entendu).

Exemple 2.40.

1. Le cas de k un corps et L une extension de corps de k sera traité en détail dans la partie 3.
2. Soit $X = \mathbb{A}^1_{\mathbb{R}} = \mathrm{spec}(\mathbb{R}[T])$. Il y a deux $\mathbb{C}$-points de X dont l'image est $x = (T^2+1)$. En effet, le corps résiduel de x est $\mathbb{R}[T]/(T^2+1)$, et les éléments de $\hom_{\mathrm{spec}\, \mathbb{R}}(\mathrm{spec}\, \mathbb{C}, X)$ qui envoient le point de $\mathrm{spec}\, \mathbb{C}$ sur x sont uniquement déterminés par les morphismes de corps résiduels $\hom_{\mathbb{R}-\mathrm{alg}}(\mathbb{R}[T]/(T^2+1), \mathbb{C})$. Il y en a deux, ce qui donne bien deux points. On peut voir ces deux points comme i et $-i$. On a bien tenu compte ici des multiplicités, car dans l'espace topologique $\mathbb{A}^1_{\mathbb{R}}$ on ne peut pas distinguer i et $-i$.

2.4 L'exemple des Proj

Nous avons vu comment donner une structure de schéma affine à $\operatorname{spec} A$ pour tout anneau A. On va maintenant définir un schéma $\operatorname{Proj} B$ pour tout anneau gradué B, qui pourra être vu comme l'analogue des variétés projectives.

Soit $B = \bigoplus_{d\geq 0} B_d$ un *anneau gradué*. Les éléments de B_d sont appelés les éléments homogènes de degré d. Pour mieux visualiser les choses, on pourra considérer toute la suite en prenant comme référence $B = A[x_0, \dots, x_n]$ avec A un anneau, B_d étant alors les polynômes homogènes de degré d. Un idéal I de B est dit *homogène* s'il est engendré par des éléments homogènes. C'est équivalent à demander que $I = \oplus_{d\geq 0}(I \cap B_d)$, et dans ce cas (B/I) est gradué, et on a $(B/I)_d = B_d/(B_d \cap I)$. On note $B_+ = \oplus_{d>0} B_d$. On pourra remarquer que le radical d'un idéal homogène est homogène.

Définition 2.41. On note $\operatorname{Proj} B$ l'ensemble des idéaux premiers homogènes de B qui ne contiennent pas B_+.

On va munir $\operatorname{Proj} B$ d'une structure de schéma. Dans le cas où $B = k[x_0, \dots, x_n]$, l'espace $\mathbb{P}^n_k$ correspondra alors à $\operatorname{Proj}(k[x_0, \dots, x_n])$. On comprend assez bien pourquoi il faut travailler avec des polynômes homogènes : dans l'espace projectif $(x_0, \dots, x_n) = (\lambda x_0, \dots, \lambda x_n)$ pour tout $\lambda \in k^*$. Ensuite, imposer la condition de ne pas contenir B_+ vient du fait que $(0, \dots, 0)$ n'appartient pas à l'espace projectif.

La construction du schéma $\operatorname{Proj} B$ est très analogue à celle de $\operatorname{spec} A$. On définit la topologie en prenant comme fermés les ensembles $V_+(I)$ pour I un idéal homogène de B, où $V_+(I)$ est l'ensemble des $\mathfrak{p} \in \operatorname{Proj} B$ contenant I. On a les mêmes propriétés que dans le cas des spectres :

$$V_+(B_+) = \emptyset \qquad V_+(I) \cup V_+(J) = V_+(IJ) = V_+(I \cap J)$$
$$V_+(\{0\}) = \operatorname{Proj} B \qquad \bigcap_r V_+(I_r) = V_+\left(\sum I_r\right)$$

On utilise ici le fait que si I est un idéal homogène ne contenant pas B_+, I est premier si et seulement si pour tous a, b *homogènes*, on a $ab \in I \Rightarrow a \in I$ ou $b \in I$. Les *ouverts principaux* de $\operatorname{Proj} B$ sont les $D_+(f) = \{\mathfrak{p} \in \operatorname{Proj} B \mid f \notin \mathfrak{p}\}$ pour f un élément *homogène* de B. Les $D_+(f)$ forment une base de la topologie.

Remarque 2.42. Si on fait l'hypothèse que B est engendrée en tant que B_0-algèbre par les éléments homogènes de degré 1 (c'est par exemple le cas de $A[x_0, \dots, x_n]$ l'anneau gradué des polynômes homogènes à coefficients dans un anneau A), alors les $D_+(f)$ avec f *homogène de degré 1* recouvrent $\operatorname{Proj} B$. En effet, l'idéal B engendré par les f de degré 1 est B_+ tout entier. Ainsi, soit $\mathfrak{p} \in \operatorname{Proj} B$, alors $B_+ \not\subseteq \mathfrak{p}$, ainsi $\sum_{\deg f=1}(f) \not\subseteq \mathfrak{p}$, donc il existe f de degré 1 tel que $f \notin \mathfrak{p}$, ce qui signifie que $\mathfrak{p} \in D_+(f)$.

On construit maintenant le faisceau structural $\mathcal{O}_X$ de $X = \operatorname{Proj} B$, avec les mêmes conditions que dans le cas affine. Il faut les deux propriétés suivantes :

(i) La tige $\mathcal{O}_{X,\mathfrak{p}}$ en $\mathfrak{p}$ est isomorphe à $B_{(\mathfrak{p})}$, où $B_{(\mathfrak{p})}$ est l'ensemble des éléments homogènes de degré zéro dans le localisé de B par rapport aux éléments homogènes non dans $\mathfrak{p}$. De manière plus explicite, ce sont les éléments de la forme a/b avec a et b homogènes de même degré et $b \notin \mathfrak{p}$.

(ii) L'anneau des sections $\mathcal{O}_X(D_+(f))$ sur $D_+(f)$ est isomorphe à $B_{(f)}$ qui est le sous-anneau de B_f constitué des éléments homogènes de degré 0, où l'on a gradué B_f par $\deg(x/f^k) = \deg x - k \deg f$. Ainsi, $B_{(f)}$ peut être vu comme l'ensemble des a/f^N avec a homogène de degré $N \deg f$.

Pour pouvoir définir le faisceau structural de $X = \operatorname{Proj} B$, il nous faut d'abord regarder les propriétés de la localisation sur $\operatorname{Proj} B$.

Lemme 2.43. *Soient B un anneau gradué et f un élément homogène de degré > 0. Alors :*

(a) L'application

$$u : \mathfrak{p} \mapsto (\mathfrak{p}B_f) \cap B_{(f)}$$

est une bijection de $D_+(f)$ sur $\operatorname{spec}(B_{(f)})$. Un idéal homogène I de B est inclus dans $\mathfrak{p}$ si et seulement si $u(I)$ (que l'on définit comme $u(\mathfrak{p})$ en remplaçant $\mathfrak{p}$ par I) est inclus dans $u(\mathfrak{p})$. On a en particulier $u(V_+(I)) = V_+(u(I))$.

(b) Si g est un élément homogène de degré > 0 de B avec $D_+(g) \subset D_+(f)$, alors on a un homomorphisme canonique d'anneaux $B_{(f)} \to B_{(g)}$, qui est un isomorphisme si $D_+(g) = D_+(f)$.

Démonstration. a) Montrons tout d'abord que u est bien définie. Soit $p \in D_+(f)$, alors $\mathfrak{p}B_f$ est un idéal premier de B_f, donc son image réciproque $\mathfrak{p}B_f \cap B_{(f)}$ par l'inclusion $B_{(f)} \hookrightarrow B_f$ est un idéal premier de $B_{(f)}$ (on rappelle que $\mathfrak{p}B_f \cap B_{(f)}$ n'est que l'ensemble des éléments de $\mathfrak{p}B_f$ de degré zéro). Dans la suite, on note $\rho : B \to B_f$ le morphisme de localisation, qui est compatible avec les graduations de B et de B_f.

Montrons la surjectivité de u. Soit r le degré de f et $\mathcal{Q}$ un élément de $\operatorname{spec} B_{(f)}$. $\mathcal{Q}B_f$ est alors un idéal homogène de B_f (car les éléments de $\mathcal{Q}$ sont homogènes de degré 0). Son radical $\sqrt{\mathcal{Q}B_f}$ l'est donc aussi, et $\mathfrak{p} := \rho^{-1}(\sqrt{\mathcal{Q}B_f})$ est un idéal homogène de B qui ne contient pas f. En effet, cela vient du fait que $1 \notin \mathcal{Q}$, si f appartient à $\sqrt{\mathcal{Q}B_f}$, alors il existe $N > 0, k \geq 0, l \geq 1, a, b \in B$ avec $\deg a = N \deg f > 0$, tels que $a/f^N \in \mathcal{Q}$ et

$$f^l = \frac{a}{f^N}\frac{b}{f^k} \Leftrightarrow f^{N+k+l} = ab$$

comme $N + k + l > 0$, ceci implique que ab est inversible dans B_f donc en particulier a est inversible dans B_f, ce qui impose que a est une puissance de f car $\deg a > 0$, et comme $\deg a = N \deg f$, on a $a = f^N$ et donc $a/f^N = 1 \in \mathcal{Q}$ ce qui est absurde.

On remarque aussi que les éléments homogènes de degré zéro de $\mathcal{Q}B_f$ sont les éléments de $\mathcal{Q}$. Le point important est de montrer que $\sqrt{\mathcal{Q}B_f}$ est premier. Pour cela, on prend a, b deux éléments homogènes de B_f tels que $ab \in \mathcal{Q}B_f$, alors $(a^r f^{-\deg a})(b^r f^{-\deg b})$ est homogène de degré zéro et appartient à $\mathcal{Q}B_f$, donc il appartient à $\mathcal{Q}$. Comme $\mathcal{Q}$ est premier, on a par exemple $a^r f^{-\deg a} \in \mathcal{Q}$ et donc $a^r \in \mathcal{Q}B_f$ ce qui est ce qu'on voulait. Ainsi, $\mathfrak{p}$ est premier car c'est l'image réciproque de $\sqrt{\mathcal{Q}B_f}$ par ρ. De plus, $u(\mathfrak{p}) = \sqrt{\mathcal{Q}B_f} \cap B_{(f)}$. Or, tout élément x homogène de degré zéro dans $\sqrt{\mathcal{Q}B_f}$ vérifie : pour un certain $k > 0$, $x^k \in \mathcal{Q}B_f$ et x^k est homogène de degré zéro, d'où $x^k \in \mathcal{Q}$ ce qui veut dire $x \in \mathcal{Q}$, car $\mathcal{Q}$ est premier. Finalement, $u(\mathfrak{p}) = \mathcal{Q}$ et u est bien surjective.

Pour montrer l'injectivité, on peut remarquer qu'il suffit de montrer la seconde assertion de a), en effet si pour I, on prend un idéal premier $\mathfrak{q}$, alors par symétrie des rôles de $\mathfrak{p}$ et $\mathfrak{q}$, on aurait $u(\mathfrak{p}) = u(\mathfrak{q}) \Leftrightarrow \mathfrak{p} = \mathfrak{q}$.

Pour montrer la seconde assertion de a), on remarque que si $\mathfrak{p} \in D_+(f)$ et I est un idéal homogène de B avec $u(I) \subset u(\mathfrak{p})$, alors pour tout x homogène dans I, on a $(x^r/f^{\deg x}) \in u(I)$ d'où $(x^r/f^{\deg x}) \in u(\mathfrak{p}) \subset \mathfrak{p}B_f$, ceci implique que $x^r \in (\mathfrak{p}B_f \cap B) = \mathfrak{p}$. Et finalement, $x \in \mathfrak{p}$ car $\mathfrak{p}$ est premier.

b) Si $D_+(g) \subset D_+(f)$, on peut écrire $g^n = fb$ avec $b \in B$, et on peut supposer b homogène quitte à le remplacer par l'une des ses composantes homogènes. On en déduit un homomorphisme canonique $B_{(f)} \to B_{(g)}$ obtenu en envoyant a/f^N sur ab^N/g^{nN}. Si $D_+(f) = D_+(g)$ c'est un isomorphisme. Il suffit d'échanger les rôles de f et g pour le voir. □

Théorème 2.44. *Soit $X = \operatorname{Proj} B$. Pour f homogène de degré > 0, on pose $\mathcal{O}_X(D_+(f)) = B_{(f)}$ et pour $D_+(g) \subset D_+(f)$, on définit des morphismes de restriction $\mathcal{O}_X(D_+(f)) \to \mathcal{O}_X(D_+(g))$ via le lemme 2.43, b). Alors*

(a) La condition ci-dessus définit un faisceau $\mathcal{O}_X$ sur X, tel que pour tout $f \in B_+$, l'espace annelé $D_+(f)$ (muni de la restriction de $\mathcal{O}_X$) soit isomorphe à $\operatorname{spec} B_{(f)}$. En particulier, $\operatorname{Proj} B$ est un schéma.

(b) La tige $\mathcal{O}_{X,\mathfrak{p}}$ est isomorphe à $B_{(\mathfrak{p})}$ pour tout $\mathfrak{p}$ de $\operatorname{Proj} B$.

Démonstration. a) Remarquons d'abord que $\operatorname{Proj} B \subset \operatorname{spec} B$ et que la topologie sur $\operatorname{Proj} B$ est celle induite par $\operatorname{spec} B$. En effet, si $g \in B$ s'écrit $g = g_0 + \ldots + g_d$ avec $g_i \in B_i$, alors $V(g) \cap \operatorname{Proj} B = \bigcap_{i=1}^d V_+(g_i)$ donc $D(g) \cap \operatorname{Proj} B = \bigcup_{i=1}^d D_+(g_i)$ d'où le résultat vu que les $D(g)$ dorment une base d'ouverts de $\operatorname{spec} B$.

