Magistère de Mathématiques Fondamentales et Appliquées et d'Informatique

Mémoire de Magistère

École Normale Supérieure

Nicolas Ratazzi

octobre 2001

Table des matières

1 Introduction au thème de recherche **4**
1.1 Hauteur d'un point 5
1.2 Approximation diophantienne 6
1.2.1 Schéma général 6
1.2.2 Lemmes de Siegel 7
1.2.3 Lemmes de zéros 7
1.2.4 Applications du schéma de démonstration 8
1.3 Hauteur sur les variétés 9
1.3.1 Théorie de l'intersection arithmétique 9
1.3.2 Degré et hauteur 11
1.3.3 Propriétés fondamentales 13
1.3.4 Applications 14

2 Théorème de Bombieri-Vaaler **15**
2.1 Introduction 16
2.2 Hauteurs, mesures quelques rappels 16
2.2.1 Hauteurs 17
2.2.2 Module d'un corps localement compact 17
2.2.3 Mesure de Haar et Adèles 18
2.3 Théorème de Minkowski adélique 19
2.4 Le cube slicing 23
2.4.1 Le théorème de Vaaler 23
2.4.2 Cube slicing inequality 26
2.5 Théorèmes de Siegel 28
2.6 Une application 30

3 Mémoire de DEA : Lemme de Esnault-Viehweg-Dyson **32**
3.1 Rappels de géométrie algébrique 34
3.1.1 Les différentielles 34
3.1.2 Normalisation et applications propres 36
3.1.3 Morphismes entre courbes 38
3.1.4 Les diviseurs 38
Diviseurs de Weil et de Cartier 38

Diviseurs et fibrés en droite . . . 39
3.1.5 Éclatements . . . 40
Construction de **Proj** . . . 40
Éclatements . . . 41
3.1.6 Formule de la projection pour les faisceaux . . . 44
3.2 Théorie de l'intersection . . . 45
3.2.1 Ordre des zéros et des pôles . . . 46
3.2.2 Cycles et équivalence rationnelle . . . 46
3.2.3 Image directe de cycles . . . 47
3.2.4 Degré d'un cycle . . . 51
3.2.5 Degré et polynôme de Hilbert . . . 52
Schémas projectifs . . . 52
Polynôme de Hilbert . . . 52
3.2.6 Image réciproque plate de cycles . . . 55
3.2.7 Intersection avec des diviseurs . . . 56
3.2.8 Commutativité des classes d'intersection . . . 58
3.2.9 Classe de Chern d'un fibré en droites . . . 61
3.2.10 Diviseurs numériquement effectifs . . . 62
3.3 Le lemme de Dyson selon M. Nakamaye. . . . 65
3.3.1 Énoncé des théorèmes . . . 65
Indice d'une section . . . 65
Le lemme de Dyson . . . 66
3.3.2 Le faisceau d'idéaux $\mathcal{I}_d(s)$ . . . 67
Les faisceaux d'idéaux $\mathcal{I}_d(s)$ et $\mathfrak{I}_{\zeta,d,t}$ . . . 67
Le support de $O_{\mathbb{P}}/\mathcal{I}_{\zeta,d,t}$ . . . 68
Un calcul de volume . . . 70
3.3.3 Le théorème du produit . . . 71
3.3.4 Fin de la preuve du théorème 3.3.2 . . . 74
Le lemme clé . . . 74
Construction du cycle effectif . . . 76
Minoration de deg R_i . . . 77
Conclusion . . . 78
3.3.5 Preuve du théorème 3.3.1 . . . 80

A Groupes formels de Lubin Tate **82**
A.1 Préliminaires . . . 83
A.2 Groupes formels . . . 83
A.2.1 Définitions . . . 83
A.2.2 Le lemme fondamental . . . 84
A.3 L'extension totalement ramifiée K_π . . . 86
A.3.1 Premières propriétés . . . 87
A.3.2 L'extension K_π/K et son groupe de Galois . . . 88
A.4 L'extension L_π . . . 89

A.5 Sous-groupes de ramification 91
A.5.1 “Rappels” 91
A.5.2 Sous-groupes de ramification 91

B Mémoire de maitrise : Théorie de Galois différentielle 93
B.1 Introduction 94
B.2 Préliminaires 94
B.2.1 Dérivations et corps différentiels 94
B.2.2 Le groupe de Galois différentiel 96
B.3 Strucure algébrique du groupe de Galois différentiel 96
B.3.1 La topologie de Zariski 96
B.3.2 Deux lemmes algébriques 97
B.3.3 La structure algébrique de $Gal_\partial(M/K)$ 98
B.4 Outils d’algèbre différentielle 100
B.4.1 Extension d’idéaux premiers 100
B.4.2 Un lemme sur les anneaux de polynômes 101
B.4.3 Les isomorphismes admissibles 102
B.5 Le coeur de la théorie 103
B.5.1 Préliminaires et compléments 103
B.5.2 Normalité de l’extension de Picard-Vessiot 104
B.5.3 Complétion de la théorie de Galois différentielle 105
B.6 Résolution par quadrature des équations différentielles linéaires 106
B.6.1 Étude des extensions de Liouville 107
B.6.2 Deux lemmes sur les groupes algébriques linéaires 108
B.6.3 Trigonalisation simultanée d’automorphismes 109
B.6.4 Démonstration du théorème VI.1 110
B.6.5 Application à l’équation de Riccati 112

Chapitre 1

Introduction au thème de recherche

Sommaire

1.1 Hauteur d'un point **5**
1.2 Approximation diophantienne **6**
1.2.1 Schéma général 6
1.2.2 Lemmes de Siegel 7
1.2.3 Lemmes de zéros 7
1.2.4 Applications du schéma de démonstration 8
1.3 Hauteur sur les variétés **9**
1.3.1 Théorie de l'intersection arithmétique 9
1.3.2 Degré et hauteur 11
1.3.3 Propriétés fondamentales 13
1.3.4 Applications 14

1.1 Hauteur d'un point

Dans toute la suite, on note k un corps de nombres (i.e. une extension finie de $\mathbb{Q}$) et on note $[k:\mathbb{Q}]$ son degré. On note M_k l'ensemble des valeurs absolues sur k. On normalise la valeur absolue p-adique par : $|p|_p = p^{-1}$, et on note $d_v = [k_v : \mathbb{Q}_v]$ le degré local, où k_v désigne le complété de k pour la topologie définie par v.

Définition 1.1.1 Soit $x = (x_0 : ... : x_n) \in \mathbb{P}_n(k)$, on définit la *hauteur (logarithmique absolue)* de x par :

$$h(x) = \sum_{v \in M_k} \frac{d_k}{[k:\mathbb{Q}]} \log \max\{|x_0|_v,...,|x_n|_v\}.$$

On note facilement que cette définition est indépendante du corps k et du choix d'un système de coordonnées projectives pour le point x. Ceci nous permet d'étendre la définition à un point $x \in \mathbb{P}_n(\overline{\mathbb{Q}})$. Par ailleurs, le plongement naturel $\overline{\mathbb{Q}} \hookrightarrow \mathbb{P}_1(\overline{\mathbb{Q}})$ qui à x associe $(1:x)$ nous permet de définir la hauteur d'un point de $\overline{\mathbb{Q}}$ par : $h(x) = h(1:x)$.
L'objectif de cette notion de hauteur est de définir une fonction qui, d'une part, mesure la "complexité" arithmétique du point (de manière simpliste, $\frac{999}{1000}$ est plus compliqué que 1), d'autre part vérifie certaines propriétés de finitude. La nature arithmétique de la hauteur découle de la définition. Le théorème suivant nous donne la propriété de finitude fondamentale de la hauteur. Ce résultat simple est utilisé dans la majorité des démonstrations de théorèmes de géométrie diophantienne (par exemple, cf. plus loin, les théorèmes de Siegel, Faltings...).

Théorème 1.1.1. *(Northcott) Soit d et h deux réels positifs. L'ensemble :*

$$\left\{x \in \mathbb{P}_n(\overline{\mathbb{Q}}) /\ [\mathbb{Q}(x):\mathbb{Q}] \leq d,\ h(x) \leq h\right\}$$

est fini. Notamment, l'ensemble des points appartenant à un corps k fixé et de hauteur bornée, est fini.

Corollaire 1.1.1. *(Kronecker) Soit k un corps de nombre, et soit $x = (x_0 : \ldots : x_n)$ un point de $\mathbb{P}_n(k)$ tel que pour un certain i, x_i est non nul. Alors :*

$$h(x) = 0 \qquad \Longleftrightarrow \qquad \forall j \in [\![0,n]\!] \ \ \frac{x_j}{x_i} \in \mu_\infty \ \text{ou}\ \frac{x_j}{x_i} = 0.$$

Le dernier point important concernant la hauteur des points est la positivité : pour tout point x, $h(x)$ est positif ou nul.

Ces résultats appellent naturellement deux questions :

1. Le théorème de Kronecker caractérise les points de hauteur nulle, et on sait donc, si $x \in \overline{\mathbb{Q}}$, que si $x \notin \mu_\infty$ alors $h(x) > 0$. Question : comment minorer $h(x)$? On constate que pour $x = 2^{\frac{1}{d}}$, on a $h(x) = \frac{\log 2}{d}$ qui tend vers zéro quand d tend vers $+\infty$. Ainsi on ne

peut minorer $h(x)$ au mieux que par une fonction de d. Une conjecture de Lehmer (1932) indique que le cas particulier précédent est essentiellement le pire :
Conjecture 1.1.1. *Il existe une constante $c > 0$ telle que $\forall x \in \overline{\mathbb{Q}}$, on a :*

$$d = [\mathbb{Q}[x] : \mathbb{Q}] \Longrightarrow h(x) \geq \frac{c}{d}.$$

Cette conjecture est toujours une question ouverte mais on a quand même un certain nombre de réponses partielles. En 1979, Dobrowolski [Dob79] a montré que $h(x) \geq \frac{c}{d}\left(\frac{\log(\log d)}{log d}\right)^3$, et en 1999 Amoroso et David [AD99] ont montré que la conjecture de Lehmer est vraie si l'extension $\mathbb{Q}[x]/\mathbb{Q}$ est normale.

2. On peut aussi se demander si on ne pourrait pas généraliser la notion de hauteur d'un point à celle de hauteur d'une variété (un point étant vu comme une variété de dimension 0). La réponse à cette question est affirmative et découle de la théorie de l'intersection arithmétique. On retrouve encore (cf. [BGS94]) des résultats de finitude du même type que le théorème de Northcott.

1.2 Approximation diophantienne

1.2.1 Schéma général

Un grand nombre de démonstrations en théorie de la transcendance et de l'approximation diophantienne suivent le même schéma : on construit un polynôme auxiliaire F qui s'annule avec un grand ordre en un certain nombre de points approximants, puis on borne l'ordre d'annulation de F en ces points afin d'en tirer une contradiction. On peut illustrer ceci en donnant la démonstration (très simple) du théorème de Liouville : "Soit $x \in \overline{\mathbb{Q}}$ de degré $d \geq 2$, et soit $\varepsilon > 0$, alors il existe seulement un nombre fini de rationnels $\frac{p}{q} \in \mathbb{Q}$ tels que :

$$\left|\frac{p}{q} - x\right| \leq \frac{1}{q^{d+\varepsilon}}."$$

Démonstration : *étape 1 : construction du polynôme.* Dans ce cas précis, le choix évident est de prendre le polynôme F minimal de x, à coefficients dans $\mathbb{Z}$.
Étape 2 : le polynôme s'annule en certains points approximant $\frac{p}{q}$. On suppose que $\frac{p}{q}$ est proche de x et que q est grand, on veut montrer que $F(\frac{p}{q}) = 0$. F est de degré d et à coefficients entiers, donc : $F(\frac{p}{q}) = \frac{N}{q^d}$ pour un entier N. On effectue alors un développement de Taylor en x et on obtient une estimation du type :

$$\left|\frac{N}{q^d}\right| \leq \frac{C(x)}{q^{d+\varepsilon}} \text{ où } C(x) \text{ est une constante dépendant uniquement de } x.$$

On en déduit que $|N| \leq \frac{C(x)}{q^{\varepsilon}}$. Or N est entier, donc pour q assez grand $N = 0$, i.e., $F(\frac{p}{q}) = 0$.

Étape 3 : borne sur l'ordre d'annulation. Le polynôme F est minimal, donc $\frac{p}{q}$ annule F à l'ordre 0.
Étape 4 : contradiction. Si on avait une infinité de rationnels approximants, l'étape 2 montre que pour q assez grand $F(\frac{p}{q}) = 0$ et l'étape 3 indique au contraire que $\frac{p}{q}$ n'annule pas F, d'où la contradiction. □

Cette version se généralise en le théorème de Roth, mais on peut remarquer que la même démonstration fournit facilement la version suivante du théorème de Liouville : "soit x de degré d, il existe une constante $C(x)$ telle que pour tout rationnel $\frac{p}{q}$, on a $\left|\frac{p}{q} - x\right| \geq \frac{C(x)}{q^d}$."

1.2.2 Lemmes de Siegel

Dans l'exemple précédent l'étape 3 est très facile, mais ceci n'est qu'illusoire : cela provient du fait que le polynôme F est en une variable. Dans la plupart des cas, c'est justement cette étape qui est la plus difficile. En général, l'étape 1 est assez facile, et se montre en utilisant des lemmes du type lemme de Siegel (on trouvera un lemme de Siegel assez fin, le théorème de Bombieri-Vaaler, au chapitre 3 de ce mémoire). Ces lemmes sont essentiellement des généralisations du principe des tiroirs :

Théorème 1.2.1. *(Siegel version 1) Soit $A \in \mathcal{M}_{m,n}(\mathbb{Z})$ et $m < n$, alors, il existe $X \in \mathbb{Z}^n$ non nul tel que :*

$$||X||_\infty \leq (n||A||_\infty)^{\frac{m}{n-m}}, \text{ et } AX = 0.$$

Théorème 1.2.2. *(Siegel version 2) Soit k un corps de nombres de degré d. Soit m et $n > md$ deux entiers positifs, et soit $\delta \geq \frac{md}{n-md}$ réel strictement positif. Soit L_1,..., L_m des formes linéaires en n variables à coefficients dans k, avec $\forall i \leq m \quad h(L_i) \leq h$. Alors, il existe $X \in \mathbb{Z}^n - \{0\}$ tel que $\forall i \leq m$, $L_i(X) = 0$, et $h(X) \leq \delta(h + \log n)$.*

En simplifiant légérement, les deux versions affirment l'existence d'une solution entière x non triviale (d'un système ayant plus d'inconnues que d'équations) vérifiant

$$h(x) \lessapprox h(\text{équations}) \times \frac{d \times \text{nombre d'équations}}{\text{nombre d'inconnues} - d \times \text{nombre d'équations}}.$$

1.2.3 Lemmes de zéros

Une méthode de démonstration de l'étape 3 consiste à utiliser des lemmes de zéros. On peut classer les lemmes de zéros en deux catégories : d'une part les lemmes initialement dus à Masser-Wüstholz puis généralisés par Philippon (cf. par exemple [Phi86]), d'autre part le lemme de Dyson, généralisé par Esnault-Viehweg ([EV84]) pour s'appliquer à des polynômes en un nombre quelconque de variables. L'énoncé précis du lemme de Esnault-Viehweg-Dyson est assez technique ; on le trouvera avec une démonstration (suivant Nakamaye) au chapitre 4 de ce mémoire. On donne par contre, dès à présent, un lemme suivant la philosophie de Masser-Wüstholz.

Soit k un corps de nombres, $x \in \mathbb{G}_m^n(k)$, et soit $N_1, \dots, N_n$ des entiers strictement positifs. On note $\mathcal{P}_j \subset [\![1,N_j]\!]$, $j \in [\![1,n]\!]$ et $\sum_j = \{x^{p_j \dots p_n} \ / \ (p_j,\dots,p_n) \in \mathcal{P}_j \times \dots \times \mathcal{P}_n\}$, et $\sum_{n+1} = \{x\}$. On a alors

Lemme 1.2.1. *(Lemme de zéros) Soit $F \in \mathbb{Q}[X_1,\dots,X_n]$ un polynôme non identiquement nul de degré inférieur à L et s'annulant sur $\sum_1$. Il existe un entier $r \in [\![1,n]\!]$ et une sous variété algébrique V propre et $\mathbb{Q}$-irréductible de $\mathbb{G}_m^n(\overline{\mathbb{Q}})$, rencontrant $\sum_{r+1}$ et telle que :*

$$codim(V) \leq r \quad et \quad deg\left(\bigcup_{p \in \mathcal{P}_r} [p]V\right) \leq (N_1 \dots N_r L)^{codim}(V).$$

1.2.4 Applications du schéma de démonstration

Le schéma de démonstration que l'on vient d'esquisser a été extrêmement fructueux, on donne ici quelques applications. Dans toutes ces applications la hauteur intervient essentiellement de la manière suivante : en utilisant le théorème de Northcott, on montre qu'un ensemble de points est fini en montrant que cet ensemble est de hauteur bornée.

Théorème 1.2.3. *(Théorème de Roth) Soit $\varepsilon > 0$ et soit $x \in \overline{\mathbb{Q}}$. Alors, l'équation*

$$\left| x - \frac{p}{q} \right| \leq \frac{1}{q^{2+\varepsilon}}$$

n'a qu'un nombre fini de solutions $\frac{p}{q} \in \mathbb{Q}$.

On peut trouver une preuve de ce théorème suivant le schéma de démonstration indiqué précédemment dans [EV84] : la preuve du théorème de Roth utilise toute la puissance du lemme de Esnault-Viehweg (et pas simplement la version à 2 variables due à Dyson et qui ne permet d'obtenir qu'un exposant $\sqrt{2[\mathbb{Q}(x) : \mathbb{Q}]} + \varepsilon$ au lieu du $2 + \varepsilon$ obtenu ici). Notons que dans le cas d'un nombre quadratique, on retrouve le théorème de Liouville.

On donne maintenant un cas particulier d'un théorème de Siegel concernant les courbes affines. On note R_S l'anneau des S-entiers de k un corps de nombres, avec S un ensemble fini de places, c'est-à-dire :

$$R_S = \{x \in k \ / \ |x|_v \leq 1 \ \forall v \in M_k, \, v \notin S\}.$$

Théorème 1.2.4. *(Théorème de Siegel) Soit S un ensemble fini de places d'un corps de nombres k contenant les places à l'infini. Soit $f \in k[X]$ un polynôme à racines simples et de degré supérieur à 3. Alors l'équation $y^2 = f(x)$ n'a qu'un nombre fini de solutions dans R_S.*

Théorème 1.2.5. *(Conjecture de Mordell : théorème de Faltings) Soit C une courbe projective au-dessus d'un corps de nombre k, de genre $g \geq 2$, alors $C(k)$ est fini.*

Avant d'énoncer le théorème suivant, qui est une généralisation en dimension supérieure du théorème de Dobrowolski concernant le problème de Lehmer, on définit *l'indice d'obstruction* $\delta(x)$ d'un point $x \in \mathbb{G}_m^n(\overline{\mathbb{Q}})$ comme étant le degré d'un polynôme de degré minimal annulant x.

Théorème 1.2.6. *(Amoroso-David) Pour tout entier $n \geq 1$, il existe un nombre réel $c(n) > 0$, tel que pour tout élément $x \in \mathbb{G}_m^n(\overline{\mathbb{Q}})$, dont les coordonnées sont multiplicativement indépendantes, on ait*

$$h(x) \geq \frac{c(n)}{\delta(x)} \log(3\delta(x))^{-\kappa(n)}, \text{ avec } \kappa(n) = (n+1)(n+1)!^n - n.$$

La démonstration de ce théorème, que l'on trouve dans [AD99], utilise le lemme de Philippon avec multiplications. On obtient en corollaire de ce résultat une réponse affirmative à la conjecture de Lehmer dans le cas où l'extension $\mathbb{Q}[x]/\mathbb{Q}$ est normale.

1.3 Hauteur sur les variétés

1.3.1 Théorie de l'intersection arithmétique

Soit k un corps de nombres de degré $[k : \mathbb{Q}]$, O_k son anneau d'entiers et $S = \mathrm{Spec}(O_k)$ le schéma affine associé. On rappelle que, par définition, l'ensemble sous-jacent à Spec (A) (A un anneau) est l'ensemble des idéaux premiers de A. De plus, on dit que X est un *schéma* si il est localement de la forme Spec A. Pour tout plongement $\sigma : k \hookrightarrow \mathbb{C}$ et pour tout k-schéma ou S-schéma, on note X_σ le $\mathbb{C}$-schéma déduit de X par le changement de base σ. On constate que $X(\mathbb{C})$, comme schéma sur $\mathbb{Z}$, s'identifie avec l'union disjointe des X_σ. Dans ce qui suit, on appellera *variété arithmétique, projective, régulière*, tout schéma X régulier, plat et projectif sur S, et dont la fibre générique $X \times_S K$ est régulière. Moralement (en regardant la variété comme étant au-dessus de $\mathbb{Z}$), on considère un système d'équations polynômiales homogènes à coefficients dans $\mathbb{Z}$

$$f_1(x_0, \ldots, x_N) = \ldots = f_k(x_0, \ldots, x_N) = 0.$$

Ce système définit le schéma projectif $X = \mathrm{Proj}(S)$, où S est le quotient (sans torsion du fait des hypothèses) de $\mathbb{Z}[X_0, \ldots, X_N]$ par l'idéal engendré par $f_1, \ldots, f_k$. Les points de X sont les idéaux homogènes premiers de S non contenus dans l'idéal irrelevant. La projection $\pi : X \to \mathrm{Spec}(\mathbb{Z})$ est définie par $\mathcal{P} \mapsto \mathcal{P} \cap \mathbb{Z}$. Les fibres de π sont les $\pi^{-1}(p\mathbb{Z}) = X/p = \mathrm{Proj}(S/pS)$ pour p premier, et $\pi^{-1}((O)) = X_\mathbb{Q} = \mathrm{Proj}(S \otimes \mathbb{Q})$. La variété X est régulière et plate, donc X/p est une variété lisse sur $\mathbb{F}_p$, pour tout p sauf un nombre fini où la variété n'est même pas forcément réduite.

On va esquisser la construction de la hauteur d'une variété arithmétique projective régulière selon Bost-Gillet-Soulé [BGS94], généralisant ainsi la notion de hauteur d'un point. On va notamment voir que l'on retrouve la fondamentale propriété de finitude, des résultats de positivité, et une analogie importante avec la notion de degré géométrique. La construction se fait en plusieurs étapes. On commence par définir un groupe de Chow arithmétique $\widehat{CH}^*(X)$. Sans trop entrer dans les détails, disons qu'un élément z de $\widehat{CH}^p(X)$ est une classe (Z,g) où Z est une classe de cycle de codimension p appartenant au groupe de Chow $CH^p(X)$ et où g est une classe de courant de Green pour $Z(\mathbb{C})$. Un courant de Green g pour un cycle analytique Z de codimension p étant par définition une forme différentielle réelle de type $(p-1,\, p-1)$ à coefficients des distributions, tel que si F_∞ est l'involution antiholomorphe provenant de la conjugaison complexe, si $d = \partial + \overline{\partial}$ et $d^c = \frac{i}{4\pi}(\partial - \overline{\partial})$, et si δ_Z est le courant d'intégration sur Z, on a

$$F_\infty^*(g) = (-1)^p g \ \text{ et } \ dd^c g + \delta_Z \ \text{ est une forme différentielle lisse de type } (p,p),$$

où on injecte l'espace des formes différentielles dans celui des courants par

$$\omega \mapsto [\eta \mapsto \int \eta \wedge \omega].$$

Tout morphisme $f : X \to Y$ de variété arithmétique régulière induit un morphisme contravariant de groupe

$$f^* : \widehat{CH}^p(Y) \to \widehat{CH}^p(X) \text{ défini “formellement” par } f^*[(Z,g)] = [(f^*Z, f_{\mathbb{C}}^* g)].$$

Quand X et Y sont de plus équidimensionnelles, que f est propre et que sa restriction à $X_k = X \times \mathrm{Spec}(k)$ est lisse, alors on peut aussi définir un morphisme image directe

$$f_* : \widehat{CH}^p(X) \to \widehat{CH}^{p-\delta}(Y) \ \text{ par } f_*[(Z,g)] = [(f_*Z, f_{\mathbb{C}*})],$$

où $\delta = \dim X - \dim Y$. Au niveau des groupes de Chow $CH^*(X)$, ces deux morphismes sont définis rigoureusement dans les rappels de théorie de l'intersection au chapitre 4 de ce mémoire. Dans ce même chapitre, on définit un produit d'intersection $X \cdot Y$ pour des classes de cycles X et Y de codimension 1. Ce produit d'intersection s'étend en un produit d'intersection $X \cdot Y$ pour des classes de cycles X et Y de codimensions quelconques. Dans le cas de schémas de type fini au-dessus d'un corps on trouve une construction dans [Ful98]. Dans le cas d'un schéma noethérien et régulier, on trouve une construction, à valeur dans le groupe de Chow tensorisé par $\mathbb{Q}$, dans [SABK92]. On définit ensuite un star-produit pour des courants de Green $g_1 * g_2$. Cela nous permet de construire un produit d'intersection arithmétique :

$$\widehat{CH}^p(X) \otimes \widehat{CH}^q(X) \to \widehat{CH}^{p+q}(X) \otimes \mathbb{Q}.$$

On retrouve alors toutes les propriétés classiques, comme, la formule de la projection : sous de bonnes hypothèses (par exemple si f est propre et plat), on a

$$f_*(x \cdot f^*(y)) = f_*(x) \cdot y.$$

Soit $\overline{L}$ un fibré en droites hermitien sur une variété arithmétique X, c'est-à-dire un couple (L, h) où L est un O_X-module localement libre de rang 1, et h un produit scalaire hermitien de classe C^∞ sur le fibré holomorphe $L_{\mathbb{C}}$, invariant par F_∞. On définit la *première classe de Chern de* $\overline{L}$, $\hat{c}_1(\overline{L})$ comme étant la classe de $(\mathrm{div}(s), -\log ||s||^2)$ pour toute section s de $H^0(X,L)$ de norme $||s||$ sur $X(\mathbb{C})$. On définit de plus la forme $c_1(\overline{L})$ comme étant la forme lisse associée au courant défini par $\hat{c}_1(\overline{L})$.

1.3.2 Degré et hauteur

Dans le cas $X = S = \mathrm{Spec}(O_k)$ les groupes $\widehat{CH}^p(X)$ s'annulent pour tout $p > 1$. On note par

$$\deg_k \ : \ \widehat{CH}^*(S) \to \mathbb{Z} \text{ la projection sur } \widehat{CH}^0(X) \simeq CH^0(X) \simeq \mathbb{Z} \text{ ,et par}$$

$$\widehat{\deg} \ : \ \widehat{CH}^*(X) \to \mathbb{R},$$

le degré arithmétique $\widehat{\deg}$ défini comme étant la projection sur $\widehat{CH}^1(S)$ suivie du morphisme $\widehat{CH}^1(S) \to \widehat{CH}^1(\mathrm{Spec}(\mathbb{Z}))$ (attaché à l'unique morphisme de S sur $\mathrm{Spec}(\mathbb{Z})$ qui, à un idéal premier $\mathcal{P}$ de O_k, associe sa restriction à $\mathbb{Z}$), et suivi de l'isomorphisme $\widehat{CH}^1(\mathrm{Spec}(\mathbb{Z})) \simeq \mathbb{R}$ qui, à la classe $(0,2\lambda)$, associe le réel λ.
En récitant les définitions de tous les objets, on voit qu'un élément de $Z^1(S)$ est un couple $(\sum_{\mathcal{P}} n_{\mathcal{P}},\lambda)$ où $\mathcal{P}$ est un élément de S, $n_{\mathcal{P}}$ un entier presque toujours nul, et λ une application qui, à un plongement σ, associe un réel $\lambda(\sigma)$ tel que $\lambda(\sigma) = \lambda(\overline{\sigma})$. On montre alors que

$$\widehat{\deg}\left(\sum_{\mathcal{P}} n_{\mathcal{P}},\lambda\right) = \sum_{\mathcal{P}} n_{\mathcal{P}} \log(N\mathcal{P}) + \frac{1}{2} \sum_{\sigma \ : \ k \to \mathbb{C}} \lambda(\sigma),$$

où $N\mathcal{P}$ est la norme de $\mathcal{P}$.
Par ailleurs, comme le produit de deux éléments de $\widehat{CH}^1(S)$ s'annule (car il appartient à $\widehat{CH}^2(S) = 0$), la structure multiplicative de $\widehat{CH}^*(S)$ est simplement donnée par sa structure de $\mathbb{Z} = \widehat{CH}^0(S)$-module. En particulier, on a

$$\deg_k(xy) = \deg_k(x)\deg_k(y), \ \text{ et } \ \widehat{\deg}(xy) = \widehat{\deg}(x)\deg_k(y) + \deg_k(x)\widehat{\deg}(y).$$

On définit maintenant l'accouplement $\widehat{CH}^*(X) \times Z_*(X) \to \widehat{CH}^*(\mathrm{Spec}(O_k)) \otimes \mathbb{Q}$. Pour cela, on suppose que X est une variété arithmétique, régulière, projective et équidimensionnelle, de dimension d. Soit p et q deux entiers positifs, soit $Y \in Z_p(X)$ un cycle de dimension p et soit $x \in \widehat{CH}^q(X)$ une classe de cycle arithmétique de codimension q. On va définir, en suivant [BGS94], un élément $(x|Y) \in \widehat{CH}_{p-q}(S) \otimes \mathbb{Q} = \widehat{CH}^{q-p+1}(S) \otimes \mathbb{Q}$:

Quand p est différent de q et de $q+1$, on pose $(x|Y) = 0$.

Quand $p = q$, on pose $(x|Y) = \pi_*[(Z \cdot Y, g\delta_Y)] = [(\pi_*(Z \cdot Y), \pi_*(g\delta_Y))] \in \widehat{CH}^1(S) \otimes \mathbb{Q}$, où (Z,g) est un représentant "convenable" de x.

Quand $p = q+1$, on note $z(x)$ la projection de x dans le groupe de Chow $CH^*(X)$, et on note $z(Y)$ la classe de Y. On pose alors $(x|Y) = \pi_*(z(x) \cdot z(Y)) \in CH^0(S) = \widehat{CH}^0(S) = \mathbb{Z}$.

On peut maintenant définir la hauteur d'une variété X arithmétique, projective, régulière, et plus généralement la hauteur d'un cycle d'une telle variété. Soit X une telle variété, et soit $\overline{L} = (L,h)$ un fibré en droite hermitien sur X. Pour tout cycle $Z \in Z_p(X)$ de dimension p, on définit la *hauteur de Z relativement à $\overline{L}$* comme étant le réel

$$h_{\overline{L}}(Z) = \widehat{\deg}\left(\widehat{c}_1(\overline{L})^p | Z\right) \in \mathbb{R}.$$

On a en particulier

$$h_L(X) = \widehat{\deg}(\widehat{c}_1(\overline{L})^p).$$

Un point important est de noter que cette hauteur est définie par analogie au degré

$$deg_{L_k}(Z) = \pi_{k*}\left(c_1(L_k)^{p-1}[Z_k]\right) = deg_k\left(\widehat{c}_1(\overline{L})^{p-1}|Z\right) \in \mathbb{Z}.$$

Donnons quelques exemples pour illustrer cette notion. Tout d'abord, on peut montrer que si Z est le cycle attaché à un point rationnel $P \in \mathbb{P}^n(k)$, et si on considère le fibré trivial $\overline{L} = \overline{O(1)}$, alors on retrouve la hauteur classique, munie de la norme $\mathbb{L}^2$ à l'infini (au lieu de la norme infinie dans la définition donnée précédemment). Par ailleurs, on montre par récurrence que

$$h_{\overline{O(1)}}(\mathbb{P}^N_{\mathbb{Z}}) = \frac{1}{2}\sum_{p=1}^{N}\sum_{j=1}^{p}\frac{1}{j}.$$

Si $P \in \mathbb{Z}[X_0, \ldots, X_N]$ est un polynôme homogène de degré d non nul, et si Y est le cycle défini dans $\mathbb{P}^n_{\mathbb{Z}}$ par $\{P = 0\}$, alors, en notant ω_{FS} la forme de Fubini-Study, on montre que

$$h_{\overline{O(1)}}(Y) = \frac{1}{2}\sum_{p=1}^{N}\sum_{j=1}^{p}\frac{1}{j} + \int_{\mathbb{P}^N(\mathbb{C})} \log \frac{|P(z_0, \ldots, z_N)|}{\sum_{i=0}^{N}|z_i|^2}\omega_{FS}^N.$$

Avant de passer aux propriétés importantes vérifiées par cette hauteur, on peut signaler qu'il existe une construction plus "élémentaire" de la hauteur des variétés, au moins dans le cas de sous-variétés (au sens k-schéma intègre de type fini) de $\mathbb{P}^n_k$. Cette construction, dûe à Philippon, est basée sur la notion de forme de Chow : si V est une sous-variété de dimension r d'un espace projectif, on construit dans un espace projectif dual une hypersurface constituée par les r-uplets d'hyperplans intersectant V. Dans l'espace projectif dual, cette hypersurface est définie par une équation F : la forme de Chow. En prenant la hauteur de cette forme (i.e. la hauteurs des coefficients de F) avec une normalisation convenable à l'infini (cf. [Phi95]), on retombe sur la hauteur $h_{\overline{O(1)}}(V)$ définie précédemment. Un des inconvénients est qu'on pert ainsi l'analogie avec le degré.

1.3.3 Propriétés fondamentales

On indique tout d'abord une propriété de finitude, équivalent du théorème Northcott en dimension supérieure.

Théorème 1.3.1. *Soit $\overline{L}$ un fibré en droites hermitien sur une variété arithmétique projective X. Si L est ample sur X, alors, pour tout réel $A > 0$, l'ensemble*

$$\left\{Z \in Z_p(X)\ Z \text{ est effectif, } deg_{L_k}(Z) \leq A,\, h_L(Z) \leq A\right\}$$

est fini.

La seconde propriété fondamentale, est une propriété de positivité. On indique ici un résultat de [BGS94] généralisant un énoncé de Faltings.

Théorème 1.3.2. *Soit $S = Spec\ O_k$, et $Z \in Z_p(\mathbb{P}^N_S)$ un cycle effectif, on a :*

$$h_{\overline{O(1)}}(Z) \geq \frac{1}{2}[k : \mathbb{Q}]\,deg_k(Z) \sum_{l=1}^{N} \sum_{j=1}^{l} \frac{1}{j} \geq 0.$$

Par ailleurs, de même que l'on a une formule “à la Hilbert-Samuel” pour le degré, on peut aussi montrer une telle formule pour la hauteur d'une variété intègre (i.e. irréductible et réduite). Plus précisément, soit $\overline{L}$ un fibré en droite hermitien sur une variété arithmétique projective X, et soit Z un sous-schéma intègre de dimension p de X, plat sur S. Quand L_k est ample, on a la formule

$$\dim_k H^0(Z_k,L_k^n) = \deg_{L_k}(Z_k)\frac{n^{p-1}}{(p-1)!} + O(n^{p-2}).$$

Soit $H^0(Z,L^n)$ l'ensemble des sections de L^n sur Z. On le munit de la norme sup $|| \, ||_\infty$ des sections de L^n sur $X(\mathbb{C})$. Soit V_∞ le covolume de $H^0(Z,L^n)$ dans $H^0(Z,l^n) \otimes_{\mathbb{Z}} \mathbb{R}$ pour la mesure de Haar qui donne le volume 1 à la boule unité, et posons $\widehat{\deg}(H^0(Z,L^n);\ || \, ||_\infty) = -\log(V_\infty)$. On rappelle enfin qu'une forme lisse η de type (p,p) sur une variété complexe X est dite positive si pour tout polydisque $\mathbb{D}^p$ de $\mathbb{C}^p$ et pour toute application holomorphe $\varphi\ :\ \mathbb{D}^p \to X$, la forme volume $\varphi^*\eta$ sur $\mathbb{D}^p$ est positive. On a alors le théorème

Théorème 1.3.3. *(Gillet-Soulé) Supposons que L est ample et que la forme $c_1(\overline{L})$ est positive, alors,*

$$\widehat{deg}\left(H^0(Z,L^n);\ || \, ||_\infty\right) = h_{\overline{L}}(Z)\frac{n^p}{p!} + O(n^{p-1}\log n).$$

Enfin notons pour poursuivre l'analogie entre hauteur et degré, que l'on retrouve dans la théorie des hauteurs un théorème de Bézout arithmétique.

Théorème 1.3.4. *Soit $X \in Z_p(\mathbb{P}_S^N)$ et $Y \in Z_q(\mathbb{P}_S^N)$ deux cycles effectifs tels que $p+q \geq N+1$ et tels que X et Y s'intersectent proprement sur P_k^N. On a*

$$\frac{h_{\overline{O(1)}}(X \cdot Y)}{deg_k(X)deg_k(Y)} \leq \frac{h_{\overline{O(1)}}(X)}{deg_k(X)} + \frac{h_{\overline{O(1)}}(Y)}{deg_k(Y)} + [k:\mathbb{Q}]c(N,p,q),$$

où $c(N,p,q)$ est une constante ne dépendant que de N, p et q.

1.3.4 Applications

On indique quelques illustrations de la théorie des hauteurs sur les variétés. On doit (avant que Bombieri n'en fournisse une preuve "élémentaire") à P. Vojta une nouvelle preuve du théorème de Faltings, utilisant cette théorie des hauteurs en dimension supérieure, et plus dans la philosophie des preuves d'approximations diophantiennes. Par ailleurs, après avoir à nouveau généralisé la théorie de l'intersection arithmétique, on doit à Ullmo et à Zhang une preuve de la conjecture de Bogomolov dans le cas des variétés abéliennes (i.e. variétés projectives lisses munies d'une structure de groupe algébrique). Rappelons qu'une sous-variété X d'une variété abélienne A est dite de torsion s'il existe un point de torsion x et une sous-variété abélienne B tels que $X = x + B$.

Théorème 1.3.5. *(Conjecture de Bogomolov) Soit A une variété abélienne. Soit X une sous-variété de A, qui n'est pas de torsion. Il existe un réel ε strictement positif tel que l'ensemble*

$$\left\{x \in X(\overline{\mathbb{Q}}) \ / \ \ h(x) \leq \varepsilon\right\}$$

n'est pas Zariski dense.

Enfin on peut donner une version "absolue" du lemme de Siegel (absolue au sens où le système d'équations n'est plus à coefficients dans un corps de nombre k, mais à coefficients dans la clôture algébrique $\overline{\mathbb{Q}}$ de $\mathbb{Q}$). Dans l'énoncé suivant, on note $h_{\mathbb{L}^2}(x)$ la hauteur d'un point x muni de la norme $\mathbb{L}^2$ à l'infini (au lieu de la norme infinie).

Théorème 1.3.6. *(Lemme de Siegel absolu) Soit V un sous $\overline{\mathbb{Q}}$-espace vectoriel de $\overline{\mathbb{Q}}^{n+1}$ de dimension d, et soit ε un réel strictement positif. Alors, il existe $y \in V - \{0\}$ tel que*

$$h_{\mathbb{L}^2}(y) \leq \frac{1}{d}h(V) + \frac{1}{2}\log d + \varepsilon.$$

Chapitre 2

Théorème de Bombieri-Vaaler

Sommaire

2.1 Introduction **16**

2.2 Hauteurs, mesures quelques rappels **16**

2.2.1 Hauteurs 17

2.2.2 Module d'un corps localement compact 17

2.2.3 Mesure de Haar et Adèles 18

2.3 Théorème de Minkowski adélique **19**

2.4 Le cube slicing **23**

2.4.1 Le théorème de Vaaler 23

2.4.2 Cube slicing inequality 26

2.5 Théorèmes de Siegel **28**

2.6 Une application **30**

2.1 Introduction

Une technique de base en théorie de la transcendance et en approximation diophantienne consiste à construire un polynôme auxiliaire ayant un certain nombre de propriétés agréables (souvent un grand ordre d'annulation en certains points, contredisant ainsi une borne superieure obtenue autrement (lemme de Dyson par exemple)). Ceci s'applique par exemple pour les théorèmes de Liouville, Roth ainsi que la seconde inégalité de Dobrowolski. Dans quelques cas particuliers on est capable d'expliciter le polynôme, mais ceci n'est pas vrai en général et on est conduit à chercher des méthodes indirectes. L'idée de Thue (1909) est la suivante : On exprime les coefficients du polynôme comme des inconnues, et on est conduit à résoudre en entiers relatifs un ensemble de M équations en $N > M$ inconnues. En utilisant le lemme des tiroirs, Thue en déduit l'existence d'une "petite" solution non nulle. Siegel (1929) a mis ceci en forme de principe et il a prouvé que :

Théorème 2.1.1. *Si $N > M$ et si il existe $B > 0$ tel que les $(a_{mn}) \in \mathbb{Z}$, non tous nuls, sont bornés par B, alors le système $\forall i \in [1,M] \quad \sum_{j=1}^{N} a_{ij}x_j = 0$ admet une solution $(x_1,\ldots,x_N) \in \mathbb{Z}^N$ non triviale et dont tous les termes sont bornés par $(1+NB)^{\frac{M}{N-M}}$.*

Depuis, tous les résultats de ce type sont référencés comme "lemme de Siegel". Le théorème de Bombieri-Vaaler qu'on présente est de ce type.

Théorème 2.1.2. *Si $N > M$ et si les $(a_{mn}) \in \mathbb{Z}$, alors le système, où $A = (a_{mn})$,*

$$\forall i \in [1,M] \quad \sum_{j=1}^{N} a_{ij}x_j = 0$$

, que l'on suppose constitué de M équations indépendantes, admet une solution $(x_1,\ldots,x_N) \in \mathbb{Z}^N$ non triviale telle que :

$$\max_{1\leq n\leq N} |x_n| \leq \left(D^{-1}\sqrt{|det(A^tA)|}\right)^{\frac{1}{N-M}} \quad \text{où } D = pgcd(\Delta_M \;/\; \Delta_M \in \{mineurs\ M\times M\ de\ A\}).$$

En fait on va démontrer un résultat plus fort :

Théorème 2.1.3. *Avec les notations et hypothèses du th précédent, il existe $N-M$ solutions $X_l = (x_{1l},\ldots,x_{Nl})$, avec $l \in [1,N-M]$, entières indépendantes, telles que :*

$$\prod_{l=1}^{N-M} \max_{1\leq n\leq N} |x_{nl}| \leq D^{-1}\sqrt{|det(A^tA)|}.$$

On peut généraliser le problème en prenant : k un corps de nombre, K/k une extension algébrique finie de degré r, $a_{mn} \in \mathbb{Z}_K$ anneau des entiers de K et les x_j cherchés dans $\mathbb{Z}_k$.

2.2 Hauteurs, mesures quelques rappels

On fixe ici les notations que l'on conservera jusqu'au bout :

2.2.1 Hauteurs

Soit k un corps de nombre, on note k_v la complétion de k selon v. On note $d = [k : \mathbb{Q}]$ et $d_v = [k_v : \mathbb{Q}_v]$ le degré local. On normalise les valeurs absolues $|.|_v$ suivant :
(i) si v/p alors $|p|_v = p^{-\frac{d_v}{d}}$.
(ii) si v/∞ et si $x \in k_v$ alors $|x|_v := |x|^{\frac{d_v}{d}}$.

Attention, ces normalisations sont différentes de celles du cours.

Avec nos normalisations, on a la formule du produit : $\forall x \in k^* \prod_v |x|_v = 1$.

Notons qu'une autre normalisation est aussi intéressante : $||x||_v = |x|_v^{\frac{d}{d_v}}$.
Soit $\mathbf{x} \in k^N$, $\mathbf{x} = (x_1, \ldots, x_N)$, on pose : $|\mathbf{x}|_v := \max_{1 \leq n \leq N} |x_n|_v$. La hauteur de $\mathbf{x}$ est $h(\mathbf{x}) = \prod_v |\mathbf{x}|_v$.
Soit $X = (x_{mn}) \in \mathcal{M}_{MN}(k)$ et $rgX = M < N$. Si $J \subset [1,N]$ est tel que $\sharp J = M$, on pose $X_J = (x_{mn})_{n \in J}$.

Définition 2.2.1 pour toute place de k on définit la hauteur locale en v, $H_v(X)$ par :
(i) si v/∞ $H_v(X) := |det\ XX^*|_v^{\frac{1}{2}}$ où X^* est la transconjuguée de X.
(ii) sinon $H_v(X) := \max_{\sharp J = M} |det\ X_J|_v$.

Remarque : si v/∞ on a aussi $H_v(X) = (\sum_{\sharp J = M} ||det\ X_J||_v^2)^{\frac{d_v}{2d}}$.

Définition 2.2.2 En formant le produit des hauteurs locales on obtient la hauteur globale.

On a facilement les deux propositions :
Proposition 2.2.1. *H est stable par extension de corps, et pour tout $C \in GL_M(k)$, $H(CX) = H(X)$.*
Proposition 2.2.2.
Si $X = \begin{pmatrix} X_1 \\ X_2 \end{pmatrix}$ $X_i \in \mathcal{M}_{M_i \times N}(k)$ avec $M_1 + M_2 = M$, alors : pour toute place v on a :

$$H_v(X) \leq H_v(X_1) H_v(X_2).$$

Enfin on étend tout ceci aux X de rang $N < M$ en opérant sur la transposée.

