Faculté
des Sciences
Département de Mathématique

UMONS
Université de Mons

Existence de corps différentiellement clos rigides

UNE APPROCHE GÉOMÉTRIQUE ET MODÈLE THÉORIQUE.

Mémoire réalisé par Kimmo Lehtonen
pour l'obtention du diplôme de Master en sciences mathématiques

Service : Service de logique

Directeur : Quentin Brouette

Année académique 2022–2023

Faculté des Sciences ◆ Université de Mons ◆ Place du Parc 20 ◆ B-7000 Mons

Table des matières

Introduction

En français, le terme "rigide" est généralement utilisé pour décrire un objet qui n'est pas déformable, c'est-à-dire qu'il conserve sa forme et sa structure initiale. Lorsque nous appliquons cette notion à des structures mathématiques, nous cherchons à traduire cette idée de stabilité.

Prenons $\mathcal{M}$ une structure d'une théorie quelconque. Dans ce contexte, nous dirons que $\mathcal{M}$ est rigide si son groupe d'automorphismes est trivial, c'est-à-dire si le seul automorphisme de $\mathcal{M}$ est l'identité. Autrement dit, il n'existe aucun automorphisme de $\mathcal{M}$ qui modifie sa structure ou ses propriétés de manière significative. La rigidité de $\mathcal{M}$ signifie donc qu'il n'y a pas de déformations ou de transformations non triviales possibles sur cette structure.

Par exemple dans le cas d'un groupe G, le groupe des automorphismes de G sera le groupe des automorphismes *de groupes* de G. Les seuls groupes rigides sont le groupe trivial et le groupe d'ordre 2. La problématique des modèles rigides est vite résolue dans cette catégorie.

Enrichissons la structure $\mathcal{M}$ et plongeons-la dans la théorie des corps (commutatifs). Nous considérons ici les morphismes *de corps*. Considérons un corps K et son corps premier k (e.g. $\mathbb{Q}$ si K est de caractéristique 0). Puisqu'un élément de $\mathrm{Gal}(K/k)$ est un automorphisme de K et que réciproquement un automorphisme de K doit forcément fixer k, un corps K est rigide si et seulement si son groupe de Galois sur k est trivial. Nous avons une multitude d'exemples et non exemples de modèles rigides dans cette catégorie.

Exemple.

- Le corps premier k est rigide : son groupe de Galois est trivial.
- Le corps $\mathbb{Q}(\sqrt{2})$ n'est pas rigide car $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \langle \sigma \rangle$ où σ envoie $\sqrt{2}$ sur son conjugué $-\sqrt{2}$.
- Toute extension galoisienne sur k de degré $\geqslant 2$ n'est pas rigide.
- Le corps $\mathbb{Q}(\sqrt[3]{2})$ est rigide car le polynôme $X^3 - 2$ n'a qu'une seule racine dans $\mathbb{Q}(\sqrt[3]{2})$ et donc $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ est réduit à l'identité.
- Le corps des réels.
- Un corps algébriquement clos n'est jamais rigide.

Nous allons maintenant aborder l'un des cadres de ce mémoire. Enrichissons encore la structure de $\mathcal{M}$ et munissons-la désormais d'une fonction unaire ∂ appelée *dérivée* qui vérifie les axiomes suivants :

- pour tous $m,n \in M$, $\partial(m+n) = \partial(m) + \partial(n)$;
- pour tous $m,n \in M$, $\partial(mn) = \partial(m)n + m\partial(n)$.

Nous dirons que $\mathcal{M}$ un corps *différentiel*. Les morphismes de la catégorie des corps différentiels sont les morphismes de corps qui commutent avec la dérivée. Une remarque fondamentale est que tout corps, muni de la dérivée triviale $\partial : M \to M : x \mapsto 0$, est un corps différentiel. Nous pouvons alors nous attendre à ce que ces deux théories se comportent de façon similaire.

Nous dirons que $\mathcal{M}$ est *différentiellement clos* s'il vérifie pour tous polynômes différentiels f et g à coefficients dans M, avec $\mathrm{ord}(f) > \mathrm{ord}(g)$, l'existence d'un élément $x \in M$ tel que $f(x) = 0$ et $g(x) \neq 0$. Un tel corps est forcément algébriquement clos.

Contrairement aux corps algébriquement clos, D. Marker a montré récemment dans [4] qu'il existe des corps différentiellement clos rigides. Ce travail visera, en particulier, à construire de telles structures.

En particulier, un corps différentiellement clos rigide doit satisfaire une propriété qui n'est jamais vérifiée dans le cas de la théorie des corps algébriquement clos. Nous dirons que $L \supseteq M$ est une clôture différentielle de M si L est un corps différentiellement clos qui se plonge dans tout corps différentiellement clos dans lequel M se plonge. D. Marker a montré la proposition suivante, que nous prouverons également dans le cadre de ce mémoire :

Proposition 1. Soit K un corps différentiel et L une clôture différentielle de K telle que $K \neq L$. Il existe un automorphisme *différentiel* de L/K non trivial.

Cette proposition est vraie dans le cas des corps algébriquement clos. En fait, si L est un corps algébriquement clos, nous pouvons toujours trouver un sous-corps propre K tel que L est la clôture algébrique de K. Le théorème d'Artin-Schreier (1927) dit en particulier que pour tout corps algébriquement clos L, il existe un corps K tel que $L = K(i)$. Une question que nous pouvons nous poser est la suivante :

Pour tout corps différentiellement clos L, existe-t-il un sous-corps différentiel propre K tel que $L = K(i)$?

Comme il existe effectivement des corps différentiellement clos rigides, la réponse est clairement **non**. Cette proposition met en évidence une propriété spécifique de la théorie des corps algébriquement clos qui la différencie de celles des corps différentiellement clos. En effet, un corps différentiellement clos n'est pas nécessairement la clôture différentielle d'un sous-corps différentiel propre.

Dans ce travail, nous nous appuierons sur les travaux de Marker tels qu'ils sont exposés dans [4]. Les constructions de corps différentiellement clos rigides que nous examinerons reposent sur des ensembles définissables spécifiques que nous présenterons : les ensembles de Rosenlicht et les noyaux de Manin. L'idée centrale de ces constructions est de créer un corps différentiellement clos qui possède une propriété remarquable : pour tout élément $a \in K$, il induit un ensemble définissable D_a et pour tout élément distinct $b \in K$, le corps K vérifie $|D_a(K)| \neq |D_b(K)|$. Cette condition garantit qu'un automorphisme de K ne peut pas envoyer a sur b.

Afin de mieux comprendre ces outils, nous aborderons la géométrie algébrique et la théorie des modèles. En effet, les noyaux de Manin sont définis à partir de courbes elliptiques et leurs propriétés sont établies à l'aide des techniques de la théorie des modèles. Ainsi, nos constructions seront le fruit d'une combinaison de la géométrie algébrique et de la théorie des modèles. De plus, nous mènerons une étude plus ou moins approfondie des corps différentiellement clos, par le point de vue de la théorie des modèles.

Échauffement

Mettons-nous en route et commençons par montrer les quelques résultats que nous venons d'avancer.

Lemme. Les seuls groupes rigides sont le groupe trivial et le groupe $\mathbb{Z}/2\mathbb{Z}$.

Démonstration. La seule application définissable sur $G = \{1_G\}$ est l'identité et donc c'est forcément un groupe rigide.

Soit G un groupe rigide d'ordre plus grand ou égal à 2. Premièrement, un tel groupe doit être abélien car sinon il y aurait une conjugaison non triviale. En effet, supposons au contraire qu'il existe un élément $h \in G \setminus Z(G)$ et considérons la conjugaison $g \mapsto hgh^{-1}$, c'est un automorphisme de G non trivial car il existe un élément $g_0 \in G$ tel que $g_0 h \neq hg_0$, c'est-à-dire que $g_0 \neq hg_0h^{-1}$. Ensuite, tout élément doit être d'ordre au plus 2 car sinon l'endomorphisme $g \mapsto g^{-1}$ est un automorphisme non trivial (un groupe qui satisfait cette condition est forcément abélien car $gh = g^{-1}h^{-1} = (hg)^{-1} = hg$). Ainsi, un groupe rigide est un $\mathbb{F}_2$-espace vectoriel, en définissant la multiplication scalaire par $n \cdot g = g^n$, pour $n \in \mathbb{F}_2$ et $g \in G$. De plus, sa dimension en tant que $\mathbb{F}_2$-espace vectoriel doit être 1 car sinon nous pouvons construire un automorphisme non trivial en échangeant deux éléments d'une base de G. Nous en concluons que $G = \mathbb{Z}/2\mathbb{Z}$. De plus ce groupe est bien rigide car le groupe des matrices inversibles est réduit à $\{(1)\}$. □

Lemme. Tout sous-corps euclidien de $\mathbb{R}$ est rigide.

Démonstration. Soient S un sous-corps euclidien de $\mathbb{R}$ et σ un automorphisme de S. Nous allons montrer que σ est trivial (mis à part la dernière proposition bien sûr).

Premièrement, montrons que σ doit forcément être compatible avec l'ordre. Puisque σ est un morphisme de corps injectif $\sigma(x) = 0$ si et seulement si $x = 0$. De plus, comme S est euclidien, tout élément positif de S est un carré. Ainsi pour $x > 0$ dans S, il existe $y \in S$ tel que $x = y^2$. Alors $\sigma(x) = \sigma(y^2) = \sigma(y)^2 > 0$. Pour $x, y \in S$ tels que $x > y$, puisque $x - y > 0$, nous obtenons que $\varphi(x-y) > 0$, c'est-à-dire que $\varphi(x) > \varphi(y)$.

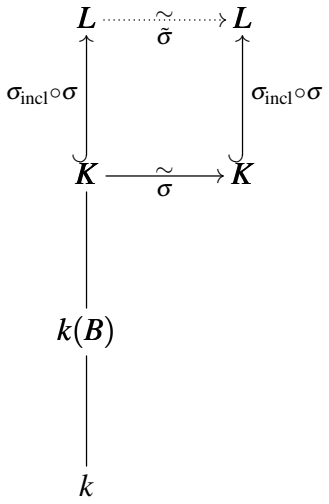
Montrons maintenant que $\varphi(x) = x$ pour tout $x \in S$. Supposons par l'absurde, et sans perdre de généralité, qu'il existe un $x \in S$ tel que $\varphi(x) > x$ (sinon prendre $-x$). Comme $\mathbb{Q}$ est dense dans S, il existe un rationnel q tel que $\varphi(x) > q > x$. Or σ fixe $\mathbb{Q}$ et donc en appliquant φ à $q > x$, nous obtenons que $\varphi(x) > q > \varphi(x)$, une contradiction. □

Proposition. Tout corps algébriquement clos possède un automorphisme non trivial.

Prouvons cette proposition d'abord dans le cas de caractéristique nulle.

Démonstration. Soit L un corps algébriquement clos et k son corps premier. Soit B une base de transcendance de L sur k.

L'extension $L/k(B)$ est algébrique, de plus, le corps $k(B)$ n'est pas algébriquement clos car nous n'avons ajouté aucun élément algébrique. Il existe donc x un élément de L algébrique sur $k(B)$ qui n'est pas dans $k(B)$. Soit P_x le polynôme minimal de x sur $k(B)$ et considérons K le corps de décomposition de P_x sur $k(B)$. Alors l'extension $K/k(B)$ est galoisienne de degré strictement supérieur à 1 et donc il existe σ un automorphisme de corps de K non trivial qui fixe $k(B)$. Soit σ_{incl} le morphisme d'inclusion de K dans L.



Par le théorème d'extension de plongements, puisque $\sigma_{\text{incl}} \circ \sigma$ est un plongement de corps de K dans L et que L est algébrique sur K, il existe un plongement de corps $\tilde{\sigma} : L \to L$ tel que $\tilde{\sigma}_{|K} = \sigma$. Comme σ est non trivial sur K, le morphisme $\tilde{\sigma}$ est non trivial. De plus, c'est un automorphisme car c'est un plongement de L dans lui-même. □

Par exemple, pour $\mathbb{C}$ nous pouvons regarder le morphisme $\sigma : \mathbb{C} \to \mathbb{C}$ défini par $\sigma(a+bi) = a-bi$. C'est l'automorphisme de corps de $\mathbb{C}$ qui fixe $\mathbb{R}$ et qui envoie i sur son conjugué $-i$. Remarquons que l'extension $\mathbb{C}/\mathbb{R}$ est galoisienne.

Remarque. Il existe une multitude de façons de créer des automorphismes non triviaux. Si la base de transcendance B a au moins deux éléments distincts, nous pouvons construire une fonction qui échange ces deux éléments et l'étendre au corps algébriquement clos. De façon analogue, si la base B a au moins un élément t, nous pouvons considérer $\sqrt{t}$ qui est algébrique sur $k(B)$.

Remarque. Si $car(k) = p$, avec p premier, il nous suffit de choisir un bon x tel que le degré du polynôme minimal de x sur $k(B)$ ne soit pas divisible par p. Pour cela, nous pouvons considérer l'extension de corps $\mathbb{F}_{p^n}(B)$ pour un naturel $n > 1$ qui n'est pas divisible par p et prendre un élément primitif x de $\mathbb{F}_{p^n}(B)$ sur $\mathbb{F}_p(B)$.

Chapitre I

Géométrie algébrique

Nous cherchons à étudier l'ensemble des zéros de polynômes. Ces ensembles peuvent représenter des objets géométriques comme le cercle unité, en prenant l'ensemble des solutions de l'équation $x^2 + y^2 = 1$.

I.1 Anneau noethérien

Avant d'entrer dans ce qui est appelé la géométrie algébrique, il nous faut savoir quelques propriétés fondamentales sur les anneaux commutatifs.

Tout au long du mémoire, lorsque nous parlerons d'anneau ou de corps, il s'agira toujours sauf mention contraire, d'anneau ou de corps commutatif. Nous nous plaçons dans ce cadre commutatif car sinon ces structures n'auraient pas toujours des bonnes propriétés. Par exemple, pour un polynôme à une variable de degré n, lorsque nous avons la commutativité, nous avons au plus de n solutions. Par contre, si A est un anneau non commutatif et $a \in A$ est une racine du polynôme $P(X) = X^n - 1 \in A[X]$, alors pour tout $b \in A$ qui ne commute pas avec a, bab^{-1} est une racine distincte de a, ainsi nous n'aurons pas un très bon contrôle sur le nombre des racines.

Plaçons-nous donc dans un anneau (commutatif) A de caractéristique quelconque.

Définition I.1. On dit que A est **noethérien** s'il vérifie la condition de chaîne ascendante sur ses idéaux, c'est-à-dire que toute suite croissante d'idéaux de A est stationnaire au sens de l'inclusion ensembliste.

Exemple I.2.

- Tout corps K est noethérien car les seuls idéaux sont $\{0\}$ et K. Ainsi, dans ce contexte, les chaînes d'idéaux de K ont au plus deux éléments distincts et donc sont forcément stationnaires.

- Un exemple d'anneau non noethérien est celui de l'anneau des polynômes à une infinité de variables sur un corps. Il nous suffit de regarder pour tout naturel n les idéaux $I_n = (X_1, \dots, X_n)$ et $I_0 = \{0\}$. La suite des idéaux $(I_n)_{n\in\mathbb{N}}$ forme une chaîne croissante non stationnaire.

Cette première définition d'anneau noethérien nous accompagnera plus loin dans ce chapitre. Nous pouvons la formuler autrement, ce qui nous sera également très utile par la suite.

Lemme I.3. *A est noethérien si et seulement tout idéal de A est finiment engendré.*

Démonstration. Nous souhaitons montrer que A est noethérien si et seulement si pour tout idéal $I \subseteq A$, il existe $a_1, \dots, a_n \in I$ tels que $I = (a_1, \dots, a_n)$.

Supposons par contraposée qu'il existe un idéal $I \subseteq A$ qui n'est pas finiment engendré, montrons alors que A n'est pas noethérien. Par hypothèse sur I, nous pouvons trouver une suite d'éléments $a_1, \dots, a_n, \dots \in I$ telle que pour tout naturel non nul n, nous ayons $(a_1, \dots, a_n) \neq I$. Nous obtenons une suite strictement croissante d'idéaux de A non stationnaire :

$$(a_1) \subseteq (a_1, a_2) \subseteq \dots \subset (a_1, \dots, a_n) \subseteq \dots \neq I.$$

Puisque A ne vérifie pas la condition de chaîne ascendante, nous en déduisons que A n'est pas noethérien.

Réciproquement, supposons maintenant que tout idéal de A est finiment engendré. Soit $(I_n)_{n\in\mathbb{N}}$ une chaîne ascendante d'idéaux de A. Nous voulons montrer que cette chaîne est constante à partir d'un certain rang. Posons

$$J = \bigcup_{n\in\mathbb{N}} I_n.$$

Puisque les I_n sont emboîtés, l'ensemble J est un idéal de A et donc finiment engendré : il existe $a_1, \dots, a_m \in A$ tels que $J = (a_1, \dots, a_m)$. De plus, pour tout $1 \leqslant i \leqslant m$, comme $a_i \in J$, il existe un rang n_i tel que $a_i \in I_{n_i}$ pour un certain idéal de la chaîne. Soit $n_0 = \max\{n_1, \dots, n_m\}$, alors pour tout $n \geqslant n_0$, nous avons que :

$$(a_1, \dots, a_m) = (\{a_1, \dots, a_m\}) \subseteq I_n \subseteq J = (a_1, \dots, a_m).$$

Donc $I_n = J$ pour tout $n \geqslant n_0$: la chaîne est donc stationnaire. □

Exemple I.4. Dans un anneau principal, tout idéal est engendré par un seul élément et donc finiment engendré. Ainsi, tout anneau principal est noethérien. En particulier $\mathbb{Z}$ et $K[X]$ (pour un corps K) sont des anneaux noethériens.

Nous avons une autre propriété intéressante sur les anneaux noethérien :

Lemme I.5. *Si A est noethérien, alors tout ensemble non vide d'idéaux de A admet un élément maximal pour l'inclusion.*

Démonstration. Par contraposée, supposons qu'il existe un ensemble M non vide d'idéaux sans élément maximal. Prenons I_0 n'importe quel élément de M. En particulier I_0 n'est pas maximal, et donc il existe $I_1 \in M$ tel que $I_0 \subseteq I_1$ et $I_0 \neq I_1$. En répétant cet argument, nous construisons une chaîne d'idéaux strictement croissante et non stationnaire, ce qui contredit que A soit noethérien. □

C'est en fait une équivalence, mais ce qui nous intéresse ici est l'implication.

La propriété de noethérianité d'un anneau est intéressante car elle se transfère à son anneau des polynômes, contrairement aux anneaux principaux [1]. C'est l'objet du théorème suivant :

Théorème I.6 (Théorème de la base de Hilbert)**.** *Si A est noethérien, alors $A[X]$ est noethérien.*

Démonstration. Soit I un idéal de $A[X]$. Montrons que I est finiment engendré. C'est une preuve plutôt algorithmique.

Cas de base : prenons f_1 un élément de I de degré minimal.

Pas de récurrence : si $(f_1,\dots,f_n) = I$, alors I est finiment engendré et c'est terminé. Sinon, $(f_1,\dots,f_n) \neq I$, prenons $f_{i+1} \in I \setminus (f_1,\dots,f_n)$ de degré minimal.

Nous voulons montrer que cet algorithme se termine toujours. Supposons au contraire qu'il ne s'arrête pas. Alors, nous avons une chaîne ascendante d'idéaux de la forme $(f_1) \subseteq (f_1,f_2) \subseteq \dots \subseteq (f_1,f_2,\dots)$ avec $f_i \in A[X]$. Notons a_j le coefficient de la plus grande puissance de f_j. La suite $(a_1) \subseteq (a_1,a_2) \subseteq \dots (a_1,a_2,\dots) \subseteq A$ est une chaîne ascendante d'idéaux de A. Puisque A est noethérien, la chaîne est stationnaire et nous avons $(a_1,a_2,\dots) = (a_1,a_2,\dots,a_m)$ pour un certain $m \in \mathbb{N} \setminus \{0\}$. Montrons alors que $I = (f_1,\dots,f_m)$. Si ce n'est pas le cas, prenons $f_{m+1} \in I \setminus (f_1,\dots,f_m)$. Le coefficient de sa plus grande puissance a_{m+1} peut alors s'écrire comme un élément de $(a_1,\dots,a_m)$:

$$a_{m+1} = \sum_{j=1}^{m} u_j a_j$$

avec $u_j \in A$.

Posons

$$g(X) = \sum_{j=1}^{m} u_j f_j(X) X^{\deg f_{m+1} - \deg f_j}.$$

Les exposants de g sont $\geqslant 0$ car $\deg f_{m+1} \geqslant \deg f_j$. De plus $g \in (f_1,\dots,f_m)$ et a le même degré et coefficient dominant que f_{m+1}.

1. En fait, l'anneau $A[X]$ est principal si et seulement si A est un corps.

Or, comme $f_{m+1} \notin (f_1, \ldots, f_m)$, nous avons que $f_{m+1} - g \notin (f_1, \ldots, f_m)$ (sinon $f_{m+1} - g + g = f_{m+1} \in (f_1, \ldots, f_m)$.). Cependant $f_{m+1} - g$ est de degré inférieur à f_{m+1} car la plus grande puissance de f_{m+1} et de g ont le même coefficient, ce qui mène à une contradiction avec la minimalité du degré de f_{m+1}. Nous en déduisons qu'un tel élément f_{m+1} n'existe pas et donc que notre algorithme se termine.

□

Corollaire I.7. *Soit $n \in \mathbb{N}$. Si A est noethérien, alors $A[X_1, \ldots, X_n]$ est noethérien.*

Démonstration. Par induction sur n, comme c'est déjà vérifié pour le cas de base $n = 0$, il suffit de montrer que pour tout naturel k, si $A[X_1, \ldots, X_k]$ est noethérien alors $A[X_1, \ldots, X_{k+1}]$ est noethérien. Appliquons le théorème précédent avec l'anneau $A[X_1, \ldots, X_k]$, nous obtenons que $A[X_1, \ldots, X_k][X_{k+1}]$ est noethérien. Or $A[X_1, \ldots, X_k][X_{k+1}]$ et $A[X_1, \ldots, X_{k+1}]$ sont isomorphes et donc $A[X_1, \ldots, X_{k+1}]$ est aussi noethérien. □

Remarque I.8. Ce corollaire nous sera vital plus loin dans ce chapitre. Il nous dit en particulier que, pour un corps K, tout idéal de $K[X_1, \ldots, X_n]$ est finiment engendré.

Remarque I.9. Cette propriété de transfert est fausse en général pour les anneaux principaux : si A est principal, $A[X]$ n'est pas toujours principal. Par exemple pour un corps K, l'anneau $K[X]$ est principal mais $K[X, Y]$ ne l'est pas : l'idéal (X, Y) ne peut pas être engendré par un seul élément de $K[X, Y]$.

I.2 Ensembles algébriques affines

Le reste de ce chapitre se base sur le livre [7] de D. Perrin. Ainsi, les principaux résultats de ce chapitre se retrouveront dans cet ouvrage. Nous agrémenterons l'expédition d'exemples, de détails ou encore de quelques autres résultats qui nous intéressent plus particulièrement.

Soient K un corps de caractéristique quelconque et n un naturel non nul. Nous allons étudier les zéros d'ensembles de polynômes.

Définition I.10. Soit S un sous-ensemble de $K[X_1, \ldots, X_n]$. On définit $V(S)$ l'**ensemble algébrique affine défini par** S le sous-ensemble de K^n donné par :

$$V(S) = \{x \in K^n : \forall P \in S, P(x) = 0\}.$$

Exemple I.11. L'ensemble vide et K^n tout entier sont des ensembles algébriques affines. En effet, on a $V(\{1\}) = \varnothing$ et $V(\{0\}) = K^n$.

On appelle K^n l'espace affine de dimension n sur K. Nous noterons parfois $\mathbb{A}^n(K)$ cet ensemble algébrique affine.

Exemple I.12.

- Pour $n = 1$, les ensembles algébriques affines de la droite K sont la droite et les ensembles finis. En effet, s'il existe $P \in S$ de degré $d \geqslant 1$, alors P a au plus d racines et donc $V(S)$ a au plus d éléments. Sinon tous les éléments de S sont de degré $\leqslant 0$ et nous avons que $V(S) = \varnothing$ si l'un des éléments de S est non nul, et $V(S) = K$ si $S = \{0\}$.
- Pour $n = 2$, les ensembles algébriques sont le plan, l'ensemble vide, les ensembles finis des points du plan et les courbes. Par exemple $V(\{X^2 + Y^2 - 1\})$ est le cercle unité dans le plan pour la norme euclidienne en prenant $K = \mathbb{R}$.
- Soit $K = \mathbb{R}$. Considérons $SL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : det(A) = 1\}$ l'ensemble des matrices inversibles à coefficients dans $\mathbb{R}$ de taille $n \times n$ dont le déterminant est égal à 1. Cet ensemble est un ensemble algébrique affine dans $\mathbb{R}^{n^2}$ car le déterminant est une application polynomiale : un élément $A \in SL_n(\mathbb{R})$, vu en tant que vecteur dans $\mathbb{R}^{n^2}$, est une racine du polynôme $det(X_1, \ldots, X_{n^2}) - 1 \in \mathbb{R}[X_1, \ldots, X_{n^2}]$. Nous avons donc que

$$SL_n(\mathbb{R}) = V(\{det(X_1, \ldots, X_{n^2}) - 1\}).$$

Remarque I.13. Les propriétés du corps K jouent un rôle important dans la définition des ensembles algébriques affines. Par exemple, considérons l'ensemble algébrique affine $V = V(\{X^2 + Y^2 + 1\})$. Vu dans $\mathbb{R}^2$, l'ensemble V est vide car l'équation $X^2 + Y^2 = -1$ n'a pas de solutions dans $\mathbb{R}^2$, par contre si nous nous plaçons dans $\mathbb{C}$, nous obtenons une infinité de solutions et donc V est infini dans $\mathbb{C}^2$.

Remarque I.14. Soient S et $S' \subseteq K[X_1, \ldots, X_n]$. Si $S \subseteq S'$, alors $V(S) \supseteq V(S')$. Nous pouvons voir V comme une application décroissante de $\mathcal{P}(K[X_1, \ldots, X_n])$ dans $\mathcal{P}(K^n)$.

Une propriété fondamentale des ensembles algébriques affines est celle énoncée dans la proposition suivante. Elle nous permet de nous cantonner seulement aux idéaux de l'anneau $K[X_1, \ldots, X_n]$ et même à un nombre fini de polynômes.

Avant de l'énoncer, rappelons-nous que par la remarque I.8, tout idéal I de $K[X_1, \ldots, X_n]$ est finiment engendré, c'est-à-dire que I peut s'écrire sous la forme $I = (f_1, \ldots, f_m)$ avec $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$.

Proposition I.15. *Soit $S \subseteq K[X_1, \ldots, X_n]$ et (S) l'idéal engendré par S dans $K[X_1, \ldots, X_n]$. Soit $I = (f_1, \ldots, f_m)$ un idéal de $K[X_1, \ldots, X_n]$. L'application V vérifie :*

i. $V(S) = V((S))$.

ii. $V(I) = V(\{f_1, \ldots, f_m\}) = V(f_1) \cap V(f_2) \cap \cdots \cap V(f_m)$.

Démonstration. i. Par la remarque I.14, comme $S \subseteq (S)$, nous avons déjà que $V(S) \supseteq V((S))$. Montrons l'autre inclusion. Soit $x \in V(S)$. Soit $Q \in (S)$, nous pouvons écrire Q sous la forme

$$Q(X) = \sum_{P \in S'} Q_P(X)P(X),$$

avec $S' \subseteq S$ fini et $Q_P \in K[X_1, \dots X_n]$ pour tout $P \in S'$. Or, puisque $x \in V(S)$, pour tout $P \in S$, l'élément x vérifie que $P(x) = 0$, nous avons alors

$$Q(x) = \sum_{P \in S'} Q_P(x)P(x) = \sum_{P \in S'} Q_P(x).0 = 0,$$

et donc $x \in V((S))$.

ii. La première égalité découle du point i avec $S = \{f_1, \dots, f_m\}$ et $(S) = I$. La seconde égalité est issue de l'équivalence entre l'intersection dans la théorie des ensembles et le symbole $\wedge$ dans le langage : $E \cap F = \{x : x \in E \wedge x \in F\}$. □

Remarque I.16. Si V est un ensemble algébrique affine de la forme $V(f)$ pour un certain $f \in K[X_1, \dots, X_n]$, on dit que V est une hypersurface. Nous pouvons reformuler la proposition précédente : tout ensemble algébrique affine est une intersection finie d'hypersurfaces.