On considère alors pour f homogène de degré > 0, l'application $u : D_+(f) \to \operatorname{spec} B_{(f)}$ définie au lemme 2.43. D'après ce qui précède, cette application est continue vu que c'est la restriction à $D_+(f) \subset D(f) \simeq \operatorname{spec} B_f$ de l'application $\operatorname{spec} B_f \to \operatorname{spec} B_{(f)}$ associée à l'inclusion $B_{(f)} \hookrightarrow B_f$. D'autre part, u est bijective et fermée d'après le lemme 2.43 a) car les $V_+(I)$ pour I idéal homogène forme une base des fermés de la topologie, l'application u est donc bicontinue. Enfin, comme u est compatible aux restrictions, les conditions de recollement pour $\mathcal{O}_X$ sont bien vérifiées sur l'ouvert $D_+(f)$ car elles le sont sur $\operatorname{spec} B_{(f)}$ d'après le lemme 2.43. Comme les $D_+(f)$ forment une base de la topologie de X (ils sont stables par intersection finie), on a bien un faisceau $\mathcal{O}_X$ sur X et par définition, la restriction de $\mathcal{O}_X$ à $D_+(f)$ fait de $D_+(f)$ un espace annelé isomorphe à $\operatorname{spec} B_{(f)}$.

b) La tige $\mathcal{O}_{X,\mathfrak{p}}$ est la limite pour $f \notin \mathfrak{p}$ des $\mathcal{O}_X(D_+(f)) = B_{(f)}$. Ainsi, cette tige est $B_{(p)}$ par le même argument que dans la proposition 2.17. □

Remarque 2.45.
1. On n'a plus du tout $\mathcal{O}_X(X) = B$ pour $X = \operatorname{Proj} B$. Par exemple, si $X = \mathbb{P}^n_k = \operatorname{Proj} k[x_0, \ldots, x_n]$, alors on a un recouvrement de X par les ouverts principaux $D_+(x_i) = \operatorname{spec} k[x_0/x_i, \ldots, x_n/x_i]$. On voit donc que $\mathcal{O}_X(\mathbb{P}^n_k) = k$.
2. On aurait aussi pu définir le faisceau $\mathcal{O}_X$ sur $X = \operatorname{Proj} B$ en prenant pour $\mathcal{O}_X(U)$ les fonctions $s : U \to \amalg_{\mathfrak{p} \in U} B_{(\mathfrak{p})}$ vérifiant : pour tout p de U, $s(\mathfrak{p}) \in B_{(\mathfrak{p})}$, et au voisinage de tout $\mathfrak{p}$ de U, s provient d'un élément de $B_{(f)}$ pour un certain f.

2.5 Sous-schémas

Contrairement à la géométrie différentielle, le cadre des schémas de la géométrie algébrique ne fournit pas de notion naturelle de sous-schémas. On ne pourra définir que les notions assez distinctes de sous-schéma ouvert et fermé, qui correspondent en quelque sorte aux deux points de la proposition 1.7.

Définition 2.46. Soit X un schéma. Un *sous-schéma ouvert* de X est un ouvert U de X muni de la restriction du faisceau de $\mathcal{O}_X$ à U.

Une *immersion ouverte* est un morphisme de schémas $X \to Y$ qui induit un isomorphisme entre X et un sous-schéma ouvert de Y.

Un sous-schéma ouvert U de X est un schéma. Pour vérifier ceci, il faut trouver un recouvrement affine de U. On a un recouvrement de X par des $\operatorname{spec}(A_i)$. Chaque $U \cap \operatorname{spec}(A_i)$ est un ouvert de $\operatorname{spec}(A_i)$, donc s'écrit comme l'union d'ouverts principaux $D(f_{ij})$. Il ne reste plus qu'à remarquer que ces ouverts principaux sont affines, ce qui vient de la construction des faisceaux structuraux qui donne $D(f_{ij}) \simeq \operatorname{spec}((A_i)_{f_{ij}})$.

Exemple 2.47. Si A est un anneau et $f \in A$, le morphisme de schémas $\operatorname{spec}(A_f) \to \operatorname{spec}(A)$ induit par $A \to A_f$ est une immersion ouverte sur $D(f)$.

Pour un sous-schéma fermé, c'est plus compliqué : il n'y pas de structure canonique de faisceau sur un fermé d'un schéma. On commence donc par définir les immersions fermées :

Définition 2.48. Une *immersion fermée* est un morphisme de schémas $f\colon X \to Y$ tel que :

1. L'application continue induite par f est un homéomorphisme de X sur un fermé de Y.
2. Le morphisme de faisceaux $f^\sharp\colon \mathcal{O}_Y \to f_\star \mathcal{O}_X$ associé à f est surjectif sur les tiges.

Un *sous-schéma* fermé d'un schéma Y est une classe d'équivalence d'immersions fermées $i\colon X \to Y$ où l'on identifie deux morphismes (X, i) et (X', i') lorsqu'il existe un isomorphisme $\phi\colon X \to X'$ tel que $i' \circ \phi = i$.

Exemple 2.49.

1. Si A est un anneau et I est un idéal de A, le morphisme d'anneaux $A \to A/I$ induit un morphisme de schémas $f\colon \operatorname{spec}(A/I) \to \operatorname{spec}(A)$. Comme on l'a vu, f induit un homéomorphisme entre $\operatorname{spec}(A/I)$ et le fermé $V(I)$. De plus, pour $\mathfrak{p} \in V(I)$, le morphisme $f^\sharp_{\mathfrak{p}}\colon A_{\mathfrak{p}} \to (A/I)/(\mathfrak{p}/I)$ est surjectif. Ceci fait de $\operatorname{spec}(A/I)$ un sous-schéma fermé de $\operatorname{spec}(A)$. En particulier, en reprenant la remarque 2.30 on voit qu'on a en fait une immersion fermée $\operatorname{spec}(A_{\mathrm{red}}) \to \operatorname{spec} A$ et plus généralement une immersion fermée $X_{\mathrm{red}} \to X$ qui fait de X_{red} un sous-schéma fermé de X.
   Remarquons que les sous-schémas fermés $\operatorname{spec}(A/I)$ et $\operatorname{spec}(A/\sqrt{I})$ sont a priori différents, mais on le même espace topologique sous-jacent $V(I) = V(\sqrt{I})$.
2. De même qu'avec les spectres, si B est un anneau gradué et I est un idéal homogène de P, alors pour le morphisme canonique $\widetilde{f}\colon B \to B/I$ d'anneaux gradués, on peut définir une immersion fermée de $\operatorname{Proj}(B/I)$ vers $\operatorname{Proj}(B)$, dont l'application continue $f\colon \operatorname{Proj}(B/I) \to \operatorname{Proj}(B)$ est donnée par $f(\mathfrak{p}) = \widetilde{f}^{-1}(\mathfrak{p})$. Cette immersion a pour image le fermé $V_+(I)$.

2.6 L'espace projectif

On travaille sur un corps k. Soit B l'anneau gradué $k[x_0, \ldots, x_n]$.

Définition 2.50. L'*espace projectif* de dimension n sur k est $\mathbb{P}^n_k := \operatorname{Proj}(B)$.

De même que l'espace affine $\mathbb{A}^n_k$ est un analogue de k^n, la proposition suivante montre que l'espace projectif est un analogue de $(k^{n+1} \setminus \{0\})/k^\times$.

Proposition 2.51. *Les points fermés de $\mathbb{P}^n_k$ sont en bijection avec $\bar{k}^{n+1} \setminus \{0\}$ modulo l'action des groupes $\operatorname{Aut}_k \bar{k}$ et $\bar{k}^\times$.*

Démonstration. Soit P un point fermé de $\mathbb{P}^n_k$, notons $\mathfrak{m}$ l'idéal homogène de B associé. Quitte à permuter des indices, on peut supposer que $P \in D_+(x_0)$. En gardant la notation du lemme 2.43, l'idéal $u(\mathfrak{m})$ de $A = k[x_1/x_0, \dots, x_n/x_0]$ est un point fermé de $\operatorname{spec}(A)$. Il existe donc $a = (1, a_1, \dots, a_n) \in \bar{k}^{n+1}$ tel que $u(\mathfrak{m})$ est l'ensemble des $f \in A$ qui s'annulent en a. Soit $\mathfrak{m}' \in \operatorname{Proj}(B)$ l'idéal de B engendré par les polynômes homogènes qui s'annulent sur l'orbite de a sous l'action des groupes $\operatorname{Aut}_k \bar{k}$ et $\bar{k}^\times$. Alors $\mathfrak{m}' \in D_+(x_0)$ et $u(\mathfrak{m}) = u(\mathfrak{m}')$, donc comme u est une bijection, $\mathfrak{m} = \mathfrak{m}'$. □

Le *degré* d'un point $P \in \mathbb{P}^n_k$ est le degré de l'extension $k(P)/k$. Comme le corps résiduel est un objet local, le degré d'un point appartenant à un ouvert affine peut se calculer dans cet ouvert affine. Ainsi, si P est un point correspondant à un $(n+1)$-uplet $a = (a_0, \dots, a_n)$, alors $\deg P = [k(a) : k]$.

Définition 2.52. Une *variété projective* sur un corps k est un schéma de la forme $\operatorname{Proj}(B/I)$ avec I un idéal homogène de $B = k[x_0, \dots, x_n]$. C'est en particulier un sous-schéma fermé de $\mathbb{P}^n_k$.

Une *variété quasi-projective* est un sous-schéma ouvert d'une variété projective.

2.7 Dimension

Théorème 2.53. *Soit X un schéma intègre de type fini sur k dont on note K le corps des fonctions. Alors :*

1. *La dimension de X est finie et* $\dim X = \operatorname{degtr}_k(K)$
2. *Pour tout ouvert non vide U de X, on a* $\dim X = \dim U$
3. *Pour tout point fermé $P \in X$, on a* $\dim X = \dim \mathcal{O}_{X,P}$

Démonstration. Chaque ouvert affine de X a le même corps de fonctions que X d'après le théorème 2.33, donc a pour dimension $\operatorname{degtr}_k(K)$ d'après le théorème 1.29. Le premier point découle alors de la proposition 1.4.

Le deuxième point découle du premier par le théorème 2.33.

Pour le troisième point, le deuxième permet de se ramener au cas où X est affine, cas qui est évident. □

Corollaire 2.54. *Soit X un schéma de type fini sur k, pas forcément intègre, dont toutes les composantes irréductibles ont la même dimension. Alors pour tout ouvert non vide de U, on a* $\dim(U) = \dim(X)$.

Démonstration. Les composantes irréductibles de X recouvrent X, donc il existe une composante Y qui intersecte U. Munissons Y de sa structure de sous-schéma fermé réduit de X. Comme Y est irréductible réduit de type fini, le théorème 2.53 assure que $\dim(X) = \dim(Y) = \dim(Y \cap U) \leq \dim(X)$, donc $\dim(X) = \dim(U)$. □

Ceci va nous permettre de caractériser les hypersurfaces projectives.

Définition 2.55. Une *hypersurface* de l'espace projectif $\mathbb{P}^n_k$ est une variété en dimension n dont toutes les composantes irréductibles sont de dimension $n-1$.

Proposition 2.56. *Les hypersurfaces intègres sont données par les* $\operatorname{Proj}(B/(f))$ *où $f \in B := k[x_0, \dots, x_n]$ est un polynôme homogène non constant.*

Démonstration. Soit $\mathrm{Proj}(B/I)$ une hypersurface intègre, avec I un idéal premier homogène. Prenons $x \in B \setminus I$ homogène et irréductible non constant (x existe car I ne contient pas B_+), notons $U = D_+(x)$. Alors si $U \cap V_+(I)$ est non vide, toutes ses composantes irréductibles sont de dimension $n-1$ d'après le corollaire 2.54. D'après 1.33, l'idéal $u(I)$ de $B_{(x)}$ (en gardant les notations de 2.43) est engendré par un élément f/x^k, où $f \in B$ est un polynôme homogène qui n'est pas multiple de x. Soit $g \in I$ homogène de degré d. On peut écrire

$$\frac{g}{x^d} = \frac{a}{x^l}\frac{f}{x^k}$$

avec a homogène qui n'est pas multiple de x. Comme af n'est pas multiple de x, $k+l-d$ est négatif et donc g est dans l'idéal (f). Maintenant on sait qu'il existe $h \in I$ homogène et un entier l tels que $f/x^k = h/x^l$. Comme f n'est pas divisible par x, $l-k$ est positif et $fx^{l-k} = h \in I$. Or I est premier, donc $f \in I$. Ceci montre que $I{=}(f)$. □

2.8 Régularité d'une hypersurface, espace tangent

On part d'abord d'une hypersurface affine. Soient $A = k[x_1, \ldots, x_n]$, f un élément de A non nul et x un point fermé de $\mathrm{spec}(A/(f))$. Soit y le point fermé de $\mathbb{A}^n_k$ correspondant à x, d'idéal maximal $\mathfrak{m}$.

Notons E le $k(y)$-espace vectoriel $k(y)^n$ et E^* son dual. Soit $\mathcal{D}$ l'application de A dans E^* définie par

$$\mathcal{D}(P)(t_1, \ldots, t_n) = \sum_{i=1}^{n} \frac{\partial P}{\partial x_i}(y) t_i$$

« Classiquement », l'espace tangent en x de $\mathrm{spec}(A/(f))$ se définit comme $\ker \mathcal{D}(f)$. L'objectif sera de traduire ceci de manière plus « schématique ».

Notons $M = \mathfrak{m}/(f)$ l'idéal maximal de $A/(f)$ correspondant au point x. On a une suite exacte de $k(y)$-espaces vectoriels

$$0 \to (f)/((f) \cap \mathfrak{m}^2) \to \mathfrak{m}/\mathfrak{m}^2 \to M/M^2 \to 0$$

On a vu à la section 1.5 que la restriction de $\mathcal{D}$ à $\mathfrak{m}$ induit un isomorphisme de $k(y)$-espaces vectoriels entre $\mathfrak{m}/\mathfrak{m}^2$ et E^*. Appliquons alors $\mathcal{D}$ aux deux premiers termes : on obtient la suite exacte

$$0 \to \mathcal{D}((f)) \to E^* \to M/M^2 \to 0$$

Comme on travaille avec des espaces vectoriels, le passage au dual préserve l'exactitude (le noyau du dual d'une flèche est l'ensemble des formes linéaires qui s'annulent sur l'image de la flèche, l'image du dual d'une flèche est l'ensemble des formes linéaires qui s'annulent sur le noyau de la flèche). On obtient la suite exacte

$$0 \leftarrow \mathcal{D}((f))^* \leftarrow E \leftarrow (M/M^2)^* \leftarrow 0$$

Comme précisé plus haut, le noyau de la flèche de gauche est l'ensemble des formes linéaires sur E^* qui s'annulent sur $\mathcal{D}((f))$ (vu comme sous-espace de E^*), c'est-à-dire les éléments de E qui annulent les éléments de $\mathcal{D}((f))$ (par l'isomorphisme naturel $(E^*)^* \simeq E$). Ceci donne une injection de $(M/M^2)^*$ dans E d'image $\ker \mathcal{D}(f)$ (puisque $\mathcal{D}((f))$ est le $k(y)$-espace engendré par $\mathcal{D}(f)$) : ainsi $(M/M^2)^*$ se réalise comme l'espace tangent. Il ne reste alors plus qu'une étape vers une caractérisation véritablement intrinsèque, qui prend la forme du lemme suivant (qu'on admettra) :

Lemme 2.57. *Soient A un anneau et M un idéal maximal de A. Alors les A-modules M/M^2 et MA_M/M^2A_M sont isomorphes.*

Ayant en tête le théorème 2.53, on en vient donc naturellement aux définitions suivantes qui généralisent les développements de la section 1.5 :

Définition 2.58. Soit X un schéma. L'*espace tangent* de X en un point $x \in X$ est le dual du $k(x)$-espace vectoriel $\mathcal{M}_x/\mathcal{M}_x^2$, où $\mathcal{M}_x$ est l'idéal maximal de $\mathcal{O}_{X,x}$. Il est noté $T_{X,x}$.