2.2.2 Module d'un corps localement compact

Définition 2.2.3 Soit G un groupe localement compact, $\lambda \in Aut(G)$, et α une mesure de Haar sur G. La mesure α est unique à une constante multiplicative près, donc λ transforme α en $c\alpha$, $c \in \mathbb{R}_*^+$. La constante c, indépendante de α est appelée module de λ et notée $mod_G(\lambda)$.
Proposition 2.2.3. *Pour tout X ensemble mesurable, on a $\alpha(\lambda(X)) = mod_G(\lambda)\alpha(X)$.*

Proposition 2.2.4. *Soit k corps localement compact, et soit $A \in GL_N(k)$, on a :*

$$mod_{k^N}(A) = mod_k(det\ A).$$

Démonstration : Toute matrice $A \in GL_N(k)$ est un produit d'éléments de l'un des trois types suivant :

$$\text{matrice de permutation} \tag{2.1}$$

$$(x_1,\ldots,x_n) \mapsto (ax_1,\ldots,x_n)\ a \in k^* \tag{2.2}$$

$$(x_1,\ldots,x_n) \mapsto (x_1 + \sum_{i=2}^{n} a_i x_i, x_2,\ldots,x_n)\ . \tag{2.3}$$

Et on conclut facilement dans chacun de ces trois cas. □

Théorème 2.2.1. *Soit v une place finie et K/Q_v une extension de degré d_v, alors,*

$$mod_K x = ||x||_v^{d_v}.$$

2.2.3 Mesure de Haar et Adèles

On note O_k l'anneau des entiers de k et si v est une place finie de k on note O_v l'anneau compact maximal de k_v, i.e, $O_v = \{x \in k_v\ /\ |x|_v \leq 1\}$. On note $k_{\mathcal{A}}$ l'anneau des adèles de k. Le groupe $k_{\mathcal{A}}$ additif est localement compact, on peut donc lui associer une mesure de Haar notée λ ou dx : on prend λ_v ou dx_v la mesure de Haar sur k_v normalisée par :
(i) si $v/p \quad \lambda_v(O_v) = |\mathcal{D}_v|_v^{\frac{d}{2}}$, où $\mathcal{D}_v$ est la différente de k en v.
(ii) si v/∞ et $k_v = \mathbb{R}$, $\quad \lambda_v$ est la mesure de Lebesgue sur $\mathbb{R}$.
(iii) si v/∞ et $k_v = \mathbb{C}$, $\quad \lambda_v$ est la mesure de Lebesgue sur $\mathbb{C}$ multipliée par 2.
Enfin $\lambda = \prod_v \lambda_v$ est la mesure de Haar voulue sur $k_{\mathcal{A}}$. Plus précisément λ détermine (par définition de $k_{\mathcal{A}}$) une mesure sur tous les sous groupes ouverts $\prod_{v\in\mathcal{P}} k_v \times \prod_{v\notin\mathcal{P}} O_v$ où $\mathcal{P}$ est un ensemble fini de places, contenant toutes les places à l'infini. La mesure de Haar est alors celle qui coincide avec λ sur cette famille de sous groupes).
On considère k comme sous groupe discret de $k_{\mathcal{A}}$ par le plongement diagonal et on note $\varphi\ :\ k_{\mathcal{A}} \longrightarrow\ k_{\mathcal{A}}/k$ la surjection canonique sur le groupe compact $k_{\mathcal{A}}/k$. La mesure de Haar induite sur $k_{\mathcal{A}}/k$ par φ est encore notée λ et de par le choix des normalisations on a :

$$\lambda(k_{\mathcal{A}}/k) = 1$$

Soit $G = G_1 \times \ldots \times G_L$ produit tel que $\forall i \leq L$, $G_i \in \{k_{\mathcal{A}};\ k_{\mathcal{A}}/k\}$. La mesure de Haar λ sur chaque facteur détermine une unique mesure produit sur G, que l'on note V_G ou V si il n'y a pas de confusion possible. (Remarquons que V est clairement une mesure de Haar sur G). Soit G un groupe de la forme précédente et supposons que $G_l = k_{\mathcal{A}}$, on définit alors :

$$\begin{aligned} \varphi_l\ :\ G &\to \varphi_l(G) \\ (g_1,\ldots,g_L) &\mapsto (g_1,\ldots,\varphi(g_l),\ldots,g_L) \end{aligned}$$

Si $\forall i \leq l$ $G_l = k_{\mathcal{A}}$, on pose $\Phi_l = \prod_{i=1}^{l} \varphi_i$ le morphisme composé.

Proposition 2.2.5. *Si $\phi = \varphi_i$ ou $\phi = \Phi_l$, et si $X \subset G$ est mesurable tel que $\phi|_X$ est injectif, alors $V(X) = V(\phi(X))$.*

Démonstration : Par le théorème de Fubini et par définition de ϕ, il suffit de vérifier l'énoncé dans le cas de $\varphi \ : \ (k_{\mathcal{A}},\lambda) \longrightarrow (k_{\mathcal{A}}/k,\mu)$ Or par définition, on a pour X mesurable, $\mu(Y) = \lambda(\varphi^{-1}(Y))$. Donc si X est tel que φ restreint à X est injective, alors on a $\mu(Y) = \mu(\varphi(X)) = \lambda(X)$. Ceci conclut la preuve. □

Définition 2.2.4 Soit $x = (x_v) \in k_{\mathcal{A}}$ et $\alpha \in \mathbb{R}$. On définit la multiplication par α par :

$$\alpha x := y = (y_v) \in k_{\mathcal{A}} \text{ où } \begin{cases} y_v = \alpha x_v & \text{si } v/\infty, \\ y_v = x_v & \text{sinon.} \end{cases}$$

Si $L > 0$, on étend ceci à $k_{\mathcal{A}}^L$ composante par composante.

Proposition 2.2.6. *Si $X \subset k_{\mathcal{A}}^L$ alors $\alpha X \subset k_{\mathcal{A}}^L$ et on a : $V(\alpha X) = |\alpha|^{dL} V(X)$.*

Démonstration : V est une mesure produit donc il suffit clairement de le voir pour $L = 1$. Or le nombre de v/∞ est justement d, d'où le résultat. □

2.3 Théorème de Minkowski adélique

Dans toute la suite, L désigne un entier strictement positif fixé. On pose $E = k^L$, $E_v = k_v^L$ et $E_{\mathcal{A}}^L = k_{\mathcal{A}}^L$.

Pour toute place v de k, soit M_v un k_v réseau de E_v, i.e un sous O_v-module de E_v compact et ouvert. On suppose de plus que $M_v = O_v^L$ pour presque toute place. Pour toute place v/∞ de k soit S_v un ouvert non vide, symétrique, borné et convexe de E_v. On pose :

$$\mathcal{S} = \prod_{v|\infty} S_v \times \prod_{v\nmid\infty} M_v \ .$$

On a $\mathcal{S} \subset E_{\mathcal{A}}^L = k_{\mathcal{A}}^L$ et $\mathcal{S}$ est clairement un voisinage de 0, dont l'adhérence est compacte. (En effet $\overline{\prod A_i} \subset \prod \overline{A_i}$ et tous les M_v sont compacts ainsi que les $\overline{S_v}$. Donc $\overline{\mathcal{S}}$ est fermé dans un compact donc compact). Par ailleurs, k est discret dans $k_{\mathcal{A}}^L$, donc E l'est dans $E_{\mathcal{A}}^L = k_{\mathcal{A}}^L$, et on en déduit que $\mathcal{S} \cap E$ est fini. Pour tout entier $l \in [1,L]$, on pose :

$$\lambda_l = inf\{\lambda > 0 \ /(\lambda\mathcal{S}) \cap E \text{ contient } l \text{ vecteurs linéairement indépendants}\}.$$

On a bien sur $0 \leq \lambda_1 \leq \ldots \leq \lambda_L \leq \infty$. De plus (cf Weil), l'ensemble

$$M = \bigcap_{v\nmid\infty} (E \cap M_v)$$

est un k réseau, i.e un O_k module de E contenant une base de E sur k. Si on écrit $E_\infty = \prod\limits_{v/\infty} k_v^L$ alors M peut être vu comme la projection de

$$(E_\infty \times \prod_{v \nmid \infty} M_v) \bigcap E$$

sur le premier facteur (on a ici tout plongé dans $E_\mathcal{A}$ bien sur). Ainsi (car E est un sous groupe discret de $E_\mathcal{A}$), on voit M comme un sous groupe discret de E_∞. Chaque S_v est ouvert donc $M \cap \prod\limits_{v/\infty} (\lambda S_v)$ contient L vecteurs linéairement indépendant pour λ assez grand, et comme S_v est borné, le même ensemble, est $\{0\}$ pour λ assez petit non nul. Ainsi les λ_l satisfont $0 < \lambda_1 \leq \ldots \leq \lambda_L < \infty$. On peut en effet les définir par :

$$\lambda_l = inf\{\lambda > 0 \ / \ M \cap \prod_{v/\infty} (\lambda \mathcal{S}_v) \text{ contient } l \text{ vecteurs linéairement indépendant}\}.$$

On peut maintenant énoncer le (second) théorème de Minkowski :

Théorème 2.3.1. *Les λ_l définis précédemment vérifient :* $(\prod\limits_{l=1}^{L} \lambda_l)^d V(\mathcal{S}) \leq 2^{dL}$.

Pour prouver ce théorème nous aurons besoin de la

Proposition 2.3.1. *Soit $l \geq 1$ et soit $(\mu_1, \ldots, \mu_n)$ vérifiant $0 < \mu_1 \leq \ldots \leq \mu_L < \infty$, et tels que : si $\boldsymbol{x}$ et $\boldsymbol{y}$ sont deux vecteurs de $\mu_l \mathcal{S}$ tels que $\boldsymbol{x}$-$\boldsymbol{y} \in E$, alors $\forall n \in [l,L]$ $x_n = y_n$. Sous ces hypothèses, on a $(\prod\limits_{l=1}^{L} \mu_l)^d V(\mathcal{S}) \geq 1$.*

Démonstration : La démonstration de cette proposition ce fait en trois étapes :
<u>première étape</u> : Si $\mathcal{T} \in E_\mathcal{A}$ est de la même forme que $\mathcal{S}$ et si $\mu \geq 1$, alors

$$\forall l \in [1,L] \quad V(\Phi_l(\mu \mathcal{T})) \geq \mu^{d(L-l)} V(\Phi_l(\mathcal{T})).$$

Supposons d'abord $l = L$ et soit $\mathbf{y} \in \mathcal{T}$. Comme $0 \in \mathcal{T} - \mathbf{y}$, on a (par convexité des T_v pour v/∞ et par notre définition de la multiplication par un réel) :

$$\mu(\mathcal{T} - \mathbf{y}) \supset \mathcal{T} - \mathbf{y}.$$

Donc on a

$$\Phi_l(\mu(\mathcal{T}) - \mu(\mathbf{y})) \supset \Phi_l(\mathcal{T} - \mathbf{y}),$$

d'où en passant à la mesure V invariante par translation :

$$V(\Phi_l(\mu(\mathcal{T})) \supset V(\Phi_l(\mathcal{T})),$$

ce qui conclut le cas $l = L$.
Supposons maintenant que $l \in [1,L-1]$, on identifie $E_\mathcal{A} = k_\mathcal{A}^L$ avec $k_\mathcal{A}^l \times k_\mathcal{A}^{L-l}$. Pour un vecteur $\mathbf{y} \in k_\mathcal{A}^{L-l}$ on définit

$$\mathcal{T}(\mathbf{y}) = \{\mathbf{x} \in k_\mathcal{A}^l \ / \ (\mathbf{x},\mathbf{y}) \in \mathcal{T}\}.$$

Il s'ensuit que :
$$\Phi_l(\mathcal{T}(\mathbf{y})) = \{\mathbf{x} \in k_{\mathcal{A}}^l \ / \ (\mathbf{x},\mathbf{y}) \in \Phi_l(\mathcal{T})\}.$$
Si on remplace $\mathcal{T}$ par $\mu\mathcal{T}$, alors :
$$V(\Phi_l(\mathcal{T}\mathbf{y})) = \int\limits_{\mathbf{y}\in k_{\mathcal{A}}^{L-l}} \int\limits_{\substack{\mathbf{x}\in(k_{\mathcal{A}}/k)^L \\ (\mathbf{x},\mathbf{y})\in\Phi_l((\mu\mathcal{T}))}} dV(\mathbf{x})dV(\mathbf{y}), \ i.e \ :$$
$$V(\Phi_l(\mathcal{T})) = \int\limits_{\mathbf{y}\in k_{\mathcal{A}}^{L-l}} V(\Phi_l(\mu\mathcal{T})(\mathbf{y}))dV(\mathbf{y}).$$
On fait le changement de variable $\mathbf{y} \mapsto \mu\mathbf{y}$ dans la dernière intégrale de sorte que :
$$V(\Phi_l(\mu\mathcal{T})) = \mu^{d(L-l)} \int\limits_{\mathbf{y}\in k_{\mathcal{A}}^{L-l}} V(\Phi_l((\mu\mathcal{T})(\mu\mathbf{y})))dV(\mathbf{y}).$$
par ailleurs on constate facilement que $(\mu\mathcal{T})(\mu\mathbf{y}) = \mu(\mathcal{T}(\mathbf{y}))$. De plus, comme $\mu \geq 1$ on a (la preuve a déja été faite) :
$$V(\Phi_l(\mu(\mathcal{T}(\mathbf{y})))) \geq V(\Phi_l(\mathcal{T}(\mathbf{y}))).$$
On en déduit finalement :
$$V(\Phi_l(\mu\mathcal{T})) = \mu^{d(L-l)} \int\limits_{\mathbf{y}\in k_{\mathcal{A}}^{L-l}} V(\Phi_l(\mathcal{T}(\mathbf{y})))dV(\mathbf{y}), \text{ donc}$$
$$V(\Phi_l(\mu\mathcal{T})) \geq \mu^{d(L-l)} V(\Phi_l\mathcal{T}).$$
Ceci complète la preuve de l'étape 1.

Pout tout $l \in [1,L-1]$, on applique la première étape à l'ensemble $\mathcal{T} = \mu_l\mathcal{S}$ avec $\mu = \frac{\mu_{l+1}}{\mu_l}$ on trouve que
$$V(\Phi_l(\mu_{l+1}\mathcal{S})) \geq (\frac{\mu_{l+1}}{\mu_l})^{d(L-l)} V(\Phi_l(\mu_l\mathcal{S}).$$
étape 2 : Montrons que l'application $\varphi_{l+1} \ : \ \Phi_l(\mu_{l+1}\mathcal{S}) \to (k_{\mathcal{A}}/k)^{l+1} \times k_{\mathcal{A}}^{L-l-1}$ est injective. Soient $\mathbf{x}$ et $\mathbf{y}$ deux points distincts de $\Phi_l(\mu_{l+1}\mathcal{S})$, il existe $\mathbf{x'}$ et $\mathbf{y'}$ deux points distincts de $\mu_{l+1}\mathcal{S}$ tels que $\Phi_l(\mathbf{x'}) = \mathbf{x}$ et $\Phi_l(\mathbf{y'}) = \mathbf{y}$. Supposons par l'absurde que $\varphi_{l+1}(\mathbf{x}) = \varphi_{l+1}(\mathbf{y})$, ceci implique que
$$l \neq l+1 \ \ x_n = y_n$$
et que
$$\Phi_{l+1}(\mathbf{x'}) = \Phi_{l+1}(\mathbf{y'}).$$

Mais cette dernière égalité montre que **x'-y'** $\in E$ et donc, par hypothèses sur les μ_l, on a

$$\forall n \in [l+1,L] \ \ x'_n = y'_n.$$

Or Φ_l est l'identité sur la $(l+1)^{eme}$ coordonnée donc $x_{l+1} = y_{l+1}$ donc **x**=**y** ce qui est absurde. Ceci conclut la seconde étape.

<u>étape 3</u> : conclusion :
V est une mesure de Haar, donc l'étape 2 nous dit que

$$V(\Phi_l(\mu_{l+1}\mathcal{S})) = V(\Phi_{l+1}(\mu_{l+1}\mathcal{S})).$$

En combinant ceci avec l'inégalité précédant l'étape 2 et en prenant le produit pour l décrivant $[1,L-1]$, on en déduit :

$$V(\Phi_L(\mu_L\mathcal{S})) \geq \prod_{l=1}^{L-1}(\frac{\mu_{l+1}}{\mu_l})^{d(L-l)}V(\Phi_1(\mu_1\mathcal{S})).$$

Pour conclure il nous reste à noter deux choses :
Tout d'abord $V(\Phi_L(\mu_L\mathcal{S})) \leq V((k_{\mathcal{A}}/k)^L) = 1$ par choix des normalisations.
Ensuite $\Phi_1 = \varphi_1$ est clairement injective sur $\mu_1\mathcal{S}$ donc (cf rappels sur les mesures de Haar) on a : $V(\Phi_1(\mu_1\mathcal{S})) = V(\mu_1\mathcal{S}) = (\mu_1)^{dL}V(\mathcal{S})$. En combinant ces deux remarques on conclut la démonstration du théorème. $\square$

On peut maintenant passer à la preuve du théorème de Minkowski.
Démonstration : Pour chaque λ_l on associe un vecteur $\mathbf{u}_l$ de E, de telle sorte que les $\mathbf{u}_1,\ldots,\mathbf{u}_L$ sont linéairement indépendant sur k et tels que $\forall l \in [1,L]$ et $\forall \lambda > \lambda_l$, on a

$$\{\mathbf{u}_1,\ldots,\mathbf{u}_L\} \subset (\lambda\mathcal{S}) \cap E.$$

Soit alors $U = (\mathbf{u}_1,\ldots,\mathbf{u}_L)$ la matrice $L \times L$ de vecteurs colonnes les $\mathbf{u}_l$. L'application $x \mapsto Ux$ ainsi définie est un automorphisme de $E_{\mathcal{A}}$, et comme $det(U)$ est dans k, son module est 1. De plus les $U^{-1}S_v$, $v \mid \infty$, et $U^{-1}M_v$, sinon ont clairement les mêmes propriétés que respectivement S_v et M_v. On peut donc prendre les vecteurs de la base canonique comme vecteurs associés à $U^{-1}\mathcal{S}$. Enfin comme $\mathcal{S}$ et $U^{-1}\mathcal{S}$ ont même mesure de Haar, on peut aussi supposer que $\mathbf{u}_l = \mathbf{e}_l$.
On applique maintenant la proposition précédente avec $\mathcal{S}$ et $\mu_l = \frac{1}{2}\lambda_l$ pour tout l dans $[1,L]$. Il sufit, pour voir si la proposition précédente s'applique, de considérer le cas $l=1$ et les valeurs l telles que $\lambda_{l-1} < \lambda_l$. Soit donc **x** et **y** deux points distincts de $\mu_l\mathcal{S}$ tels que **x-y** $\in E$. Comme chaque S_v est convexe et symétrique pour $v \mid \infty$, on a **x-y** $\in 2\mu_l\mathcal{S} = \lambda_l\mathcal{S}$. Or $\mathcal{S}$ est ouvert et par hypothèses, $\lambda_{l-1} < \lambda$, donc, il existe $\delta > 0$ tel que $\mathbf{e}_l,\ldots,\mathbf{e}_{l-1}$,**x-y** $\in (\lambda_l - \delta)\mathcal{S}$. Donc ces vecteurs ne peuvent être linéairement indépendant sur k, par définition de λ_l. Or les $\mathbf{e}_i$ étant trivialement indépendant, on en déduit :

$$\forall j \in [1,l-1] \ \exists \alpha_j \in k \ \ \mathbf{x\text{-}y} = \sum_{j=1}^{l-1}\alpha_j\mathbf{e}_j.$$

En particulier, $x_n = y_n$ pour tout $n \in [l,L]$. On peut donc appliquer la proposition précédente, et on obtient :

$$\prod_{i=1}^{L} \mu_i^d V\mathcal{S} \leq 1.$$

Coomme $\mu_i = \frac{\lambda_i}{2}$ ceci conclut la démonstration. □

2.4 Le cube slicing

Soit N un entier positif. Pour toutes place v de k, soit C_v le cube v-adique dans k_v^N défini par :

$$C_v = \{\mathbf{x} \in k_v^N \ / \ \max_{1 \leq n \leq N} ||x_n||_v < \frac{1}{2}\} \ \text{ si } v \text{ est réel,} \tag{2.4}$$

$$C_v = \{\mathbf{x} \in k_v^N \ / \ \max_{1 \leq n \leq N} ||x_n||_v < \frac{1}{\sqrt{2\pi}}\} \ \text{ si } v \text{ est complexe,} \tag{2.5}$$

$$C_v = \{\mathbf{x} \in k_v^N \ / \ \max_{1 \leq n \leq N} ||x_n||_v \leq 1\} \ \text{ sinon.} \tag{2.6}$$

En fait, on choisit la normalisation de telle sorte que C_v est de volume 1 quand $v \mid \infty$. Par ailleurs il est à peu près immédiat que $C = \prod_v C_v$ est un ouvert de $k_{\mathcal{A}}^N$, dont la fermeture est compacte. Considérons $Y \in \mathcal{M}_{N \times L}(k)$ de rang $L < N$. Si $I \subset [1,N]$ est tel que $\# I = L$, on écrit $Y = (y_{nl})$, $n \in I$ et $l \in [1,L]$ la matrice carrée correspondante. Rappel :

$$H_v(X) = \prod_{v \nmid \infty} \underset{\sharp J = M}{max} |det\ X_J|_v \times \prod_{v \mid \infty} (\sum_{\sharp J = M} ||det\ X_J||_v^2)^{\frac{d_v}{2d}}.$$

On pose aussi $\mathcal{S} = \prod_v \{\mathbf{x} \in k_v^L / \ Y\mathbf{x} \in C_v\}$. Y est injective, c'est donc une "tranche" L-dimensionnelle du cube unité.

2.4.1 Le théorème de Vaaler

Définition 2.4.1 Une application $f \ : \ \mathbb{R}^n \to [0, +\infty[$ est dite log-concave si :

$$\forall x_1,\, x_2 \in \mathbb{R}^n \ \ \forall \lambda \in]0,1[\text{ on a } \ \ f(\lambda x_1 + (1-\lambda) x_2) \geq f(x_1)^{\lambda} f(x_2)^{1-\lambda}.$$

Définition 2.4.2 Une mesure de probabilité ν sur $(\mathbb{R}^n, \mathcal{B}(\mathbb{R}^n))$ est dite log-concave si

$$\forall U_1,\, U_2 \text{ ouvert convexe de } \ \mathbb{R}^n \ \forall \lambda \in]0,1[\text{ on a } \ \ \nu(\lambda U_1 + (1-\lambda) U_2) \geq \nu(U_1)^{\lambda} \nu(U_2)^{1-\lambda}.$$

Lemme 2.4.1. *Soit ν une mesure de probabilité log-concave telle que $Supp(\nu)$ engendre un sous espace vectoriel P_r de dimension r. Alors il existe une fonction f log-concave définie sur P_r telle que $d\nu = f d\mu_r$, où μ_r est la mesure de Lebesgue r dimensionnelle. Réciproquement, une telle mesure $f d\mu_r$ est log-concave.*

Démonstration : On va admettre ce lemme, tout comme le suivant. Le résultat est plausible. $\square$

Définition 2.4.3 Soit ν_1 et ν_2 deux mesures de probabilités sur $\mathbb{R}^n$. On dit que ν_2 est plus pointue (peaked en anglais) que ν_1 si :

$$\forall U \text{ fermé convexe symétrique de } \mathbb{R}^n \ \nu_1(U) \leq \nu_2(U).$$

Définition 2.4.4 Soit f_1 et f_2 deux densités de probabilités sur $\mathbb{R}^n$. On dit que f_2 est plus pointue que f_1 si les mesures associées le sont.

Lemme 2.4.2. *Si ν_1, ν_2, λ_1 et λ_2 sont des mesures de probabilités log-concaves telles que λ_i est plus pointue que ν_i, $i \in \{1,2\}$, alors $\lambda_1 \times \lambda_2$ est plus pointue que $\nu_1 \times \nu_2$.*

Lemme 2.4.3. *Soit $n_1, \ldots, n_J \in \mathbb{N}$ tels que $\sum n_i = N$ et $Q_N = \prod S_{n_i}$ dans $\mathbb{R}^N$, où S_n est la boule unité euclidienne de $\mathbb{R}^n$. Alors, $1_{Q_N}(x)$ est plus pointue que la densité gaussienne $exp(-\pi|x|^2)$ sur $\mathbb{R}^N$.*

Démonstration : On ne va faire la preuve de ce lemme que dans le cas qui nous interesse (cf corollaire du th de Vaaler un peu plus loin), c'est à dire quand $\forall i \ n_i = 1$. Dans le cas général c'est la même méthode avec plus de calcul.

On a affaire à des mesures produit, donc le lemme 2 nous indique qu'il suffit de montrer le résultat en dimension 1, i.e voir que $\lambda_1 = 1_{[-\frac{1}{2},\frac{1}{2}]}$ est plus pointue que la densité $\lambda_2 = exp(-\pi x^2)$ sur $\mathbb{R}$. Soit donc U un fermé convexe symétrique, i.e $U = [-a,a]$ $a > 0$. $\lambda_1(U) = min(1,2a)$, donc si $2a \geq 1$, le résultat est acquis car λ_2 est une mesure de probabilité donc de masse totale ≤ 1. Sinon $\lambda_1(U) = 2a$ et $\lambda_2(U) = 2\int_0^a e^{-\pi x^2} dx$. Posons alors $F(x) = x - \int_0^x e^{-\pi y^2} dy$. F est bien définie et dérivable sur $\mathbb{R}_*^+$, on a $F'(x) = 1 - e^{-\pi x^2} \geq 0$, donc F est strictement croissante. Or $F(0) = 0$, donc $F(a) \geq 0$, d'où le résultat. $\square$

On peu maintenant passer au théorème proprement dit :

Théorème 2.4.1. ***(Vaaler)*** *: Soit $n_1, \ldots, n_J \in \mathbb{N}$ tels que $\sum n_i = N$ et $Q_N = \prod S_{n_i}$ dans $\mathbb{R}^N$, où S_n est la boule unité euclidienne de $\mathbb{R}^n$. Si $A \in \mathcal{M}_{N\times L}(\mathbb{R})$, est de rang $L < N$, on a :*

$$\int_{\mathbb{R}^L} 1_{Q_N}(A\boldsymbol{x}) d\lambda^L(\boldsymbol{x}) \geq |det\ {}^tAA|^{-\frac{1}{2}}$$

Démonstration : Posons $L' = N - L$, et P_L le sous espace vectoriel engendré par les colonnes de A. Soit B la matrice dont les colonnes forment une base orthonormale de $P_L^\perp$ et soit $W = (A,B) \in GL_N(\mathbb{R})$. On a la décomposition $\mathbb{R}^N = \mathbb{R}^L \times \mathbb{R}^{L'}$, donc tout vecteur z peut s'écrire sous la forme : $z = (x,y)$. Soit alors $\varepsilon \in]0,1]$, posons :

$$H_\varepsilon = \left\{ z \in \mathbb{R}^N \ / \ z = (x,y) \quad \max_{1\leq j\leq L} |y_i| \leq \frac{\varepsilon}{2} \right\}$$

$$H'_\varepsilon = \left\{ y \in \mathbb{R}^L \;/\; \max_{1 \le j \le L} |y_i| \le \frac{\varepsilon}{2} \right\}.$$

H_ε est clairement un convexe, fermé symétrique. Donc son image par l'application linéaire inversible W est encore un convexe fermé symétrique. Le lemme 3 nous donne alors :

$$\int_{H_\varepsilon} exp(-\pi|Wz|^2) d\mu_N(z) \le \int_{H_\varepsilon} 1_{Q_N}(Wz) d\mu_N(z)$$

On multiplie par $\mu_{L'}(H'_\varepsilon)^{-1} = \frac{1}{\varepsilon^{L'}}$ et on a donc :

$$\frac{1}{\varepsilon^{L'}} \int_{\mathbb{R}^L} \int_{H'_\varepsilon} exp(-\pi|Ax+By|^2) d\mu_{L'}(y) d\mu_L(x) \le \frac{1}{\varepsilon^{L'}} \int_{\mathbb{R}^L} \int_{H'_\varepsilon} 1_{Q_N}(Ax+By) d\mu_{L'}(y) d\mu_L(x)$$

L'orthogonalité implique que $|Ax+By|^2 = |Ax|^2 + |By|^2$ et donc la limite quand $\varepsilon \mapsto 0^+$ du membre de gauche est $\int exp(-\pi|Ax|^2) d\mu_L(x)$. En effet on calcule explicitement $|By|^2 = |y|^2$ en utilisant l'orthonormalité de B et on est alors ramené par Fubini en dimension 1 ($L' = 1$ bien sur). Dans ce cas un petit calcul à la main nous donne le résultat. Par ailleurs cette dernière intégrale vaut $|{}^tAA|^{-\frac{1}{2}}$. On remarque en effet que ${}^tAA$ est définie positive, on peut donc prendre sa racine carré C (ie, C definie positive, telle que $C^2 = {}^tAA$). En effectuant le changement de variable $y := Cx$ et en remarquant que, $\int_{\mathbb{R}^K} exp(-\pi|y|^2) d\mu_{L'}(y) = 1$ on en déduit le résultat.
On veut maintenant calculer le membre de droite de l'inégalité (quand $\varepsilon \mapsto 0^+$).
$\forall \varepsilon \in]0,1]$ et $\forall x \in \mathbb{R}^{L'}$, on a :

$$\frac{1}{\varepsilon^{L'}} \int_{H'_\varepsilon} 1_{Q_N}(Ax+By) d\mu_{L'}(y) \le 1$$

Or Q_N et H'_ε sont bornés, donc $\frac{1}{\varepsilon^{L'}} \int_{H'_\varepsilon} 1_{Q_N}(Ax+By) d\mu_{L'}(y) = 0$ quand $|x|$ est assez grand (et ce, indépendamment de ε). Donc $\int_{\mathbb{R}^L} = \int_C$ où C est un compact indépendant de ε. Donc sur C on peut intervertir $\int_C$ et $\lim\limits_{\varepsilon \mapsto 0^+}$, notamment la limite du membre de droite vaut :

$$\int_{\mathbb{R}^K} \lim_{\varepsilon \mapsto 0} \frac{1}{\varepsilon^{L'}} \int_{H'_\varepsilon} 1_{Q_N}(Ax+By) d\mu_{L'}(y) d\mu_K(x).$$

Or l'intégrande de la première intégrale vaut $1_{Q_N}(Ax)$ quand $Ax \in Q_N$, sauf éventuellement sur la frontière qui est de mesure de Lebesgue nulle. D'où le résultat. □

Corollaire 2.4.1. *Soit $Y \in \mathcal{M}_{N \times L}(\mathbb{R})$, de rang L et si v est réelle, on a :*

$$\int_{\mathbb{R}^L} 1_{C_v}(Y\boldsymbol{x}) d\lambda^L(\boldsymbol{x}) \ge |det\ {}^tYY|^{-\frac{1}{2}}$$

Démonstration : On prend $n_i = 1$ pour tout i, et on conclut alors directement. □

2.4.2 Cube slicing inequality

Rappel : $\mathcal{S} = \prod_v \{\mathbf{x} \in k_v^L / \ Y\mathbf{x} \in C_v\}$.
Théorème 2.4.2. ***(cube slicing inequality)*** *: Si $Y \in \mathcal{M}_{N\times L}(k)$ est de rang $L < N$, et si $\mathcal{S}$ est l'ensemble défini juste au dessus, alors c'est un sous-ensemble de $E_{\mathcal{A}}$ et il est de la forme (définie dans la partie précédente) :*

$$\prod_{v|\infty} S_v \times \prod_{v\nmid\infty} M_v \ .$$

De plus, on a l'inégalité :

$$H(Y)^{-d}|\Delta_k|^{-\frac{L}{2}} \leq V(\mathcal{S}) \ ,$$

où Δ_k est le discriminant de k.
Démonstration : étape 1 : on donne une borne inférieure pour chaque volume local $\int_{E_v} 1_{C_v}(Y\mathbf{x})d\beta_v^L(\mathbf{x})$. Si v est réelle, on a

$$\int_{E_v} 1_{C_v}(Y\mathbf{x})d\beta_v^L(\mathbf{x}) \geq |det\ {}^tYY|_v^{-\frac{1}{2}} = \left(\sum_{|I|=L} ||det\ Y_L||_v^2\right)^{-\frac{1}{2}}$$

par le théorème de Vaaler.
Si v est complexe, on a

$$\int_{E_v} 1_{C_v}(Y\mathbf{x})d\beta_v^L(\mathbf{x}) \geq ||det\ Y^*Y||_v^{-1} = \left(\sum_{|I|=L} ||det\ Y_L||_v^2\right)^{-1} .$$

Pour vérifier cette inégalité, posons $Y = A + iB$ et $\mathbf{x} = \mathbf{s} + i\mathbf{t}$. Dans ce cas , et avec la notation

$$C_v' = \left\{\xi \in \mathbb{R}^{2L}\ (\xi_j)^2 + (\xi_{L+j})^2 < \frac{1}{2\pi}\ \forall j \in [1,L]\ \right\}, \text{ on a :}$$

$$\int_{E_v} 1_{C_v}(Y\mathbf{x})d\beta_v^L(\mathbf{x}) = 2^L \int_{\mathbb{R}^L}\int_{\mathbb{R}^L} 1_{C_v'}\left(\begin{pmatrix} A & -B \\ B & A \end{pmatrix}\begin{pmatrix} \mathbf{s} \\ \mathbf{t} \end{pmatrix}\right) d\mathbf{s}d\mathbf{t} \ .$$

On peut maintenant appliquer le théorème de Vaaler au membre de droite de cette égalité donc, le membre de gauche est :

$$\geq \left|\left| det \begin{pmatrix} A & -B \\ B & A \end{pmatrix}^T \begin{pmatrix} A & -B \\ B & A \end{pmatrix}\right|\right|_v^{-\frac{1}{2}}$$

$$= ||det(A+iB)^*(A+iB)||_v^{-1}$$

$$= ||det\ Y^*Y||_v^{-1}$$

Si $v \nmid \infty$, il existe $J \subset [1,L]$ de cardinal L tel que $\max\limits_{|I|=L} ||det\ Y_I||_v = ||Y_J||_v$. Or par hypothèses, Y est de rang L, donc $detY_J \neq 0$. En faisant le changement de variables, $\mathbf{x} := Y_J^{-1}\mathbf{x}$, on obtient :

$$\int_{E_v} 1_{C_v}(Y\mathbf{x})d\beta_v^L(\mathbf{x}) = mod_{k_v}(det\ Y_J^{-1}) \int_{E_v} 1_{C_v}(YY_J^{-1}\mathbf{x})d\beta_v^L(\mathbf{x})\ ,\ i.e\ :$$

$$\int_{E_v} 1_{C_v}(Y\mathbf{x})d\beta_v^L(\mathbf{x}) = ||det\ Y_J||_v^{-d_v} \int_{E_v} 1_{C_v}(W\mathbf{x})d\beta_v^L(\mathbf{x}), \text{ où } W = YY_J^{-1}.$$

Quitte à permuter les coordonnées de $\mathbf{x}$ on peut supposer que $J = [1,L]$. Dans ce cas, la matrice extraite W_J est la matrice identité de taille N, donc $||w_{jl}||_v \leq 1$ pour tout $j \in [1,L]$. De plus $||det\ W_I||_v \leq 1$ pour tout I de cardinal L. Ceci car rayer la i^{eme} ligne dans W revient à rayer la i^{eme} ligne dans Y. Or $det(UV) = detUdetV$ et J est tel que $||Y_J||_v$ est maximum. En particulier si on considère la matrice W_I définie par

$$I = \{1,\ldots,l-1,l+1,\ldots,L,L+j\} \text{ pour j variant dans } [1,L]\ \text{, un}$$

developpement par rapport à la l^{eme} colonne nous donne : $||det\ W_I||_v = ||w_{L+j,l}||_v \leq 1$. Comme $||.||_v$ est ultramétrique, $W\mathbf{x} \in C_v$ si et seulement si pour tout $l \in [1,L]$ $||x_l||_v \leq 1$. Donc on a :

$$\int_{E_v} 1_{C_v}(W\mathbf{x})d\beta_v^L(\mathbf{x}) = \beta_v^L\ \left\{O_v^L\right\} = |\mathcal{D}_v|_v^{\frac{dL}{2}}.$$

<u>étape 2</u> : $\mathcal{S}$ est de la forme voulue.
Si v est une place infinie, alors il est clair que $\mathcal{S}_v = \{\mathbf{x} \in E_v\ Y\mathbf{x} \in C_v\}$ est non vide, convexe, symetrique et borné (car le cube C_v l'est). De plus C_v est ouvert donc $\mathcal{S}_v$ l'est aussi.
Si v est une place finie il clair (pour les mêmes raisons et car Y est injective) que $M_v = \{\mathbf{x} \in E_v\ Y\mathbf{x} \in C_v\}$ est un O_v-module ouvert et compact. Pour presque toute place finie v on a :

$$||y_{nl}||_v = 1 \text{ dès que } y_{nl} \neq 0 \text{ est un coefficient de Y, et } \ ||det\ Y_J^{-1}||_v = 1.$$

En particulier $O_v^L \subset M_v$ pour presque toute place finie, et l'étape 1 pour v place finie nous donne :

$$\beta_v^L(M_v) = \int_{E_v} 1_{C_v}(Y\mathbf{x})d\beta_v^L(\mathbf{x}) = |\mathcal{D}_v|_v^{\frac{dL}{2}}.$$

Donc par notre choix de normalisation de β_v^L, $\beta_v^L(M_v) = \beta_v^L(O_v^L)$ et donc pour presque toute place finie v on a $M_v = O_v^L$. Ceci montre que $\mathcal{S}$ est un sous ensemble de la forme voulue de $E_{\mathcal{A}}$.
<u>conclusion</u> : il nous reste à montrer l'inégalité pour conclure.
Comme $\mathcal{S}$ est d'adhérence compacte, on peut écrire :

$$\int_{E_{\mathcal{A}}} 1_{C_v}(Y\mathbf{x})dV(\mathbf{x}) = \prod_v \int_{E_v} 1_{C_v}(Y\mathbf{x})d\beta_v^L(\mathbf{x}).$$

Ainsi on conclut facilement en utilisant les minorations de l'étape 1 et en remarquant que

$$\prod_{v \nmid \infty} |\mathcal{D}_v|_v^{-d} = |\Delta_k|.$$

□

2.5 Théorèmes de Siegel

On dispose maintenant de tous les outils nécessaires pour énoncer les théorèmes qui nous intéressent. Le résultat clé est le suivant :

Théorème 2.5.1. *Soit $Y \in \mathcal{M}_{N\times L}(k)$ de rang $L < N$. Il existe L vecteurs $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_L$ de $E = k^L$ linéairement indépendant tels que $Y\boldsymbol{u}_l \in O_k^N$ pour tout l et tel que, si r_2 est le nombre de places complexes à l'infini, on a :*

$$\prod_{l=1}^{L} h(Y\boldsymbol{u}_l) \leq \left(\left(\frac{2}{\pi}\right)^{r_2}\sqrt{|\Delta_k|}\right)^{\frac{L}{d}} H(Y).$$

Démonstration : Soit $\mathcal{S}$ la "tranche" L-dimensionnelle du cube précédemment définie, soit $\lambda > 0$ et soit $\mathbf{u}$ un vecteur non nul de $(\lambda\mathcal{S}) \cap E$. Par définition de $\lambda\mathcal{S}$, on a :

$$\max_{1\leq n\leq N} ||(Y\mathbf{u})_n||_v < \frac{\lambda}{2} \;\; \textit{si } v \textit{ est réelle} \tag{2.7}$$

$$\max_{1\leq n\leq N} ||(Y\mathbf{u})_n||_v < \frac{\lambda}{\sqrt{2\pi}} \;\; \textit{si } v \textit{ est complexe} \tag{2.8}$$

$$\max_{1\leq n\leq N} ||(Y\mathbf{u})_n||_v \leq 1 \;\; \textit{sinon.} \tag{2.9}$$

De plus, comme $\mathbf{u} \in E$, $Y\mathbf{u} \in k^N$ et donc l'inégalité (9) montre que $Y\mathbf{u} \in O_k^N$. On prend le produit sur toutes les places et un petit calcul (en utilisant le fait que $r_1 + 2r_2 = d$, où r_1 est le nombre de plongements réels), montre que :

$$\prod_v \left(\max_{1\leq n\leq N} ||(Y\mathbf{u})_n||_v^{\frac{d_v}{d}}\right) = h(Y\mathbf{u}) < \frac{\lambda}{2}\left(\frac{2}{\pi}\right)^{\frac{r_2}{d}}.$$

Soit $0 < \lambda_1 \leq \lambda_2 \leq \ldots \leq \lambda_L < \infty$ les minimums successifs de $\mathcal{S}$. Comme précédemment, il existe un ensemble de vecteurs linéairement indépendant $\mathbf{u}_1, \ldots, \mathbf{u}_L$ tel que $\forall\lambda > \lambda_l$ on a $\mathbf{u}_l \in (\lambda\mathcal{S}) \cap E$. On a $Y\mathbf{u}_l \in O_k^N$ et :

$$\forall l \in [1,L] \;\; h(Y\mathbf{u}_l) \leq \left(\frac{\lambda_l}{2}\right)\left(\frac{2}{\pi}\right)^{\frac{r_2}{d}}$$

On prend alors le produit sur tout les l, on applique le théorème de Minkowski puis l' inégalité du cube slicing ce qui conclut. $\square$

Théorème 2.5.2. ***Siegel 1*** *Soit $A \in \mathcal{M}_{M\times N}(k)$ de rang $M < N$. Alors il existe $N-M$ vecteurs linéairement dans O_k^N, $\boldsymbol{x}_1,\ldots,\boldsymbol{x}_{N-M}$, satisfaisant :*

$$(1)\ \forall l \in [1,L]\ A\boldsymbol{x}_l = 0 \text{ et,}$$

$$\prod_{l=1}^{N-M} h(\boldsymbol{x}_l) \leq \left(\left(\frac{2}{\pi}\right)^{r_2}\sqrt{|\Delta_k|}\right)^{\frac{N-M}{d}} H(A).$$

Démonstration : Le rang de A est M, donc l'espace des solutions est de dimension $N-M = L$. Soit $\mathbf{y}_1,\ldots\mathbf{y}_L$ une base des solutions, posons $Y = (\mathbf{y}_1,\ldots\mathbf{y}_L)$ pour la matrice correspondante. On peut appliquer le théorème précédent à Y. Si $\mathbf{u}_1,\ldots\mathbf{u}_L$ sont les vecteurs ainsi obtenus, notons enfin $\mathbf{x}_l = Y\mathbf{u}_l$, pour $l \in [1,L]$. Clairement ces vecteurs sont linéairement indépendants (par injectivité de Y) et sont solutions du système (1). De plus, on a :

$$\prod_{l=1}^{L} h(\mathbf{x}_l) \leq \left(\left(\frac{2}{\pi}\right)^{r_2}\sqrt{|\Delta_k|}\right)^{\frac{L}{d}} H(Y).$$

Par un théorème de P. Gordan (admis, cf [3]) on a $H(Y) = H(A)$, d'où le résultat. $\square$

On va maintenant donner divers raffinements de ce théorème.

Soit K une extension finie du corps de nombre k telle que $[K/k] \geq 2$. On considère toujours le même système avec cette fois A à coefficient dans K. On voudrait déterminer une base de solutions dans k^N.

Soit F un corps de nombre contenant K, qui est galoisien sur k de groupe de Galois $G(F/k)$. En particulier F est galoisien sur K de groupe $G(F/K)$, sous groupe d'indice r de $G(F/k)$. Soit $\sigma_1,\ldots,\sigma_r$ un système de représentants des classes de $G(F/K)$ dans $G(F/k)$. On note $\mathcal{A}$ la matrice de taille $Mr \times N$:

$$\mathcal{A} = \begin{pmatrix} \sigma_1(A) \\ \sigma_2(A) \\ \ldots \\ \sigma_r(A) \end{pmatrix}.$$

On peut alors exprimer une seconde version du Lemme de Siegel.

Théorème 2.5.3. ***Siegel 2*** *Soit $\mathcal{A}$ la matrice précédente que l'on suppose de rang $Mr < N$. Alors il existe $N-Mr$ vecteurs linéairement indépendants $\boldsymbol{x}_1,\ldots,\boldsymbol{x}_{N-Mr}$ dans O_k^N satisfaisant :*

$$\forall l \in [1,N-Mr] \quad A\boldsymbol{x}_l = 0$$

et

$$\prod_{l=1}^{N-Mr} h(\boldsymbol{x}_l) \leq \left(\left(\frac{2}{\pi}\right)^{r_2}|\Delta_k|^{\frac{1}{2}}\right)^{\frac{N-Mr}{d}} H(\mathcal{A}).$$

Démonstration : Soit $\omega_1,\dots,\omega_r$ une base de K sur k. Pour tout m et n il existe des $b_{mn}(j)$ dans k tels que $a_{mn} = \sum \omega_j b_{mn}(j)$ **(1)**. On a ainsi :

$$\sum_{n=1}^{N} a_{mn}x_n = \sum_{j=1}^{r} \omega_j \left(\sum_{n=1}^{N} b_{mn}(j)x_n\right)$$

On trouve un vecteur $\mathbf{x}$ solution dans k^N si et seulement si $\mathbf{x}$ est solution du système

$$\sum_{n=1}^{N} b_{mn}(j)x_n = 0, \quad m \in [1,M], \ \ j \in [1,r]. \qquad \mathbf{(2)}$$

On définit donc les matrices B(j), pour $j \in [1,r]$ par $B(j) = (b_{mn}(j))$, et on les assemble par blocs pour former une matrice de taille $Mr \times N$:

$$\mathcal{B} = \begin{pmatrix} B(1) \\ \dots \\ B(r) \end{pmatrix}.$$

On définit aussi une matrice de taille $Mr \times Mr$ que l'on définit par blocs :
$\Omega = (\sigma_i(\omega_j)I_M)$ où I_M est l'identité de taille M. Si on applique σ_i à l'égalité **(1)**, on obtient le système matriciel $\Omega\mathcal{B} = \mathcal{A}$ **(3)**. Or par construction, Ω est inversible, donc on a nécessairement $rg(\mathcal{B}) = rg(\mathcal{A} = Mr < N$, on peut donc appliquer Siegel 1 au système **(2)** déterminé par $\mathcal{B}$: il existe N-Mr vecteurs linéairement indépendants $\mathbf{x}_1,\dots,\mathbf{x}_{N-Mr}$ dans O_k^N vérifiant ce qu'il faut.
(Le seul point à vérifier est que $H(\mathcal{B}) = H(\mathcal{A})$ ce qui est clair par **(3)**). □

Enfin, dans la borne sur les hauteurs obtenue dans Siegel 2, la hauteur $H(\mathcal{A})$ dépend de l'extension galoisienne F. Il peut être plus agréable d'avoir une borne dépendant seulement de la hauteur des lignes de A. On note $A^{(m)}$, $m \in [1,M]$ la m^{eme} ligne de A.

Corollaire 2.5.1. *Soit $\mathcal{A}$ vérifiant les hypothèses du théorème précédent, alors :*

$$H(\mathcal{A}) \leq H(A)^r \leq \prod_{m=1}^{M} \left(H(A^{(m)})\right)^r.$$

On peut donc réénoncer le théorème précédent en utilisant ces bornes.

Démonstration : $H(\mathcal{A}) \leq \prod_v H_v(\sigma_i(A)) = H(A)^r \leq H(A^{(m)})^r$, d'où le résultat. □

2.6 Une application

Pour la preuve du résultat qui suit la référence est l'article de Bombieri-Mueller.

Définition 2.6.1 Soit $\alpha = \sqrt[r]{\frac{a}{b}}$ avec a et b des entiers premiers entre eux, tels que α est de degré r sur $\mathbb{Q}$. On dit que $\mu(\alpha)$ est une mesure d'irrationnalité pour α si :

$$\forall\varepsilon > 0 \ \forall p,q \geq 1 \ \ |\alpha - \frac{p}{q}| > \frac{C(\alpha,\varepsilon)}{q^{\mu+\varepsilon}} > 0.$$

On dit que $\mu(\alpha)$ est effective si de plus $C(\alpha,\varepsilon)$ est effectivement calculable pour tout $\varepsilon > 0$. On note μ_{eff} la meilleure des mesures effectives.

Théorème 2.6.1. *Soit $r \geq 3$, a et b comme ci-dessus, $\lambda = \frac{\ln|a-b|}{\ln b}$, et soit $\alpha \in \mathbb{Q}(\sqrt[r]{\frac{a}{b}})$.*

$$\text{Si } \lambda < 1 - \frac{2}{r}, \text{ alors } \mu_{eff}(\alpha) \leq \frac{2}{1-\lambda} + 6\left(\frac{r^5 \ln r}{\ln b}\right)^{\frac{1}{3}}.$$

Exemple 2.6.1 2,67 est une mesure d'irrationnalité pour $\left(\frac{m^4+m+1}{m^4+7}\right)^{\frac{1}{r}}$, pour tout $m > m_o(r)$.