Proposition I.17. *Soit $J \subseteq \mathbb{N}$ un ensemble quelconque d'indices. Pour tout $i \in \mathbb{N}$, soit $S_i \subseteq K[X_1, \dots, X_n]$.*

i.
$$\bigcap_{j \in J} V(S_j) = V(\bigcup_{j \in J} S_j).$$

ii.
$$\bigcup_{i=1}^{m} V(S_i) = V(\prod_{i=1}^{m} S_i).$$

Démonstration. i. Soit $x \in K^n$. Nous avons que $x \in \bigcap_{j \in J} V(S_j)$ si et seulement si pour tout $j \in J$, l'élément x appartient à $V(S_j)$, c'est-à-dire que pour tout $P \in S_j$, l'égalité $P(x) = 0$ est vérifiée. Cela revient à dire que x annule tous les polynômes dans $\bigcup_{j \in J} S_j$ et donc que $x \in V(\bigcup_{j \in J} S_j)$.

ii. Vérifions le cas $m = 2$. Soit $x \in V(S_1) \cup V(S_2)$. Si $x \in V(S_1)$, alors pour tout $P_1 \in S_1, P_1(x) = 0$. Ainsi pour tout $P_2 \in V(S_2), P_1(x)P_2(x) = 0$ et donc $x \in V(S_1S_2)$. L'argument pour $x \in V(S_2)$ est identique.

Réciproquement, soit $x \in V(S_1S_2)$. Supposons que $x \notin V(S_1)$. Alors il existe $P \in S_1$ tel que $P(x) \neq 0$. Or pour tout $P_2 \in S_2$, l'élément x vérifie $P(x)P_2(x) = 0$ et donc par intégrité de K, $P_2(x) = 0$ et ainsi $x \in V(S_2)$. Le même argument fonctionne pour montrer que si $x \notin V(S_2)$, alors $x \in V(S_1)$. Ainsi x est forcément dans $V(S_1)$ ou $V(S_2)$, c'est-à-dire que $x \in V(S_1) \cup V(S_2)$.

Pour le cas général, il suffit de se reporter au cas $m = 2$ pour des ensembles S_i bien choisis.

□

Remarque I.18. En particulier, cette proposition nous dit qu'une intersection quelconque d'ensembles algébriques affines est toujours un ensemble algébrique affine, et que toute union finie d'ensembles algébriques affines est un ensemble algébrique affine.

Proposition I.19. *Les ensembles algébriques affines sont les fermés d'une topologie sur K^n.*

Démonstration. Les ensembles $\varnothing$ et K^n sont des fermés par l'exemple I.11. Par la proposition précédente et sa remarque, les ensembles algébriques affines sont stables par union finie et par intersection quelconque. □

Définition I.20. On appelle cette topologie la topologie de Zariski [2].

Remarque I.21. La topologie de Zariski est une topologie assez différente de celles rencontrées dans le cadre de l'analyse classique, par exemple des espaces métriques. Un espace métrique est forcément séparé ce qui n'est pas le cas pour la topologie de Zariski.

Exemple I.22. Regardons l'espace affine $\mathbb{A}^1(K)$ muni de la topologie de Zariski. Alors cette topologie est exactement la topologie cofinie. En effet, dans l'exemple I.12, nous avons vu que les fermés sont K et les ensembles finis. Puisque les ouverts sont les complémentaires des fermés, les ouverts sont les ensembles cofinis (ou K).

Plus généralement sur $\mathbb{A}^n(K)$, la topologie de Zariski est plus fine que la topologie cofinie car tout ensemble fini est un fermé de Zariski. Un élément $x = (x_1, \ldots, x_n) \in K^n$ induit un ensemble algébrique affine avec $\{x\} = V(X_1 = x_1, \ldots, X_n = x_n)$. Puisque toute union finie d'ensembles algébriques affines est un ensemble algébrique affine, tout ensemble fini est un ensemble algébrique affine. En particulier, les ensembles cofinis de $\mathbb{A}^n(K)$ sont des ouverts pour la topologie de Zariski.

2. Le nom vient du mathématicien Oscar Zariski très influent dans le domaine de la géométrie algébrique au 20ème siècle.

Remarque I.23. Par la remarque I.16, les hypersurfaces forment une base des fermés pour la topologie de Zariski, par conséquent leurs complémentaires forment une base pour les ouverts. Ainsi tout ouvert est une union finie d'ensembles de la forme $K^n \setminus V(F)$ avec $F \in K[X_1,\dots,X_n]$.

I.3 Idéal d'un ensemble algébrique affine

Nous nous sommes intéressés à une certaine opération : celle qui pour un ensemble quelconque de polynômes dans $K[X_1,\dots X_n]$ rend tous les éléments qui s'annulent en chacun de ses polynômes. Nous allons maintenant essayer de faire l'opération l'inverse : pour un ensemble de points de K^n, nous allons regarder les polynômes qui s'annulent en chacun de ces points.

Définition I.24. Soit V un sous-ensemble de K^n. On définit $I(V)$ l'**idéal de V** le sous-ensemble de $K[X_1,\dots,X_n]$ donné par :

$$I(V) = \{f \in K[X_1,\dots,X_n] : \forall x \in V, f(x) = 0\}.$$

La philosophie derrière est de trouver une application *inverse* à l'application V définie précédemment et ainsi avoir une correspondance biunivoque entre les ensembles algébriques affines, et les idéaux des ensembles algébriques affines. Malheureusement, ce ne sera pas aussi simple et nous n'aurons pas toujours $I = I(V(I))$ pour un idéal quelconque I de $K[X_1,\dots,X_n]$.

Remarque I.25.

- Pour un ensemble quelconque $V \subseteq K^n$ nous avons bien, comme son nom l'indique, que $I(V)$ est un idéal. En effet, si P et $Q \in I(V)$, alors pour tout $x \in V$, nous avons $P(x) = Q(x) = 0$ et donc $P(x) + Q(x) = 0$ d'où $P+Q \in I(V)$. De plus, pour tout polynôme $R \in K[X_1,\dots,X_n]$, nous avons $R(x)P(x) = R(x).0 = 0$, ainsi $R.P \in I(V)$.
- L'application I est décroissante et va de $\mathcal{P}(K^n)$ dans $\mathcal{P}(K[X_1,\dots,X_n])$.
- Nous avons $I(\varnothing) = K[X_1,\dots,X_n]$.

Lemme I.26. *Pour K infini,* $I(K^n) = \{0\}$.

Démonstration. Raisonnons par récurrence sur n. Soit $n = 1$ et soit un polynôme non nul $P \in K[X]$. Alors P a au plus un nombre de racines égal à son degré. Comme K est infini, nous pouvons prendre un élément dans K qui n'annule pas P et donc $P \notin I(K)$. De plus, $0 \in I(K)$ car 0 s'annule en tout élément de K.

Par hypothèse de récurrence, supposons que nous avons pour tout $n \leqslant l$ la propriété $I(K^n) = \{0\}$. Soit $P \in K[X_1,\dots,X_l,X_{l+1}]$ un polynôme non nul. Mettons en évidence la variable X_{l+1}, nous nous retrouvons alors avec P de la forme :

$$P(X_1,\dots,X_l,X_{l+1}) = a_r(X_1,\dots,X_l)X_{l+1}^r + \cdots + a_0(X_1,\dots,X_l),$$

avec les $a_i(X_1,\dots,X_l) \in K[X_1,\dots,X_l]$ et $a_r(X_1,\dots,X_l)$ non nul. Par hypothèse de récurrence, comme $a_r(X_1,\dots,X_l) \neq 0$, il existe un élément $x = (x_1,\dots,x_l) \in K^l$ tel que $a_r(x_1,\dots,x_l) \neq 0$. Par conséquent $P(x_1,\dots,x_l,X_{l+1})$ a au plus r racines et n'est donc pas nul partout. Nous en déduisons que $P(X_1,\dots,X_l,X_{l+1})$ n'est pas nul. □

Par contre, si K est fini, alors il est de cardinalité une puissance d'un nombre premier p, disons $q = p^m$ pour un certain naturel m. Par le théorème de Lagrange, nous aurions que le polynôme $X^q - X$ s'annule sur tout K car pour tout $x \in K$, l'ordre de x divise q. C'est en fait une équivalence : $I(K^n) = \{0\}$ si et seulement si K est infini.

Remarque I.27. Ce lemme nous dit aussi que pour un ensemble quelconque S de $K[X_1,\dots,X_n]$, est vérifié $V(S) = K^n$ si et seulement si $S = \{0\}$. En effet, l'implication de droite à gauche est directe. Par contraposée, supposons que nous avons un polynôme $P \in S$ non nul. Alors $P \notin I(K^n) = \{0\}$ et donc il existe un élément x de K^n tel que $P(x) \neq 0$. Ainsi $x \notin V(S)$, nous en déduisons que $V(S) \neq K^n$.

Lemme I.28. *Si V est un ensemble algébrique affine, alors $V(I(V)) = V$.*

Démonstration. Comme V est un ensemble algébrique affine, il existe un idéal I de $K[X_1,\dots,X_n]$ tel que $V = V(I)$.

Nous avons que $V \subseteq V(I(V))$. En effet, si $x \in V$, alors x annule tout polynôme dans $I(V)$ par définition et donc $x \in V(I(V))$.

Réciproquement, nous avons $I \subseteq I(V(I)) = I(V)$ car si $P \in I$, comme $V = V(I)$, tout élément $x \in V$ annule le polynôme P et donc $P \in I(V(I))$. De plus, puisque V est une application décroissante, nous avons que $V = V(I) \supseteq V(I(V))$. □

Nous avons donc sur les ensembles algébriques affines $V \circ I = Id_{K^n}$. Les exemples qui suivent montrent que par contre, la fonction composée $I \circ V$ ne vérifie pas $I \circ V = Id_{K[X_1,\dots,X_n]}$ sur les idéaux de l'anneau des polynômes à n variables sur K.

Exemple I.29.

- Prenons un exemple où K n'est pas algébriquement clos, par exemple $K = \mathbb{R}$ et $n = 2$. Regardons $I = (X^2 + Y^2 + 1)$, comme nous en avons discuté auparavant, nous avons $V(I) = \varnothing$ et donc $I(V(I)) = I(\varnothing) = \mathbb{R}[X,Y]$. Ainsi,

$$I(V(I)) \neq I.$$

- Un autre problème qui peut surgir vient du fait que l'application V ne prend pas en compte les puissances. Prenons encore $K = \mathbb{R}$ et $n = 2$. Considérons cette fois $I = (X^2)$. Nous avons que $V(I) = \{(0,y) : y \in \mathbb{R}\}$ et $I(V(I)) = (X)$. Or $X \notin I$ et donc $I(V(I)) \neq I$.

Si nous demandons que K soit algébriquement clos, nous pouvons nous débarrasser du premier problème. Pour le second, nous allons étudier de plus près les liens entre I et $I(V(I))$ plus loin dans ce chapitre.

Ceci dit, même si nous n'avons pas toujours $I(V(I)) = I$, comme vu dans le lemme I.28, nous avons toujours l'inclusion $I \subseteq I(V(I))$.

Discussion I.30. Considérons le morphisme d'anneaux défini par

$$r : K[X_1, \ldots, X_n] \longrightarrow \mathcal{F}(V, K) = \{\text{fonctions de } V \text{ dans } K\}$$

qui envoie un polynôme P sur sa restriction sur V, la fonction polynomiale $P_{|V}$. Le noyau $\mathrm{Ker}(r)$ est alors exactement $I(V)$. En effet :

$$\begin{aligned}\mathrm{Ker}(r) &= \{P \in K[X_1, \ldots, X_n] : P_{|V} = 0\} \\ &= \{P \in K[X_1, \ldots, X_n] : \forall x \in V, P(x) = 0\} \\ &= I(V).\end{aligned}$$

Nous pouvons nous intéresser au quotient de l'anneau $K[X_1, \ldots, X_n]$ par le noyau $\mathrm{Ker}(r)$. Alors :

$$K[X_1, \ldots, X_n]/I(V) \cong \Gamma(V) = \{P : V \to K : P \in K[X_1, \ldots, X_n]\}.$$

Définition I.31. Pour un ensemble algébrique affine V, on appelle l'**anneau des fonctions régulières sur** V l'ensemble $\Gamma(V)$ défini ci-dessus.

On appelle aussi parfois $\Gamma(V)$ l'algèbre affine de V.

I.4 Espaces topologiques irréductibles

Nous allons étudier d'un peu plus près la topologie de Zariski, cela ne nous coûte pas grand chose de généraliser un peu cette notion. Soit $(X, \mathcal{T})$ un espace topologique non vide.

Définition I.32. On dit que $(X, \mathcal{T})$ est irréductible si pour tout fermé F et G, si $X = F \cup G$ alors $F = X$ ou $G = X$.

Exemple I.33. L'espace affine $\mathbb{A}^n(K)$ muni de la topologie de Zariski est un espace topologique irréductible. En effet, soient deux fermés de Zariski de $\mathbb{A}^n(K)$, c'est-à-dire deux ensembles algébriques affines, disons $V(I)$ et $V(J)$ pour deux idéaux I et J de $K[X_1, \ldots, X_n]$, tels que $\mathbb{A}^n(K) = V(I) \cup V(J)$. Alors

$$V(I) \cup V(J) = V(\{P.Q : P \in I \text{ et } Q \in J\}) = K^n.$$

Par la remarque I.27, nous savons que $V(S) = K^n$ si et seulement si $S = \{0\}$, ce qui revient à dire que $\{P.Q : P \in I \text{ et } Q \in J\} = \{0\}$, i.e. $I = \{0\}$ ou $J = \{0\}$, ou encore que $V(I) = K^n$ ou $V(J) = K^n$, ce que nous voulions.

Exemple I.34. Par l'exemple I.22, et puisque K muni de la topologie de Zariski est un espace topologique irréductible, le corps K muni de la topologie cofinie est aussi irréductible (les topologies se cofondent). N'importe quel ensemble infini X muni de la topologie cofinie est aussi irréductible : si $X = F \cup G$ avec F et G deux fermés. Dire que F est fermé, c'est dire qu'il est fini ou égal à l'espace tout entier. Nous en déduisons que F ou G est infini et donc $F = X$ ou $G = X$.

Nous pouvons trouver d'autres caractérisations, notamment en termes d'ouverts :

Lemme I.35. *Les assertions suivantes sont équivalentes :*

i. $(X, \mathcal{T})$ *est irréductible ;*

ii. Toute réunion finie de fermés propres est propre ;

iii. Pour tout ouvert U *et* V *de* X*, si* $U \cap V = \varnothing$ *alors* $U = \varnothing$ *ou* $V = \varnothing$ *;*

iv. Toute intersection finie d'ouverts non vides est non vide ;

v. Tout ouvert non vide de X *est partout dense.*

Démonstration. Être irréductible n'est rien d'autre qu'un cas particulier de la contraposée de ii, et donc ii implique i. Réciproquement, supposons au contraire que la réunion finie des fermés propres n'est pas propre, nous avons ainsi $F_1, \ldots, F_n$ des fermés de X tels que :

$$F_1 \cup \ldots \cup F_n = X.$$

Puisque X est irréductible, nous avons que $F_1 = X$ ou $F_2 \cup \ldots \cup F_n = X$. En itérant n fois cet argument sur le deuxième membre, nous trouvons que

$$F_1 = X \text{ ou } F_2 = X \text{ ou } \ldots \text{ ou } F_n = X,$$

et donc qu'un des fermés n'est pas propre.

Un raisonnement analogue permet de montrer l'équivalence entre iii et iv.

Montrons que i est équivalent à iii. Soient U et V des ouverts de X. Nous avons que :

$$U \cap V = \varnothing \implies U = \varnothing \text{ ou } V = \varnothing$$

ce qui revient à dire

$$U^{\complement} \cup V^{\complement} = X \implies U^{\complement} = X \text{ ou } V^{\complement} = X.$$

Comme ceci est vrai pour tout ouvert U et V, tous les fermés sont couverts dans l'argument et l'équivalence en est déduit.

Nous venons de montrer les équivalences entre les quatre premiers points. Il suffit pour terminer de prouver les implications i $\implies$ v $\implies$ iii.

Montrons que si X est irréductible, alors tout ouvert de X non vide est dense dans X. Soit U un ouvert non vide de X, nous avons toujours que $U \cup U^{\complement} = X$, or $U \subseteq \overline{U}$ et donc $X = \overline{U} \cup U^{\complement}$. Comme $\overline{U}$ et U sont tous les deux des fermés de X, par irréductibilité de X, nous avons que $\overline{U} = X$ ou $U^{\complement} = X$. Comme U est non vide, son complémentaire ne peut pas être l'espace tout entier : nous en déduisons que $\overline{U} = X$ et donc U est bien dense dans X.

Prouvons la dernière implication. Supposons que U et V sont des ouverts tous les deux non vides et montrons que leur intersection est non vide. Alors puisque ce sont des ouverts, par hypothèse ils sont dense dans X. Rappelons qu'une partie de X est partout dense si et seulement si pour tout ouvert de X, leur intersection est non vide. Comme U est dense et V est un ouvert, nous avons que $U \cap V \neq \varnothing$. □

Cette dernière assertion nous dit en quelque sorte que les ouverts d'un espace topologique irréductible sont plutôt *grands* et donc les fermés, par complémentaire, assez *petits*.

Remarque I.36. Nous pouvons nous demander quel est le lien entre connexe et irréductible [3]. En fait, tout espace irréductible est connexe. En effet, si $X = F \cup G$ est la réunion de deux fermés non vides, alors puisque X est irréductible, $F = X$ ou $G = X$, et donc en supposant sans perdre de généralité que $G = X$, il en découle que $F \cap G = F \cap X = F \neq \varnothing$.

Remarque I.37. Tout espace topologique séparé qui n'est pas réduit à un point n'est pas irréductible. En effet, prenons deux points distincts x et y dans X. Puisque X est séparé, il existe deux ouverts de O_x et O_y tels que $x \in O_x$ et $y \in O_y$ avec $O_x \cap O_y = \varnothing$. Or ces deux ouverts sont non vides et donc X n'est pas irréductible.

En particulier, tout espace métrique n'est pas irréductible car tout espace métrique est séparé. Ainsi, les topologies usuelles induites par les normes $\|\cdot\|_p$ sur $\mathbb{R}$ ne sont pas irréductibles.

Revenons sur la topologie qui nous intéresse le plus, à savoir celle de Zariski. Pour un ensemble algébrique affine de K^n muni de la topologie de Zariski (induite par celle de $\mathbb{A}^n(K)$), nous avons une caractérisation très utile de l'irréductibilité. Désormais, pour une partie de S de X, lorsque nous dirons que S est irréductible, ce sera au sens de l'espace topologique de S muni de la topologie induite.

Théorème I.38. *Soit V un ensemble algébrique affine de $\mathbb{A}^n(K)$ muni de sa topologie de Zariski. Les assertions suivantes sont équivalentes :*

i. V est irréductible ;

ii. $I(V)$ est premier ;

3. En anglais, un espace topologique irréductible est parfois appelé *hyperconnected space*.

iii. $\Gamma(V)$ *est intègre.*

Démonstration. L'équivalence entre ii et iii découle du fait que pour un anneau A et un idéal I de A, le quotient A/I est intègre si et seulement si I est un idéal premier. Puisque $\Gamma(V) \cong K[X_1,\dots,X_n]/I(V)$ et $I(V)$ est un idéal de l'anneau $K[X_1,\dots,X_n]$, nous avons l'équivalence.

Supposons que V est irréductible. Montrons que $I(V)$ est premier, c'est-à-dire que si f et g deux polynômes de $K[X_1,\dots,X_n]$ sont tels que $f.g \in I(V)$, alors $f \in I(V)$ ou $g \in I(V)$. Soient f et g de tels polynômes. Alors $(f.g) \subseteq I(V)$, d'où par décroissance de V :

$$V = V(I(V)) \subseteq V(f.g) = V(f) \cup V(g).$$

Donc $V = \big(V(f) \cup V(g)\big) \bigcap V = \big(V(f) \cap V\big) \bigcup \big(V(g) \cap V\big)$. Puisque V est irréductible, et que $V(f)$, $V(g)$ et V sont tous des fermés et donc $V(f) \cap V$ et $V(g) \cap V$ aussi, nous avons $V(f) \cap V = V$ ou $V(g) \cap V = V$. Sans perdre de généralité, supposons que $V(f) \cap V = V$. Cela revient à dire que $V \subseteq V(f)$, i.e. $V(I(V)) \subseteq V(f)$ et donc $f \in I(V)$ (car $V \subseteq V(S)$ si et seulement si $S \subseteq I(V)$).

Réciproquement, supposons par contraposée que $V = V_1 \cup V_2$ avec V_1 et V_2 deux fermés propres de V et montrons que $I(V)$ n'est pas premier. Soit $i \in \{1,2\}$. Nous avons toujours $I(V) \subseteq I(V_i)$ par décroissance de I. De plus, comme V_i est un sous-ensemble propre de V, nous avons $I(V_i) \neq I(V)$ car I est injective sur l'ensemble des ensembles algébriques affines. En effet, puisque $V = V(I(V))$, si $V_1 \neq V$ mais $I(V_1)) = I(V)$, alors en appliquant V à cette égalité, nous obtenons $V_1 = V$, une contradiction. Soit $f_i \in I(V_i) \setminus I(V)$. Alors $f_1.f_2$ est nul sur tout V car V est la réunion de V_1 et V_2, et f_1 et f_2 s'annulent respectivement sur V_1 et V_2. Nous en déduisons que $f_1.f_2 \in I(V)$. Or par hypothèse sur f_i, pour $i \in \{1,2\}$, le polynôme $f_i \notin I(V)$ et donc $I(V)$ n'est pas premier. □

Remarque I.39. Nous avons une autre preuve que l'espace affine $\mathbb{A}^n(K)$ est irréductible pour la topologie de Zariski. En effet, nous avons que $I(K^n) = \{0\}$, or cet idéal est premier et donc K^n est irréductible.

Dans un anneau factoriel A, l'idéal engendré par un élément $a \in A$ est premier si et seulement si a est irréductible, c'est-à-dire qu'il est non nul, non inversible et ne peut pas s'écrire comme produit de deux non inversibles. En particulier dans $K[X_1,\dots,X_n]$, puisque c'est un anneau factoriel, si P est un polynôme irréductible, alors (P) est premier et donc $V(P)$ est un ensemble algébrique affine irréductible.

Corollaire I.40. *Si* $V = V(P)$ *avec* P *un polynôme irréductible de* $K[X_1,\dots,X_n]$, *alors* V *est irréductible.*

Proposition I.41. *Soit* Y *un sous-espace topologique de* X. *Si* Y *est irréductible, alors* $\overline{Y}$ *l'est aussi. De plus, pour tout ouvert* U *de* X, *les applications*

$$Y \mapsto \overline{Y} \text{ et } Z \mapsto Z \cap U$$

sont des bijections réciproques entre les parties fermées irréductibles de U et les parties fermées irréductibles de X qui rencontrent U.

Démonstration. Supposons que $\overline{Y} = F_1 \cup F_2$ est l'union de deux fermés F_1 et F_2 de $\overline{Y}$. Comme $\overline{Y}$ est un fermé, les ensembles F_1 et F_2 sont aussi des fermés de X car $F_1 = G_1 \cap \overline{Y}$ est une intersection de deux fermés, pour un certain fermé G_1 de X. Nous avons que Y est recouvert par deux fermés de Y, à savoir $Y = (F_1 \cap Y) \cup (F_2 \cap Y)$. Puisque Y est irréductible, il s'ensuit que $Y = F_1 \cap Y$ ou $Y = F_2 \cap Y$, ce qui revient à dire que $Y \subseteq F_1$ ou $Y \subseteq F_2$. D'où $\overline{Y} \subseteq \overline{F_1} = F_1$ ou $\overline{Y} \subseteq \overline{F_2} = F_2$, et donc $\overline{Y}$ est bien irréductible.

Soit Z un fermé irréductible de X tel que $Z \cap U \neq \varnothing$. Nous avons que

$$Z \mapsto Z \cap U \mapsto \overline{Z \cap U} = Z$$

car $Z \cap U$ est un ouvert non vide de Z qui est irréductible, d'où $Z \cap U$ est dense dans Z. Soit Y un fermé irréductible de U, nous avons aussi

$$Y \mapsto \overline{Y} \mapsto \overline{Y} \cap U = Y$$

car Y est un fermé de U. Nous en déduisons que ce sont bien des bijections réciproques. □

Lemme I.42. *Si X est un espace topologique irréductible, tout ouvert non vide de X est irréductible. Réciproquement, si X est un espace topologique quelconque dont un ouvert dense est irréductible, alors X est irréductible.*

Démonstration. Soit U un ouvert de X non vide. Prenons V_1 et V_2 des ouverts de U. Comme U est ouvert, ce sont aussi des ouverts de X, car ce sont des intersections de deux ouverts de X. Ainsi, si $V_1 \cap V_2 = \varnothing$, par irréductibilité de X, alors $V_1 = \varnothing$ ou $V_2 = \varnothing$ et donc U est bien irréductible.

Réciproquement, soient V_1 et V_2 des ouverts de X. Soit U un ouvert dense de X, alors les ouverts $U \cap V_1$ et $U \cap V_2$ sont non vides. Puisque ce sont des ouverts de U et que U est irréductible, nous avons que $\big(U \cap V_1\big) \cap \big(U \cap V_2\big) \neq \varnothing$. Or $V_1 \cap V_2$ contient cette intersection et donc est non vide. □

Le théorème fondamental de l'arithmétique nous dit que tout entier peut se décomposer comme un produit de nombres premiers d'une unique façon, à permutation près. De façon plus générale, pour n'importe quel anneau factoriel et en particulier l'anneau des polynômes à n variables sur un corps, un élément a toujours une unique décomposition, à permutation près, en irréductibles (pour l'anneau des entiers, un nombre est irréductible si et seulement si c'est un nombre premier).

De manière tout à fait analogue, nous allons décrire une décomposition d'un fermé de Zariski en irréductibles.

Théorème I.43. *Soit V un ensemble algébrique affine de K^n non vide. Alors V peut s'écrire de façon unique, à permutation près, sous la forme*

$$V = V_1 \cup \ldots \cup V_r$$

avec pour tout $1 \leqslant i \leqslant r$, l'ensemble V_i est un ensemble algébrique affine irréductible et $V_i \nsubseteq V_j$ pour tout $j \neq i$.

Démonstration. Premièrement, montrons l'existence d'une telle décomposition. Si V est irréductible, alors c'est terminé. Supposons alors que V n'est pas irréductible, c'est-à-dire qu'il existe deux fermés de Zariski V_1 et $\tilde{V}_1$ tels que $V = V_1 \cup \tilde{V}_1$, avec $V_1 \neq V$ et $\tilde{V}_1 \neq V$. Ainsi, nous avons forcément que $V_1 \nsubseteq \tilde{V}_1$ et vice-versa. Si V_1 et $\tilde{V}_1$ sont tous les deux irréductibles, alors nous avons notre décomposition. Sinon, une des deux composantes n'est pas irréductible et nous pouvons répéter l'argument. Sans perdre de généralité, supposons que V_1 n'est pas irréductible. Alors il existe deux fermés de Zariski V_2 et $\tilde{V}_2$ qui recouvrent V_1. Ainsi, en continuant à itérer cet argument, nous arrivons soit à une décomposition en irréductibles, soit à une chaîne infinie et strictement décroissante de fermés de Zariski

$$V_1 \supseteq V_2 \supseteq \ldots$$

Dans le premier cas, nous avons terminé. Supposons alors être dans le second. En appliquant I à la chaîne des ensembles algébriques affines, nous obtenons une chaîne infinie et croissante d'idéaux. De plus, les inclusions sont strictes car l'application I est injective et les inclusions $V_j \supseteq V_{j+1}$ sont strictes pour tout naturel non nul j. Nous avons donc une contradiction avec $K[X_1, \ldots, X_n]$ noethérien.

Pour montrer l'unicité de la décomposition telle que décrite dans l'énoncé du théorème, supposons avoir deux écritures de V :

$$V = V_1 \cup \ldots \cup V_n \text{ et } V = W_1 \cup \ldots \cup W_k.$$

Pour $i \in \{1, \ldots, n\}$, nous avons que

$$V_i = V_i \cap V = V_i \cap \big(W_1 \cup \ldots \cup W_k\big) = (V_i \cap W_1) \cup \ldots \cup (V_i \cap W_k).$$

Comme V_i est irréductible, il en découle que $V_i = V_i \cap W_1$ ou …ou $V_i = V_1 \cap W_k$, c'est-à-dire que $V_i \subseteq W_j$ pour un certain $j \in \{1, \ldots, k\}$. Réciproquement, par le même argument, il existe un $i' \in \{1, \ldots, n\}$ tel que $W_j \subseteq V_{i'}$, d'où

$$V_i \subseteq W_j \subseteq V_{i'}.$$

Par hypothèse, comme une composante irréductible ne peux pas être incluse dans une autre, nous en déduisons que $V_i = V_{i'}$ et donc que $V_i = W_j$. Nous avons donc

montré que pour tout $i \in \{1,\dots,n\}$, il existe un $j \in \{1,\dots,k\}$ tel que $V_i = W_j$. De plus, nous avons que $V_i \neq V_{i'}$ implique que $W_j \neq W_{j'}$ car sinon nous aurions $V_i = W_j = W_{j'} = V_{i'}$, une contradiction. Ainsi, chaque V_i apparaît une unique fois dans la décomposition en W_j.