On dit que X est *régulier* (ou *lisse*) en x si l'anneau local $\mathcal{O}_{X,x}$ est régulier, c'est-à-dire que $\dim_{k(x)} \mathcal{M}_x/\mathcal{M}_x^2 = \dim \mathcal{O}_{X,x}$, et on dit que X est régulier s'il est régulier en chaque point.

Remarque 2.59. Une immersion ouverte induit un isomorphisme d'espaces tangents, et une immersion fermée induit une injection d'espaces tangents.

Remarque 2.60. On admet que la régularité d'un schéma se vérifie sur ses points fermés (se référer à [Har10, 6.14] pour les détails).

Le développement ci-dessus montre que pour $X = \operatorname{spec}(A/(f))$, l'espace tangent est entièrement fixé par l'injection $(f)/((f) \cap \mathfrak{m}^2) \to \mathfrak{m}/\mathfrak{m}^2$, c'est-à-dire par la valeur de f modulo $\mathfrak{m}^2$; et que l'espace tangent est de dimension $n-1$ si cette valeur est non nulle, et de dimension n sinon.

Dans le cas d'une hypersurface projective $X = \operatorname{Proj}(B/(f))$ étudiée en un point x, on se ramène au cas affine. On regarde l'immersion fermée $i\colon X \to \mathbb{P}_k^n$. Supposons que la coordonnée x_0 ne s'annule pas en $y = i(x)$; alors i induit une immersion fermée $\operatorname{spec}(B_{(x_0)}/(f_0)) \to \operatorname{spec}(B_{(x_0)})$ entre des sous-schémas affines ouverts de X et $\mathbb{P}_k^n$ respectivement (où f_0 désigne l'image de f dans $B_{(x_0)}$). L'inclusion de l'espace tangent en x de X dans celui de $\mathbb{P}_k^n$ est alors l'inclusion de l'espace tangent de $\operatorname{spec}(B_{(x_0)}/(f_0))$ dans celui de $\operatorname{spec}(B_{(x_0)})$. Choisir $T_{X,x}$ parmi les sous-espaces de codimension au plus 1 de $T_{\mathbb{P}_k^n,y}$ revient donc au choix de f_0 modulo $\mathfrak{m}_{y,0}^2$ (avec $\mathfrak{m}_{y,0}$ l'idéal de y dans $\operatorname{spec}(B_{(x_0)})$), c'est à dire au choix de f modulo $\mathfrak{m}_y^2$ (avec $\mathfrak{m}_y$ l'idéal de y dans $\mathbb{P}_k^n$).

Remarque 2.61. Le développement de cette section étudie la régularité d'une hypersurface de l'espace affine. Le raisonnement est le même pour l'étude de l'intersection d'une variété affine lisse X avec une hypersurface $\operatorname{spec}(k[x_1, \dots, x_n]/(f))$. Ecrivons $X = \operatorname{spec}(A)$ où cette fois-ci $A = k[x_1, \dots, x_n]/I$, où I est un idéal. L'intersection étudiée est alors $\operatorname{spec}(A/(\bar{f}))$ où $\bar{f}$ est la valeur de f modulo I. Remplaçons également E par $T_{X,x}$. Cette réécriture permet d'utiliser exactement le même raisonnement (mais ici le fait que $\mathcal{D}$ induit un isomorphisme entre $\mathfrak{m}/\mathfrak{m}^2$ et $(T_{X,x})^*$ provient simplement de l'hypothèse de régularité sur X ; la section 1.5 montrait que cette hypothèse s'appliquait à l'espace affine). Cela montre alors que l'intersection de X avec une hypersurface $\operatorname{spec}(k[x_1, \dots, x_n]/(f))$ est lisse en un point x si et seulement si $\bar{f} \notin \mathfrak{m}_x^2$, où m_x^2 est l'idéal de x dans X.

De même que ci-dessus, cette caractérisation est la même dans un cadre projectif.

2.9 Notion d'$\mathcal{O}_X$-module

Définition 2.62. Soit X un schéma. Un $\mathcal{O}_X$-module (ou faisceau de modules sur X) est un faisceau de groupes abéliens $\mathcal{F}$ sur X tel que pour tout ouvert U de X, $\mathcal{F}(U)$ soit un module sur l'anneau $\mathcal{O}_X(U)$, avec de plus une compatibilité entre les applications de restriction $\mathcal{F}(U) \to \mathcal{F}(V)$ et $\mathcal{O}_X(U) \to \mathcal{O}_X(V)$ si $V \subset U$.

Un *morphisme d'$\mathcal{O}_X$-modules* est un morphisme $\mathcal{F} \to \mathcal{G}$ de faisceaux tel que pour tout ouvert U de X, le morphisme de groupes $\mathcal{F}(U) \to \mathcal{G}(U)$ soit un morphisme de $\mathcal{O}_X(U)$-modules. On définit aussi la notion de sous $\mathcal{O}_X$-modules et de quotient de $\mathcal{O}_X$-modules.

Pour deux $\mathcal{O}_X$-modules $\mathcal{F}$ et $\mathcal{G}$, on appelle $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G}$ le faisceau de modules sur X associé au préfaisceau $U \mapsto \mathcal{F}(U) \otimes_{\mathcal{O}_X(U)} \mathcal{G}(U)$ (voir 2.63 pour la définition). Sa fibre en un point P est $\mathcal{F}_P \otimes_{\mathcal{O}_{X,P}} \mathcal{G}_P$.

Proposition 2.63. *Soit $\mathcal{F}$ un préfaisceau sur un espace topologique X. Alors on définit un faisceau $\mathcal{F}^+$ sur X en prenant pour $\mathcal{F}^+(U)$ l'ensemble des applications $s : U \to \amalg_{x \in U} \mathcal{F}_x$ telles que pour tout x de U, $s(x) \in \mathcal{F}_x$ et d'autre part s coïncide avec une section de $\mathcal{F}$ au voisinage de x. Le faisceau $\mathcal{F}^+$ vérifie $(\mathcal{F}^+)_x = \mathcal{F}_x$ pour tout $x \in X$ et il est équipé d'un morphisme de préfaisceau $\mathcal{F} \to \mathcal{F}^+$ vérifiant la propriété universelle suivante : tout morphisme de $\mathcal{F}$ dans un faisceau $\mathcal{G}$ s'étend de manière unique en un morphisme de faisceaux $\mathcal{F}^+ \to \mathcal{G}$.*

Définition 2.64. Soit X un schéma. Un *faisceau d'idéaux* sur X est un sous $\mathcal{O}_X$-module du faisceau structural $\mathcal{O}_X$.

Soient A un anneau et M un A-module. On pose $X = \operatorname{spec} A$.

Définition 2.65. On définit un $\mathcal{O}_X$-module $\widetilde{M}$ sur X par le même procédé que celui utilisé dans la définition du faisceau structural $\mathcal{O}_X$. En particulier, on a $\widetilde{M}(D(f)) = M_f = M \otimes_A A_f$ pour tout f de A, et $\widetilde{M}_{\mathfrak{p}} = M_{\mathfrak{p}} = M \otimes_A A_{\mathfrak{p}}$ pour tout $\mathfrak{p}$ de $\operatorname{spec} A$.

Remarque 2.66. On construit bien un faisceau ainsi, car toutes les applications de restriction sont déjà été définies. En effet, d'après la partie sur la construction de $\operatorname{spec} A$, si $D(g) \subset D(f)$ alors on a un morphisme $A_f \to A_g$, et c'est un isomorphisme si $D(f) = D(g)$. On obtient donc un morphisme de restriction $M_f \to M_g$, et les propriétés de recollement sont bien vérifiées car elles le sont pour le faisceau structural $\mathcal{O}_X$.

On peut traiter le cas analogue pour un anneau $S = \bigoplus_{d \geq 0} S_d$ gradué et $M = \bigoplus_{d \geq 0} M_d$ un S-module gradué (c'est à dire $S_k \cdot M_l \subset M_{k+l}$). On fait l'hypothèse supplémentaire que S *est engendrée comme S_0-algèbre par une famille finie d'éléments de S_1*. Typiquement S peut être le quotient de l'anneau gradué $A[x_0, \ldots, x_n]$ avec $S_0 = A$. On pose $X = \operatorname{Proj} S$.

Définition 2.67. On définit un $\mathcal{O}_X$-module $\widetilde{M}$ de la même manière qu'on a défini $\mathcal{O}_X$. En particulier, $\widetilde{M}_{\mathfrak{p}} = M_{(\mathfrak{p})}$ pour tout p dans $\operatorname{Proj} S$, et $\widetilde{M}|_{D_+(f)} = \widetilde{M_{(f)}}$ pour tout f élément homogène de S, où $M_{(\mathfrak{p})}$ désigne le sous $S_{(\mathfrak{p})}$-module des éléments homogènes de degré zéro du localisé de M par rapport aux éléments homogènes non dans $\mathfrak{p}$, et $M_{(f)}$ désigne le sous $S_{(f)}$-module des éléments de degré zéro du localisé M_f.

Remarque 2.68. Ici aussi, il faudrait normalement montrer que définir $\widetilde{M}$ uniquement sur les ouverts principaux suffit mais comme dans le cas de $X = \operatorname{spec} A$, tout a déjà été montré précédemment lors de la construction du faisceau structural sur $\operatorname{Proj} S$.

Définition 2.69. Soit $X = \operatorname{Proj} S$. Pour tout $n \in \mathbb{Z}$, on pose $\mathcal{O}_X(n) = \widetilde{S(n)}$, où $S(n)$ désigne le module gradué S avec la graduation « décalée » suivant la formule $S(n)_d = S_{n+d}$. Pour tout $\mathcal{O}_X$-module $\mathcal{F}$, on définit de la même manière $\mathcal{F}(n) = \mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{O}_X(n)$.

Exemple 2.70. Si on prend $S = k[x_0, \ldots, x_n]$, alors $X = \mathbb{P}^n_k = \operatorname{Proj} S$ et on a :

$$H^0(X, \mathcal{O}_X(d)) = S_d$$

Proposition 2.71. *Soit Y une sous-variété finie de $\mathbb{P}^n_k$ (c'est-à-dire, ici, que l'espace sous-jacent est fini). Alors pour tout entier naturel d, les anneaux $H^0(Y, \mathcal{O}_Y(d))$ et $H^0(Y, \mathcal{O}_Y)$ sont isomorphes (mais de manière non canonique).*

Démonstration. Si $\mathcal{F}$ est un faisceau sur l'espace discret Y, alors $\mathcal{F}(Y)$ est le produit des $\mathcal{F}(P)$ sur les points P de $\mathcal{F}$. Cela nous ramène au cas où Y est réduit à un point, qui correspond à un idéal homogène maximal $\mathfrak{m}$ de $S = k[x_0, \dots, x_n]$. On peut alors écrire $Y = \mathrm{Proj}(S/I)$ où I est un idéal homogène de S dont le radical est $\mathfrak{m}$. Soit j tel que x_j ne s'annule pas en Y. Alors x_j est inversible modulo $\mathfrak{m}$, donc aussi modulo $\mathfrak{m}^k$ pour tout entier naturel k, d'après le lemme de Hensel. Comme le radical de I est $\mathfrak{m}$, une des puissances de $\mathfrak{m}$ est contenue dans I. Ainsi x_j est inversible modulo I.

L'application de S dans $S(d)$ définie par $f \mapsto x_j^d f$ induit alors un isomorphisme de S/I dans $S(d)/I(d) = (S/I)(d)$. □

3 La fonction zêta de Hasse-Weil

A chaque variété sur un corps fini, on peut associer une fonction analytique, la fonction zêta de Hasse-Weil, qui présente des propriétés similaires à la célèbre fonction zêta de Riemann

$$\zeta(s) = \prod_{p \text{ premier}} (1 - p^{-s})^{-1}.$$

On présentera ici les définitions et propriétés dont nous aurons besoin, qui sont tirées de [Mus11].

3.1 Quelques préliminaires

Soit $k = \mathbb{F}_q$. On dit qu'un schéma X est une *variété* sur k si c'est un k-schéma de type fini.

Soit X une variété sur k. On va éclaircir la notion de K-points, avec K une extension algébrique de k (ce qui est le seul cas que l'on considère). On a par la définition 2.39

$$X(K) := \hom_{\mathrm{spec}\, k}(\mathrm{spec}\, K, X)$$

Or on a vu qu'un morphisme de schéma entre $\mathrm{spec}\, K$ et X est la donnée de deux applications $(f, f_\sharp)$, avec $f : \mathrm{spec}\, K = \{(0)\} \to X$ et de $f_\sharp : \mathcal{O}_X \to f_* \mathcal{O}_{\mathrm{spec}\, K}$. Ceci revient donc à se donner un point fermé $x \in X$ et un k-morphisme $k(x) \hookrightarrow K$. Ainsi, $X(K)$ se réécrit :

Proposition 3.1. *Si K est une extension algébrique de k, alors*

$$X(K) = \bigsqcup_{x \in X_{cl}} \hom_{k-\mathrm{alg}}(k(x), K)$$

avec X_{cl} l'ensemble des points fermés de X.