Chapitre 3

Mémoire de DEA : Lemme de Esnault-Viehweg-Dyson

Sommaire

3.1 Rappels de géométrie algébrique 34

3.1.1 Les différentielles 34

3.1.2 Normalisation et applications propres 36

3.1.3 Morphismes entre courbes 38

3.1.4 Les diviseurs 38

3.1.5 Éclatements 40

3.1.6 Formule de la projection pour les faisceaux 44

3.2 Théorie de l'intersection 45

3.2.1 Ordre des zéros et des pôles 46

3.2.2 Cycles et équivalence rationnelle 46

3.2.3 Image directe de cycles 47

3.2.4 Degré d'un cycle 51

3.2.5 Degré et polynôme de Hilbert 52

3.2.6 Image réciproque plate de cycles 55

3.2.7 Intersection avec des diviseurs 56

3.2.8 Commutativité des classes d'intersection 58

3.2.9 Classe de Chern d'un fibré en droites 61

3.2.10 Diviseurs numériquement effectifs 62

3.3 Le lemme de Dyson selon M. Nakamaye. 65

3.3.1 Énoncé des théorèmes 65

3.3.2 Le faisceau d'idéaux $\mathcal{I}_d(s)$ 67

3.3.3 Le théorème du produit 71

3.3.4 Fin de la preuve du théorème 3.3.2 74

3.3.5 Preuve du théorème 3.3.1 80

Mémoire de DEA dirigé par Marc Hindry

Un schéma de démonstration classique en approximation diophantienne est le suivant : on construit un polynôme auxiliaire F qui s'annule avec un grand ordre en un certain nombre de points approximants, puis on borne l'ordre d'annulation de F en ces points afin d'en tirer une contradiction. La première étape s'effectue en général avec des lemmes du type lemme de Siegel (cf par exemple [BV83]). Pour la seconde étape, une méthode consiste à appliquer des lemmes de zéros. On peut distinguer deux types de lemmes de zéros : le premier type, du originellement à Masser-Wüstholz, impose une configuration géométrique précise pour l'ensemble des points d'annulations et utilise l' opérateur de translation donné par la loi du groupe algébrique avec lequel on travaille ; le second type laisse plus libre sur la configuration initiale, mais, utilisant des dérivations, il s'utilise essentiellement en caractéristique nulle. On obtient dans ce dernier cas les lemmes de Dyson (on trouve une preuve du théorème de Roth par cette méthode dans [Sch91]).

L'objet de ce mémoire est de démontrer deux théorèmes du type lemme de Dyson, en suivant exactement l'article "Intersection theory and diophantine approximation" de M. Nakamaye, paru dans le *Journal of Algebraic Geometry*, volume 8, de 1999. Le théorème 1 est une légère amélioration d'une version dûe à Esnault-Viehweg (cf [EV84]), le second théorème, est dû à Nakamaye. Le grand intérêt de la démonstration que l'on va présenter ici, est de simplifier la preuve de Esnault-Viehweg, qui utilise le théorème d'annulation de Kodaira généralisé. On remplace ici l'emploi de théorèmes d'annulation cohomologiques profonds par l'utilisation de la théorie de l'intersection. On commence tout d'abord par effectuer un certain nombre de rappels de géométrie algébrique, puis, en suivant le livre de Fulton [Ful98], on donne les bases de la théorie de l'intersection dont nous aurons besoin. La dernière partie est consacrée à la preuve des deux théorèmes.

Dans toute la suite, un *schéma* désignera un schéma de type fini noethérien au dessus d'un corps K, une *variété* désignera un schéma intègre, une *sous-variété* désignera un sous-schéma intègre fermé, et un *point* désignera un point fermé.
K désignera un corps algébriquement clos, de caractéristique zéro, et on notera $\mathcal{R}(X)$ le corps des fonctions rationnelles sur X.

3.1 Rappels de géométrie algébrique

3.1.1 Les différentielles

Théorème 3.1.1. *Soit L/K une extension de corps qui est finiment engendrée, alors $dim_L\ \Omega_{L/K}$=$deg_{tr}(L/K)$.*
Démonstration : Soit L/K une extension et soit M une extension de corps, algébrique ou transcendante finie, du corps L. Notons $r(M) = \dim_M \Omega_{M/K}$, et $r(L) = \dim_L \Omega_{L/K}$, on va comparer r(M) et r(L). Le corps L est de caractéristique 0, donc par le théorème de l'élément primitif, on sait que $M = L(t_1, \ldots, t_n, x)$ avec x algébrique sur $L(t_1, \ldots, t_n)$ et $t_1, \ldots, t_n$ algébriquement indépendants sur L. On va étudier séparément deux cas :
1. On suppose ici que $M = L(t)$ avec t transcendant sur L, montrons l'égalité de dimensions $r(M) = r(L) + 1$. On a :

$$\Omega_{L[t]/K} \simeq (\Omega_{L/K} \otimes_L L[t]) \oplus L[t]dt,$$

en localisant par rapport à t, i.e en inversant t, on en déduit donc que

$$\Omega_{M/K} \simeq (\Omega_{L/K} \otimes_L M) \oplus Mdt.$$

On en déduit immédiatement le résultat.
2. On suppose maintenant que $M = L(x)$ avec x algébrique sur L de polynôme minimal f, montrons que $r(M) = r(L)$. On a :

$$\Omega_{M/K} \simeq \left(\Omega_{L/K} \otimes_L M \oplus MdX\right)/L\delta f$$

où $\delta f(x) = (df)(x) + f'(x)dX$. L'égalité précédente découle de la seconde suite exacte fondamentale. Or $f'(x) \neq 0$, donc $f'(x)$ est inversible dans M, donc on a :

$$\Omega_{M/K} \simeq \Omega_{L/K} \otimes_L M.$$

On en déduit l'égalité des dimensions.
Par une récurrence descendante immédiate on déduit le résultat, de cette étude. □

Lemme 3.1.1. *Soit A un anneau local, intègre, noethérien, de corps résiduel K et de corps des fractions F. Si M est un A-module de type fini, et si on a l'égalité de dimension $dim_K M \otimes_A K = dim_F M \otimes_A F = r$, alors, M est libre de rang r.*

Démonstration : Comme $\dim_K M \otimes_A K = r$, alors par le lemme de Nakamaya, on sait que M est engendré par r éléments. On a donc une application surjective $\varphi : A^r \to M$, de noyau Ker φ. En passant au corps des fractions, on en déduit la suite exacte :

$$0 \to \mathrm{Ker}\ \varphi \otimes_A F \to F^r \to M \otimes_A F \to 0.$$

Or on sait que $\dim_F M \otimes_A F = r$, donc on en déduit que Ker $\varphi \otimes_A F = 0$, et donc, Ker $\varphi = 0$, ce qui conclut. □

Proposition 3.1.1. *Soit B un anneau local contenant K, tel que $K \simeq B/\mathfrak{M}$ où $\mathfrak{M}$ est l'idéal maximal de B. Si B est noethérien, et est la localisation d'une K-algèbre de type fini, alors $\Omega_{B/K}$ est un B-module libre de rang dim B si et seulement si B est régulier.*

Démonstration : 1. On suppose que $\Omega_{B/K}$ est un B-module libre de rang dim B. Il suffit de montrer que l'application $\delta : \mathfrak{M}/\mathfrak{M}^2 \to \Omega_{B/K} \otimes_B K$ donnée dans la seconde suite exacte fondamentale, est un isomorphisme. Or avec nos hypothèses, δ est clairement surjective, il suffit donc de montrer qu'elle est injective. Pour cela, il suffit de voir que l'application duale

$$\delta' : \mathrm{Hom}_K(\Omega_{B/K} \otimes K, K) \to \mathrm{Hom}_K(\mathfrak{M}/\mathfrak{M}^2, K)$$

est surjective. Le membre de gauche de δ' est isomorphe à $\mathrm{Hom}_B(\Omega_{B/K}, K)$. Or on peut, par définition, identifier ce B-module avec $\mathrm{Der}_K(B, K)$. Si $d : B \to K$ est une dérivation, alors $\delta'(d)$ est simplement obtenu par restriction à $\mathfrak{M}$ (en notant que $d(\mathfrak{M}^2) = 0$). Montrons maintenant que δ' est surjective : soit $h \in \mathrm{Hom}_K(\mathfrak{M}/\mathfrak{M}^2, K)$, on veut construire une K-dérivation de B dans K telle que $\delta'(d) = h$. On note pour cela que tout $b \in B$ s'écrit de manière unique sous la forme $b = \lambda + m$, avec $\lambda \in K$ et $m \in \mathfrak{M}$. On pose alors, $d(b) = h(\overline{m})$ où $\overline{m}$ est la projection de m dans $\mathfrak{M}/\mathfrak{M}^2$. On vérifie alors que d répond à la question.

2. On montre maintenant la réciproque. Soit donc B anneau local, régulier, de dimension r. On a dim $\mathfrak{M}/\mathfrak{M}^2 = r$, donc par l'isomorphisme δ on sait que :
$\dim_K \Omega_{B/K} \otimes_B K = r$. Par ailleurs, si F est le corps de fractions de B, alors on a, par changement de base $\Omega_{B/K} \otimes_B F = \Omega_{F/K}$. Or par le théorème 3.1.1, on sait que $\dim_F \Omega_{F/K} = deg_{tr}(F/K) = \dim B$. Enfin, comme B est la localisation d'une K-algèbre de type fini, on sait que $\Omega_{B/K}$ est un B-module de type fini. Le lemme 3.1.1 précédent nous permet alors de conclure que $\Omega_{B/K}$ est un B-module libre de rang r. □

Théorème 3.1.2. *Soit X une variété sur K, alors, $\Omega_{X/K}$ est localement libre de rang dim $X = n$, si et seulement si, X est une variété lisse sur K.*

Démonstration : Si tous les points fermés sont lisses, alors X est lisse, car le localisé d'un anneau local régulier en un idéal premier est encore local régulier. Ainsi il suffit de montrer que si x est un point fermé de X, alors, x est lisse. Soit donc x un tel point, alors, $B = O_{X,x}$ est de dimension n, de corps résiduel K et est un localisé d'une K-algèbre de type fini, car X est de type fini sur K. On a :

$$\begin{aligned}
(\Omega_{X/K})_x &\simeq (\Omega_{U/K})_x \text{ avec } U = \text{Spec } A \text{ voisinage de } x,\\
&\simeq \widetilde{(\Omega_{A/K})}_x,\\
&\simeq \Omega_{A_x/K},\\
&\simeq \Omega_{B/K} \text{ car } O_{X,x} \simeq O_{U,x} \simeq A_x.
\end{aligned}$$

Donc par la proposition 3.1.1, on en déduit que B est un anneau régulier, c'est à dire que le point x est lisse, si et seulement si $(\Omega_{X,K})_x$ est libre de rang n. □

Corollaire 3.1.1. *Soit X une variété sur K, alors il existe un ouvert lisse U de X.*

Démonstration : Posons $n = \dim X$. Le corps $L = \mathcal{R}(X)$ est de degré de transcendance n sur K, donc on a (par le théorème 3.1.1) $\dim_L \Omega_{L/K} = \deg_{tr}(L/K) = n$. Or $\Omega_{L/K}$ est la tige de $\Omega_{X/K}$ au point générique, x, de X. Comme X est noethérien, il existe un voisinage U ouvert de x tel que $(\Omega_{X/K})_U$ est libre de rang n. Le théorème précédent permet alors de conclure. □

3.1.2 Normalisation et applications propres

On effectue ici des rappels concernant la notion de normalisation d'une variété, et concernant les morphismes propres.

Définition 3.1.1 Soit X une variété, on dit que le couple $(\tilde{X},\pi)$ est la *normalisation de X*, si $\tilde{X}$ est une variété normale telle que $\mathcal{R}(X) = \mathcal{R}(\tilde{X})$, et si $\pi : \tilde{X} \to X$ est un morphisme fini surjectif égal à l'identité au niveau de $\mathcal{R}(X)$. Notons que cette définition n'est valide que si l'on a l'existence et l'unicité d'une normalisation. C'est ce que nous dit le théorème suivant :

Théorème 3.1.3. *Soit X une variété, alors il existe, à isomorphisme unique près, une unique normalisation $(\tilde{X},\pi)$.*

Démonstration : 1. On montre d'abord l'unicité : on considère pour cela un recou- vrement de X par des ouverts affines U_i = Spec A_i. Soit (Y_1,π_1) et (Y_2,π_2) deux normalisations de X, notons $S_{i,1} = O_{Y_1}(\pi_1^{-1}(U_i))$ et pareil pour $S_{i,2}$. Alors, $S_{i,1}$ et $S_{i,2}$ sont tous deux intégralement clos dans $\mathcal{R}(X)$ et donc égaux à la clôture intégrale de A_i dans $\mathcal{R}(X)$. Comme π_1 et π_2 sont finis, on peut définir un isomorphisme ϕ_i, de $\pi_1^{-1}(U_i)$ sur $\pi_2^{-1}(U_i)$ en le définissant comme induit par l'application identité entre $S_{i,1}$ et $S_{i,2}$. Ces isomorphismes ϕ_i sont les seuls qui induisent l'identité sur les corps de fonctions, donc on peut les recoller pour former ainsi l'unique isomorphisme entre les deux normalisations.
2. Montrons maintenant l'existence du couple $(\tilde{X},\pi)$. On commence par supposer X affine : X = Spec A. Soit B la clôture intégrale de A, on sait que B est un A-module de type fini. Soit donc Y = Spec B et π le morphisme de Y dans X définit par l'inclusion de A dans B. Alors, Y est normale et π vérifie les conditions voulues. Dans le cas général on recouvre X par des ouverts affines U_i puis, pour tout i on fabrique une normalisation de

U_i que l'on recolle en une normalisation sur X grâce à l'unicité. □

Proposition 3.1.2. *Soit X une variété et Z une variété normale et $f : Z \to X$ un morphisme surjectif, alors f induit un morphisme $\tilde{f} : Z \to \tilde{X}$, tel que $\pi \circ \tilde{f} = f$.*
Démonstration : Comme précédemment on se ramène au cas où $X = \text{Spec } A$ est affine. Dans ce cas, on vient de voir que $\tilde{X} = \text{Spec } B$, où B est la clôture intégrale de A dans $\mathcal{R}(X)$. Ainsi il suffit de définir, un morphisme ϕ de $B \subset \text{Frac}(A)$ dans $A_1 = O_Z(f^{-1}(X))$ prolongeant le morphisme de A dans A_1, d'où le résultat. □

On rappelle maintenant un lemme concernant les applications propres et séparées :
Lemme 3.1.2. *Soit $f : X \to Y$ et $g : Y \to Z$ deux morphismes de schémas noethériens.*
1. Si $g \circ f$ est de type fini, alors f est de type fini.
2. Si $g \circ f$ est séparé, alors f est séparé.
3. Si $g \circ f$ est propre et si g est séparé, alors f est propre.
4. Le composé de deux morphismes propres est propre.
5. Les morphismes propres sont stables par changement de base.
6. Si on peut recouvrir Y par des ouverts Y_i tels que le morphisme $f^{-1}(Y_i) \to Y_i$ est propre pour tout i, alors f est propre.
Démonstration : On commence par montrer le point 1. : par noethérianité de X il suffit de montrer que f est localement de type fini. Soit $U = \text{Spec } A$ un ouvert de Y. On recouvre $g(U)$ par des ouverts affines $U_i = \text{Spec } A_i$, $i \in I$. Or $g \circ f$ est de type fini, donc, pour tout i, $(g \circ f)^{-1}(U_i)$ est recouvert par des ouverts Spec A_{ij} où A_{ij} est une A_i algèbre de type fini. Or

$$\bigcup_I (g \circ f)^{-1}(U_i) = (g \circ f)^{-1}(\bigcup_I U_i) \supset (g \circ f)^{-1}(g(U)) \supset f^{-1}(U).$$

Donc on a recouvert $f^{-1}(U)$ par des ouverts affines Spec A_{ij} où les A_{ij} sont des A_i-algèbres de type fini, donc a fortiori des A-algèbres de type fini.
Les points 2. et 3. sont des conséquences faciles des critères valuatifs pour les morphismes séparés, respectivement propres. Montrons par exemple le point 3. : Le morphisme $g \circ f$ est propre , en particulier de type fini, donc par le point 1., f est de type fini, et par le point 2., f est séparé. Soit donc A un anneau de valuation, $U = \text{Spec } A$, $T = \text{Spec}(\text{Frac } A)$, et des morphismes $U \to X$ et $T \to Y$ rendant commutatif le diagramme

$$\begin{tikzcd}
U \arrow[r] \arrow[d] & X \arrow[d, "f"] \\
T \arrow[r, "u_1", "u_2"'] \arrow[d, "id_T"'] & Y \arrow[d, "g"] \\
T \arrow[r, "h"'] & Z
\end{tikzcd}$$

et montrons qu'il existe (au moins) un morphisme de T dans X tel que tous les diagrammes continuent à commuter. Soit $h = g \circ u_1 : T \to Z$, alors comme $g \circ f$ est propre, il existe

une application de T dans X commutant avec h. En composant ce morphisme avec f on obtient une seconde flèche, u_2 de T dans Y, or g étant séparé, on a nécessairement $u_1 = u_2$, d'où le résultat.
Les points 4. et 6. se démontrent exactement comme le point précédent, et le point 5. se démontre facilement, en utilisant la propriété universelle du produit fibré. □

3.1.3 Morphismes entre courbes

On rappelle ici deux résultats classiques concernant les applications entre courbes, dont nous aurons besoin dans le point 4. de la preuve du théorème fondamental concernant l'image directe de cycles algébriques.

Proposition 3.1.3. *Soit X une courbe propre et lisse sur K, soit Y une courbe propre sur K, et soit $f : X \to Y$ un morphisme non constant. Alors, f est surjectif, $K(X)$ est une extension finie de $K(Y)$ et f est fini.*

Démonstration : Notons π_X la projection propre de X sur K, et π_Y celle de Y sur K. On a $\pi_Y \circ f = \pi_X$, donc le point 3. du lemme 3.1.2 nous assure que f est propre. En particulier, $f(X)$ est un fermé irréductible de Y. Or $\dim Y = 1$, donc f est constante ou surjective. Par l'hypothèse on conclut que f est surjective. On en déduit que $K(Y)$ s'injecte dans $K(X)$, et comme ces deux corps sont des extensions de degré de transcendance 1 sur K, $K(X)$ est nécessairement algébrique finie sur $K(Y)$. Montrons maintenant que le morphisme est fini. Soit $V = \text{Spec } B$ un ouvert de Y, et soit A la fermeture intégrale de B dans $K(X)$. Alors, A est un B module de type fini, et l'ouvert $U = \text{Spec A}$ est exactement l'image réciproque de V par f. □

Proposition 3.1.4. *Soit C une courbe propre et lisse sur K et $f \in K(C)$ une application rationnelle non constante. Alors, f définit un mophisme non constant de C dans $\mathbb{P}^1$.*

Démonstration : L'application rationnelle définit un morphisme $\varphi : C \to \mathbb{P}^1$ en posant pour $P \in C$:

$$\begin{cases} \varphi(P) = [f(P) : 1] & \text{si } P \text{ n'est pas un pôle de } f, \\ \varphi(P) = [1 : 0] & \text{sinon.} \end{cases}$$

Ce morphisme (qu'on a pu définir car C est lisse) répond à la question. □

3.1.4 Les diviseurs

Diviseurs de Weil et de Cartier

Définition 3.1.2 Soit X une variété de dimension n, on note $Z_{n-1}X$ le groupe libre engendré par les sous-variétés de codimension 1 de X. Un élément de $Z_{n-1}X$ est appelé un *diviseur de Weil.*

Définition 3.1.3 Soit X un schéma et soit $\mathcal{R}$ le faisceau d'anneaux quotients totaux de O_X. Un *diviseur de Cartier* est une section globale de $\mathcal{R}^*/O_X^*$, i.e c'est la donnée de

$(U_i,f_i)_i$, où (U_i) est un recouvrement ouvert de X et $f_i \in \mathcal{R}(U_i)^*$, tel que sur $U_i \cap U_j$ on a $\frac{f_i}{f_j} \in O_X(U_i \cap U_j)^*$. L'ensemble des diviseurs de Cartier sur X forme un groupe noté CaDiv X : si $D = (U_i,f_i)_i$ et $E = (U_i,g_i)_i$, on note $D + E$ le diviseur de Cartier $(U_i,f_ig_i)_i$.

Un diviseur de Cartier $D = (U_i,f_i)_i$ sur un schéma X est dit *effectif* si : pour tout i, $f_i \in O_X(U_i)$. Dans ce cas on définit le *sous-schéma de Cartier de codimension 1* associé, Y, comme étant le sous-schéma fermé défini par le faisceau d'idéaux $\mathfrak{I}$ localement engendré par f_i. Ceci définit clairement une correspondance biunivoque entre les diviseurs de Cartier effectifs sur X et les sous-schémas Y fermés localement principaux, i.e dont le faisceau d'idéaux est localement engendré par un seul élément.
On définit le *support* d'un diviseur de Cartier D, comme étant :
Supp D= $|D| = \bigcup$ Z sous-variétés de X telles qu'il existe f_i, équation locale de D, appartenant à $O_{X,Z}$, et telle que $f_i \neq$ unité.
Soit $s : X \to Y$ un morphisme de schémas, et soit $D = (U_i,f_i)_i$ un diviseur de Cartier sur Y. Si X est une variété et si $s(X) \not\subset |D|$, alors on définit le diviseur de Cartier *image réciproque* s^*D de D dans X comme étant $s^*D = (s^{-1}(U_i),f_i \circ s)_i$.

Quand X est une variété, on peut construire un morphisme naturel ϕ de CaDiv X dans $Z_{n-1}X$: soit $D \in$ CaDiv X et soit V une sous-variété de codimension 1 de X. On pose

$$\mathrm{ord}_V D = \mathrm{ord}_V f_i, \text{ où } i \text{ est tel que } U_i \cap V \neq \emptyset.$$

(ceci a un sens car si j est tel que $U_j \cap V \neq \emptyset$, alors $\frac{f_i}{f_j} \in O_X(U_i \cap U_j)^*$, donc $\mathrm{ord}_V f_i = \mathrm{ord}_V f_j$).
On définit ainsi un diviseur de Weil : $[D] = \sum\limits_V \mathrm{ord}_V D\ [V]$.

Définition 3.1.4 On appelle diviseur de Cartier *principal* tout diviseur de Cartier appartenant à l'image du morphisme canonique $\mathcal{R}^* \to \mathcal{R}^*/O_X^*$. Dans le cas des variétés, ceci correspond aux diviseurs de la forme (X,f), où $f \in \mathcal{R}(X)^*$. On note Pic X le groupe quotient CaDiv X /{diviseurs principaux}.
En supposant connue, la définition de $A_{n-1}X$ (cf paragraphe II.2 à venir), on constate alors que le morphisme ϕ précédemment défini, induit un morphisme (en général ni injectif ni surjectif)

$$\phi : \text{Pic X} \to A_{n-1}X.$$

On trouvera une démonstration du résultat suivant dans [Har77], p 141 :
Théorème 3.1.4. *Si X est une variété séparée localement factorielle, alors ϕ est un isomorphisme.*
Corollaire 3.1.2. *Si X est une variété lisse, séparée alors ϕ est un isomorphisme.*
Remarque : une variété projective est propre donc séparée, donc si X est une variété projective lisse de dimension n sur un corps K algébriquement clos, Pic $X \simeq A_{n-1}X$.

Diviseurs et fibrés en droite

Si X est un schéma, et $D = (U_i,f_i)_i$ un diviseur de Cartier, on peut toujours lui associer un fibré en droite $O_X(D)$: par définition, $O_X(D)$ est le sous-faisceau de O_X-modules de

$\mathcal{R}$, engendré sur U_i par f_i^{-1}.

Proposition 3.1.5. *Soit D un diviseur de Cartier effectif sur un schéma X et soit Y le sous-schéma de Cartier associé, alors :* $\mathfrak{I}_Y \simeq O_X(-D)$.

Démonstration : Le faisceau $O_X(-D)$ est le sous-faisceau de $\mathcal{R}$, localement engendré par f_i. Or comme D est effectif, pour tout i, f_i est dans $O_X(U_i)$, donc $O_X(-D)$ est en fait un sous-faisceau de O_X. C'est donc $\mathfrak{I}_Y$. □

Proposition 3.1.6. *Si X est un schéma intègre alors l'application de Pic X dans, le groupe des classes d'isomorphismes de faisceaux inversibles sur X pour l'opération ⊗, est un isomorphisme.*

Démonstration : Il faut d'abord montrer que tout faisceau inversible est isomorphe à un sous-faisceau inversible de $\mathcal{R}$. On sait que X est intègre donc $\mathcal{R}$ est le faisceau constant $\mathcal{R}$. Soit $\mathcal{L}$ un faisceau inversible de O_X-modules, considérons le faisceau $\mathcal{L} \otimes_{O_X} \mathcal{R}$, et soit $(U_i)_i$ une trivialisation de $\mathcal{L}$. Sur U_i, on a : $(\mathcal{L} \otimes_{O_X} \mathcal{R})_{|U_i} \simeq \mathcal{R}_{|U_i}$. De plus, l'espace X est irréductible, donc, si $\mathcal{F}$ est un faisceau tel que la restriction aux ouverts d'un recouvrement de X est le faisceau constant, alors, $\mathcal{F}$ est en fait constant. Ainsi le faisceau $\mathcal{L} \otimes_{O_X} \mathcal{R}$ est constant, isomorphe à $\mathcal{R}$. Or $\mathcal{L}$ en est un sous-faisceau, d'où le résultat.

Montrons maintenant la bijectivité : soit $\mathcal{L}(D)$ un sous-faisceau inversible de $\mathcal{R}$. On choisit une trivialisation U_i et pour tout i, f_i l'inverse d'un générateur de $\mathcal{L}(D)_{|U_i}$. Le diviseur $D = (U_i, f_i)$ ainsi construit, définit une application qui est clairement réciproque de celle qui à un diviseur de Cartier associe un fibré en droite, d'où le résultat. □

Corollaire 3.1.3. *Soit* $X = \prod_{i=1}^{m} \mathbb{P}^{n_i}$, *alors tout fibré en droite sur X est isomorphe à* $O_X(d_1, \ldots, d_m)$ *pour un certain* $d = (d_1, \ldots, d_m) \in \mathbb{Z}^m$.

Remarque : on peut noter que $H^0(\mathbb{P}, O_{\mathbb{P}}(d_1, \ldots, d_m)$ est isomorphe à l'espace vectoriel des polynômes multihomogènes de degré $d = (d_1, \ldots, d_m)$ sur $K[X_1, Y_1, \ldots, X_m, Y_m]$.

Définition 3.1.5 Soit s une section d'un fibré en droite, L, sur un schéma X. On note $(s_i)_i$ la section s vue dans la trivialisation $(U_i)_i$ de L. Par définition, on appelle *schéma des zéros de* s le sous-schéma de Cartier de codimension 1, $Z(s)$, engendré par s_i sur U_i.

3.1.5 Éclatements

On définit ici l'éclatement selon une sous-variété, et on en rappelle les principales propriétés.

Construction de Proj

On connait le Proj d'un anneau gradué, on va ici définir le **Proj** d'un faisceau d'algèbre graduée $\mathcal{S}$ sur un schéma X. Dans la suite de cette partie on supposera que :

$(\star)$: X noethérien, $\mathcal{S}$ faisceau quasi-cohérent de O_X modules, ayant une structure de faisceau de O_X algèbre graduée, telle que $\mathcal{S} = \bigoplus_{d \geq 0} \mathcal{S}_d$ où $\mathcal{S}_0 = O_X$ et où $\mathcal{S}_1$ est un O_X-module cohérent qui engendre localement $\mathcal{S}$ comme O_X algèbre.

Construction Soit X un schéma et $\mathcal{S}$ un faisceau gradué de O_X-algèbre satisfaisant l'hypothèse $(\star)$. Pour tout ouvert affine $U = \text{Spec}(A)$ de X, on écrit $\mathcal{S}(U) = \Gamma(U,\mathcal{S}_{|U})$. On considère ensuite Proj$(\mathcal{S}(U))$ et son morphisme naturel

$$\pi_U : \text{Proj } \mathcal{S}(U) \to U.$$

Si $f \in A$, alors $U_f = \text{Spec } A[\frac{1}{f}]$. Comme $\mathcal{S}$ est quasi-cohérent, Proj$(\mathcal{S}(U_f))$ est isomorphe à $\pi_U^{-1}(U_f)$, donc si U et V sont deux ouverts affines de X, alors $\pi_U^{-1}(U \cap V)$ est naturellement isomorphe à $\pi_V^{-1}(U \cap V)$. On peut donc recoller les schémas Proj$(\mathcal{S}(U))$, et on obtient alors un schéma **Proj**$(\mathcal{S})$ muni d'un morphisme **Proj(**$\mathcal{S}$**)** $\xrightarrow{\pi} X$ tel que, pour tout $U = \text{Spec } A \subset X$ on a :

$$\pi^{-1}(U) \simeq \text{Proj}(\mathcal{S}(U)).$$

De plus les faisceaux inversibles $O(1)$ sur chaque Proj$(\mathcal{S}(U))$ sont compatibles à la donnée de recollement fournie par cette construction (cf [Har77] II.5.12.C), donc se recollent ensembles pour former un faisceau inversible $O(1)$ sur **Proj** $\mathcal{S}$, canoniquement déterminé par cette construction.

On a ainsi construit **Proj** $\mathcal{S}$ avec un morphisme π : **Proj** $\mathcal{S} \to X$, et un faisceau inversible $O(1)$ associés. Tout ce qu'on sait sur Proj se transpose sur **Proj**.

Exemple 3.1.1 Si $\mathcal{S} = O_X[T_0, \dots, T_n]$ alors **Proj** $\mathcal{S} = \mathbb{P}^n_X$ muni du twist standard.

On rappelle ici un théorème classique sur les morphismes projectifs :

Théorème 3.1.5. *1. un morphisme projectif entre schémas noethériens est propre.*
2. Soit A un anneau, et X un A-schéma, si $\mathcal{L}$ est un faisceau inversible sur X engendré par les sections globales $s_0, \dots, s_n \in H^0(X,\mathcal{L})$, alors, il existe un unique A-morphisme $g : X \to \mathbb{P}^n_A$ tel que $\mathcal{L} \simeq g^*O(1)$ et tel que pour tout i, $s_i = g^*(x_i)$.

Proposition 3.1.7. *Si $(X,\mathcal{S})$ vérifie $(\star)$, soit $Y =$ **Proj** $\mathcal{S}$ muni de la projection naturelle π. Alors, π est un morphisme propre.*

Démonstration : Soit $U \subset X$ un ouvert affine. Le morphisme π_U est projectif, donc est propre par le point 1. du théorème 3.1.5 précédent. Mais alors on sait dans ce cas, d'après le point 6. du lemme 3.1.2 que π est propre. □

Éclatements

On commence par rappeler la notion intuitive d'éclatement selon un point, puis on s'intéresse à la notion plus générale d'éclatement selon un idéal.

Formellement, pour éclater un point P de $\mathbb{A}^n$, l'idée est de remplacer P par l'ensemble des droites passant par P, i.e par une copie de $\mathbb{P}^{n-1}$. Rigoureusement, on choisit le point P comme origine de $\mathbb{A}^n$, et on considère l'ensemble

$$B_P = \left\{(x,l) \in \mathbb{A}^n \times \mathbb{P}^{n-1} / \ x \in l\right\}$$

muni de la projection $\pi : B_P \to \mathbb{A}^n$. Le couple (B_P,π) est appelé l'éclatement de $\mathbb{A}^n$ en P. On retrouve bien l'idée formelle en considérant les fibres de l'application π : si $x \neq P$, alors $\pi^{-1}(x) = (x,l)$ où l est l'unique droite passant par x et P ; si $x = P$, alors $\pi^{-1}(P) = \{P\} \times \mathbb{P}^{n-1}$.

Proposition 3.1.8. *L'éclatement B_P de $\mathbb{A}^n$ en un point P est le fermé algébrique définit par $\mathbb{V}(x_iy_j - x_jy_i/\ 0 \leq i < j \leq n)$.*

Démonstration : Soit $x = (x_1 \ldots, x_n) \in \mathbb{A}^n$ et $l = [y_1, \ldots, y_n] \in \mathbb{P}^{n-1}$. Le point x est sur la droite l si et seulement si x est colinéaire à $(y_1, \ldots, y_n)$, donc si et seulement si la matrice

$$\begin{pmatrix} x_1 & \ldots & x_n \\ y_1 & \ldots & y_n \end{pmatrix}$$

est de rang inférieur à 1. Finalement, $x \in l$ si et seulement si les mineurs $x_iy_j - x_jy_i$ 2×2 de la matrice sont tous nuls, donc B_P est exactement de la forme annoncée. $\square$

On passe maintenant à la définition générale d'éclatement selon un fermé.

Définition 3.1.6 Soit X un schéma noethérien et soit $\mathfrak{I}$ un faisceau cohérent d'idéaux de X. On considère le faisceau d'algèbres graduées $\mathcal{S} = \bigoplus_{d \geq 0} \mathfrak{I}^d$. Alors le couple $(X,\mathcal{S})$ satisfait l'hypothèse $(\star)$, et on peut donc considérer BL_Y(X)=**Proj** $\mathcal{S}$, où Y désigne le sous-schéma fermé de X défini par $\mathfrak{I}$. On dit que BL_Y(X) est *l'éclatement de X de centre Y.*

Rappelons que si $f : X \to Y$ est un morphisme de schémas, et si $\mathfrak{I} \subset O_Y$ est un faisceau d'idéaux sur Y, on définit *le faisceau image inverse* $\mathfrak{I}' \subset O_X$ comme étant le faisceau $f^{-1}\mathfrak{I} \cdot O_X$. En général, ce faisceau est différent du faisceau image réciproque $f^*\mathfrak{I} = f^{-1}\mathfrak{I} \otimes_{f^{-1}O_Y} O_X$, par contre l'application naturelle de $f^*\mathfrak{I}$ dans O_X est d'image $f^{-1}\mathfrak{I} \cdot O_X$.

Proposition 3.1.9. *Soit X un schéma noethérien, $\mathfrak{I}$ un faisceau cohérent d'idéaux et soit $\pi : BL_Y(X) \to X$ l'éclatement de X de centre Y, alors :*
1. Le faisceau image inverse $\pi^{-1}\mathfrak{I} \cdot O_{BL_Y(X)}$ est isomorphe à $O_{BL_Y(X)}(1)$, et en particulier inversible.
2. Si $U = X - Y$ alors le morphisme $\pi : \pi^{-1}(U) \to U$ est un isomorphisme.

Démonstration : 1. Par construction, l'éclatement $\mathrm{BL}_Y(X)$, arrive équipé d'un faisceau naturel $O_{\mathrm{BL}_Y(X)}(1)$. Si U est un ouvert affine de X, alors par construction de **Proj**, ce faisceau $O(1)$ sur Proj $\mathcal{S}(U)$ est le faisceau associé au $\mathcal{S}(U)$-module gradué

$$\mathcal{S}(U)(1) = \bigoplus_{d \geq 0} \mathfrak{I}^{d+1}(U) = \mathfrak{I} \cdot \mathcal{S}(U).$$

Donc le faisceau image inverse est égal à $O_{\mathrm{BL}_Y(X)}(1)$.
2. Par définition de U, on a : $\mathfrak{I}_{|U} = O_U$. Ainsi, par construction de **Proj**, on en déduit que $\pi^{-1}(U) \simeq \mathrm{Proj}(O_U[T]) \simeq U$, d'où le résultat. $\square$

On pose $E = \pi^{-1}(Y)$, et on l'appelle le *diviseur exceptionnel* de l'éclatement.

Lemme 3.1.3. *Soit (X,O_X) un schéma localement noethérien et soit $f : \mathcal{L}_1 \to \mathcal{L}_2$ un morphisme surjectif de faisceaux inversibles sur X. Alors f est un isomorphisme.*

Démonstration : Dire que f est un isomorphisme se teste sur les tiges. Soit donc $x \in X$ montrons que l'application induite $f_x : E = (\mathcal{L}_1)_x \to (\mathcal{L}_2)_x = F$ est un isomorphisme. L'application f_x est un morphisme surjectif entre deux O_x-modules libres de rang 1. L'anneau A est noethérien, donc E est un A-module noethérien, et donc le noyau Ker f est de type fini. Par le lemme de Nakayama, il suffit donc de voir que Ker $f \subset \mathfrak{M}$Ker f pour conclure. En tensorisant par $- \otimes_A A/\mathfrak{M}$, on en déduit le diagramme commutatif :

$$\begin{array}{ccccccccc}
0 & \longrightarrow & Ker f & \longrightarrow & E & \xrightarrow{f} & F & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & 0 & \longrightarrow & E/\mathfrak{M}E & \xrightarrow{f_{\mathfrak{M}}} & F/\mathfrak{M}F & \longrightarrow & 0
\end{array}$$

En effet, il est clair que le lemme est vrai si A est un corps, d'où l'isomorphisme obtenu dans la suite exacte du bas. On en déduit que Ker $f = \mathfrak{M}$Ker f, ce qui conclut. $\square$

Théorème 3.1.6. ***(propriété universelle de l'éclatement)*** *Soit X un schéma noethérien, soit $\mathfrak{I}$ un faisceau d'idéaux, et soit $\pi : BL_Y(X) \to X$ l'éclatement de X de centre Y. Si $f : Z \to X$ est un morphisme tel que $f^{-1}\mathfrak{I} \cdot O_Z$ est un faisceau d'idéaux inversible sur Z, alors il existe un unique morphisme $g : Z \to BL_Y(X)$ factorisant f.*

Démonstration : Supposons le théorème démontré dans le cas où X est un schéma affine, alors par unicité de g et par construction de $BL_Y(X)$, on en déduit le théorème dans le cas général, par recollement. On suppose donc que X est affine, $X =$ Spec A où A est noethérien, et que le faisceau d'idéaux cohérent $\mathfrak{I}$ est déterminé par l'idéal I de A. On a alors $\mathrm{BL}_Y(X)$ =Proj S où $S = \bigoplus_{d\geq 0} I^d$. Si $a_0,\dots,a_n \in I$ désignent des générateurs de I, on définit un morphisme surjectif naturel d'anneaux gradués $\phi : A[X_0,\dots,X_n] \to S$ en envoyant X_i sur a_i. Ce morphisme induit une immersion fermée $\mathrm{BL}_Y(X) \hookrightarrow \mathbb{P}^n_A$. Le noyau de ϕ est constitué des polynômes F homogènes tels que $F(a_0,\dots,a_n) = 0$ dans A. Soit $f : Z \to X$ comme dans l'énoncé, on va maintenant construire le morphisme g. Comme I est engendré par $a_0,\dots,a_n$, les inverses $s_0,\dots,s_n$ de ces n éléments, considérés comme des sections globales sur Z engendrent le faisceau image inverse $\mathcal{L} = f^{-1}\mathfrak{I} \cdot O_Z$. Donc par le théorème 3.1.5 il existe un unique morphisme $g : Z \to \mathbb{P}^n_A$ tel que $\mathcal{L} \simeq g^*O(1)$ et tel que pour tout i $s_i = g^{-1}X_i$. Soit $F(X_0,\dots,X_n)$ un élément homogène de degré d de Ker ϕ, alors $F(a_0,\dots,a_n) = 0$ dans A, donc $F(s_0,\dots,s_n) = 0$ dans $H^0(Z,\mathcal{L}^d)$. De ceci on déduit que g se factorise à travers $\mathrm{BL}_Y(X)$, d'où l'existence de g.

Montrons maintenant l'unicité du morphisme g. Pour tout morphisme $h : Z \to \mathrm{BL}_Y(X)$ se factorisant par f, on a :

$$f^{-1}\mathfrak{I} \cdot O_Z = h^{-1}(\pi^{-1}\mathfrak{I} \cdot \mathrm{BL}_Y(X)) \cdot O_Z = h^{-1}(O_{\mathrm{BL}_Y(X)}(1)),$$

la dernière égalité découlant de la proposition précédente. Par le rappel, on en déduit une application surjective $h^*O_{\mathrm{BL}_Y(X)}(1) \to f^{-1}\mathfrak{I} \cdot O_Z = \mathcal{L}$. Or on sait par le lemme 3.1.3

que ce morphisme surjectif est un isomorphisme, donc $h^*O_{\mathrm{BL}_Y(X)}(1) \simeq \mathcal{L}$. Les sections s_i de $\mathcal{L}$ sont nécéssairement les images réciproques des sections X_i de $O(1)$ sur $\mathbb{P}^n_A$, donc l'assertion d'unicité du théorème 3.1.5 entraine l'unicité de g. $\square$

Proposition 3.1.10. *Soit X une variété sur K, soit $\mathfrak{I}$ un faisceau d'idéaux non nul, cohérent et soit $\pi : BL(X) \to X$ l'éclatement de X selon le fermé F associé à $\mathfrak{I}$. Alors, $BL(X)$ est une variété sur K, birationnelle à X.*

Démonstration : Le morphisme π est propre, donc de type fini sur K. De plus X est intègre, donc le faisceau associé à $\bigoplus \mathfrak{I}^n$ est intègre, donc, $BL(X)$ est une variété. De plus on sait déjà que π est un isomorphisme en dehors du diviseur exceptionnel, en particulier, π est une application birationnelle. $\square$

3.1.6 Formule de la projection pour les faisceaux

Avant d'énoncer et de démontrer la formule de la projection pour les faisceaux, on commence par rappeler le résultat suivant :

Théorème 3.1.7. *Soit $\pi : X \to Y$ un morphisme de schémas, soit $\mathcal{F}$ un faisceau sur X, et soit $\mathcal{G}$ un faisceau sur Y. On a une bijection canonique de $Hom(\pi^*\mathcal{G},\mathcal{F})$ sur $Hom(\mathcal{G},\pi_*\mathcal{F})$.*

Démonstration : Soit $f \in \mathrm{Hom}(\pi^*\mathcal{G},\mathcal{F})$, soit V un ouvert de Y, et soit $s \in \mathcal{G}$. Alors, $t : x \mapsto s_{\pi(x)}$ est une section de $\pi^*\mathcal{G}$ sur $U = \pi^{-1}(V)$. Donc $f_U(t)$ est une section de $\mathcal{F}$ sur $U = \pi^{-1}(V)$, c'est à dire, est une section de $\pi_*\mathcal{F}$ sur V. Les applications $g_V : \mathcal{G}(V) \to \pi_*\mathcal{F}(V)$ ainsi définies forment un morphisme $g : \mathcal{G} \to \pi_*\mathcal{F}$. L'application qui à f associe g est la bijection recherchée. $\square$

En particulier, si on applique ce théorème avec $\mathcal{F} = \pi^*\mathcal{G}$ et $f = Id_{\pi^*\mathcal{G}}$, on obtient un morphisme naturel de $\mathcal{G}$ dans $\pi_*\pi^*\mathcal{G}$.
De plus, en suivant la démonstration, on constate que, si π est surjective, alors, le morphisme naturel précédent est injectif.

Avant de passer à la formule de la projection, on rappelle un résultat concernant les faisceaux engendrés par leurs sections globales.

Lemme 3.1.4. *Soit $f : X \to Y$ un morphisme de schémas, $\mathcal{F}$ et $\mathcal{G}$ deux faisceaux de O_Y-module engendrés par leurs sections globales, alors :*
1. $\mathcal{F} \otimes_{O_Y} \mathcal{G}$ est engendré par ses sections globales.
2. $f^{-1}(\mathcal{F})$ et $f^*(\mathcal{F})$ sont engendrés par leurs sections globales.

Démonstration : Soit $y \in Y$, la tige de $\mathcal{F} \otimes_{O_Y} \mathcal{G}$ en y est $\mathcal{F}_y \otimes_{O_y} \mathcal{G}_y$. Si f_y et g_y sont des sections globales de $\mathcal{F}$ et, respectivement, $\mathcal{G}$, telles que $f_y(y) \neq 0$ et $g_y(y) \neq 0$, alors : la section $f_y \otimes g_y$ est une section globale du produit tensoriel, non nulle en y. Le point 2 se démontre de la même manière puisque on sait calculer les tiges en tout point des deux faisceaux : si $x \in X$, alors $(f^{-1}(\mathcal{F}))_x = \mathcal{F}_{f(x)}$ et $(f^*(\mathcal{F}))_x = \mathcal{F}_{f(x)} \otimes_{O_x} O_{f(x)}$. $\square$

Proposition 3.1.11. ***formule de la projection*** *Si $f : (X,O_X) \to (Y,O_Y)$ est un morphisme d'espace annelés, si $\mathcal{E}$ est un faisceau de O_Y-module localement libre de rang* *fini, et si $\mathcal{F}$ est un faisceau de O_X-module, on a :*

$$f_*\left(\mathcal{F} \otimes_{O_X} f^*\mathcal{E}\right) \simeq f_*\mathcal{F} \otimes_{O_Y} \mathcal{E}.$$

Démonstration : On va démontrer ceci en trois étapes. Les étapes 1 et 2 consistent à définir un morphisme naturel de $f_*\left(\mathcal{F} \otimes_{O_X} f^*\mathcal{E}\right)$ sur $f_*\mathcal{F} \otimes_{O_Y} \mathcal{E}$. L' étape 3 montre l'isomorphisme.
étape 1 : soit $\mathcal{M}$ et $\mathcal{N}$ deux faisceaux de O_X-modules, et soit U un ouvert de X. On a une application canonique

$$H^0(f^{-1}(U),\mathcal{M}) \times H^0(f^{-1}(U),\mathcal{N}) \to H^0(f^{-1}(U),\mathcal{M} \otimes_{O_X} \mathcal{N}),$$

bilinéaire sur $H^0(f^{-1}(U),O_X) = H^0(U,f_*(O_X))$ donc à fortiori sur $H^0(U,O_Y)$. Cette application définit donc un morphisme canonique

$$\varphi : f_*(\mathcal{M}) \otimes_{O_Y} f_*(\mathcal{N}) \to f_*(\mathcal{M} \otimes_{O_X} \mathcal{N}).$$

étape 2 : on sait que * et $_*$ sont adjoints, plus précisément, si $\mathcal{M}$ est un O_Y-module et $\mathcal{N}$ un O_X-module, on a l'isomorphisme :

$$Hom_{O_X}\left(f^*(\mathcal{M}),\mathcal{N}\right) \simeq Hom_{O_Y}\left(\mathcal{M},f_*(\mathcal{N})\right).$$

(Notamment, si on prend $\mathcal{N} = f^*(\mathcal{M})$, alors le morphisme $Id_{f^*(\mathcal{M})}$ induit un morphisme naturel :

$$\psi : \mathcal{M} \to f_*(f^*(\mathcal{M})).$$

étápe 3 : en regroupant les deux étapes précédentes, on a un morphisme naturel :

$$f_*(\mathcal{F}) \otimes_{O_Y} \mathcal{E} \overset{1\otimes\psi}{\to} f_*(\mathcal{F}) \otimes_{O_Y} f_*(f^*(\mathcal{E})) \overset{\varphi}{\to} f_*(\mathcal{F} \otimes_{O_X} f^*(\mathcal{E})).$$

Montrons que c'est un isomorphisme. Comme $\mathcal{E}$ est localement libre de rang n, on peut, le problème étant local sur Y, supposer $\mathcal{E} = O_Y^n$. De plus, f^* et f_* commutent au produit fini, donc on peut même supposer que $\mathcal{E} = O_Y$. Dans ce cas, le membre de droite est isomorphe à $f_*(\mathcal{F})$ et le membre de droite aussi, d'où le résultat. □

3.2 Théorie de l'intersection

On va maintenant s'attacher à rappeler les bases de la théorie de l'intersection, bases dont nous aurons besoin par la suite.