Nous pouvons répéter le même argument en inversant les rôles de W_j et V_i et montrer que chaque W_j apparaît une seule fois dans la décomposition en V_i. Nous en déduisons que les deux décompositions sont identiques. □

Ce théorème est vrai plus généralement pour tout espace topologique vérifiant la condition de chaîne descendante sur ses parties fermées. De tels espaces topologiques sont appelés des espaces noethériens.

Définition I.44. Pour un ensemble algébrique affine V, on appelle les éléments de la décomposition ci-dessus les **composantes irréductibles de** V.

Remarque I.45. Les composantes irréductibles sont des fermés irréductibles et maximaux pour l'inclusion. En effet, si W est un irréductible et $W \supseteq V_i$ pour une certaine composante irréductible V_i de V, alors en remplaçant V_i par W dans la décomposition, nous en obtenons une autre. Par unicité de la décomposition, $W = V_i$ et donc V_i est bien maximal. De plus, supposons qu'il existe une composante irréductible V_i qui n'est pas fermée. Alors $\overline{V_i}$ est aussi irréductible et $V_i \subseteq \overline{V_i}$. Par maximalité de V_i, il en résulte que $V_i = \overline{V_i}$, c'est-à-dire que V_i est un fermé.

Exemple I.46. Soit $f \in K[X_1,\dots,X_n]$ et $V(f)$ l'ensemble algébrique affine associé. Si f est sans facteur carré, c'est-à-dire que sa décomposition en irréductibles est de la forme $f = f_1 \dots f_r$, alors la décomposition en facteurs irréductibles de V est donnée par $V(f) = V(f_1) \cup \dots \cup V(f_r)$. En effet, nous avons que $V(f) = V(f_1) \cup \dots \cup V(f_r)$. De plus, chaque $V(f_i)$ est irréductible car les f_i sont irréductibles, et $V(f_i) \nsubseteq V(f_j)$ pour $i \neq j$ car les polynômes sont distincts et irréductibles. Ainsi, c'est bien une décomposition en irréductibles.

Nous traiterons le cas général où $f = f_1^{\alpha_1} \dots . f_r^{\alpha_r}$ est la décomposition en irréductibles de f plus loin dans ce chapitre.

I.5 Nullstellensatz

L'objectif de cette section sera de prouver le Nullstellensatz pour les corps algébriquement clos. Ce théorème va nous permettre de nous débarrasser, dans le cas où K est algébriquement clos, du second problème présenté dans l'exemple I.29.

À partir de maintenant, considérons K un corps algébriquement clos, de caractéristique nulle. Commençons par définir une certaine propriété sur les idéaux :

Définition I.47. Soit $I \subseteq A$ un idéal d'un anneau commutatif A. On définit le **radical** de I et le note comme

$$\sqrt{I} = \{x \in A : \exists r \in \mathbb{N}, x^r \in I\}.$$

On dit que I est **radiciel** si $I = \sqrt{I}$.

Exemple I.48. Reprenons notre exemple I.29, nous voyons bien que (X) est radiciel mais que (X^2) ne l'est pas. De plus, nous avons que $\sqrt{(X^2)} = (X)$. Ce sont les idéaux non radiciels qui posent problème.

Remarque I.49. Si I est premier, alors I est radiciel. En effet, soit $a \in \sqrt{I}$, c'est-à-dire qu'il existe un naturel r tel que $a^r \in I$. Puisque I est premier, comme $a^r = a^{r-1}a$, nous avons que $a \in I$ ou $a^{r-1} \in I$. En répétant l'argument un nombre fini de fois, nous obtenons que $a \in I$.

Être radiciel est donc une propriété *plus faible* que la primalité d'un idéal. Ainsi, en passant à l'anneau quotient nous n'aurons pas forcément un anneau intègre mais nous aurons quand même une propriété intéressante.

Définition I.50. Soit A un anneau commutatif. On dit que A est **réduit** s'il n'a pas d'éléments nilpotents autre que 0, c'est-à-dire que pour tous $a \in A$ et $r \in \mathbb{N}$, si $a^r = 0$, alors $a = 0$

Le lien entre idéaux radiciels et anneaux réduits s'opère grâce au lemme suivant.

Lemme I.51. *Soit I un idéal d'un anneau commutatif A. L'anneau quotient A/I est réduit si et seulement si I est radiciel.*

Démonstration. Soit $a \in A$ et $r \in \mathbb{N}$. Nous avons

$$\left(a^r \in I \Rightarrow a \in I\right) \iff \left(a^r = 0 \text{ dans } A/I \Rightarrow a = 0 \text{ dans } A/I\ \right),$$

et donc I est radiciel si et seulement si A/I est réduit. □

Exemple I.52. Nous avons toujours que $I(V)$ est radiciel. En effet, si P^r s'annule sur V, alors par intégrité de $K[X_1, \ldots, X_n]$, le polynôme P s'annule aussi sur V. Dire que $I(V)$ est radiciel, c'est dire que l'anneau de ses fonctions polynomiales $\Gamma(V)$ est réduit car $\Gamma(V) \cong K[X_1, \ldots, X_n]/I(V)$.

Énonçons maintenant le Nullstellensatz[4]. Ce théorème est aussi appelé le théorème des zéros de Hilbert. Nous le prouverons un peu plus loin dans cette section.

4. Littéralement *théorème du lieu d'annulation*.

Théorème I.53 (Nullstellensatz)**.** *Soit I un idéal de $K[X_1,\dots,X_n]$. Alors :*

$$I(V(I)) = \sqrt{I}.$$

Ce théorème donne en particulier une correspondance entre les idéaux premiers (voir remarque précédente) et les ensembles algébriques affines irréductibles. Avant de le prouver, attardons-nous sur une version plus faible de ce théorème.

Théorème I.54 (Nullstellensatz faible)**.** *Soit I un idéal propre de $K[X_1,\dots,X_n]$. Alors :*

$$V(I) \neq \varnothing.$$

Nous allons prouver ce théorème dans le cas non dénombrable (par exemple $K = \mathbb{C}$).

Démonstration. Si I n'est pas maximal, considérons $J \supseteq I$ un idéal maximal (qui existe bien par I.5 car $K[X_1,\dots,X_n]$ est noethérien), et donc $V(I) \supseteq V(J) \neq \varnothing$. Ainsi, sans perdre de généralité, nous pouvons supposer I maximal.

Soit $L = K[X_1,\dots,X_n]/I$, c'est un corps puisque I est maximal. En outre, comme $K[X_1,\dots,X_n]$ est un K-espace vectoriel de dimension au plus dénombrable, il en va de même pour L. Montrons que $L = K$. Pour cela, comme K est algébriquement clos, il suffit de montrer que L est algébrique sur K. Supposons au contraire que L n'est pas algébrique sur K, alors il existerait un élément transcendant dans $L \setminus K$. En particulier, le corps L admet un sous-corps isomorphe à $K(t)$, le corps des fractions rationnelles à une variable. Or, le corps $K(t)$ contient la famille non-dénombrable des $\frac{1}{t-a}$ pour $a \in K$ (les $t-a$ sont tous nul nuls). De plus, cette famille est libre sur K. En effet, supposons qu'il existe des scalaires $\lambda_i \in K$ tels que

$$\sum_{i=1}^{m} \frac{\lambda_i}{t-a_i} = 0.$$

Soit $j \in \{1,\dots,m\}$, alors en multipliant par $(t-a_j)$, nous obtenons

$$\sum_{i=1}^{m} \frac{\lambda_i}{t-a_i} = \sum_{\substack{i=1 \\ i\neq j}}^{m} \frac{\lambda_i(t-a_j)}{t-a_i} + \lambda_j = 0.$$

Par conséquent, en évaluant en $t = a_j$, nous trouvons que $\lambda_j = 0$. Cet argument fonctionnant pour tout j, nous en concluons que les λ_i sont tous nuls.

Ainsi, nous avons une tour d'extension de corps

$$K \subseteq K(t) \cong M \subseteq L,$$

avec L/K dénombrable mais $K(t)/K$ non dénombrable, ce qui n'est pas possible, et donc $L = K$.

Soit $\overline{X_1}, \ldots, \overline{X_n}$ les images des $X_1, \ldots, X_n$ dans L par la projection canonique de $K[X_1, \ldots, X_n]$ dans L. Alors si $P(X_1, \ldots, X_n) \in I$, nous avons que $P(\overline{X_1}, \ldots, \overline{X_n}) = 0$ dans $L = K$, d'où $(\overline{X_1}, \ldots, \overline{X_n}) \in V(I) \neq \varnothing$. □

Prouvons maintenant le Nullstellensatz *fort*.

Démonstration du théorème I.53. Posons

$$R = K[X_1, \ldots, X_n],\ I = (P_1, \ldots, P_r) \text{ et } V = V(I).$$

Remarquons déjà que $\sqrt{I} \subseteq I(V(I))$. En effet, si $Q^r \in I$, alors pour tout $x \in V$, nous avons $Q^r(x) = 0$. Puisque R est intègre, cela revient à dire $Q(x) = 0$, c'est-à-dire $Q \in I(V(I))$.

Réciproquement, soit $F \in I(V)$. Nous voulons trouver un naturel m tel que $F^m \in I$. Considérons l'anneau $A = R[Y]/(1 - YF)$. L'imagine $\overline{Y}$ de Y par la projection canonique de R dans A vérifie que $\overline{Y}F = 1$, c'est-à-dire que $\overline{Y}$ est l'inverse de F dans A. Soit J l'idéal $(P_1, \ldots, P_r, 1 - YF)$ de $R[Y]$. Nous avons que $V(J) = \varnothing$ dans K^{n+1}. En effet, si $(x_1, \ldots, x_n, y) \in V(J)$, le tuple $x = (x_1, \ldots, x_n)$ annulerait les P_i et donc appartiendrait à V, par conséquent $F(x) = 0$ et donc x ne pourrait pas annuler $1 - YF$. Par la contraposée du Nullstellensatz faible, nous en déduisons que $J = R[Y]$. En particulier $1 \in J$, c'est-à-dire qu'il existe $Q, Q_i \in R[Y]$ tels que

$$1 = \sum_{i=1}^{r} P_i Q_i + Q(1 - YF).$$

Dans A, cette égalité donne que

$$1 = \sum_{i=1}^{r} P_i(X_1, \ldots, X_n) Q_i(X_1, \ldots, X_n, \overline{Y}). \tag{I.1}$$

Soit m un naturel tel que $m \geqslant \deg_Y(Q_i)$ pour tout $i \in \{1, \ldots, r\}$. Alors nous pouvons écrire en isolant Y, pour tout i,

$$Q_i(X_1, \ldots, X_n, Y) = \sum_{j=1}^{m} \tilde{Q}_{i,j}(X_1, \ldots, X_n) Y^j, \text{ avec } \tilde{Q}_{i,j} \in R.$$

Dans A, l'équation I.1 devient alors, après avoir multiplié par F^m,

$$\begin{aligned} F^m &= \sum_{i=1}^{r} \Big(\sum_{j=1}^{m} P_i(X_1, \ldots, X_n) \tilde{Q}_{i,j}(X_1, \ldots, X_n) \overline{Y}^j \Big) F^m \\ &= \sum_{i=1}^{r} \Big(\sum_{j=1}^{m} P_i(X_1, \ldots, X_n) \tilde{Q}_{i,j}(X_1, \ldots, X_n) F^{m-j} \Big). \end{aligned}$$

Cette égalité reste vraie dans R, d'où $F^m \in I$. □

Remarque I.55. En fait, ces deux versions du Nullstellensatz sont équivalentes. En effet, si nous avons le Nullstellensatz fort, alors pour un idéal $I \subseteq K[X_1,\dots,X_n]$, si $V(I) = \varnothing$, alors $\sqrt{I} = I(\varnothing) = K[X_1,\dots,X_n]$. D'où $1 \in \sqrt{I}$ et donc $1 \in I$, c'est-à-dire que $I = K[X_1,\dots,X_n]$.

Rappelons-nous que $V \circ I = Id_{K^n}$. Ainsi, puisque $I(V(I)) = \sqrt{I}$, en appliquant V, nous obtenons que $V(I) = V(\sqrt{I})$, c'est-à-dire qu'un idéal et son radical engendrent le même fermé de Zariski.

Exemple I.56. Si $I = (X, Y^2)$, alors par le Nullstellensatz, nous avons $I(V(I)) = \sqrt{(X,Y^2)} = (X,Y)$.

Corollaire I.57. *Soit $S \subseteq K^n$ un ensemble quelconque. Son adhérence pour la topologie de Zariski est donné par $\overline{S} = V(I(S))$.*

Démonstration. L'ensemble étant $V(I(S))$ un fermé de Zariski contenant S, il nous reste à montrer que c'est le plus petit.

Supposons qu'il existe un idéal I de $K[X_1,\dots,X_n]$ tel que $V(I) \supseteq S$. Alors $I(V(I)) \subseteq I(S)$, c'est-à-dire par décroissance de V, que $V(\sqrt{I}) \supseteq V(I(S))$. Par la remarque précédente, cela revient à $V(\sqrt{I}) = V(I) \supseteq V(I(S))$, ainsi $V(I(S))$ est contenu dans tout fermé de Zariski contenant S. □

Pour différencier l'idéal engendré dans des corps différents, nous noterons $I_K(S)$ l'idéal engendré par S dans $K[X_1,\dots,X_n]$.

Définition I.58. Soient V un ensemble algébrique affine de K^n, $a \in L$ dans une extension de K et $I_L(a)$ l'idéal $I(a)$ engendré dans L pour sa propre topologie de Zariski. On dit que a est un **point générique** de V si $V(I_L(a) \cap K[X_1,\dots,X_n]) = V$.

Remarque I.59. Il faut faire attention au lieu de définition des différents ensembles. L'ensemble $V(I_L(a))$ est défini dans L, c'est un fermé de Zariski pour l'espace affine $\mathbb{A}^n(L)$. Ainsi,

En particulier, si a est un point générique de V, alors il est dense pour la topologie de Zariski induite sur V, c'est-à-dire que a appartient à tous les ouverts non vide de V (en regardant ces ensembles dans L).

Lemme I.60. *Soit V un ensemble algébrique affine. Les assertions suivantes sont équivalentes :*

1. *Il existe un point générique dans une extension transcendante de K de degré fini.*
2. *L'ensemble V est irréductible.*

Démonstration. Soit V un ensemble algébrique affine irréductible. Alors $I(V)$ est premier : considérons $L = \mathrm{Frac}(K[X_1,\dots,X_n]/I)$ une extension transcendante de K de degré fini car le degré de transcendance est borné par celui de $K[X_1,\dots,X_n]$ sur K qui n'est rien d'autre que n. Prenons dans L l'élément $a = (X_1,\dots,X_n)+I$.

Il faut faire bien attention où sont les idéaux, notons $I_L(a)$ l'idéal engendré par a dans L et posons $I_K(a) = I_L(a)\cap K[X_1,\dots,X_n]$. Clairement $I_K(a)$ est premier, et donc pour montrer que a est un point générique de V, il faut et il suffit de montrer que $I = I_K(a)$ car en appliquant le Nullstellensatz sur l'égalité $V(I) = V(I_K(a))$, nous obtenons que $\sqrt{I} = \sqrt{I(a)}$, or ce sont des idéaux premiers et donc $I = I(a)$.

Soit $f \in K[X_1,\dots,X_n]$. Nous avons en utilisant les propriétés du quotient,

$$\begin{aligned} f \in I &\Leftrightarrow f(X_1,\dots,X_n)+I = 0 \\ &\Leftrightarrow f(X_1,\dots,X_n+I) = 0 \\ &\Leftrightarrow f(a) = 0 \Leftrightarrow f \in I(a). \end{aligned}$$

La réciproque est immédiate, il suffit de considérer l'équation $f(a) = 0$ dans L pour tout polynôme de $K[X_1,\dots,X_n]$, et de redescendre dans K. □

Remarque I.61. Si V est un singleton, alors l'élément $a \in V$ est un point générique car c'est un fermé de Zariski, donc son adhérence est lui-même.

Lemme I.62. *Soient V un ensemble algébrique affine de K^n avec un point générique a et $f \in K[X_1,\dots,X_n]$. Alors, pour tout $b \in V$, si $f(a) \neq 0$, alors $f(b) \neq 0$.*

Démonstration. Soit L l'extension de K qui contient a. Notons que l'égalité

$$f(a) = 0$$

se vérifie dans cette extension. Soit $b \in V = V(I) = V(I_K(a))$. Supposons que $f(a) \neq 0$, alors $f \notin I_L(a)$, d'où $f \notin I_K(a)$ car $f \in K[X_1,\dots,X_n]$ et donc $f(b) \neq 0$. □

Exemple I.63.

Reprenons notre exemple I.46 dans le cas général.

Proposition I.64. *Soit $f \in K[X_1,\dots,X_n]$ avec comme décomposition en irréductibles $f = f_1^{\alpha_1}\dots f_r^{\alpha_r}$. Nous avons que :*

- *$I(V(f)) = (f_1\dots f_r)$;*
- *La décomposition en irréductibles est donnée par $V(f_1)\cup\dots\cup V(f_r)$.*

Démonstration. Nous avons que $V(f) = V(f_1^{\alpha_1})\cup\dots\cup V(f_r^{\alpha_r})$, et en appliquant I, nous obtenons que $I(V(f)) = I(V(f_1^{\alpha_1}))\cap\dots\cap I(V(f_r^{\alpha_r}))$.

Mais le Nullstellensatz nous dit que $I(V(f_i^{\alpha_i})) = \sqrt{(f_i^{\alpha_i})} = (f_i)$. D'où :

$$I(V(f)) = \bigcap_{i=1}^{r} I(V(f_i^{\alpha_i})) = \bigcap_{i=1}^{r} (f_i) = (f_1 \dots f_r).$$

De plus, nous avons $V(f) = V(I(V(f))) = V(f_1 \dots f_r) = V(f_1) \cup \dots \cup V(f_r)$ et donc, puisque les f_i sont irréductibles, les ensembles $V(f_i)$ sont irréductibles. Comme il n'y aucune inclusion entre ces ensembles, les $V(f_i)$ forment une décomposition de $V(f)$ en irréductibles. □

Soient V un ensemble algébrique affine, l'idéal associé $I(V)$ et son algèbre *affine* $\Gamma(V) \cong K[X_1, \dots, X_n]/I(V)$. Nous allons développer un *dictionnaire d'algèbre géométrie*.

Proposition I.65. *Les applications $W \mapsto I(W)$ et $I \mapsto V(I)$ sont des bijections réciproques entre les ensembles algébriques affines de K^n et les idéaux radiciels de $K[X_1, \dots, X_n]$. De plus,*

- *W irréductible $\Leftrightarrow$ $I(W)$ premier $\Leftrightarrow$ $\Gamma(W)$ intègre ;*
- *W est un singleton $\Leftrightarrow$ $I(W)$ maximal $\Leftrightarrow$ $\Gamma(W) = K$.*

Démonstration. Nous avons déjà que $V(I(V)) = V$, de plus le Nullstellensatz nous dit que $I(V(I)) = \sqrt{I} = I$ car nous ne considérons que les idéaux radiciels. Les applications définies sont donc bien des bijections.

Quant à la première chaîne d'équivalences, ce n'est rien d'autre que le théorème I.38.

Pour le second point, considérons le morphisme φ défini par :

$$\begin{aligned} \varphi : K[X_1, \dots, X_n] &\to K \\ P &\mapsto P(w) \end{aligned}$$

Alors $K[X_1, \dots, X_n]/Ker(\varphi) \cong K$, d'où $W = \{w\}$ si et seulement si $Ker(\varphi) = I(\{w\}) = I(W)$, ce qui est équivalent à dire que $\Gamma(W) = K$.

De plus, nous avons que $I(W)$ est maximal si et seulement si $V(I(W))$ est un fermé de Zariski minimal. Or tout singleton est un fermé de Zariski, ainsi $V(I(W))$ est un singleton. De plus, comme nous considérons uniquement les idéaux radiciels, nous avons aussi que $V(I(W)) = W$, et donc W est un singleton. □

Nous avons donc une équivalence des propriétés énoncées entre différentes structures : les ensembles algébriques affines, les idéaux radiciels de $K[X_1, \dots, X_n]$ et l'anneau des fonctions régulières $\Gamma(V)$. Une autre équivalence est la suivante :

Proposition I.66. *V est fini si et seulement si $\Gamma(V)$ est un K-espace vectoriel de dimension finie.*

Démonstration. Supposons que $V = \{v_1, \ldots, v_r\}$ soit fini et considérons le morphisme d'anneaux $\varphi : K[X_1, \ldots, X_n] \to K^r$ qui envoie P sur $(P(v_1), \ldots, P(v_r))$. Son noyau n'est rien d'autre que $I(V)$, et donc comme $\Gamma(V) \cong K[X_1, \ldots, X_n]/I(V)$, l'anneau $\Gamma(V)$ s'injecte dans K^r.

Réciproquement, supposons que $\Gamma(V)$ soit un K-espace vectoriel de dimension finie. Pour $i \in \{1, \ldots, n\}$, considérons $\overline{X_i}$ l'image de X_i par la projection canonique dans $\Gamma(V)$. Pour une question de dimension, pour un naturel $s > \mathrm{Dim}_K(\Gamma(V))$, la famille d'éléments $1, \ldots, \overline{X_i}^s$ n'est pas libre. Par conséquent, il existe des éléments a_j de K tels que

$$a_s \overline{X}_i^s + \ldots + a_1 \overline{X}_i + a_0 = 0,$$

avec $a_s \neq 0$. En particulier, si $v = (v_1, \ldots, v_n) \in V$, nous obtenons l'égalité

$$a_s v_i^s + \ldots + a_1 v_i + a_0 = 0.$$

Ainsi, pour tout $i \in \{1, \ldots, n\}$, il existe un polynôme à une variable qui s'annule sur la projection de V sur sa i-ème coordonnée et donc V est fini. □

Discussion I.67. Jusqu'ici, nous nous sommes cantonnés à étudier les ensembles algébriques affines définis sur K^n. Élargissons un peu nos horizons et considérons les ensembles algébriques affines définis sur un ensemble algébrique affine de $V \subseteq K^n$.

Soit W un ensemble algébrique affine contenu dans V. Alors $I(W) \supseteq I(V)$ et donc $I(W)$ détermine un idéal $I_V(W) = \{f \in \Gamma(V) : \forall w \in W, f(w) = 0\}$ de l'anneau $\Gamma(V)$. C'est le noyau de l'application

$$\begin{aligned} \varphi : \Gamma(V) &\to \Gamma(W) \\ P &\mapsto P_{|W} \end{aligned}$$

De plus, nous avons l'isomorphisme $\Gamma(V)/I_V(W) \cong \Gamma(W)$. En particulier l'idéal $I_V(W)$ est radiciel car $\Gamma(W)$ est réduit.

Soit π la projection canonique de $K[X_1, \ldots, X_n]$ dans $\Gamma(V)$. Si I est un idéal de $\Gamma(V)$, nous pouvons définir $V(I) = \{x \in V : \forall f \in I, f(x) = 0\}$, ce qui revient à définir $V(I) = V(\pi^{-1}(I))$. Nous avons alors les équivalences suivantes :

Proposition I.68. *Les applications $W \mapsto I_V(W)$ et $I \mapsto V(I)$ sont des bijections réciproques entre les sous-ensembles algébriques affines de V et les idéaux radiciels de $\Gamma(V)$. De plus,*

- *W irréductible $\Leftrightarrow$ $I_V(W)$ premier $\Leftrightarrow$ $\Gamma(W)$ intègre ;*
- *W est un singleton $\Leftrightarrow$ $I_V(W)$ maximal $\Leftrightarrow$ $\Gamma(W) = K$;*
- *W est une composante irréductible de $V \Leftrightarrow$ $I_V(W)$ est un idéal premier minimal de $\Gamma(V)$.*

Démonstration. Un idéal I de $\Gamma(V)$ est radiciel si et seulement si l'idéal $\pi^{-1}(I)$ est un idéal radiciel de $K[X_1,\dots,X_n]$. En effet, si $p^k \in \pi^{-1}(I)$ alors $\pi(p^k) \in I$. De plus, comme π est un morphisme d'anneaux, nous avons que $\pi(p)^k \in I$, et puisque I est radiciel, il en découle que $\pi(p) \in I$, c'est-à-dire $p \in \pi^{-1}(I)$. Réciproquement, si $p^k + I(V) \in I$, alors $p^k \in \pi^{-1}(I)$, d'où $p \in \pi^{-1}(I)$ et donc $p + I(V) \in I$. Ainsi, nous avons que les applications de l'énoncé définissent bien des bijections réciproques. Un même argument montre que $I_V(W)$ est premier si et seulement si $\pi^{-1}(W)$ est premier et nous en déduisons le premier point.

En outre, dire que W est une composante irréductible de V, c'est dire que c'est un irréductible maximal contenu dans V. En appliquant I_V, c'est donc équivalent à ce que $I_V(W)$ soit un idéal premier minimal de $\Gamma(V)$.

Pour le second point, nous pouvons associer à $x \in V$ le morphisme de K-algèbres $\mu_x : \Gamma(V) \to K : f \mapsto f(x)$. Son noyau est l'idéal $I(\{x\}) = \{f \in \Gamma(V) : f(x) = 0\}$, qui est maximal. □

Considérons maintenant un corps K quelconque. Nous allons montrer que l'intersection de deux courbes planes sans facteur commun est finie. Prenons donc $f, g \in K[X,Y]$ deux polynômes non nuls et sans facteur commun.

Lemme I.69. *Il existe $d \in K[X]$ non nul et des polynômes $a, b \in K[X,Y]$ tels que $d = af + bg$.*

Démonstration. Plaçons-nous dans $K(x)[Y]$. Alors, comme les polynômes f et g sont premiers entre-eux, par Bézout, il existe $\overline{a}$ et $\overline{b} \in K(x)[Y]$ tels que $1 = \overline{a}f + \overline{b}g$. Posons d le plus petit commun multiple des dénominateurs de $\overline{a}$ et $\overline{b}$. C'est un polynôme en X, c'est-à-dire que $d \in K[X]$. Alors en multipliant par d, nous obtenons $d = \overline{a}df + \overline{b}dg$, avec $\overline{a}d$ et $\overline{b}d \in K[X,Y]$. □

Prouvons maintenant l'assertion énoncée plus tôt, que nous pouvons reformuler de cette façon :

Théorème I.70. *$V(f) \cap V(g)$ est fini.*

Démonstration. Si $(x,y) \in V(f) \cap V(g)$, alors par le lemme précédent, nous avons que $d(x) = 0$. Puisque $d(X)$ est un polynôme en une seule variable, il a un nombre fini de racines et donc x ne peut prendre qu'un nombre fini de valeurs. En appliquant le même argument pour y, nous obtenons que l'intersection est finie. □

Exemple I.71. L'ensemble $X = \{(t, \sin(t)) : t \in \mathbb{R}\}$ n'est pas un sous-ensemble algébrique affine de $\mathbb{R}^2$. Par l'absurde, supposons qu'il existe des polynômes $f_1,\dots,f_r$ dans $\mathbb{R}[X,Y]$ tels que $V(f_1,\dots,f_r) = X$. Pour tout $1 \leqslant i \leqslant r$, nous avons que $X \subseteq V(f_i)$. Soit $V(Y) = \{(x,0) : x \in \mathbb{R}\}$, nous avons que $X \cap V(Y)$ est d'ordre infini car pour tout entier k, cette intersection contient $(k\pi, 0)$.

En outre, il existe un f_j tel que Y ne divise pas f_j car sinon nous aurions $(f_1,\dots,f_r) = (Y)$ mais $V(Y) \neq X$. Or $X \cap V(Y) \subseteq V(f_j) \cap V(Y)$, ce qui contredit le théorème précédent qui affirme que $V(f_j) \cap V(Y)$ est d'ordre fini.

I.6 Morphisme d'ensembles algébriques affines

Soit K un corps quelconque. Un morphisme entre deux structures est par essence une application d'une structure vers l'autre qui *préserve* la structure. Dans notre cas, la structure d'un ensemble algébrique affine $V \subseteq K^n$ n'est rien d'autre qu'un ensemble muni d'une topologie, celle induite par la topologie de Zariski sur K^n. Ainsi, les morphismes que nous allons considérer sont les fonctions continues au sens de cette topologie.

Soient $V \subseteq K^n$ et $W \subseteq K^m$ deux ensembles algébriques affines définis sur K.

Définition I.72. Soit $\varphi : V \to W$ une application dont l'image s'écrit composante par composante par $\varphi = (\varphi_1,\dots,\varphi_m)$, avec $\varphi_i : V \to K$.

On dit que φ est un morphisme si les composantes φ_i sont polynomiales, c'est-à-dire que $\varphi_i \in \Gamma(V)$. On dit aussi que φ est une application **régulière**. L'ensemble des applications régulières de V dans W est noté $\mathrm{Reg}(V,W)$.

Nous pouvons nous demander si cela définit bien un morphisme au sens donné plus tôt.