En particulier, $X(k)$ est l'ensemble des points fermés x de X de corps résiduel k.

On en déduit alors le résultat suivant :

Proposition 3.2. *Si K est une extension de degré r de k, alors :*

$$X(K) = \bigsqcup_{\deg(x)|r} \hom_{k-\text{alg}}(k(x), K)$$

En effet, il ne peut avoir un morphisme de corps $k(x) \hookrightarrow K$ que si $\deg(x) = [k(x) : k]$ divise $[K : k] = r$.

De plus, si on note $\deg(x) = e$ avec e divisant r, alors on a une action transitive du groupe de Galois $G(\mathbb{F}_{q^r}, \mathbb{F}_q) \simeq \mathbb{Z}/r\mathbb{Z}$ sur $\hom_{k-\text{alg}}(k(x), K)$ donnée par la composition à gauche car on travaille avec des morphismes de k-algèbres. Le stabilisateur de chaque élément est isomorphe à $G(\mathbb{F}_{q^r}, \mathbb{F}_{q^e})$. On en déduit donc par l'équation des classes que :

$$|\hom_{k-\text{alg}}(k(x), K)| = e$$

et on a alors le résultat suivant :

Proposition 3.3. *Si X est une variété sur un corps fini k et que K/k est une extension de degré r alors*

$$|X(K)| = \sum_{e|r} e \times |\{x \in X_{cl} \mid \deg(x) = e\}|$$

En vertu de la proposition 2.38, ce nombre est fini et borné par $r^2 s^r$ où s est un nombre qui ne dépend que de X.

Remarque 3.4. Si X est affine, en considérant une injection fermée $X \hookrightarrow \mathbb{A}^n_k$ défini par les équations $f_1, \ldots, f_d$, on trouve alors :

$$X(K) = \{u \in K^n \mid f_i(u) = 0, \forall 1 \leq i \leq d\}$$

Remarque 3.5. On note que $|X(K)|$ ne dépend que du cardinal de K dès que K est fini.

3.2 La fonction zêta de Hasse-Weil

On est maintenant en mesure de définir la fonction zêta d'une variété :

Définition 3.6 (Fonction zêta de Hasse-Weil)**.** Soit X une variété sur un corps fini k. On pose $N_m = |X(\mathbb{F}_{q^m})|$ et on définit la fonction zêta de X par :

$$Z(X, t) = \exp\left(\sum_{m \geq 1} \frac{N_m}{m} t^m\right)$$

D'après la remarque 3.5 et la proposition 3.3, N_m est bien défini et la série a un rayon de convergence non nul.

On peut donner une autre forme de la fonction zêta analogue à l'expression sous forme de produit eulérien de la fonction zêta de Riemann.

Proposition 3.7. *Pour toute variété X sur $\mathbb{F}_q$:*

$$Z(X, t) = \prod_{x \in X_{cl}} (1 - t^{\deg(x)})^{-1}$$

Démonstration. On note $a_r := |\{x \in X_{cl} \mid \deg(x) = r\}|$ pour tout $r \geq 1$, alors le membre de droite se réécrit $\prod_{r=1}^{\infty}(1-t^r)^{-a_r}$ (le produit converge bien). De plus, on sait par la proposition 3.3 que $N_m = \sum_{r|m} r a_r$. Passons maintenant au calcul de $Z(X,t)$:

$$\begin{aligned}\log Z(X,t) &= \sum_{m\geq 1} \frac{N_m}{m} t^m = \sum_{m\geq 1}\sum_{r/m} \frac{r a_r}{m} t^m \\ &= \sum_{r\geq 1} a_r \sum_{l\geq 1} \frac{t^{rl}}{l} \\ &= \sum_{r\geq 1} (-a_r)\log(1-t^r) = \sum_{r\geq 1} \log(1-t^r)^{-a_r} \\ &= \log\left(\prod_{r\geq 1}(1-t^r)^{-a_r}\right)\end{aligned}$$

et on obtient le résultat en passant à l'exponentielle des deux côtés de l'égalité. □

Remarque 3.8. Si $q = (q')^m$ alors on peut définir sur X une structure naturelle de variété sur $\mathbb{F}_{q'}$ et comme $[k(x) : \mathbb{F}_{q'}] = m[k(x) : \mathbb{F}_q]$ on en déduit par la proposition que $Z(X/\mathbb{F}_{q'}, t) = Z(X/\mathbb{F}_q, t^m)$.

Remarque 3.9. Dans la dernière partie du mémoire, on utilisera la notation suivante : pour X une variété sur $\mathbb{F}_q$, on note :

$$\zeta_X(s) = Z(X, q^{-s}) = \prod_{P\in X_{cl}} (1-q^{-s\deg P})^{-1} = \exp\left(\sum_{m=1}^{+\infty} \frac{N_m}{m} q^{-ms}\right)$$

3.3 Quelques calculs et propriétés

Exemple 3.10 (Espace affine). Soit $k = \mathbb{F}_q$ et $X = \mathbb{A}^n$ il est clair que pour toute extension finie k' de k, $X(k') = (k')^n$, ainsi :

$$\begin{aligned}Z(\mathbb{A}^n, t) &= \exp\left(\sum_{m\geq 1} \frac{q^{mn}}{m} t^m\right) \\ &= \exp\left(-\log(1-q^n t)\right) \\ &= \frac{1}{1-q^n t}\end{aligned}$$

On va maintenant énoncer une proposition qui va nous aider à calculer la fonction zêta de certaines variétés.

Proposition 3.11. *Si X est une variété sur $\mathbb{F}_q$ et Y est une sous-variété fermée de X, alors en posant $U = X \setminus Y$, on a :*

$$Z(Y,t) = Z(X,t) \times Z(U,t)$$

Démonstration. On a de manière évidente que $|X(\mathbb{F}_{q^m})| = |Y(\mathbb{F}_{q^m})| + |U(\mathbb{F}_{q^m})|$ pour tout $m \geq 1$. La propostion vient du fait que $\exp(u+v) = \exp u \exp v$ pour tout $u, v \in t\mathbb{Q}[|t|]$. □

On peut maintenant calculer la fonction zêta de l'espace projectif :

Corollaire 3.12. *La fonction zêta de l'espace projectif est :*

$$Z(\mathbb{P}^n_{\mathbb{F}_q}, t) = \frac{1}{(1-t)(1-qt)\dots(1-q^n t)}$$

Démonstration. On procède par récurrence sur n :

Pour $n = 0$: $\mathbb{P}^0_{\mathbb{F}_q} = \mathbb{A}^0$ est un espace constitué d'un point et par l'exemple 3.10, on a $Z(\mathbb{P}^0_{\mathbb{F}_q}, t) = \frac{1}{1-t}$.

Maintenant supposons la propriété vraie au rang $n-1$: On a une injection fermée $\mathbb{P}^{n-1}_{\mathbb{F}_q} \hookrightarrow \mathbb{P}^n_{\mathbb{F}_q}$ donnée par :

$$(x_1 : \dots : x_n) \in \mathbb{P}^{n-1}_{\mathbb{F}_q} \mapsto (0 : x_1 : \dots : x_n) \in \mathbb{P}^n_{\mathbb{F}_q}$$

et le complémentaire de l'image de cette injection est $\{(1 : x_1 : \dots : x_n)\}$ qui est isomorphe à $\mathbb{A}^n$ par $(1 : x_1 : \dots : x_n) \in \mathbb{P}^n_{\mathbb{F}_q} \mapsto (x_1, \dots, x_n) \in \mathbb{A}^n$. On conclut finalement en utilisant 3.11. □

4 Le théorème de Bertini

4.1 La méthode du crible

La méthode introduite par Poonen dans [Poo04] pour étendre le théorème de Bertini aux corps finis est connue sous le nom de *méthode du crible*. Etudions d'abord un exemple d'une application arithmétique de cette méthode.

La densité des entiers sans facteurs carrés

On définit la *densité* d'une partie A de $\mathbb{N}$ par :

$$\mu(A) := \lim_{n \to +\infty} \frac{\mathrm{card}(A \cap [\![0; n]\!])}{n+1}$$

Par exemple, la densité de $k\mathbb{N}$ est $\frac{1}{k}$ ce que l'on peut interpréter comme « la probabilité qu'un entier soit divisible par k est $1/k$ ».

On définit de même les densités supérieures et inférieures en prenant la lim sup et la lim inf dans la définition.

Calculons la densité des entiers sans facteurs carrés.

Un entier n est sans facteur carré si et seulement si pour tout p premier, p^2 ne divise pas n. On sait de plus par le lemme chinois que les événements « p divise n » et « q divise n » sont indépendants. On s'attend donc à ce que la probabilité qu'un entier soit sans facteur carré soit :

$$\mu(\{\text{entiers sans facteurs carrés}\}) = \prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p^2}\right),$$

et on va voir que c'est effectivement le cas. Mais l'argument d'indépendance ne tient plus lorsque l'on considère une infinité de nombres premiers. On a donc recours à la méthode du crible : on va considérer tous les nombres premiers $\leq r$ avec r arbitraire, calculer la proportion

des facteurs sans carrés pour ces nombres premiers $\leq r$ et ensuite faire grandir r. Il faudra montrer alors que l'erreur qu'on commet en omettant les grands nombres premiers tend bien vers 0. Cela revient à établir que la densité supérieure des entiers qui sont divisibles par p^2 pour un p premier grand est 0. Il faut donc montrer que :

$$\lim_{r\to\infty} \limsup_{B\to\infty} \left(\frac{\operatorname{card}\{n \leq B \mid p^2 \text{ divise } n \text{ pour un } p > r\}}{B} \right) = 0,$$

ce que l'on prouve ainsi :

$$\begin{aligned}
\operatorname{card}\left\{n \leq B \;\middle|\; p^2 \text{ divise } n \text{ pour un } p > r\right\} &\leq \sum_{\substack{p>r \\ p \text{ premier}}} \operatorname{card}\left\{n \leq B \;\middle|\; p^2 \text{ divise } n\right\} \\
&= \sum_{\substack{p>r \\ p \text{ premier}}} \lfloor B/p^2 \rfloor \\
&\leq \sum_{n>r} B/n^2 \\
&\leq B \int_r^\infty \frac{dx}{x^2} \\
&= B/r
\end{aligned}$$

Il reste alors à diviser par B, prendre la limite lorsque $B \to \infty$, et enfin prendre la limite lorsque $r \to \infty$ ce qui donne bien 0.

Principe de la méthode

Dans l'exemple ci-dessus, la propriété d'être sans facteur carré s'est décomposée en une collection de propriétés relatives à chaque nombre premier, ces propriétés étant indépendantes. On a alors pu faire un crible : on commence par supprimer les entiers qui ne vérifient pas la propriété en 2, puis, parmi ceux qui restent, les entiers qui ne vérifient pas la propriété en 3, puis en 5, puis en 7, et ainsi de suite. L'enjeu était alors de montrer que le calcul naïf passe correctement à la limite.

Pour démontrer le théorème de Bertini sur un corps fini, on aura recours au même genre de méthodes : on a une propriété géométrique des polynômes, et cette propriété se décompose en des propriétés locales en les points (fermés) du plan. Le crible ne porte alors plus sur les nombres premiers, mais sur les points.

4.2 Comptage des courbes lisses du plan affine

On définit la *densité* d'une partie $\mathcal{P} \subseteq \mathbb{F}_q[x,y]$ par :

$$\mu(\mathcal{P}) = \lim_{d\to+\infty} \frac{\operatorname{card}\left(\mathcal{P} \cap \mathbb{F}_q[x,y]_{\leq d}\right)}{\operatorname{card} \mathbb{F}_q[x,y]_{\leq d}}$$

et on définit la densité supérieure de la même manière en utilisant la lim sup. On a alors le résultat suivant :

Théorème 4.1. *Si $\mathcal{P}$ est l'ensemble des $f \in \mathbb{F}_q[x,y]$ tels que $\{f = 0\}$ est lisse en tous les points fermés de $\mathbb{A}^2$, (ici on précise lisse de dimension 1, c'est à dire $0 \notin \mathcal{P}$), alors*

$$\mu(\mathcal{P}) = \zeta_{\mathbb{A}^2}(3)^{-1}$$

D'après les calculs de la partie 3.3, cette valeur vaut $\frac{q-1}{q}$.

La démonstration suit un crible sur les points fermés. Ces points fermés seront répartis en trois catégories, suivant leur degré (faible, moyen, haut).

Les points de faible degré

Soit $r > 0$, on définit $\mathcal{P}_r$ comme l'ensemble des $f \in \mathbb{F}_q[x,y]$ tels que f soit lisse en tout point P fermé de degré $< r$ de $\mathbb{A}^2$.

Lemme 4.2. *On a*

$$\mu(\mathcal{P}_r) = \prod_{\deg P < r} \left(1 - q^{-3\deg P}\right)$$

Démonstration. Soient $\mathfrak{m}_P \subset \mathbb{F}_q[x,y]$ l'idéal maximal correspondant à P et $I := \prod_{\deg P<r} \mathfrak{m}_P^2$. Remarquons que :

1. f appartient à $\mathcal{P}_r$ si et seulement si l'image de f par le morphisme :

$$\mathbb{F}_q[x,y]_{\leq d} \xrightarrow{\phi_d} \prod_{\deg P<r} \frac{\mathbb{F}_q[x,y]}{\mathfrak{m}_P^2}$$

   est non nulle en chaque facteur.

2. Pour d assez grand, le morphisme ϕ_d est surjectif. En effet, le lemme chinois nous autorise à voir ϕ_d sous la forme

$$\mathbb{F}_q[x,y]_{\leq d} \xrightarrow{\phi_d} \frac{\mathbb{F}_q[x,y]}{I}$$

   et si $V_d = \operatorname{Im}\phi_d$, on a $V_{d+1} = V_d + xV_d + yV_d$, donc la suite V_d est strictement croissante pour l'inclusion puis elle stationne car le $\mathbb{F}_q$-espace vectoriel $\frac{\mathbb{F}_q[x,y]}{I} \simeq \prod \frac{\mathbb{F}_q[x,y]}{\mathfrak{m}_P^2}$ est de dimension finie (d'après 1.39).