3.2.1 Ordre des zéros et des pôles

Soit X une variété, et V une sous-variété de X de codimension 1. L'anneau local $O_{V,X}$ est par définition, l'anneau local au point générique de V. Il est de dimension 1. Soit $r \in \mathcal{R}^*(X)$, on définit l'*ordre* d'annulation de r selon V, que l'on note $\text{ord}_V(r)$, de telle sorte que ce soit un homomorphisme, i.e :

$$\forall r,s \in \mathcal{R}^*(X) \quad \text{ord}_V(rs) = \text{ord}_V(r) + \text{ord}_V(s).$$

Tout $r \in \mathcal{R}^*(X)$ peut s'écrire sous la forme $r = \frac{a}{b}$, avec $a,b \in O_{V,X}$, donc on a nécessairement, $\text{ord}_V(r) = \text{ord}_V(a) - \text{ord}_V(b)$. Finalement, il suffit de définir ord_V pour des éléments de $A = O_{V,X}$. On pose alors :

$$\forall r \in A \;\; \text{ord}_V(r) = l_A\left(A/(r)\right), \text{ où } l_A(M) \text{ désigne la longueur du A-module } M.$$

Proposition 3.2.1. *Pour* $r \in K^*(X)$ *fixé, il existe seulement un nombre fini de sous-variétés V de codimension 1 de X telle que* $\text{ord}_V(r) \neq 0$.
Démonstration : Soit U un ouvert dense, lisse de X, et soit $U_1 = \text{Spec } A$ un ouvert affine de U, sur lequel r est régulière. On pose $Z = X - U_1$. Z est un fermé propre de X, or X est noethérien, donc Z ne contient qu'un nombre fini de sous-variétés V de codimension 1 de X ; toutes les autres rencontrent U_1. Il suffit donc de monter que : il n'y a qu'un nombre fini de sous-variétés V de U_1, telles que $v_V(r) \neq 0$, où v_V désigne la valuation associée à l'anneau de valuation discrète $O_{V|U}$. Comme r est régulière sur U, on a toujours $v_V(r) \geq 0$. De plus, $v_V(r) > 0$ si et seulement si V est inclus dans le sous-schéma fermé de U défini par l'idéal Ar de A. Comme $r \neq 0$, ce fermé est un sous-ensemble propre de U, et donc ne contient qu'un nombre fini de fermés irréductibles de codimension 1 de U.
□

3.2.2 Cycles et équivalence rationnelle

Définition 3.2.1 Soit X un schéma. On appelle groupe des k-cycles sur X, et on note Z_kX, le groupe abélien libre engendré par les sous-variétés V de dimension k de X. Un élément de Z_kX est appelé un *k-cycle*, et si V est une sous-variété k-dimensionnelle de X, on note $[V]$ l'élément correspondant de Z_kX.
On a parfois besoin de définir directement la notion de cycle associé au schéma X. Soit donc $X_1, \ldots, X_n$ les composantes irréductibles de X. Les anneaux locaux $O_{X_i,X}$ sont de dimension 0 et la *multiplicité géométrique* m_i de X_i dans X est alors par définition la longueur de $O_{X_i,X}$. Ceci nous permet de definir le *cycle fondamental* :

$$[X] = \sum_{i=1}^{n} m_i[X_i].$$

Définition 3.2.2 Si $\alpha = \sum_V n_V[V]$ est un cycle on définit le *support* de α, comme étant

$$\text{supp } \alpha = |\alpha| = \bigcup_{n_V \neq 0} V.$$

Si W est une sous-variété de dimension $k+1$ de X, et si r est un élément de $\mathcal{R}^*(W)$, on définit le k-cycle de X, $\operatorname{div}(r)$ associé par :

$$\operatorname{div}(r) = \sum_V \operatorname{ord}_V(r)[V], \text{ V décrit l'ensemble des sous-variétés de codimension 1 de W.}$$

Définition 3.2.3 Un k-cycle α est *rationnellement équivalent* à 0, $\alpha \sim 0$, s'il existe un nombre fini de sous-variétés W_i de dimension $k+1$ de X, et des $r_i \in \mathcal{R}^*(W_i)$ tels que $\alpha = \sum \operatorname{div}(r_i)$. Comme $\operatorname{div}(r^{-1}) = -\operatorname{div}(r)$, les cycles rationnellement équivalents à zéro forment un sous-groupe $\operatorname{Rat}_k X$ de $Z_k X$. Le groupe des classes de k-cycles modulo équivalence rationnelle sur X est le groupe noté :

$$A_k X = Z_k X / \operatorname{Rat}_k X.$$

On définit alors

$$Z_* X = \bigoplus_{k=0}^{\dim(X)} Z_k X \text{ et de même, } A_* X = \bigoplus_{k=0}^{\dim(X)} A_k X.$$

On écrit $\alpha = \sum_{k \geq 0} \alpha_k$ la décomposition d'un élément de $A_* X$. Un cycle est dit *positif* s'il est non nul et si tous ses coefficients sont positifs. Une classe de cycle est dite positive (ou effective) si elle peut être représentée par un cycle positif (ou effectif).

3.2.3 Image directe de cycles

Soit $f : X \to Y$ un morphisme propre (i.e séparé, de type fini et universellement fermé). Si V est une sous-variété de X, alors $f(V) = W$ est une sous-variété de Y (l'image continue d'un ensemble irréductible est irréductible). On a un plongement induit de $\mathcal{R}(W)$ dans $\mathcal{R}(V)$ et, si dim V = dim W alors $\mathcal{R}(W)$ est une extension algébrique, finie de $\mathcal{R}(V)$ (car sur un schéma intègre W, de type fini au dessus d'un corps K, on a $\dim W = \deg_{tr}(\mathcal{R}(W)/K)$). On pose :

$$\deg(V/W) = \begin{cases} 0 & \text{si dim V} < \text{dim W}, \\ [\mathcal{R}(V) : \mathcal{R}(W)] & \text{si dim V} = \text{dim W}. \end{cases}$$

On définit alors l'*image directe* de $[V]$ par f comme étant :

$$f_*[V] = \deg(V/W)[W],$$

et on étend ceci par linéarité en un morphisme $f_* : Z_k X \to Z_k Y$.

Proposition 3.2.2. ***(fonctorialité)*** *Si $g : Y \to Z$ est un autre morphisme propre, alors*

$$(gf)_* = g_* f_*.$$

Démonstration : Le résultat découle de la multiplicativité du degré. En effet :

$$\begin{aligned}(gf)_*[V] &= \deg(V,gf(V))[W] \text{ et}\\ g_*f_*[V] &= g_*(\deg(V,f(V))[f(V)]\\ &= \deg(V,f(V))\deg(f(V),gf(V))[W].\end{aligned}$$ □

Avant de passer à la proposition fondamentale de ce paragraphe, on indique ici deux résultats d'algèbre commutative concernant la fonction longueur. On travaille ici avec des anneaux noethériens.
Soit φ un endomorphisme du A-module de type fini M, posons

$$M_\varphi = \text{Coker } \varphi \text{ et } {}_\varphi M = \text{Ker } \varphi.$$

On dit que $e_A(\varphi,M)$ est défini si M_φ et ${}_\varphi M$ sont de longueur finie sur A. On pose alors $e_A(\varphi,M) = l_A(M_\varphi) - l_A({}_\varphi M)$.
Lemme 3.2.1. *Si $e_A(\varphi,M)$ est défini, alors : $e_A(\varphi,M) = \sum_p e_{A_p}(\varphi_p,M_p)$, où la somme porte sur les idéaux maximaux de A.*
Démonstration : D'une part cette égalité est vraie au niveau des longueurs (en localisant la chaîne définissant la longueur en un idéal maximal p, on constate en effet que A/p intervient exactement $l_{A_p}(M_p)$ fois), et d'autre part, en utilisant l'exactitude du foncteur $\varinjlim$, on constate que : $(M_\varphi)_p = (M_p)_{\varphi_p}$ et pareil pour le noyau. Le résultat est alors immédiat. □
Lemme 3.2.2. *Soit $A \to B$ un morphisme local d'anneaux locaux, soit d le degré (éventuellement infini) de l'extension de corps résiduels, et soit $\varphi : M \to M$ un endomorphisme B-linéaire de B-module. Si d est fini, alors, $e_A(\varphi,M)$ est défini si et seulement si $e_B(\varphi,M)$ est défini ; et dans ce cas :*

$$e_A(\varphi,M) = de_B(\varphi,M).$$

Démonstration : Comme pour le lemme précédent, le résultat découle d'un énoncé similaire aux niveaux des longueurs : sous les mêmes hypothèses, on a :
M est de longueur finie sur A si et seulement si M est de longueur finie sur B ; et dans ce cas, on a $l_A(M) = dl_B(M)$. Il suffit donc de montrer cette égalité pour conclure, or les deux cotés de l'égalité sont additifs sur les suites exactes, donc il suffit même de la montrer dans le cas où $M = B/q$, avec q l'idéal maximal de B. Si p est l'idéal maximal de A, comme le morphisme de A dans B est local, on a $pB/q = 0$, donc $l_A(M) = l_{A/p}(M) = d = dl_B(M)$, d'où le résultat. □

On peut maintenant passer au résultat qui nous intéresse directement.

Dans la proposition suivante, si X et Y sont deux variétés et si $r \in \mathcal{R}(X)$, on note $N_{X/Y}(r)$ la norme de r, c'est-à-dire le $\mathcal{R}(Y)$-endomorphisme défini sur $\mathcal{R}(X)$ par la multiplication par r.

Proposition 3.2.3. *Soit $f : X \to Y$ un morphisme surjectif, propre, de variétés, et soit $r \in \mathcal{R}(X)^*$, alors :*

$$\begin{cases} f_*([div\ r]) = 0 & si\ dim\ Y < dim\ X, \\ f_*([div\ r]) = [div\ (N_{X/Y}(r))] & si\ dim\ Y = dim\ X. \end{cases}$$

Démonstration : 1. On suppose tout d'abord que $X = \mathbb{P}^1$ et que $Y = \text{Spec } K$. Dans ce cas, $\mathcal{R}(X) = K(t)$, avec $t = \frac{x_1}{x_0}$. Comme la fonction ord est un morphisme, on peut supposer que r est un polynôme irréductible sur K[t] de degré d. Alors, r engendre un idéal premier dans K[t] qui correspond à un point P de X tel que $\text{ord}_P(r) = d$. L'autre point où l'ordre de r est non nul est le pôle $\infty = (0 : 1)$ à l'infini. En ce point r est d'ordre $-d$, donc $f_*([\text{div } r]) = df_*[P] - df_*[\infty] = d[Y] - d[Y] = 0$. (En effet, $\mathcal{R}(P) = K[t]/(r)$ est de degré d sur K alors que $\mathcal{R}(\infty)$ est de degré 1 sur K).
2. On suppose maintenant que f est un morphisme fini. Posons $K = \mathcal{R}(X)$ et $L = \mathcal{R}(Y)$. Soit W une sous-variété de Y de codimension 1, notons $A = O_{Y,W}$ et $\mathfrak{M}$ son idéal maximal, alors il existe un anneau B intègre, fini sur A, de corps de fraction L, avec $B \otimes_A K = L$, tel que, les sous-variétés V_i de X qui s'envoient sur W, correspondent aux idéaux maximaux $\mathfrak{M}_i$ de B, avec $B_{\mathfrak{M}_i} = O_{X,V_i}$. En effet, en prenant U un voisinage affine de w, point générique de W, on peut supposer X affine, $X = \text{Spec } A_X$. De plus, comme le morphisme f est fini, on peut se restreindre au départ, à l'ouvert affine $f^{-1}(\text{Spec } A_X)$. On suppose donc $Y = \text{Spec } A_Y$, et dans ce cas, on constate que $B = A \otimes_{A_Y} A_X$ convient (car f est fini). Ainsi pour prouver la proposition quand dim X = dim Y, on doit montrer que :

$$\sum_{f(V_i)=W} \text{ord}_{V_i}(r)[\mathcal{R}(V_i) : \mathcal{R}(W)] = \text{ord}_W N(r).$$

Les fonctions ord et N sont des morphismes donc il suffit de prouver cette égalité dans le cas où r appartient à B. On considère alors le morphisme local d'anneaux locaux de A dans $B_i = B_{\mathfrak{M}_i}$, dont l'extension résiduelle est de degré $d_i = [\mathcal{R}(V_i) : \mathcal{R}(W)]$, et on considère $\varphi : B \to B$ le morphisme de multiplication par r. On a :

$$\text{ord}_{V_i}(r) = l_{B_i}(B/(r)) = l_{B_i}(\text{Coker } \varphi_i)$$

où on a posé φ_i le morphisme induit par φ sur B_i. Pour tout i, on sait que d_i est fini, on peut donc appliquer le lemme 3.2.2, puis le lemme 3.2.1 (en utilisant l'intégrité de B) pour obtenir :

$$\sum_{f(V_i)=W} \text{ord}_{V_i}(r)[\mathcal{R}(V_i) : \mathcal{R}(W)] = l_A(\text{Coker } \varphi).$$

Par ailleurs, N(r) est par définition égale à det φ_K où φ_K est le morphisme induit par φ sur L=frac B. Finalement, on est ramené à montrer que :

$$l_A(\text{Coker } \varphi) = \text{ord}_W(\det \varphi_K).$$

Or ceci est vrai (cf [Ful98] lemme A.3), d'où le point 2.

3. On montre ici le cas général quand dim X = dim Y. On considère pour cela les normalisations ($\tilde{X}$,π_X) et ($\tilde{Y}$,π_Y) respectives de X et Y. Le morphisme surjectif f induit un morphisme $\tilde{f}$ de $\tilde{X}$ dans $\tilde{Y}$. Par fonctorialité on sait que : $\pi_{Y*} \circ \tilde{f}_* = f_* \circ \pi_{X*}$. Or un morphisme fini est propre, donc le résultat est vrai pour π_X et π_Y. De plus $\tilde{f}$ est propre d'après le lemme 3.1.2. Par définition, la normalisation ($\tilde{X}$,π_X) induit l'identité au niveau des applications rationnelles, donc, on peut supposer X normale, puis par fonctorialité on peut aussi supposer Y normale. Soit W une sous-variété de codimension 1 de Y, alors $A = O_{Y,W}$ est de valuation discrète (car local, noethérien, de dimension 1 et intégralement clos). On note y_0 le point générique de W et on note B la clôture intégrale de A dans $\mathcal{R}(X)$. Soit $\mathfrak{p}$ un idéal maximal de B. On considère alors le diagramme commutatif suivant,

$$\begin{array}{ccc} U = \text{Spec } \mathcal{R}(X) & \xrightarrow{u_1} & X \\ {\scriptstyle i}\downarrow & & \downarrow{\scriptstyle f} \\ T = \text{Spec } B_{\mathfrak{p}} & \xrightarrow{u_2} & Y \end{array}$$

où, u_1 envoie U sur le point générique, x_1 de X, et où u_2 envoie le point générique de T sur le point générique, y_0, de W dans Y. Par le critère valuatif de propreté, on en déduit l'existence d'une variété V, qui s'envoie sur W par f (le "sur" vient de ce que f est fermée), et dont l'anneau local O_V est dominé par $B_{\mathfrak{p}}$. De plus, l'anneau local O_V associé à l'idéal maximal $\mathfrak{p}$ est intégralement clos et de dimension 1. En effet, supposons par l'absurde que dim $O_V \geq 2$, c'est à dire qu'il existe un fermé irréductible F, strictement compris entre V et X. Dans ce cas, $f(F)$ est un fermé irréductible de Y, contenant W. Si $f(F) = Y$, alors dim $X >$ dim Y, ce qui contredirait notre hypothèse. Ainsi, $f(F)$ est strictement contenu dans Y et donc, comme dim $O_W = 1$, $f(F) = W$. Mais alors on aurait deux morphismes distincts de Spec $B_{\mathfrak{p}}$ dans X faisant commuter le diagramme précédent. Comme f est séparée, ceci est idiot, donc c'est que $F = V$, et en particulier que dim $O_V = 1$. Finalement, $B_{\mathfrak{p}} = O_V$ est de valuation discrète. Or, si $\mathfrak{p}_1$ et $\mathfrak{p}_2$ sont deux idéaux maximaux distincts de B, alors les variétés V_1 et V_2 associées sont nécessairement distinctes. En effet, si $V_1 = V_2$, alors les anneaux $O_{V_1} = B_{\mathfrak{p}_1}$ et $O_{V_2} = B_{\mathfrak{p}_2}$ coincident, donc les idéaux $\mathfrak{p}_1$ et $\mathfrak{p}_2$ sont égaux, ce qui est idiot. On est ainsi ramené à la situation du point 2., ce qui nous permet de conclure.
4. On montre ici le cas général quand dim $X >$ dim Y. Par récurrence descendante, on peut supposer dim X = dim $Y + 1$. Posons $K = \mathcal{R}(Y)$. Par définition du degré, deg(V,$f(V)$), le coefficient de Y dans $f_*[\text{div}(r)]$ est :

$$\sum \text{ord}_V(r)[\mathcal{R}(V) : K], \text{ où la somme porte sur les } V \text{ telles que } f(V) = Y.$$

On peut donc remplacer Y par Spec K et X par l'extension $X_K = X \times_Y \text{Spec } K$ (l'application déduite de f par ce changement de base reste propre par le lemme 3.1.2), et donc supposer que X est une courbe au dessus de Y = Spec K. Soit $\pi : \tilde{X} \to X$, la normalisation de X. C'est une courbe lisse sur K, donc le paragraphe précédent nous indique l'existence d'un morphisme $g : \tilde{X} \to \mathbb{P}^1_K$ fini, surjectif. En notant p la projection de $\mathbb{P}^1_K$

sur Y, on obtient ainsi le diagramme commutatif

$$\begin{array}{ccc} \tilde{X} & \xrightarrow{\pi} & X \\ {\scriptstyle g}\big\downarrow & & \big\downarrow{\scriptstyle f} \\ \mathbb{P}^1_K & \xrightarrow[p]{} & Y. \end{array}$$

On sait que π est propre, donc $f \circ \pi$ aussi, or p est projectif donc propre et donc, h est aussi un morphisme propre. En notant $\tilde{r}$ l'image de r dans $\mathcal{R}(\tilde{X})$ par l'isomorphisme $\mathcal{R}(X) \simeq \mathcal{R}(\tilde{X})$, on a :

$$\begin{array}{rcll} f_*[\text{div r}] & = & f_*\pi_*[\text{div } \tilde{r}] & \text{par le point 3. appliqué à } \pi, \\ & = & p_*g_*[\text{div } \tilde{r}] & \text{par fonctorialité,} \\ & = & 0 & \text{par le point 3. appliqué à } g \text{ et le point 1. appliqué à } p. \end{array}$$

Ceci conclut la démonstration. □

Théorème 3.2.1. *Si $f : X \to Y$ est propre et si α est un k-cycle sur X, rationnellement équivalent à 0, alors le cycle $f_*\alpha$ est rationnellement équivalent à 0 sur Y.*

Démonstration : Par linéarité, on peut supposer α =div r pour un $r \in \mathcal{R}(V)$, où V est une sous-variété de X. On peut alors supposer que $X = V$ puis que $f(X) = Y$. On est alors exactement dans les conditions d'application du lemme précédent qui nous permet de conclure. □

Corollaire 3.2.1. *Le morphisme $f : X \to Y$, induit un morphisme covariant de groupe $f_* : A_kX \to A_kY$.*

3.2.4 Degré d'un cycle

Définition 3.2.4 Soit X un schéma au dessus de Spec K. On dit que X est *complet* si le morphisme canonique $p : X \to \text{Spec } K$ est propre.

Définition 3.2.5 Soit X complet et $\alpha = \sum n_P[P]$ un 0-cycle sur X. En identifiant $\mathbb{Z}$ et $A_0(\text{Spec } K)$, on définit le *degré du cycle α* comme étant :

$$\deg \alpha = \sum n_P[\mathcal{R}(P) : K] = p_*(\alpha).$$

On remarque, en utilisant le théorème 3.2.1, que les cycles rationnellement équivalents ont même degré. En effet, si $\alpha \sim \beta$ alors $p_*(\alpha) \sim p_*(\beta)$, i.e $p_*(\alpha) = p_*(\beta) + \sum[\text{div } r_i]$ où $r_i \in \mathcal{R}(W_i)^*$ avec W_i sous-variété de dimension 1 de Spec K. Or il n'y a pas de telle variété car Spec K est de dimension 0, d'où la remarque.
On identifie $A_0(\text{Spec } K) = \mathbb{Z}[\text{Spec } K] \simeq \mathbb{Z}$, et on étend deg en un morphisme

$$\deg : A_*X \to \mathbb{Z} \text{ en posant, } \forall n \geq 1 \ \forall \alpha \in A_nX \quad \deg \alpha = 0.$$

Proposition 3.2.4. *Soit $f : X \to Y$ un morphisme de schémas complets et soit α appartenant à A_*X. On a : $deg_X\alpha = deg_Y f_*(\alpha)$.*

Démonstration: Les schémas X et Y sont des K-schémas donc $p_Y \circ f = p_X$. Le résultat suit par fonctorialité de $_*$. $\square$

3.2.5 Degré et polynôme de Hilbert

On va ici faire le lien entre la multiplicité tels qu'elle a été introduite précédemment, et, la multiplicité d'intersection, définie à partir du polynôme de Hilbert. On pose les jalons pour pouvoir faire la même chose, un peu plus loin, avec le degré. On commence par rappeler sans démonstration, certains résultats sur les schémas projectifs.

Schémas projectifs

Soit $S = K[X_0, \ldots, X_n]$, S est une K-algèbre graduée, telle que $S_0 = K$, et telle que S_1 est un K-module de type fini qui engendre S comme K-algèbre. On pose $U_i = \mathbb{P}^n_{X_i} \simeq \operatorname{Spec} K[X_0, \ldots, X_n, X_i^{-1}]$.
On rappelle qu'un schéma X est dit *projectif* si il est isomorphe à un sous-schéma fermé de $\mathbb{P}^n = \operatorname{Proj} S$.
Soit X un schéma fermé de $\mathbb{P}^n$, définit par le faisceau d'idéaux $\mathfrak{I}_X$. On considère l'idéal homogène I_X de S engendré par tous les polynômes homogènes $p(X_0, \ldots, X_n)$ tels que:

$$\forall i \in [\![1,n]\!],\ X_i = 1 \Rightarrow p(X_0, \ldots, 1, \ldots, X_n) \in \mathfrak{I}_X(U_i).$$

Dans ce cas on sait que $\widetilde{I_X} = \mathfrak{I}_X$, et on dit que le S-module de type fini $S(X) = S/I_X$ est l'anneau de coordonnées de X. En fait, on peut montrer que:

$$\forall l \gg 0,\ \ S(X)_l \simeq H^0(X, O_X(l)).$$

Polynôme de Hilbert

Définition 3.2.6 Un polynôme $P \in \mathbb{Q}[X]$ est dit *numérique* si:

$$\forall n \in \mathbb{Z},\ \ n \gg 0 \Rightarrow P(n) \in \mathbb{Z}.$$

Proposition 3.2.5. *1. Si $P \in \mathbb{Q}[X]$ est numérique, alors, il existe $c_0, \ldots, c_r \in \mathbb{Z}$ tels que: $P(z) = c_0 \binom{z}{r} + \cdots + c_r \binom{z}{0}$. En particulier, $P(n)$ est entier pour tout $n \in \mathbb{Z}$.*
2. Si $f : \mathbb{Z} \to \mathbb{Z}$ est une fonction, et s'il existe un polynôme numérique Q tel que $\Delta f(n) = f(n+1) - f(n) = Q(n)$ pour $n \gg 0$, alors il existe un polynôme P numérique tel que: $\forall n \gg 0$, on a: $f(n) = P(n)$.

Démonstration: Le point 1. se démontre par récurrence sur le degré de P, et le point 2. se prouve en utilisant le 1. $\square$

Théorème 3.2.2. *Soit M un module gradué, de type fini, sur un anneau S gradué et noethérien. Alors, il existe une filtration $0 = M_0 \subset \ldots \subset M^q = M$ dont les quotients successifs M^i/M^{i-1} sont de la forme $(S/\mathfrak{p}_i)(l_i)$, où les $\mathfrak{p}_i$ sont des idéaux premiers homogènes de S, et les $l_i \in \mathbb{Z}$. De plus, cette filtration vérifie:*

1. Si $\mathfrak{p}$ est un idéal homogène premier de S, alors Ann $M \subset \mathfrak{p} \iff \mathfrak{p}_i \subset \mathfrak{p}$ pour un certain i.
2. Pour tout idéal premier minimal de M, le nombre de fois où $\mathfrak{p}$ apparait dans l'ensemble $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_q\}$ est égal à $l_{S_\mathfrak{p}}(M_\mathfrak{p})$.
Démonstration: Si on admet l'existence de la filtration (dont l'existence est prouvée dans [Har77] p 50), le théorème est facile. Supposons donnée une filtration de M, alors Ann $M \subset \mathfrak{p} \iff$ Ann $(M^i/M^{i-1}) \subset \mathfrak{p}$ pour un certain i. Or Ann $((S/\mathfrak{p}_i)(l)) = \mathfrak{p}_i$, ce qui prouve le point 1. Par ailleurs le point 2. est classique, on localise la filtration de M en un idéal premier minimal $\mathfrak{p}$. Comme $\mathfrak{p}$ est minimal dans l'ensemble $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_q\}$, on aura $(M^i)_\mathfrak{p} = (M^{i-1})_\mathfrak{p}$ après localisation, sauf dans le cas où $\mathfrak{p} = \mathfrak{p}_i$. Or dans ce dernier cas, en oubliant la graduation, $(M^i)_\mathfrak{p}/(M^{i-1})_\mathfrak{p} \simeq (S/\mathfrak{p})_\mathfrak{p} = K(\mathfrak{p})$ où $K(\mathfrak{p})$ est le corps résiduel. Ainsi $M_\mathfrak{p}$ est un $S_\mathfrak{p}$-modules de longueur finie égale au nombre de fois où apparait $\mathfrak{p}$ dans l'ensemble $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_q\}$. □

Définition 3.2.7 Si $\mathfrak{p}$ est un idéal minimal d'un S-module gradué, M, on définit la *multiplicité* de M en $\mathfrak{p}$ comme étant: $\mu_\mathfrak{p}(M) = l_{S_\mathfrak{p}}(M_\mathfrak{p})$.

Remarquons que si X est un sous-schéma fermé de $\mathbb{P}^n$ et si $\mathfrak{p}$ est un idéal minimal de l'anneau de coordonnées homogène S(X) de X, correspondant à la composante irréductible W de X, alors la multiplicité $\mu_\mathfrak{p}(S(X))$ que l'on vient de définir est juste la multiplicité géométrique de W dans X.

Définition 3.2.8 La définition précédente nous permet de définir la *fonction de Hilbert* φ_M de M, S-module gradué avec $S = K[X_0, \ldots, X_n]$:

$$\text{on pose, pour tout } l \in \mathbb{Z} \ \ \varphi_M(l) = dim_K M_l.$$

Théorème 3.2.3. ***(Hilbert-Serre)*** *Soit M un S-module gradué, où $S = K[X_0, \ldots, X_n]$, alors, il existe un unique polynôme $P_M(z) \in \mathbb{Q}[z]$ tel que:*

$$\forall l \gg 0, \ \ \varphi_M(l) = P_M(l).$$

De plus, deg $P_M(z) =$ dim $Z(AnnM)$. En particulier, si X est une sous-variété de $\mathbb{P}^n$, d'anneau de coordonnées $M = S(X)$, alors: deg $P_{S(X)}(z) =$ dim X.
Démonstration: La fonction $\varphi_.$ est additive sur les suites exactes, et si M est l'extension de M' par M'', alors, $Z(AnnM) = Z(AnnM') \cup Z(AnnM'')$. Ainsi, en considérant la filtration de M, avec des quotients du type $(S/\mathfrak{p})(l)$, il suffit de prouver le théorème dans le cas où $M = (S/\mathfrak{p})(l)$. Or le décallage par l correspond au changement de variable $z \mapsto z + l$ dans la fonction φ_M. Il suffit donc de traiter le cas où $l = 0$.
Si $\mathfrak{p} = (X_0, \ldots, X_n)$, alors, dès que $l > 0$, on a $\varphi_M(l) = 0$. En prenant comme convention que, le degré du polynôme nul et la dimension de l'ensemble vide sont égaux à 0, on en déduit le résultat.
Sinon, soit i tel que $X_i \notin \mathfrak{p}$. Considérons la suite exacte:

$$0 \to M \xrightarrow{X_i} M \to M'' = M/X_iM \to 0.$$

Alors, $\varphi_{M''}(l) = \varphi_M(l) - \varphi_M(l-1) = (\Delta\varphi_M)(l-1)$. Par ailleurs, $Z(AnnM) = Z(\mathfrak{p}) \cap H$, où H est l'hyperplan $\{X_i = 0\}$. Or on est justement dans le cas, où $Z(\mathfrak{p}) \not\subset H$, donc par le théorème de la dimension projective, on en déduit que :

$$\dim\, Z(AnnM'') = \dim\, Z(\mathfrak{p}) - 1.$$

Par récurrence sur dim $Z(AnnM)$, on peut alors supposer que le résultat est vrai pour M''. Dans ce cas, le point 2. de la proposition 3.2.5 nous permet de conclure. □

Définition 3.2.9 Le polynôme P_M obtenu au théorème précédent est appelé *polynôme de Hilbert* de M. Si X est un sous-schéma fermé de $\mathbb{P}^n$, d'anneau de coordonnées $S(X)$, on appelle *polynôme de Hilbert de* X le polynôme $P_X = P_{S(X)}$.

Définition 3.2.10 Pour X, sous-schéma fermé de $\mathbb{P}^n$ de dimension k, on définit le *degré* de X comme étant : $\deg_g\, X = k!\, a_k$, où a_k est le coefficient dominant de P_X.

Définition 3.2.11 On dit que H est une *hypersurface de* $\mathbb{P}^n$, si $H = V(F)$, où F est un polynôme homogène non nul de $K[X_0, \ldots, X_n]$.

Proposition 3.2.6. *1. Si Y est un sous-schéma fermé de $\mathbb{P}^n$, non vide, alors $\deg_g\, Y$ est un entier positif.*
2. $\deg_g\, \mathbb{P}^n = 1$.
3. Si H est une hypersurface de $\mathbb{P}^n$ engendrée par un polynôme P de degré d, alors $\deg_g\, H = d$.

Démonstration : 1. Par le théorème précédent, on sait que dim Y = deg P_Y, or, $Y \neq \emptyset$, donc deg $P_Y \geq 0$. De plus, P_Y est numérique, donc $\deg_g\, Y$ est bien un entier par la proposition 3.2.5. Enfin, pour tout entier l assez grand, $P_Y(l) = \varphi_Y(l) \geq 0$, d'où le résultat.
2. On calcule le polynôme de Hilbert de $\mathbb{P}^n$, i.e le polynôme de $S = K[X_0, \ldots, X_n]$. Or $\forall l > 0$, $\varphi_S(l) = \binom{l+n}{n}$, donc $P_S(l) = \binom{l+n}{n}$, et deg $\mathbb{P}^n = 1$.
3. Si $f \in S(Y)$ est homogène de degré d, alors on a la suite exacte de module gradués :

$$0 \to S(Y)(-d) \xrightarrow{f} S(Y) \to S(Y)/(f) \to 0.$$

On en déduit, par additivité de la fonction φ, que :

$$\varphi_{S(Y)/(f)}(l) = \varphi_{S(Y)}(l) - \varphi_{S(Y)}(l-d).$$

En appliquant ceci à $f = P$, on en déduit que : $P_H(z) = \binom{z+n}{n} - \binom{z-d+n}{n}$. En particulier on trouve $\deg_g\, H = d$, ce qui conclut. □

Définition 3.2.12 Soit Y un sous-schéma fermé de $\mathbb{P}^n$, de dimension k et d'idéal I_Y, et soit H une hypersurface, d'idéal I_H, ne contenant pas Y. On peut écrire :

$$[Y \cap H] = \sum_{i=1}^{s} m_i [Z_i] \quad \text{où } m_i \text{ est la multiplicité géométrique de } Y \cap H.$$

On a déja vu que $m_i = \mu_{p_i}(S/(I_H + I_Y))$. On note encore cette multiplicité, $i(Y,H;Z_i)$ et on l'appelle *multiplicité d'intersection de* Y *et* H *selon* Z_i.

Théorème 3.2.4. ***(Bézout)*** *Avec les notations précédentes, on a :*

$$deg_g\ H \cap Y = \sum_{i=1}^{s} i(Y,H;Z_i) deg_g\ Z_j = (deg_g\ Y)(deg_g\ H).$$

Démonstration : Si H est définie par le polynôme homogène f, de degré d, alors, on a la suite exacte :

$$0 \to S(Y)(-d) \xrightarrow{f} S(Y) \to S(Y)/(f) \to 0.$$

Or $S(Y)/(f) = S/(I_H + I_Y) = M$, donc en passant aux polynômes de Hilbert on en déduit : $P_M(z) = P_Y(z) - P_Y(z-d)$ **(1)**. Il nous reste pour conclure à comparer le coefficient dominant des deux membres de l'égalité **(1)**.
Notons dim $Y = k$ et $\deg_g Y = e$, alors le membre de droite est donc :

$$\frac{e}{k!}z^k - \frac{e}{k!}(z-d)^k + \ldots = \frac{de}{(k-1)!}z^{k-1} + \ldots,$$

où les termes dans ... sont de degrés strictement plus petits. Donc le coefficient dominant est $de = (\deg_g Y)(\deg_g H)$.
Considérons maintenant le membre de gauche. Par le théorème 3.2.2, on sait que M admet une filtration : $0 = M_0 \subset \ldots \subset M^q = M$ dont les quotients successifs M^i/M^{i-1} sont de la forme $(S/\mathfrak{p}_i)(l_i)$. Donc le polynôme P_M est la somme des polynômes P_i associés aux $(S/\mathfrak{p}_i)(l_i)$. Si $Z(\mathfrak{p}_i)$ est un sous-schéma fermé de $\mathbb{P}^n$, de dimension k_i et de degré d_i, alors P_i est de coefficient dominant $\frac{d_i}{k_i}$. Comme on s'intéresse à comparer les coefficients dominants dans l'égalité **(1)**, il suffit de s'intéresser aux P_i de degré $k-1$, c'est à dire aux $\mathfrak{p}_i$ qui sont des idéaux premiers de M minimaux, c'est à dire ceux correspondants aux composantes irréductibles Z_i. Or chacune intervient exactement m_i fois, donc le coefficient dominant de P_M est exactement

$$\frac{1}{(r-1)!}\sum_{i=1}^{s} i(Y,H;Z_i)\deg_g Z_i.$$

En comparant les deux nombres ainsi obtenus, on peut conclure. □

3.2.6 Image réciproque plate de cycles

Définition 3.2.13 Un morphisme de schémas f de X dans Y est dit *plat*, si le Y-schéma X défini par f est plat sur Y, i.e si O_X est plat sur Y, i.e si pour tout $x \in X$, $O_{X,x}$ est un $O_{Y,f(x)}$-module plat.

Exemple 3.2.1 Si U est un ouvert de X, l'inclusion (et plus généralement toute immersion ouverte) de U dans X est plate.

Définition 3.2.14 Un morphisme $f : X \to Y$ est de *dimension relative* n si pour toute sous-variété V de Y et pour toute composante irréductible V' de $f^{-1}(V)$ on a :

$$\text{dim V'} = \text{dim V} + n.$$

Exemple 3.2.2 L'inclusion ouverte $U \to X$ est de dimension relative 0.

Soit donc $f : X \to Y$ un morphisme de schémas, plat, de dimension relative n, et Z un sous-schéma de Y, on pose :

$$f^*[Z] = [f^{-1}(Z)].$$

Quand V est une variété, $f^{-1}(V) = X \times_Y V$ est un sous-schéma de X, de pure dimension dim V $+ n$ et $[f^{-1}(V)]$ est le cycle associé. En prolongeant par linéarité on construit ainsi un morphisme :

$$f^* : Z_k Y \to Z_{k+n} X.$$

Corollaire 3.2.2. ***(fonctorialité)*** *Si $f : X \to Y$ et $g : Y \to Z$ sont plats, alors gf est plat et*

$$(gf)^* = f^* g^*.$$

Démonstration : Si V est une sous-variété de Z, alors :

$$(gf)^*[V] = [(gf)^{-1}(V)] = [f^{-1}(g^{-1}(V)] = f^* g^*[V]$$

ce qui nous donne le résultat par linéarité. □

On indique, sans démonstration (cf [Ful98] p 19), un résultat rassurant concernant le passage à l'image réciproque plate. Nous n'en aurons pas besoin.

Théorème 3.2.5. *Soit $f : X \to Y$ un morphisme plat de dimension relative n, et soit α un k-cycle de Y rationnellement équivalent à 0. Alors $f^*\alpha$ est rationnellement équivalent à 0 dans $Z_{k+n}X$.*

3.2.7 Intersection avec des diviseurs

Définition 3.2.15 Soit X un schéma, V une sous-variété de dimension k de X et D un diviseur de Cartier de X. On définit une classe notée

$$D \cdot [V] \text{ ou } D \cdot V \text{ dans } A_{k-1}(|D| \cap V) \text{ comme suit :}$$

soit $j : V \hookrightarrow X$ l'inclusion naturelle, deux cas se présentent :
1. Si $V \not\subset |D|$ alors D se restreint en un diviseur de Cartier j^*D sur V et dans ce cas

$$D \cdot [V] = [j^*D].$$

2. Sinon, $V \subset |D|$ et dans ce cas,

$$D \cdot [V] = [C] \quad \text{où}$$

$[C]$ est le diviseur de Weil dans $A_{k-1}(V)$ associé à C, C étant par définition un diviseur de Cartier sur V tel que $j^*O_X(D) \simeq O_X(C)$.

Convention : 1. Soit $Y_1,\ldots,Y_r$ des sous-schémas fermés d'un schéma X. Soit Y un sous-schéma fermé de X contenant tous les Y_i et soit $\varphi_i : Y_i \hookrightarrow Y$. Pour tout $i \leq r$, soit $\alpha_i \in A_*Y_i$ et $\beta \in A_*Y$. On écrira :

$$\beta = \sum_{i=1}^{r} \alpha_i \text{ dans } A_*Y \text{ pour } \beta = \sum_{i=1}^{r} \varphi_{i\,*}(\alpha_i).$$

2. Si V est une sous-variété de dimension k de X, D un diviseur de Cartier sur X et Y un sous-schéma fermé de X contenant $|D| \cap V$, on notera encore $D \cdot [V]$ pour l'image dans $A_{k-1}(Y)$ de $D \cdot [V]$.

Définition 3.2.16 La convention précédente nous permet de définir la classe d'intersection $D \cdot \alpha \in A_{k-1}(|D| \cap \alpha)$. On pose :

$$D \cdot \alpha = \sum_{n_V \neq 0} n_V D \cdot [V].$$

Théorème 3.2.6. *Soit D un diviseur de Cartier sur X un schéma, et soit α et α' deux k-cycles sur X. Alors :*
1. $D \cdot (\alpha + \alpha') = D \cdot \alpha + D \cdot \alpha'$ dans $A_{k-1}(|D| \cap (|\alpha| \cup |\alpha'|))$.
2. Si D' est un autre diviseur de Cartier sur X, $(D + D') \cdot \alpha = D \cdot \alpha + D' \cdot \alpha$.
3. ***(formule de la projection)*** *Soit $f : X_1 \to X$ un morphisme propre, α_1 un k-cycle sur X_1 et g le morphisme de $f^{-1}(|D|) \cap |\alpha_1| \to |D| \cap f(|\alpha_1|)$ induit par f. Alors :*

$$g_*(f^*D \cdot \alpha_1) = D \cdot (f_*(\alpha_1)) \text{ dans } A_{k-1}(|D| \cap f(|\alpha_1|)).$$

4. Si D est principal, alors $D \cdot \alpha = 0$ dans $A_{k-1}(|\alpha|)$.
Démonstration : Point 1. C'est juste dire que $n_V(\alpha + \alpha') = n_V(\alpha) + n_V(\alpha')$.
Point 2. On peut supposer $\alpha = [V]$ avec V sous-variété de X. Le résultat vient alors de ce que les opérations { se restreindre à V } et { prendre les diviseurs de Weil associés } commutent à l'addition.
Point 3. On peut supposer $\alpha_1 = [V]$ et par fonctorialité de * et de $_*$, on peut aussi supposer que $X_1 = V$ et que $f(V) = X$. Dans ce cas :

$$g_*(f^*D \cdot \alpha) = f_*([f^*D]) \text{ et } D \cdot f_*(\alpha) = \deg(X_1/X)[D].$$

Considérons, une trivialisation par des cartes affines, $U_i = \text{Spec } A_i$, du diviseur de Cartier D : $D = (U_i,r_i)_i$. Alors on consate qu'il suffit de vérifier l'égalité sur chaque U_i. On peut donc supposer $X = U_i$ affine, et $D = \text{div } r$ pour $r \in \mathcal{R}(X)$. Dans ce cas la proposition 3.2.3 nous dit que :
Si dim X = dim X_1, c'est fini.
Sinon $f_*[\text{div}(f^*r)] = [\text{div}(N(f^*r))] = \text{div}(r^d) = d[\text{div } r]$, avec $d = \deg(X_1/X)$.
Point 4. Là encore, on peut supposer que $\alpha = [V]$ et que $X = V$. On a alors $D \cdot \alpha = [D]$. Or D est un diviseur principal, et on sait que dans ce cas $[D] = 0$. □

3.2.8 Commutativité des classes d'intersection

Théorème 3.2.7. *Soit D et D' deux diviseurs de Cartier sur une variété X de dimension n. Alors :*

$$D \cdot [D'] = D' \cdot [D] \text{ dans } A_{n-2}(|D| \cap |D'|).$$

La démonstration se fait en quatre étapes, selon que les deux diviseurs de Cartier, D et D', que l'on considère sont effectifs et s'intersectent proprement ou non.

Définition 3.2.17 On dit que deux diviseurs de Cartier, D et D' sur une variété X, *s'intersectent proprement* si $|D| \cap |D'|$ ne contient aucune sous-variété V de codimension 1 de X.

On considère donc D et D', deux diviseurs de Cartier sur une variété X. Si ils sont tous deux effectifs, on introduit la notion *d'excès d'intersection* $\varepsilon(D,D')$, définie par la formule :

$$\varepsilon(D,D') = \max \{\mathrm{ord}_V(D) \cdot \mathrm{ord}_V(D') \ /\mathrm{codim}(V,X) = 1\},$$

Ainsi, $\varepsilon(D,D') = 0$ si et seulement si D et D' s'intersectent proprement.
Le sous-schéma fermé $D \cap D'$ de X est localement défini par les équations (a,a'), où a est l'équation locale de D et a' celle de D'. Notons $\pi : BL(X) \to X$ l'éclatement de X selon $D \cap D'$, et $E = \pi^{-1}(D \cap D')$ le diviseur exceptionnel. On a :

$$\pi^* D = E + C,\ \pi^* D' = E + C' \ \text{ où } C \text{ et } C' \text{ sont des diviseurs effectifs sur } BL(X)\ .$$

On énonce deux lemmes avant de passer à la démonstration proprement dite :
Lemme 3.2.3. *Avec les notations précédentes, on a : 1.* $C \cap C' = \emptyset$.
2. Si $\varepsilon(D,D') > 0$, *alors,* $\varepsilon(C,E)$ *et* $\varepsilon(C',E)$ *sont strictement inférieurs à* $\varepsilon(D,D')$.
Démonstration : Le problème est local (on travaille avec les ouverts définissant localement D et D'), et on suppose donc, $X = \mathrm{Spec}\ A$, $D = \mathrm{div}(a)$ et $D' = \mathrm{div}(a')$. Ainsi, $Bl(X) =$ **Proj** $(\bigoplus I^n)$ où $I = (a,a')$. Le morphisme gradué

$$A[X,Y] \to \bigoplus_{n \geq 0} I^n$$

qui envoie X sur a et Y sur a', définit une immersion fermée de $BL(X)$ dans $\mathbb{P}^1_A$. Plus précisément, $BL(X)$ est contenu dans le sous-schéma fermé de $\mathbb{P}^1_A$ sur lequel $a'X - aY$ s'annule. Soit x et y les deux sections de $O(1)$ (où O(1) désigne l'image réciproque du fibré $O_{\mathbb{P}^1_A}(1)$) induites par X et Y respectivement. Montrons que C est le schéma des zéros $Z(x)$ de x, et de même, que $C' = Z(y)$.
L'équation $a' = (yx^{-1})a$ indique (D est effectif, donc a est régulière) que E et $\pi^* D$ coincïdent sur l'ouvert $\{x \neq 0\}$, et l'équation $a = (xy^{-1})a'$ indique que $\pi^* D$ et $E + Z(x)$ coincïdent sur l'ouvert $\{y \neq 0\}$. Donc on a $C = \pi^* D - E = Z(x)$. Le même raisonnement vaut pour C'. De plus, comme $Z(x) \cap Z(y) = \emptyset$, on en déduit le point 1.