Lemme I.73. *Les morphismes de V dans W sont des applications continues pour la topologie de Zariski.*

Démonstration. Soit $F = V(f_1,\dots,f_r)$ un fermé de Zariski de W. Montrons que son image réciproque par φ est bien un fermé de Zariski de V. Nous avons que

$$\begin{aligned}\varphi^{-1}(V(f_1,\dots,f_r)) &= \{x \in V : \varphi(x) \in V(f_1,\dots,f_r)\}\\ &= \{x \in V : \forall j \in \{1,\dots,r\}, f_j(\varphi(x)) = 0\}\\ &= \bigcup_{1\leqslant j\leqslant r} V(f_j \circ \varphi).\end{aligned}$$

Les applications $f_j \circ \varphi$ sont bien polynomiales car φ est un morphisme de V dans W et donc l'union définit bien un fermé de Zariski de V. □

Exemple I.74. Prenons $V = W = \mathbb{R}^2$ et $\varphi : (x,y) \mapsto (\frac{x}{2},\frac{y}{3})$. L'application φ est un endomorphisme de $\mathbb{R}^2$. Soit $V = V(X^2+Y^2-1)$, le cercle unité dans le plan. Alors $\varphi^{-1}(V) = V(\frac{X^2}{4}+\frac{Y^2}{9}-1)$ est une ellipse avec des axes de longueurs 2 et 3.

Nous verrons plus tard que contrairement dans les cas des groupes, même si φ est un morphisme bijectif, sa réciproque n'est pas nécessairement un morphisme (et donc φ n'est pas forcément un *isomorphisme*).

Remarque I.75. Les morphismes de V dans W ne sont pas les seules applications continues pour la topologie de Zariski.

Si φ est une bijection de $\mathbb{R}$ dans lui-même, alors elle est continue pour la topologie de Zariski. En effet, soit F un fermé de Zariski propre de $\mathbb{R}$. C'est forcément un ensemble fini, disons $F = \{x_1, \ldots, x_r\}$. Alors $\varphi^{-1}(F) = \{y_1, \ldots, y_r\}$ où y_i est l'image réciproque de x_i par φ (c'est la seule par injectivité) qui n'est rien d'autre que le fermé $V((X-y_1)\ldots(X-y_r))$. Si nous prenons une application bijective f non polynomiale (par exemple l'extension de $x \mapsto x^{-1}$ sur $\mathbb{R}$ en ajoutant $0 \mapsto 0$), nous obtenons une application continue qui n'est pas un morphisme au sens de la définition ci-dessus.

Considérons quelques exemples.

Exemple I.76.

- Les éléments de $\Gamma(V)$ sont les morphismes de V dans $\mathbb{A}^1(K)$.
- La projection de V sur K^p pour $p \subseteq n$ est un morphisme de V dans K^p.
- Soit $V = V(Y - X^2)$ la parabole dans le plan. Soit $\varphi : V \to K : (x,y) \mapsto x$. Alors φ est un isomorphisme, avec comme fonction réciproque $x \mapsto (x, x^2)$.

Chapitre II

Géométrie algébrique projective

Nous avons traité dans le premier chapitre le cas *affine*. Malheureusement cet outil n'est pas très puissant pour étudier les objets géométriques, comme par exemple les points d'intersections de deux courbes dans le plan dont nous avons vu un résultat plutôt faible dans le cas affine.

Nous allons considérer un objet mathématique qui permet d'étudier notamment cette question. Ainsi, nous allons plonger notre espace affine dans une structure vérifiant de bien meilleures propriétés, nous verrons plus loin dans ce chapitre comment ce plongement s'opère (voir II.7). Cette nouvelle structure, appelée l'espace projectif, va nous permettre de dompter l'infini et de le considérer, en fait, comme une notion affine. Le contenu de ce chapitre est tiré de [7].

II.1 L'espace projectif

Soit K un corps et E un K-espace vectoriel de dimension finie $n+1$.

Discussion II.1. Nous construisons sur E une relation d'équivalence binaire $\sim$ définie sur $E \setminus \{0\}$ par *être colinéaire*, c'est-à- dire :

$$x \sim y \text{ s'il existe un scalaire } \lambda \in K^\times \text{ tel que } x = \lambda y.$$

La relation $\sim$ définit bien une relation d'équivalence. Soient $x, y \in E \setminus \{0\}$.

- Nous avons toujours $x \sim x$ car $x = 1.x$.
- Si $x \sim y$, alors il existe $\lambda \in K^\times$ tel que $x = \lambda y$, et donc $y = \lambda^{-1} x$, i.e. $y \sim x$.
- Si $x \sim y$ et $y \sim z$, alors il existe $\lambda_1, \lambda_2 \in K^\times$ tels que $x = \lambda_1 y$ et $y = \lambda_2 z$, d'où $x = \lambda_1 \lambda_2 z$, c'est-à-dire $x \sim z$.

Les classes d'équivalences sont les ensembles maximaux d'éléments colinéaires sur K, c'est-à-dire qui ont la même direction. Nous appellerons les droites passant par 0 les droites vectorielles de E (une droite est un sous-espace vectoriel de E si

et seulement si elle passe par 0). Ainsi, les classes d'équivalences de $\sim$ forment les droites vectorielles de E auxquelles le 0 a été enlevé. Autrement dit, les classes d'équivalences de $\sim$ sont en bijection avec les sous-espaces vectoriels de E de dimension 1.

Puisque nous avons une relation d'équivalence, nous pouvons nous intéresser au quotient de $E \setminus \{0\}$ par celle-ci. Deux éléments de E ne seront distincts dans ce quotient que s'ils n'appartiennent pas à la même droite vectorielle.

Définition II.2. On appelle l'**espace projectif associé à** E, noté $\mathbb{P}(E)$, le quotient $(E \setminus \{0\})/\sim$. On dit que $\mathbb{P}(E)$ est de **dimension** n.

Dans le cas particulier où $E = K^{n+1}$, nous écrirons $\mathbb{P}(E) = \mathbb{P}^n(K)$, et l'appellerons l'**espace projectif standard de dimension** n.

Réciproquement, un **espace projectif** est un espace projectif associé à un espace vectoriel E.

Exemple II.3. Soit $K = \mathbb{R}$ et $E = \mathbb{R}^3$. L'espace projectif de dimension 2 associé est appelé le plan projectif réel. C'est donc l'ensemble des droites vectorielles de $\mathbb{R}^3$ sans l'origine.

Exemple II.4. Prenons $K = \mathbb{C}$ ou $K = \mathbb{R}$, et munissons $K^{n+1} \setminus \{0\}$ de sa topologie produit induite par le module. Nous pouvons munir le plan projectif $\mathbb{P}^n(K)$ d'une topologie naturelle induite par celle de $K^{n+1} \setminus \{0\}$.

Pour la construire, posons π la projection canonique de $K^{n-1} \setminus \{0\}$ dans $\mathbb{P}^n(K)$. Une partie U de $\mathbb{P}^n(K)$ est dite ouverte si et seulement si $\pi^{-1}(U)$ est un ouvert de K. Les parties ouvertes forment bien une topologie sur $\mathbb{P}^n(K)$ car l'image réciproque d'une intersection (respectivement une union) est l'intersection (respectivement l'union) des images réciproques. C'est la topologie la plus fine qui rend π continue. Cette topologie est appelée la topologie quotient.

Alors, l'espace projectif $\mathbb{P}^n(K)$ muni de la topologie quotient est compact et connexe. En effet, soient O_1 et O_2 deux ouverts de $\mathbb{P}^n(K)$ tels que $\mathbb{P}^n(K) = O_1 \cup O_2$. Alors $\pi^{-1}(O_1) \cup \pi^{-1}(O_2) = \pi^{-1}(O_1 \cup O_2) = K^{n+1} \setminus \{0\}$. Puisque $K^{n+1} \setminus \{0\}$ est connexe, nous devons avoir que $\pi^{-1}(O_1 \cap O_2) = \pi^{-1}(O_1) \cap \pi^{-1}(O_2) \neq \varnothing$, d'où $O_1 \cap O_2 \neq \varnothing$, et donc $\mathbb{P}^n(K)$ est bien connexe.

Pour montrer la compacité, considérons la sphère unité S dans $K^{n+1} \setminus \{0\}$, l'ensemble défini par

$$S = \{(x_0, \ldots, x_n) \in K^{n+1} \setminus \{0\} : ||x||^2 = \sum_{i=0}^{n} |x_i|^2 = 1\}.$$

Cet ensemble est compact car c'est un fermé borné dans un espace euclidien (nous pouvons voir $\mathbb{C}^{n+1}$ comme l'espace euclidien $\mathbb{R}^{2(n+1)}$). De plus, la restriction de π à S est surjective car S contient un élément de n'importe quelle droite vectorielle.

Ainsi, par continuité de π, nous obtenons que $\mathbb{P}^n(K) = \pi(S)$ est aussi compact. En effet, prenons un recouvrement $(O_i)_{i\in I}$ potentiellement infini d'ouverts de $\mathbb{P}^n(K)$. Comme l'image réciproque de ce recouvrement contient S qui est compact, nous pouvons en tirer un sous-recouvrement fini $(\pi^{-1}(O_k))_{k=1}^m$ de S. Or $\pi_{|S}$ est surjective et $\pi(\pi^{-1}(A)) \subseteq A$ pour n'importe quelle partie $\mathbb{P}^n(K)$, ainsi $(O_k)_{k=1}^m$ recouvre bien $\mathbb{P}^n(K)$.

Il nous reste à vérifier que $\mathbb{P}^n(K)$ est séparé pour la topologie quotient, ceci fait, nous pourrons en conclure que $\mathbb{P}^n(K)$ est compact. L'argument nécessaire est un peu plus long, par conséquent nous ne le ferons pas ici. Nous pourrons trouver une démonstration à l'aide d'une simple recherche dans la bibliothèque de l'humanité.

Soient π la projection canonique de E dans $\mathbb{P}(E)$ et F un sous-espace vectoriel de E de dimension $m+1$. Nous pouvons considérer l'image de $F \setminus \{0\}$ dans $\mathbb{P}(E)$ par π, c'est l'espace projectif associé à F, de dimension m.

Définition II.5. Un **sous-espace projectif de** $\mathbb{P}(E)$ est l'image d'un sous-espace vectoriel F non nul de E par π. Son image est notée $\overline{F}$. On lui donne comme **dimension** $\dim_K(F) - 1$. Par convention, l'ensemble vide est de dimension -1.

Exemple II.6. Si F est de dimension 1, c'est une droite vectorielle et son image $\overline{F}$ est réduite à un point, nous dirons que $\overline{F}$ est un **point projectif**. Un sous-espace projectif est de dimension 0 si et seulement s'il est réduit à un point projectif. Si F est de dimension 2, son image $\overline{F}$ est de dimension 1, que nous appellerons **droite projective**. Un **plan projectif** sera un sous-espace projectif de dimension 2 et un **hyperplan projectif** un sous-espace projectif de dimension $n-1$ où n est la dimension de l'espace projectif ambiant.

Pour décrire les éléments de $\mathbb{P}(E)$, nous utilisons les éléments de E. Soit $\bar{x} \in \mathbb{P}(E)$ tel que $\bar{x} = \pi(x_0, \ldots, x_n)$, nous dirons que $\bar{x}$ est un point de **coordonnées homogènes** $(x_0, \ldots, x_n)$. Forcément, les x_i sont non tous nuls car les seuls points colinéaires avec 0 est 0 qui n'est pas considéré dans l'espace projectif. En outre, si $\lambda \in K^\times$ et $\bar{x} = \pi(x_0, \ldots, x_n)$, l'élément $(\lambda x_0, \ldots, \lambda x_n)$ est un autre système de coordonnées homogènes de $\bar{x}$. Nous écrirons $\bar{x} = [x_0, \ldots, x_n]$.

Exemple II.7. Soit $K = \mathbb{R}$ et $E = \mathbb{R}^2$. Considérons l'hyperplan $H = \{(x, 0) \in \mathbb{R}^2\}$ de $\mathbb{R}^2$.

L'image de H dans $\mathbb{P}^1(\mathbb{R})$ est un point projectif P_∞, appelé point *à l'infini*. Il a comme coordonnées homogènes $[1,0]$. Son complémentaire $\overline{H}^\complement$ dans $\mathbb{P}^1(\mathbb{R})$ est formé des points projectifs de la forme $[x,1]$ car $[x,y] = [1,0]$ si et seulement si $y = 0$ (la condition $x = 0$ n'est pas nécessaire car le vecteur nul n'est pas projeté). De plus $\overline{H}^\complement$ est en bijection avec $\mathbb{A}^1(\mathbb{R})$. En effet, pour $x \neq y$, nous obtenons que

$[x,1] \neq [y,1]$ car $(x,1) = (\lambda y, \lambda)$ si et seulement si $\lambda = 1$ et $x = y$. Nous avons donc la bijection suivante :

$$\begin{aligned}\mathbb{P}^1(\mathbb{R}) &\cong \overline{H}^{\complement} \dot{\cup} \overline{H} \\ &\cong \mathbb{A}^1(\mathbb{R}) \dot{\cup} \mathbb{P}^0(\mathbb{R}) \\ &\cong \mathbb{A}^1(\mathbb{R}) \dot{\cup} \{P_\infty\}.\end{aligned}$$

Nous pouvons voir la droite projective comme une droite affine à laquelle nous avons ajouté un point à l'infini. C'est une sorte de *complétion* du plan affine.

Plus généralement, nous obtenons que

$$\mathbb{P}^n(K) \cong \mathbb{A}^n(K) \dot{\cup} \mathbb{P}^{n-1}(K),$$

c'est-à-dire que l'espace projectif de dimension n peut être vu comme l'espace affine de dimension n auquel nous avons rajouté un hyperplan à l'infini. Nous pouvons également réécrire $\mathbb{P}^{n-1}(K)$ par récurrence...

Proposition II.8. *Soient V et W deux sous-espaces projectifs de $\mathbb{P}(E)$ de dimensions respectives r et s telles que $r+s \geqslant n$. Le sous-espace projectif $V \cap W$ est de dimension $\geqslant r+s-n$. En particulier $V \cap W \neq \varnothing$.*

Démonstration. Comme V et W sont des sous-espaces projectifs de $\mathbb{P}(E)$, il existe deux sous-espaces vectoriels F_V et F_W de E tels que $\overline{F}_V = V$ et $\overline{F}_W = W$. Notons que $\overline{F_V \cap F_W} = \overline{F}_V \cap \overline{F}_W$ car $\pi(V \cap W) = \pi(V) \cap \pi(W)$.

Par la formule de Grassman, nous avons que

$$\dim_K(F_V \cap F_W) = \dim_K(F_V) + \dim_K(F_W) - \dim_K(F_V + F_W) \geqslant r+s-n+1.$$

En passant à l'espace projectif, nous obtenons que $\dim(\overline{F}_V \cap \overline{F}_W) \geqslant r+s-n$.

De plus $V \cap W \neq \varnothing$ car dans le pire des cas, l'intersection est de dimension 0 et donc réduite à un point projectif. □

Exemple II.9. Dans $\mathbb{P}^2(K)$, deux droites projectives se rencontrent toujours en un unique point projectif. C'est une propriété qui différencie l'espace projectif de l'espace affine : deux droites parallèles dans le plan affine ne se rencontrent jamais, alors que dans le plan projectif, elles se rencontrent en un point *à l'infini*.

Dans $\mathbb{P}^3(K)$, un plan projectif et une droite projective se coupent en au moins un point. De plus, si la droite n'est pas incluse dans le plan, l'intersection est réduite à exactement un point projectif.

Exemple II.10. Soit le plan projectif $\mathbb{P}^2(K)$. Dans l'espace affine, prenons l'hyperplan $H = \{(x,y,0) \in K^3\}$. Alors $\overline{H} = \{[x,y,0] : (x,y,0) \in K^3\}$ est une droite

projective. Posons $D_\infty = \overline{H}$ que nous appellerons droite à l'infini. Son complémentaire est donné par $\overline{H}^{\complement} = \{[x,y,1] : (x,y,1) \in K^3\} \cong \mathbb{A}^2(K)$. Ainsi

$$\mathbb{P}^2(K) \cong \mathbb{A}^2(K) \dot{\cup} D_\infty.$$

Nous écrirons alors $[x,y,1] = (x,y)$ pour un élément du plan affine dans le plan projectif et $[x,y,0] = (x,y)$ pour un élément de la droite à l'infini lorsque le contexte ne prête pas à ambiguïté.

Soit $\overline{D}$ une droite projective de $\mathbb{P}^2(K)$. C'est l'image d'un sous-espace vectoriel de dimension 2 de K^3, donc déterminé par une équation linéaire $ax+by+cz = 0$ avec a,b et c non tous nuls.

Si $a = b = 0$, alors $D = H$ et donc $\overline{D} = D_\infty$.

Sinon, regardons l'image de D dans $\mathbb{A}^2(K)$. Nous trouvons les points (x,y) vérifiant $ax+by+c = 0$, c'est-à-dire les points de la droite affine définie par cette équation. L'image de D dans D_∞ est l'ensemble des $[x,y,0]$ qui vérifient $ax+by = 0$, qui est réduit au seul point $(-b,a)$. En effet, puisque $a \neq 0$ ou $b \neq 0$ (supposons sans perdre de généralité que $a \neq 0$), le couple (x,y) est solution si et seulement si $x = \frac{-b}{a}y$, c'est-à-dire $(\frac{-b}{a}y, y) = (-b,a)$ car $\frac{y}{a}(-b,a) = (\frac{-b}{a}y, y)$. Le point projectif $(-b,a)$ est le point à l'infini de $\overline{D}$, ce qui correspond à sa direction dans le plan affine. Si D' est une droite affine parallèle à D, alors elles auront la même direction, c'est-à-dire le même point à l'infini dans $\mathbb{P}^2(K)$.

Ainsi, les droites projectives différentes de D_∞ sont en bijection avec les droites affines. De plus, elles sont munies d'un point à l'infini correspondant à la direction de leur droite affine associée.

Exemple II.11. Reprenons la même décomposition du plan projectif mais considérons désormais, à la place des droites projectives, la conique définie par $C \equiv z^2 = xy$.

L'image de C dans $\mathbb{A}^2(K)$ est donné par $z = 1$, d'où $\overline{C} \equiv xy = 1$ est une hyperbole dans le plan affine.

À l'infini, c'est-à-dire dans D_∞, nous obtenons comme équation $xy = 0$, c'est-à-dire que $x = 0$ ou $y = 0$. Les seuls points à l'infini sont donc les éléments $[1,0,0]$ et $[0,1,0]$, ce sont les directions des asymptotes de l'hyperbole $xy = 1$.

Discussion II.12. Quelles sont les applications définissables dans l'espace projectif ? Pour qu'elles soient bien définies, il est nécessaire que deux membres d'une même classe d'équivalence de $\sim$ soient envoyés sur la même image.

Par exemple, la fonction $f(x,y) = (x^2,y)$ ne définit pas une bonne fonction sur le plan projectif car en considérant le point projectif $[1,2] = [2,4]$, nous obtenons que $f[2,4] = [4,4] = [1,1]$ mais $f[1,2] = [1,2] \neq [1,1]$.

Prenons u un automorphisme de E. Nous pouvons lui associer une bijection de l'espace projectif. Considérons l'application $\overline{u}$ définie par :

$$\begin{aligned}\overline{u} : \mathbb{P}(E) &\to \mathbb{P}(E)\\ [x] &\mapsto [u(x)]\end{aligned}$$

Elle est bien définie car si $[x] = [y]$, c'est-à-dire qu'il existe un scalaire non nul tel que $y = \lambda x$, alors $u(y) = \lambda u(x)$ par linéarité de u, et donc $[u(y)] = [\lambda u(x)] = [u(x)]$.

De plus, si $[y]$ est dans l'image, alors comme u est surjectif, il existe $x \in E$ tel que $u(x) = y$, donc $[u(x)] = [y]$, d'où $\overline{u}$ est surjective. Supposons maintenant avoir $[u(x)] = [u(y)]$, il existe donc $\lambda \in K^\times$ tel que $u(x) = \lambda u(y)$. Par linéarité et injectivité de u, nous devons avoir que $x = \lambda y$, et donc $[x] = [y]$, par conséquent $\overline{u}$ est injective.

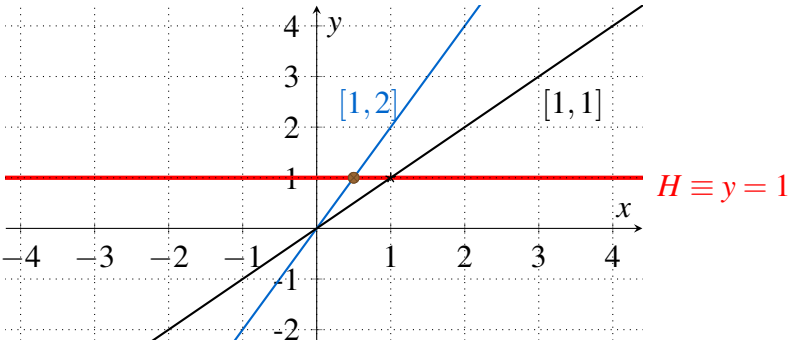
Définition II.13. Soit $u \in \mathrm{Aut}_K(E)$. La bijection de $\mathbb{P}(E)$ associée $\overline{u}$ est appelée une homographie.

Terminons cette section avec plusieurs exemples.

Exemple II.14. Soit la matrice inversible $A = \begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix}$. L'homographie associée à A dans le plan projectif est donné par $[x, y] \mapsto [x + 2y, 3x + y]$.

Regardons comment cette homographie transforme le point $[1, 2]$ dans le plan projectif. Nous avons $\overline{A}[1, 2] = [5, 5] = [1, 1]$.

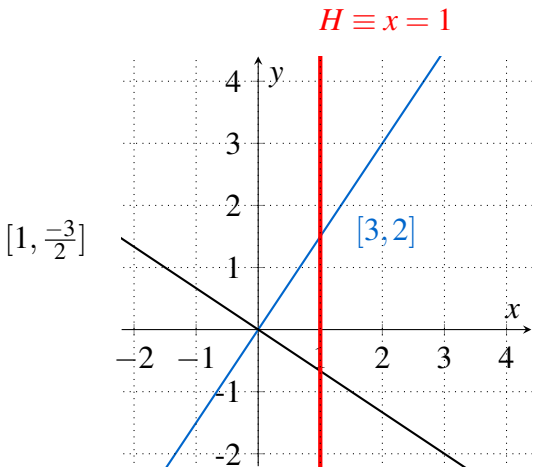
Prenons comme hyperplan $H \equiv y = 1$.



Nous voyons sur le dessin qu'en fait $[1, 2] = [\frac{1}{2}, 1]$ est envoyé sur $[1, 1]$. Le point projectif $[-2, 1]$, c'est-à-dire la droite affine passant par 0 de direction $(-2, 1)$, est envoyé sur $[0, 5]$ qui est la droite à l'infini du plan projectif et correspond à la droite verticale passant par l'origine du plan affine.

Exemple II.15. Soit $\theta \in [0, 2\pi[$. Posons $B = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$. C'est la matrice de rotation d'angle θ dans le plan.

Pour $\theta = \frac{\pi}{2}$, l'homographie associée envoie $[x,y]$ sur $[-y,x]$. Prenons l'hyperplan $H \equiv x = 1$. Les coordonnées homogènes du point projectif $[3,2]$ sur l'hyperplan est donné par $[1,\frac{2}{3}]$. Ainsi $\overline{B}[1,\frac{2}{3}] = [\frac{-2}{3},1] = [1,\frac{-3}{2}]$.



Nous avons comme point à l'infini $[0,1]$, dont la préimage par $\overline{B}$ est donnée par $[1,0]$, la droite horizontale passant par l'origine.

Exemple II.16. Soit h une homothétie de E, c'est-à-dire une application telle qu'il existe un scalaire $\lambda \in K^\times$ vérifiant $h(x) = \lambda x$ pour tout $x \in E$. Alors $\overline{h}$ est l'identité sur le plan projectif car si $x \in E$, alors $\overline{h}[x] = [h(x)] = [\lambda x] = [x]$.

Réciproquement, si u vérifie $[x] = [u(x)]$ pour tout point projectif $[x]$, alors u est une homothétie. En effet, nous avons que pour tout $x \in E$, il existe $\lambda_x \in K^\times$ tel que $[u(x)] = [\lambda_x x]$. Pour obtenir que u soit une homothétie, il faut intervertir le *il existe* avec le *pour tout*.

Si x et y sont libres sur K, alors par linéarité de u, nous avons que

$$u(x+y) = \lambda_{x+y}(x+y) = \lambda_{x+y}x + \lambda_{x+y}y = \lambda_x x + \lambda_y y.$$

Ainsi $(\lambda_{x+y} - \lambda_x)x + (\lambda_{x+y} - \lambda_y)y = 0$. Puisque x et y sont libres, nous devons avoir que $\lambda_{x+y} = \lambda_x = \lambda_y$. Si x et y ne sont pas libres, alors $x = \lambda y$ pour un certain scalaire λ, d'où $u(x) = \lambda_x x = u(\lambda y) = \lambda\lambda_y y = \lambda_y x$, et donc $\lambda_y = \lambda_x$.

Nous avons donc montré que $\lambda_x = \lambda_y$ pour tous $x,y \in E$, et donc que λ_x ne dépend pas de x : nous pouvons donc inverser les deux quantificateurs et nous en déduisons que u est une homothétie.

Ainsi, si nous considérons μ le morphisme de groupes qui va de $GL(E)$ dans l'ensemble des homographies de $\mathbb{P}(E)$ qui envoie h sur $\overline{h}$, nous obtenons que $\mathrm{Ker}(\mu) = \{h : h \in GL(E) \text{ est une homothétie}\}$. Par conséquent :

Corollaire II.17. *L'ensemble des homographies de $\mathbb{P}(E)$ est isomorphe au quotient du groupe général linéaire de E par le sous-groupe des homothéties.*

II.2 Topologie de Zariski projective

Nous allons adapter la topologie de Zariski définie dans l'espace affine à l'espace projectif. Nous travaillerons toujours dans un corps infini K et avec n un naturel non nul.

Une première différence notable est que les polynômes de $K[X_0,\dots X_n]$ ne définissent pas des fonctions sur l'espace projectif. Par exemple dans l'espace projectif $\mathbb{P}^1(\mathbb{R})$, avec $F(X,Y)=X^2+Y$, nous avons que $F(1,-2)=0$ mais $F(-1,2)=3\neq 0$ bien que $[1,-2]=[-1,2]$.

Pour pallier ce problème, nous allons nous intéresser à une certaine classe de polynômes.

Définition II.18. Soit $F\in K[X_0,\dots,X_n]$. Si F est un monôme, on définit son **degré total** comme la somme des degrés en chacune des variables. Plus généralement, le degré total de F est le maximum des degrés totaux de ses monômes.

On dit qu'un polynôme $F\in K[X_0,\dots,X_n]$ est **homogène** si tous ses monômes sont de même degré total.

Par exemple $F(X,Y)=X^2+XY+Y^2$ est homogène mais $G(X,Y)=X^2+Y$ ne l'est pas.

Soit F un polynôme homogène de degré d. Si pour un certain $[x_0,\dots,x_n]\in\mathbb{P}^n(K)$ nous avons $F(x_0,\dots,x_n)=0$, alors $F(\lambda(x_0,\dots,x_n))=\lambda^d F(x_0,\dots,x_n)=0$ pour tout $\lambda\in K^\times$. Ainsi tout élément de la classe $[x_0,\dots,x_n]$ est racine de F si et seulement si un système de coordonnées homogènes de $[x]$ est racine de F.

Définition II.19. Soit $F\in K[X_0,\dots,X_n]$ et $[x]\in\mathbb{P}^n(K)$. On dit que $[x]$ est un **zéro** de F si pour tout $\lambda\in K^\times$, l'égalité $F(\lambda x)=0$ est vérifiée.

Ainsi, si F est homogène et $[x]\in\mathbb{P}^n(K)$, alors $[x]$ est un zéro de F si et seulement si $F(x)=0$. Nous écrirons alors juste $F(x)=0$ pour indiquer que $[x]$ est un zéro de F. Plus généralement, tout polynôme peut s'écrire comme une somme de monômes homogènes. Nous avons la proposition suivante :

Proposition II.20. *Si $F=F_r+\dots+F_0$ avec chacun des F_i homogène de degré total i, nous avons que $F(x)=0$ si et seulement si $F_i(x)=0$ pour tout $i\in\{0,\dots,r\}$.*

Démonstration. Si $F_i(x)=0$ pour tout $i\in\{0,\dots,r\}$, alors $F(x)=0$.

Réciproquement, supposons que $F(x)=0$, c'est-à-dire pour tout $\lambda\in K^\times$,

$$F(\lambda x)=\lambda_r F_r(x)+\dots+\lambda F_1(x)+F_0(x)=0.$$

Considérons le polynôme dans $K[Y]$ donné par $G(Y)=Y^rF_r(x)+\dots+YF_1(x)+F_0(x)$. Si $G(Y)\neq 0$, comme c'est un polynôme de degré fini à une seule indéterminée, ainsi il n'a qu'un nombre fini de racines. Or K est infini, et donc il existe une infinité de solutions λ, d'où les $F_i(x)$ sont tous nuls.

□

Nous allons maintenant développer la topologie de Zariski projective.