D'après ces deux remarques et le résultat 1.39, on a pour d assez grand

$$\mu(\mathcal{P}_r) = \prod_{\deg P < r} \left(1 - q^{-3\deg P}\right)$$

□

Les points de degré moyen

On pose :

$$\mathcal{Q}_r = \bigcup_d \left\{ f \in \mathbb{F}_q[x,y]_{\leq d} \;\middle|\; \begin{array}{l} \text{il existe } P \text{ tel que } r < \deg P < d/3 \\ \text{en lequel } \{f = 0\} \text{ n'est pas lisse} \end{array} \right\}$$

Lemme 4.3. *On a*

$$\overline{\mu}(\mathcal{Q}_r) \xrightarrow[r\to+\infty]{} 0$$

Démonstration. On sait par la preuve du lemme précédent que $\mathbb{F}_q[x,y]_{\leq d} \to \frac{\mathbb{F}_q[x,y]}{\mathfrak{m}_P^2}$ est surjective pour $d \geq \dim \frac{\mathbb{F}_q[x,y]}{\mathfrak{m}_P^2} = 3\deg P$. Ainsi, la densité des éléments de $\mathbb{F}_q[x,y]_{\leq d}$ qui sont dans $\mathfrak{m}_P^2$ est $q^{-3\deg P}$. Ainsi :

$$\overline{\mu}(\mathcal{Q}_r) \leq \limsup_{d\to+\infty} \sum_{r<\deg P\leq d/3} q^{-3\deg P},$$

et le terme de droite tend vers 0 lorsque $r \to +\infty$ car $\sum_{P \text{ point fermé}} q^{-3\deg P}$ converge. En effet :

$$\sum_{P\text{point fermé}} q^{-3\deg P} = \sum_{e=0}^{+\infty} c_e q^{-3e}$$

avec c_e le nombre de points fermés de $\mathbb{A}^2$ de degré e, qui vérifie $c_e = O(q^{2e})$ d'après 1.11. □

Les points de haut degré

On définit :

$$\mathcal{R} = \bigcup_d \left\{ f \in \mathbb{F}_q[x,y]_{\leq d} \;\middle|\; \begin{array}{l} \text{il existe un point } P \text{ tel que } \deg P > d/3 \\ \text{en lequel } f = 0 \text{ n'est pas lisse} \end{array} \right\}$$

Lemme 4.4. *On a* $\mu(\mathcal{R}) = 0$

Démonstration. Avant de commencer , il est important de noter que :

$$\dim_{\mathbb{F}_q} \mathbb{F}_q[x,y]_{\leq d} = \frac{(d+1)(d+2)}{2} = \Theta(d^2)$$

Si f_0, g_1, g_2, h sont choisis aléatoirement dans $\mathbb{F}_q[x,y]_{\leq d}$, $\mathbb{F}_q[x,y]_{\leq (d-1)/p}$, $\mathbb{F}_q[x,y]_{\leq (d-1)/p}$, $\mathbb{F}_q[x,y]_{\leq d/p}$ respectivement (p étant la caractéristique de $\mathbb{F}_q$), alors

$$f := f_0 + xg_1^p + yg_2^p + h^p$$

est un polynôme choisi aléatoirement dans $\mathbb{F}_q[x,y]_{\leq d}$. Montrons ce fait : comme p est la caractéristique de $\mathbb{F}_q$, l'application $\phi : (f_0, g_1, g_2, h) \mapsto f_0 + g_1^p + g_2^p + h^p$ est linéaire entre deux espaces de dimension finie sur $\mathbb{F}_q$. Donc pour tout $f \in \mathbb{F}_q[x,y]_{\leq d}$, $\operatorname{card} \phi^{-1}(\{f\}) = \operatorname{card} \ker \phi$. La loi est donc bien uniforme et on peut générer f ainsi. Ceci nous permettra de découpler les dérivées partielles de f :

• Tout d'abord : Si f_0 est fixé, la probabilité conditionnelle sur g_1 que $\dim\left\{\frac{\partial f}{\partial x} = 0\right\} = 1$ est $1 - o(1)$ quand $d \to \infty$, et ce uniformément en f_0. En effet, on a :

$$\frac{\partial f}{\partial x} = \frac{\partial f_0}{\partial x} + g_1^p$$

Donc $\dim\{\frac{\partial f}{\partial x} = 0\}$ ne dépend que de g_1 (ici f_0 est fixé), et cette dimension peut être égale à 0,1 ou 2.

Remarque 4.5. L'équation $\frac{\partial f}{\partial x} = \frac{\partial f_0}{\partial x} + g_1^p$ d'inconnue g_1 a au plus une solution par unicité de la racine p-ième dans $\mathbb{F}_q$. C'est ce que nous utilisons dans la suite.

Si $\dim\{\frac{\partial f}{\partial x}=0\}=2$ alors $\frac{\partial f}{\partial x}\equiv 0$ ce qui donne au plus une valeur possible pour g_1. Le cas $\dim\{\frac{\partial f}{\partial x}=0\}=0$ est impossible car un polynôme non nul définit forcément une variété de dimension 1. Ainsi :

$$\mathbb{P}\left(\dim\left\{\frac{\partial f}{\partial x}=0\right\}=1\right)=1-\frac{1}{q^{\Theta(d^2)}}=1-o(1)$$

• Supposons f_0 et g_1 choisis tels que $\dim\left\{\frac{\partial f}{\partial x}=0\right\}=1$, la probabilité conditionnelle sur g_2 tel que $\dim\left\{\frac{\partial f}{\partial x}=\frac{\partial f}{\partial y}=0\right\}=0$ est $1-o(1)$ quand $d\to\infty$, uniformément en f_0 et g_1.

Remarque 4.6. Ici, comme dans le cas précédent, $\frac{\partial f}{\partial y}=\frac{\partial f_0}{\partial y}+g_2^p$ ne dépend que de g_2 car f_0 est fixé ; et cette équation d'inconnue g_2 a au plus une solution.

Remarque 4.7. Dire que $\dim\left\{\frac{\partial f}{\partial x}=\frac{\partial f}{\partial y}=0\right\}=1$ signifie que $X=\left\{\frac{\partial f}{\partial x}=0\right\}$ et $Y=\left\{\frac{\partial f}{\partial y}=0\right\}$ ont une composante irréductible en commun de dimension 1, en effet $X\cap Y$ s'écrit comme union de ses composantes irréductibles. Soit Z une composante irréductible de dimension 1 de $X\cap Y$, alors $Z\subset X$ donc Z est une composante irréductible de X. De même, Z est une composante irréductible de Y.

On va étudier $\frac{\partial f}{\partial y}$ sur chaque composante irréductible de X. On écrit $\frac{\partial f}{\partial x}$ sous forme de produit de facteurs irréductibles :

$$\frac{\partial f}{\partial x}=R_1^{\alpha_1}\dots R_s^{\alpha_s}$$

avec $s\leq d-1$, les R_i deux à deux premiers entre eux et irréductibles, on pose $d_i=\deg R_i$. Pour tout idéal $\mathfrak{a}$, on définit $Z(\mathfrak{a})=\{P\in\mathbb{A}^2\mid f(P)=0,\forall f\in\mathfrak{a}\}$. Soit $\mathfrak{a}_i$ l'idéal engendré par R_i ; on a $X=Z\left(\frac{\partial f}{\partial x}\right)=Z(\mathfrak{a}_1)\cup\ldots\cup Z(\mathfrak{a}_s)$. On montre aisément que $Z(\mathfrak{a})$ est irréductible si et seulement si $\mathfrak{a}$ est un idéal premier. Ici, les R_i étant irréductibles, $\mathfrak{a}_i$ est bien un idéal premier donc $Z(\mathfrak{a}_i)$ est une partie irréductible de $\mathbb{A}^2$ et pour $i\neq j$, on a $Z(\mathfrak{a}_i)\not\subset Z(\mathfrak{a}_j)$; par unicité c'est donc l'écriture de X en composantes irréductibles. Donc X et Y ont une composante irréductible en commun si et seulement si $\frac{\partial f}{\partial y}$ est divisible par un des R_i (c'est-à-dire $\frac{\partial f}{\partial y}\in(R_i)$). Il vient donc que :

$$\mathbb{P}\left(\dim\left\{\frac{\partial f}{\partial x}=\frac{\partial f}{\partial y}=0\right\}=1\right)=\mathbb{P}\left(\bigcup_{i=1}^{s}\left(\frac{\partial f}{\partial y}\in(R_i)\right)\right)\leq\sum_{i=1}^{s}\mathbb{P}\left(\frac{\partial f_0}{\partial y}+g_2^p\in(R_i)\right)$$

Soit $g_{2,0}$ (de degré au plus $(p-1)/d$) une solution de $\frac{\partial f_0}{\partial y}+g_{2,0}^p\in(R_i)$ (si elle existe). Alors pour un g_2 quelconque, $\frac{\partial f_0}{\partial y}+g_2^p\in(R_i)$ si et seulement si $g_2^p-g_{2,0}^p=(g_2-g_{2,0})^p\in(R_i)$, si et seulement si $g_2-g_{2,0}\in(R_i)$ (car R_i est irréductible donc (R_i) est premier), si et seulement s'il existe Q tel que $g_2-g_{2,0}=QR_i$, et alors Q est nécessairement de degré au plus $\frac{d-1}{p}-d_i$. Tout ceci montre que

$$\mathbb{P}\left(R_i\text{ divise }\frac{\partial f}{\partial y}\right)\leq\frac{\operatorname{card}\mathbb{F}_q[x,y]_{\leq(d-1)/p-d_i}}{\operatorname{card}\mathbb{F}_q[x,y]_{\leq(d-1)/p}}=\begin{cases}q^{(d_i^2-d_i(3+2(d-1)/p))/2}\leq q^{-d/p} & \text{si } d_i\leq\frac{d-1}{p}\\ 0 & \text{sinon}\end{cases}$$

Cette étude permet d'avoir la borne uniforme désirée :

$$\mathbb{P}\left(\dim\left\{\frac{\partial f}{\partial x}=\frac{\partial f}{\partial y}=0\right\}=1\right)\leq sq^{-d/p}\leq dq^{-d/p}\xrightarrow[d\to\infty]{}0$$

• Enfin, si on fixe f_0, g_1 et g_2 tels qu'ils vérifient les conditions précédentes, alors la probabilité conditionnelle sur le choix de h tel que $\left\{f = \frac{\partial f}{\partial x} = \frac{\partial f}{\partial y} = 0\right\}$ n'ait pas de point de degré supérieur à $d/3$ est $1 - o(1)$ lorsque $d \to \infty$, uniformément en f_0, g_1, g_2.

Pour montrer cela on utilise le théorème de Bézout :

Théorème 4.8 (Bézout)**.** *Soit C, D deux courbes algébriques affines planes sur un corps k algébriquement clos de degré m et n respectivement. Si les deux courbes n'ont pas de composantes irréductibles en commun, alors le nombre de points d'intersection de C et D comptés avec multiplicités est mn.*

Le choix de f_0, g_1 et g_2 permet d'appliquer le théorème à $C = \left\{\frac{\partial f}{\partial x} = 0\right\}$ et $D = \left\{\frac{\partial f}{\partial y} = 0\right\}$(Ici, le corps qu'on considère n'est pas algébriquement clos, le théorème de Bézout fournit donc une borne supérieure). Comme la multiplicité d'un point d'intersection est au moins égale à son degré, il vient

$$\sum_{P \in C \cap D} \deg(P) \leq (d-1)^2$$

Il y a donc au plus $\frac{3(d-1)^2}{d} \underset{+\infty}{\sim} 3d$ points de degré supérieur à $d/3$ dans $C \cap D = \left\{\frac{\partial f}{\partial x} = \frac{\partial f}{\partial y} = 0\right\}$.

Fixons un tel point P. On cherche à majorer la probabilité en h que f passe par P. On peut appliquer le même raisonnement que précédemment, si h_0 est une solution particulière de l'équation $f(P) = 0$, alors h_1 est une autre solution si et seulement si $h_0 - h_1 \in \mathfrak{m}_P$, ainsi l'ensemble des solutions est $h_0 + \mathfrak{m}_P$. La probabilité vaut alors au plus

$$\frac{\operatorname{card}(\mathbb{F}_q[x,y]_{\leq d/p} \cap \mathfrak{m}_P)}{\operatorname{card} \mathbb{F}_q[x,y]_{\leq d/p}}.$$

D'après un raisonnement de la partie sur les points de faible degré (croissance en e puis stationnement de l'image de la projection canonique $\mathbb{F}_q[x,y]_{\leq e} \to \mathbb{F}_q[x,y]/\mathfrak{m}_P$), cette quantité est majorée par $q^{-\min(d/p, \deg(P))} = q^{-d/p}$.

Remarque 4.9. Si la caractéristique vaut 2 (*i.e* $p = 2$), alors au lieu de majorer par $q^{-d/p}$, il faudrait majorer par $q^{-\min(d/2, d/3)} = q^{-d/3}$, et on poursuit la preuve de la même manière.

Donc finalement, en regardant sur tous les points de $C \cap D$ de degré supérieur à $d/3$:

$$\mathbb{P}\left(\left\{f = \frac{\partial f}{\partial x} = \frac{\partial f}{\partial y} = 0\right\} \text{ contient un point de degré } \geq d/3\right) \leq \frac{3(d-1)^2/d}{q^{d/p}} \xrightarrow[d \to \infty]{} 0$$

Ainsi, on a bien

$$\mu(\mathcal{R}) = 0$$

□

Enfin, on a pour tout $r > 0$,

$$\mathcal{P} = \mathcal{P}_r - \mathcal{Q}_r - \mathcal{R}$$

et quand $r \to \infty$,

$$\begin{aligned} \mu(\mathcal{P}_r) &\to \zeta_{\mathbb{A}^2}(3)^{-1} \\ \overline{\mu}(\mathcal{Q}_r) &\to 0 \\ \mu(\mathcal{R}) &= 0 \end{aligned}$$

et donc :

$$\mu(\mathcal{P}) = \zeta_{\mathbb{A}^2}(3)^{-1}$$

4.3 Le théorème de Bertini sur un corps fini

Nous passons maintenant au grand résultat de ce mémoire : le théorème de Bertini sur un corps fini. A l'origine, le théorème de Bertini affirme entre autres que si X est une variété projective lisse sur un corps algébriquement clos alors il existe un hyperplan dont l'intersection avec X est lisse.