On constate aussi sur cette description que $C \subset X \times \{0\}$ et $C' \subset X \times \{\infty\}$ (où $\mathbb{P}^1_A = \mathbb{P}^1 \times X$) s'envoient isomorphiquement, par π, sur des sous-schémas de D et D' respectivement. Par conséquent, si $\tilde{V}$ est une sous-variété de codimension 1 de $BL(X)$, contenue dans $C \cap E$ où $C' \cap E$, alors, $V = \pi(\tilde{V})$ est une sous-variété (car π est propre donc fermée) de codimension 1 de X, contenue dans $D \cap D'$. Or on sait par la formule de la projection que $[D] = \pi_*[E + C]$, donc :

$$\mathrm{ord}_V D \geq \mathrm{ord}_{\tilde{V}} E + \mathrm{ord}_{\tilde{V}} C,$$

et la même chose pour D'. Supposons par l'absurde que $\varepsilon(C,E) \geq \varepsilon(D,D') > 0$, et soit $\tilde{V} \subset C \cap E$ choisie pour réaliser le max $\varepsilon(C,E)$. Dans ce cas :

$$\begin{array}{rcl} \varepsilon(D,D') & \geq & \mathrm{ord}_V D \cdot \mathrm{ord}_V D', \\ & \geq & \left(\mathrm{ord}_{\tilde{V}} E + \mathrm{ord}_{\tilde{V}} C\right)\left(\mathrm{ord}_{\tilde{V}} E + \mathrm{ord}_{\tilde{V}} C'\right), \\ & \geq & \left(\mathrm{ord}_{\tilde{V}} E\right)^2 + \varepsilon(C,E). \end{array}$$

Or, $\mathrm{ord}_{\tilde{V}} E > 0$, donc ceci est absurde. □

Lemme 3.2.4. *Soit D et D' deux diviseurs de Cartier sur la variété X, et $\pi : Y \to X$ est un morphisme birationnel propre de variétés. Supposons que $\pi^* D = B \pm C$, et que $\pi^* D' = B' \pm C'$ pour des diviseurs de Cartier B, C, B', C' sur la variété Y, vérifiant $|B| \cup |C| \subset \pi^{-1}(|D|)$, $|B'| \cup |C'| \subset \pi^{-1}(|D'|)$. Si le théorème 3.2.7 est vrai pour chacune des paires (B,B'), (B,C'), (C,B') et (C,C') sur Y, alors il est vrai pour la paire (D,D') sur X.*

Démonstration : Notons g le morphisme induit par π entre $\pi^{-1}(|D| \cap |D'|)$ et $|D| \cap |D'|$. On rappelle (cf la preuve de la formule de la projection) que $D \cdot \pi_*[\pi^* D'] = D \cdot [D']$, donc en appliquant la formule de la projection avec $\alpha_1 = \pi^* D'$, on obtient :

$$\begin{array}{rcl} D \cdot [D'] & = & g_*((B \pm C) \cdot [B' \pm C']), \\ & = & g_*(B \cdot [B'] \pm B \cdot [C'] \pm C \cdot [B'] + C \cdot [C']), \\ & = & g_*(B \cdot [B'] \pm C' \cdot [B] \pm B' \cdot [C] + C' \cdot [C]), \\ & = & g_*((B' \pm C') \cdot [B \pm C]), \\ & = & D' \cdot [D]. \end{array}$$

Notons qu'on a utilisé la birationnalité dans la première égalité. □

On peut maintenant démontrer le théorème 3.2.7 :
étape 1. : D et D' sont effectifs et s'intersectent proprement. C'est un argument d'algèbre commutative.
étape 2. : D et D' sont effectifs. On fait une preuve par récurrence sur $\varepsilon(D,D')$. Le cas, $\varepsilon = 0$ correspond à l'étape 1., par une remarque faite précédemment. Si $\varepsilon(D,D') > 0$, on éclate X selon le fermé $D \cap D'$. Par le point 2. du lemme 3.2.3 et par hypothèse de récurrence, le théorème est vrai pour les paires (C,E) et (C',E). De plus, le théorème est évidemment vrai pour la paire (E,E), et comme $C \cap C' = \emptyset$ l'étape 1. nous indique que

le théorème est aussi vrai pour la paire (C,C'). Finalement, on peut appliquer le lemme 3.2.4 qui nous permet de conclure.
étape 3. : D' (ou D) est effectif. Considérons $\mathcal{J}$ le *faisceau des dénominateurs de* D, c'est à dire : si $U = \text{Spec } A$ est un ouvert affine sur lequel D a pour équation affine d, $\mathcal{J}$ est déterminé par l'idéal $\{a \in A \ /ad \in A\}$. Soit $\pi : BL(X) \to X$, l'éclatement de X selon le sous-schéma défini par $\mathcal{J}$, de diviseur exceptionnel E. Alors :

$$\pi^* D = C - E \text{ pour un diviseur effectif } C \text{ sur } BL(X).$$

Là encore, une application du lemme 3.2.4 permet de conclure, car le théorème est vrai pour les paires $(C,\pi^* D')$, et $(E,\pi^* D')$ par l'étape 2.
étape 4. : D et D' sont quelconques. On considère le même éclatement qu'à l'étape précédente. Le théorème est vrai pour les paires $(C,\pi^* D')$, et $(E,\pi^* D')$ par l'étape 3., et donc le lemme 3.2.4 nous permet de conclure. □

Corollaire 3.2.3. *Soit D un diviseur de Cartier sur un schéma X, et soit α un k-cycle rationnellement équivalent à 0. Alors $D \cdot \alpha = 0$ dans $A_{k-1}(|D|)$.*

Démonstration : Il suffit de voir le résultat pour $\alpha = [\text{div r}]$, $r \in \mathcal{R}(W)^*$, et W une sous-variété de dimension $k+1$. Par fonctorialité de *, on peut remplacer X par W. Or :

$$\begin{aligned} D \cdot [\text{div r}] &= \text{div r} \cdot [D] \text{ dans } A_{k+1-2}(|D| \cap |\text{div r}|), \\ &= 0 \text{ par le point 4. du théorème 3.2.6, dans } A_{k-1}(|D|). \end{aligned}$$ □

Définition 3.2.18 Si D est un diviseur de Cartier sur un schéma X et si Y est un sous-schéma fermé de X, alors on a un morphisme de $Z_k Y$ dans $A_{k-1}(|D| \cap Y)$ qui envoie α sur $D \cdot \alpha$. De plus, le corollaire précédent nous indique que ce morphisme passe au quotient, d'où un morphisme : $A_k Y \to A_{k-1}(|D| \cap Y)$ appelé *intersecté avec Y.*

Corollaire 3.2.4. *Soit D et D' deux diviseurs de Cartier sur un schéma X. Alors, si α est un k-cycle sur X, $D \cdot (D' \cdot \alpha) = D' \cdot (D \cdot \alpha)$ dans $A_{k-2}(|D| \cap |D'| \cap |\alpha|)$.*

Démonstration : On sait que $D' \cdot \alpha \in A_{k-1}(|D'| \cap \alpha|)$ et qu'intersecter avec D envoie $A_{k-1}(|D'| \cap |\alpha|)$ dans $A_{k-2}(|D| \cap |D'| \cap |\alpha|)$, et de même avec $D' \cdot (D \cdot \alpha)$. On prend $\alpha = [V]$ et on peut aussi restreindre D et D' à V. Dans ce cas :

$$\begin{aligned} D \cdot (D' \cdot \alpha) &= D \cdot [D'] \\ &= D' \cdot [D] \\ &= D' \cdot (D \cdot \alpha) \text{ dans } A_{k-2}(|D| \cap |D'| \cap |\alpha|). \end{aligned}$$ □

Définition 3.2.19 Soit $D_1, \ldots, D_n$ des diviseurs de Cartier sur un schéma X, alors : pour tout k-cycle α sur X, on définit par récurrence

$$D_1 \cdot \ldots \cdot D_n \cdot \alpha \text{ dans } A_{k-n}(|D_1| \cap \ldots \cap |D_n| \cap |\alpha|).$$

Le corollaire précédent nous indique que cette définition est indépendante de l'ordre des D_i, et le théorème 3.2.6 nous dit que ceci est linéaire en les D_i et en α.

Plus généralement, pour tout polynôme homogène $P(T_1,\ldots,Tn)$ de degré d à coefficients entiers et pour tout sous-schéma fermé Z contenant $(|D_1|\cup\ldots\cup|D_n|)\cap|\alpha|$ on définit naturellement la classe :

$$P(D_1,\ldots,D_n)\cdot\alpha\in A_{k-d}(Z).$$

Enfin si X est de pure dimension, on notera $P(D_1,\ldots,D_n)$ pour $P(D_1,\ldots,D_n)\cdot[X]$.

3.2.9 Classe de Chern d'un fibré en droites

Soit L un fibré en droites sur un schéma X. Pour toute sous-variété V de X, la restriction $L_{|V}$ de L à V est isomorphe à $O_V(C)$ où C est un diviseur de Cartier sur V. Le diviseur de Weil associé [C] définit un élément de $A_{k-1}(X)$ que l'on note :

$$[C]=c_1(L)\cap[V].$$

On étend ceci par linéarité en un morphisme de $Z_k(X)$ dans $A_{k-1}(X)$. Si $L=O_X(D)$ pour un diviseur de Cartier D sur X, la définition de la classe d'intersection implique que :

$$c_1(O_X(D))\cap\alpha=D\cdot\alpha \text{ dans } A_{k-1}(X).$$

De ce qui précède on déduit le théorème suivant :

Théorème 3.2.8. *1. Si α est rationnellement équivalent à 0 sur X, alors $c_1(L)\cap\alpha=0$.*
2. Le morphisme précédent induit donc un morphisme de A_kX dans $A_{k-1}X$.
3. La commutativité, l'additivité et la formule de projection sont vérifiées.

Exemple 3.2.3 **(fondamental)** Par définition d'un fibré en droite, si L est un tel fibré sur une variété X, et si s est une section non nulle de $H^0(X,L)$, de schéma des zéros $Z(s)$, alors $c_1(L)\cap[X]=[Z(s)]$.

Dans le cas où α est un k-cycle sur $\mathbb{P}^n$, on définit le *degré (projectif) de* α, comme étant :

$$\deg_{\mathbb{P}^n}\alpha=\deg\, c_1(O(1))^k\cap\alpha.$$

On peut maintenant faire le lien entre le degré défini à partir du polynôme de Hilbert, et le degré projectif que l'on vient d'introduire.

Théorème 3.2.9. *Soit X une sous-schéma fermé de $\mathbb{P}^n$ de pure dimension k, alors : $deg_g X = deg_{\mathbb{P}^n}\,[X]$.*

Démonstration : Par le même raisonnement que celui fait dans la preuve du théorème 3.2.4, on montre que : si $[X]=\sum_{i=1}^m m_i[X_i]$ où les X_i sont les composantes irréductibles de X, de multiplicités m_i, alors, $\deg_g X=\sum_{i=1}^m m_i\deg_g X_i$. Par ailleurs la même formule est valable pour le degré, $\deg_{\mathbb{P}^n}$. Donc il suffit de vérifier le théorème dans le cas où X est une sous-variété de $\mathbb{P}^n$ de dimension k. On le fait par récurrence sur la dimension :
Si $\dim X=0$, c'est clair.

Si le résultat est vrai pour les sous-variétés de dimension $\leq k$, soit X de dimension k. On considère alors H, un hyperplan de $\mathbb{P}^n$ ne contenant pas X, tel que $[X \cap H]$ représente la classe $c_1(O(1)) \cap [X]$. On a :

$$\begin{aligned} \deg_g X &= \deg_g X \cap H = \deg_{\mathbb{P}^n}[X \cap H] \text{ d'après le théorème 3.2.4, puis par récurrence,} \\ &= \deg\, c_1(O(1))^{k-1} \cap [X \cap H] = \deg\, c_1(O(1))^{k-1} \cap c_1(O(1)) \cap [X] = \deg_{\mathbb{P}^n}\, [X]. \end{aligned}$$

La récurrence nous permet donc de conclure. □

Corollaire 3.2.5. *Si X est un sous-schéma fermé de dimension m de $\mathbb{P}^r$, alors :*

$$\lim_{l \to \infty} \frac{h^0(X,O_X(l))}{l^m} = \frac{deg\ c_1(O(1))^m}{m!}.$$

Démonstration : On utilise le théorème 3.2.9 pour dire que :

$$P_X(l) \underset{+\infty}{\simeq} \frac{\deg\ c_1(O(1))^m l^m}{m!}.$$

On applique alors le théorème 3.2.3 pour conclure, avec $M = S(X)$. On sait en effet que pour l assez grand, on a d'une part, $\varphi_{S(X)}(l) = \dim_K H^0(X,O_X(l))$, et d'autre part, $\varphi_{S(X)} = P_X(l)$, ce qui conclut. □

Proposition 3.2.7. *On a : deg $(c_1(O_{\mathbb{P}}(d))^m = m! \prod_{i=1}^{m} d_i$.*

Démonstration : On note $H_i = \mathbb{P}^1 \times \ldots \times \{x_i\} \times \ldots \mathbb{P}^1$ où $\{x_i\}$, point de $\mathbb{P}^1$, est en $i^{\text{ème}}$ position. On a alors :

$$\begin{aligned} \deg\ (c_1(O_{\mathbb{P}}(d))^m) &= \deg(\sum_{i=1}^{m} d_i H_i)^m, \\ &= \deg(\sum \frac{m!}{i_1! \ldots i_m!} d_1^{i_1} \ldots d_m^{i_m} H_1^{i_1} \ldots H_m^{i_m}), \text{ par multilinéarité,} \\ &= m! \prod_{i=1}^{m} d_i. \end{aligned}$$

□

3.2.10 Diviseurs numériquement effectifs

On donne ici la définition des diviseurs *nef* et on indique certaines propriétés dont nous aurons besoin par la suite.

Définition 3.2.20 Soit X un schéma propre. Un diviseur de Cartier, D, sur X est dit *numériquement effectif (ou nef)* si, pour toute sous-variété Y de X, on a :

$$\deg\ (D^{\dim Y} \cdot Y) \geq 0.$$

Proposition 3.2.8. *Soit X un schéma propre, D un diviseur de Cartier, et L le faisceau associé. Si L est engendré par ses sections globales, alors D est nef.*

Démonstration : Soit Y une sous-variété de X. Le faisceau L est engendré par ses sections globales, donc il existe une section non nulle $s_Y \in H^0(Y,L)$. Le cycle associé au schéma des zéros de s_Y, $[Z(s_Y)]$, est un cycle effectif qui représente $c_1(L) \cap Y = D \cdot Y$. On itère ce raisonnement pour fabriquer un cycle effectif qui représente $c_1(L)^{\dim Y} \cap Y$, ce qui conclut. □

On donne ici une version asymptotique du théorème de Riemann-Roch, concernant les diviseurs numériquement effectifs. On admet pour cela une version asymptotique du théorème de Riemann-Roch-Hirzebruch pour les fibrés en droites :

Théorème 3.2.10. *soit D un diviseur de Cartier sur un schéma propre X de dimension r. On a, si χ dénote la caractéristique d'Euler-Poincaré :*

$$\chi(X,nD) = n^r \frac{deg\ D^r}{r!} + O(n^{r-1}).$$

De ceci on peut déduire la version concernant les diviseurs numériquement effectifs.

Théorème 3.2.11. *soit D un diviseur de Cartier nef sur un schéma propre X de dimension r. On a :*

$$
\begin{aligned}
&1. \quad h^i(X,nD) = O(n^{r-1}) \text{ pour } i > 0, \text{ et de plus,}\\
&2. \quad h^0(X,nD) = n^r \frac{deg\ D^r}{r!} + O(n^{r-1}).
\end{aligned}
$$

Démonstration : Le point 1. associé au théorème précédent nous donne le point 2. Il suffit donc de prouver le point 1. On note $L = O_X(-D)$, et on pose :

$$\mathcal{I}_1 = O_X \cap L,\ \mathcal{I}_2 = O_X \cap L^{-1}, \text{ et pour } i \in \{1,2\},\ \ O_{Z_i} = O_X/\mathcal{I}_i.$$

On remarque que $\mathcal{I}_2 \otimes L \simeq \mathcal{I}_1$, et que $\dim Z_i < \dim X$. On a le diagramme commutatif exact (L est inversible, donc le produit tensoriel $- \otimes L$ est exact) :

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \mathcal{I}_1 & \longrightarrow & O_X & \longrightarrow & O_{Z_1} & \longrightarrow & 0\\
 & & {\scriptstyle\simeq}\downarrow & & & & & & \\
0 & \longrightarrow & \mathcal{I}_2 \otimes L & \longrightarrow & O_X(-D) & \longrightarrow & O_{Z_2} \otimes L & \longrightarrow & 0.
\end{array}
$$

On tensorise par $L^{\otimes n}$, et on écrit la suite exacte longue de cohomologie pour chaque ligne :

$$H^i(X,L^{\otimes n} \otimes \mathcal{I}_1) \to H^i(X,L^{\otimes n}) \to H^i(Z_1,L^{\otimes n} \otimes O_{Z_1}) \quad \text{et,}$$

$$H^i(X,L^{\otimes n+1} \otimes \mathcal{I}_2) \to H^i(X,L^{\otimes n+1}) \to H^i(Z_2,L^{\otimes n+1} \otimes O_{Z_2}).$$

Or on sait que $H^i(X,\mathcal{I}_1 \otimes L^{\otimes n}) = H^i(X,\mathcal{I}_2 \otimes L^{\otimes n+1})$, donc :

$$
\begin{aligned}
h^i(X,L^{\otimes n+1}) &\leq h^i(X,\mathcal{I}_2 \otimes L^{\otimes n+1}) + h^i(Z_2,O_{Z_2} \otimes L^{\otimes n+1}) \quad \text{par le théorème du rang,}\\
&= h^i(X,\mathcal{I}_1 \otimes L^{\otimes n}) + h^i(Z_2,O_{Z_2} \otimes L^{\otimes n+1}) \ \ ,\\
&\leq h^i(X,L^{\otimes n}) + h^{i-1}(Z_1,O_{Z_1} \otimes L^{\otimes n}) + h^i(Z_2,O_{Z_2} \otimes L^{\otimes n+1}).
\end{aligned}
$$

On en déduit, par récurrence sur $r = \dim X$, que :

$$h^i(X,L^{\otimes n+1}) \leq h^i(X,L^{\otimes n}) + O(n^{r-2}) \text{ pour tout } i \geq 2.$$

En sommant ces inégalités, on en déduit que

$$h^i(X,L^{\otimes n}) = O(n^{r-1}) \text{ pour tout } i \geq 2.$$

Ainsi par le théorème asymptotique précédent on a :

$$h^0(X,L^{\otimes n}) - h^1(X,L^{\otimes n}) = n^r \frac{\deg D^r}{r!} + O(n^{r-1}).$$

Pour conclure, on va distinguer deux cas.
Si $h^0(X,L^{\otimes n}) = 0$ pour tout $n > 0$, alors, le membre de gauche de l'égalité est négatif. Or par hypothèse $\deg D^r \geq 0$, donc $h^1(X,L^{\otimes n}) = O(n^{r-1})$, ce qui conclut.
Sinon, il existe un entier $n_0 \geq 1$ tel que $h^0(X,L^{\otimes n_0}) > 0$. Donc, il existe un diviseur de Cartier effectif M, tel que $L^{\otimes n_0} = O_X(M)$. En considérant la suite exacte, (on note encore M le fermé associé au diviseur M)

$$0 \to O_X(-M) \to O_X \to O_M \to 0,$$

on en déduit que :

$$h^1(X,L^{\otimes n+n_0}) - h^1(X,L^{\otimes n}) \leq h^1(M,L^{\otimes n+n_0} \otimes O_M) = O(n^{r-2}).$$

Donc, on peut là encore conclure que $h^1(X,L^{\otimes n}) = O(n^{r-1})$. □

On rappelle maintenant la notion de diviseur ample, ainsi que le lien le plus évident (i.e le sens facile du critère de Nakai-Moishezon) entre les notions de ample et nef.

Définition 3.2.21 On dit qu'un diviseur D sur un schéma X est *ample* si il existe n assez grand tel que nD est très ample. On dit qu'un diviseur D sur un schéma X est *très ample* si il existe une immersion fermée $f : X \to \mathbb{P}^r$ pour un certain entier r, telle que $f^*(O_{\mathbb{P}^r}(1)) = O(D)$.

Proposition 3.2.9. *Si D est un diviseur ample sur un schéma X, alors, D est nef.*

Démonstration : Soit m tel que mD est très ample. On note $f : X \to \mathbb{P}^r$ l'immersion fermée telle que $f^*(O_{\mathbb{P}^r}(1)) = O(mD)$. En notant p_X et $p_{\mathbb{P}^r}$ les projections respectives de X et de $\mathbb{P}^r$ sur Spec K, on a, si Y est une sous-variété de X :

$$\begin{aligned}
\deg_X((mD)^{\dim Y} \cdot Y) &= \deg_X(c_1(f^*O_{\mathbb{P}^r}((1)))^{\dim Y} \cap Y, \\
&= (p_X)_* \left[(c_1(f^*O_{\mathbb{P}^r}(1))^{\dim Y} \cap Y\right], \\
&= (p_{\mathbb{P}^r})_* f_* \left[(c_1(f^*O_{\mathbb{P}^r}(1)))^{\dim Y} \cap Y\right], \text{ par fonctorialité,} \\
&= (p_{\mathbb{P}^r})_* \left[(c_1(O_{\mathbb{P}^r}(1)))^{\dim Y} \cap f_* Y\right], \text{ par formule de la projection,} \\
&= \deg_{\mathbb{P}^r}[f_*(Y)].
\end{aligned}$$

Or $f_*(Y)$ est une sous-variété de $\mathbb{P}^r$, et dans ce cas on sait, par le théorème 3.2.9 que $\deg_{\mathbb{P}^r}[f_*(Y)] = \deg_g(f_*(Y))$. Enfin, le point 1. de la proposition 3.2.6 nous indique que ce nombre est positif. $\square$

Cette proposition nous permet de retrouver la proposition 3.2.7 affirmant que :

$$\deg\ (c_1(O_{\mathbb{P}}(d))^m = m!\prod_{i=1}^{m} d_i.$$

En effet : le n-uplet d est tel que, pour tout i, $d_i \geq 1$, donc le faisceau $O_{\mathbb{P}}(d)$ est ample, donc nef. On peut donc lui appliquer le théorème de Riemann-Roch asymptotique précédent. Si D représente le diviseur de Cartier associé à $O_{\mathbb{P}}(d)$, on a :

$$h^0(X,nD) = n^m \frac{\deg\ D^m}{m!} + O(n^{m-1}).$$

Or par définition, $\deg\ D^m = \deg\ c_1(O_{\mathbb{P}}(d))^m$, donc :

$$\deg\ c_1(O_{\mathbb{P}}(d))^m = m! \frac{1}{n^m} h^0(X,nD) + O(n^{-1}).$$

Il nous suffit donc de calculer $h^0(X,nD)$ pour conclure. Or ceci se calcule en identifiant $H^0(X,nD)$ et l'espace vectoriel des polynômes multihomogènes de degré nd sur $K[X_1,Y_1,\ldots,X_m,Y_m]$. On a donc $h^0(X,nD) = \prod_{i=1}^m (nd_i + 1) = n^m \prod_{i=1}^m (d_i + \frac{1}{n})$. On en déduit :

$$\deg\ c_1(O_{\mathbb{P}}(d))^m = m! \prod_{i=1}^{m} (d_i + \frac{1}{n}) + O(n^{-1}).$$

On conclut alors en passant à la limite sur n.

3.3 Le lemme de Dyson selon M. Nakamaye.

3.3.1 Énoncé des théorèmes

On commence d'abord par rappeler la notion diophantienne d'indice d'une section puis on énonce les deux théorèmes principaux.

Indice d'une section

On note

$$\mathbb{P} = \prod_{i=1}^{m} \mathbb{P}^1, \text{ et } \ d = (d_1,\ldots,d_m) \text{ avec } \forall i \in [\![1,m]\!],\ d_i \geq 1.$$

On pose $\pi_j : \mathbb{P} \to \mathbb{P}^1$ la projection (fermée) sur la $\text{j}^{\text{ème}}$ composante. On considère $\zeta = ((\lambda_1 : \eta_1), \dots, (\lambda_m : \eta_m))$ un point fermé de $\mathbb{P}$, on note $O_{\mathbb{P}^1, \pi_j(\zeta)}$ l'anneau local en $\pi_j(\zeta)$. C'est un anneau de valuation discrète, car local, noethérien régulier de dimension 1. On note z_j une uniformisante locale de cet anneau et on note (abusivement) aussi z_j le pull-back de z_j dans $\mathbb{P}$. On obtient ainsi un système de paramètres locaux de $O_{\mathbb{P},\zeta}$. Soit alors $s \in H^0(\mathbb{P}, O_{\mathbb{P}}(d))$, où $d = (d_1, \dots, d_m)$. On sait (car ζ est lisse) que :

$$O_{\mathbb{P},\zeta} \hookrightarrow \widehat{O_{\mathbb{P},\zeta}} \simeq K[\![z_1, \dots, z_m]\!].$$

En prenant une trivialisation locale de $O_{\mathbb{P}}(d)$ en ζ, on a donc, localement en ζ :

$$s = \sum_{(\alpha_1, \dots, \alpha_m) \in \mathbb{N}^m} a_{\alpha_1, \dots, \alpha_m} z_1^{\alpha_1} \dots z_m^{\alpha_m}.$$

Si $s \neq 0$, on définit alors *l'indice de s en ζ* comme étant :

$$\operatorname{Ind}(\zeta, s) = \min \left\{ \sum_{\nu=1}^{m} \frac{\alpha_\nu}{d_\nu} \ / \ a_{\alpha_1, \dots, \alpha_m} \neq 0 \right\}.$$

Proposition 3.3.1. *L'indice de s en ζ est indépendant du choix d'un système de paramètres locaux.*

Le lemme de Dyson

On considère $\zeta_1, \dots, \zeta_M$, M points de $\mathbb{P}$ vérifiant l'hypothèse **(H)** : pour tout j, si $i_1 \neq i_2$, alors, $\pi_j(\zeta_{i_1}) \neq \pi_j(\zeta_{i_2})$, autrement dit, on ne peut pas trouver i et j tels que les points ζ_i et ζ_j appartiennent à une sous-variété produit propre de $\mathbb{P}$.

On commence par définir une fonction *volume* intervenant dans l'énoncé des théorèmes.

Définition 3.3.1 Soit $I^m = \{(x_i) \in \mathbb{R}^m \ / 0 \leq x_i \leq 1\}$, on définit la fonction Vol(t) par :

$$\text{Vol(t)} = \text{Vol}\left(\left\{(x_i) \in I^m \ / \sum_{i=1}^{m} x_i \leq t\right\}\right).$$

On peut maintenant énoncer les deux théorèmes :

Théorème 3.3.1. ***Dyson 1*** *Soit $s \in H^0(\mathbb{P}, O_{\mathbb{P}}(d))$ une section non nulle et soit $\zeta_1, \dots, \zeta_M$ vérifiant l'hypothèse **(H)**. Soit $t_i = Ind(\zeta_i, s)$ et $M' = \max\{M-2, 0\}$, alors, on a :*

$$\sum_{i=1}^{M} Vol(t_i) \leq \prod_{i=1}^{m-1} \left(1 + \max_{i+1 \leq j \leq m} \left\{\frac{M' d_j}{d_i}\right\}\right).$$

Théorème 3.3.2. ***Dyson 2*** *Avec les mêmes hypothèses que dans le théorème précédent, et en posant* $\delta = \max_{2 \le i+1 \le j \le m} \left\{ \frac{d_j}{d_i} \right\}$, *on a :*

$$\sum_{i=1}^{M} Vol(t_i - m\delta) \le 1.$$

On va tout d'abord démontrer le théorème 3.3.2, puis on indiquera comment obtenir le théorème 3.3.1 par une méthode similaire.

Le plan de la démonstration est le suivant : en utilisant le théorème du produit, on construit un cycle effectif qui représente la classe $c_1(O_{\mathbb{P}}(d))^m$. En notant R_i la partie de l'intersection supportée par Z_i (où Z_i est le support d'un faisceau d'idéaux à construire, renseignant sur l'indice au point ζ_i), on obtient ainsi une majoration de $\sum_{i=1}^{M} \deg R_i$. En considérant un éclatement bien choisi de $\mathbb{P}$ on réussi alors, en utilisant la formule de la projection, à obtenir une minoration des deg R_i. En mettant bout à bout la majoration et la minoration, ainsi qu'un petit calcul de volume, on en déduit le résultat.

3.3.2 Le faisceau d'idéaux $\mathcal{I}_d(s)$

On construit ici les faisceaux informant sur l'indice d'une section aux points ζ_i, et on étudie quelques propriétés de leur support.

Les faisceaux d'idéaux $\mathcal{I}_d(s)$ et $\mathfrak{I}_{\zeta,d,t}$

But : fabriquer un faisceau d'idéaux $\mathcal{I}_d(s)$ sur $\mathbb{P}$ tel que :

$s \in H^0(\mathbb{P}, O_{\mathbb{P}}(d) \otimes_{O_{\mathbb{P}}} \mathcal{I}_d(s))$ et tel que $\mathcal{I}_d(s)$ informe sur l'indice de s aux points $\{\zeta_i\}_{i \le M}$.

Soit $\zeta \in \mathbb{P}$ et $t \in \mathbb{R}^+$. On définit $\mathfrak{I}_{\zeta,d,t}$ comme suit :

$$\mathfrak{I}_{\zeta,d,t} = \left\langle \left\{ M_\alpha = \prod_{i=1}^{m} z_i^{\alpha_i} \ / \ \alpha_i \le d_i \text{ et } \mathrm{Ind}(\zeta, M_\alpha) \ge t \right\} \right\rangle .$$

Par définition, $\mathfrak{I}_{\zeta,d,t} \subset O_{\zeta,\mathbb{P}}$. De plus, chaque z_i provient d'une section définie sur un petit ouvert produit, affine. Quitte à restreindre on peut supposer que les (sections associées aux) z_i sont toutes définies sur

$$U = \prod_{k=1}^{m} \mathrm{Spec}\ A_k = \mathrm{Spec}\ \bigotimes_{k=1}^{m} A_k .$$

De plus, quitte à restreindre une nouvelle fois on peut aussi supposer que pour tout i, $\pi_i(\zeta)$ est le seul zéro de z_i sur $U_i = \mathrm{Spec}\ A_i$. On note encore $\mathfrak{I}_{\zeta,d,t}$ le faisceau d'idéaux quasi-cohérent associé à $\mathfrak{I}_{\zeta,d,t} \cap A$, où, $A = \bigotimes_{i=1}^{m} A_i$. Enfin, si $i \ : \ U \longrightarrow \mathbb{P}$ désigne l'inclusion naturelle, on définit ainsi un faisceau d'idéaux cohérent, inclus dans $O_{\mathbb{P}}$ en posant :

$$\mathcal{I}_{\zeta,d,t} = i_* \mathfrak{I}_{\zeta,d,t}.$$

On remarque que cette construction est indépendante du choix de U. Plus précisément, si V est un autre ouvert produit, affine, inclus dans U, alors comme la construction est locale, on a : $\mathfrak{I}_{\zeta,d,t,V} \simeq \mathfrak{I}_{\zeta,d,t,U|V}$.
Par ailleurs, en faisant l'identification entre, $H^0(\mathbb{P},O_{\mathbb{P}}(d))$ et l'espace des polynômes multihomogènes de degré d en les variables $(X_1,Y_1,\ldots,X_m,Y_m)$ sur K, on constate que le K-espace vectoriel $H^0\left(\mathbb{P},\mathcal{I}_{\zeta,d,t} \otimes_{O_{\mathbb{P}}} O_{\mathbb{P}}(d)\right)$, est engendré par les polynômes

$$\prod_{\nu=1}^{m} (\eta_\nu X_\nu - \lambda_\nu Y_\nu)^{i_\nu} Y_\nu^{d_\nu - i_\nu} \text{ avec, } \forall \nu \leq m \ \ 0 \leq i_\nu \leq d_\nu \text{ et } \sum_{\nu=1}^{m} \frac{i_\nu}{d_\nu} \geq t.$$

On pose enfin :

$$\mathcal{I}_d(s) = \bigcap_{j=1}^{M} \mathcal{I}_{\zeta_j,d,t_j}.$$

Le support de $O_{\mathbb{P}}/\mathcal{I}_{\zeta,d,t}$

On pose $Z = \mathrm{Supp}(O_{\mathbb{P}}/\mathcal{I}_{\zeta,d,t})$ et Z_i pour les supports associés aux t_i. Le lemme suivant nous en donne une description explicite. On rappelle tout d'abord une notation : si J est un ensemble de polynômes, contenu dans $K[X_1,Y_1,\ldots,X_m,Y_m]$, on notera

$$V(J) = \{\xi \in \mathbb{P} / \ \forall P \in < J > \ \ P(\xi) = 0 \ \}.$$

Lemme 3.3.1. *Avec les notations précédentes on a* $Z = \bigcup_{I \subset [\![1,m]\!]} S_I$ *où :*

$$S_I = \begin{cases} \emptyset & si \ |I| \geq t, \\ V\left(\eta_\nu X_\nu - \lambda_\nu Y_\nu ; \ \nu \notin I\right) & sinon. \end{cases}$$

Démonstration : Quitte à faire un changement de système de coordonnées, on peut supposer que, pour tout ν, $\eta_\nu \neq 0$. Soit $P \in S_I$, montrons que $P \in Z$. Soit $\underline{i}$ un m-uplet d'éléments de $\prod [\![1,d_\nu]\!]$ tel que $\sum \frac{i_\nu}{d_\nu} \geq t$, alors il existe $\nu_0 \notin I$ tel que $i_{\nu_0} \neq 0$. En effet, $P \in S_I$ donc S_I est non vide, donc $|I| < t$. Si pour tout $\nu \notin I$ on avait $i_\nu = 0$, alors on aurait

$$t \leq \sum_{i=1}^{m} \frac{i_\nu}{d_\nu} = \sum_{\nu \in I} \frac{i_\nu}{d_\nu} < t, \ \text{ ce qui est idiot.}$$

Notamment on a $(\eta_\nu X_\nu - \lambda_\nu Y_\nu)^{i_{\nu_0}}(P) = 0$ et on a donc :

$$\forall \underline{i} \text{ tel que} \begin{cases} \sum_{\nu=1}^{m} \frac{i_\nu}{d_\nu} \geq t, \\ \forall \nu \in [\![1,m]\!] \ \ 0 \leq i_\nu \leq d_\nu \end{cases} \text{ on a } \prod_{\nu=1}^{m} (\eta_\nu X_\nu - \lambda_\nu Y_\nu)^{i_\nu} Y_\nu^{d_\nu - i_\nu}(P) = 0.$$

En particulier on en déduit que $P \in Z$.
Réciproquement, soit $P \in Z$ et soit J l'ensemble des $\nu \in [\![1,m]\!]$ tels que P appartient à $V(\eta_\nu X_\nu - \lambda_\nu Y_\nu)$. Montrons que P appartient à S_{J^c}, où J^c désigne le complémentaire dans $[\![1,m]\!]$ de J. Par définition de J il suffit de vérifier que $|J| \geq t$. Soit Q le monôme

$$\prod_{\nu \notin J} (\eta_\nu X_\nu - \lambda_\nu Y_\nu)^{d_\nu} \prod_{\nu \in J} Y_\nu^{d_\nu}.$$

Alors, par définition de J, si $\nu \notin J$, $(\eta_\nu X_\nu - \lambda_\nu Y_\nu)(P) \neq 0$; et si $\nu \in J$, $Y_\nu(P) \neq 0$ (sinon $\pi_\nu(P) = (0:0)$ dans $\mathbb{P}^1$, car pour tout ν, $\eta_\nu \neq 0$, ce qui est impossible). Donc $Q(P) \neq 0$. Soit alors $\underline{i}$ défini par : $i_\nu = 0$ si $\nu \in J$ et $i_\nu = d_\nu$ sinon. Dans ce cas on a :

$$Q = \prod_{\nu=1}^{m} (\eta_\nu X_\nu - \lambda_\nu Y_\nu)^{i_\nu} Y_\nu^{d_\nu - i_\nu} \text{ et } \sum_{\nu=1}^{m} \frac{i_\nu}{d_\nu} = |J^c|.$$

Or $P \in Z$ et $Q(P) \neq 0$ donc $|J| \geq t$. □

Lemme 3.3.2. *Soit μ et λ dans $[\![1,M]\!]$ deux entiers distincts, et ζ_μ et ζ_λ deux points de $\mathbb{P}$ vérifiant l'hypothèse **(H)**, alors, $m \geq t_\mu + t_\lambda$.*

Démonstration : Quitte à faire un changement de système de coordonnées, on peut supposer que : $\zeta_\lambda = ((1:0), \ldots, (1:0))$ et que $\zeta_\mu = ((0:1), \ldots, (0:1))$. Si
$F = \sum_{\underline{i}} \alpha_{\underline{i}} \prod_{\nu=1}^{m} X_\nu^{i_\nu} Y_\nu^{d_\nu - i_\nu}$ est une section globale non nulle de $\mathcal{I}_d(s)$, alors, pour tout n-uplet $\underline{i}$ tels que $\alpha_{\underline{i}} \neq 0$, on a :

$$\prod_{\nu=1}^{m} X_\nu^{i_\nu} Y_\nu^{d_\nu - i_\nu} \text{ est un des générateurs de } H^0(\mathbb{P}, O_{\mathbb{P}}(d) \otimes_{O_{\mathbb{P}}} \mathcal{I}_{\zeta_\lambda, d, t_\lambda}),$$

et la même chose est vraie pour (ζ_μ, d, t_μ). On en déduit :

$$\sum_{\nu=1}^{m} \frac{i_\nu}{d_\nu} \geq t_\lambda \text{ et } \sum_{\nu=1}^{m} \frac{d_\nu - i_\nu}{d_\nu} \geq t_\mu.$$

L'inégalité attendue en résulte immédiatement. □

Proposition 3.3.2. *Sous les mêmes hypothèses, on a $Z_\mu \cap Z_\lambda = \emptyset$.*

Démonstration : Comme précédemment on suppose que : $\zeta_\lambda = ((1:0), \ldots, (1:0))$ et que $\zeta_\mu = ((0:1), \ldots, (0:1))$. Si $Z_\mu \cap Z_\lambda \neq \emptyset$, alors il existe I_μ et I_λ deux sous-ensembles de $[\![1,m]\!]$ tels que :

$$|I_\mu| < t_\mu \text{ et } |I_\lambda| < t_\lambda \text{ et tels que } V\left(X_\nu / \nu \notin I_\mu\right) \cap V\left(Y_\nu / \nu \notin I_\lambda\right) \neq \emptyset.$$

Soit $\nu \notin (I_\mu \cup I_\lambda)$, alors $V(X_\nu) \cap V(Y_\nu) \neq \emptyset$, ce qui est idiot. Donc on a $I_\mu \cup I_\lambda = [\![1,m]\!]$ et en particulier $m < t_\mu + t_\lambda$, ce qui contredit le lemme précédent. □

Soit $\mathbb{P}'$ une sous-variété produit de $\mathbb{P}$, on pose $O_{\mathbb{P}'}(d) = O_{\mathbb{P}}(d)_{|\mathbb{P}'}$. Le lemme 3.3.1 nous indique que : $\forall i \in [\![1,M]\!]$, le support $Z_i = \mathrm{Supp}(O_{\mathbb{P}}/\mathcal{I}_{\zeta_i,kd,t_i})$ ne dépend pas de k pour $k > 0$, donc

$$\bigcup_{i=1}^{M} Z_i = \mathrm{Supp}(O_{\mathbb{P}}/\mathcal{I}_{kd}(s)) \text{ n'en dépend pas non plus.}$$

Proposition 3.3.3. *Si $\mathbb{P}' \subset Z_i$ pour un entier $i \in [\![1,m]\!]$ alors,*

$$\forall k > 0,\ H^0\left(\mathbb{P}',O_{\mathbb{P}'}(kd) \otimes \mathcal{I}_{kd}(s)\right) = 0.$$

Démonstration : On a $\mathcal{I}_{kd}(s) \subset \mathcal{I}_{\zeta_i,kd,t_i}$ et $\mathbb{P}' \subset Z_i$. Par indépendance par rapport à k, on sait que : $Z_i = \mathrm{Supp}(O_{\mathbb{P}}/\mathcal{I}_{\zeta_i,kd,t_i})$. Soit $\xi \in \mathbb{P}'$, alors $\xi \in Z_i$, donc pour toute section s appartenant à $H^0\left(\mathbb{P}',O_{\mathbb{P}'}(kd) \otimes \mathcal{I}_{kd}(s)\right)$, ceci implique que $s(\xi) = 0$ et donc que $s = 0$, d'où le résultat. □

Par ailleurs on a un résultat contraire si la sous-variété produit $\mathbb{P}'$ de $\mathbb{P}$ n'est contenue dans aucun Z_i. On renvoie à l'article [EV84] (lemme 2.8) pour une démonstration de ce fait :

Proposition 3.3.4. *Si pour tout i, $\mathbb{P}' \not\subset Z_i$, alors, pour un k suffisamment grand, on a :*

$$H^0\left(\mathbb{P}',O_{\mathbb{P}'}(kd) \otimes \mathcal{I}_{kd}(s)\right) \neq 0.$$

Un calcul de volume

On indique ici un calcul de volume qui nous servira dans la dernière étape de la démonstration. Il concerne l'espace des sections globales de $O_{\mathbb{P}}(nd) \otimes \mathcal{I}_{\zeta,nd,t}$.

Proposition 3.3.5. *Si ζ est un point de $\mathbb{P}$, on a :*

$$\mathit{Vol}(t) = \lim_{n\to\infty} \frac{h^0\left(\mathbb{P},O_{\mathbb{P}}(nd)\right) - h^0\left(\mathbb{P},O_{\mathbb{P}}(nd) \otimes \mathcal{I}_{\zeta,nd,t}\right)}{n^m \prod_{k=1}^m d_k}.$$

Démonstration : On note $I(d,t) = \left\{ (x_\nu) \in [0,1]^m \ / \ \sum\limits_{\nu=1}^{m} x_\nu \leq t \right\}$. On sait que :

$$\left(\prod_{i=1}^{m} d_i\right) \mathrm{Vol}(t) = \lim_{n\to\infty} \frac{1}{n^m} \left| I(d,t) \bigcap \prod_{i=1}^{m} \frac{1}{nd_i}\mathbb{Z} \right|.$$

Par ailleurs,

$$\begin{aligned} I(d,t) \bigcap \prod_{i=1}^{m} \frac{1}{nd_i}\mathbb{Z} &= \left\{ (x_\nu) \in [0,1]^m \ / x_\nu = \frac{i_\nu}{nd_\nu},\ i_\nu \in \mathbb{Z} \text{ et } \sum_{\nu=1}^{m} x_\nu \leq t \right\}, \\ &= \left\{ \left(\frac{i_\nu}{d_\nu}\right) \in [0,n]^m \ / \ i_\nu \in \mathbb{Z},\ \sum_{\nu=1}^{m} \frac{i_\nu}{nd_\nu} \leq t \right\}, \\ &= \left\{ (i_\nu) \in \mathbb{Z}^m \ / \ 0 \leq i_\nu \leq nd_\nu,\ \sum_{\nu=1}^{m} \frac{i_\nu}{nd_\nu} \leq t \right\}. \end{aligned}$$

On en déduit donc que :

$$\left(\prod_{i=1}^{m} d_i\right) \mathrm{Vol}(t) = \lim_{n\to\infty} \frac{1}{n^m} \left| \left\{ (i_\nu) \in \mathbb{Z}^m \ / \ 0 \le i_\nu \le nd_\nu, \ \sum_{\nu=1}^{m} \frac{i_\nu}{nd_\nu} \le t \right\} \right|.$$

Or, par définition du faisceau d'idéaux $\mathcal{I}_{\zeta,nd,t}$, on sait que :

$$h^0\left(\mathbb{P}, O_{\mathbb{P}}(nd)\right) - h^0\left(\mathbb{P}, O_{\mathbb{P}}(nd) \otimes \mathcal{I}_{\zeta,nd,t}\right) = \left| \left\{ (i_\nu) \in \mathbb{Z}^m \ / \ 0 \le i_\nu \le nd_\nu, \ \sum_{\nu=1}^{m} \frac{i_\nu}{nd_\nu} < t \right\} \right|.$$

Donc en passant à la limite, on en déduit bien le résultat voulu. □

On indique également une conséquence de ce calcul, qui nous servira dans la démonstration du théorème 3.3.1. Il s'agit d'une version affaiblie de la proposition précédente, dans le cas où on remplace le faisceau $O_{\mathbb{P}}(d)$ par un fibré en droite L.

Proposition 3.3.6. *Si ζ est un point de $\mathbb{P}$, et L un fibré en droite sur $\mathbb{P}$ tel que $L \otimes O_{\mathbb{P}}(-d)$ admet une section globale, alors :*

$$Vol(t) \le \lim_{n\to\infty} \frac{h^0\left(\mathbb{P}, L^{\otimes n}\right) - h^0\left(\mathbb{P}, L^{\otimes n} \otimes \mathcal{I}_{\zeta,nd,t}\right)}{n^m \prod_{k=1}^{m} d_k}.$$

Démonstration : Considérons l'espace vectoriel $V_{n,t}$ engendré par :

$$\left\{ \prod_{i=1}^{m} z_k^{i_k} \quad / \sum_{k=1}^{m} \frac{i_k}{nd_k} < t, \ \ 0 \le i_k \le nd_k \right\}.$$

Par définition de $V_{n,t}$ et du faisceau d'idéaux $\mathcal{I}_{\zeta,nd,t}$, on sait que :

$$\dim V_{n,t} = h^0(\mathbb{P}, O_{\mathbb{P}}(nd)) - h^0(\mathbb{P}, O_{\mathbb{P}}(nd) \otimes \mathcal{I}_{\zeta,nd,t}).$$

Ainsi, il suffit de montrer que $\dim V_{n,t} \le h^0\left(\mathbb{P}, L^{\otimes n}\right) - h^0\left(\mathbb{P}, L^{\otimes n} \otimes \mathcal{I}_{\zeta,nd,t}\right)$ pour conclure. Or $L \otimes O_{\mathbb{P}}(-d)$ est un fibré en droite sur $\mathbb{P}$ qui, par hypothèse, admet une section globale. Donc il est engendré par ses sections globales (ceci découle du corollaire 3.1.3 et du fait que $O(d)$ est engendré par ses sections globales si $d = (d_1, \ldots, d_m) \ge 0$). On peut prendre une section globale $\gamma \in H^0(\mathbb{P}, L \otimes O_{\mathbb{P}}(-d))$, telle que $\gamma(\zeta) \neq 0$. Mais alors, en tensorisant n fois par γ, on peut plonger $V_{n,t}$ dans $H^0(\mathbb{P}, L^{\otimes n})$ et ce, de manière disjointe de $H^0(\mathbb{P}, L^{\otimes n} \otimes \mathcal{I}_{\zeta,nd,t})$. Ceci prouve l'inégalité de dimension cherchée. □

3.3.3 Le théorème du produit

On donne dans cette partie la démonstration d'un *théorème du produit*, dans l'esprit de celui introduit par Faltings dans [Fal91].

Définition 3.3.2 Soit f un polynôme de $K[X_1,\ldots,X_m]$ de multidegré $d=(d_1,\ldots,d_m)$, et soit W une variété sur K, on appelle *multiplicité* de f selon la variété W, et on note :

$$\mathrm{mult}_W f = r \text{ si } \forall\beta=(\beta_1,\ldots,\beta_m) \text{ avec } \sum_{i=1}^m \beta_i \le r-1 \text{ on a : } \prod \frac{\partial^{\beta_i}}{\partial X_i^{\beta_i}} f_{|W} = 0,$$

et si il existe β, avec $\sum_{i=1}^m \beta_i = r$, tel que ceci est faux.

Lemme 3.3.3. *Soit X une variété sur K et W une sous-variété, alors l'ensemble*

$$U = \{x \in W \ / mult_x f = mult_W f\}$$

est un ouvert non vide de W.