Définition II.21. Soit $S \subseteq K[X_0, \dots X_n]$. On définit $V_p(S)$ l'**ensemble algébrique projectif défini par** S le sous-ensemble de $\mathbb{P}^n(K)$ donné par :

$$V_p(S) = \{[x] \in \mathbb{P}^n(K) : \forall F \in S, F(x) = 0\}.$$

Remarque II.22. La proposition II.20 nous dit qu'il suffit seulement de considérer les polynômes homogènes lorsque nous regardons l'ensemble des racines dans $\mathbb{P}^n(K)$ d'un polynôme. Par conséquent, nous pouvons supposer que S ne contient que de polynômes homogènes.

L'application V_p vérifie des propriétés similaires à V. Par exemple, si I est l'idéal engendré par S, alors $V_p(I) = V_p(S)$. De plus, comme $K[X_0, \dots, X_n]$ est noethérien, nous avons que $I = (F_1, \dots, F_r)$ pour certains polynômes homogènes.

Si S est généré par des éléments non homogènes, par exemple $X^2 + XY^2$ et $XY + X$, alors $V_p(S) = V_p(X^2, XY^2, XY, X)$.

Exemple II.23.

- L'espace projectif est un ensemble algébrique projectif car $V_p(\{0\}) = \mathbb{P}^n(K)$. Nous avons aussi que $V_p(K[X_0, \dots, X_n]) = \varnothing$.
- Soit $m = (X_0, \dots, X_n)$ l'idéal des polynômes sans termes constants. Nous appellerons cet idéal l'**idéal inconvenant** [1], nous verrons un peu plus loin qu'il mérite bien cette adjectif. L'ensemble algébrique projectif $V(m)$ est l'ensemble vide car $[x] \in \mathbb{P}^n(K)$ doit vérifier que $x_0 = 0 = x_1 = \dots = x_n$, or 0 n'a pas d'image dans le plan projectif.
- Les singletons sont des ensembles algébriques projectifs.
  Soit $[x] = [x_0, \dots, x_n] \in \mathbb{P}^n(K)$. Sans perdre de généralité supposons $x_0 \neq 0$, alors quitte à diviser chaque composante de x par x_0, nous pouvons supposer que $x_0 = 1$. Alors, nous avons que $\{[x]\} = V_p(X_1 - x_1X_0, \dots, X_n - x_nX_0) = V$.
  Nous avons bien que $[x] \in V$. Réciproquement, soit $[y] = [y_0, \dots, y_n] \in V$, c'est-à-dire que $y_1 = x_1y_0$, … et $y_n = x_ny_0$. Forcément nous devons avoir que $y_0 \neq 0$ car les y_i sont non tous nuls. Par conséquent $x = y_0y$ avec $y_0 \in K^\times$, i.e. $[x] = [y]$.

Remarque II.24. Comme pour les ensembles algébriques affines, la fonction V_p est décroissante. De plus, une intersection quelconque ou une union finie d'ensembles algébriques projectifs est encore un ensemble algébrique projectif. Puisque $\varnothing$ et $\mathbb{P}^n(K)$ sont des ensembles algébriques projectifs, nous avons :

1. En anglais, cet idéal est appelé *the irrelevant ideal*. Daniel Perrin propose dans son ouvrage [7] de le traduire en français par *l'idéal inconvenant*.

Corollaire II.25. *Les ensembles algébriques projectifs sont les fermés d'une topologie sur* $\mathbb{P}^n(K)$.

Nous appellerons cette topologie, la **topologie de Zariski projective**.

Remarque II.26. Pour des sous-ensembles algébriques projectifs de $\mathbb{P}^n(K)$, nous considérerons la topologie induite par celle de $\mathbb{P}^n(K)$.

Comme l'irréductibilité est une notion d'espace topologique, nous avons aussi les mêmes propriétés que dans le cas affine. La décomposition en irréductibles est vérifiée dans tout espace topologique noethérien. Or la topologie de Zariski sur $\mathbb{P}^n(K)$ est aussi un espace noethérien, ainsi nous avons aussi une unique décomposition en irréductibles pour tout ensemble algébrique projectif.

Proposition II.27. *Les homographies sont des homéomorphismes de l'espace projectif muni de la topologie de Zariski projective.*

Démonstration. Soit $\overline{u}$ une homographie de $\mathbb{P}(E)$. Il nous faut vérifier qu'elle est bien continue au sens de la topologie de Zariski projective.

Comme dans le cas affine, nous montrons que :

$$\overline{u}^{-1}(V_p(F_1,\ldots,F_m)) = V_p(F_1 \circ u,\ldots,F_m \circ u).$$

Comme u est un automorphisme de E, la composée $F_i \circ u$ est un polynôme homogène, le tout forme donc bien un fermé de Zariski projectif. Idem pour u^{-1}. □

Définition II.28. Un idéal $I \subseteq K[X_0,\ldots,X_n]$ est dit homogène s'il est engendré par des polynômes homogènes.

Lemme II.29. *Un idéal* $I \subseteq K[X_0,\ldots,X_n]$ *est homogène si et seulement si pour tout* $F \in I$ *de la forme* $F = F_r + \ldots + F_0$ *avec* F_i *homogène de degré i, l'idéal I contient tous les* F_i.

Démonstration. L'implication de droite à gauche est immédiate.

Réciproquement, supposons que I est homogène, c'est-à-dire qu'il existe des polynômes homogènes G_i de degrés α_i engendrant I. Soit $F = F_r + \ldots + F_0 \in I$ avec les F_i homogènes de degré i. Si $r = 0$, alors $F = F_0 \in I$. Sinon, par récurrence sur r, il suffit de montrer que $F_r \in I$. Nous pouvons écrire

$$F = \sum_{i=1}^{k} H_i G_i,$$

avec $H_i \in K[X_0,\ldots,X_n]$. En isolant les termes de plus haut degré et en notant $U_{i,r-\alpha_i}$ le monôme de degré $r-\alpha_i$ de U_i, nous obtenons que $F_r = \sum_{i=1}^{k} U_{i,r-\alpha_i} G_i$, d'où $F_r \in I$. □

Exemple II.30. Soient $V \subseteq \mathbb{P}^n(K)$ un ensemble algébrique projectif et $C(V) = \pi^{-1}(V) \cup \{0_{K^{n+1}}\}$. L'ensemble $C(V)$ est appelé le **cône de** V. Si I est un idéal homogène propre de $K[X_0,\dots,X_n]$, et si $V = V_p(I)$, alors $C(V) = V(I)$ est un ensemble algébrique affine de $\mathbb{A}^{n+1}(K)$. Un élément $(x_0,\dots,x_n) \in K^{n+1}$ non nul annule tous les éléments de I, i.e. $x \in V(I)$, si et seulement si $[x]$ annule tous les élément de I car I est homogène, c'est-à-dire que $[x] \in V_p(I)$. Ainsi $I_p(V) = I(V(I))$.

Sinon $I = K[X_0,\dots,X_n]$ et $C(V) = V(X_0,\dots,X_n) = \{0\}$.

Réciproquement, on dit qu'un ensemble algébrique affine V est un **cône affine** s'il est non vide et si pour tout $\lambda \in K$ et $x \in V$, il vérifie $\lambda x \in V$ (en particulier, il contient le vecteur nul).

Définition II.31. Soit V un sous-ensemble de $\mathbb{P}^n(K)$. On définit $I_p(V)$, l'**idéal (projectif) de V** le sous-ensemble de $K[X_0,\dots,X_n]$ donné par :

$$I_p(V) = \{F \in K[X_0,\dots,X_n] : \forall [x] \in V, F(x) = 0\}.$$

Exemple II.32. Nous avons que $I_p(\varnothing) = K[X_0,\dots,X_n]$ et $I_p(\mathbb{P}^n(K)) = \{0\}$.

Remarque II.33. L'idéal $I_p(V)$ est homogène, et plus précisément engendré par un nombre fini de polynômes homogènes. Comme dans le cas affine, l'application I_p est décroissante. Aussi, l'idéal $I_p(V)$ est radiciel.

De plus, si V est un ensemble algébrique projectif, nous avons $V_p(I_p(V)) = V$ mais en généralement seulement $I \subseteq I_p(V_p(I))$ pour un idéal I de $K[X_0,\dots,X_n]$. Nous pouvons également vérifier que $I_p(V)$ est premier si et seulement si V est irréductible. La preuve est semblable au cas affine : nous nous en dispenserons dans le cadre de ce travail.

II.3 Nullstellensatz projectif

De façon analogue au cas affine, nous voulons une correspondance entre les ensembles algébriques projectifs et les idéaux Supposons maintenant que K soit algébriquement clos.

Lemme II.34. *Si I est homogène, alors $\sqrt{I}$ l'est aussi.*

Démonstration. Soit $F \in \sqrt{I}$, c'est-à-dire qu'il existe un naturel m tel que $F^m \in I$. En particulier, si $F = F_r + \dots + F_0$ avec les F_i homogènes de degré i, nous avons que $F_r^m \in I$ par homogénéité de I. Ainsi, par définition de $\sqrt{I}$, nous en déduisons que $F_r \in \sqrt{I}$. En réitérant l'argument sur la somme $F_{r-1} + \dots + F_0$ et ainsi de suite, nous trouvons par le lemme II.29 que $\sqrt{I}$ est homogène. □

Ce lemme permet de nous rassurer quant au deuxième point du Nullstellensatz.

Théorème II.35 (Nullstellensatz projectif)**.** *Soit I un idéal homogène de $K[X_0,\dots,X_n]$ et soit $V = V_p(I)$. Alors :*

i. L'ensemble algébrique projectif $V_p(I)$ est vide si et seulement si l'idéal inconvenant est contenu dans $\sqrt{I}$;

ii. Si $V_p(I) \neq \varnothing$, alors $I_p(V_p(I)) = \sqrt{I}$.

L'idéal inconvenant porte bien son nom, nous devons traiter son cas à part car il empêche la correspondance entre les idéaux radiciels et les ensembles algébriques projectifs. Ainsi le Nullstellensatz projectif est énoncé en deux parties, une pour traiter ce cas pathogène et une pour la correspondance.

Démonstration. Posons $m = (X_0,\dots,X_n)$ l'idéal inconvenant.

Prouvons *i*. Si $I = K[X_0,\dots,X_n]$, alors $V_p(I) = \varnothing$ et donc le résultat est immédiat. Sinon $I \neq K[X_0,\dots,X_n]$. Considérons le cône $C(V) = V(I) \subseteq K^{n+1}$. En lui appliquant le Nullstellensatz affine, nous obtenons que $I(V(I)) = \sqrt{I}$. Or dire que $V = V_p(I) = \varnothing$, c'est dire que $C(V)$ est réduit à l'origine dans l'espace affine, d'où $V(\sqrt{I}) = \{0\}$. Comme nous avons une bijection entre les idéaux premiers et les ensembles algébriques affines irréductibles, que $V(m) = \{0\}$ et m est premier, nous avons forcément $\sqrt{I} = m$. La réciproque est immédiate.

Prouvons *ii*. Supposons que $V = V_p(I) \neq \varnothing$. Soit $C(V)$ le cône affine de V. Par l'exemple II.30, nous savons que $I_p(V) = I(V(I))$. Par conséquent,

$$I_p(V_p(I)) = I(C(V)) = I(V(I)) = \sqrt{I},$$

par le Nullstellensatz affine. □

Le Nullstellensatz projectif donne ainsi une bijection entre les ensembles algébriques projectifs et les idéaux homogènes radiciels de $K[X_0,\dots,X_n]$ qui ne contiennent pas l'idéal inconvenant.

II.4 Quelques liens entre les topologies de Zariski affine et projective

Nous allons voir quelques liens entre les ensembles algébriques affines et projectifs.

Dans $\mathbb{P}^n(K)$, nous identifions l'espace affine $\mathbb{A}^n(K)$ au complémentaire de $\overline{H} = \{[0,x_1,\dots,x_n] : (0,x_1,\dots,x_n) \in K^{n+1}\}$, c'est-à-dire à l'ensemble

$$\overline{H}^{\complement} = \{[1,x_1,\dots,x_n] : (1,x_1,\dots,x_n) \in K^{n+1}\}.$$

Définition II.36. Soit $F \in K[X_1,\ldots,X_n]$ de la forme $F = F_r + \ldots + F_0$ avec les F_i homogènes de degré i. On définit ${}^hF$ le **polynôme homogénéisé** de F comme :

$$ {}^hF = F_r + F_{r-1}X_0 + \ldots + F_0X_0^r \in K[X_0,X_1,\ldots,X_n]. $$

Par exemple si $F(X,Y) = Y^2 - X^3 - aX - b$, alors ${}^hF(X,Y,Z) = Y^2Z - X^3 - aXZ^2 - bZ^3$ (nous choisissons ici Z à la place de X_0).

Le polynôme homogénéisé est bien sûr homogène (il est fait pour ça).

Notons que, comme dans le cas affine, l'adhérence pour la topologie de Zariski d'un ensemble $S \subseteq \mathbb{P}^n(K)$ est donné par $V_p(I_p(S))$. En particulier, en appliquant I_p, nous obtenons que $I_p(S) = I_p(V_p(I_p(S))) = I_p(\overline{S})$ où $\overline{S}$ désigne la fermeture de S pour la topologie de Zariski projective.

Proposition II.37. *Soit $V \subseteq \mathbb{A}^n(K)$ un ensemble algébrique affine. Soit $\overline{V}$ l'adhérence de V pour la topologie de Zariski projective dans $\mathbb{P}^n(K)$. Alors :*

$$ I_p(\overline{V}) = {}^hI(V) := \{{}^hF : F \in I(V)\}. $$

Démonstration. Soit $F \in I_p(\overline{V})$ un polynôme homogène. Nous voulons montrer que $F \in {}^hI(V)$. Si $a = (a_1,\ldots,a_n) \in V$, alors par identification de l'espace affine, l'élément $(1,a) \in \overline{V}$, ainsi $F(1,a) = 0$, d'où $F(1,X_1,\ldots,X_n) \in I(V)$. Mais

$$ F = X_0^d \, {}^hF(1,X_1,\ldots,X_n) $$

pour un certain d (le degré du polynôme homogénéisé est *minimal* mais pas forcément celui de F) d'où $F \in {}^hI(V)$ car c'est un idéal et ${}^hF(1,X_1,\ldots,X_n) \in {}^hI(V)$.

Réciproquement, soit $F \in I(V)$. Nous voulons montrer que ${}^hF \in I_p(\overline{V})$. Soit $a \in V$, nous avons que $F(a) = 0 = {}^hF(1,a)$, d'où ${}^hF \in I_p(V)$. Or $I_p(V) = I_p(\overline{V})$, ainsi nous avons bien l'inclusion voulue. □

Corollaire II.38. *Soit C une courbe cubique affine définie par*

$$ C \equiv Y^2 = X^3 + aX + b $$

dans $\mathbb{A}^2(K)$ vue dans le plan projectif $\mathbb{P}^2(K)$ en lui attribuant comme troisième coordonnée $Z = 1$. Alors son adhérence pour la topologie de Zariski projective dans le plan projectif est donnée par la courbe cubique projective dans $\mathbb{P}^2(K)$ d'équation

$$ \overline{C} \equiv Y^2Z = X^3 + aXZ^2 + bZ^3. $$

Définition II.39. Si $V \subseteq \mathbb{A}^n(K)$, son adhérence (pour la topologie de Zariski projective) dans $\mathbb{P}^n(K)$ est appelée la **clôture projective de** V.

Nous terminons cette petite section en citant le résultat suivant :

Proposition II.40 ([12]). *Si V est irréductible, alors $V = \overline{V} \cap \mathbb{A}^n(K)$ et $\overline{V}$ est irréductible où $\overline{V}$ est la clôture projective de V.*

Réciproquement, si W est un ensemble algébrique projectif irréductible, alors $V \cap \mathbb{A}^n(K)$ est irréductible et nous avons

$$\text{soit } W \cap \mathbb{A}^n(K) = \varnothing, \text{ soit } W = \overline{W \cap \mathbb{A}^n(K)}.$$

Chapitre III

Courbes elliptiques

Nous allons introduire dans ce chapitre la notion de courbe elliptique. L'objectif sera de simplement les présenter ainsi que quelques une de leurs propriétés : nous ne mènerons pas une étude approfondie.

III.1 Vocabulaire et définition

Plaçons-nous dans le plan projectif $\mathbb{P}^2(K)$ avec K un corps de caractéristique nulle. Nous identifierons l'espace affine $\mathbb{A}^2(K)$ dans le plan projectif par l'ensemble :

$$\mathbb{A}^2(K) = \{[x,y,1] : x,y \in K\}.$$

Nous allons nous intéresser plus précisément à une famille d'ensembles algébriques affines : les courbes cubiques.

Définition III.1. Une **courbe cubique**, ou plus simplement une **cubique** sur K est un ensemble algébrique affine de la forme $V(f)$ où $f \in K[x,y]$ est un polynôme de degré (total) 3.

Nous noterons plutôt $C \equiv f(x,y) = 0$ pour désigner une cubique.

Soit C une cubique définie par $f(x,y) \in K[x,y]$.

Définition III.2. On dit que (u,v) est un K-point si u et v sont dans K.

Exemple III.3. Soit $f(x,y) = x^3 - y$. La cubique associée est donnée par $C \equiv y = x^3$. La courbe C est définie sur $\mathbb{Q}$ mais aussi sur $\mathbb{R}$ ou $\mathbb{C}$, nous pouvons choisir dans quel corps la regarder.

Les points $(0,0)$ et $(1,1)$ de la cubique sont des $\mathbb{Q}$-points et donc des $\mathbb{R}$-points et $\mathbb{C}$-points. Le point $(-\frac{1}{2} + i\frac{\sqrt{3}}{2}, 1)$ est un $\mathbb{C}$-point de C, mais pas un $\mathbb{R}$-point.

Exemple III.4. Si $f(x,y) = y^2 - x^3 - 7x - 1$, la cubique associée est donnée par

$$C \equiv y^2 = x^3 - 7x + 1.$$

Le corollaire II.38 nous dit que la clôture projective de C est donnée par

$$\overline{C} \equiv Y^2Z = X^3 - 7XZ^2 + Z^3.$$

Nous utiliserons les lettres capitales pour désigner les polynômes définissant des ensembles algébriques projectifs et des lettres minuscules pour le cas affine.

En fait, la cubique que nous venons de voir est sous une forme très spéciale :

Définition III.5. On dit qu'une cubique C est **sous la forme de Weierstrass** si elle est de la forme :

$$C \equiv y^2 = x^3 + ax + b.$$

Nous verrons ultérieurement que nous pourrons nous ramener à des cubiques de cette forme pour celles qui nous intéressent.

Définition III.6. Soit $P = (u,v)$ un K-point de C. On dit que P est un **point singulier de** C si

$$\frac{\partial f}{\partial x}(u,v) = \frac{\partial f}{\partial y}(u,v) = 0.$$

Nous dirons que C est **singulière** si elle admet au moins un point singulier. Dans le cas contraire, nous dirons que C est **lisse**.

Ainsi, un point $P \in C$ est un point singulier si et seulement si $\nabla f(P) = 0$.

Exemple III.7. La cubique $C \equiv y = x^3$ définie par $f(x,y) = y - x^3$ est lisse car $\frac{\partial f}{\partial y}(u,v) = 1$ pour tout $(u,v) \in C$.

Par contre, la cubique définie par $f(x,y) = y^2 - x^3$ est singulière car

$$\frac{\partial f}{\partial x}(u,v) = -3u^2 \text{ et } \frac{\partial f}{\partial y}(u,v) = 2v,$$

d'où $(0,0)$ est un point singulier. C'est même le seul car nous devons forcément avoir $v = 0$, et puisque $f(u,0) = u^2 = 0$, nous devons aussi avoir $u = 0$.

Nous dirons que la clôture projective d'une cubique C est lisse si C l'est. Nous parlerons également de cubique projective C pour une clôture projective d'une cubique dans le plan affine.

Nous admettrons le résultat suivant.

Proposition III.8 ([12], Chapitre III)**.** *Soit C une cubique projective lisse définie sur K, avec un K-point. Alors C peut être mise sous la forme de Weierstrass.*

Être mise sous la forme de Weierstrass signifie qu'il existe une application rationnelle sur K de C vers une courbe définie par une équation de Weierstrass. Désormais, pour une cubique admettant un K-point, nous nous cantonnerons à une forme $C \equiv y^2 = x^3 + ax + b$.

Définition III.9. Une courbe elliptique est une paire (E,P) où E est une cubique projective lisse et P est un K-point.

Par la proposition précédente, toute courbe elliptique peut être mise sous la forme de Weierstrass.

Exemple III.10. La cubique projective associée à la cubique $E \equiv y^2 = x^3 + x$ munie du point $(0,0) = [0,0,1]$ est une courbe elliptique. Clairement $(0,0) \in E$. Posons $f(x,y) = y^2 - x^3 - x$. Alors $\frac{\partial f}{\partial x}(u,v) = -3u^2 - 1$ et $\frac{\partial f}{\partial y}(u,v) = 2v$. D'où $\frac{\partial f}{\partial x}(u,v) = 0 = \frac{\partial f}{\partial y}(u,v)$ si et seulement si $u = \frac{\pm\sqrt{3}}{3}$ et $v = 0$. Or les points $(\frac{\pm\sqrt{3}}{3}, 0)$ ne sont pas dans E.

Définition III.11. Soit C une cubique d'équation $y^2 = x^3 + ax + b$. On définit le **discriminant de C**, noté $\Delta(C)$, le nombre $\Delta(C) = -16(4a^3 + 27b^2)$.

Nous mettrons en parallèle le discriminant tout juste défini et le discriminant d'une équation polynomiale de degré 3 de la forme $z^3 + pz + q = 0$ donné par $\Delta = -4p^3 - 27q^2$. Comme la partie en x de C est de la forme $x^3 + ax + b$, le nombre $\Delta(C)$ n'est rien d'autre qu'un multiple du discriminant usuel pour le polynôme en x. Ainsi, ils s'annulent en même temps.

Exemple III.12. Regardons sur nos précédents exemples.

Pour $C \equiv y^2 = x^3$, nous avons que $\Delta(C) = 0$, notons que C n'était pas lisse. De l'autre côté, le discriminant de la cubique lisse $E \equiv y^2 = x^3 + x$ est égal à $\Delta(E) = -64 \neq 0$.

Nous avons la proposition suivante :

Proposition III.13. *Soit C une cubique d'équation $y^2 = x^3 + ax + b$. La cubique C est lisse si et seulement $\Delta(C) \neq 0$.*

Démonstration. Posons $p(x) = x^3 + ax + b$. La cubique C est lisse si et seulement si elle n'a pas de point singulier. Or il existe un point singulier $(u,v) \in C$ si et seulement s'il existe $(u,v) \in C$ tel que $2v = 0$ et $p'(u) = 0$, c'est-à-dire que $v = 0$ et u est une racine multiple de p. Mais p admet une racine multiple si et seulement si son discriminant est nul, c'est-à-dire que $\Delta(C) = 0$. □

Exemple III.14. La cubique $C \equiv y^2 = X^3 - 27X + 54$ n'est pas une courbe elliptique car $\Delta(C) = 0$.

III.2 Loi de groupe

Soit (E,P) une courbe elliptique d'équation $E \equiv y^2 = x^3 + ax + b$ définie sur un corps K de caractéristique nulle. Nous noterons $\overline{E}$ sa clôture projective. Nous allons définir sur l'ensemble des points de $\overline{E}$ une loi de groupe $+$.

Discussion III.15. Remarquons qu'en fait, toute cubique affine lisse est une courbe elliptique dans le plan projectif. Le point $[0,1,0]$ est toujours dans $\overline{E}$ car si

$$F(X,Y,Z) = Y^2Z - X^3 - aXZ^2 - bZ^3,$$

alors $F(0,1,0) = 0$, c'est-à-dire que $[0,1,0] \in \overline{E}$: c'est le point à l'infini. Le point P ne nous est donc plus utile. Nous l'abandonnons sur le bord de la route… Ce point jouera le rôle du neutre de l'opération $+$. Nous notons $[0,1,0] = \mathcal{O}$.

Soient P,Q deux points de $\overline{E}(K)$ et D la droite passant par ces deux points. En premier lieu, nous définissons l'opération binaire $*$ qui envoie le couple de point P et Q sur $P*Q$, le troisième point d'intersection de D avec $\overline{E}$ (possiblement à l'infini, en $\mathcal{O}$). Nous pouvons bien définir cette fonction car dans le plan projectif, une courbe de degré 3 et une courbe de degré 1 (une droite) s'intersectent en exactement trois points. Si $P = Q$, nous prenons D la droite tangente au point P.

Soit D' la droite passant par $P*Q$ et $\mathcal{O}$. Nous définissons alors $P+Q$ comme le troisième point d'intersection de la droite D' avec $\overline{E}$.

Notons que l'opération $*$ n'est pas une loi de groupe car elle n'a pas d'inverse.

Proposition III.1.

(1) La loi $+$ est bien définie sur $\overline{E}(K)$.

(2) La loi $+$ est associative est commutative.

(3) Le point $\mathcal{O}$ en est un élément neutre de $+$.

(4) Pour tout point $P \in \overline{E}(K)$, il existe un point $-P \in \overline{E}(K)$ tel que

$$P + (-P) = \mathcal{O}.$$

Démonstration.

(1) Il faut montrer que $P+Q$ est bien dans $\overline{E}(K)$. Mais la partie en x de $\overline{E}(K)$ est définie par une équation du troisième degré dans K, ainsi si K admet deux racines, alors il admet forcément la troisième, d'où $P*Q$ est dans $\overline{E}(K)$, et donc que $(P*Q)*\mathcal{O}$ est dans $\overline{E}(K)$.

(2) La loi $+$ est clairement commutative. L'associativité est une conséquence de la formule explicite de la loi de groupe que nous allons donner.

(3) Soit D la droite qui passe par P et $\mathcal{O}$. Alors D intersecte $\overline{E}(K)$ aux points $P,\mathcal{O}$ et un certain Q. Alors forcément la droite qui passe par $\mathcal{O}$ et P est le point Q.

(4) Si $P=(x,y)$, alors nous pouvons prendre $-P=(x,-y)$. Clairement $-P$ est toujours dans $\overline{E}(K)$. De plus, la droite qui passe par P et $-P$ est une droite verticale, ainsi $P*Q=\mathcal{O}$. Par conséquent, comme la droite D' passe deux fois par $\mathcal{O}$, elle passe une troisième fois par $\mathcal{O}$ (nous prenons la tangente au point), d'où $P+(-P)=\mathcal{O}$.

□

Ainsi le plongement dans le plan projectif de $E(K)$ nous permet d'obtenir une loi de groupe bien définie sur les points de la courbe.

Corollaire III.16. *La structure $(\overline{E}(K),+,\mathcal{O})$ est un groupe abélien.*

Nous pouvons donner une description sur les points de $E(K)$ de la loi de groupe $+$.

Proposition III.17. *Soit $E\equiv y^2=x^3+ax+b$ une courbe elliptique sur K. Soient $P=(x_1,y_1)$ et $Q=(x_2,y_2)$ des points distincts de $E(K)$. Posons $\lambda=\frac{y_2-y_1}{x_2-x_1}$ et $\nu=\frac{y_1x_2-y_2x_1}{x_2-x_1}$. Nous avons que $P+Q=(x_3,y_3)$ est donné par :*

$$\begin{cases} x_3=\lambda^2-x_1-x_2 \\ y_3=-\lambda x_3-\nu \end{cases}.$$

Démonstration. Soit D la droite qui passe par P et Q. Elle a comme équation $y-y_1=\lambda(x-x_1)$. En substituant y dans l'équation de E, nous obtenons une équation polynomiale $f(x)=0$. Plus précisément, nous avons que

$$x^3+ax+b-y_1^2-2\lambda(x-x_1)-\lambda^2x^2+2\lambda^2x_1x-\lambda^2x_1^2=0.$$

Nous voyons que c'est un polynôme monique dont le coefficient en x^2 est donné par $-\lambda^2$. Mais la somme des racines de l'équation polynomiale cubique est donnée par $-\frac{-\lambda^2}{1}=\lambda^2$. Nous savons déjà que x_1 et x_2 sont des racines de l'équation polynomiale car ce sont les abscisses des points dans l'intersection de D et $E(K)$. Par conséquent nous avons la troisième racine : $x_3=\lambda^2-x_1-x_2$. Pour trouver y_3, il suffit de substituer x_3. □

Exemple III.18. Soit $E\equiv y^2=x^3+17$. Soient $P_1=(-1,4)$ et $P_2=(2,5)\in E(K)$. La droite qui passe par P_1 et P_2 a comme pente $\frac{1}{3}$ et $\nu=\frac{13}{3}$. Le point $P+Q=(x_3,y_3)$ est donc donné par $x_3=\frac{1}{9}+1-2=\frac{-8}{9}$ et $y_3=-\frac{-8}{9}\frac{1}{3}-\frac{13}{3}=-\frac{109}{27}$, d'où

$$P+Q=(\frac{-8}{9},\frac{-109}{27}).$$

Définition III.19. Une **variété algébrique affine** (respectivement **projective**) est un ensemble algébrique affine (respectivement projectif) irréductible.