Comme nous le verrons dans la partie 5.1, ce théorème tombe en défaut pour un corps fini. La question que l'on se pose ici est de savoir s'il devient vrai lorsqu'on l'on ne cherche pas à intersecter X avec un hyperplan mais avec une hypersurface. Pour y répondre, il nous faut d'abord introduire quelques objets dont nous aurons besoin dans la suite.

Si $k = \mathbb{F}_q$ est un corps fini, on pose $S = \mathbb{F}_q[x_0, \dots, x_n]$. On note alors S_d le $\mathbb{F}_q$-espace vectoriel des polynômes homogènes de degré d et enfin $S_{\text{homog}} = \bigcup_{d \geq 0} S_d$. Enfin, pour tout $f \in S_{\text{homog}}$, on note H_f le sous-schéma donné par $\text{Proj}(S/(f)) \subseteq \mathbb{P}^n$. On définit la *densité* d'une partie $\mathcal{P} \subset S_{\text{homog}}$ par :

$$\mu(\mathcal{P}) := \lim_{d \to +\infty} \frac{\text{card}(\mathcal{P} \cap S_d)}{\text{card}\, S_d}$$

si la limite existe. On définit également $\overline{\mu}(\mathcal{P})$ et $\underline{\mu}(\mathcal{P})$ en prenant respectivement la lim sup et la lim inf dans la définition de la densité. On est maintenant en mesure d'énoncer le théorème de Bertini sur un corps fini. Celui-ci permet en particulier de répondre à notre question par l'affirmative : on peut trouver des hypersurfaces qui intersectent notre variété de façon lisse.

Théorème 4.10 (Bertini sur un corps fini)**.** *Soit X une sous-variété quasiprojective lisse de $\mathbb{P}^n$ de dimension $m \geq 0$ sur $\mathbb{F}_q$. Soit*

$$\mathcal{P} = \{f \in S_{\text{homog}} \mid H_f \cap X \text{ est lisse de dimension } m-1\}$$

Alors $\mu(\mathcal{P}) = \zeta_X(m+1)^{-1}$.

Remarque 4.11. On retrouve en particulier le résultat que nous avons démontré dans le cas du plan affine : $X = \mathbb{A}^2$ est un sous-schéma lisse quasiprojectif de $\mathbb{P}^2$ de dimension 2 sur $\mathbb{F}_q$ et on avait bien trouvé que $\mu(\mathcal{P}) = \zeta_{\mathbb{A}^2}(3)^{-1}$.

L'idée de la preuve est comme dans le cas du plan de regarder les polynômes par degré croissant et d'enlever ceux pour lesquels $H_f \cap X$ n'est pas lisse de dimension $m-1$.

On peut généraliser ce que l'on a vu dans le cas du plan : la condition de régularité en un point P fermé d'une fonction f ne dépend que des coefficients de Taylor d'ordre 1 de f dans le corps résiduel de P, ce qui donne $m+1$ conditions dans $k(P)$. On s'attend donc à ce que la probabilité d'être lisse en P soit de $1 - q^{-(m+1)\deg P}$, et lorsqu'on considère un nombre fini de points, les conditions sont indépendantes (on le verra dans la preuve), donc les probabilités se multiplient. On s'attend donc à ce que la probabilité que $H_f \cap X$ soit lisse de dimension $m-1$ soit

$$\prod_{P \text{ fermé}} (1 - q^{-(m+1)\deg P}) = \zeta_X(m+1)^{-1}.$$

Seulement la légitimité du produit infini n'est pas fondée. Cette difficulté se contourne de la même manière que dans le cas du plan.

On démontre en fait une variante plus forte du théorème de Bertini qui permet d'imposer des conditions de Taylor sur la densité des fonctions qui nous intéressent.

Expliquons donc d'abord ce qu'on entend par conditions de Taylor. Soit Z une sous-variété finie de $\mathbb{P}^n$, c'est à dire, ici, que l'espace topologique sous jacent de Z est fini. Notons $P_1, \ldots, P_s$ les points de Z (ce sont alors des points fermés). Les immersions ouvertes $P_i \to Z$ sont des immersions fermées (Z est discret) qui se composent en des immersions fermées $\iota_i \colon P_i \to \mathbb{P}^n_k$, et on a $H^0(Z, \mathcal{O}_Z) = H^0(P_1, \mathcal{O}_{P_1}) \oplus \ldots \oplus H^0(P_s, \mathcal{O}_{P_s})$. Inversement, si on a un nombre fini d'immersions fermées $\iota_i \colon P_i \to \mathbb{P}^n$ sur des points, les P_i sont des spectres d'anneaux A_i et en prenant Z égal à $\operatorname{spec}(A_1 \oplus \ldots \oplus A_s)$, les immersions ι_i se factorisent avec les immersions $P_i \to Z$ en une immersion fermée $Z \to \mathbb{P}^n$.

Soit $f \in S_d$. Pour chaque i allant de 1 à s, soit $j(i)$ le plus petit indice j tel que la coordonnée x_j soit inversible sur P_i (c'est-à-dire P_i appartient à l'ouvert affine $U_j = D_+(x_j)$). Alors $x_{j(i)}^{-d} f$ est un élément de $\mathcal{O}_{\mathbb{P}^n}(U_{j(i)})$, donc s'envoie sur $H^0(P_i, \mathcal{O}_{P_i})$ par l'immersion fermée ι_i. On note alors $f|_Z$ l'élément de $H^0(Z, \mathcal{O}_Z)$ qui recolle ces morceaux.

Si pour chaque point P_i, l'immersion ι_i est l'immersion $\operatorname{Proj}(S/\mathfrak{m}_i^{k_i})$, où $\mathfrak{m}_i$ est l'idéal de S correspondant à P_i et k_i est un entier positif, alors $f|_Z$ représente les différentes valeurs de f modulo $\mathfrak{m}_i^{k_i}$. La remarque 1.38 explique pourquoi on appelle cela une condition de Taylor.

Théorème 4.12 (Bertini avec des conditions de Taylor)**.** *Soit X une sous-variété quasiprojective de $\mathbb{P}^n$ sur $\mathbb{F}_q$. Soit Z une sous-variété finie de $\mathbb{P}^n$, on suppose que $U := X \setminus (Z \cap X)$ est lisse de dimension $m \geq 0$. Soit $T \subseteq H^0(Z, \mathcal{O}_Z)$. On pose*

$$\mathcal{P} = \{f \in S_{\text{homog}} \mid H_f \cap U \text{ est lisse de dimension } m-1 \text{ et } f|_Z \in T\}$$

alors

$$\mu(\mathcal{P}) = \frac{\operatorname{card} T}{\operatorname{card} H^0(Z, \mathcal{O}_Z)} \zeta_U(m+1)^{-1}$$

Pour démontrer ce théorème, on reprend la preuve dans le cas du plan, en séparant les points selon leur degré. On considère les points de degré faible, moyen puis élevé.

Les points de faible degré

De la même manière que dans le cas du plan, on pose une une application ϕ_d qui restreint les fonctions aux idéaux qui vont nous intéresser ici.

Soit $A = \mathbb{F}_q[x_1, \ldots, x_n]$ l'anneau des fonctions sur $\mathbb{A}^n := \{x_0 \neq 0\} \subset \mathbb{P}^n$. On identifie S_d avec l'ensemble $A_{\leq d} = \{f \in A \mid \deg f \leq d\}$

Lemme 4.13. *Soit Y un sous-schéma fini de $\mathbb{P}^n$ sur un corps k, alors l'application*

$$\phi_d : S_d = H^0(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(d)) \to H^0(Y, \mathcal{O}_Y(d))$$

est surjective pour $d \geq \dim H^0(Y, \mathcal{O}_Y) - 1$.

Remarque 4.14. D'après la proposition 2.71, on peut aussi considérer que l'application ϕ_d est à valeurs dans $H^0(Y, \mathcal{O}_Y)$.

Démonstration. On admet ici que l'application ϕ_d est surjective à partir de d assez grand. On va en revanche montrer que, ce fait étant connu, nécessairement la suite est constante à partir de $\dim H^0(Y, \mathcal{O}_Y) - 1$.

On veut déhomogénéiser les éléments de S_d pour avoir une application $\mathbb{F}_q$-linéaire de $A_{\leq d}$ vers $H^0(Y, \mathcal{O}_Y)$. Pour cela, on note $Y = \{Y_1, \ldots, Y_s\} \subset \mathbb{P}^n$. On cherche alors une forme

linéaire non nulle y_0 telle que pour tout $i \in [\![1, s]\!]$, $y_0(\widetilde{Y_i}) \neq 0$ avec $\widetilde{Y_i}$ un antécédent de Y_i par $\mathbb{F}_q^{n+1} \to \mathbb{P}^n$. Il suffira ensuite de compléter y_0 en une base $(y_0, \ldots, y_n)$ de $(\mathbb{F}_q^{n+1})^*$.

Cela revient à se donner un hyperplan ne contenant aucun des $\widetilde{Y_i}$, on va raisonner par cardinalité. Comptons le nombre d'hyperplans de $\mathbb{F}_q^{n+1}$: un hyperplan H est caractérisé par $H = \ker \phi$ avec ϕ une forme linéaire et ϕ est unique à homothétie près. Or une forme linéaire n'est rien d'autre qu'un polynôme homogène de degré 1. On trouve donc $q^{n+1} - 1$ formes linéaires non nulles et en tenant compte du fait que deux formes linéaires proportionnelles donnent le même hyperplan, on obtient finalement en notant c_q le nombre d'hyperplans de $\mathbb{F}_q^{n+1}$ que

$$c_q = \frac{q^{n+1} - 1}{q - 1}.$$

Donc $c_q \sim q^n$ lorsque q tend vers l'infini.

Maintenant, pour $x \in \mathbb{F}_q^{n+1} \setminus \{0\}$, comptons le nombre b_q d'hyperplans contenant x. On peut supposer que la première coordonnée x_0 de x est non nulle. Une forme linéaire u qui s'annule en x est alors entièrement déterminée par ses coordonnées u_1, …, u_n. En retirant la forme linéaire nulle et en quotientant par $q - 1$, on trouve

$$b_q = \frac{q^n - 1}{q - 1}$$

et $b_q \sim q^{n-1}$ quand q tend vers l'infini.

Finalement, il y a au plus $sb_q = O(q^{n-1})$ hyperplans passant par au moins un point de Y, ainsi si on élargit $\mathbb{F}_q$ (en prenant une extension finie $\mathbb{F}_{q'}$ de degré suffisamment grand) on aura $c_q > b_q$ et on trouve l'existence d'une forme linéaire y_0 (à valeurs $\mathbb{F}_{q'}$) qui convient.

On a donc un changement de variables qui est un isomorphisme de $\mathbb{F}_q$-espaces vectoriels entre S_d et un sous-$\mathbb{F}_q$-espace de $\mathbb{F}_{q'}[x_0, \ldots, x_n]_{\leq d}$, tel que l'image de x_0 ne s'annule pas sur Y. On renomme $(x_0, \ldots, x_n)$ l'image du $(n+1)$-uplet $(x_0, \ldots, x_n)$ initial par le changement de variables. En prenant $x_0 = 1$, on voit que ϕ_d peut être vu comme une application d'une sous-$\mathbb{F}_q$-algèbre de $\mathbb{F}_{q'}[x_1, \ldots, x_n]$ isomorphe à $A_{\leq d}$ (qu'on notera abusivement $A_{\leq d}$) vers $B := H^0(Y, \mathcal{O}_Y)$. Soit $b = \dim B$, pour tout $i \geq -1$, on note B_i l'image de $A_{\leq i}$ dans B. Alors on a $0 = B_{-1} \subseteq B_0 \subseteq B_1 \subseteq \ldots$, et donc $B_j = B_{j+1}$ pour un certain $j \in [\![-1, b-1]\!]$. Comme dans la partie précédente on peut exprimer B_{k+1} en fonction de B_k :

$$B_{j+2} = B_{j+1} + \sum_{i=1}^{n} \phi_d(x_i) B_{j+1} = B_j + \sum_{i=1}^{n} \phi_d(x_i) B_j = B_{j+1}.$$

Ainsi on a $B_j = B_{j+1} = B_{j+2} = \ldots$ et donc la suite (B_i) est stationnaire. Comme on sait qu'à partir d'un certain rang ϕ_d est surjective, forcément la suite stationne en B. Donc ϕ_d est surjective pour $d \geq j$ et donc en particulier lorsque $d \geq b - 1$. □

Si U est un schéma de type fini sur $\mathbb{F}_q$, on pose $U_{<r}$ l'ensemble des points fermés de U de degré $< r$. On définit de la même manière $U_{>r}$.

Lemme 4.15 (densité des points singuliers de faible degré)**.** *Avec les hypothèses et notations du théorème, on pose :*

$$\mathcal{P}_r := \{f \in S_{\text{homog}} \mid H_f \cap U \text{ est lisse de dimension } m-1 \text{ en tout } P \in U_{<r} \text{ et } f|_Z \in T\}$$

Alors :

$$\mu(\mathcal{P}_r) = \frac{\operatorname{card} T}{\operatorname{card} H^0(Z, \mathcal{O}_Z)} \prod_{P \in U_{<r}} \left(1 - q^{-(m+1)\deg P}\right).$$

Démonstration. On note $U_{<r} = \{P_1, \ldots, P_s\}$. Soit $\mathfrak{m}_i$ l'idéal associé à P_i et Y_i le sous-schéma fermé de U correspondant au faisceau d'idéaux $\mathfrak{m}_i^2 \subset \mathcal{O}_U$, enfin soit $Y = \bigcup Y_i$. Alors $H_f \cap U$ n'est pas lisse de dimension $m-1$ en P_i si et seulement si la restriction de f à Y_i est nulle d'après la remarque 2.61. Ainsi, $\mathcal{P}_r \cap S_d$ est l'image réciproque de

$$T \times \prod_{i=1}^{s} \left(H^0(Y_i, \mathcal{O}_{Y_i}) \setminus \{0\}\right)$$

par l'application $\mathbb{F}_q$-linéaire

$$\phi_d : S_d = H^0(\mathcal{O}_{\mathbb{P}^n}, \mathcal{O}_{\mathbb{P}^n}(d)) \to H^0(Y \cup Z, \mathcal{O}_{Y\cup Z}(d)) \simeq H^0(Z, \mathcal{O}_Z) \times \prod_{i=1}^{s} H^0(Y_i, \mathcal{O}_{Y_i}), \qquad (2)$$

le dernier isomorphisme provenant de la proposition 2.71. Rappelons que cet isomorphisme n'est pas canonique : il dépend d'un choix, en chaque point de $Y \cup Z$, d'une coordonnée x_j ne s'annulant pas en le point. Pour les points de Z, il faut choisir j minimal, de sorte que ce choix coincide avec celui qui a servi à définir $f|_Z$.