Démonstration : On note immédiatement que $\forall x \in W$, $\mathrm{mult}_x f \ge \mathrm{mult}_W f$. Or, si pour tout $x \in W$ l'inégalité était stricte, alors on aurait $\mathrm{mult}_W f \ge \mathrm{mult}_W f + 1$, ce qui est idiot. Ainsi, l'ensemble U n'est pas vide. Montrons que son complémentaire F est fermé. Par définition,

$$\begin{aligned} F &= \{x \in W \ /\mathrm{mult}_x f > \mathrm{mult}_W f\} \\ &= \{x \in W \ /\mathrm{mult}_x f \ge \mathrm{mult}_W f + 1\} \\ &= \left\{ x \in W \ /\forall\alpha=(\alpha_1,\ldots,\alpha_m)\in\mathbb{N}^m \text{ tel que } \sum_{i=1}^m \alpha_i \le \mathrm{mult}_W f \text{ on à } D^\alpha f(\eta) = 0 \right\}. \end{aligned}$$

La dernière expression de F montre qu'il s'agit bien d'un fermé. □

Lemme 3.3.4. *Soit $\varphi : X \to Y$ un morphisme dominant entre variétés lisses sur K. Si $\Omega_{X/Y}$ est localement libre de rang $n = \dim X - \dim Y$ sur X, alors pour tout point fermé $x \in X$, l'application $T_\varphi : T_x \to T_{\varphi(x)}$ est surjective.*

Démonstration : Soit $x \in X$, on applique la $1^{ère}$ suite exacte fondamentale tensorisée par $K(x)$, corps résiduel au point x :

$$\varphi^*\Omega_{Y/K} \otimes K(x) \xrightarrow{u} \Omega_{X/K} \otimes K(x) \xrightarrow{v} \Omega_{X/Y} \otimes K(x) \to 0.$$

Les variétés X et Y sont lisses, donc par la réciproque de la proposition 3.1.1, les trois espaces intervenant dans la suite exacte précédente sont de dimensions respectives dim Y, dim X et n; donc u est injective. De plus, si x est un point fermé de X alors $K(x) \simeq K$, donc, d'après la démonstration de la proposition 3.1.1, u est juste l'application naturelle de $\mathfrak{M}_y/\mathfrak{M}_y^2$ dans $\mathfrak{M}_x/\mathfrak{M}_x^2$, où $y = \varphi(x)$. Ainsi en passant au dual on en déduit que T_φ est surjective de T_x sur T_y. □

Lemme 3.3.5. *Soit $\varphi : X \to Y$ un morphisme dominant entre variétés sur K. Alors il existe un ouvert U non vide de X tel que pour tout point fermé $x \in U$, l'application $T_\varphi : T_x \to T_{\varphi(x)}$ est surjective.*

Démonstration : Le corollaire 3.1.1 nous dit qu'il existe un ouvert (dense) de X qui est lisse et pareil pour Y. Donc quitte à se restreindre à ces ouverts, on peut supposer que X et Y sont lisses. Comme on est en caractéristique 0, et par le théorème 3.1.1, on sait que :

$$\dim \Omega_{\mathcal{R}(X)/\mathcal{R}(Y)} = \deg_{tr} \mathcal{R}(X)/\mathcal{R}(Y) = \dim X - \dim Y =: n.$$

Or $\Omega_{\mathcal{R}(X)/\mathcal{R}(Y)}$ est la tige au point générique x du faisceau $\Omega_{X/\mathcal{R}(Y)}$, et le schéma X est noethérien, donc il existe un voisinage ouvert U de x tel que $\Omega_{X/Y|U}$ est libre de rang n. On conclut alors en appliquant le lemme 3.3.4 précédent. □

Théorème 3.3.3. ***théorème du produit*** *Soit $f \in K[X_1, \ldots, X_m]$ un polynôme non nul de multidegré $d_1, \ldots, d_m$, et soit*

$$X(f) = \left\{ x \in K^m \ / \forall\ 0 \leq \alpha_i \leq \max_{i+1 \leq j \leq m} d_j,\ \ D^\alpha f(x) = 0 \right\},$$

$$\text{où } \alpha = (\alpha_1, \ldots, \alpha_m) \text{ et } D^\alpha f = \frac{\partial^{\alpha_1}}{\partial X_1^{\alpha_1}} \cdots \frac{\partial^{\alpha_{m-1}}}{\partial X_{m-1}^{\alpha_{m-1}}} f.$$

Soit $W \subset X(f)$ une composante irréductible, alors W est inclus dans une sous-variété produit propre de K^m, c'est à dire : il existe $x_d \in K$ tel que $W \subset K^d \times \{x_d\} \times K^{n-d-1}$.

Démonstration : Si $X(f)$ est vide, le résultat est immédiat, sinon, on va montrer que on est dans une des deux alternatives suivantes : soit $\pi_m(W)$ est réduit à un point, soit W est de la forme $W' \times K$ pour une sous-variété W' de K^{m-1}.

Dans le premier cas : $W \subset K^{m-1} \times \{.\}$ ce qui conclut.

Dans le second cas : soit $\lambda \in K$ et soit $f_\lambda(X_1, \ldots, X_{m-1}) = f(X_1, \ldots, X_{m-1}, \lambda)$, on a

$$\frac{\partial^{\alpha_1} \ldots \partial^{\alpha_{m-2}}}{\partial X_1^{\alpha_1} \ldots \partial X_{m-2}^{\alpha_{m-2}}} f_\lambda(X_1, \ldots, X_{m-1}) = \prod_{i=1}^{m-2} \frac{\partial^{\alpha_i}}{\partial X_i^{\alpha_i}} f(X_1, \ldots, X_m)_{|X_m = \lambda}.$$

$$\text{Or le polynôme } \prod_{i=1}^{m-2} \frac{\partial^{\alpha_i}}{\partial X_i^{\alpha_i}} f(X_1, \ldots, X_m) \text{ s'annule sur } W' \times K \text{ pour } \alpha_i \leq \max_{i+1 \leq j \leq m} d_j,$$

$$\text{donc } \prod_{i=1}^{m-2} \frac{\partial^{\alpha_i}}{\partial X_i^{\alpha_i}} f_\lambda(X_1, \ldots, X_{m-1})_{|W'} = 0 \text{ pour } 0 \leq \alpha_i \leq \max_{i+1 \leq j \leq m-1} d_j.$$

$$\text{Ainsi } W' \subset X(f_\lambda), \text{ et,}$$

par récurrence sur m, on en déduit que W' est inclus dans une sous-variété produit propre de K^{m-1}, donc W aussi. Il reste à montrer que si $\pi_m(W) \neq 0$, alors W est bien de la forme annoncée.

La variété W est une variété irréductible sur le corps K, donc d'après le corollaire 3.1.1 il existe un ouvert dense U_1 de W formé de points lisses. Par ailleurs le lemme 3.3.3 nous dit que l'ensemble U_2 sur lequel $\mathrm{mult}_\eta f = \mathrm{mult}_W f$ est un ouvert dense. De plus on suppose que $\pi_m : W \to K$ est surjective, donc le lemme 3.3.5 nous dit qu'il existe un ouvert dense U_3 tel que pour tout point fermé $\eta \in U_3$, l'application induite sur les espaces tangents $T_\eta W \to T_{\pi_m(\eta)} K$ est surjective. Ainsi, en prenant un point η assez général, i.e un point fermé, dans l'intersection des trois ouverts précédents, on peut supposer ces trois conditions vérifiées simultanément en η. Enfin, après translation en l'origine, on suppose aussi que $T_\eta W \subset T_0(K^m)$. On a alors :

$$\textbf{(1)}\quad T_\eta W + \left\langle \frac{\partial}{\partial X_1}, \cdots, \frac{\partial}{\partial X_{m-1}} \right\rangle = T_0(K^m).$$

Fait : il existe $i \in [\![1,m-1]\!]$ tel que $\mathrm{mult}_\eta(\frac{\partial}{\partial X_i}(f)) = \mathrm{mult}_\eta(f) - 1$.
En effet, soit D un opérateur différentiel, d'ordre $\leq \mathrm{mult}_\eta(f) - 1$, et soit $\frac{\partial}{\partial X} \in T_\eta W$. Si $D = D^\alpha$ où D^α est un opérateur de la forme définie précédemment, alors comme $D^\alpha(f)$ s'annule sur W et $\frac{\partial}{\partial X} \in T_\eta W$, on a :

$$\left(D^\alpha \frac{\partial}{\partial X}(f)\right)_{|\eta} = \frac{\partial}{\partial X} D^\alpha(f)_{|\eta} = 0.$$

Sinon, le même raisonnement appliqué à $D = D^\alpha \partial$ avec $\partial \in T_\eta W$ marche encore. En utilisant **(1)**, on peut donc encore conclure comme précédemment.

$$\text{Ainsi,}\quad \textbf{(2)}\ \ \forall \frac{\partial}{\partial X} \in T_\eta W \text{ on a : } \mathrm{mult}_\eta \frac{\partial}{\partial X}(f) \geq \mathrm{mult}_\eta(f).$$

Supposons par l'absurde que le fait est faux. Alors, pour tout i dans $[\![1,m-1]\!]$, on a : $\mathrm{mult}_\eta \frac{\partial}{\partial X_i} f \geq \mathrm{mult}_\eta(f)$. Or l'égalité **(1)** implique :

$$\frac{\partial}{\partial X_m} = \sum_{i=1}^{m-1} \lambda_i \frac{\partial}{\partial X_i} + \lambda \frac{\partial}{\partial X}.$$

Mais alors, **(2)** implique $\mathrm{mult}_\eta \frac{\partial}{\partial X_m} f \geq \mathrm{mult}_\eta f$, donc pour tout α et tout β tels que $0 \leq \sum \alpha_i \leq 1$ et $0 \leq \sum \beta_i \leq \mathrm{mult}_\eta f - 1$, on a $\partial^{\alpha+\beta} f_{|\eta} = 0$. On en déduit que $\mathrm{mult}_\eta f \geq \mathrm{mult}_\eta f + 1$ ce qui est absurde, d'où le fait.

On applique ceci à $\frac{\partial}{\partial X_i} f$ où l'indice i est celui obtenu par le fait. En itérant, après $\mathrm{mult}_\eta f$ itérations, on obtient :

$$\left(\prod_{k=1}^{m-1} \frac{\partial^{i_k}}{\partial X_k^{i_k}} f\right)(\eta) \neq 0 \text{ avec } \sum_{k=1}^{m-1} i_k = \mathrm{mult}_\eta f = \mathrm{mult}_W f.$$

Or par définition de $X(f)$, $D^\alpha(f)_{|W} = 0$ pour tout $\alpha_i \in [\![0, \max d_j]\!]$, notamment pour tout $\alpha_i \in [\![0,d_m]\!]$. Donc il existe nécessairement un entier k tel que $i_k \geq d_m + 1$. On en déduit que $\mathrm{mult}_W f \geq d_m + 1$, or $\deg_{X_m} f = d_m$, donc ceci est possible seulement si la sous-variété W est de la forme $W' \times K$, ce qu'on voulait démontrer. □

3.3.4 Fin de la preuve du théorème 3.3.2

On utilise dans cette partie le lemme du produit pour démontrer le lemme clé, puis on se sert de la théorie de l'intersection pour conclure.

Le lemme clé

Lemme 3.3.6. ***(lemme clé)*** *Soit $s \in H^0(\mathbb{P},O_{\mathbb{P}}(d))$ une section non nulle, soit M points, $\zeta_1,\ldots,\zeta_M$ vérifiant l'hypothèse **(H)**, et soit $t_i = Ind(\zeta_i,s)$. Il existe un entier n*

suffisamment grand, tel que : si $V \subset \mathbb{P}$ est une sous-variété qui n'est contenue dans aucun Z_i, alors,

$$H^0\left(V,O_P(nd) \otimes \bigcap_{i=1}^{M} \mathcal{I}_{\zeta_i,nd,t_i-m\delta}\right) \neq 0.$$

Démonstration : On commence tout d'abord par montrer l'existence d'une section avec un n_V qui dépend à priori de la variété V :
Soit $K^m \subset \mathbb{P}$ un ouvert affine contenant les points ζ_i, pour tout $i \in [\![1,M]\!]$. Sur K^m, on identifie la section s avec un polynôme, que l'on note toujours s, de multi-degré inférieur à d. Par le théorème du produit on sait que l'ensemble $X(s)$, des zéros communs de $D^\alpha(s)$ pour tout m-uplet d'entiers $\alpha = (\alpha_1, \ldots, \alpha_m)$ tel que $0 \leq \alpha_i \leq \max_{i+1 \leq j \leq m} d_j$, est contenu dans l'union d'un nombre fini de sous-variétés produits propres. Par ailleurs, pour $k \in [\![1,M]\!]$ et $0 \leq \alpha_i \leq \max_{i+1 \leq j \leq m} d_j$, on a :

$$\mathrm{Ind}(\zeta_k, D^\alpha(s)) \geq \mathrm{Ind}(\zeta_k, s) - \sum_{i=1}^{m-1} \frac{\alpha_i}{d_i}.$$

En effet, notons y le membre de droite de l'inégalité, et soit β un m-uplet d'entiers tels que $\sum_{i=1}^{m} \frac{\beta}{d_i} \leq y - 1$. Dans ce cas, on a :

$$\sum_{i=1}^{m-1} \frac{\alpha_i + \beta_i}{d_i} + \frac{\beta_m}{d_m} \leq y - 1 + \sum_{i=1}^{m-1} \frac{\alpha_i}{d_i} = \mathrm{Ind}(\zeta_k, s) - 1,$$

Donc on a bien : $(\partial^\beta D^\alpha s)(\zeta_k) = 0$, d'où l'inégalité. De plus, par définition de δ, on a l'inégalité $\sum_{i=1}^{m-1} \frac{\alpha_i}{d_i} \leq m\delta$. En accolant les deux inégalités, on en déduit que

$$\mathrm{Ind}(\zeta_k, D^\alpha s) \geq t_k - m\delta.$$

Ainsi, si V est une sous-variété comme dans l'énoncé qui, de plus, n'est contenue dans aucune sous-variété propre de $\mathbb{P}$, alors par le théorème du produit, il existe α vérifiant les inégalités habituelles, tel que $D^\alpha(s)$ donne une section non nulle sur V. L'inégalité précédente assure de plus que cette section non nulle s_V, appartient à l'espace

$$H^0\left(V,O_P(d) \otimes \bigcap_{i=1}^{M} \mathcal{I}_{\zeta_i,d,t_i-m\delta}\right).$$

Sinon V est comme dans l'énoncé mais est incluse dans une sous-variété produit propre $\mathbb{P}'$. Il suffit de montrer que, dans le cas où $V = \mathbb{P}'$, le résultat est vrai en conservant, pour tout i l'indice t_i. En effet, en faisant une récurrence sur la dimension (car $\dim \mathbb{P}' < \dim \mathbb{P}$), et en appliquant le lemme à $\mathbb{P}'$ et à la section s' non nulle obtenue pour $\mathbb{P}'$, on en déduit le résultat dans le cas général. On suppose donc $V = \mathbb{P}'$. Dans ce cas, la proposition 3.3.4

nous donne l'existence d'une section non nulle $s_V \in H^0\left(V, O_P(n_V d) \otimes \bigcap_{i=1}^M \mathcal{I}_{\zeta_i, n_V d, t_i}\right)$, pour un n_V assez grand, ce qu'on voulait démontrer.
On montre maintenant que l'on peut trouver un entier n indépendant de V :
Il suffit pour cela de constater que l'on appelle la proposition 3.3.4 un nombre fini de fois, indépendant de V. Donc en prenant comme entier n, le produit des n_i obtenus par les différents appels de la proposition, on peut conclure. □

Le fait, que l'entier obtenu dans le lemme précédent soit indépendant de V, nous permet, quitte à travailler avec $d := nd$ dans ce qui suit, de supposer que, si $Z \not\subset Z_i$ pour tout i, alors il existe

$$0 \neq s_Z \in H^0\left(Z, O_P(d) \otimes \bigcap_{i=1}^{M} \mathcal{I}_{\zeta_i, d, t_i - m\delta}\right). \tag{3.1}$$

On va utiliser (3.1) pour construire un cycle effectif, qui représente $c_1(O_{\mathbb{P}}(d))^m$.

Construction du cycle effectif

Soit $s_{\mathbb{P}}$ une section donnée par l'équation (3.1), on note $Z(s_{\mathbb{P}})$ son schéma des zéros. Alors $[Z(s_{\mathbb{P}})]$ est un diviseur effectif représentant la classe $c_1(O_{\mathbb{P}}(d))$. Soit Z une composante irréductible de $Z(s_{\mathbb{P}})$, alors, deux cas peuvent se présenter :
Si il existe i tel que $Z \subset Z_i$, on prend $0 \neq s_Z \in H^0(Z, O_{\mathbb{P}}(d)))$, et dans ce cas, $[Z(s_Z)]$ est un cycle effectif représentant la classe $c_1(O_{\mathbb{P}}(d)) \cap Z$.
Sinon, $Z \not\subset Z_i$ pour tout $i \in [\![1,M]\!]$. Dans ce cas, l'équation (3.1) nous donne une section non nulle $s_Z \in H^0\left(Z, O_P(d) \otimes \bigcap_{i=1}^M \mathcal{I}_{\zeta_i, d, t_i - m\delta}\right)$, et, là encore, $[Z(s_Z)]$ est un cycle effectif représentant la classe $c_1(O_{\mathbb{P}}(d)) \cap Z$.
On réitère ce raisonnement de manière à obtenir ainsi un représentant effectif de la classe $c_1(O_{\mathbb{P}}(d))^m$. Par ailleurs, on sait par la proposision 3.3.2 que les supports, Z_i, sont deux à deux disjoints. On peut donc écrire :

$$c_1(O_{\mathbb{P}}(d))^m = R + \sum_{i=1}^{M} R_i, \text{ où } R_i \text{ est le cycle effectif de support inclus dans } Z_i.$$

Notamment, en passant au degré, on en déduit, par effectivité de R, que :

$$\sum_{i=1}^{M} \deg R_i = \deg\,(c_1(O_{\mathbb{P}}(d))^m) - \deg R \leq \deg\,(c_1(O_{\mathbb{P}}(d))^m).$$

Or on connait le degré de $c_1(O_{\mathbb{P}}(d))^m$. En effet, par la proposition 3.2.7, on sait que : $\deg\,(c_1(O_{\mathbb{P}}(d))^m = m! \prod_{i=1}^{m} d_i$. Pour conclure la preuve du théorème 3.3.2, il nous suffit donc de prouver le lemme :

Lemme 3.3.7. *Pour tout $i \in [\![1,M]\!]$, on a : deg $R_i \geq \left(m! \prod_{k=1}^{m} d_k\right)$ Vol$(t_i - m\delta)$.*

Minoration de deg R_i

Pour démontrer le lemme 3.3.7, on commence par prouver le résultat suivant :

Lemme 3.3.8. *Soit $i \in [\![1,M]\!]$, et soit $\pi : BL_Y(\mathbb{P}) \to \mathbb{P}$ l'éclatement de $\mathbb{P}$ le long du fermé Y défini par l'idéal $\mathcal{I}_{\zeta_i,d,t_i-m\delta}$, et de diviseur exceptionnel E. Alors :*

$$deg\ R_i \geq deg\ c_1(O_{\mathbb{P}}(d))^m - deg\ c_1(\pi^* O_{\mathbb{P}}(d)(-E))^m.$$

Démonstration : Soit $s_{\mathbb{P}}$, la section non nulle de $H^0(\mathbb{P},O_{\mathbb{P}}(d))$ utilisée dans la construction précédente. Dans ce cas, le cycle $\pi^*[Z(s_{\mathbb{P}})] - E$ est un représentant effectif de $c_1(\pi^* O_{\mathbb{P}}(d)(-E))$. En effet, par choix de $s_{\mathbb{P}}$ c'est un cycle effectif, et en remarquant que

$$c_1(\pi^* O_{\mathbb{P}}(d)(-E)) = c_1(\pi^* O_{\mathbb{P}}(d)) - c_1(O_{BL_Y(\mathbb{P})}(E)),$$

on constate qu'il représente bien la classe $c_1(\pi^* O_{\mathbb{P}}(d)(-E))$. Soit V une composante irréductible de $\pi^*[Z(s_{\mathbb{P}})] - E$, on va distinguer deux cas :

cas 1 : $\pi(V) \subset Z_i$. Comme $\mathcal{I}_{\zeta,d,t-m\delta}$ est engendré par ses sections globales, le lemme 3.1.4 nous permet d'affirmer que le faisceau $\pi^* O_{\mathbb{P}}(d)(-E)$ est engendré par ses sections globales. On peut donc choisir un représentant effectif pour $c_1(\pi^* O_{\mathbb{P}}(d)(-E)) \cap V$.

cas 2 : $\pi(V) \not\subset Z_i$. Dans ce cas, $V \not\subset E$, et l'application $\pi_{|V}$ est birationnelle. En posant $Z = \pi(V)$, on constate que V est égal à $\tilde{Z}$, la transformée stricte de Z.

Si $\exists j \neq i$ tel que $Z \subset Z_j$, soit $s_Z \in H^0(Z,O_{\mathbb{P}}(d))$ la section non nulle utilisée précédemment pour la construction du cycle effectif représentant $c_1(O_{\mathbb{P}}(d))^m$. Comme $Z_i \cap Z_j = \emptyset$, on a aussi, $\tilde{Z} \cap E = \emptyset$, et donc $\pi^* s_Z \in H^0\left(\tilde{Z},\pi^* O_{\mathbb{P}}(d)(-E)\right)$. Donc $\pi^*[Z(s_Z)]$ représente $c_1(\pi^* O_{\mathbb{P}}(d)(-E)) \cap \tilde{Z}$.

De même, si $\forall j\ Z \not\subset Z_j$, on considère la section non nulle $s_Z \in H^0(Z,O_{\mathbb{P}}(d))$ utilisée précédemment pour la construction du cycle effectif qui représente $c_1(O_{\mathbb{P}}(d))^m$. On obtient ainsi une section non nulle $\pi^* s_Z \in H^0(\tilde{Z},\pi^* O_{\mathbb{P}}(d))$. Comme la section s_Z appartient à $H^0\left(Z,O_P(d) \otimes \bigcap_{i=1}^M \mathcal{I}_{\zeta_i,d,t_i-m\delta}\right)$, le cycle $\pi^*[Z(s_Z)] - E_{|\tilde{Z}}$ est un cycle effectif représentant la classe de Chern $c_1(\pi^*(O_{\mathbb{P}}(d)(-E)) \cap \tilde{Z}$.

Finalement, en itérant ce procédé, on construit, un 0-cycle effectif, D, représentant la classe $c_1(\pi^* O_{\mathbb{P}}(d)(-E))^m$. De plus, par construction, ce 0-cycle s'écrit, $D_1 + S$, où D_1 est fabriqué en relevant les sections utilisées pour la construction de $c_1(O_{\mathbb{P}}(d)^m$, et où S est le cycle de support inclus dans Z_i. On sait que le morphisme π est propre par la proposition 3.1.7, on peut donc appliquer la formule de la projection du théorème 3.2.6. Celle-ci nous dit que, $\pi_*(D_1)$ coincïde avec $R + \sum_{\substack{j=1 \\ j\neq i}}^{M} R_j$. On a donc :

$$R + \sum_{j=1}^{M} R_j - \pi_*(D) = R_i - \pi_*(S).$$

En passant au degré (on utilise le fait que $\deg_X(\pi_*\alpha) = \deg_{BL_Y(X)}(\alpha)$), et en utilisant que $\deg D = \deg c_1(\pi^*(O_{\mathbb{P}}(d)(-E))^m$ et que $\pi_*(S)$ est effectif, on conclut. $\square$

Conclusion

On va maintenant pouvoir démontrer le lemme 3.3.7 et ainsi conclure la preuve du théorème 3.3.2. On veut montrer que :

$$\deg c_1(O_{\mathbb{P}}(d))^m - \deg c_1(\pi^* O_{\mathbb{P}}(d)(-E))^m \geq \left(m! \prod_{k=1}^{m} d_k\right) \mathrm{Vol}(t_i - m\delta).$$

Proposition 3.3.7. *On a l'égalité :*

$$(\frac{deg\ c_1(\pi^* O_{\mathbb{P}}(d)(-E))^m}{m!} = \lim_{n\to\infty} \frac{h^0\left(BL_Y(\mathbb{P}),\pi^* O_{\mathbb{P}}(nd)(-nE)\right)}{n^m}. \tag{3.2}$$

Démonstration : Le diviseur $\pi^* O_{\mathbb{P}}(d)(-E)$ est engendré par ses sections globales. En effet, le faisceau $\mathcal{I}_{\zeta,d,t_i-m\delta}$ l'est, et l'affirmation suit donc du lemme 3.1.4. En particulier on en déduit, grâce à la proposition 3.2.8, que le diviseur $\pi^* O_{\mathbb{P}}(d)(-E)$ est numériquement effectif. Donc on obtient le résultat en appliquant la version de Riemann-Roch asymptotique donnée dans le théorème 3.2.11. $\square$

On remarque ensuite que, si $L = \pi^* O_{\mathbb{P}}(nd)(-nE)$, on a :

$$H^0(\mathbb{P},\pi_*(L)) = \pi_*(L)(\mathbb{P}) = L(\pi^{-1}(\mathbb{P})) = L(BL_Y(\mathbb{P})) = H^0(BL_Y(\mathbb{P}),L).$$

Ainsi, la formule de la projection pour les faisceaux nous donne :

$$h^0\left(BL_Y(\mathbb{P}),\pi^* O_{\mathbb{P}}(nd)(-nE)\right) = h^0\left(\mathbb{P},O_{\mathbb{P}}(nd) \otimes \pi_* O_{BL_Y(\mathbb{P})}(-nE)\right). \tag{3.3}$$

D'après le point 1. de la proposition 3.1.9, E est le diviseur effectif, tel que

$$\pi^{-1}\mathcal{I}_{\zeta,d,t-m\delta} \cdot O_{BL_Y(\mathbb{P})} = O_{BL_Y(\mathbb{P})}(-E).$$

On a donc une inclusion naturelle (cf le théorème 3.1.7 et les remarques qui suivent) de $\mathcal{I}_{\zeta,d,t-m\delta}$ dans $\pi_* O_{BL_Y(\mathbb{P})}(-E)$. La même construction nous donne, pour tout $n \geq 1$, une inclusion naturelle,

$$\iota_n : \mathcal{I}_{\zeta,d,t-m\delta}^{\otimes n} \hookrightarrow \pi_* O_{BL_Y(\mathbb{P})}(-nE).$$

La proposition suivante va nous permettre de calculer le membre de droite de l'égalité (3.3) précédente pour n assez grand.

Proposition 3.3.8. *L'inclusion ι_n est un isomorphisme pour tout n assez grand.*

Démonstration : Soit $U = \text{Spec } A$ un ouvert affine de $\mathbb{P}$ tel que l'anneau A est une K-algèbre de type fini. Par construction $\pi^{-1}(U) \simeq \text{Proj } \mathcal{S}(U)$, où $\mathcal{S} = \sum_{d\geq 0} \mathcal{S}_d$, avec dans notre cas, $\mathcal{S}_d = \mathcal{I}_{\zeta,d,t}^{\otimes d}$, où $\mathcal{I}_{\zeta,d,t}$ est cohérent. L'anneau $\mathcal{S}(U) = \sum_{d\geq 0} \mathcal{S}_d(U)$ est un anneau gradué, engendré par $\mathcal{I}(U)$, comme $O_{\mathbb{P}}(U) = A-$algèbre. De plus $\mathcal{I}(U)$ est un A-module de type fini. On a finalement (cf [Har77] p.125)

$$\forall n \gg 0 \quad \mathcal{S}_n(U) \simeq \widetilde{\mathcal{S}(U)(n)}(\pi^{-1}(U)).$$

Or par définition du faisceau $O_{BL(\mathbb{P})}(n)$, on sait que

$$O_{BL(\mathbb{P})}(n)_{|\pi^{-1}(U)} \simeq O_{\text{Proj}(\mathcal{S}(U))}(n) \simeq \widetilde{\mathcal{S}(U)(n)}.$$

On en déduit que

$$\forall n \gg 0 \quad O_{BL(\mathbb{P})}(n)(\pi^{-1}(U)) \simeq \widetilde{\mathcal{S}(U)(n)}(\pi^{-1}(U)) \simeq \mathcal{S}_n(U).$$

On peut réécrire ceci sous la forme :

$$\forall n \gg 0 \quad \mathcal{I}_{\zeta,d,t}^{\otimes n}(U) \simeq (\pi_* O_{BL(\mathbb{P})}(n))(U),$$

et ce, pour tout ouvert affine $U = \text{Spec } A$ de $\mathbb{P}$ tel que A est une K-algèbre de type fini. Or $\mathbb{P}$ est de type fini sur K, donc il existe un recouvrement de $\mathbb{P}$ par de tels ouverts. Donc on sait en particulier que :

$$\forall n \gg 0 \quad \mathcal{I}_{\zeta,d,t}^{\otimes n}(\mathbb{P}) \simeq O_{BL(\mathbb{P})}(n)(BL(\mathbb{P})).$$

Or le faisceau $\mathfrak{I}_{\zeta,d,t}$ est cohérent sur l'espace projectif $\mathbb{P}$, donc par un théorème de Serre (cf [Har77] p.121), on sait que pour n assez grand, $\mathfrak{I}_{\zeta,d,t}^{\otimes n}$ est engendré par ses sections globales. Le même résultat vaut pour $O_{BL(\mathbb{P})}(1)$. Ainsi l'isomorphisme au niveau des sections globales nous donne bien l'isomorphisme de i_n pour n assez grand. □

Ainsi, en injectant la proposition dans l'égalité (3.3), puis en mettant (3.3) dans l'identité (3.2), on en déduit :

$$\frac{c_1(\pi^* O_{\mathbb{P}}(d)(-E))^m}{m!} = \lim_{n\to\infty} \frac{h^0\left(\mathbb{P}, O_{\mathbb{P}}(nd) \otimes \mathcal{I}_{\zeta_i,d,t_i-m\delta}^{\otimes n}\right)}{n^m}. \tag{3.4}$$

On veut évaluer le membre de droite de (3.4). Pour cela, on rappelle que

$$\mathcal{I}_{\zeta_i,d,t_i-m\delta}^{\otimes n} \subset \mathcal{I}_{\zeta_i,nd,t_i-m\delta}, \text{ donc,}$$

$$h^0\left(\mathbb{P}, O_{\mathbb{P}}(nd) \otimes \mathcal{I}_{\zeta_i,d,t_i-m\delta}^{\otimes n}\right) \leq h^0\left(\mathbb{P}, O_{\mathbb{P}}(nd) \otimes \mathcal{I}_{\zeta_i,nd,t_i-m\delta}\right).$$

On déduit de cette inégalité, que :

$$\lim_{n\to\infty} \frac{h^0\left(\mathbb{P}, O_{\mathbb{P}}(nd) \otimes \mathcal{I}_{\zeta_i,d,t_i-m\delta}^{\otimes n}\right)}{n^m} \leq \lim_{n\to\infty} \frac{h^0\left(\mathbb{P}, O_{\mathbb{P}}(nd) \otimes \mathcal{I}_{\zeta_i,nd,t_i-m\delta}\right)}{n^m}. \tag{3.5}$$

Enfin, en combinant les deux équations, (3.4) et (3.5), on constate que :

$$\frac{c_1(O_{\mathbb{P}}(d))^m - c_1(\pi^* O_{\mathbb{P}}(d)(-E))^m}{m!} \geq \lim_{n\to\infty} \frac{h^0(\mathbb{P},O_{\mathbb{P}}(nd)) - h^0\left(\mathbb{P},O_{\mathbb{P}}(nd)\otimes \mathcal{I}_{\zeta_i,nd,t_i-m\delta}\right)}{n^m}.$$

On conclut alors en utilisant le calcul de volume fait à la proposition 3.3.5.

3.3.5 Preuve du théorème 3.3.1

La preuve du théorème 3.3.1 est presque similaire à la preuve précédente. La seule différence est le lemme clé 3.3.6, puisque on veut fabriquer une section non nulle, sans modifier l'indice.
Le problème vient de ce que, quand on considère les dérivées de s, de manière à appliquer le théorème du produit, on fait diminuer l'indice. Pour remédier à cela, une méthode consiste à multiplier les dérivées de s par un polynôme ayant un indice suffisamment grand aux points ζ_k, $k \in [\![1,M]\!]$. Le plus simple consiste à considérer le twist de la dérivée $D^\alpha s$, par le diviseur

$$D(\alpha) = \sum_{i=1}^{M}\sum_{k=1}^{m-1} \alpha_k \pi_k^*\left(\pi_k(\zeta_i)\right).$$

En effet, $\alpha_k \pi_k^*\left(\pi_k(\zeta_i)\right)$ est le diviseur définit par le polynôme $(\eta_{k,i}X_k - \lambda_{k,i}Y_k)^{\alpha_k}$ où $(\lambda_{k,i} : \eta_{k,i})$ est la $k^{ème}$ composante de ζ_i. Donc le diviseur $\sum_{k=1}^{m-1} \alpha_k \pi_k^*\left(\pi_k(\zeta_i)\right)$, est défini par le polynôme $\prod_{k=1}^{m-1}(\eta_{k,i}X_k - \lambda_{k_i}Y_k)^{\alpha_k}$. Or,

$$\operatorname{Ind}\left(\zeta_k, \prod_{k=1}^{m-1}(\eta_{k,i}X_k - \lambda_{k_i}Y_k)^{\alpha_k} D^\alpha s\right) \geq \operatorname{Ind}\left(\zeta_k, \prod_{k=1}^{m-1}(\eta_{k,i}X_k - \lambda_{k_i}Y_k)^{\alpha_k}\right) + \operatorname{Ind}\left(\zeta_k, D^\alpha s\right).$$

Le dernier terme est d'indice supérieur à t_k en ζ_k, donc en twistant par le diviseur $D(\alpha)$ on se ramène à la situation voulue, mais on a un résultat qui n'est pas tout à fait assez fin (et qui en plus dépend de α), donc on va encore raffiner un peu.
Tout d'abord, on constate que si, dans la démonstration du lemme clé, on prend un ouvert affine K^m tel que le point ζ_1 est de coordonnées $(\infty,\ldots,\infty)$, alors l'indice en ζ_1 va rester stable par dérivation. Ensuite, on peut toujours choisir un système de coordonnées tel que, on ait de plus $\zeta_2 = (0,\ldots,0)$. Donc, quitte à travailler avec la section $\prod_{k=1}^{m-1} X_k^{\alpha_k} D^\alpha s$ (qui est bien de degré $\leq d$), on peut considérer qu'on a pas de problème non plus en ζ_2. On traite alors le cas des autres points par la méthode indiquée précédemment : on twist par le diviseur

$$D'(\alpha) = \sum_{i=3}^{M}\sum_{k=1}^{m-1} \alpha_k \pi_k^*\left(\pi_k(\zeta_i)\right).$$

On pose alors, $\delta_i = \max_{i=1\leq j\leq m} d_j$, et $L = O_{\mathbb{P}}(d)(D'(\delta))$. Par définition, tous les α_i intervenant dans le lemme clé sont inférieurs à δ_i, donc on obtient bien un résultat indépendant de la variété qui va intervenir, et on conclut par la même preuve que celle du lemme clé que, pour toute variété V telle que $\forall i\ V \not\subset Z_i$, on a :

$$H^0\left(V,L \otimes \bigcap_{i=1}^{M} \mathcal{I}_{\zeta_i,d,t_i}\right) \neq 0.$$

Le reste de la preuve est exactement pareil que ce qu'on a déjà fait. Il faut évidemment appliquer la proposition 3.3.6 au lieu de la proposition 3.3.5, et remplacer la valeur de $deg(c_1(O_{\mathbb{P}}(d))^m$ par celle de $deg(c_1(L))^m$ (le calcul se fait par exemple en utilisant la version asymptotique du théorème de Riemann-Roch).

Annexe A

Groupes formels de Lubin Tate

Sommaire

A.1 Préliminaires **83**
A.2 Groupes formels **83**
A.2.1 Définitions 83
A.2.2 Le lemme fondamental 84
A.3 L'extension totalement ramifiée K_π **86**
A.3.1 Premières propriétés 87
A.3.2 L'extension K_π/K et son groupe de Galois 88
A.4 L'extension L_π **89**
A.5 Sous-groupes de ramification **91**
A.5.1 "Rappels" 91
A.5.2 Sous-groupes de ramification 91

Exposé effectué avec Jérome Plût

A.1 Préliminaires

Soit $\mathcal{O}$ un anneau de valuation discrète de corps des fractions K, d'idéal maximal $\mathfrak{m}$, d'uniformisante π.

Proposition A.1.1. *la chaîne* $\mathcal{O} \supset \mathfrak{m} \supset \mathfrak{m}^2 \supset \dots$ *forme une base de voisinages de* 0.

Démonstration : Si v est la valuation normalisée et $|\,.\,| = q^{-v}$, $q \geq 2$, alors :
$\mathfrak{m}^n = \{x \in K / \mid x \mid < \frac{1}{q^{n-1}}\}$ ce qui conclut. □

Définition A.1.1 On appelle n^{eme} groupe d'unités supérieure le sous groupe de $\mathcal{O}^\times$, et on note

$$U_K^n := \{x \in K^* / \mid 1 - x \mid < \frac{1}{q^{n-1}}\} = 1 + \mathfrak{m}^n.$$

Remarque : la chaîne $\mathcal{O}^\times = U_K \supset U_K^1 \supset U_K^2 \supset \dots$ forme une base de voisinages de 1.

Proposition A.1.2. $\forall n \geq 1 \;\; \mathcal{O}^\times / U_K^n \simeq (\mathcal{O}/\mathfrak{m}^n)^\times$ *et* $U_K^n / U_K^{n+1} \simeq \mathcal{O}/\mathfrak{m}$.

Démonstration : i) *L'application* $\varphi \; : \; \begin{array}{l} \mathcal{O}^\times \to (\mathcal{O}/\mathfrak{m}^n)^\times \\ u \mapsto u \mod \mathfrak{m}^n \end{array}$ *est surjective et* $\ker\ \varphi = U_K^n$.

ii) *L'application* $\psi \; : \; \begin{array}{l} U_K^n \to \mathcal{O}/\mathfrak{m}^n \\ u \mapsto u \mod \mathfrak{m}^n \end{array}$ *est surjective et* $\ker\ \psi = U_K^{n+1}$. □

Proposition A.1.3. *Les applications* $\mathcal{O}_K \to \varprojlim \mathcal{O}_K/\mathfrak{m}^n$ *et* $\mathcal{O}_K^\times \to \varprojlim \mathcal{O}_K^\times / U_K^n$ *sont des isomorphismes et des homéomorphismes.*

A.2 Groupes formels

A.2.1 Définitions

Définition A.2.1 Soit A un anneau. Deux séries formelles F et G à coefficients dans A sont dites congruentes $\mod (\deg n)$ si elles coïncident pour tous les termes de degré strictement inférieur à n.

Définition A.2.2 Soit A un anneau et $F \in A[[X,Y]]$. On dit que F est une loi de groupe formel commutative sur l'anneau A, si :

$$\begin{array}{lll} (a) & F(X,F(Y,Z)) = F(F(X,Y),Z) & (\textit{associativité}) \\ (b) & F(X,Y) = F(Y,X) & (\textit{commutativité}) \\ (c) & F(X,0) = X & (\textit{élément neutre}) \\ (d) & \exists!\ G(X) \in A[[X]] \ \ F(X,G(X)) = 0 & (\textit{inverse}) \\ (e) & F(X,Y) \equiv X + Y \pmod{\deg 2} & \end{array}$$

Exemple A.2.1 Soit $A = \mathcal{O}_K$ un anneau de valuation discrète de corps de fraction K, et d'idéal maximal $\mathfrak{m}_K$. Soit F une loi de groupe formel définie sur $\mathcal{O}_K$. Alors F munit $\mathfrak{m}_K$ d'une structure de groupe commutatif. On note $\mathfrak{m}_{K,F}$ ou $\mathfrak{m}_F$ ce groupe.
Exemple A.2.2 Dans la situation de l'exemple précédent, en posant $F(X,Y) = X + Y + XY$ on retrouve la loi de groupe multiplicatif de $1 + \mathfrak{m}_K$.

Définition A.2.3 On dit que K est un corps local si K est un corps complet, valué, de corps résiduel k fini. Soit K local, $q = \mathrm{Card}(k)$ et π une uniformisante de $\mathcal{O}_K$. On pose

$$\mathcal{F}_\pi := \{f \in \mathcal{O}_K[[X]] \ / \ f(X) \equiv \pi X \pmod{\deg 2} \quad \text{et} \quad f(X) \equiv X^q \mod \pi\ \}$$

Exemple A.2.3 $f(X) = \pi X + X^q \in \mathcal{F}_\pi$
Exemple A.2.4 Si $K = \mathbb{Q}_p$, $\pi = p$ alors $f(X) = (1+X)^p - 1$ appartient à $\mathcal{F}_p$.

A.2.2 Le lemme fondamental

Définition A.2.4 Soient F et G deux lois de groupe formel, on dit que $f : F \to G$ est un morphisme, si $f \in XA[[X]]$ et si $f \circ F = G(f \times f)$. On note $\mathrm{Hom}(F,G)$ les morphismes de F dans G et $\mathrm{End}(F)$ les endomorphismes de F.
Lemme A.2.1. *fondamental* *Soient f et g dans $\mathcal{F}_\pi$, $n \in \mathbb{N}^\star$ et soit $\phi_1(X_1,\ldots,X_n)$ une forme linéaire en $X_1,\ldots,X_n$, à coefficients dans $\mathcal{O}_K$. Alors, il existe une unique $F \in \mathcal{O}_K[[X_1,\ldots,X_n]]$ telle que :*

$$F = \phi_1 \pmod{\deg 2} \tag{A.1}$$

$$f \circ F = F \circ (g \times \cdots \times g) \tag{A.2}$$

Démonstration : Pour soulager la typographie on s'autorise à écrire $X = (X_1,\ldots,X_n)$ et $g = (g\times,\ldots,\times g)$. Comme F ne doit pas contenir de terme constant, on cherche F sous la forme $F = \sum_{\nu=1}^{+\infty} H_\nu(X)$ où H_ν est homogène de degré ν. On pose $F_r(X) = \sum_{\nu=1}^{r} H_\nu(X)$.

F est solution du problème si et seulement si $\begin{cases} F_1 & = \phi_1 \\ f \circ F_r & = F_r \circ g \pmod{\deg(r+1)} \forall r \geq 1. \end{cases}$

On détermine H_ν par récurrence : pour $\nu = 1$, H_1 est uniquement déterminé et vaut ϕ_1. On suppose maintenant que $\forall \nu \in [1,r],\ \ H_\nu$ est construit et uniquement déterminé.

Construisons H_{r+1} : Ecrivons $f\circ F_r = F_r\circ g+E_{r+1} \pmod{\deg(r+2)}$ où E_{r+1} est "l'erreur" et satisfait $E_{r+1} = 0 \pmod{\deg(r+1)}$. En écrivant $f(X) = \pi X + X^2(\sum \ldots)$, on constate facilement que :

$$f \circ F_{r+1} = f \circ F_r + \pi H_{r+1} \pmod{\deg(r+2)}. \tag{A.3}$$

En effet,

$$f \circ F_{r+1} = f \circ (F_r + H_{r+1}) = f \circ F_r + \pi H_{r+1} + \pi H_{r+1}^2 \times (\sum \ldots) + 2H_{r+1} \times F_r \times (\sum \ldots).$$

Or tous les termes de H_{r+1}^2 sont de degré $2r+2 \geq r+2$ et F_r n'a pas de termes constants. Par ailleurs,

$$F_{r+1} \circ g = F_r \circ g + \pi^{r+1} H_{r+1} \pmod{\deg(r+2)}. \tag{A.4}$$

En effet :

$$F_{r+1} \circ g = F_r \circ g + H_{r+1} \circ g$$

et

$$H_{r+1} \circ g = \sum \alpha \prod_{j=1}^{n} g(X_j)^{i_j} \quad et \quad g(X_j)^{i_j} = \pi^{i_j} X_j^{i_j} + X_j^{i_j+1}(\sum \ldots),$$

donc

$$\prod_{j=1}^{n} g(X_j)^{i_j} = \pi^{r+1} \prod_{j=1}^{n} X_j^{i_j} + (\text{termes de degré} \geq r+2),$$

d'où : $H_{r+1}\circ g = \pi^{r+1} H_{r+1} \pmod{\deg(r+2)}$. Avec (3) et (4) on en déduit que nécessairement on doit poser

$$H_{r+1} = \frac{-E_{r+1}}{\pi(1-\pi^r)}.$$

L'unicité est donc acquise et pour conclure il nous reste à voir que H_{r+1} est bien à coefficients dans $\mathcal{O}_K$, c'est à dire que $E_{r+1} \equiv 0 \mod \pi$. Or f et g sont congrues à X^q $\mod \pi$, donc

$E_{r+1}(X) = f \circ F_r(X) - F_r \circ g(X) = (F_r(X))^q - F_r(X^q) \equiv 0 \mod \pi.$ □

Proposition A.2.1. ***(Tate)*** *Soit $f \in \mathcal{F}_\pi$, il existe une unique loi de groupe formel à coefficients dans $\mathcal{O}_K$, notée F_f, telle que $f \in End(F_f)$. Une telle loi de groupe formel est appelée loi de groupe formel de Lubin-Tate.*

Démonstration : Dans le lemme précédent, on prend $n = 2$, $\phi_1 = X + Y$ et $f = g$. Il suffit de voir que l'unique F_f ainsi obtenue est bien une loi de groupe formel :
associativité : On constate que $F_f(F_f(X,Y),Z)$ et $F_f(X,F_f(Y,Z))$ sont solutions de :

$$H(X,Y,Z) = X + Y + Z \pmod{\deg 2}$$
$$f \circ H = H \circ (f \times \cdots \times f)$$

Par unicité dans le lemme fondammental on en déduit l'associativité.
élément neutre : Les séries formelles $F_f(X,0)$ et X sont solutions de :

$$H(X) = X \pmod{\deg 2}$$
$$f \circ H = H \circ f$$

La commutativité et la congruence $\pmod{\deg 2}$ sont évidentes. D'où le résultat. $\square$

Désormais on travaillera uniquement avec des lois de groupes formel de Lubin-Tate.
Exemple A.2.5 Si $K = \mathbb{Q}_p$ et $f = (1+X)^p - 1$ alors $F_f = X + Y + XY$.
Proposition A.2.2. *Soit $f \in \mathcal{F}_\pi$ et soit F_f la loi de groupe correspondante. Pour tout $a \in \mathcal{O}_K$, il existe un unique $[a]_f \in \mathcal{O}_K[[X]]$ tel que : $[a]_f$ commute avec f et $[a]_f \equiv aX \pmod{\deg 2}$.*
De plus on a alors $[a]_f \in End(F_f)$.
Démonstration : On a immédiatement l'existence et l'unicité de $[a]_f$ par le lemme fondamental, comme solution de $H(T) = aT \pmod{\deg 2}$ et $f \circ H = H \circ f$. Reste à voir que c'est un endomorphisme de F_f, ce qui ce fait encore par la même méthode : On vérifie que $F_f([a]_f(X),[a]_f(Y))$ et $[a]_f(F_f(X,Y))$, sont toutes deux congrues à $aX + aY \pmod{\deg 2}$ et solutions de $f \circ H = H \circ (f \times f)$. $\square$

Remarque : Soit $f \in \mathcal{F}_\pi$, alors $[\pi]_f = f$.
Proposition A.2.3.

$$\begin{aligned} L'application\ \varphi\ :\ \mathcal{O}_K &\to End(F_f) \quad est\ un\ morphisme\ injectif\ d'anneaux. \\ a &\mapsto [a]_f \end{aligned}$$

Démonstration : On vérifie que l'on a bien un morphisme d'anneau par le même raisonnement que précédemment. L'injectivité vient de ce que $[a]_f = aX \pmod{\deg 2}$. $\square$

Définition A.2.5 On appelle $\mathcal{O}_K$ module formel de Lubin-Tate pour π la donnée d'une loi de groupe formel de Lubin-Tate et du morphisme φ précédent.

Proposition A.2.4. *Si f et g sont dans $\mathcal{F}_\pi$, alors $F_f \simeq F_g$.*
Démonstration : Pour tout $a \in A$, $f,g \in \mathcal{F}_\pi$ notons $[a]_{f,g}$ l'unique solution de $[a]_{f,g}(T) = aT \pmod{\deg 2}$ et $f([a]_{f,g}(T)) = [a]_{f,g}(g(T))$. Si a est inversible dans $\mathcal{O}_K$, en notant toujours par la même méthode que $[1]_{f,g}(T) = T$, on voit que $[a]_{f,g}$ fourni l'isomorphisme voulu. $\square$

A.3 L'extension totalement ramifiée K_π

On remarque que tout $\mathcal{O}_K$ module formel donne naissance à un (vrai) $\mathcal{O}_K$ module quand on "lit" la série F_f là où elle converge. Pour ce faire on choisit $\mathfrak{m}_s$ l'idéal maximal de K_s une clôture séparable du corps local K.