Nous omettrons les termes affine ou projectif si le contexte ne prête pas à confusion.

Définition III.20. Un **groupe algébrique** G sur K est une variété algébrique (affine ou projective) G sur K munie d'un morphisme de variétés $G \times G \to G$, la multiplication de G, où $G \times G$ est muni de la topologie de Zariski, d'un élément neutre e et d'un morphisme de variétés $G \to G$, l'opération inverse, qui vérifient les axiomes de groupes.

Remarque III.21. Les morphismes de la catégorie des groupes algébriques seront les morphismes de variétés algébriques qui sont aussi des morphismes de groupes.

Exemple III.22. Les courbes elliptiques forment un exemple fondamental de groupes algébriques.

Exemple III.23. Le groupe additif $\mathbb{G}_a^n = (K, +, 0)$ est un groupe algébrique. C'est l'espace affine de dimension n.

Exemple III.24. Un groupe topologique est un groupe $(G, \cdot, 1)$ muni d'une topologie sur G, telle que la loi de groupe et l'inverse soient des applications continues, où la topologie sur $G \times G$ est la topologie produit.

La notion est assez similaire à celle de groupe algébrique mais diffère sur un point : la topologie sur $G \times G$ n'est pas celle du produit pour un groupe algébrique. Ainsi, un groupe algébrique n'est pas forcément un groupe topologique.

Prenons le groupe algébrique $\mathbb{G}_a$ sur un corps K infini. Alors, nous avons vu dans le premier chapitre que la topologie de Zariski correspondait la topologie cofinie. Or, la loi de groupe n'est pas continue pour la topologie produit car $0 \in K$ et il existe une infinité de $a \in K$ tels que $a - a = 0$, c'est-à-dire que

$$(1, -1)K = +^{-1}(\{0\}),$$

qui n'est pas le produit de deux ensembles finis.

III.3 Isogénies

Il est naturel de s'interroger sur les morphismes de ce nouveau type de structure.

Définition III.25. Soient E_1 et E_2 deux courbes elliptiques définies sur un corps K. Une isogénie de E_1 dans E_2 sur K est un morphisme de variétés φ de C_1 vers C_2 définis sur K compatible avec les lois de groupe, c'est-à-dire que $\varphi(P+Q) = \varphi(P) + \varphi(Q)$, pour tous $P, Q \in \overline{E}_1$,

En particulier, le point à l'infini de E_1 est envoyé sur le point à l'infini de E_2. En fait, c'est équivalent. Nous pouvons montrer que si φ est un morphisme de variétés qui envoient $\mathcal{O}_1$ sur $\mathcal{O}_2$, alors c'est une isogénie.

Nous allons lister quelques propriétés sur les isogénies. Pour une preuve de ces résultats, nous pourrons consulter la bible des courbes elliptiques [12].

Théorème III.26 ([12], Théorème II.2.3)**.** *Soit $\varphi : C_1 \to C_2$ un morphisme de courbes. Alors φ est soit constante, soit surjective.*

De ce théorème, nous avons qu'une isogénie est soit surjective, soit triviale. Nous nous intéressons à un certain type d'isogénie.

Exemple III.27. Soit m un entier. Considérons l'application $[m] : E \to E$ qui somme $P \in \overline{E}(K)$ m fois P si $m > 0$, envoie P sur $\mathcal{O}$ si $m = 0$ et somme m fois $-P$ si $m < 0$.

C'est bien une isogénie car $[m](P+Q)$ est donné par

$$(P+Q)+\ldots+(P+Q) = (P+\ldots+P)+(Q+\ldots+Q) = [m](P)+[m](Q),$$

par commutativité de $\overline{E}(K)$. De plus, nous pouvons facilement montrer que $[m]$ est un morphisme de variétés par une induction, en utilisant que $+$ est un morphisme.

Les isogénies de ce type sont toujours surjectives pour $m \neq 0$.

Proposition III.28 ([12], Théorème II.2.3 & Proposition III.4.2)**.** *Soit m un entier non nul. L'isogénie $[m] : E \to E$ est surjective.*

Exemple III.29. Soit E la courbe elliptique d'équation $y^2 = x^3 - x$ définie sur $\mathbb{C}$. L'application $[i] : E \to E : (x,y) \mapsto (-x, iy)$ est une isogénie de E dans elle-même.

Nous donnons une dernière propriété sur les isogénies.

Proposition III.30 ([12], Corollaire 4.9)**.** *Toute isogénie non nulle est à noyau fini.*

Cela implique que tout élément dans l'image a seulement un nombre fini de préimages car a et b ont la même image par f si et seulement si $a - b \in \mathrm{Ker}(f)$.

Discussion III.31. Qui dit groupe, dit points de torsion. Notons que le noyau de l'isogénie $[m]$ nous donne les points de m-torsions, ce qui justifie la prochaine notation.

Définition III.32. Nous écrivons l'ensemble des points de m-torsion de $E(K)$ par $E(K)[m]$. Le groupe de torsion de $E(K)$ est donné par :

$$\mathrm{Tor}(E(K)) = \bigcup_{m=1}^{\infty} E(K)[m].$$

Nous admettrons le résultat suivant, énoncé dans [2] dans un cadre plus général. Nous le restreignons à notre contexte.

Théorème III.33 ([2], Lemme 8.3.19)**.** *Les points de torsion d'une courbe elliptique E définie sur un corps algébriquement clos est Zariski dense dans E.*

Chapitre IV

Notions de théorie des modèles

Sans trop quitter ce que nous avons fait jusqu'à maintenant, nous allons étudier dans ce chapitre une notion générale de théorie des modèles : les prégéométries. En particulier, cette notion généralise le concept de clôture dans la logique du premier ordre. Un exemple notable est la clôture algébrique d'un corps. Avant d'en arriver là, nous considérons d'abord la notion de **fortement minimal**. Ce chapitre répertoriera des résultats classiques de théorie des modèles. Nous pourrons retrouver les prochains résultats dans [2] ou bien [14].

Dans ce contexte, nous considérons une théorie complète T dans un langage $\mathcal{L}$ au plus dénombrable qui admet au moins une structure infinie $\mathcal{M}$. Nous désignons par $\mathcal{L}_M$ le langage $\mathcal{L}$ auquel nous avons ajouté une constante pour chaque élément de M. Nous noterons également une suite finie d'éléments $a_1, \ldots, a_n$ par $\overline{a}$. Soit $\varphi(\bar{v})$ une $\mathcal{L}_M$-formule.

IV.1 Ensemble fortement minimal

Définition IV.1. Soit D un sous-ensemble définissable infini de M^n. On dit que D est **minimal** si pour tout ensemble définissable $Y \subseteq D$, on a Y fini ou bien $D \setminus Y$ fini.

De plus, si $D = \varphi(\bar{v}, M^n)$, on dit aussi que φ est **minimale**.

On dit que D et φ sont **fortement minimaux** s'ils sont minimaux dans toute extension élémentaire de $\mathcal{M}$.

La théorie T est dite **fortement minimale** si la formule $v = v$ est fortement minimale.

Remarque IV.2. Si T est fortement minimale et $\mathcal{M} \models T$, alors $\mathcal{M}$ est fortement minimale. Nous pouvons reformuler que T est fortement minimale si et seulement si pour tout modèle $\mathcal{M}$ de T et toute partie définissable de $\mathcal{M}$ est finie ou cofinie.

Exemple IV.3. Soient $\mathcal{L} = \{E\}$ et la $\mathcal{L}$-théorie T qui axiomatise que E est une relation d'équivalence avec, pour tout naturel n non nul, une unique classe d'équivalence de cardinalité n. Soit $\mathcal{M} \models T$ qui vérifie en plus de ne pas avoir de classe infinie. Nous avons que M est minimale, c'est-à-dire que la formule $v = v$ est minimale. En effet, tout sous-ensemble définissable de M peut s'écrire comme l'union et/ou l'intersection d'un nombre fini de classes d'équivalence ou leur complémentaire. Appartenir à l'union et l'intersection implique qu'il y a un nombre fini de réalisations puisqu'il n'y a que des classes finies. Nous en déduisons que les seuls ensembles définissables sont soit finis, soit cofinis.

Par contre, $v = v$ n'est pas fortement minimale. Si nous regardons une extension élémentaire $\mathcal{N} \succeq \mathcal{M}$ telle que N a une classe infinie, avec $a \in N$ dans cette classe, la formule $\varphi(x,a) \equiv E(x,a)$ définit un ensemble infini dont le complémentaire dans N est aussi infini.

Exemple IV.4. Soit $T = ACF_0$ la théorie des corps algébriquement clos de caractéristique 0 dans le langage $\mathcal{L} = \{+, \cdot, 0, 1\}$. C'est une théorie complète qui a l'élimination des quantificateurs. Ainsi, toute $\mathcal{L}_M$-formule $\varphi(\bar{x})$ peut s'écrire sous la forme

$$\varphi(\bar{x}) \equiv \bigvee_{i \in I} \Big(\bigwedge_{j \in J_i} p_j(\bar{x}) = 0 \wedge \bigwedge_{l \in L_i} q_l(\bar{x}) \neq 0 \Big)$$

où I, J_i, L_i sont des ensembles finis d'indices et les p_j et q_l sont des polynômes à coefficients dans M.

Si pour tout $i \in I$, l'ensemble J_i est non vide et il existe un $p_j(\bar{x}) \neq 0$, l'ensemble des réalisations de φ dans $\mathcal{M}$, noté $\varphi(M)$, est un ensemble fini car un polynôme non nul à un nombre fini de racines.

Sinon il existe un $i_0 \in I$ tel que $J_{i_0} = \varnothing$ (quitte à enlever $p_j = 0$ de la formule). Alors la formule $\neg\varphi(\bar{x})$ est réalisé seulement un nombre fini de fois, c'est-à-dire que l'ensemble $\varphi(M)$ est cofini. En effet, pour i_0, nous avons $J_{i_0} = \varnothing$ et une formule intérieure de la forme

$$\bigwedge_{l \in L_{i_0}} q_l(\bar{x}) \neq 0.$$

Par conséquent, comme la négation de $\varphi(\bar{x})$ est la conjonction de la négation des formules intérieures, une réalisation de $\neg\varphi(\bar{x})$ devra satisfaire

$$\bigvee_{l \in L_{i_0}} q_l(\bar{x}) = 0,$$

qui n'est réalisé qu'un nombre fini de fois.

De tout ça, nous déduisons que que tout sous-ensemble définissable de M est soit fini, soit cofini. Ainsi, la structure $\mathcal{M}$ est minimale. Nous avons aussi que $\mathcal{M}$ est fortement minimale car le raisonnement reste valable pour n'importe quel

corps algébriquement clos M et donc ses extensions élémentaires aussi. Par conséquent, la formule $v = v$ est fortement minimale et donc la théorie ACF_0 aussi.

Exemple IV.5. Soient K un corps, le langage $\mathcal{L} = \{+, 0, \lambda_k : k \in K\}$ et T la $\mathcal{L}$-théorie des K-espaces vectoriels où λ_k est la multiplication scalaire par k. Cette théorie a l'élimination des quantificateurs. Nous pouvons alors facilement montrer que si D est un sous-ensemble définissable infini d'un K-espace vectoriel E, alors les sous-ensembles définissables de D sont les sous-ensembles finis du K-espace vectoriel engendré par D ou bien leur complémentaire, ainsi D est fortement minimal et T aussi.

Exemple IV.6. Soit $T = Th(\mathbb{Z}, s)$ où s vérifie $s(x) = x + 1$, pour tout x. Cette théorie est fortement minimale. En effet, soit $\mathcal{Z} \models T$. Comme T a l'élimination des quantificateurs, toute $\mathcal{L}_Z$-formule peut s'écrire comme une disjonction finie de sous-formules du type $s^n(x) = s^m(z) \wedge s^{n'}(x) \neq s^{m'}(z')$. Nous en déduisons que tout ensemble définissable dans Z est soit fini soit cofini, et donc que $\mathcal{Z}$ est fortement minimal.

IV.2 Clôture algébrique

Soient A un sous-ensemble de M et $D \subseteq M$ un ensemble fortement minimal dans $\mathcal{M}$.

Définition IV.7. On dit que $b \in M$ est **algébrique** sur A s'il existe une $\mathcal{L}_A$-formule $\varphi(x, \bar{a})$ avec un nombre fini de réalisations, c'est-à-dire que $\varphi(M, \bar{a})$ est fini, et tel que $\mathcal{M} \models \varphi(b, \bar{a})$. On note $acl(A)$ l'ensemble des éléments algébriques sur A.

On dit que b est **définissable** dans A s'il existe une $\mathcal{L}_A$-formule $\varphi(x, \bar{a})$ avec $\varphi(M, \bar{a}) = \{b\}$. On note $dcl(A)$ l'ensemble des éléments définissables sur A. C'est un sous-ensemble de $acl(A)$.

Nous dirons que l'une formule $\varphi(\bar{x})$ est **algébrique dans** $\mathcal{M}$ si elle y est réalisée un nombre fini de fois.

Exemple IV.8. Un exemple notable est le cas de la théorie des corps dans laquelle les éléments algébriques correspondent aux racines de polynômes et donc aux éléments algébriques au sens classique du terme.

Par exemple, pour $A = \mathbb{R}$, l'élément i est algébrique sur $\mathbb{R}$ car la formule $\varphi(x) \equiv x^2 + 1 = 0$ définit l'ensemble $\{i, -i\}$. Par contre, l'élément i n'est pas définissable sur $\mathbb{R}$ car aucune formule dans le langage $\mathcal{L}_A$ ne le distingue de $-i$: son polynôme minimal isole son type et donc i et $-i$ satisfont les mêmes formules.

En outre, si $\mathcal{M}$ est un modèle de ACF_0 qui contient $\mathbb{R}$, alors $acl(\mathbb{R}) = \mathbb{C}$. Dans ce contexte, si K est un sous-corps de $\mathcal{M}$, alors l'ensemble $acl(A)$ correspond

exactement à la clôture algébrique au sens habituel de la théorie des corps. Si K n'est pas un corps, alors $acl(K)$ correspond à la clôture algébrique du corps engendré par K.

D'autre part $dcl(\varnothing) = k$ où k est le corps premier de $\mathcal{M}$. Comme k est le corps engendré par le langage, les morphismes fixent k point par point. Pour un corps K, nous avons que $dcl(K) = K$ car si $x \notin K$, alors x est racine d'un polynôme minimal de degré au moins 2, et nous ne pouvons distinguer deux éléments d'un même polynôme minimal de degré > 1 par une formule.

Exemple IV.9. Soient K un corps et T théorie des K-espaces vectoriels. Soit E un K-espace vectoriel. Pour toute partie $A \subseteq E$, la clôture algébrique $acl(A)$ correspond au sous-K-espace vectoriel de E engendré par A.

Considérons maintenant acl dans le cas particulier où D est fortement minimal. Ainsi, pour $A \subseteq D$, on définit $acl_D(A) = \{b \in D : b \text{ est algébrique sur } A\}$. Nous noterons juste acl pour acl_D si le contexte ne prête pas à ambiguïté. Nous pouvons voir acl comme une fonction qui va de $\mathcal{P}(D)$ dans $\mathcal{P}(D)$. Cette application satisfait des propriétés analogues à la clôture algébrique des corps : c'est l'objet du lemme suivant.

Lemme IV.10. *Soit $A \subseteq D$ un ensemble de paramètres. La clôture algébrique vérifient les propriétés suivantes :*

i. (Croissance) $A \subseteq acl(A)$;

ii. (Monotonie) si $A \subseteq B$, alors $acl(A) \subseteq acl(B)$;

iii. (Idempotence) $acl(acl(A)) = acl(A)$;

iv. (Finitude) si $a \in acl(A)$, alors il existe A_0 un sous-ensemble de A fini tel que $a \in acl(A_0)$.

Démonstration. i. Soit $a \in A$. La formule $\varphi(x) \equiv x - a$ définit l'ensemble $\{a\}$ qui est fini et donc $A \subseteq acl(A)$.

ii. Soit $a \in acl(A)$. Il existe φ une $\mathcal{L}_A$-formule qui n'a qu'un nombre fini de réalisations dans $\mathcal{M}$. Or $A \subseteq B$ et donc φ est aussi une $\mathcal{L}_B$-formule, avec un nombre fini de réalisations, que a réalise.

iii. Par monotonie, nous avons déjà que $acl(A) \subseteq acl(acl(A))$. Montrons l'autre inclusion.

Soit $a \in acl(acl(A))$, alors il existe une $\mathcal{L}_{acl(A)}$-formule $\varphi(x, \bar{a})$ avec $\bar{a} = (a_1, \ldots, a_n) \in acl(A)^n$ et $\varphi(M, \bar{a})$ fini de cardinal k. Or les a_i sont algébriques sur A, ainsi il existe des $\mathcal{L}_A$-formules $\varphi_i(x, \bar{b}_i)$ définissant des ensembles finis dans $\mathcal{M}$ contenant respectivement chacun a_i, où les $\bar{b}_i$ sont des collections finies de A. Considérons la formule

$$\psi(x, \bar{b}_1, \ldots, \bar{b}_n) \equiv \exists y_1, \ldots, y_n \big(\varphi_1(y_1, \bar{b}_1) \wedge \ldots \wedge \varphi_n(y_n, \bar{b}_n) \wedge \exists^{\leqslant k} z, \varphi(z, y_1, \ldots, y_n) \wedge \varphi(x, y_1, \ldots, y_n) \big).$$

Cette formule est une $\mathcal{L}_A$-formule ayant un nombre fini de réalisations. De plus, nous avons que $\mathcal{M} \models \psi(a, \bar{b}_1, \ldots, \bar{b}_n)$.

iv. C'est immédiat, il suffit de prendre les paramètres d'une formule algébrique que a réalise.

□

Ce lemme est valable pour tout ensemble définissable D. Par contre, nous avons besoin que D soit fortement minimal pour le prochain énoncé qui rappellera la théorie des espaces vectoriels.

Proposition IV.11 (Lemme d'échange)**.** *Soit $D \subseteq M$ fortement minimal. Soient $A \subseteq D$ et $a, b \in D$. Si $a \in acl(A \cup \{b\}) \setminus acl(A)$, alors $b \in acl(A \cup \{a\})$.*

Démonstration. Nous écrivons $acl(A, b)$ pour $acl(A \cup \{b\})$. Soit $a \in acl(A, b) \setminus acl(A)$. Alors il existe une $\mathcal{L}_A$-formule $\varphi(x, b)$ [1] telle que $a \in \{x \in D : \varphi(x, b)\}$ et $|\{x \in D : \varphi(x, b)\}| = n$ pour un certain naturel non nul n.

Considérons la formule

$$\psi(w) \equiv \exists x_1, \ldots, x_n, \Big(\bigwedge_{i \neq j} x_i \neq x_j \wedge \bigwedge_{i=1}^{n} \varphi(x_i, w) \Big) \wedge \Big(\forall x_{n+1}, \varphi(x_{n+1}, w) \Rightarrow \bigvee_{i=1}^{n} x_{n+1} = x_i \Big).$$

Cette formule affirme que l'ensemble $\{x \in D : \varphi(x, w)\}$ est de cardinalité n.

On a $M \models \psi(b)$ car $\varphi(x, b)$ a n réalisations. Si ψ définit un ensemble fini, puisque $\varphi(x, y)$ est une $\mathcal{L}_A$-formule, la formule ψ est aussi une $\mathcal{L}_A$-formule et donc $b \in acl(A)$. Par conséquent $\varphi(x, b)$ est une $\mathcal{L}_{acl(A)}$-formule, ainsi $a \in acl(acl(A)) = acl(A)$, ce qui contredit la définition de a.

Comme D est fortement minimal, l'ensemble défini par ψ est cofini dans D. Si nous montrons que $\{y \in D : \varphi(a, y) \wedge \psi(y)\}$ est fini, la preuve est terminée car b appartient à cet ensemble et donc $b \in acl(A, a)$.

Supposons au contraire que ce n'est pas le cas. Comme D est fortement minimal, cet ensemble est cofini. Posons $l \in \mathbb{N}$ la cardinalité de son complémentaire dans D. Soit $\chi(x)$ la formule qui exprime que

$$|D \setminus \{y \in D : \varphi(x, y) \wedge \psi(y)\}| = l.$$

1. Il existe en fait une $\mathcal{L}_{A \cup \{b\}}$-formule $\varphi_0(x)$, mais nous ajoutons le paramètre b dans l'argument de $\varphi_0(x)$, ce qui induit une $\mathcal{L}_A$-formule $\varphi(x, b)$.

Elle est analogue à celle décrite ci-dessus pour ψ. Pareillement, si $\chi(x)$ est fini, alors comme a la réalise, nous devons avoir $a \in acl(A)$ ce qui contredit les hypothèses, ainsi $\chi(x)$ définit un ensemble cofini. Nous pouvons alors choisir $a_1, \ldots,$ a_{n+1} tels qu'ils réalisent tous $\chi(x)$ dans $\mathcal{M}$. Les ensembles

$$B_i = \{w \in D : \varphi(a_i, w) \wedge \psi(w)\}$$

sont cofinis par définition des a_i et donc il existe $\hat{b} \in \bigcap_{i=1}^{n+1} B_i$. Alors $\mathcal{M} \models \varphi(a_i, \hat{b})$, d'où $|\{x \in D : \varphi(x, \hat{b})\}| \geqslant n+1$, ce qui contredit que $\mathcal{M} \models \psi(\hat{b})$.

□

Remarque IV.12. Ce lemme n'est en général pas vrai si D n'est pas fortement minimal. Prenons T la théorie des $\mathbb{Z}$-modules dans le langage $\mathcal{L} = \{+, 0, m_z\}$ où m_z est le multiplication scalaire par $z \in \mathbb{Z}$. Dans cette théorie, l'opération de clôture *acl* ne vérifie pas le lemme d'échange.

Prenons $D = \mathbb{Z}^2$ et considérons les modules engendrés

$$\langle (1,0), (0,1) \rangle \text{ et } \langle (2,1), (0,1) \rangle.$$

Prenons $A = \{(0,1)\}$, $a = (2,1)$ et $b = (1,0)$. On a

$$(2,1) \in \langle A \cup \{(1,0)\} \rangle = \langle (0,1), (1,0) \rangle$$

mais

$$(1,0) \notin \langle A \cup \{(2,1)\} \rangle = \langle (0,1), (2,1) \rangle.$$

C'est pour cette raison que dans le cadre des modules, la notion de dimension au sens des espaces vectoriels n'a pas de sens : il existe des modules avec des familles génératrices et libres de cardinalités différentes. Par exemple, nous prouvons facilement que les ensembles $\{1\}$ et $\{2,3\}$ sont libres sur $\mathbb{Z}$ et génèrent le $\mathbb{Z}$-module $\mathbb{Z}$.

Exemple IV.13. Dans le cas de la théorie des K-espaces vectoriels, ce lemme est exactement le lemme d'échange que nous connaissons.

IV.3 Prégéométrie

Nous allons encore incrémenter d'un cran la généralité de ce type d'opération qu'est la clôture. Nous venons d'aborder *acl* qui nous donne une importante diversité d'exemples de clôture modulo l'existence d'ensembles fortement minimaux.

Définition IV.14. Soit X un ensemble et $cl : \mathcal{P}(X) \to \mathcal{P}(X)$ un opérateur sur les parties de X. On dit que (X, cl) est une **prégéométrie** si elle vérifie pour tous $A, B \subseteq X$ et $a, b \in X$:

i. (Croissance & idempotence) $A \subseteq cl(A)$ et $cl(cl(A)) = cl(A)$.
ii. (Monotonie) Si $A \subseteq B \subseteq X$, alors $cl(A) \subseteq cl(B)$.
iii. (Échange) Si $a \in cl(A \cup \{b\})$, alors $a \in cl(A)$ ou $b \in cl(A \cup \{a\})$.
iv. (Finitude) Si $a \in cl(A)$, alors il existe un ensemble fini $A_0 \subseteq A$ tel que $a \in cl(A_0)$.

De plus, pour toute partie $A \subseteq X$, on dit que A est **clos** si $cl(A) = A$.

Exemple IV.15. Soit X un ensemble dans n'importe quelle théorie. Munissons X de $cl : \mathcal{P}(X) \to \mathcal{P}(X) : A \mapsto A$. Le couple (X, cl) est une prégéométrie qu'on appelle triviale. C'est en effet une prégéométrie : nous vérifions facilement les trois premiers points, et pour le dernier il suffit de considérer $A_0 = \{a\}$.

Remarque IV.16. Les exemples fournis par (D, acl) où D est fortement minimal vus plus tôt sont des prégéométries. Si D n'était pas fortement minimal, comme l'exemple IV.12 le montre, nous n'aurions pas forcément la propriété de l'échange.

Considérons à partir de maintenant (X, cl) une prégéométrie.

Définition IV.17. Soit $A \subseteq X$. On dit que A est **libre** si pour tout $a \in A$, $a \notin cl(A \setminus \{a\})$. On dit que B est une **base de** X si B est libre et si $cl(B) = X$.

Remarque IV.18. Nous avons vraiment une généralisation du vocabulaire des bases pour les espaces vectoriels. Soit E un K-espace vectoriel et $A \subseteq E$. Dire que A est libre c'est dire que chaque élément $a \in A$ ne peut pas s'écrire comme une K-combinaison linéaire de $A \setminus \{a\}$, c'est-à-dire comme un élément de $\langle A \setminus \{a\} \rangle = acl(A \setminus \{a\})$, ce qui est exactement la définition de libre ci-dessus. De plus, un ensemble libre A est une base de E si elle est génératrice, c'est-à-dire que $acl(A) = \langle A \rangle = E$.

Les espaces vectoriels forment un cas de prégéométrie fondamental.

Remarque IV.19. Pour une sous-structure $Y \subseteq X$, nous pouvons définir l'opération cl^Y définie par $cl^Y(A) = cl(A) \cap Y$ pour tout $A \subseteq X$. Alors Y muni de cette opération est une prégéométrie.

Nous dirons que $B \subseteq Y$ est une **base** de Y si B est libre et si $cl^Y(B) = Y$.

Lemme IV.20. *Soit $Y \subseteq X$. Il existe toujours une base de Y. De plus, si B_1 et B_2 sont des bases de Y, alors B_1 et B_2 ont même cardinal.*

La preuve est similaire au cas des espaces vectoriels. Un sous-ensemble libre maximal de Y forme une base de Y. De plus, le lemme d'échange nous permet majorer le cardinal de la base B_1 par celui de B_2 et vice-versa. Pour une preuve complète, nous pourrons consulter le lemme 6.1.9 de [2].

Nous pouvons ainsi vraiment parler de dimension au même sens que pour les espaces vectoriels. C'est bien défini puisque toute base a la même cardinalité.

Définition IV.21. Soit $Y \subseteq X$ et B une base de Y. La **dimension** de Y est la cardinalité de B.

Exemple IV.22. Prenons $\mathcal{M} \models ACF_0$ contenant $\mathbb{R}$ et regardons K une extension algébrique de $\mathbb{Q}$. Alors comme $acl(\varnothing) = \overline{\mathbb{Q}}$, nous devons avoir que K est de dimension 0. Si X est transcendant sur $\mathbb{Q}$, alors $\mathbb{Q}(X)$ est de dimension 1. Le corps des réels est de dimension $2^{\aleph_0}$.

Dans ce cas, la dimension d'une extension de $\mathbb{Q}$ n'est rien d'autre que son **degré de transcendance**.

Exemple IV.23. Si X est munie de la prégéométrie triviale, alors la dimension d'un sous-ensemble $Y \subseteq X$ est juste son cardinal.

Définition IV.24. Soit $A \subseteq X$. On appelle (X, cl_A) la **localisation sur** A où pour toute partie $B \subseteq X$, $cl_A(B) = cl(A \cup B)$ définie sur $\mathcal{P}(X)$.

Lemme IV.25. *Pour tout $A \subseteq X$, (X, cl_A) est une prégéométrie.*

Démonstration. Vérifions les différents axiomes. Soient $B, C \subseteq X$ et $a, b \in X$. Attention à ne pas trop cligner des yeux.

i. $B \subseteq cl(B) \subseteq cl_A(B) = cl(A \cup B)$ car $B \subseteq A \cup B \Rightarrow cl(B) \subseteq cl(A \cup B)$. De plus, $cl_A(cl_A(B)) = cl_A(cl(A \cup B)) = cl(A \cup cl(A \cup B)) = cl(A \cup B) = cl_A(B)$ car $A \subseteq cl(A \cup B)$.

ii. Si $B \subseteq C \subseteq X$, alors $cl_A(B) = cl(A \cup B) \subseteq cl(A \cup C) = cl_A(C)$ car $B \subseteq C \Rightarrow A \cup B \subseteq A \cup C$.

iii. Si $a \in cl_A(B \cup \{b\}) = cl(A \cup B \cup \{b\})$, alors puisque (X, cl) est une prégéométrie, $a \in cl(A \cup B)$ ou $b \in cl(A \cup B \cup \{a\})$, c'est-à-dire que $a \in cl_A(A)$ ou $b \in cl_A(B \cup \{a\})$.

iv. Si $a \in cl_A(B) = cl(A \cup B)$, alors il existe un ensemble fini $B_0 \subseteq A \cup B$ tel que $a \in cl(B_0)$. En particulier $a \in cl(A \cup B_0)$ d'où $a \in cl_A(B_0)$.