Par le lemme 4.13 appliqué à $Y \cup Z$, on sait que ϕ_d est surjective pour d assez grand, d'où :

$$\mu(\mathcal{P}_r) = \lim_{d\to\infty} \frac{\operatorname{card}\left(T \times \prod_{i=1}^{s}(H^0(Y_i, \mathcal{O}_{Y_i}) \setminus \{0\})\right)}{\operatorname{card}\left(H^0(Z, \mathcal{O}_Z) \times \prod_{i=1}^{s} H^0(Y_i, \mathcal{O}_{Y_i})\right)} = \frac{\operatorname{card} T}{\operatorname{card} H^0(Z, \mathcal{O}_Z)} \prod_{i=1}^{s} \left(1 - q^{-(m+1)\deg P_i}\right),$$

car l'anneau de fonctions $H^0(Y_i, \mathcal{O}_{Y_i})$ a une filtration : $0 \subset \mathfrak{m}_i/\mathfrak{m}_i^2 \subset \mathcal{O}_{U,P_i}/\mathfrak{m}_i^2 = H^0(Y_i, \mathcal{O}_{Y_i})$ dont les quotients sont des $k(P_i)$-espaces vectoriels de dimension m et 1 respectivement. □

Les points de degré moyen

Comme dans la partie précédente, on cherche d'abord à calculer la proportion des fonctions qui ne vont pas être lisses en un point P de degré fixé :

Lemme 4.16. *Soit U une sous-variété lisse quasiprojective de $\mathbb{P}^n$ de dimension $m \geq 0$ sur $\mathbb{F}_q$. Si $P \in U$ est un point fermé de degré $e \leq \frac{d}{m+1}$, alors la proportion des $f \in S_d$ telles que $H_f \cap U$ n'est pas lisse de dimension $m-1$ en P est $q^{-(m+1)e}$.*

Démonstration. L'idée est toujours la même : si $\mathfrak{m}$ est l'idéal associé à P sur U, les fonctions $f \in S_d$ qui ne vont pas marcher sont celles telles que $f \in \mathfrak{m}^2$. On peut formaliser la situation ainsi. Soit Y le sous schéma fermé de U correspondant à $\mathfrak{m}^2$. Alors les fonctions $f \in S_d$ qui nous intéressent sont celles du noyau de l'application de restriction $\phi_d : H^0(\mathbb{P}^n, \mathcal{O}(d)) \to H^0(Y, \mathcal{O}_Y(d)) \simeq H^0(Y, \mathcal{O}_Y)$. Maintenant, $\dim H^0(Y, \mathcal{O}_Y) = (m+1)e \leq d$, donc d'après le lemme 4.13 ϕ_d est surjective. On en déduit par le théorème du rang que la $\mathbb{F}_q$-codimension de $\ker \phi_d$ dans S_d est $(m+1)e$, ce qui donne le résultat. □

On est maintenant en mesure de montrer que la densité des points de degré moyen qui posent problème est nulle :

Lemme 4.17. *Soit U une sous-variété lisse quasiprojective de $\mathbb{P}^n$ de dimension $m \geq 0$ sur $\mathbb{F}_q$. Posons*

$$\mathcal{Q}_r^{moy} := \bigcup_{d\geq 0} \left\{ f \in S_d \;\middle|\; \begin{array}{l} \text{il existe } P \in U \text{ avec } r \leq \deg P \leq \dfrac{d}{m+1} \text{ tel que } H_f \cap U \\ \text{n'est pas lisse de dimension } m-1 \text{ au point } P \end{array} \right\}.$$

Alors

$$\overline{\mu}(\mathcal{Q}_r^{moy}) = 0.$$

Démonstration. On utilise le lemme précédent et la majoration $\operatorname{card} U(\mathbb{F}_{q^m}) \leq cq^{em}$ pour un $c > 0$ ne dépendant que de U. Cette majoration provient de [LW54].

$$\begin{aligned} \frac{\operatorname{card}(\mathcal{Q}_r^{moy} \cap S_d)}{\operatorname{card} S_d} &\leq \sum_{e=r}^{\lfloor d/(m+1)\rfloor} \operatorname{card}\{P \in U_{cl} \mid \deg P = e\}\, q^{-(m+1)e} \quad \text{(par le lemme précédent)} \\ &\leq \sum_{e=r}^{\lfloor d/(m+1)\rfloor} \operatorname{card} U(\mathbb{F}_{q^m}) q^{-(m+1)e} \\ &\leq \sum_{e=r}^{\infty} cq^{em} q^{-(m+1)e} \\ &= \frac{cq^{-r}}{1-q^{-1}} \end{aligned}$$

Ainsi, $\overline{\mu}(\mathcal{Q}_r^{moy}) \leq cq^{-r}/(1-q^{-1})$ qui tend vers 0 quand r tend vers l'infini. □

Les points de haut degré

Lemme 4.18. *Soit P un point fermé de $\mathbb{A}^n$ de degré e sur $\mathbb{F}_q$. Alors la proportion des fonctions f qui s'annulent en P est au plus $q^{-\min(d+1,e)}$.*

Démonstration. Soit $\mathrm{ev}_P : A_{\leq d} \to \mathbb{F}_{q^e}$ la fonction d'évaluation en P. La preuve du lemme 4.13 montre que $\dim_{\mathbb{F}_q}(\mathrm{ev}_P(A_{\leq d}))$ augmente strictement avec d jusqu'à stationner en $e = \dim_{\mathbb{F}_q} \mathbb{F}_q^e$. On a donc pour tout d : $\dim_{\mathbb{F}_q}(\mathrm{ev}_P(A_{\leq d})) \geq \min(d+1, e)$ et donc la codimension de $\ker(\mathrm{ev}_P)$ est au moins $\min(d+1, e)$. □

Lemme 4.19. *Soit U une sous-variété quasiprojective lisse de $\mathbb{P}^n$ de dimension $m \geq 0$ sur $\mathbb{F}_q$. On pose :*

$$\mathcal{Q}^{haut} := \bigcup_{d\geq 0} \left\{ f \in S_d \;\middle|\; \begin{array}{l} \text{il existe un point } P \in U_{>d/(m+1)} \text{ tel que } H_f \cap U \\ \text{n'est pas lisse de dimension } m-1 \text{ au point } P \end{array} \right\}$$

Alors

$$\overline{\mu}(\mathcal{Q}^{haut}) = 0$$

Soit P un point fermé. Si on a montré le résultat pour deux ouverts V et W, alors le résultat est vrai pour $V \cup W$. On peut donc supposer que U est un ouvert affine contenant P. U est alors paramétré par un système de coordonnées locales $t_1, \ldots, t_n \in A$ de $\mathbb{A}^n$ autour de P

tel que au voisinage de P, U soit donné par les équations $t_{m+1} = \ldots = t_n = 0$ et l'assertion « f n'est pas lisse en P » soit équivalente à :

$$f(P) = \partial_1 f(P) = \ldots = \partial_m f(P) = 0$$

On n'expliquera pas ici comment se ramener à ce cas.

Ceci fait, on suit le modèle de la démonstration dans le cas du plan : soient $\tau = \max_i(\deg t_i)$, $\gamma = \lfloor (d-\tau)/p \rfloor$, et $\eta = \lfloor d/p \rfloor$. Si on choisit au hasard $f_0 \in A_{\leq d}$, $g_1, \ldots, g_m \in A_{\leq \gamma}$ et $h \in A_{\leq \eta}$, alors on génère aléatoirement tous les polynômes de $A_{\leq d}$ par :

$$f = f_0 + g_1^p t_1 + \ldots + g_m^p t_m + h^p$$

On peut donc calculer la probabilité que f ne soit pas lisse en P grâce à ce découpage qui permet de découpler les dérivées partielles. En effet, $\partial_i f = \partial_i f_0 + g_i^p \partial_i t_i$. On va choisir $f_0, g_1, \ldots, g_m, h$ chacun leur tour : pour $1 \leq i \leq m$, posons

$$W_i := U \cap \{\partial_1 f = \ldots = \partial_i f = 0\}.$$

On montre alors, comme dans le cas du plan, une série de lemmes permettant d'estimer les probabilités conditionnées sur le choix des g_i.

Lemme 4.20. *Pour $1 \leq i \leq m-1$, supposons que l'on ait choisi $f_0, g_1, \ldots, g_i$ tels que $\dim W_i \leq m - i$. Alors la probabilité que $\dim W_{i+1} \leq m - i - 1$ est $1 - o(1)$, où le $o(1)$ ne dépend que de U.*

Démonstration. Si on appelle $V_1, \ldots, V_l$ les $\mathbb{F}_q$-composantes irréductibles de dimension $m-i$ de $(W_i)_{\mathrm{red}}$, alors par une version généralisée du théorème de Bézout (voir [Ful84, p. 10]),

$$l \leq C_U(\deg \partial_1 f) \ldots (\deg \partial_i f) = O(d^i) \text{ lorsque } d \to \infty$$

avec C_U une constante qui dépend uniquement de U.

Remarque 4.21. On notera que le $O(d^i)$ ne dépend que de U.

Maintenant, soit $k \in \{1, \ldots, i\}$. Comme $\dim V_k \geq 1$, il existe un j qui dépend de k tel que la projection de la coordonnée $x_j(V_k)$ soit une variété de dimension 1 (sinon si pour tout j, $x_j(V_k)$ est de dimension 0, alors V_k serait de dimension 0). Il faut contrôler la taille de l'ensemble :

$$G_k := \left\{ g_{i+1} \in A_{\leq \gamma} \;\middle|\; \partial_{i+1} f = \partial_{i+1} f_0 + g_{i+1}^p \partial_{i+1} t_{i+1} \text{ est nul sur } V_k \right\}$$

Or si g et g' sont dans G_k, en prenant la différence et en divisant par $\partial_i t_i$, on voit que $g - g'$ est nul sur V_k. Ainsi, si G_k n'est pas vide, en notant I_k l'idéal de $A_{\leq \gamma}$ des fonctions s'annulant sur V_k, alors tous les éléments de G_k ont la même image dans $A_{\leq \gamma}/I_k$. Donc la probabilité pour que g soit dans G_k est $1/\operatorname{card}(A_{\leq \gamma}/I_k)$. Or la codimension de I_k est plus grande que $\gamma+1$ car tous les polynômes en x_j non nuls ne s'annulent pas sur V_k et $\dim_{\mathbb{F}_q} \mathbb{F}_q[x_j]_{\leq \gamma} = \gamma + 1$, ainsi $\operatorname{card}(A_{\leq \gamma}/I_k) \geq q^{\gamma+1}$. Donc la probabilité que $\partial_{i+1} f$ soit nulle sur l'un des V_k est au plus $l q^{-\gamma-1} = O\left(d^i q^{-(d-\tau)/p)}\right) = o(1)$ lorsque $d \to \infty$. □

Remarque 4.22. Ici, on voit que la démonstration est très similaire au cas du plan. En effet, pour ne pas diminuer la dimension entre W_i et W_{i+1} il faut que $\{\partial_{i+1} f = 0\}$ ait une composante irréductible en commun avec W_i. On a alors utilisé à nouveau le théorème de Bézout pour borner le nombre de composantes irréductibles de W_i et utiliser un argument d'algèbre linéaire pour trouver le résultat.

Lemme 4.23. *Supposons que l'on ait choisi $f_0, g_1, \ldots, g_m$ de sorte que W_m soit de dimension 0. Alors la probabilité que $H_f \cap W_m \cap U_{>d/(m+1)}$ soit vide est $1 - o(1)$ lorsque $d \to \infty$, où le $o(1)$ ne dépend que de U.*

Démonstration. En réutilisant le théorème de Bézout comme dans la preuve précédente on obtient que $\operatorname{card} W_m = O(d^m)$. Pour un point $P \in W_m$, l'ensemble H des $h \in A_{\leq\eta}$ pour lesquels H_f passe par P est soit vide, soit un translaté du noyau de $\ker(\mathrm{ev}_P : A_{\leq\eta} \to k(P))$. Si $\deg P > d/(m+1)$, alors par le lemme 4.18 , on a

$$\frac{\operatorname{card} H}{\operatorname{card} A_{\leq\eta}} \leq q^{-\nu}$$

où $\nu = \min(\lfloor d/p \rfloor + 1, d/(m+1))$, ainsi :

$$\mathbb{P}(H_f \cap W_m \cap U_{>d/(m+1)} \neq \emptyset) \leq \operatorname{card}(W_m) q^{-\nu} = O(d^m q^{-\nu}) = o(1) \text{ lorsque } d \to \infty$$

car ν croît linéairement en d. □

On peut maintenant conclure la preuve du lemme 4.23. Soit $f \in S_d$ choisi aléatoirement. Les deux lemmes précédents montrent qu'avec probabilité $\prod_{i=0}^{m-1}(1-o(1))\cdot(1-o(1)) = 1-o(1)$, on a $\dim W_i = m - i$ pour tout $i = 0, \ldots, m$ et $H_f \cap W_m \cap U_{>d/(m+1)}$ vide. Mais $H_f \cap W_m$ est la sous-variété de U définie par les équations $f(P) = \partial_1 f(P) = \ldots = \partial_m f(P) = 0$, donc $H_f \cap W_m \cap U_{>d/(m+1)}$ est exactement l'ensemble des points de $H_f \cap U$ de degré $> d/(m+1)$ où $H_f \cap U$ n'est pas lisse de dimension $m - 1$.