A.3.1 Premières propriétés

Proposition A.3.1. *Si F est un $\mathcal{O}_K$ module formel, alors $\mathfrak{m}_s$ est un $\mathcal{O}_K$ module pour $x + y := x +_F y$ et $a.x := [a]_F(x)$. On le note $\mathfrak{m}_{s,F}$.*

Proposition A.3.2. *Si $f : F \to G$ est un morphisme de $\mathcal{O}_K$ module formel, alors*

$$l'application\ encore\ notée\ f : \begin{array}{c} \mathfrak{m}_{s,F} \to \mathfrak{m}_{s,G} \\ x \mapsto f(x) \end{array}\ est\ un\ morphisme\ de\ \mathcal{O}_K\ module.$$

Définition A.3.1 On pose $E_\pi(n) := \{\lambda \in \mathfrak{m}_{s,F}\ /\pi^n.\lambda = 0\} = \ker([\pi^n]_F)$ le sous $\mathcal{O}_K$ module de π^n torsion de $\mathfrak{m}_{s,F}$, et on pose $E_\pi := \varinjlim E_\pi(n) = \bigcup_{n=1}^{\infty} E_\pi(n)$.

Remarquons que $E_\pi(n)$ est aussi un $\mathcal{O}_K/\pi^n\mathcal{O}_K$ module, car tous ses éléments sont tués par $\pi^n\mathcal{O}_K$.

Lemme A.3.1. *Soit M un $\mathcal{O}_K$ module et soit $M_n = \ker(\pi^n : M \to M)$. Si $\pi : M \to M$ est surjective, et si M_1 de cardinal q, alors : M_n est de cardinal q^n.*

Démonstration : On démontre le résultat par récurrence sur n. Le cas $n = 1$ découle des hypothèses. Supposons le résultat vrai au rang $n-1$. Considérons la suite :

$$0 \to M_1 \to M_n \xrightarrow{\pi} M_{n-1} \to 0.$$

π surjective nous donne l'exactitude en M_{n-1} et de ce fait l'exactitude de la suite. Ainsi M_n à q^n éléments. □

Théorème A.3.1. *Le $\mathcal{O}_K/\pi^n\mathcal{O}_K$ module $E_\pi(n)$ est libre de rang 1.*

Démonstration : Par la proposition 2.4, on est libre de choisir $f \in \mathcal{F}_\pi$ comme on veut pour définir $F_f = F$. On prend donc $f = \pi X + X^q = [\pi]_F(X)$. Le polynome f est séparable donc $E(1) = \ker[\pi]_F$ a exactement q éléments, car toutes les racines de f sont de valuation strictement positives. En effet, si x est une solution, soit $x = 0$ et donc $v(x) = +\infty$, soit $v(x) = \frac{1}{q-1} > 0$. De plus $E_\pi(n) = \ker[\pi^n]_F$, donc pour pouvoir appliquer le lemme précédent, avec $M = \mathfrak{m}_{s,F}$, il suffit de voir que $[\pi]_F$ est surjective de M dans M. Soit $y \in M$ et soit x une solution de $\pi x + x^q = y$ dans K_s, alors :
si $v(x) + 1 = qv(x)$, on a $x \in M$. Sinon, $0 < v(y) = inf(v(x)+1, qv(x)) \leq qv(x)$, donc $x \in M$. Il reste à voir que l'on peut trouver une racine de $P(X) = \pi X + X^q - y$ dans K_s. Si P est séparable, on a gagné, sinon P et P' ont une racine commune x dans une clôture algébrique de K. Comme $P' = \pi + qX^{q-1}$, on a alors $P(x) = x(\pi - \frac{\pi}{q}) - y = 0$, soit $x = y\frac{q}{(q-1)\pi}$ donc x est séparable, ce qui conclut.
Le lemme précédent nous dit que $E_\pi(n)$ est de cardinal q^n. Soit $\lambda_n \in E_\pi(n) - E(n-1)$, le morphisme $\mathcal{O}_K \to E_\pi(n)$ de multiplication par λ_n est un morphisme de $\mathcal{O}_K$ module de noyau (π^n), d'où le résultat par cardinalité. □

Corollaire A.3.1. *Le module E_π est isomorphe à $K/\mathcal{O}_K$.*

Démonstration : Le résultat suit du théorème en passant à la limite inductive. □

Corollaire A.3.2. *L'application $a \mapsto [a]_F$ donne les isomorphismes suivant :*

$$\mathcal{O}_K / \pi^n \mathcal{O}_K \simeq End_{\mathcal{O}_K}(E_\pi(n)) \text{ et } U_K / U_K^n \simeq Aut_{\mathcal{O}_K}(E_\pi(n)).$$

Démonstration : Le corollaire découle facilement de la proposition 1.2 et du théorème. □

A.3.2 L'extension K_π/K et son groupe de Galois

Définition A.3.2 Le corps $K_\pi(n) := K(E_\pi(n))$ est appelé une extension de Lubin-Tate. On pose $K_\pi := \varinjlim K_\pi(n) = \bigcup_{n=1}^{\infty} K_\pi(n)$. $K_\pi(n)$ et K_π ne dépendent que de π et pas de F.

Théorème A.3.2. *1. L'extension $K_\pi(n)/K$ est abélienne, totalement ramifiée, de degré $q^{n-1}(q-1)$, de groupe de Galois* $\mathrm{Gal}(K_\pi(n)/K) \simeq U_K / U_K^n$.
2. Si $\lambda_n \in E_\pi(n) - E(n-1)$, alors $K_\pi(n) = K[\lambda_n]$ et λ_n est une uniformisante.
3. $N_{K_\pi(n) \quad K}(-\lambda_n) = \pi$.

Démonstration : Comme précédemment on choisit $f = \pi X + X^q$, et en notant f^n la n^{ieme} itérée de f, on pose $\phi_n(X) := \frac{f^n(X)}{f^{n-1}(X)}$. Le polynome ϕ_n est d'Eisenstein et de degré $q^{n-1}(q-1)$, donc l'extension $K(\lambda_n)/K$ est totalement ramifiée de degré $q^{n-1}(q-1)$, et λ_n est une uniformisante. Comme $\phi_n(\lambda_n) = 0$, et que ϕ_n est unitaire de coefficient constant π on a aussi $N_{K_\pi(n) \quad K}(-\lambda_n) = \pi$.
On sait que $K(\lambda_n) \subset K_\pi(n)$. De plus $\forall \sigma \in \mathrm{Gal}(K_\pi(n)/K)$, on a, $\sigma_{|E_\pi(n)} \in Aut_{\mathcal{O}_K}(E_\pi(n))$. On peut donc considérer l'application

$$\begin{aligned} \varphi \ : \ \mathrm{Gal}(K_\pi(n)/K) &\to Aut_{\mathcal{O}_K}(E_\pi(n)) \\ \sigma &\mapsto \sigma_{|E_\pi(n)} \end{aligned}$$

Elle est injective car $K_\pi(n)$ est engendré par $E_\pi(n)$. Or

$$\mathrm{Card}(\mathrm{Gal}(K_\pi(n)/K)) \ \geq \ [K(\lambda_n) : K] \ = \ \mathrm{Card}(U_K / U_K^n).$$

Donc φ est bijective et l'extension est abélienne. Enfin $[K_\pi(n) : K] = [K(\lambda_n) : K]$ donc $K_\pi(n) = K(\lambda_n)$. □

Corollaire A.3.3. *L'extension K_π/K est totalement ramifiée de groupe de Galois*

$$Gal(K_\pi/K) \simeq \mathcal{O}^\times.$$

Démonstration : Par définition, $\mathrm{Gal}(K_\pi/K) = \varprojlim \mathrm{Gal}(E_\pi(n)/K)$, et par les préliminaires on sait que $\mathcal{O}^\times$ est isomorphe à $\varprojlim U_K / U_K^n$. □

Exemple A.3.1 Si $K = \mathbb{Q}_p$, $\pi = p$, $f = (1+X)^p - 1$ alors $E_\pi = \{racines\ p^{\nu\ ieme}\ de\ 1\ \ /\nu \in \mathbb{N}\ \}$ et $K_\pi = \mathbb{Q}_{p^\infty}$.

A.4 L'extension L_π

Soit K un corps local ; on note $A = \mathcal{O}_K$ son anneau de valuation. On fixe une clôture séparable K^{sep} de K. Soit K^{nr} l'extension maximale non ramifiée de K dans K^{sep} ; son corps résiduel est une clôture algébrique k^{alg} de k, d'où

$$\mathrm{Gal}\,(K^{\mathrm{nr}}/K) \;=\; \widehat{\mathbf{Z}}.$$

Soit π une uniformisante de K.

Définition A.4.1 On appelle L_π l'extension composée dans K^{sep} de K^{nr} et K_π.

On remarque que les extensions K^{nr} et K_π sont linéairement disjointes.

Soient π et ω deux uniformisantes de K, avec $\omega = u\pi$, $u \in A^\star$; on choisit également $f \in \mathcal{F}_\pi$ et $g \in \mathcal{F}_\omega$. On note σ l'automorphisme de Frobenius de $\mathrm{Gal}\,(K^{\mathrm{nr}}/K)$. Soit également B l'anneau de valuation de $\widehat{K^{\mathrm{nr}}}$.

Proposition A.4.1. *Il existe une unité ε de B telle que $\sigma\varepsilon = \varepsilon u$, et une série entière $\varphi \in B[[X]]$, telles que :*

(i) $\varphi(X) = \varepsilon X \pmod{X^2}$;

(ii) ${}^\sigma\varphi = \varphi \circ [u]_f$;

(iii) $\varphi \circ F_f = F_g(\varphi \times \varphi)$;

(iv) Pour tout $a \in A$, $\varphi \circ [a]_f = [a]_g \circ \varphi$.

Lemme A.4.1. *On a deux suites exactes :*

$$0 \longrightarrow A \longrightarrow B \xrightarrow{\sigma - \mathrm{id}} B \longrightarrow 0$$

$$1 \longrightarrow A^\star \longrightarrow B^\star \xrightarrow{\sigma/\,\mathrm{id}} B^\star \longrightarrow 1$$

Soient R l'anneau de valuation de K^{nr}, et $\mathfrak{m}_R$ son idéal maximal. Montrons par récurrence que, pour tout n, la suite ($\star$) $0 \to A/\mathfrak{m}^n \to R/\mathfrak{m}_R^n \xrightarrow{\sigma-1} R/\mathfrak{m}_R^n \to 0$ est exacte : pour $n = 1$, la suite s'écrit

$$0 \longrightarrow k \longrightarrow k^{\mathrm{alg}} \xrightarrow{x \mapsto x^q - x} k^{\mathrm{alg}} \longrightarrow 0$$

et est donc exacte. Pour n quelconque, écrivons :

$$\begin{array}{ccccccccc}
0 & \longrightarrow & R/\mathfrak{m}_R^n & \longrightarrow & R/\mathfrak{m}_R^{n+1} & \longrightarrow & R/\mathfrak{m}_R & \longrightarrow 0 \\
 & & \downarrow \sigma - 1 & & \downarrow \sigma - 1 & & \downarrow \sigma - 1 & \\
0 & \longrightarrow & R/\mathfrak{m}_R^n & \longrightarrow & R/\mathfrak{m}_R^{n+1} & \longrightarrow & R/\mathfrak{m}_R & \longrightarrow 0
\end{array}$$

Le lemme du serpent montre que le noyau de $\sigma - 1 : R/\mathfrak{m}_R^{n+1} \to R/\mathfrak{m}_R^{n+1}$ a q^{n+1} éléments ; or il contient $A/\mathfrak{m}_R^{n+1}$, ce qui montre l'exactitude de la suite ($\star$), puis, par passage à la limite, celle de la suite

$$0 \longrightarrow A \longrightarrow B \xrightarrow{\sigma-1} B \longrightarrow 0.\square$$

Lemme A.4.2. *Il existe $\varphi \in B[[X]]$ vérifiant (i) et (ii).*

D'après le lemme précédent, il existe $\varepsilon \in B^\star$ tel que $\sigma\varepsilon = u\varepsilon$. On va construire une suite d'éléments de B, (b_r) tels que, pour $\varphi_r(X) = \varepsilon X + b_2X^2 + \cdots + b_rX^r$, on ait :

$$\sigma\varphi_r = \varphi_r \circ [u]_f \qquad (\text{mod } X^{r+1}).$$

Pour $r = 1$, ceci est vrai par choix de ε. Supposons $b_1, \ldots, b_r$ construits ; soient c le coefficient de X^{r+1} dans $\varphi^r \circ [u]_f - \sigma\varphi_r$, et a un élément de B tel que $\sigma a - a = c/(\varepsilon u)^{r+1}$; le lecteur vérifiera qu'alors $b_{r+1} = a\varepsilon^{r+1}$ convient. $\varphi(X) = \varepsilon X + b_2X^2 + \cdots + b_rX^r + \cdots$ vérifie alors (i) et (ii). $\square$

On note h^{-1} l'inverse d'une série entière h pour la composition.

Lemme A.4.3. *On peut choisir φ dans le lemme A.4.2 telle que $g = {}^\sigma\varphi \circ f \circ \varphi^{-1}$.*

On pose $h = \sigma\varphi \circ f \circ \varphi^{-1}$; alors :

$$h \;=\; \varphi \circ [u]_f \circ f \circ \varphi^{-1} \;=\; \varphi \circ f \circ [u]_h \circ \varphi^{-1}.$$

f et $[u]_f$ étant à coefficients dans A, il vient :

$${}^\sigma h \;=\; {}^\sigma\varphi \circ f \circ [u]_f \circ {}^\sigma\varphi^{-1} \;=\; {}^\sigma\varphi \circ f \circ \varphi^{-1} \;=\; h,$$

d'où $h \in A[[X]]$. On vérifie que $h \in \mathcal{F}_\rho$ pour $\rho = (\sigma\varepsilon/\varepsilon)\pi$. Soit alors $\tilde{\varphi} = [1]_{g,h} \circ \varphi$; alors $\tilde{\varphi}$ vérifie toujours (i) et (ii), et on a ${}^\sigma\tilde{\varphi} \circ f \circ {}^\sigma\tilde{\varphi} = g$. $\square$

Soit φ une telle série entière. On vérifie, en utilisant le lemme fondamental A.2.1, que

$$\varphi \circ F_f \circ \left(\varphi^{-1} \times \varphi^{-1}\right) = F_g \quad \text{et} \quad \varphi \circ [a]_f \circ \varphi^{-1} = [a]_g,$$

ce qui achève la preuve de la proposition A.4.1. $\square$

Lemme A.4.4. *Tout sous-corps E de K^{sep} contenant K est fermé.*

Le groupe de Galois de K^{sep} sur E fixe en effet E, et donc son adhérence ; celle-ci est donc égale à E. $\square$

Proposition A.4.2. *Les deux extensions L_π et L_ω sont égales.*

On a, d'après la proposition précédente : ${}^\sigma\varphi \circ [\pi]_f = [\omega]_g \circ \varphi$. On en déduit que φ est un isomorphisme entre $E_\pi(n)$ et $E_\omega(n)$, et donc que les deux extensions $K_\pi\widehat{K^{\mathrm{nr}}}$ et $K_\omega\widehat{K^{\mathrm{nr}}}$ coïncident. Le lemme A.4.4 précédent prouve alors que :

$$L_\pi \;=\; \widehat{K^{\mathrm{nr}}}K_\pi \cap K^{\mathrm{sep}} \;=\; \widehat{K^{\mathrm{nr}}}K_\omega \cap K^{\mathrm{sep}} \;=\; L_\omega.\square$$

Définition A.4.2 Soit $r_\pi : K^\star \to \mathrm{Gal}\,(L_\pi/K) = \mathrm{Gal}\,(K_\pi/K) \times \mathrm{Gal}\,(K^{\mathrm{nr}}/K)$ l'homomorphisme de groupes défini par :

(i) $r_\pi(\pi)$ induit l'identité sur K_π et l'automorphisme de Frobenius sur K^{nr} ;

(ii) Si $u \in A^\star$, alors $r_\pi(u)$ induit l'identité sur K^{nr}, et $[u^{-1}]_f$ sur K_π.

Proposition A.4.3. *L'homomorphisme r_π ne dépend pas du choix de l'uniformisante π.*

Soient π et $\omega = \pi u$ deux uniformisantes, $f \in \mathcal{F}_\pi$, $g \in \mathcal{F}_\omega$, et φ une application donnée par la proposition A.4.1. On va montrer que $r_\pi(\omega) = r_\omega(\omega)$; ceci montrera que les r_π coïncident sur les uniformisantes de K, ce qui suffit puisque celles-ci engendrent le groupe multiplicatif de K.

Par définition de r_π et r_ω, sur K^{nr}, $r_\pi(\omega)$ et $r_\omega(\omega)$ induisent toutes deux l'isomorphisme de Frobenius ; en outre, $r_\omega(\omega)$ induit l'identité sur K_ω. Il suffit donc pour arriver au résultat de montrer que $s = r_\pi(\omega)$ induit l'identité sur K_ω.

Puisque $s = r_\pi(\pi) \cdot r_\pi(u)$ et φ a ses coefficients dans $\widehat{K^{\mathrm{nr}}}$, il vient ${}^s\varphi = {}^\sigma\varphi = \varphi \circ [u]_f$. Soient $\lambda \in E_g$ et $\mu = \varphi^{-1}(\lambda) \in E_f$. Alors :

$$\begin{aligned} s(\lambda) &= {}^s\varphi(s(\mu)) \\ &= \left(\varphi \circ [u]_f \circ \left[u^{-1}\right]_f\right)(\mu) \\ &= \lambda. \end{aligned}$$

Ceci montre que $r_\pi(\pi)$ induit l'identité sur K_ω, d'où le résultat. □

A.5 Sous-groupes de ramification

A.5.1 "Rappels"

Soient L/K une extension galoisienne de corps locaux, de groupe de Galois G, et x un générateur de la $\mathcal{O}_K$-algèbre $\mathcal{O}_L$.

Pour u réel, on note G_u le sous-groupe de G

$$G_u = \{s \in G, v_L(sx - x) \geq u + 1\}.$$

On définit la numérotation supérieure de ces groupes par : $G^v = G_{\varphi^{-1}(V)}$, où φ est l'application continue, affine par morceaux, telle que $\varphi(0) = 0$ et $\varphi'(u) = (G_0 : G_u)^{-1}$ pour u non entier.

On a alors, pour tout sous-groupe distingué H de G :

$$G^v/H = (G/H)^v.$$

A.5.2 Sous-groupes de ramification

Soit, pour n entier, U_K^n le sous-groupe de $U_K = \mathcal{O}_K^\star$ défini par $U_K^n = 1 + \mathfrak{m}_K^n$; pour v réel, on pose $U_K^v = U_K^{\lceil v \rceil}$.

Théorème A.5.1. *On considère l'extension $K_\pi(n)/K$ précédemment construite, et l'homomorphisme*

$$r_{K_\pi(n)} : \left\{ \begin{array}{ccc} K^\star & \longrightarrow & \mathrm{Gal}\,(K_\pi(n)/K) \\ u & \longmapsto & \left[u^{-1}\right]_f \end{array} \right.$$

Alors, pour tout v réel : $r_{K_\pi(n)}^{-1}(G^v) = U_K^v$.

Soient $i \leq n$, $u \in U_K^i \smallsetminus U_K^{i+1}$, et α une racine primitive n-ième, c'est-à-dire, α tel que $[\pi^n]_f(\alpha) = 0$ et $[\pi^{n-1}]_f(\alpha) \neq 0$. Alors : $s(\alpha) = [u^{-1}]_f(\alpha)$. Soit $v \in \mathcal{O}_K$ telle que $u^{-1} = 1 + \pi^i v$; alors v est une unité de $\mathcal{O}_K$, et

$$s(\alpha) \;=\; \big[1 + \pi^i v\big]_f(\alpha) \;=\; F_f(\alpha,\beta) \qquad \text{pour } \beta = \big[\pi^i v\big]_f(\alpha),$$

d'où :

$$s(\alpha) - \alpha \;=\; \beta + \sum_{i,j>1} \gamma_{i,j}\alpha^i\beta^j, \qquad \text{pour des } \gamma_{ij} \in \mathcal{O}_L,$$

et finalement, α étant une uniformisante de $K_\pi(n)$ et β une uniformisante de $K_\pi(n-i)$, il vient

$$v_{K_\pi(n)}(s\alpha - \alpha) = [K_\pi(n) : K_\pi(n-i)] = q^i,$$

d'où : si $q^{i-1} < u \leq q^i - 1$, $r^{-1}(G_u) = U_K^i$, puis si $i - 1 < v \leq i$, $r^{-1}(G^v) = U_K^v$. □

Corollaire A.5.1. *Soient $L = K^{nr}K_\pi$, et $r : K^\star \to G = \mathrm{Gal}\,(L/K)$ l'application précédemment construite. Alors $r^{-1}(G^v) = U_K^v$.*

On obtient directement le résultat pour K_π en passant à la limite projective ; le résultat pour L s'obtient alors en remarquant que, en écrivant
$\mathrm{Gal}\,(L/K) = \mathrm{Gal}\,(K^{\mathrm{nr}}/K) \times \mathrm{Gal}\,(K_\pi/K)$, on a $r(U_K) \subset \mathrm{Gal}\,(K_\pi/K)$. □

Corollaire A.5.2 (Hasse-Arf). *Soit E une sous-extension de L ; alors les sauts dans la filtration (G^v) apparaissent seulement pour les valeurs entières de v.*

Annexe B

Mémoire de maitrise : Théorie de Galois différentielle

Sommaire

B.1 Introduction **94**
B.2 Préliminaires **94**
B.2.1 Dérivations et corps différentiels 94
B.2.2 Le groupe de Galois différentiel 96
B.3 Strucure algébrique du groupe de Galois différentiel **96**
B.3.1 La topologie de Zariski 96
B.3.2 Deux lemmes algébriques 97
B.3.3 La structure algébrique de $Gal_\partial(M/K)$ 98
B.4 Outils d'algèbre différentielle **100**
B.4.1 Extension d'idéaux premiers 100
B.4.2 Un lemme sur les anneaux de polynômes 101
B.4.3 Les isomorphismes admissibles 102
B.5 Le coeur de la théorie **103**
B.5.1 Préliminaires et compléments 103
B.5.2 Normalité de l'extension de Picard-Vessiot 104
B.5.3 Complétion de la théorie de Galois différentielle 105
B.6 Résolution par quadrature des équations différentielles linéaires **106**
B.6.1 Étude des extensions de Liouville 107
B.6.2 Deux lemmes sur les groupes algébriques linéaires 108
B.6.3 Trigonalisation simultanée d'automorphismes 109
B.6.4 Démonstration du théorème VI.1 110
B.6.5 Application à l'équation de Riccati 112

Mémoire de maitrise effectué avec Denis Conduché

B.1 Introduction

Depuis Galois, nous savons qu'il existe une correspondance entre les les sous-corps du corps de décomposition M d'une équation algébrique sur un corps K, et les sous-groupes du groupe des K-automorphismes de M. Ritt et Kolchin ont développé, à partir des idées de Picard et Vessiot, une théorie similaire en considérant l'extension attachée à une équation différentielle linéaire. Le but de cet exposé est d'expliciter et de démontrer cette correspondance. Ceci nous permettra de plus de voir sous quelles conditions une équation différentielle linéaire est résoluble par quadratures.
Dans ce qui suit, les anneaux et les corps seront toujours supposés commutatifs.

B.2 Préliminaires

B.2.1 Dérivations et corps différentiels

Définition B.2.1 Soit A un anneau intègre, une application $\partial : A \longrightarrow A$ est une *dérivation* si :
$\forall a,b \in A\ \partial(a+b) = \partial(a) + \partial(b)$ et $\forall a,b \in A\ \partial(ab) = a\partial(b) + \partial(a)b$.
Le couple (A,∂) est appelé *anneau différentiel*, et tout x de A vérifiant $\partial(x) = 0$ est *une constante*.

Théorème B.2.1. *(i) Une dérivation ∂ sur un anneau intègre A admet une unique extension au corps des fractions K de A.*

(ii) L'ensemble des constantes sur K est un sous-corps de K.

Démonstration : L'unicité est claire, car $aa^{-1} = 1$ implique $\partial(a^{-1}) = -a^{-1}\partial(a)a^{-1}$. En posant
$\partial(\frac{a}{b}) = \frac{\partial(a)b - a\partial(b)}{b^2}$ on définit bien une dérivation sur K : la définition est valide car $\forall c \in K$ $\partial(\frac{a}{b}) = \partial(\frac{ac}{bc})$.
La seconde assertion est immédiate. □

Exemple B.2.1

(i) La *dérivation triviale* : $\forall x \in K\ \partial(x) = 0$.
Celle-ci est certes peu intéressante mais on remarque que c'est l'unique possible sur $\mathbb{Q}$. Par ailleurs, tout corps peut être muni de la dérivation triviale : en ce sens la théorie des corps différentiels est une généralisation de la théorie classique.

(ii) Soit (A,∂) un anneau différentiel, notons $A[x_i]$ l'anneau des polynômes en une infinité de variables $(x_i)_{i\in\mathbb{N}}$. On peut prolonger ∂ en une dérivation sur $A[x_i]$, qui sera déterminée de manière unique par : $\partial x_i = x_{i+1}$. On a ainsi fabriqué *une indéterminée différentielle* et on note $A\{x\}$ l'anneau différentiel obtenu, ainsi que $A{<}x{>}$ son corps des fractions (la dérivation s'y étendant de manière unique par la proposition II.1). Plus généralement, si K et L sont deux corps différentiels tels que $K \subset (L,\partial)$, et S un sous ensemble de L, on note $K < S >$ le plus petit sous-corps différentiel de L contenant K et S.

Définition B.2.2

(i) Soient (K_1,∂_1), et (K_2,∂_2), deux corps différentiels. Une application $\varphi \ : \ K_1 \longrightarrow K_2$ est un *morphisme différentiel* si φ est un morphisme de corps et $\varphi \circ \partial_1 = \partial_2 \circ \varphi$. On définit de même *isomorphisme différentiel et automorphisme différentiel.*

(ii) (M,∂_1) est une *extension différentielle* de (K,∂) si M est un surcorps de K et si $\partial_{1_{|K}} = \partial$. On notera C le corps des constantes de K et C_M celui de M.

On pourrait en fait montrer que toute K-extension peut être munie d'une structure différentielle compatible avec K (on peut trouver une démonstration dans [Ros68]).

Définition B.2.3 Soit $y_1,...,y_n \in K$ corps différentiel, on appelle *matrice Wronskienne de* $(y_1,...,y_n)$ et on note $Wr(y_1,...,y_n)$ la matrice carré de d'ordre n $(\partial^{i-1}y_j)_{i,j\leq n}$.

Lemme B.2.1. *Soit* (K,∂) *un corps différentiel et* $y_1,\ldots,y_n \in K$. *On a :* $y_1,\ldots,y_n$ *sont linéairement indépendants sur* C *si et seulement si le wronskien* $|Wr(y_1,\ldots,y_n)| \neq 0$.

On déduit de ce lemme qu'une équation différentielle linéaire de degré n a au plus n solutions linéairement indépendantes dans une extension différentielle.

Définition B.2.4 Soit (K,∂) un corps différentiel et $\mathcal{L}(y) = \sum_{i=0}^{n-1} a_i\partial^i y + \partial^n y = 0$ une équation différentielle linéaire homogène, avec pour tout i, a_i dans K.
Si (M,∂_1) est une extension différentielle de K, telle que $C_M = C$ et $M = K{<}u_1,\ldots,u_n{>}$ où les u_i sont n solutions indépendantes de $\mathcal{L}(y) = 0$ (*), alors M est appelée *extension de Picard Vessiot* de K associée à (*).

Remarquons dès à présent, certaine similitude entre la théorie de Galois classique et la théorie de Galois différentielle : dans la théorie classique, à une équation algébrique on associe son corps de décomposition, ici à une équation différentielle linéaire on associe son extension de Picard Vessiot. On indique, à titre culturel, le résultat suivant démontré dans [Kol48] :

Théorème B.2.2. *Si K est de caractéristique 0 et C algébriquement clos, l'extension de Picard-Vessiot de K associée à (*) existe et est unique à isomorphisme différentiel près.*

B.2.2 Le groupe de Galois différentiel

Définition B.2.5

(i) Soit (M,∂) l'extension de Picard Vessiot de (*). *Le groupe de Galois différentiel de (*)*, (ou de (M/K)) est l'ensemble des K-automorphismes différentiels de M. On le note $Gal_\partial(M/K)$.

(ii) Soit L une sous K-extension de M, posons

$$\check{L} := \{\varphi \in Gal_\partial(M/K) \ / \ \varphi(a){=}a \ \forall a \in L\} = Gal_\partial(M/L),$$

et pour $H \subset Gal_\partial(M/K) = G$, posons $\check{H} := \{a \in M \ / \ \varphi(a){=}a \ \forall \varphi \in H\} = M^H$.

Lemme B.2.2. *$\check{L}$ est un sous-groupe de G et $\check{H}$ est un sous-corps différentiel de M. De plus $\check{\check{\check{L}}} = \check{L}$, et $\check{\check{\check{H}}} = \check{H}$.*

Définition B.2.6 Les sous K-extensions L de M (respectivement les sous-groupes H de $Gal_\partial(M/K)$) sont dits *fermés* si $\check{\check{L}} = L$, (respectivement si $\check{\check{H}} = H$).

Malheureusement ceci laisse complètement de côté un point véritablement important : quel corps ou sous-groupe est fermé ? Afin de pouvoir poursuivre notre étude, et notamment pouvoir répondre à cette question, nous devons maintenant introduire de nouveaux outils.

B.3 Strucure algébrique du groupe de Galois différentiel

B.3.1 La topologie de Zariski

Définition B.3.1 Soit C un corps et $n \in \mathbb{N}$, un ensemble $F \in C^n$ est *Zariski fermé* (ou Z-fermé) si : $\exists S \subset C[X_1, \ldots, X_n]$ tel que $F = \bigcap_{f\in S} f^{-1}(0)$.

Remarquons immédiatement que :

$$\bigcap_{f\in S} f^{-1}(0) = \bigcap_{f\in <S>} f^{-1}(0) \text{ , où } <S> \text{ est l'idéal engendré par S .}$$

De plus, $C[X_1, \ldots, X_n]$ étant noethérien, on se ramène au cas où S est fini.

Définition B.3.2 On dit qu'un espace topologique vérifie *la condition de la chaîne descendante*, si :

si $F_1 \supset F_2 \supset F_3 \supset \ldots$ est une suite décroissante de fermés, alors on $F_n = F_{n+1}$ pour tout n assez grand.

Théorème B.3.1. *Les ensembles Zariski fermés définissent une topologie sur C^n. On l'appelle la topologie de Zariski sur C^n. De plus, muni de cette topologie, C^n vérifie la condition de la chaîne descendante.*

Corollaire B.3.1. *Toute partie de C^n muni de la topologie de Zariski est l'union disjointe d'un nombre fini d'ouverts fermés connexes (pour la topologie induite).*
Démonstration : Le résultat découle facilement de la propriété de la chaine descendante. □

Exemple B.3.1
(i) Si $n = 1$ les ensembles Zariski fermés sont : C, l'ensemble vide et les ensembles finis.
(ii) Si on considère $GL_n(C)$ comme sous ensemble de C^{n^2+1}, c'est- à-dire, $GL_n(C) = \{(A,a) \in C^{n^2+1} \ / \ a.det(A) = 1\}$, alors $GL_n(C)$ est Z-fermé dans C^{n^2+1}. De plus la multiplication et l'inverse sont continus.

Définition B.3.3 On dit qu'un sous-groupe G de $GL_n(C)$, en tant que sous ensemble de C^{n^2+1}, est un *groupe algébrique linéaire* s'il est fermé pour la topologie de Zariski.

Lemme B.3.1. *Si G est un sous-groupe de $GL_n(C)$ (muni de la topologie de Zariski) et H un sous-groupe Z-fermé de G, alors le normalisateur de H, $N_G(H)$, est Z-fermé.*
Démonstration : Soit $h \in H$ et $\varphi : G \to G$, $a \mapsto aha^{-1}$. $\varphi^{-1}(H)$ est fermé car φ est continue et H est fermé. Ainsi $\bigcap \varphi^{-1}(H)$ est fermée et de même l'ensemble $\{a \ / \ a^{-1}Ha \subset H\}$ est fermé, d'où le résultat. □

B.3.2 Deux lemmes algébriques

Lemme B.3.2. *Soit K un corps différentiel de corps des constantes C algébriquement clos et L une extension différentielle de K, de corps des constantes C_L.*
(i) soient $(f_\alpha)_{\alpha \in I}$ (I ensemble quelconque) et g des polynômes à n indéterminées sur K, alors : si $\forall \alpha \in I \ f_\alpha = 0$ et $g \neq 0$ a une solution dans C_L, il existe déjà une solution dans C.
(ii) Soit $k_1, \ldots, k_r \in C_L$, alors, si $(k_1, \ldots, k_r)$ sont algébriquement dépendants sur K, ils le sont déjà sur C.

Démonstration : Soit (u_β) une base de K sur C, $f_\alpha = \sum h_{\alpha\beta} u_\beta$ où les $h_{\alpha\beta} \in C[X_1, \ldots, X_n]$ sont uniques. Grace au wronskien, on constate que les (u_β) restent linéairement indépendants sur C_L, donc si $x \in C_L$ est tel que $\forall \alpha \ f_\alpha(x) = 0$, alors $\forall \alpha,\beta \ h_{\alpha\beta}(x) = 0$. Posons alors J l'idéal engendré par les $(h_{\alpha\beta})$, $J \neq C[X_1,..,X_n]$, donc le théorème des zéros de Hilbert (cf [Lan93]) appliqué à J nous indique que les $h_{\alpha\beta}$ s'annulent déja sur C.
Ecrivons $g = \sum t_\gamma u_\gamma$ avec $t_\gamma \in C[X_1, \ldots, X_n]$ et supposons par l'absurde que :

$$h_{\alpha\beta}(x) = 0 \Rightarrow g(x) = 0 \ sur \ C \ . \ Dans \ ce \ cas, \ \forall \gamma \ t_\gamma(x) = 0$$

donc le théorème des zéros de Hilbert nous dit que : si I est l'idéal engendré par les $(h_{\alpha\beta})$, alors $t_\gamma^{r_\gamma} \in I$ avec (r_γ) une suite d'entiers : toute solution du système dans C_L annule g, contradiction.

Pour la seconde partie : si f est telle que $f(k_1,\dots,k_r) = 0$ sur K, alors $f = \sum h_\beta u_\beta$, donc par l'argument précédent : $\forall \beta\ h_\beta(k_1,\dots,k_r) = 0$, d'où le résultat. □

On notera dans la suite $deg_{tr}(I/K) = n$ le degré de transcendance de I sur le corps K. On trouvera la définition et les propriétés élémentaires dans [Lan93].

Lemme B.3.3. *Soit K un corps et I un anneau intègre contenant K, de degré de transcendance n fini sur K, et soit P un idéal propre premier de I, alors le degré de transcendance de I/P sur K est strictement inferieur à celui de I sur K.*

Démonstration : $deg_{tr}(I/K) = n$. Soit u dans P, non dans K. u n'est pas algébrique sur K, car sinon u est inversible (I integre donc le terme constant de $Pm_K(u)$ est non nul). On complète u en une base de transcendance $(u = u_1,\dots,u_n)$ sur I. La surjection canonique $\pi : I \to I/P$ est un homomorphisme d'algèbre qui induit une application de $K[u_1,...,u_n][X]$ dans $K[\pi(u_2),...,\pi(u_n)][X]$. Pour $y \in I$, π envoie un polynôme anulateur de y sur un polynôme anulateur de $\pi(y)$. Donc I/P algébrique sur $K[\pi(u_2),...,\pi(u_n)]$, donc $deg_{tr}(I/P) \leq n-1$. □

B.3.3 La structure algébrique de $Gal_\partial(M/K)$

Définition B.3.4 Soient M et L deux K-extensions différentielles. L'application $\sigma\ :\ M \longrightarrow\ L$,
K-isomorphisme différentiel est *un isomorphisme admissible* si il existe un corps N qui est une extension différentielle de M et de L.

Remarquons que si σ est un isomorphisme admissible de M, extension de Picard-Vessiot de (*), dans L, alors pour tout i, $\mathcal{L}(\sigma(u_i)) = 0$ donc, $\forall i\ \sigma(u_i) = \sum_{j=1}^n k_{ij}u_j$ avec $k_{ij} \in C_N$ (où N est une extension différentielle de M et L). Or σ est bijectif donc $(k_{ij})_{i,j\leq n}$ est dans $GL_n(C_N)$.

Lemme B.3.4. *Soit (K,C) corps différentiel et $M = K < u_1,\dots,u_n >$ une extension de Picard-Vessiot de K. Il existe S ensemble de polynômes de $C[X_1,\dots,X_{n^2}]$ tel que :*

(i) Si σ est un K-isomorphisme admissible de M, la matrice $(k_{ij})_{i,j\leq n}$ associée est telle que
$(k_{ij}) \in \bigcap_{f\in S} f^{-1}(0)$.

(ii) Si N est une extension de M et $(k_{ij})_{i,j\leq n} \in GL_n(C_N) \cap \bigcap_{f\in S} f^{-1}(0)$, il existe un K-isomor-phisme admissible σ de M dans N, dont la matrice associée est (k_{ij}).

Démonstration : Soit $\varphi : y_i \mapsto u_i$ de $K\{y_1,...,y_n\}$ dans M l'évaluation, morphisme différentiel canonique, où $y_1,...,y_n$ sont des indéterminées différentielles. $\Gamma = \mathrm{Ker}\ \varphi$ est un idéal différentiel premier (car Im φ intègre) de $K\{y_1,...,y_n\}$. Soit ψ l'homomorphisme différentiel de $K\{y_1,...,y_n\}$ dans $M[c_{i,j}]$ défini par $\psi(y_i) = \sum_{j=1}^n c_{i,j}u_j$. Posons $\Delta = \psi(\Gamma)$ et S l'ensemble des polynômes de $C[c_{i,j}]$ obtenus en décomposant les éléments de Δ sur une base de M. On va montrer que S est l'ensemble cherché.

1. Soit σ un K-isomorphisme différentiel admissible de M ($u_i \mapsto \sum_{j=1}^{n} k_{i,j}u_j$). Le diagramme suivant (où $p(c_{ij}) = k_{ij}$) commute :

$$\begin{tikzcd} K\{y_1,\dots,y_n\} \arrow[r, "\varphi"'] \arrow[d, "\psi"'] & M \arrow[d, "\sigma"'] \\ M[(c_{i,j})] \arrow[r, "p"'] & L \end{tikzcd}$$

Donc, Γ étant envoyé sur 0 dans L, Δ l'est aussi, et par l'argument utilisé dans la démonstration du lemme III.2, S s'annule en $(k_{i,j})$.

2. Soit $(k_{ij})_{i,j\leq n} \in GL_n(C_N) \cap \bigcap_{f\in S} f^{-1}(0)$. On a Ker $(\varphi) \subset$ Ker $(\psi op$) donc, par propriété universelle, il existe σ, K-homomorphisme différentiel de $K\{u_1,...,u_n\}$ dans $K\{\sigma u_1,...,\sigma u_n\}$, avec $\sigma u_i = \sum_{j=1}^{n} k_{i,j}u_j$. Il suffit de montrer que σ est injectif : on pourra alors étendre au quotient M et conclure.

Supposons donc σ non injectif : (pour alléger les notations on écrira $u = (u_1,...,u_n)$ et $k = (k_{i,j})$).

On pose $P = Ker\sigma$ et on applique le lemme III.3 sur les degrés de transcendance :

$deg_{tr}(K{<}\sigma u{>}/K) < deg_{tr}(K{<}u{>}/K)$. Or, par additivitée des degrés de transcendance on a :

$deg_{tr}(K < u > /K) + deg_{tr}(K < u,\sigma u > /K < u >) = deg_{tr}(K < u,\sigma u > /K < \sigma u >) + deg_{tr}(K{<}\sigma u{>}/K)$

D'où :

$$\begin{aligned} deg_{tr}(K{<}u{>}(k)/K{<}u{>}) &= deg_{tr}(K{<}u,\sigma u{>}/K{<}u{>}) \\ &\leq deg_{tr}(K{<}u,\sigma u{>}/K{<}\sigma u{>}). \end{aligned}$$

car $K{<}u,\sigma u{>}= K{<}u{>}(k)$: $Wr(u)(k_{ij}) = Wr(\sigma u)$. Or en appliquant le lemme III.2 aux $k_{i,j} \in C_N$ on en extrait une famille algébriquement libre maximale sur C, qui reste algébriquement libre sur $K{<}u{>}$. Donc $deg_{tr}(C(k)/C) \leq deg_{tr}(K{<}u,\sigma u{>}/K{<}u{>})$, d'où l'égalité.

De même, en remplaçant σ et u par σ^{-1} et σu,

$deg_{tr}(C_{K<\sigma u>}(k)/C_{K<\sigma u>}) = deg_{tr}(K{<}u,\sigma u{>}/K{<}\sigma u{>})$. Et visiblement :

$deg_{tr}(C_{K<\sigma u>}(k)/C_{K<\sigma u>}) \leq deg_{tr}(C(k)/C)$. D'où la contradiction. □

Nous pouvons maintenant énoncer un des résultats majeur de notre étude, qui découle immédiate-ment du lemme précédent :

Théorème B.3.2. *Le groupe de Galois différentiel d'une extension de Picard-Vessiot est un groupe algébrique linéaire sur le corps des constantes.*

Avant de pouvoir plonger plus avant dans la théorie de Galois différentielle, et d'arriver à l'énoncé de la correspondance entre sous-groupes fermés et sous K-extensions fermées, nous devons étudier plus en détails les particularités introduites par le mot *différentiel* : plutot que de travailler directement sur des automorphismes, nous passons par l'intermédiaire d'isomorphismes admissibles. Selon I.Kaplansky, l'introduction de ces objets, et les complications qu'ils apportent, sont inévitables si l'on veut pouvoir traiter le sujet à un niveau qui reste relativement élémentaire.

B.4 Outils d'algèbre différentielle

B.4.1 Extension d'idéaux premiers

Lemme B.4.1. *Soit I un idéal différentiel d'une $\mathbb{Q}$-algèbre A, et soit $a \in A$ tel que $\exists n \; a^n \in I$. Alors $(\partial a)^{2n-1} \in I$. En particulier, $\sqrt{I}$ est un idéal différentiel.*

Démonstration : On sait que $\partial(a^n) = na^{n-1}\partial(a) \in I$ (idéal différentiel), donc, comme $\mathbb{Q} \subset A$, on a
$a^{n-1}\partial(a) \in I$. On montre alors par récurrence, que : $\forall k \;\; a^{n-k}(\partial(a))^{2k-1} \in I$, et on conclut en appliquant ceci à $n = k$. □

Lemme B.4.2. *Soit A un anneau différentiel, I idéal différentiel radical et $S \subset A$. Si $ab \in I$, alors $a\partial(b) \in I$ et $\partial(a)b \in I$.*
De plus, si $T = \{x \in A \;/\; xS \subset I\}$, alors T est un idéal différentiel radical de A.

Démonstration : Comme $\partial(ab) = a\partial b + \partial(a)b \in I$, on a $a\partial(a)b\partial b + (a\partial b)^2 \in I$, ainsi : $(a\partial b)^2 \in I$ et comme I est radical $a\partial b \in I$.
De plus, T est clairement un idéal, il est différentiel par l'argument précédent, et I radical donne facilement T radical. □

Remarquons que si A est un anneau commutatif et $(I_s)_{s\in S}$ une famille d'idéaux radicaux, alors $\bigcap_{s\in S} I_s$ est un idéal radical. De plus, sur un anneau différentiel, une intersection quelconque d'idéaux différentiels est un idéal différentiel. Ainsi, si $S \subset A$, il existe un plus petit idéal radical différentiel contenant S :

$$\bigcap_{I \; ideal \; rad \; diff \supset S} I.$$

On le note $\{S\}$.

Lemme B.4.3. *Soit A un anneau différentiel, $a \in A$ et $S \subset A$, alors :*
(i) $a\{S\} \subset \{aS\}$
(ii) si $T \subset A$, alors $\{S\}\{T\} \subset \{ST\}$.

Démonstration : Posons $S_1 = \{x \in A \;/\; ax \in \{aS\}\}$. C'est un idéal radical différentiel par le lemme IV.2, et $S \subset S_1 \Rightarrow \{S\} \subset S_1 \Rightarrow a\{S\} \subset aS_1 \subset \{aS\}$.
De même, $T_1 = \{x \in A \;/\; x\{T\} \subset \{ST\}\}$ est un idéal radical différentiel et contient S donc contient $\{S\}$. □

Lemme B.4.4. *Soit A un anneau différentiel et T un sous ensemble multiplicativement clos de A. Soit Q un idéal radical, maximal sur l'ensemble des idéaux J tels que $T \cap J$ est vide, alors Q est premier.*

Démonstration : Supposons par l'absurde que : $\exists a,b \in A$ $ab \in Q$, $a \notin Q$ et $b \notin Q$.
$\{Q,a\}$ et $\{Q,b\}$ sont des idéaux différentiels radicaux contenant strictement Q. Ainsi, il existe t_1 dans $T \cap \{Q,a\}$ et t_2 dans $T \cap \{Q,b\}$ avec $t_1 t_2 \in (T \cap \{Q,a\})(T \cap \{Q,b\}) \subset \{Q,a\}\{Q,b\} \subset Q$ par le lemme IV.3, d'où $T \cap Q \neq \emptyset$, contradiction. □

Théorème B.4.1. *Soit B un anneau différentiel et A un sous anneau différentiel de B. Soit I un idéal différentiel radical de B tel que $P = I \cap A$ est un idéal différentiel premier de A. Dans ce cas, I peut être étendu en un idéal différentiel premier de B, I_1, avec $I_1 \cap A = P$.*

Démonstration : Posons $T = \{x \in A \ / \ x \notin P\}$. Comme P est premier, T est multiplicativement clos. Soit I_1 un idéal radical, maximal au sens du lemme IV.4, et contenant I (existe par le lemme de Zorn). Le lemme IV.4 donne alors : I_1 est premier, $I_1 \cap A \subset P$ et contient $I \cap A = P$. □

Théorème B.4.2. *Soit B un anneau différentiel, A un sous-anneau différentiel et I un idéal différentiel radical de B tel que : $(ab \in I \ (a \in A,\, b \in B) \Rightarrow (a \in I \text{ ou } b \in I)\ )$. Alors : I peut s'écrire comme une intersection d'idéaux (I_α) différentiels premiers de B tels que $\forall \alpha\ I_\alpha \cap A = P$ (avec $P = I \cap A$).*

Démonstration : Notons que P est un idéal différentiel de A. Soit $x \in B$ $x \notin I$, on veut construire un idéal I_x différentiel premier de B, contenant I, tel que $I_x \cap A = P$ et tel que $x \notin I_x$. On aura alors $I = \bigcap I_x$. Soit $T = \{ax^n \ / \ a \in A \ a \notin P \ n \in \mathbb{N}\}$, T est multiplicativement clos car P est premier, et par hypothèse $T \cap I = \emptyset$, donc il existe un idéal de B différentiel radical I_x maximal tel que $I_x \cap T = \emptyset$ et contenant I (par Zorn). Ainsi le lemme IV.4 implique que I_x est premier.
De plus, $1 \notin P$ (sinon P=A, donc $I = B : I = I_\alpha$) donc $x \in T$ i.e $x \notin I_x$.
Enfin, soit $a \in I_x \cap A$, d'où $ax \in I_x$: si $a \in P$ c'est fini, sinon $ax \in T \cap I_x = \emptyset$ ce qui est impossible, donc $P = I \cap A \subset I_x \cap A \subset P$. □

B.4.2 Un lemme sur les anneaux de polynômes

Lemme B.4.5. *Soit K un corps et L une K-extension. Soit $\mathfrak{b}$ un ensemble éventuellement infini*
$B = L[(X_i)_{i \in \mathfrak{b}}]$, $A = K[(X_i)_{i \in \mathfrak{b}}]$, P un idéal de A, J idéal engendré par P dans B et $I = \sqrt{J}$, alors :

(i) Si P est un idéal radical alors $I \cap A = P$.
(ii) Si P est un idéal premier et si $ab \in I$ avec $a \in A$ $b \in B$, alors $a \in P$ ou $b \in I$.
(iii) Si $Car(K) = 0$ et $P \neq A$, soit Y une des indéterminées et $s \in L$ $s \notin K$, alors $Y - s \notin I$.