□

Soient $Y \subseteq X$ et $A \subseteq X$. On dit que Y est libre sur A si Y est libre dans (X, cl_A). On note $\dim(Y/A)$, appelée la **dimension de Y sur A**, la dimension de Y dans (X, cl_A).

Exemple IV.26. Si X est muni de la prégéométrie triviale et $A, Y \subseteq X$, alors $\dim(Y/A) = |Y \setminus A|$. En effet, une base de $Y \cup A$ est donnée par $Y \setminus A$.

Exemple IV.27. Dans ACF_0, le corps des complexes $\mathbb{C}$ est de dimension (de degré de transcendance) 0 sur $\mathbb{R}$. Plus généralement, si K est une extension de $\mathbb{Q}$, alors toute extension algébrique de K sera de degré 0 sur K.

Définition IV.28. On dit que (X, cl) est une **géométrie** si $cl(\varnothing) = \varnothing$ et si pour tout $x \in X$, $cl(\{x\}) = \{x\}$.

Si E est un K-espace vectoriel muni de acl, alors (E, acl) n'est pas une géométrie car $acl(\varnothing) = \{0\}$. Pareil, dans ACF_0, si $\mathcal{M}$ est un corps algébriquement clos, alors $acl(\varnothing) = \overline{\mathbb{Q}}$.

Discussion IV.29. Si (X, cl) est une prégéométrie, nous pouvons construire une géométrie associée assez naturelle. Soit $X_0 = X \setminus cl(\varnothing)$.

Considérons la relation d'équivalence $\sim$ sur X_0 définie comme suit. Pour $a, b \in X_0$, nous dirons que $a \sim b$ si et seulement si $cl(\{a\}) = cl(\{b\})$. C'est bien une relation d'équivalence : nous avons clairement $a \sim a$ et $a \sim b$ si et seulement si $b \sim a$ par symétrie de l'égalité. De plus, si $a \sim b$ et $b \sim c$, c'est-à-dire $cl(\{a\}) = cl(\{b\}) = cl(\{c\})$, et donc $a \sim c$.

Nous définissons alors la prégéométrie $(\hat{X}, \hat{cl})$ définie sur $\hat{X} = X_0/\sim$ par

$$\hat{cl}(A/\sim) = \{[b] : b \in cl(A) \cap X_0\}.$$

C'est exactement le même procédé que nous avons réalisé pour construire l'espace projectif $\mathbb{P}^n(E)$. Nous en rediscuterons un peu plus tard dans cette section.

Corollaire IV.30. *Soit E un K-espace vectoriel. L'espace projectif $\mathbb{P}(E)$ muni de l'application définie ci-dessus est une géométrie induite par la prégéométrie de (E, acl).*

Exemple IV.31. Regardons cette construction dans le cas d'AFC_0.

Prenonds $X = \mathbb{C}$ le corps des complexes, alors $acl(\varnothing) = \overline{\mathbb{Q}}$, regardons donc $\mathbb{C}_0 = \mathbb{C} \setminus \overline{\mathbb{Q}}$. C'est l'ensemble des éléments transcendants de $\mathbb{C}$ sur $\mathbb{Q}$. Deux éléments a et b transcendants seront équivalents si $\overline{\mathbb{Q}}(a) = \overline{\mathbb{Q}}(b)$, c'est-à-dire qu'ils sont algébriques sur $\overline{\mathbb{Q}}$, ou plus simplement sur $\mathbb{Q}$ car $acl(acl(\varnothing)) = acl(\varnothing)$. Par exemple les éléments π et $-\sqrt{2}\pi$ sont équivalents.

Une classe d'équivalence d'un élément transcendant a est l'ensemble maximal des éléments transcendants deux-à-deux algébriques sur $\mathbb{Q}$.

Lemme IV.32. *La structure $(\hat{X}, \hat{cl})$ est une géométrie.*

Démonstration. Vérifions que c'est une géométrie. Nous avons que $\hat{cl}(\varnothing) = \{[b] : b \in cl(\varnothing) \setminus cl(\varnothing)\}$.

De plus, par construction, tous les éléments de $[b]$ ont la même clôture et sont les seuls, car $[c] \in \hat{cl}(\{[b]\})$ si et seulement si $c \in [b]$. Nous en déduisons que $\hat{cl}(\{[b]\}) = \{[b]\}$. □

Nous allons maintenant donner quelques définitions que nous illustrerons un peu plus loin.

Définition IV.33. On dit que (X, cl) est **trivial** si pour toute partie $A \subseteq X$,

$$cl(A) = \bigcup_{a \in A} cl(\{a\}).$$

Définition IV.34. On dit que (X, cl) est **modulaire** si pour tous sous-ensembles $A, B \subseteq X$ clos de dimension finie,

$$dim(A \cup B) = dim(A) + dim(B) - dim(A \cap B).$$

On dit que (X, cl) est **localement modulaire** si $(X, cl_{\{a\}})$ est modulaire pour un certain $a \in X$.

Passons un certain moment pour mieux comprendre ces différentes propriétés.

Exemple IV.35 (Prégéométrie triviale)**.** Reprenons l'exemple IV.15. Montrons que la prégéométrie (X, cl) est triviale au sens de la définition ci-dessus. Soit $A \subseteq X$. Nous avons que $cl(A) = A = \bigcup_{a \in A} \{a\} = \bigcup_{a \in A} cl(\{a\})$.

De plus, cette prégéométrie est une géométrie. En effet : $cl(\varnothing) = \varnothing$ par définition de cl et pour tout $x \in X$, $cl(\{x\}) = \{x\}$.

Il faut faire attention qu'une prégéométrie triviale [2] n'est pas forcément une géométrie comme l'illustre l'exemple suivant.

Exemple IV.36 (Successeur)**.** Soit $\mathcal{L} = \{s\}$ où s est une fonction unaire et $T = Th(\mathbb{Z}, s)$ où $s(x) = x + 1$ est la fonction de successeur. Soit $D \models T$. Alors $acl(\varnothing) = \varnothing$ et pour toute partie $A \subseteq D$, $acl(A) = \{s^n(a) : a \in A, n \in \mathbb{Z}\}$. Nous savons déjà que acl est une prégéométrie puisque D est fortement minimal. De plus, $acl(A) = \{s^n(a) : a \in A, n \in \mathbb{N}\}$.

Ici, (D, acl) est une prégéométrie triviale qui n'est pas une géométrie. Elle est bien triviale puisque

$$acl(A) = \{s^n(a) | a \in A, n \in \mathbb{N}\} = \bigcup_{a \in A} \{s^n(a) : n \in \mathbb{N}\} = \bigcup_{a \in A} acl(\{a\}).$$

Cependant, elle n'est pas une géométrie car $acl(\{a\}) \neq \{a\}$.

Remarque IV.37. Toute prégéométrie triviale est modulaire.

Exemple IV.38 (Géométrie projective)**.** Reprenons l'exemple IV.9 sur les espaces vectoriels. Soit $E \models T$ un K-espace vectoriel de cardinalité infinie. Le couple (E, acl) est une prégéométrie puisque E est fortement minimal. Par la formule de Grassmann, (E, acl) est modulaire. Ce n'est pas une géométrie car $acl(\varnothing) =$

2. À partir de maintenant, nous utiliserons cette terminaison au sens de la définition IV.33.

$\{0\} \neq \varnothing$ mais aussi car pour tout $a \in E \setminus \{0\}$, l'ensemble $acl(\{a\})$ est l'espace vectoriel engendré par a dans E. C'est la droite qui passe par a et 0.

Comme précédemment, construisons la géométrie associée $(\hat{E}, \hat{acl})$. Retirons donc $\{0\} = acl(\varnothing)$ de E : posons $E_0 = E \setminus \{0\}$. Définissons alors la relation d'équivalence pour tout élément $a, b \in E_0$: $a \sim b$ si et seulement si $acl(a) = acl(b)$, c'est-à-dire si et seulement si a et b décrivent la même droite passant par l'origine (a et b sont non-nuls donc ils décrivent bien une seule et même droite). C'est exactement la relation d'équivalence que nous avions définie pour construire l'espace projectif. Il ne nous reste plus qu'à quotienter E_0 par cette relation d'équivalence pour retrouver l'espace projectif $\mathbb{P}(E)$.

De plus, si S est un sous-ensemble de E, alors $cl(S) = \langle S \rangle$ et en notant $\overline{S}$ son image dans le plan projectif, nous obtenons que $\hat{cl}(\overline{S}) = \{[b] : b \in \langle S \rangle \setminus \{0\}\}$. C'est donc l'ensemble des droites vectorielles de l'espace vectoriel engendré par S.

Exemple IV.39 (Corps algébriquement clos)**.** Soit K un corps algébriquement clos de degré de transcendance au moins 4 sur $\mathbb{Q}$ (par exemple $\mathbb{C}$). Nous allons montrer que (K, acl) n'est pas une prégéométrie modulaire. Rappelons-nous que dans ce cas, la dimension est le degré de transcendance.

Soit $k = \mathbb{Q}$ le corps premier de K. Prenons x, y, x' et y' des éléments transcendants de K algébriquement indépendants sur k. Soient $a, b \in K$ tels que $ax + b = y$ et $ax' + b = y'$. La famille x, x', a, b génère le même sous-corps de K que x, y, x', y' et donc sont algébriquement indépendants : ils forment un ensemble générateur, de même cardinal que la base, donc ils sont libres. Par conséquent, les corps $k(x)$ et $k(x')$ sont isomorphes sur la clôture algébrique de $k(a,b)$. Cet isomorphisme envoie y sur y' et nous avons alors

$$acl(k(x,y)) \cap acl(k(a,b)) \subseteq acl(k(x,y)) \cap acl(k(x',y')) = k,$$

car x, x', y, y' sont algébriquement indépendants sur k. Alors, nous obtenons que

$$\begin{aligned} \dim(k(x,y,a,b)) &= 3 \\ &< \dim(k(x,y)) + \dim(k(a,b)) - \dim(k) \\ &= 2 + 2 - 0 = 4, \end{aligned}$$

c'est-à-dire que (K, acl) n'est pas modulaire.

Discussion IV.40 (Même ouvrage que [3], Dimensions and Homogeneity in Mathematical Structures, B. Zilber)**.**

Le mathématicien Boris Zilber avait conjecturé en 1983 que si M était un ensemble fortement minimal, alors la prégéométrie (M, acl) devait être d'un (seul) des trois types suivants. La prégéométrie (M, acl) est :

- soit triviale ;

- soit interprétable de façon équivalente comme un corps algébriquement clos ;
- soit isomorphe à une prégéométrie d'un espace projectif ou affine sur un anneau à division fini ou dénombrable.

Ce n'est que plus tard que Hrushovski, aux alentours de 1990, a exhibé une prégéométrie ne satisfaisant pas cette trichotomie.

IV.4 Dimension d'une variété algébrique

Revenons dans un cadre plus précis, celui des variétés algébriques. Nous allons définir une notion de dimension sur celles-ci.

Rappelons qu'une chaîne d'ensembles de la forme $Y_0 \subset \ldots \subset Y_n$ est de longueur n (nous comptons le nombre d'inclusions propres) et que l'ensemble vide n'est pas irréductible.

Définition IV.41. Soit X un espace topologique. On définit la **dimension de Krull** de X, noté $\dim(X)$, comme le supremum des longueurs de chaînes de parties fermés irréductibles de X. Par convention, l'ensemble vide $\varnothing$ est de dimension $-\infty$.

Si X est une variété algébrique, alors $\dim(X)$ est borné car X admet une décomposition finie en irréductibles.

Exemple IV.42. La remarque I.37 nous dit que dans un espace topologique séparé, les seuls irréductibles sont les singletons. Ainsi, dans un espace topologique séparé, tous les ensembles non vides sont de dimension 1. En effet, si $Y \subseteq X$ est non vide, alors pour tout $y \in Y$, la chaîne $\{y\} \subseteq Y$ est de longueur maximale.

Proposition IV.43. *Soient X un espace topologique et Y un sous-espace topologique de X. Alors $dim(X) > dim(Y)$.*

*Si X est de dimension finie, alors la **codimension** de Y est défini par :*

$$codim(Y) = dim(X) - dim(Y).$$

Si X est irréductible et de dimension finie, et Y est un sous-fermé propre de X, alors $dim(Y) < dim(X)$.

Démonstration. Montrons la première assertion. Soit $F_1 \subset \ldots \subset F_n$ une chaîne de fermés irréductibles de Y. Dans la proposition I.41, nous avons vu que si F est un fermé irréductible dans un sous-espace topologique, alors son adhérence est encore irréductible dans l'espace entier. Ainsi $\overline{F}_1 \subset \ldots \subset \overline{F}_n$ est aussi une chaîne de fermés irréductible de X. En outre, comme ce sont des fermés de Y, ils sont tous distincts car $F_i = \overline{F}_i \cap Y$.

Pour la seconde assertion, il suffit d'ajouter X à une chaîne maximale de Y. □

Proposition IV.44. *Soit X un espace topologique. Supposons que $X = X_1 \cup \ldots \cup X_n$ avec les X_i fermés. Alors $dim(X) = sup_{1 \leqslant i \leqslant n}\ dim(X_i)$.*

Démonstration. Par la proposition précédente, nous avons que $\dim(X) \geqslant \dim(X_i)$ pour tout i, et donc que $\dim(X) \geqslant \sup_{1 \leqslant i \leqslant n} \dim(X_i)$.

Réciproquement, posons $p = \sup_{1 \leqslant i \leqslant n} \dim(X_i)$. Si p est infini, le résultat est immédiat. Supposons donc $0 \leqslant p < +\infty$. Par l'absurde, supposons qu'il existe une chaîne de fermés irréductibles de X de longueur $p+1$:

$$F_0 \subset \ldots \subset F_{p+1}.$$

Nous avons que $F_{p+1} = (X_1 \cap F_{p+1}) \cup \ldots \cup (X_n \cap F_{p+1})$. Mais F_{p+1} est irréductible, d'où $F_{p+1} = F_{p+1} \cap X_j$ pour un certain j, c'est-à-dire que $F_{p+1} \subseteq X_j$, ce qui contredit $\dim(X_j) \leqslant p$. □

Définition IV.45. Soit V une variété algébrique affine ou projective. On définit la **dimension** de V comme sa dimension de Krull pour la topologie de Zariski.

Notons $\mathrm{tr}[K : k]$ le degré de transcendance sur k d'un corps K. Nous admettrons le théorème suivant :

Théorème IV.46 ([8], Théorème IV.1.8)**.** *Soit V une variété algébrique affine sur un corps K. Alors la dimension de V est égale au degré de transcendance sur K du corps de fonctions rationnelles de K, c'est-à-dire*

$$dim(V) = tr[Frac(\Gamma(V)) : K].$$

Exemple IV.47. L'espace affine $\mathbb{A}^n(K)$ est de dimension n car son anneau de fonctions régulières est donnée par $\Gamma(K^n) = K[X_1, \ldots, X_n]$ et $K(X_1, \ldots, X_n)$ est de degré de transcendance n sur K.

En particulier, la dimension d'une variété algébrique affine est finie.

Définition IV.48. Soient V une variété algébrique (affine ou projective) définie sur K par $I = (F_1, \ldots, F_r)$ et $a \in V$. On définit l'**espace tangent de V en a** par :

$$T_a(V) = \ \mathrm{Ker}\ d_a(F_1, \ldots, F_r),$$

où d_a désigne la matrice jacobienne des F_i au point a. C'est un K-espace vectoriel.

On dit qu'un point $a \in V$ est **lisse** si $\dim(V) = \dim_K T_a(V)$ où $\dim_K$ désigne la dimension de K-espace vectoriel. On dit que la variété V est **lisse** si tous ses points sont lisses.

Si V n'est pas irréductible, nous demandons que $\dim_a(V) = \dim\ T_a(V)$ où $\dim_a(V)$ est le supremum des dimensions des composantes irréductibles passant par a.

Proposition IV.49 (Critère jacobien)**.** *Soit $V = V(F_1, \ldots, F_r)$ une variété algébrique affine de dimension d dans $\mathbb{A}^n(K)$. La variété V est lisse si et seulement si sa jacobienne en tout point $a \in V$ est de rang $n-d$.*

Démonstration. Soit $d_a(V)$ la matrice jacobienne de V au point a :

$$d_a(V) = \begin{pmatrix} \frac{\partial F_1}{\partial X_1}(a) & \ldots & \frac{\partial F_1}{\partial X_n}(a) \\ \vdots & \ddots & \vdots \\ \frac{\partial F_r}{\partial X_1}(a) & \ldots & \frac{\partial F_r}{\partial X_n}(a) \end{pmatrix}.$$

C'est une fonction linéaire $d_a(F_1, \ldots, F_r) : K^n \to K^r$, d'où par le théorème du rang :

$$n = dim\ \mathrm{Ker}(d_a(V)) + \mathrm{Rang}(d_a(V)).$$

Cela veut dire que $\dim_K T_a(V)) = n - \mathrm{Rang}(d_a(V))$. Nous obtenons que :

$$\begin{aligned} V \text{ est lisse} &\iff \dim_K T_a(V) = d \\ &\iff \mathrm{Rang}\ d_a(F_1, \ldots, F_r) = n - d. \end{aligned}$$

□

Cette proposition reste vrai dans le cas d'une variété projective, voir [8], proposition V.2.6.

Remarque IV.50. Cette définition de lissité est consistante avec celle donnée pour les courbes elliptiques.

IV.5 Cardinal inaccessible

Nous aurons besoin pour nos constructions de cardinaux bien particuliers. Nous tirons les résultats de ce chapitre de l'appendice A de [2].

Rappelons-nous quelques propriétés sur les cardinaux et les ordinaux.

Un ensemble X est un ordinal s'il est transitif, i.e. il vérifie pour tout $x \in X$, si $y \in x$, alors $y \in X$, et si X est bien ordonné par $\in$. Soit On la classe de tous les ordinaux. C'est un ensemble bien ordonné.

Soit A muni d'un bon ordre (existe par Zorn) tel que $(A, <)$ est isomorphe à un ordinal α. Nous écrirons $|A|$ le plus petit ordinal (c'est bien défini car On est bien ordonné) tel qu'il existe un bon ordre de A isomorphe à cet ordinal.

Proposition IV.51. *Soient A et B deux ensembles. Les assertions suivantes sont équivalentes :*

(1) $|A| = |B|$;

(2) Il existe une bijection $f : A \to B$;

(3) Il existe des fonctions injectives $f : A \to B$ et $g : B \to A$.

Nous notons ω l'ordinal $|\mathbb{N}|$. Nous disons que A est dénombrable si $|A| \leqslant \omega$. Soit l'ensemble $\omega_1 = \{\alpha \in On : \alpha \text{ est dénombrable}\}$. Alors ω_1 n'est pas dénombrable car sinon $\omega_1 \in \omega_1$, ce qui contredit ZFC. Ainsi ω_1 est le premier ordinal non dénombrable. De plus, il vérifie $|\omega_1| = \omega_1$.

Définition IV.52. Nous disons que α est un **cardinal** si $|\alpha| = \alpha$.

Nous pouvons construire récursivement ω_α par :
- $\omega_0 = \omega$;
- $\omega_{\alpha+1} = \{\delta \in On : |\delta| = \omega_\alpha\}$;
- Si α est un ordinal limite, alors $\omega_\alpha = \sup_{\beta<\alpha}\omega_\beta$.

Proposition IV.53. *Chaque ω_α est un cardinal et $\omega_\alpha < \omega_\beta$ si $\alpha < \beta$.*

De plus, si κ est un cardinal, alors soit $\kappa < \omega$ ou bien $\kappa = \omega_\alpha$ pour un certain $\alpha \in On$.

Nous utiliserons la notation $\aleph_\alpha = \omega_\alpha$ pour parler du cardinal. Si κ est un cardinal, alors il y a un plus petit cardinal strictement plus grand que κ. Nous l'appelons le **successeur** de κ et le notons κ^+. Nous disons que κ est un **cardinal successeur** s'il existe un cardinal λ tel que $\lambda^+ = \kappa$, dans le cas contraire, nous disons que κ est un ordinal limite.

Définition IV.54. Soient A un ensemble et $B \subseteq A$. On dit que B est **cofinal** si pour tout $a \in A$, il existe $b \in B$ tel que $a \leqslant b$.

On définit alors $\text{cof}(A)$, la **cofinalité** de l'ensemble A comme le cardinal du plus petit sous-ensemble cofinal de A.

Soit $\alpha > \omega$ un ordinal limite. Nous définissons la **cofinalité de** α comme le plus petit cardinal λ tel qu'il existe une fonction $f : \lambda \to \alpha$ tel que l'image de f n'est pas bornée dans α. Nous notons alors $\text{cof}(\alpha) = \lambda$.

La cofinalité de α est en quelques sorte le plus petit cardinal permettant de parcourir α.

Exemple IV.55. Soit $\alpha = \omega$. Alors $\text{cof}(\omega) = \aleph_0$ car une fonction finie ne pas être à image bornée, et clairement $\text{cof}(\alpha) \leqslant \alpha$.

En outre, nous avons que $\text{cof}(\omega_\omega) = \aleph_0$ car la fonction $f : \aleph_0 \to \omega_\omega$ qui envoie n sur ω_n n'est pas borné.

Définition IV.56. Soit κ un cardinal. On dit que κ est **régulier** si $\text{cof}(\kappa) = \kappa$. Autrement, on dit que κ est **singulier**.

Exemple IV.57. Le cardinal $\aleph_0$ est régulier alors que $\aleph_\omega$ est singulier.

Proposition IV.58. *Si $\kappa \geqslant \aleph_0$ est un cardinal, alors κ^+ est régulier.*

Le cardinal $\aleph_0$ est un cardinal limite régulier, mais c'est peut-être bien le seul vérifiant ces deux propriétés.

Définition IV.59. Un cardinal $\kappa > \aleph_0$ est dit **(faiblement) inaccessible** si κ est un cardinal limite régulier.

Il est impossible dans ZFC de prouver l'existence d'un cardinal inaccessible.

Théorème IV.60. *Dans ZFC, supposée cohérente, nous ne pouvons pas démontrer l'existence d'un cardinal inaccessible, c'est-à-dire que si la théorie ZFC est cohérente, alors la théorie ZFC + $\{$il n'existe pas de cardinal inaccessible$\}$ est cohérente.*

Nous ferons le choix lors de l'une de nos constructions de corps différentiellement clos rigides d'accepter l'existence d'un tel cardinal (nous sortirons donc de la théorie ZFC).

Proposition IV.61. *Si $\kappa > \aleph_0$ est inaccessible, alors $\kappa = \aleph_\kappa$.*

Démonstration. Par induction transfinie, nous avons pour tout ordinal α, l'inégalité $\omega_\alpha > \alpha$. Or la proposition IV.53 nous dit que $\kappa = \aleph_\alpha$ pour un certain ordinal α. Si $\omega < \kappa$, alors la fonction qui envoie $\beta \mapsto \omega_\beta$ est une fonction de α dans κ qui n'est pas majorée, une contradiction avec κ régulier. □

Chapitre V

Théorie des modèles des corps différentiels

V.1 Annneaux différentiels

Nous allons travailler ici en caractéristique 0. Prenons un anneau commutatif intègre A de caractéristique nulle muni d'une fonction unaire $\delta : A \to A$.

Définition V.1. On dit que le couple (A, δ) est un **anneau différentiel** si :

- pour tous $a, b \in A$, on a $\delta(a+b) = \delta(a) + \delta(b)$;
- pour tous $a, b \in A$, on a $\delta(ab) = \delta(a)b + a\delta(b)$.

Le cas échéant, on appelle δ une **dérivée**.

Si A est un corps, nous dirons que (A, δ) est un **corps différentiel**.
La deuxième condition est appelée la règle de Leibniz.

Exemple V.2.

- Tout anneau muni de l'application δ définie par $x \mapsto 0$ est un anneau différentiel. Cette dérivée est appelée la dérivée triviale.
- Soit I un ouvert de $\mathbb{R}$. L'anneau $C^\infty(I)$ des fonctions indéfiniment dérivables sur I muni de la dérivée usuelle est un anneau différentiel.
- Soit K un corps et $K[X]$ son anneau des polynômes. L'anneau $K[X]$ muni de la dérivée usuelle est un anneau différentiel.

Travaillons désormais avec un anneau différentiel (A, δ).

Remarque V.3. Demander que $\delta(a+b) = \delta(a) + \delta(b)$ pour tous éléments x et y de A, c'est exactement dire que δ est un endomorphisme de groupes de $(A, +, 0)$. Ainsi, le noyau de cette application est aussi un groupe. C'est l'ensemble des éléments de A qui sont de dérivée nulle,

$$\mathrm{Ker}(\delta) = \{a \in A : \delta(a) = 0\}.$$

Remarque V.4. L'ensemble des dérivées de A muni de l'addition de fonctions forme un groupe dont le neutre est la dérivée triviale.

Définition V.5. Un élément de A qui est de dérivée nulle est appelée une **constante**. On note l'ensemble des constantes de A par C_A.

Lemme V.6. *L'ensemble des constantes C_A est un sous-anneau de A. De plus, si A est un corps, alors l'ensemble C_A est un sous-corps de A.*

Démonstration. Soient $a,b \in C_A$. Nous savons déjà que C_A est un groupe additif, il nous suffit donc de montrer qu'il contient 1 et est stable par multiplication. Nous avons que $\delta(1) = \delta(1.1) = \delta(1) + \delta(1)$ et donc que $\delta(1) = 0$. De plus $\delta(ab) = \delta(a)b + a\delta(b) = 0.b + a.0 = 0$, ainsi $ab \in C_A$.

Si A est un corps et $a \in C_A \setminus \{0\}$, alors $0 = \delta(1) = \delta(aa^{-1}) = 0 + a\delta(a^{-1})$ d'où $\delta(a^{-1}) = 0$ et donc $a^{-1} \in C_A$. □

Remarquons que nous avons les propriétés habituelles de la dérivée :

Lemme V.7. *Pour tout $a \in A$, pour tout naturel non nul n, nous avons que*

$$\delta(a^n) = na^{n-1}\delta(a).$$

Démonstration. Raisonnons par récurrence sur n.
Si $n = 1$, alors $\delta(a^1) = \delta(a) = 1a^0\delta(a) = \delta(a)$, ainsi le cas de base est vérifié.
Pour $n+1$, nous avons :

$$\begin{aligned}\delta(a^{n+1}) &= \delta(a^n a)\\ &= \delta(a^n)a + a^n\delta(a)\\ &= na^{n-1}\delta(a)a + a^n\delta(a) \text{ (par hypothèse de récurrence)}\\ &= (n+1)a^n\delta(a).\end{aligned}$$

□

Proposition V.8. *Il existe une unique extension de δ au corps des fractions de A. Elle est donnée pour $a,b \in A$ avec $b \neq 0$ par :*

$$\delta\left(\frac{a}{b}\right) = \frac{\delta(a)b - a\delta(b)}{b^2}.$$

Démonstration. Soient $\frac{a}{b}$ et $\frac{c}{d} \in \mathrm{Frac}(A)$. Nous avons que

$$\begin{aligned}
\delta\left(\frac{a}{b}+\frac{c}{d}\right) &= \delta\left(\frac{ad+bc}{bd}\right) \\
&= \frac{\delta(ad+bc)bd-(ad+bc)\delta(bd)}{b^2d^2} \\
&= \frac{\delta(a)bd^2+\delta(d)abd+\delta(b)bcd+\delta(c)b^2d}{b^2d^2} - \\
&\quad \frac{\delta(b)ad^2+\delta(d)abd+\delta(b)bcd+\delta(d)cb^2}{b^2d^2} \\
&= \frac{\delta(a)bd^2-\delta(b)ad^2}{b^2d^2}+\frac{\delta(c)a^2d-\delta(d)b^2c}{b^2d^2} \\
&= \delta\left(\frac{a}{b}\right)+\delta\left(\frac{c}{d}\right).
\end{aligned}$$

De manière similaire, en développant bien nous pouvons montrer que

$$\delta\left(\frac{a}{b}\cdot\frac{c}{d}\right) = \delta\left(\frac{a}{b}\right)\cdot\frac{c}{d}+\frac{a}{b}\cdot\delta\left(\frac{c}{d}\right).$$

Il faut faire attention aussi à ce que δ soit bien définie sur le corps des fractions, c'est-à-dire que pour tous $\frac{a}{b} \in \mathrm{Frac}(A)$ et c inversible de A, nous avons

$$\delta\left(\frac{a}{b}\right) = \delta\left(\frac{ac}{bc}\right).$$

Ainsi, nous avons que δ définit bien une dérivée sur $\mathrm{Frac}(A)$.