Preuve des théorèmes

Preuve du théorème 4.12 : Par le lemme 4.15 , on a

$$\lim_{r\to\infty} \mu(\mathcal{P}_r) = \frac{\operatorname{card} T}{\operatorname{card} H^0(Z, \mathcal{O}_Z)} \zeta_U(m+1)^{-1}$$

De plus, la définition des différents ensembles implique que $\mathcal{P} \subseteq \mathcal{P}_r \subseteq \mathcal{P} \cup \mathcal{Q}_r^{moy} \cup Q^{haut}$, donc $\overline{\mu}(\mathcal{P})$ et $\underline{\mu}(\mathcal{P})$ diffèrent de $\mu(\mathcal{P}_r)$ d'au plus $\overline{\mu}(Q_r^{moy}) + \overline{\mu}(Q^{haut})$. Par les lemmes 4.16 et 4.17 , on obtient :

$$\mu(\mathcal{P}) = \lim_{r\to\infty} \mu(\mathcal{P}_r) = \frac{\operatorname{card} T}{\operatorname{card} H^0(Z, \mathcal{O}_Z)} \zeta_U(m+1)^{-1}.$$

□

Preuve du théorème 4.10. Il suffit de prendre $Z = \emptyset$ et $T = \{0\}$ dans le théorème 4.12 . □

5 Applications

Avant de donner quelques applications du théorème 4.12, faisons la remarque suivante : l'appartenance d'un point fermé $P \in \mathbb{P}^n$ à une hypersurface H_f, la régularité de H_f en P ainsi que l'espace tangent peuvent être exprimées par des conditions de Taylor. Cela paraît intuitivement clair ; une condition d'ordre 0 donne la « valeur » de f en P, relative à l'appartenance de P à H_f, et une condition d'ordre 1 donne la valeur en P des dérivées d'ordre 1, relative à l'espace tangent. Explicitons ceci.

Soit x_j la plus petite coordonnée qui ne s'annule pas en P. Les propriétés que nous cherchons à exprimer sont locales : on peut donc se restreindre à l'ouvert affine donné par $x_j \neq 0$, qui est spec(A) où $A = k[x_1/x_j, \ldots, x_n/x_j]$. L'intersection de cet ouvert avec H_f est la variété H'_g donnée par $g := x_j^{-d} f = 0$, où d est le degré de f. Notons $\mathfrak{m}'_P$ l'idéal maximal de A correspondant à P.

Alors H_f passe par P si et seulement si H'_g passe par P, si et seulement si $g \in \mathfrak{m}'_P$. De même pour les propriétés d'ordre 1 : étant donné un sous-espace $V \subset T_{\mathbb{P}^n,P} = T_{\mathrm{spec}(A),P}$ de codimension au plus 1, il existe d'après la section 2.8 un élément $u \in A/\mathfrak{m}'^2_P$ tel que : $T_{H_f,P} = T_{H'_g,P} = V$ si et seulement si la valeur de g modulo $\mathfrak{m}'^2_P$ est u et H_f est lisse en P si et seulement si V est de codimension 1, si et seulement si u est non nul.

D'après la discussion qui précède l'énoncé du théorème 4.12, ce sont précisément des conditions de Taylor (non vides) pour le sous-schéma spec$(A/\mathfrak{m}'^2_P)$ de spec$(A) \subset \mathbb{P}^n$, dont l'espace topologique est le singleton $\{P\}$. Si l'on se donne plusieurs points $P_1, \ldots, P_r$, alors l'intersection de telles conditions de Taylor non vides en chacun des points P_i se traduit en une condition de Taylor globale sur l'union Z des $Z_i = \mathrm{spec}(A_i/\mathfrak{m}'^2_{P_i})$ (vus comme sous-schémas de $\mathbb{P}^n$), qui est non vide : en effet, les Z_i forment une partition de Z en ouverts (topologiquement), donc à chaque r-uplet de fonctions $g_i \in H^0(Z_i, \mathcal{O}_{Z_i})$ correspond une unique fonction de $H^0(Z, \mathcal{O}_Z)$. On a donc montré le résultat suivant :

Lemme 5.1. *Si l'on se donne un nombre fini de points fermés de $\mathbb{P}^n$ avec, pour chaque point, une propriété locale d'ordre 0 ou 1 (au sens défini ci-dessus), alors il existe un sous-schéma fini Z de $\mathbb{P}^n$ et un sous-ensemble $T \subseteq H^0(Z, \mathcal{O}_Z)$ non vide tel que*

$$\forall f \in S_{\mathrm{homog}}, \quad f|_Z \in T \iff H_f \textit{ vérifie toutes les propriétés données}$$

5.1 Optimalité du théorème 4.10

Etant donnée une variété projective lisse X sur k, le théorème 4.10 affirme l'existence d'une hypersurface dont l'intersection avec X est lisse. C'est une sorte de généralisation du « vrai » théorème de Bertini, qui porte sur les corps algébriquement clos ; seulement ce dernier est beaucoup plus fort, puisque dans ce cas l'hypersurface peut être prise de degré 1. Le résultat suivant montre que l'on ne pouvait pas se permettre d'avoir, sur les corps finis, une version moins faible du théorème de Bertini que ne l'est le théorème 4.10.

Théorème 5.2. *Soient $k = \mathbb{F}_q$ un corps fini, $n \geq 2$ et $d \geq 1$ des entiers. Il existe une hypersurface lisse X de $\mathbb{P}^n_k$ telle que pour tout $f \in S_1 \cup \ldots \cup S_d$, $H_f \cap X$ n'est pas une variété lisse de dimension $n-2$.*

Démonstration. Numérotons $f_1, \ldots, f_l$ les éléments de $S_1 \cup \ldots \cup S_d$. Pour chaque $i = 1, \ldots, l$, choisissons un point $P_i \in H_{f_i}$ distinct des P_j déjà choisis (pour $j < i$) ; c'est possible car $f_i = 0$ a une infinité de solutions dans $\bar{k}$. En utilisant le lemme 5.1 et en appliquant le théorème 4.12 à $\mathbb{P}^n$, on obtient $f \in S_{homog}$ vérifiant les deux conditions suivantes : (a) $X := H_f$ est lisse de dimension $n-1$ sauf éventuellement en les P_i, et (b) en chaque P_i, l'espace tangent de X est un hyperplan, qui en plus est égal à celui de H_{f_i} lorsque cette dernière est lisse de dimension $n-1$ en P_i. Alors X est une hypersurface lisse ; et pour chaque $i = 1, \ldots, d$, $X \cap H_{f_i}$ n'est pas une variété lisse de dimension $n-2$ car son espace tangent en P_i est de dimension $n-1$. □

5.2 Courbes remplissant l'espace, variétés évitant l'espace

Sur un corps infini k, un sous-ensemble de k^n défini par un système d'équations polynomiales non nulles (une variété algébrique au sens classique) ne peut être k^n tout entier : en effet, un polynôme non nul donne lieu à une fonction polynomiale non nulle. D'autre part, si k est algébriquement clos et les équations n'ont pas d'incompatibilité algébrique, alors le Nullstellensatz affirme que la variété ne peut pas être vide.

Ceci tombe en défaut lorsque k est un corps fini. Cependant, cela redevient vrai dans le contexte des schémas : un système d'équations a toujours une solution et une non-solution dans $\bar{k}^n$... mais on retrouve ces comportements si l'on borne le degré des points fermés que l'on considère. L'objectif de cette section est d'expliquer ce point.

Théorème 5.3. *Soient X une sous-variété quasiprojective lisse de $\mathbb{P}^n$ de dimension $m \geq 1$ sur $\mathbb{F}_q$ et F un ensemble fini de points fermés de X. Alors existe des hypersurfaces H et H' de $\mathbb{P}^n$, l'une contenant F et l'autre l'évitant, telles que $H \cap X$ et $H' \cap X$ soient lisses de dimension $m-1$.*

Démonstration. On cherche H et H' sous la forme H_f avec $f \in S_{\text{homog}}$, avec dans l'idée d'utiliser le théorème 4.12. Pour H', les conditions de Taylor sont simplement de ne pas passer par les points de F. Pour H, on se fixe, pour chaque point P de F, un hyperplan V_P de $T_{\mathbb{P}^n,P}$ ne contenant pas $T_{X,P}$. Les conditions qu'on demande sur H_f sont alors de passer par les points P de F et d'y avoir V_P pour espace tangent ; ainsi, l'espace tangent de $H_f \cap X$ en P sera $V_P \cap T_{X,P}$, de dimension $m-1$, donc $H_f \cap X$ sera lisse de dimension $m-1$ en P. D'après le lemme 5.1, ceci se traduit par des conditions de Taylor (au sens du théorème 4.12) non vides, ce qui permet de conclure. □

Corollaire 5.4. *Soient X une variété projective lisse de dimension $m \geq 1$ sur $\mathbb{F}_q$, F un ensemble fini de points fermés de X et l un entier entre 1 et $m-1$. Alors il existe des sous-variétés projectives lisses $Y \subset X$ et $Y' \subset X$ de dimension l telles que $F \subset Y$ et $F \cap Y' = \emptyset$.*

Démonstration. On procède par récurrence descendante sur l. L'initialisation est automatique pour Y (on prend X), et elle est fournie par le théoèrme 5.3 pour Y'. Pour l'hérédité : supposons qu'on ait Y_l et Y'_l vérifiant l'énoncé, avec $l > 1$. Le théorème 5.3 fournit Y_{l-1} convenable ; et pour Y'_{l-1}, il suffit de prendre n'importe quelle sous-variété de Y'_l de dimension $l-1$, par exemple une fournie par le théorème 4.10. □

Corollaire 5.5 (Courbes remplissant l'espace)**.** *Soient X une variété projective lisse de dimension $m \geq 1$ sur $\mathbb{F}_q$ et E une extension finie de $\mathbb{F}_q$. Alors il existe une courbe projective lisse $Y \subset X$ telle que $Y(E) = X(E)$.*

Démonstration. C'est une application du corollaire 5.4 avec $l = 1$ et F l'ensemble des points fermés correspondant à $X(E)$, c'est-à-dire les points de degré divisant $[E : \mathbb{F}_q]$ (d'après la proposition 3.2). □

Corollaire 5.6 (Variétés évitant l'espace)**.** *Soient X une variété projective lisse de dimension $m \geq 2$ sur $\mathbb{F}_q$, E une extension finie de $\mathbb{F}_q$ et l un entier entre 1 et $m-1$. Alors il existe une sous-variété projective $Y \subset X$ de dimension l telle que $Y(E) = \emptyset$.*

Démonstration. Comme pour les courbes remplissant l'espace, c'est une application directe du corollaire 5.4 avec F l'ensemble des points fermés de X de degré divisant $[E : \mathbb{F}_q]$. □

5.3 Singularités de dimension positive

Présentons ici une troisième application des résultats de Poonen. Ce ne sera pas une application du théorème de Bertini à proprement parler, mais plutôt une conséquence de la preuve.

Soit X une sous-variété quasiprojective lisse de $\mathbb{P}^n_k$ de dimension m sur $k = \mathbb{F}_q$. Etant donné $f \in S_{\text{homog}}$, notons $(H_f \cap X)_{\text{sing}}$ l'ensemble des points en lesquels $H_f \cap X$ n'est pas lisse de dimension $m-1$. L'intersection de cet ensemble avec chaque ouvert affine est le lieu d'annulation simultanée des $\frac{\partial \widetilde{f}}{\partial \widetilde{x_i}}$, où $\widetilde{f}$ est la déhomogénéisation de f sur cet ouvert affine et les $\widetilde{x_i}$ sont les coordonnées déhomogénéisées, donc est fermé. Ainsi $(H_f \cap X)_{\text{sing}}$ est fermé.

Le théorème 4.10 montre que pour X non vide, la probabilité que $(H_f \cap X)_{\text{sing}}$ soit non vide est non nulle. En revanche, lorsque c'est le cas, ce fermé est presque sûrement de dimension zéro : c'est ce qu'on montre ici.

Théorème 5.7. *Soit X une sous-variété quasiprojective lisse de $\mathbb{P}^n_k$ de dimension $m \geq 0$. Notons*

$$\mathcal{S} := \{f \in S_{\text{homog}} \mid \dim (H_f \cap X)_{\text{sing}} \geq 1\}$$

Alors $\mu(\mathcal{S}) = 0$.

Démonstration. Si $(H_f \cap X)_{\text{sing}}$ est de dimension non nulle, alors il est infini (sinon il serait discret donc de dimension 0). Il contient donc en particulier des points fermés de degrés aussi grand qu'on veut. Ainsi, en reprenant les notations du lemme 4.19, $S \subset Q^{haut}$. Il suffit alors de prendre $U = X$ dans ce lemme pour avoir la conclusion. □

A Résultats d'algèbre

On énonce ici quelques résultats classiques d'algèbre commutative. Les démonstrations peuvent se trouver dans n'importe quel livre sur le sujet, par exemple [Lan05].

Théorème A.1. *Si A est un anneau factoriel (resp. noethérien), alors $A[X_1, \ldots, X_n]$ est factoriel (resp. noethérien).*

Théorème A.2 (Lemme de normalisation de Noether)**.** *Soit A une algèbre de type fini sur un corps k. Alors il existe un entier d et un morphisme injectif fini $k[T_1, \ldots, T_d] \hookrightarrow A$.*

Théorème A.3. *Soient A un anneau commutatif unitaire et I un idéal de A. Le radical $\sqrt{I}$ de I est l'intersection des idéaux premiers contenant I. En particulier, le nilradical de A (l'ensemble des nilpotents) est l'intersection de tous les idéaux premiers de A.*

Références

[Ful84] William Fulton. *Introduction to Intersection Theory in Algebraic Geometry*. Number no. 54 in Conference board of the mathematical science. Conference Board of the Mathematical Sciences, 1984.

[Har10] David Harari. Géométrie algébrique. `http://www.math.u-psud.fr/~harari/enseignement/geoalg/cours.pdf`, 2010.

[Lan05] Serge Lang. *Algebra*. Graduate Texts in Mathematics. Springer New York, 2005.

[LW54] Serge Lang and André Weil. Number of points of varieties in finite fields. *American Journal of Mathematics*, 76(4) :819–827, 1954.

[Mus11] Mircea Mustaţă. Zeta functions in algebraic geometry. `http://www.math.lsa.umich.edu/~mmustata/zeta_book.pdf`, 2011.

[Poo04] Bjorn Poonen. Bertini theorems over finite fields. *Annals of mathematics*, 160(3) :1099–1127, 2004.

[Poo14] Bjorn Poonen. Selmer group heuristics and sieves. `http://www-math.mit.edu/~poonen/papers/aws2014.pdf`, 2014.