Démonstration : L est un K-espace vectoriel, si $dim_K L = 1$ le lemme est trivial. On suppose désormais $dim_K L \geq 2$.

Soit $(u_\alpha)_{\alpha \in \mathfrak{a}}$ une base de L sur K. On choisit deux éléments particuliers u_1 et u_2 de cette base. Quitte à multiplier par u_1^{-1} on suppose même que $u_1 = 1$. Tout élément f de

B s'écrit de manière unique $\sum f_\alpha u_\alpha$ avec $f_\alpha \in A$. Un tel f appartient à A si et seulement si $f_\alpha = 0$ pour $\alpha \neq 1$. De plus $J = \{\sum p_\alpha u_\alpha \ / \ p_\alpha \in P\}$, donc $J \cap A = P$.

1. On suppose que P est un idéal radical et que $b \in I \cap A$. Alors $\exists n \ b^n \in J \cap A = P$ radical donc $b \in P$ donc $P = I \cap A$.

2. Si P est premier et $ab \in I$ avec $a \in A$ et $b \in B$, alors $a^n b^n \in J$. De plus, $b^n \in B$ implique $b^n = \sum f_\alpha u_\alpha$, donc $\forall \alpha \ a^n f_\alpha \in P$. Si $a \in P$ c'est fini, sinon $\forall \alpha \ f_\alpha \in P$, donc $b \in I$.

3. On suppose par l'absurde que $Y - s \in I$. Alors $\exists m \ (Y-s)^m \in J$. Posons donc $I_0 = \{f \in L[Y] \ / \ f \in J\}$. C'est un idéal de $L[Y]$, donc principal : écrivons donc $I_0 = (f_0)$. Comme $(Y-s)^m \in I_0$, on a $f_0 \ / \ (Y-s)^m$.
Si $f_0 \in L$ alors $J = B$ et donc $P = A$ impossible par hypothèse. Ainsi $f_0 = (Y-s)^r$, $r \geq 1$. Dans la base $(u_\alpha)_{\alpha \in \mathfrak{a}}$ on peut prendre $u_2 = s$. Mais $f_0 \in J$ donc $(Y-s)^r = \sum p_\alpha u_\alpha$ avec $\forall \alpha \ p_\alpha \in P$. Ainsi $\forall \alpha \ p_\alpha \in J$, en particulier $p_1 \in J$. Or $p_1 = Y^r + 0Y^{r-1} + \cdots$ (car $(Y-s)^r = Y^r - rsY^{r-1} + \cdots$ et $s = u_2$). Le polynôme p_1 appartenant à I_0 on a $p_1 = f_0 f$ où $f \in L[Y]$ et p_1 et f_0 sont unitaires de même degré, donc $p_1 = f_0$, donc $rs = 0$ et $Car K = 0$: contradiction. □

B.4.3 Les isomorphismes admissibles

On peut maintenant énoncer les deux propositions concernant les isomorphismes admissibles.

Théorème B.4.3. *Soit M un corps différentiel de caractéristique 0, K et L deux sous-corps différentiels et $S : K \to L$ un isomorphisme différentiel. Alors S peut être étendu en un isomorphisme admissible défini sur M.*

Démonstration : Soit $(u_\alpha)_{\alpha \in \mathfrak{a}}$ une base de M sur K. Par induction transfinie sur $\mathfrak{a}$ on se ramène au problème suivant : étant donné $u \in M \ u \notin K$, on cherche à définir une extension de S à u, l'image de u étant dans une extension convenable de M.
Soit $K\{u\}$ l'anneau intègre obtenu en adjoignant u à K, et $K\{y\}$ l'anneau obtenu avec y une indéterminée différentielle. $\varphi_1 : K\{y\} \to K\{u\}$ est un morphisme différentiel, $P = Ker \ \varphi_1$ est un idéal
$y \longmapsto u$ différentiel premier.
Grace à S, on envoie P_1 sur P idéal différentiel premier de $L\{y\}$ (car S surjectif). Soit alors J l'idéal de $M\{y\}$ engendré par P : il est clairement différentiel, posons $I = \sqrt{J}$. Le lemme IV.1 nous dit que I est un idéal (radical) différentiel de $M\{y\}$, le lemme IV.5 nous donnant $I \cap L\{y\} = P$. Enfin par la proposition IV.1 on peut étendre I en un idéal premier I_1 de $M\{y\}$ satisfaisant$L\{y\} \cap I_1 = P$.
Considérons $\pi : M\{y\} \to M\{y\}/I_1$ la surjection canonique on a :

$$K\{y\} \xrightarrow{S} L\{y\} \xrightarrow{\pi} L\{\pi(y)\}$$

$Ker \ \pi_{|L\{y\}} = I_1 \cap L\{y\} = P$, donc $Ker \ \pi_{|L\{y\}} \circ S = P_1$. On a ainsi l'isomorphisme :

$$K\{u\} \simeq K\{y\}/P_1 \simeq \pi(L\{y\} \simeq L\{\pi(y)\}$$

qui étend S. Par la proposition II.1 cet isomorphisme se prolonge de manière unique en un isomorphisme différentiel de $K < u >$ sur $L < \pi(y) >$ sous extension de $M < \pi(y) >$, d'où le résultat. □

Théorème B.4.4. *Soit K un corps différentiel de caractéristique 0, M une extension de K, et soit $s \in M$ et $s \notin K$. Alors il existe φ un K-isomorphisme admissible sur M qui bouge s (i.e tel que $\varphi(s) \neq s$).*

Démonstration: Soit y une indéterminée différentielle et soit $\varphi : K\{y\} \to K\{s\}$ morphisme différentiel et $P = Ker\varphi \quad (P \neq K\{y\}$ car $s \neq 0)$ $\quad y \longmapsto s$

Soit $L = K < s >$ et J l'idéal différentiel de $L\{y\}$ engendré par P et $I = \sqrt{J}$. I est un idéal différentiel de $L\{y\}$ tel que $I \cap K\{y\} = P$ (car P est premier donc radical). Ainsi I peut être étendu en un idéal I_1 différentiel premier tel que $I_1 \cap K\{y\} = P$.

$\pi : L\{y\} \to L\{y\}/I_1$ On peut donc construire un K-isomorphisme admissible de $K < s >$

$y \longmapsto \pi(y)$ sur $K < \pi(y) >$ envoyant s sur $\pi(y)$.

Remarquons que $\pi(y) = s \Leftrightarrow y - s \in I_1$. Le lemme IV.5 indique que nous sommes dans les hypothèses de la proposition IV.2, d'où: I est une intersection d'idéaux premiers I_s tels que $\forall s \; I_s \cap K\{y\} = P$ Ainsi I est l'intersection des idéaux de la forme I_1 construit précédemment.

Par l'absurde, supposons que pour tout I_1, $y - s \in I_1$. Dans ce cas $y - s \in I$ ce qui est impossible par le lemme IV.5. On a donc construit un isomorphisme ayant les propriétés voulues, par la proposition précédente on peut l'étendre en un K-isomorphisme admissible défini sur M. □

B.5 Le coeur de la théorie

B.5.1 Préliminaires et compléments

Définition B.5.1 Une extension différentielle M de K est dite normale sur K si $M^G = K$ avec
$G = Gal_\partial(M/K)$.

Théorème B.5.1. *Soit M un corps différentiel et $G = Gal_\partial(M/K)$:*

(i) Si $H \lhd G$ alors $\forall \sigma \in G \; \sigma(\check{H}) = \check{H}$.

(ii) Si L est une sous K-extension différentielle de M telle que $\forall \sigma \in G \; \sigma(L) = L$, alors $\check{L} \lhd G$ et $G/\check{L}$ est le groupe des K-automorphismes différentiels de L qui peuvent être étendus à M.

Démonstration : Soit $\sigma \in G$ et $x \in \check{H}$, on veut montrer que $\sigma(x) \in \check{H}$.
$H \lhd G \Rightarrow \forall \varphi \in H\ \sigma^{-1}\varphi\sigma \in H \Rightarrow \sigma^{-1}\varphi\sigma(x) = x \Rightarrow \varphi\sigma(x) = \sigma(x) \Rightarrow \sigma(x) \in \check{H}$. De même $\sigma^{-1}(\check{H}) \subset \check{H}$, donc $\sigma(\check{H}) = \check{H}$.
Comme précédemment $\check{L} \lhd G$. L'application $\Phi : G \to Gal_\partial(L/K)$, $\sigma \mapsto \sigma_{|L}$ est bien définie par hypothèse et :
$Ker\Phi = \check{L}$ et $Im\Phi$ est l'ensemble des K-automorphismes différentiels de L pouvant être étendus à M. □

Lemme B.5.1. *Soit L une sous K-extension différentielle de M, fermée et H le sous-groupe correspondant. Alors $N_G(H) = \{\sigma \in G\ /\sigma(L) = L\}$.*
Démonstration : $N_G(H) = \{\sigma \in G\ /\forall\varphi \in H\ \sigma\varphi\sigma^{-1} \in H\}$, $H = \check{L}$. Soit $\sigma \in N_G(\check{L})$ et $x \in L$.
On a $\forall\varphi \in \check{L}\ \sigma^{-1}\varphi\sigma \in \check{L}$ donc $\forall\varphi \in \check{L}\ \varphi(\sigma(x)) = \sigma(x)$. Ainsi $\sigma(x) \in \check{\check{L}} = L$ donc $\sigma(L) \subset L$ et pareillement pour σ^{-1} d'où $N_G(\check{L}) \subset \{\sigma \in G\ /\ \sigma(L) = L\}$.
Réciproquement, si $\sigma \in G$ est tel que $\sigma(L) = L$ et si $\varphi \in \check{L}$, alors $\sigma(L) = L$ donc $\varphi\sigma_{|L} = \sigma_{|L}$ et $\sigma^{-1}\varphi\sigma_{|L} = Id_L$ d'où $\sigma \in N_G(\check{L})$. □

Lemme B.5.2. *Soit L une sous K-extension différentielle fermée de M, normale sur K. Supposons de plus que $N_G(\check{L})$ est fermé et que tout K-automorphisme différentiel de L peut être étendu sur M. Alors $\check{L} \lhd G$ et $G/\check{L}$ est exactement $Gal_\partial(L/K)$.*
Démonstration : $\check{L} \lhd G \Leftrightarrow N_G(\check{L}) = G$, soit donc L_1 le sous-corps correspondant à $N_G(\check{L})$. Si $L_1 = K$ alors , comme $N_G(\check{L})$ est fermé, $\check{L_1} = N_G(\check{L}) = \check{K} = G$. Montrons donc que $L_1 = K$. Par le lemme V.1 on sait que $N_G(\check{L}) = \{\sigma \in G\ /\ \sigma(L) = L\}$, c'est à dire, car tout K-automorphisme peut être prolongé sur M, on a : $Gal_\partial(L/K) = N_G(\check{L})$. Or comme L est normale , si $x \in L\ x \notin K\ \exists\sigma \in N_G(\check{L})$, $\sigma(x) \neq x$, i.e $L_1 = K$.
On a enfin $G/\check{L} \simeq Gal_\partial(L/K)$ par la proposition V.1. □

B.5.2 Normalité de l'extension de Picard-Vessiot

Lemme B.5.3. *Soit (K,C) un corps différentiel avec C algébriquement clos, et M une extension de Picard-Vessiot de K. Supposons donnés $z \in M$ et $\{x_\alpha\}_{\alpha\in I}$ et $\{y_\alpha\}_{\alpha\in I} \subset M$, et supposons qu'il existe σ, un K-isomorphisme admissible de M, envoyant $\{x_\alpha\}$ sur $\{y_\alpha\}$ en déplaçant z. Alors il existe un K-automorphisme de M réalisant la même chose.*
Démonstration : Soit $\sigma : M \to L \subset N$, et C_N le corps des constantes de N, $\sigma(u_i) = \sum k_{ij}u_j$ (*) avec $k_{ij} \in C_N$. Soit x,$y \in M$, $x = \frac{P(u)}{Q(u)}$ et $y = \frac{R(u)}{S(u)}$ où $u = (u_1, \ldots ,u_n)$, on a :
$y = \sigma(x) \Leftrightarrow R(u)Q(\sigma(u)) = P(\sigma(u))S(u)$, injectant (*), on obtient un système d'équations polynômiales en k, à coefficients dans M, et on a un tel système pour chaque α. De plus, par le lemme III.4 on a $k_{ij} \in \bigcap_{f\in S} f^{-1}(0)$, et enfin on a l'inéquation $\sigma(z) \neq z$ et $det(k_{ij}) \neq 0$, or (k_{ij}) est une solution de ce système dans C_N, donc par le lemme III.2 il existe une solution dans C, d'où l'automorphisme cherché. □

Théorème B.5.2. *Soit (K,C) comme précédemment, de caractéristique 0, alors : toute extension de Picard-Vessiot de K est normale.*

Démonstration : Soit $G = Aut_K(M)$, on a M normale $\Leftrightarrow M^G = K$. Soit $z \in M$, $z \notin K$. La proposition IV.4 nous donne un isomorphisme admissible qui déplace z, et on conclut par le lemme précédent. □

Théorème B.5.3. *Soit (K,C) comme précédemment, et M une extension de Picard-Vessiot de K, alors : Tout K-isomorphisme entre deux sous K-extensions de M peut être étendu en un K-automorphisme différentiel de M. En particulier, tout K-automorphisme de L, sous K-extension, peut être ainsi étendu.*

Démonstration : Soit σ un K-isomorphisme différentiel de L_1 dans L_2, alors par la proposition IV.3, σ peut être étendu en un K-isomorphisme admissible de M. On conclut avec le lemme . □

B.5.3 Complétion de la théorie de Galois différentielle

Théorème B.5.4. *Les sous-groupes algébriques de $G = Gal_\partial(M/K)$ sont Galois-fermés.*

Démonstration : Dans cette démonstration, si F est un polynôme de $M\{y,z\}$ et n_F le nombre de monômes qui le composent, on dira que E est *strictement plus court* que F si $n_E < n_F$.

Soit H un sous-groupe algébrique de G, montrons que H est Z-dense dans $\check{\check{H}}$ par l'absurde (ce qui entraîne le théorème). On fera la preuve dans le cas n=2, pour simplifier la typographie et la lecture, le cas général étant similaire. Soit donc, $M = K < u,v >$.

Supposons par l'absurde que $\exists f \in C[X_{i,j}]$, $f(H) = \{0\}$ et $f(\check{\check{H}}) \neq \{0\}$. Soit $\begin{pmatrix} A & C \\ B & D \end{pmatrix}$ l'inverse de $\begin{pmatrix} u & u' \\ v & v' \end{pmatrix} \in GL_2(K)$, et $F \in M\{y,z\}$ définie par :

$$F(y,z) = f(Ay + By', Az + Bz', Cy + Dy', Cz + Dz')$$

Si on prend $\sigma \in H$, de matrice $(k_{i,j})$, on obtient :

$$\begin{pmatrix} \sigma u & \sigma u' \\ \sigma v & \sigma v' \end{pmatrix} = \begin{pmatrix} k_{1,1} & k_{1,2} \\ k_{2,1} & k_{2,2} \end{pmatrix} \begin{pmatrix} u & u' \\ v & v' \end{pmatrix}$$

Ainsi ($\forall \sigma \in H$ $F(\sigma u, \sigma v) = 0$, et $\exists \sigma_1 \in \check{\check{H}}$ $F(\sigma_1 u, \sigma_1 v) \neq 0$.) (*)
Soit $I = \{F \in M\{y,z\}\ /\ F\ vérifie\ (*)\ \}$. $I \neq \emptyset$, car $F \in I$.
On note E un élément de I ayant le nombre minimal de monômes. Comme M est un corps, on peut supposer que l'un des coefficients de E vaut 1. Pour $\tau \in H$ on appelle E_τ le poynôme obtenu en prenant l'image des coefficients de E par τ. On a donc :

$\forall \sigma \in H \quad E_\tau(\sigma u,\sigma v) = \tau E(\tau^{-1}\sigma(u),\tau^{-1}\sigma(v)) = 0$. Or $E - E_\tau$ est strictement plus court que E, donc $\forall \sigma \in \check{\check{H}}\ (E - E_\tau)(\sigma u,\sigma v) = 0$.
Si $E \neq E_\tau$, il existe $a \in M$ tel que $E - a(E - E_\tau)$ est strictement plus court que E et appartient à I, ce qui est impossible, d'où : $E = E_\tau$. Ainsi tous les coefficients de E sont stables par $\tau \in H$, donc sont dans $\check{H}$. Or $\forall \sigma \in \check{\check{H}}\ \forall x \in \check{H}\ \sigma(x) = x$, donc : $\forall \sigma \in \check{\check{H}}$ $\sigma E(u,v) = E(\sigma u,\sigma v) = 0$, ce qui contredit l'hypothèse. □

Finalement en rassemblant l'analyse précédente et la proposition on obtient le théorème principal de la théorie de Galois différentielle qui découle simplement de ce qui à été fait auparavant.

Théorème B.5.5. Correspondance de Galois *Soit K un corps différentiel de caractéristique 0, de corps des constantes C algébriquement clos. Soit M une extension de Picard Vessiot de K, alors :*

(i) on a une correspondance bijective entre les sous K-extensions différentielles de M et les sous-groupes algébriques de $G = Gal_\partial(M/K)$, donnée par $\check{}$.

(ii) Un sous-groupe fermé H de G est distingué dans G si et seulement si $\check{H} = L$ est normale sur K. De plus dans ce cas, on a : $G/H \simeq Gal_\partial(L/K)$.

B.6 Résolution par quadrature des équations différentielles linéaires

Nous allons désormais nous attacher à donner une jolie application de cette théorie : similairement à la notion de *résolubilité par radicaux* d'une équation algébrique, on a, pour les équations différentielles linéaires, la notion de *résolubilité par quadratures.* On veut savoir si toutes les équations différentielles linéaires sont résolubles par quadratures, et, si non a-t-on un critère général nous permettant de différentier celles qui le sont de celles qui ne le sont pas?

Il est remarquable de constater là encore la similitude avec la théorie de Galois classique : comme nous allons le montrer, le résultat provient de la résolubilité (ou non) d'un sous-groupe du groupe de Galois.

Définition B.6.1 Soient K et M des corps différentiels. *M est une extension de Liouville de K* si il existe une tour de corps $K = K_0 \subset K_1 \subset \ldots \subset K_n = M$ telle que pour tout i on a $K_i = K_{i-1}(u_i)$, avec :

(i) $\frac{\partial(u_i)}{u_i} \in K_{i-1}$ (i.e $u_i = e^{\int a_i}$pour un $a_i \in K_{i-1}$), ou

(ii) $\partial(u_i) \in K_{i-1}$ (i.e $u_i = \int a_i$ pour un $a_i \in K_{i-1}$).

Autrement dit, une extension de Liouville se construit par quadratures, et on a un critère pour que toute solution d'une équation différentielle donnée soit liouvillienne (i.e appartienne à une extension de Liouville).

Théorème B.6.1. *Soit M une extension de Picard-Vessiot de K (corps différentiel de caractéristique 0 et de corps des constantes algébriquement clos) de groupe de Galois G(M/K). M est contenue dans une extension finie de K suivie d'une extension de Liouville si et seulement si la composante connexe de l'identité, $G(M/K)^0$, est un groupe résoluble.*

Notons que ce théorème ne nous donne pas d'algorithme nous permettant de savoir si une équation est ou non résoluble par quadratures. La démonstration de ce théorème est le but du reste de cette partie.

B.6.1 Étude des extensions de Liouville

Le lemme VI.1 est un lemme technique évident qui nous servira tout le temps dans la suite. Le lemme VI.2 étudie l'extension obtenue lorsqu'on ajoute une intégrale (cas(1) : $u = \int a$), et le lemme VI.3 lorsqu'on ajoute l' exponentielle d'une intégrale (cas(2) : $u = e^{\int a}$). La proposition VI.2 donne un premier résultat dans un cas particulier sur le sens direct du théorème VI.1 .

Lemme B.6.1. *Soit $K \subset L \subset M$ des corps différentiels. Supposons que L est une extension de Picard-Vessiot de K et que M a le même corps des constantes que K. Alors tout K-automorphisme différentiel de M envoie L sur lui-même.*

Lemme B.6.2. *Soit (K,C) un corps différentiel de caractéristique 0 et u dans une extension de K, vérifiant $\partial u = a \in K$, où a n'est pas une dérivée dans K. Alors u est transcendant sur K, $K{<}u{>}$ est une extension de Picard-Vessiot de K, et $G(K{<}u{>}/K)$ est isomorphe au groupe additif C.*

Démonstration :

(i) Supposons u algébrique : soit $u^n + bu^{n-1} + ... = 0$ minimal. En dérivant on obtient : $nau^{n-1} + \partial(b)u^{n-1} + ... = 0$. Donc $na + \partial b = 0$, d'où $a = \partial(-b/n)$ (on est en caractéristique 0) : contradiction.

(ii) Montrons qu'il n'y a pas de nouvelles constantes :
$b_1u^n + b_2u^{n-1} + ...$ est une constante entraîne $\partial(b_1)u^n + (nb_1a + \partial b_2)u^{n-1} + ... = 0$. Or u n'est pas algébrique donc $\partial b_1 = 0$ et $a = -(\partial b_2)/(nb_1) = -\partial(b_2/nb_1)$: contradiction. Soit $f(u)/g(u)$ une constante, où f/g est une fraction de $K(X)$, g de degré minimum (parmi les f'/g' tels que $f'(u)/g'(u) = f(u)/g(u)$), et g unitaire. D'après ci-dessus, f non constant entraîne g non constant. L'élément $f(u)/g(u)$ est une contante, et donc égale à $(\partial f(u))/(\partial g(u))$, ce qui contredit la minimalité de g.

(iii) Soit $\mathcal{L} : \partial(y) - a = 0$ et $\sigma \in G(K < u > /K)$. Comme σu définit σ, et doit être solution de $\mathcal{L}$, on a $\partial(\sigma u - u) = 0$, donc $\sigma u = u + c$ avec $c \in C$. Réciproquement : soit $c \in C$, et σ le K-automorphisme (algébrique) de $K{<}u{>}$ induit par $u \mapsto u + c$.

On a :

$$\begin{aligned}\partial\circ\sigma(\sum \lambda_i u^i) &= \sum(\partial(\lambda_i)(u+c)^i + i\lambda_i a(u+c)^{i-1}) \\ &= \sigma(\sum \partial(\lambda_i)u^i + i\lambda_i a u^{i-1}) \\ &= \sigma\circ\partial(\sum \lambda_i u^i).\end{aligned}$$

Donc $\sigma \in G(K<u>/K)$. ☐

Lemme B.6.3. *Soit (K,C) un corps différentiel et u dans une extension de K, vérifiant $\partial u - au = 0$, $a \in K$. Supposons que $K<u>$ a le même corps des constantes que K. Alors $K<u>$ est une extension de Picard-Vessiot de K, et $G(K<u>/K)$ est isomorphe à un sous-groupe de C^*.*

Démonstration : Si v est une solution de $\partial y - ay = 0$, $\partial(v/u) = 0$. Donc $v = cu$ avec $c \in C$ (ou, plus simplement, les $(k_{i,j})$ qui définissent σ sont dans $GL_1(C) = C^*$). Le reste est immédiat. ☐

Théorème B.6.2. *Soit M une extension de Liouville de K, sans nouvelles constantes. Alors $G(M/K)$ est résoluble.*

Démonstration : Soit $G = G(M/K)$, et $K = K_1 \subset K_2 \subset ... \subset K_n = M$ la tour définissant l'extension de Liouville. Les lemmes VI.2 ou VI.3 donnent K_2 extension de Picard-Vessiot de K. Donc par le lemme VI.1, tout élément de G envoie K_2 sur lui-même. Si $H_2 = \check{K}_2$, La proposition V.1(2) nous donne $H_2 \lhd G$ et $G/H_2 \simeq G(K_2/K_1)$. Or par les lemmes VI.2 ou VI.3 $G(K_2/K_1)$ est abélien, donc G/H_2 aussi. Par une récurrence immédiate sur n, G est résoluble. ☐

B.6.2 Deux lemmes sur les groupes algébriques linéaires

Dans cette partie, C est un corps algébriquement clos. On étudie les propriétés des groupes algébriques linéaires connexes. Ces deux lemmes servent à la démonstration du théorème VI.2(de Lie-Kolchin).

Lemme B.6.4. *Dans un sous-groupe algébrique connexe de $GL_n(C)$, tout élément qui n'est pas dans le centre a une classe de conjugaison infinie.*

Démonstration : Soit G un tel sous-groupe, et $x \in G$ ayant une classe de conjugaison finie. Posons $\varphi : G \to \{axa^{-1} \ / \ a \in G\} = \bigsqcup_{i=1}^{n}\{y_i\}$, avec $\varphi(a) = axa^{-1}$. Les $\varphi^{-1}(y_i)$ forment une partition de G. De plus $\varphi^{-1}(y_i)$ fermé (image reciproque d'un fermé par φ continue) ouvert (complémentaire d'une union finie de fermés) dans G connexe. Donc $x \in Z(G)$. ☐

Lemme B.6.5. *Si G est un sous-groupe algébrique connexe de $GL_n(C)$, alors le groupe dérivé $D(G)$ est connexe.*

Démonstration : Notons D_k les produits de k commutateurs, on a alors $D_k \subset D_{k+1}$ et $D(G) = \bigcup_k D_k$. Il suffit donc de montrer D_k connexe. Supposons D_{k-1} connexe.

Pour $a_2,..,a_k,b_1,..,b_k$ fixés, l'application $\varphi : \alpha \mapsto \alpha^{-1}b_1^{-1}\alpha b_1 a_2^{-1}b_2^{-1}a_2b_2...a_k^{-1}b_k^{-1}a_kb_k$ est continue. La réunion des images de G par φ lorsque les a_i et les b_i parcourent G est égale à D_k, et $\varphi(G)$ est connexe. Or $\varphi(G) \cap D_{k-1} \neq \emptyset$ (car $\varphi(b_1) \in D_{k-1}$) et D_{k-1} est connexe donc D_k l'est aussi □

B.6.3 Trigonalisation simultanée d'automorphismes

Le théorème VI.2 est un résultat fondamental pour la théorie des extensions de Picard-Vessiot et de Liouville. La proposition VI.3, que l'on peut démontrer directement, le relie au corps de la théorie.

Théorème B.6.3. (de Lie-Kolchin) *Soit G un sous-groupe algébrique résoluble de $GL_n(C)$, où C est un corps algébriquement clos. Si G est connexe (pour la topologie de Zariski), les éléments de G peuvent être trigonalisés simultanément.*

Démonstration : On décompose cette (longue) démonstration en 6 étapes.

(i) Supposons que G (muni de sa représentation canonique) n'est pas irréductible : il existe W sous-espace vectoriel, de dimension p, de C^n stable par G. On prend une base de W que l'on complète en une base de C^n :

$$A = \begin{pmatrix} B & * \\ 0 & B' \end{pmatrix} \qquad \forall A \in G$$

Montrons que l'application $\varphi : A \mapsto B$ est continue (la topologie utilisée est toujours la topologie de Zariski). Soit $P_{k,l}(X_{i,j}) = X_{k,l} \in C[(X_{i,j})]$, pour $1 \leq k,l \leq p$; et $F = \bigcap_{f \in S} f^{-1}(0)$ un fermé de $GL(W)$. Alors

$$\begin{aligned} \varphi^{-1}(F) &= \{(x_{i,j}) \ / \ (P_{k,l}((x_{i,j})_{i,j})_{k,l}) \in F\} \\ &= \{(x_{i,j}) \ / \ \forall f \in S \ f((P_{k,l}((x_{i,j})_{i,j}))_{k,l}) = 0\} \,. \end{aligned}$$

Or $f((P_{k,l}((x_{i,j})_{i,j}))_{k,l}) \in C[(X_{i,j})]$, donc $\varphi^{-1}(F)$ fermé de $GL_n(C)$. Donc φ est continue, ce qui entraîne $\{B \ / \ A \in G\}$ est connexe. Par récurrence, on peut donc se ramener à une forme triangulaire bloc, où les blocs sont irréductibles.

(ii) On suppose désormais G irréductible. $D(G)$ est connexe car G est connexe par le lemme VI.5. Par récurrence sur la longueur de la tour de décomposition (G est résoluble), on peut supposer $D(G)$ sous forme triangulaire.

(iii) Soit W le sous-espace vectoriel de C^n engendré par les vecteurs propres de $D(G)$. $W \neq 0$ car $D(G)$ triangulaire.
Soit $\alpha \in W$, on a $\forall T \in D(G) \ T(\alpha) = c(T)\alpha$, d'où

$$(\forall S \in G)(\forall T \in D(G)) \ S^{-1}TS(\alpha) = c(S^{-1}TS)\alpha$$

car $D(G) \lhd G$. Donc $\forall T \in D(G) \ T(S(\alpha)) = c(S^{-1}TS)S(\alpha)$. Donc pour tout $S \in G$ $S(\alpha) \in W$, ce qui entraîne que W est stable par G. G irréductible impose alors $W = C^n$. $D(G)$ est donc diagonal.

(iv) Tout élément de $D(G)$ est donc une matrice diagonale. Ses conjugués dans G, étant dans $D(G)$, sont donc diagonaux. Les seuls conjugués possibles sont alors ceux obtenus en permutant les racines du polynôme caractéristique sur la diagonale. Donc chaque élément de $D(G)$ a une classe de conjugaison finie dans G. Par le lemme VI.4, $D(G) \subset Z(G)$.

(v) Soit $T \in D(G)$, c une racine de son polynôme caractéristique, et W le sous-espace propre associé. Comme T commute à tout élément de G, W est invariant par G. Donc $W = C^n$, ce qui entraîne $D(G) \subset \{\lambda Id \ / \ \lambda \in C^*\}$.

(vi) Les commutateurs ont tous leur déterminant égal à 1, donc $D(G)$ est inclus dans $\{\lambda Id \ / \ \lambda \in \mu_n(C)\}$. Or $\mu_n(C)$ est fini, donc $D(G)$ est fini. Or par le lemme VI.5, $D(G)$ est connexe, donc $D(G) = 1$. D'où G est commutatif, et dans le cas commutatif, on connaît déjà le résultat. □

Théorème B.6.4. *Soit M une extension différentielle de K telle que $\check{\check{K}} = K$.Supposons que*
u_1,...,$u_n \in M$ vérifient: $\forall \sigma \in G(M/K) \quad \sigma u_i = a_{i,i}u_i + ... + a_{i,n}u_n \quad (*)(i = 1..n)$ (c'est à dire $(u_i)_i$ base de trigonalisation de G) avec $a_{ij} \in C_M$. Alors $K < u_1,...,u_n >$ est une extension de Liouville de K.

Démonstration : On peut supposer u_n non nul.L'équation (*) pour i=n donne $\sigma u_n = a_{n,n}u_n$, donc $\partial(u_n)/u_n$ est invariant sous σ (c'est à dire $\in \check{\check{K}}$). Donc $\partial(u_n)/u_n \in K$: l'ajout de u_n à K est du type $\exp \int a$. En divisant (*) pour i=1...n-1 par σu_n et en dérivant, on obtient :

$$\sigma(\partial\left(\frac{u_i}{u_n}\right)) = \frac{a_{i,i}}{a_{n,n}}\partial\left(\frac{u_i}{u_n}\right) + ... + \frac{a_{i,n-1}}{a_{n,n}}\partial\left(\frac{u_i}{u_n}\right).$$

D'où, par récurrence sur n, on peut ajouter les $\partial\left(\frac{u_i}{u_n}\right)$ puis les u_i/u_n qui sont alors des intégrales. Donc $K < u_1,...,u_n >$ est une extension de Liouville. □

B.6.4 Démonstration du théorème VI.1

Désormais le corps différentiel K est de caractéristique 0 et de corps des constantes algébrique-ment clos. Nous allons maintenant démontrer le théorème principal (VI.1). Le sens (inclu dans une extension de Liouville $\Longrightarrow G^0$ résoluble) ne nécessite que 2 lemmes, dont un lemme (le VI.7) sur la structure des groupes algébriques linéaires.

Lemme B.6.6. *Soit M une extension de Picard-Vessiot de K, et $N = M < z >$ une extension de M sans nouvelles constantes. Posons $L = K < z >$. Alors N est une extension de Picard-Vessiot de L et $G(N/L) \simeq L \check{\cap} M$ est un sous-groupe algébrique de $G(M/K)$.*

Démonstration : Si $M = K < u_1, \ldots, u_n >$, alors N est engendrée par les u_i sur L, et n'a pas de nouvelles constantes. Donc N est une extension de Picard-Vessiot de L. Le lemme VI.1 montre que tout K-automorphisme différentiel de N envoie M sur lui-même. D'où un homomorphisme de $G(N/L)$ dans $G(M/K)$ (la restriction). Si σ est un élément du noyau, σ laisse fixe M et L, donc aussi le corps engendré par $M \cup L$, c'est à dire N, d'où l'injectivité. Soit H l'image, H est algébrique par le théorème III.1 . De plus H laisse fixe $L \cap M$ exactement, par le théorème V.1. Donc $H = L \check{\cap} M$. □

Lemme B.6.7. *Soit G un sous-groupe de $GL_n(C)$, H un sous-groupe fermé de G. Supposons que ou bien (1) H est d'indice fini dans G, ou bien (2) $H \lhd G$ et G/H abélien. Si la composante connexe de l'identité dans H, H^0, est résoluble, Alors G^0 est résoluble.*

Démonstration :

(i) Montrons que G^0 est un sous-groupe d'indice fini dans G : $(G^0)^{-1} \subset G^0$ et, si $g \in G^0$, $gG^0 \subset G^0$ par connexité (intersection non vide). Donc G^0 est un sous-groupe de G. Par le corollaire III.1, G est réunion d'un nombre fini n de composantes connexes G_i (qui sont donc ouvertes et fermées). Soit $(x_i)_{i=1..n}$ une suite d'éléments de G, chacun dans une composante connexe. On a alors $G = \bigcup_{i=1}^n x_i G^0$, car $x_i^{-1} G_i$ ouvert fermé dans le connexe G^0. Donc G^0 est d'indice fini. Montrons que $H^0 = G^0$: $\bigsqcup_{x \in G/H} x = G$ donc $G^0 = \bigsqcup_{x \in G/H} (x \cap G^0)$ avec $H^0 = G^0 \cap H$. Donc, G/H étant fini, H^0 est fermé (car H l'est) ouvert (complémentaire d'une union finie de fermés) dans G^0 connexe.

(ii) G/H abélien entraîne $D(G) \subset H$. Or $G^0 \subset G$, donc $D(G^0) \subset H$. Par le lemme VI.4, $D(G^0)$ est connexe. Donc $D(G^0) \subset H^0$, ce qui entraîne G^0 résoluble. □

Théorème B.6.5. *Soit M une extension de Picard-Vessiot de K. Supposons $M \subset N$, où N est une extension de Liouville généralisée (suite d'extensions de types (1), (2), ou algébriques finies) de K, sans nouvelles constantes. Alors $G(M/K)^0$ est résoluble.*

Démonstration : On procède par récurrence sur le nombre d'étapes dans la chaîne de K à N.

Soit $K\!<\!u\!>$ la première étape. Alors par hypothèse de récurrence $G(M\!<\!u\!>/K\!<\!u\!>)^0$ est résoluble. Par le lemme VI.6, ce groupe est isomorphe au sous-groupe H de G correspondant à $K\!<\!u\!> \cap M$.

Supposons u algébrique sur K. Alors par le théorème de Dédekind, on sait que $\mathrm{Card}(\mathrm{hom}_{\mathrm{K-alg}}(\mathrm{K}\!<\!\mathrm{u}\!>, \mathrm{K}\!<\!\mathrm{u}\!>)) \leq [\mathrm{K}\!<\!\mathrm{u}\!>: \mathrm{K}]$. Or

$$G(K\!<\!u\!>/K) = \mathrm{Gal}_\partial(\mathrm{K}\!<\!\mathrm{u}\!>/\mathrm{K})$$

est inclus dans $\mathrm{hom}_{K-alg}(K\!<\!u\!>, K\!<\!u\!>))$, donc $\mathrm{Card}(G(K\!<\!u\!>/K))$ est fini. Par le théorème V.1.(2) ($L = M \cap K\!<\!u\!>$) $G/H \subset G(L/K)$. Donc H est d'indice fini.

Supposons u de la forme (1) ou (2). Par le lemme VI.2 ou VI.3, $K\!<\!u\!>$ est une extension de Picard-Vessiot de K avec un groupe de Galois commutatif. Donc tous les sous-corps différentiels sont normaux sur K. En particulier, $M \cap K\!<\!u\!>$ est normal, et $G(M \cap K\!<\!u\!>)$ est abélien. Dans les deux cas, le lemme VI.7 permet de conclure. □

La réciproque utilise tous les résultats démontrés aux paragraphes précédents du VI.

Théorème B.6.6. *Soit M une extension de Picard-Vessiot de K. Supposons que $G(M/K)^0$ est résoluble. Alors M peut être obtenue par une extension finie suivie d'une extension de Liouville.*

Démonstration : Soit $H = G(M/K)^0$, H est d'indice fini dans G par le 1 de la démonstration du lemme VI.7, et $L = \check{H}$ le corps intermédiaire associé. L est alors une extension finie, et $H = \check{L} = \check{\check{H}}$. Le fait que M est une extension de Liouville de L vient de l'enchaînement du théorème VI.2 et de la proposition VI.2. □

B.6.5 Application à l'équation de Riccati

(K,C) est un corps différentiel de caractéristique 0, et C est algébriquement clos. Pour $a \in K$ fixé, on étudiera l'équation de Riccati $\partial t = t^2 + a$, à partir de l'équation $\partial^2(y) + ay = 0$ (1). On notera M l'extension de Picard-Vessiot associée à (1).

Par la Correspondance de Galois (théorème V.2), étudier les sous K-extensions de M revient à étudier la structure de $G(M/K)$. Donc, pour démontrer la proposition VI.5, but de ce paragraphe, nous allons auparavant obtenir un résultat sur les sous-groupes algébriques de $SL_2(C)$.

Lemme B.6.8. *Soit G un sous-groupe de SL_2 (C). Si G est algébrique et G^0 est résoluble, ou bien G est fini, ou bien G^0 est diagonalisable et [G:G^0]≤ 2, ou bien G est trigonalisable.*

Démonstration : Si G^0 est diagonalisable, ses éléments sont des matrices diagonales ayant pour coefficients a et a^{-1}. G^0 est fermé donc algébrique, donc G^0 verifie des équations polynômiales P_i. a est alors dans l'intersection des racines des P_i, qui est finie si les P_i sont non tous nuls.
Si G^0 est fini, G est fini car [G:G^0] fini (demonstration du lemme VI.7(1)). Sinon, G^0 est l'ensemble des matrices diagonales de $SL_2(C)$. Par un calcul identique à celui du théorème VI.2(3), les vecteurs propres de G^0 sont stables par G ($G^0 \lhd G$). Donc tout élément de G permute les vecteurs de la base ou les laissent fixes : [G:G^0]≤ 2.
Si G^0 n'est pas diagonalisable, G^0 est trigonalisable (théorème VI.2), donc G^0 a un unique sous-espace propre. Il est donc invariant par G. Donc G est trigonalisable. □

Théorème B.6.7. *Soit M l'extension de Picard-Vessiot de K pour l'équation $\partial^2(y)+ay = 0$ (1). Supposons que M est une extension finie de K suivi d'une extension de Liouville , mais n'est pas de dimention finie sur K. Alors l'équation $\partial t = t^2 + a$ a une solution dans une extension quadratique de K*

Démonstration : Le wronskien correspondant à l'équation (1) verifie $\partial W = 0$, donc

$$W \in C_M = C \subset K.$$

De plus, pour tout $\sigma \in G(M/K)$, $\sigma W = \det(\sigma) W$ (voir la démonstration du lemme III.4.(2)). Donc $\sigma \in K\langle \check{W} \rangle$ ($= \check{K}$ ici) si et seulement si $\sigma \in SL_2(C)$. Donc $G = G(M/K)$ est un sous-groupe de $SL_2(C)$. De plus, G^0 est resoluble par le théorème VI.1
$[M : K]$ est infini donc G fini est exclu. Dans les deux autres cas du lemme précédent, il existe une extension quadratique L de K telle que $\check{L}$ soit trigonalisable. Donc il existe une solution u non nulle de (1) telle que : $\forall \sigma \in \check{L} \sigma(u) = c_\sigma u$, où $c_\sigma \in C$. Donc $\frac{\partial u}{u}$ appartient à L, car M est normale sur L. Posons $t = -\frac{\partial u}{u}$, t vérifie alors l'équation de Riccati. D'où le théorème. $\square$

Il existe une généralisation de la théorie que nous avons présentée aux équations aux dérivées partielles. Celle-ci est développée dans [Pom83], les groupes algébriques linéaires étant remplacés par des "semi-groupes de Lie", mais ceci n'est plus du tout élémentaire.

Bibliographie

[AD99] F. Amoroso and S. David. Le problème de lehmer en dimension supérieure. In *J. reine angew. Math.*, volume 513, pages 145–179, 1999.

[BGS94] J.B. Bost, H. Gillet, and C. Soulé. Heights of projective varieties and positive green forms. In *J. American Math. Soc.*, volume 7, pages 903–1022, 1994.

[BM83] E. Bombieri and Mueller. On effectives measures of irrationnality for $\sqrt[r]{\frac{a}{b}}$ and related numbers. In *J.reine.angew.Math*, volume 342, 1983.

[BV83] E. Bombieri and J.D. Vaaler. On siegel's lemma. In *Inventiones mathematicae*, volume 73, pages 11–32, 1983.

[Dob79] E. Dobrowolski. On a question of lehmer and the number of irreductible factors of a polynomial. In *Acta Arith.*, volume 34, pages 391–401, 1979.

[EH00] D. Eisenbud and J. Harris. *The Geometry of Schemes*. Graduate Texts in Mathematics. Springer, 2000.

[EV84] H. Esnault and E. Viehweg. Dyson's lemma for polynomials in several variables (and the Theorem of Roth). In *Invent.Math.*, volume 78, pages 445–490, 1984.

[Fal91] G. Faltings. Diophantine approximation on abelian varieties. In *Annals of Math.*, volume 133, pages 549–576, 1991.

[Ful98] W. Fulton. *Intersection Theory*. Springer, seconde edition, 1998.

[Gor73] P. Gordan. Uber den *großten* gemeinsamen factor. In *Math. Annalen*, volume 7, pages 443–448, 1873.

[Har70] R. Hartshorne. *Ample subvarieties of algebraic varieties*. Lecture Notes in Mathematics. Springer, 1970.

[Har77] R. Hartshorne. *Algebraic geometry*. Graduate Texts in Mathematics. Springer, 1977.

[HS00] M. Hindry and J. Silvermann. *Diophantine Geometry : An introduction*. Graduate Texts in Mathematics. Springer, 2000.

[Hum75] J.E. Humphreys. *Linear Algebraic groups*. Springer, 1975.

[Jon93] J. De Jong. Ample line bundles and intersection theory. In B. Edixhoven et J.-H. Everste, editor, *Diophantine Approximation and Abelian Varieties*, Lecture Notes in Mathematics, pages 69–77. Springer, 1993.

[Kap76] I. Kaplansky. *An Introduction to differential algebra*. Hermann, 2^{de} edition, 1976.

[Kol48] E.R. Kolchin. Existence theorems connected with the picard-vessiot theory of homogenous linear ordinary differential equations. In *Bull.Amer.Math.Soc*, volume 54, pages 927–932, 1948.

[Kol96] J. Kollar. *Rationnal curves on algebraic varieties*. Springer, 1996.

[Lan78] S. Lang. *Cyclotomic Fields*, pages 190–204. Graduate Texts in Mathematics. Springer, 1978.

[Lan93] S. Lang. *Algebra*. Addison-Wesley, 3^e edition, 1993.

[LT65] Lubin-Tate. Formal complex multiplication in local fields. In *Annals of Mathematics*, volume 81, pages 380–387, 1965.

[Lub70] Lubin. *Introduction à la théorie des groupes formels*. Presses de l'Ens Ulm, 1970.

[Mat70] H. Matsumura. *Commutative algebra*. Benjamin, 1970.

[Mil99] J.S. Milne. Local class field theory. notes de cours sur internet, 1999.

[Mum99] D. Mumford. *The Red Book of Varietes and Schemes*. Lecture Notes in Mathematics. Springer, seconde edition, 1999.

[Nak95] M. Nakamaye. Dyson's lemma and a theorem of Esnault and Viehweg. In *Invent. Math.*, volume 121, pages 355–377, 1995.

[Nak99] M. Nakamaye. Intersection theory and diophantine approximation. In *J.Algebraic Geometry*, volume 8, pages 135–146, 1999.

[Neu99] J. Neukirch. *Algebraic Number Theory*. Grundlehren der mathematischen Wissenschaften. Springer, 1999.

[Phi86] P. Philippon. Lemmes de zéros dans les groupes algébriques commutatifs. In *Bull. Soc. Math. France*, volume 114, pages 355–383, 1986.

[Phi95] P. Philippon. Sur des hauteurs alternaltives iii. In *J. Maths. Pures Appl.*, volume 74, pages 345–365, 1995.

[Pom83] J.F. Pommaret. *Differential Galois theory*. Gordon and Breach, 1983.

[Ros68] R. Rosenlicht. Liouville's theorem on fonctions with elementary integrals. In *Pacific Journal of Mathematics*, volume 24, pages 153–161, 1968.

[SABK92] C. Soulé, D. Abramovich, J.-F. Burnol, and J. Kramer. *Lectures on Arakelov Geometry*, volume 33. Cambridge Stud. Adv Math, 1992.

[Sch91] W.M. Schmidt. *Diophantine approximations and diophantine equations*. Lecture Notes in Mathematics. Springer, 1991.

[Ser67] J.P. Serre. local class field theory. In Cassels et Frőhlich, editor, *Algebraic Number Theory*, pages 146–161. Thompson, 1967.

[Sin90] M.F. Singer. An outline of differential galois theory. In *Computer Algebra and Differential equations*, pages 3–18. Academic Press, 1990.

[Vaa79] J.D. Vaaler. A geometric inequality with applications to linear forms. In *Pacific J. Math*, volume 83, pages 543–553, 1979.

[Wei74] A. Weil. *Basic Number Theory*. Grundlehren der mathematischen Wissenschaften. Springer, 1974.