Montrons maintenant l'unicité de cette extension. Supposons qu'il existe une autre extension de la dérivée de A sur $\mathrm{Frac}(A)$, disons δ_1. Alors $D = \delta_1 - \delta$ est une dérivée sur $\mathrm{Frac}(A)$, avec $D = 0$ sur A. Or pour tous $a, b \in A$ avec $b \neq 0$, nous avons que $D(b \cdot \frac{a}{b}) = D(a) = 0$ car $a \in A$. En outre $D(b \cdot \frac{a}{b}) = D(a)\frac{a}{b} + D(\frac{a}{b})b = D(\frac{a}{b})b = 0$. Comme b est non nul, alors $D(\frac{a}{b}) = 0$ d'où D est nulle sur $\mathrm{Frac}(A)$ et donc $\delta_1 = \delta$. □

Exemple V.9. Considérons $\mathbb{C}[X]$ muni de la dérivée usuelle sur les polynômes. Nous pouvons munir le corps des fractions de $\mathbb{C}[X]$, noté $\mathbb{C}(t)$, d'une dérivée qui est l'extension de la dérivée usuelle sur $\mathbb{C}[X]$.

Exemple V.10. Soit (K, δ) un corps différentiel. Nous pouvons étendre δ sur son anneau des polynômes $K[X]$ en définissant, pour $b \in K$,

$$\begin{aligned}
D : a &\mapsto \delta(a) \text{ pour tout } a \in K \\
X &\mapsto b
\end{aligned}$$

et en étendant cette fonction par la règle du produit. Ainsi, par exemple nous avons que

$$D(aX^n) = \delta(a)X^n + abnX^{n-1}.$$

Cette dérivée s'étend de façon unique à $K(X)$ par la proposition précédente.

Nous allons maintenant aborder un exemple fondamental pour la suite de ce mémoire : l'anneau des polynômes différentiels sur A.

Exemple V.11. Considérons $A[X_0, X_1, \dots]$ l'anneau des polynômes sur A à une infinité de variables. Nous allons construire l'anneau des polynômes différentiels à une variable sur A. Définissons D une extension de δ sur $A[X_0, X_1, \dots]$ par

$$D : a \mapsto \delta(a) \text{ pour tout } a \in A$$
$$X_n \mapsto X_{n+1}$$

que nous étendons sur tout $A[X_0, X_1, \dots]$ par la règle le Leibniz. Nous noterons à partir de maintenant $X^{(n)}$ pour désigner la variable $n-$ème variable X_n et $X^{(0)} = X$. Ainsi, nous avons que $D(X^{(n)}) = X^{(n+1)}$. Nous notons $A\{X\}$ l'ensemble des polynômes différentiels à une variable à coefficients dans A.

Définition V.12. Soit $f \in A\{X\} \setminus A$ un polynôme différentiel. On définit l'**ordre de** f comme le plus grand naturel n tel que $X^{(n)}$ apparaît dans f. Si f est constant, l'ordre de f est par convention -1.

Si f est d'ordre n, son **degré** est le degré du polynôme en $X^{(n)}$.

Si $f, g \in A\{X\}$, nous dirons que g est **plus simple** que f si $\text{ord}(g) < \text{ord}(f)$ ou bien si $\text{ord}(g) = \text{ord}(f)$, alors $\deg(g) < \deg(f)$. Nous écrirons alors $g \ll f$.

Remarque V.13. Si K est un corps de caractéristique nulle, en particulier il est infini. Ainsi $K\{X\}$ est de même cardinalité que K. De plus, puisque K est factoriel, nous avons que $K[X_0, \dots]$ est factoriel et donc $K\{X\}$ aussi. Par conséquent, tout polynôme différentiel sur K se décompose de façon unique en irréductibles.

Définition V.14. Soit I un idéal de A. On dit que I est un idéal **différentiel** si $\delta(I) \subseteq I$.

Exemple V.15.

- Soient $a \in A$ et l'ensemble $I = \{f \in A\{X\} : f(a) = 0\}$. L'idéal I est un idéal différentiel. En effet, soit $f \in I$. Comme $f(a) = 0$, en dérivant des deux côtés, nous obtenons que $\delta(f(a)) = \delta(0) = 0$. Or $\delta(f(a)) = \delta(f)(a) = 0$ par définition de δ, d'où $\delta(f) \in I$ et donc I est différentiel.
- L'anneau A est un idéal différentiel. Si $(I_j)_{j \in J}$ est une famille d'idéaux différentiels de A, alors l'intersection des I_j est aussi un idéal différentiel de A. Ainsi, pour $a \in A$, l'intersection de tous les idéaux différentiels de A contenant a est le plus petit idéal différentiel de A contenant a.

Définition V.16. Pour $a \in A$, on note $\langle a \rangle$ le plus petit idéal différentiel de A contenant a. On dit alors que $\langle a \rangle$ est l'**idéal différentiel engendré par** a.

Nous avons une description simple de l'idéal différentiel engendré par $a \in A$.

Lemme V.17. *Pour $a \in A$, l'idéal différentiel $\langle a \rangle$ est l'idéal classique engendré par toutes les dérivées de a, c'est-à-dire :*

$$\langle a \rangle = (a, \delta(a), \delta^2(a), \dots).$$

Démonstration. C'est bien un idéal différentiel. De plus, c'est le plus petit car $\langle a \rangle$ contient forcément toutes les dérivées de a et donc $\langle a \rangle \supseteq (a, \delta(a), \delta^2(a), \dots)$. □

Remarque V.18. Contrairement aux idéaux classiques, si $f \in A\{X\}$ est irréductible, alors $\langle f \rangle$ n'est pas forcément premier. Prenons par exemple $f(X) = (X'')^2 - 2X'$ qui est irréductible dans $A\{X\}$. Alors

$$\delta(f(X)) = 2X''X^{(3)} - 2X'' = 2X''(X^{(3)} - 1) \in \langle f \rangle.$$

Or, nous pouvons voir en dérivant que ni $2X''$ ni $X^{(3)} - 1$ ne sont dans $\langle f \rangle$.

Proposition V.19. *Soit I un idéal différentiel de A. Alors A/I muni de la dérivée définie par $\delta(a+I) = \delta(a) + I$, pour tout $a \in A$, est un anneau différentiel.*

Démonstration. Puisque δ est une dérivée sur A, nous avons que $\delta(a+I) = \delta(a) + \delta(I)$. De plus, comme I est différentiel, nous avons que $\delta(a) + \delta(I) = \delta(a) + I$ dans l'anneau quotient A/I. Ainsi δ est bien définie sur A/I. Quant aux propriétés de la dérivée, elles découlent immédiatement des définitions de δ et de A/I. □

Travaillons dans $K\{X\}$ où K est un corps différentiel. Nous pouvons définir sur $K\{X\}$ une dérivée qui étend celle de K en posant $\delta(X) = X'$. Nous allons montrer que tout idéal différentiel premier de $K\{X\}$ est de la forme $I(f)$ pour un $f \in K\{X\}$ irréductible. Cela a du sens car $K\{X\}$ est factoriel. Notons que la cardinalité de $K\{X\}$ est donné par la cardinalité de K si K est infini.

Un exemple d'extension de corps différentiel est le suivant :

Exemple V.20. Considérons $K = \mathbb{C}(t)$ muni de la dérivée usuelle sur les polynômes. Alors $\sqrt{t}$ est algébrique sur $\mathbb{C}(t)$ car $P(X) = X^2 - t$ est un polynôme dans $\mathbb{C}(t)[X]$ qui s'annule en $\sqrt{t}$. De plus, ce polynôme est irréductible, c'est donc le polynôme minimal de $\sqrt{t}$ sur $\mathbb{C}(t)$. C'est une extension algébrique de degré 2.

Notons que s'il existe une dérivée $\tilde{\delta}$ qui étend celle de $\mathbb{C}(t)$ sur $\mathbb{C}(\sqrt{t})$, alors elle doit satisfaire, comme $P(\sqrt{t}) = 0$,

$$\tilde{\delta}((\sqrt{t})^2 - t) = 2\sqrt{t}\tilde{\delta}(\sqrt{t}) - 1 = 0,$$

c'est-à-dire que $\delta(\sqrt{t}) = \frac{1}{2\sqrt{t}}$.

V.2 Séparant d'un polynôme différentiel

Prenons (K,δ) un corps différentiel. De manière analogue à la théorie des corps, nous voulons construire un corps différentiel qui admet une solution pour n'importe quelle équation différentielle. Pour construire un tel corps qui étend K et sa dérivée, nous pouvons nous inspirer de ce que nous connaissons déjà : dans le cas classique des corps, la construction d'un tel corps se fait en prenant le corps des fractions d'un anneau quotient bien choisi. Cet anneau s'avère être intègre pour $f \in K[X]$ irréductible car l'idéal est premier. Nous avons vu plus tôt que dans le cas différentiel, l'idéal différentiel $\langle f \rangle$ d'un polynôme f irréductible n'est pas forcément premier. Une première étape va être de palier à ce problème.

Nous allons introduire une forme alternative d'idéal différentiel "engendré" par un polynôme $f \in K\{X\}$.

Définition V.21. Soit $f \in K\{X\}$ d'ordre n. On définit le **séparant** de f par

$$s_f(X) = \frac{\partial f}{\partial X^{(n)}}(X),$$

où $\frac{\partial f}{\partial X^{(n)}}$ désigne la dérivée partielle usuelle de f en la variable $X^{(n)}$.

Exemple V.22. Si $f(X) = (X'')^2 - 2X'$, alors $s_f(X) = 2X''$. Plus généralement, si f est de la forme

$$f(X) = \sum_{i=0}^{m} g_i(X, X', \ldots, X^{(n-1)})(X^{(n)})^i,$$

alors

$$s_f(X) = \sum_{i=0}^{m-1} (i+1) g_i(X, X', \ldots, X^{(n-1)})(X^{(n)})^i.$$

En particulier $s_f(X) \ll f(X)$. Nous laisserons tomber l'indice f de s_f lorsque le contexte ne prêtera pas à ambiguïté.

Définition V.23. Soit $f(X) \in K\{X\}$. On définit $I(f)$ l'**idéal différentiel engendré par** f par :

$$I(f) = \{g \in K\{X\} : \exists k \in \mathbb{N},\ s_f^k g \in \langle f \rangle\}.$$

Lemme V.24. *Soit $f \in K\{X\}$. L'ensemble $I(f)$ est un idéal différentiel.*

Démonstration. Montrons que c'est un idéal. Soit $g \in I(f)$ et $h \in K\{X\}$. Alors $gh \in I(f)$ si et seulement si il existe un naturel r tel que $s^r gh \in \langle f \rangle$. Mais $g \in I(f)$, d'où $s^k g \in \langle f \rangle$, comme c'est un idéal, nous avons $s^k gh \in \langle f \rangle$, i.e. $gh \in I(f)$. En

outre, si $h \in I(f)$, alors il existe un naturel m tel que $s^m h \in \langle f \rangle$, d'où $s^{\max\{k,m\}}(g+h) \in \langle f \rangle$, et donc $g+h \in I(f)$.

Montrons que $I(f)$ est un idéal différentiel, c'est-à-dire que si $g \in I(f)$, alors $\delta(g) \in I(f)$. Nous avons que $s^k g \in \langle f \rangle$. Comme $\langle f \rangle$ est un idéal, nous avons aussi que $s^{k+1} g \in \langle f \rangle$, de plus il est différentiel, et donc $\delta(s^{k+1} g) \in \langle f \rangle$. Mais

$$\delta(s^{k+1} g) = (k+1) s^k g \delta(s) + s^{k+1} \delta(g).$$

Nous en déduisons que $s^{k+1}\delta(g) \in \langle f \rangle$, c'est-à-dire que $\delta(g) \in I(f)$. □

Nous allons lister différentes propriétés des idéaux de la forme $I(f)$. Nous décidons de ne pas en faire la démonstration car celle-ci s'avère très calculatoire. Pour une preuve du prochain résultat, nous pourrons consulter [5].

Proposition V.25. *Soit $f \in K\{X\}$ un polynôme différentiel irréductible d'ordre n. Soit $g \in K\{X\}$.*

(a) $I(f)$ est un idéal différentiel premier.

(b) Si $g \in I(f) \setminus \{0\}$, alors soit $ord(g) > n$, soit $ord(g) = n$ et $f | g$.

(c) Tout idéal différentiel premier est de la forme $I(f)$ pour un certain f irréductible.

Au sens de (b), si $I = I(f)$, nous disons que f ***est un polynôme minimal de*** *I.*

Ces idéaux sont un outil fondamental dans l'étude des corps différentiellement clos.

Définition V.26. Soit I un idéal différentiel premier de $K\{X\}$. On définit le **rang différentiel de** I, noté $\mathrm{RD}(I)$, comme l'ordre d'un polynôme minimal de I. Par convention, si $I = \{0\}$, alors $\mathrm{RD}(I) = \omega$.

Nous pouvons voir qu'un polynôme minimal est d'ordre minimal dans l'idéal par la propriété (b) et que $\mathrm{RD}(I) \leqslant \mathrm{ord}(g)$ pour tout $g \in I$.

Pour un élément α dans une extension de K, nous noterons $I(\alpha/K) = \{f \in K\{X\} : f(\alpha) = 0\}$. C'est un idéal différentiel premier, la condition se vérifie dans l'extension de K car α n'est pas forcément dans K. Nous définissons de manière analogue au point générique d'une variété :

Définition V.27. Soit $L \supseteq K$ un corps différentiel. On dit que $\alpha \in L$ est une **solution générique** de $f \in K\{X\}$ si $f(\alpha) = 0$ et pour tout $f \gg g \in K\{X\}$, l'élément α vérifie $g(\alpha) \neq 0$.

Si f est irréductible, cela revient à dire que $I_\delta(\alpha/k) = I(f)$.

Le rang différentiel du polynôme $I(\alpha/K)$ pour un élément α dans une extension de K donne en fait le degré de transcendance du corps différentiel qu'il engendre sur K. Nous ne prouverons pas le résultat car la preuve n'est pas très intéressante.

Lemme V.28 ([5], Lemme 1.9)**.** *Soit L un corps différentiel qui étend K. Soit $\alpha \in L$. Notons $tr[M:N]$ le degré de transcendance de M sur N. Alors*

$$RD(I(\alpha/K)) = tr[K\langle\alpha\rangle : K].$$

Corollaire V.29. *Soit $f \in K\{X\}$ un polynôme irréductible d'ordre > 0. Soit α dans une extension de K. Si α est algébrique sur K, alors α n'est pas une solution générique de f.*

Démonstration. Si α est algébrique sur K , alors l'idéal $I(\alpha/K)$ est de rang différentiel 0 car il existe un polynôme d'ordre 0 qui annule α. Supposons que α est solution générique de f. Alors comme f est irréductible, nous avons que $I(\alpha/K) = I(f)$, qui est de rang différentiel > 0, une contradiction. □

En particulier, pour que α soit une solution générique d'un polynôme différentiel d'ordre > 0, il doit être transcendant sur K.

V.3 Topologie de Kolchin

Nous voilà de retour dans une topologie de type Zariski. Cette fois-ci, nous ne regardons plus seulement les polynômes *algébriques*, ni forcément homogène, mais plutôt ceux différentiels.

Définition V.30. Soit S un sous-ensemble de $K\{X_1,\dots,X_n\}$. On définit $V_\delta(S)$ l'**ensemble différentiel affine défini par** S le sous-ensemble de K^n donné par :

$$V_\delta(S) = \{x \in K^n : \forall P \in S, P(x) = 0\}.$$

Contrairement aux autres topologies de Zariski vues précédemment, il existe des chaînes croissantes infinies d'idéaux différentiels. Par exemple,

$$\langle X^2\rangle \subseteq \langle X^2, \delta(X)^2\rangle \subseteq \dots \subseteq \langle X^2, \delta(X)^2, \dots, \delta^m(X)^2\rangle \subseteq \dots$$

Mais nous pouvons nous en sortir pour les idéaux différentiels radiciels. Nous admettrons le résultat suivant qui fait écho au théorème de la base de Hilbert I.6.

Théorème V.31 (Théorème de la base de Ritt-Raudenbush, [5] Théorème II.1.16)**.** *Soit $R \supseteq \mathbb{Q}$ un anneau différentiel dans lequel tout idéal différentiel radiciel est finiment engendré. Alors, tout idéal différentiel radiciel de $R\{X\}$ est finiment engendré.*

Corollaire V.32. *Il n'existe pas de chaîne croissante infinie d'idéaux différentiels radiciels dans $K\{X_1,\dots,X_n\}$. De plus, pour tout idéal différentiel radiciel I, il existe des polynômes différentiels $f_1,\dots,f_m$ tel que $I = \sqrt{\langle f_1,\dots,f_m\rangle}$.*

Notons que la chaîne d'idéaux vu plus tôt n'est pas une chaîne d'idéaux différentiels radiciels.

Théorème V.33. *Les ensembles différentiels affines forment une base d'une topologie sur K^n, appelée* ***topologie de Kolchin****.*

Démonstration. Même preuve que pour la topologie de Zariski. □

La topologie de Kolchin est, comme les autres topologies de Zariski que nous avons vu jusqu'à maintenant, une topologie noethérienne. Ainsi les notions d'irréductibilité demeurent. Nous parlerons de variété différentielle pour un ensemble différentiel affine.

Nous démontrerons à la section suivante une version analogue du Nullstellensatz dans le cadre de l'algèbre différentiel.

V.4 Théorie des corps différentiellement clos

Nous tirons les différents résultats de cette section du chapitre 2, paragraphe 2 de [5].

Soit (K,∂) un corps différentiel de caractéristique nulle. On définit un un corps différentiellement clos comme suit.

Définition V.34. On dit que K est **différentiellement clos** s'il vérifie pour tous polynômes différentiels $f,g \in K\{X\}$ tels que $\operatorname{ord}(f) > \operatorname{ord}(g)$, l'existence d'un $x \in K$ tel que $f(x) = 0$ et $g(x) \neq 0$.

Nous noterons DCF_0 la théorie des corps différentiellement clos dans le langage $\mathcal{L} = \{0,1,+,\times,\delta\}$ des anneaux différentiels. Cette axiomatisation vient de Blum qui a montré l'équivalence entre DCF_0 construit en tant que modèle compagnon et DCF_0 comme nous l'avons défini. Nous verrons une autre axiomatisation, plutôt géométrique, de DCF_0 dans le chapitre suivant.

Remarque V.35. Une dérivée sur un corps différentiellement clos est forcément non triviale. En effet, considérons $f(X) = X''$ et $g(X) = X'$, alors il existe une solution y de f qui n'annule pas g, c'est-à-dire que $y' \neq 0$.

De façon similaire, nous montrons qu'un corps différentiellement clos est forcément algébriquement clos.

Lemme V.36. *Soit $a \in K$ un élément algébrique sur son corps des constantes C. Alors $a \in C$. Si K est algébriquement clos alors C est algébriquement clos.*

Démonstration. Soit $a \in K$ un élément algébrique de K sur C. Soit $P \in K[X]$ le polynôme minimal de a sur C, de la forme $P(X) = \sum_{i=0}^{n} a_i X^i$. Comme $P(a) = 0$, en dérivant des deux côtés nous obtenons que

$$\delta(P(a)) = \sum_{i=1}^{n} i a_i a^{i-1} \delta(a) = \delta(a) \sum_{i=1}^{n} i a_i a^{i-1} = 0,$$

car les coefficients sont de dérivée nulle. Par minimalité de $P(X)$, nous devons avoir que le polynôme défini par $\sum_{i=1}^{n} i a_i X^{i-1}$ ne s'annule par en a et donc pas intégrité de K, nous en déduisons que $\delta(a) = 0$, c'est-à-dire que $a \in C$.

La deuxième assertion est immédiate car K admet tous les éléments algébriques sur K et donc en particulier sur C. □

Corollaire V.37. *Le corps des constantes d'un corps différentiellement clos est algébriquement clos.*

Proposition V.38. *Nous pouvons plonger (K, δ) dans un modèle de DFC_0.*

Démonstration. Soient $f, g \in K\{X\}$ tels que $\mathrm{ord}(g) < \mathrm{ord}(f)$.

Nous allons construire une extension de K qui admet un élément x tel que $f(x) = 0$ et $g(x) \neq 0$. Comme $K\{X\}$ est factoriel, nous pouvons prendre $\tilde{f}$ un facteur irréductible de f d'ordre $\mathrm{ord}(f)$. Considérons alors l'idéal $I = I(\tilde{f})$. Par la proposition V.25, c'est un idéal premier et $g \notin I$ car $\mathrm{ord}(g) < \mathrm{ord}(f)$. Considérons le quotient intègre $K\{X\}/I$. Nous définissons K_1 le corps des fractions de $K\{X\}/I$.

Notons que les propositions V.8 et V.19 nous assurent que la dérivée s'étend de façon unique sur K_1.

Or dans K_1, nous avons que

$$\begin{aligned} f \in I &\Leftrightarrow f(X) + I = 0 \\ &\Leftrightarrow f(X + I) = 0, \end{aligned}$$

c'est-à-dire que l'image de X dans K_1 est racine de f. Idem, nous montrons que l'image de X n'est pas une racine de g.

Pour construire notre corps différentiellement clos, commençons par numéroter les paires pathogènes. Soit l'ensemble des paires :

$$\{(f,g) : f,g \in K\{X\},\ \text{ord}\, f > \text{ord}\, g \text{ et} \\ \text{il n'existe pas de } x \in K \text{ tel que } f(x) = 0 \wedge g(x) \neq 0\}.$$

Le cardinal de cet ensemble est borné par celui de K. Nous construisons $\hat{K}_1$, la réunion de tous les corps différentiels construits par la procédure réalisée plus tôt pour tous les points de cet ensemble. Malheureusement $\hat{K}_1$ ne sera pas forcément différentiellement clos car nous pourrions ajouter des paires à chaque itération.

En considérant le nouvel ensemble des paires pathogènes de $\hat{K}_1$, nous construisons $\hat{K}_2$. En itérant cette construction, nous obtenons une chaîne

$$K \subseteq \hat{K}_1 \subseteq \ldots \subseteq \hat{K}_n \subseteq \ldots$$

de sous-corps différentiels. Nous définissons $\hat{K} = \cup_{i=1}^{\infty} \hat{K}_i$. C'est un corps différentiellement clos car toute paire (f,g) se retrouve dans un élément de la chaîne, dont le corps suivant admet un bon remède x tel que $f(x) = 0$ et $g(x) \neq 0$. De plus, cet ensemble est de cardinal K car nous n'ajoutons à chaque étape qu'au plus $|K|$ éléments. □

En particulier, nous pouvons le plonger dans un corps différentiellement clos de même cardinal.

La théorie DCF_0 est très similaire à ACF_0. Elles partagent toutes les deux des notions générales de théorie des modèles. Nous montrerons par exemple que DFC_0 admet l'élimination des quantificateurs, qu'elle est complète mais aussi ω-stable. Nous utiliserons des résultats classiques de théorie des modèles sur les théories ω-stables qui nous permettrons de parler d'une clôture différentielle. Cet objet est analogue à la clôture algébrique dans ACF_0.

En fait, le cheminement que nous allons réaliser pour démontrer que DCF_0 est ω-stable est similaire à celui de ACF_0, modulo des propriétés un peu moins belles sur les idéaux différentiels... Heureusement nous avons nos idéaux $I(f)$.

Rappelons un critère sur l'élimination des quantificateurs.

Théorème V.39 ([2], Corollaire 3.1.6)**.** *Soient $\mathcal{L}$ un langage avec au moins un symbole de constante et T une $\mathcal{L}$-théorie. Supposons que pour toute $\mathcal{L}$-formule sans quantificateur $\varphi(\bar{v},w)$, si $\mathcal{M},\mathcal{N} \models T$ et $\mathcal{A}$ est une sous-structure commune de $\mathcal{M}$ et $\mathcal{N}$, $\bar{a} \in A$ et qu'il existe $b \in M$ tel que $\mathcal{M} \models \varphi(b,\bar{a})$, alors il existe un existe $c \in N$ tel que $\mathcal{N} \models \varphi(c,\bar{a})$. Alors T a l'élimination des quantificateurs.*

Alors nous prouvons que :

Théorème V.40. *DCF_0 admet l'élimination des quantificateurs.*

Démonstration. Il suffit donc de montrer pour tous $K, L \models DCF_0$, pour toute structure k tel que $k \subseteq K$, $k \subseteq L$, $\overline{a} \in k$, $b \in K$, et toute $\mathcal{L}$-formule sans quantificateur $\varphi(v, \overline{w})$, si $K \models \varphi(b, \overline{a})$, alors $L \models \exists v, \varphi(v, \overline{a})$.

Quitte à se plonger dans une extension élémentaire, nous pouvons supposer que K et L sont ω-saturés. En outre, comme $\overline{a} \in k$, nous pouvons supposer que k est le corps différentiel engendré par $\overline{a}$ (les termes sont définissables).

Alors, nous affirmons que nous pouvons trouver un $\beta \in L$ tel que $k\langle b \rangle \cong k\langle \beta \rangle$. Si nous montrons cela nous aurons que $L \models \varphi(\beta, \overline{a})$ et donc notre résultat.

Supposons que b est différentiellement algébrique sur k (i.e. il annule un polynôme différentiel sur k). Soit f un polynôme minimal de l'idéal premier $I(b/k) = \{f \in k\{X\} : f(b) = 0\}$. Posons $N = \operatorname{ord}(f)$. Considérons l'ensemble de formules :

$$\Gamma(v) = \{f(v) = 0\} \cup \{h(v) \neq 0 : h(X) \in k\{X\} \text{ où } h \text{ est d'ordre} < N\}.$$

Pour tous $h_1, \ldots, h_n \in k\{X\}$ d'ordre $< N$, comme L est différentiellement clos, nous pouvons trouver un $\beta_0 \in L$ qui annule f mais pas $h_1(X) \ldots h_n(X)$, c'est-à-dire chacun des h_i. Par compacité, le type $\Gamma(v)$ est réalisé dans une extension de L. Par ω-saturation, il existe un $\beta \in L$ qui réalise $\Gamma(v)$. Nous étendons σ en posant $\sigma^*(b) = \beta$, d'où $k\langle b \rangle \cong k\langle \beta \rangle$.

Sinon b est différentiellement transcendant sur k, alors par ω-saturation (c'est le type transcendant), il existe un $\beta \in L$ tel que β est différentiellement transcendant sur k. Alors σ^* envoie $b \mapsto \beta$. □

Remarque V.41. Puisque DCF_0 admet l'élimination des quantificateurs, toute $\mathcal{L}$-formule est équivalente à une formule de la forme

$$\varphi(\overline{x}) \equiv \bigvee_{i \in I} \Big(\bigwedge_{j \in J_i} p_{i,j}(\overline{x}) = 0 \wedge q_i(\overline{x}) \neq 0 \Big),$$

où I est un ensemble fini et les $p_{i,j}$ et q_i sont des polynômes différentiels à coefficients dans $\mathbb{Q}$.

Si nous ajoutons des paramètres d'un ensemble A à la formule, alors elle sera équivalente à une formule de la forme ci-dessus mais avec des polynômes différentiels à coefficients dans le corps différentiel engendré par A dans $\mathbb{Q}$.

Corollaire V.42. *DCF_0 est modèle complète et complète.*

Démonstration. Soient $\mathcal{M}$ et $\mathcal{N}$ deux modèles de DCF_0.

Montrons que $\mathcal{M} \equiv \mathcal{N}$. Soit φ un $\mathcal{L}$-énoncé. Puisque DCF_0 a l'élimination des quantificateurs, il existe un énoncé ψ équivalent sans quantificateur. En outre, le

corps $\mathbb{Q}$ muni de la dérivée triviale peut se plonger dans tout corps différentiel de caractéristique 0, nous obtenons que :

$$\begin{aligned}\mathcal{M} \models \varphi &\iff \mathcal{M} \models \psi \\ &\iff \mathbb{Q} \models \psi \\ &\iff \mathcal{N} \models \psi \\ &\iff \mathcal{N} \models \varphi.\end{aligned}$$

Donc DCF_0 est complète.

Supposons que $\mathcal{M} \subseteq \mathcal{N}$. Soient $\varphi(\overline{x})$ une $\mathcal{L}$-formule et $\overline{a} \in M$ tels que $\mathcal{M} \models \varphi(\overline{a})$. Comme DFC_0 a l'élimination des quantificateurs, φ est équivalente à une formule sans quantificateur ψ, et donc :

$$\begin{aligned}\mathcal{M} \models \varphi(\overline{a}) &\iff \mathcal{M} \models \psi(\overline{a}) \\ &\iff \mathcal{N} \models \psi(\overline{a}) \\ &\iff \mathcal{N} \models \varphi(\overline{a}).\end{aligned}$$

Par conséquent $\mathcal{M} \preccurlyeq \mathcal{N}$ et donc DCF_0 est modèle complète. □

Soit K un modèle de DCF_0. Comme pour le cas algébrique, nous allons définir une bijection entre les types de DCF_0 et les idéaux différentiels premiers de $K\{X\}$.

Lemme V.43. *Soit $p \in S_1(K)$ un 1-type sur K. L'ensemble $I_p = \{f \in K\{X\} : \text{"}f(v) = 0\text{"} \in p\}$ est un idéal différentiel premier.*

Démonstration. Que l'idéal soit premier est clair. Si $f \in I_p$, alors $f(v) = 0$ d'où $(f(v))' = 0' = 0$, c'est-à-dire par définition de la dérivée que $f'(v) = 0$. □

Proposition V.44. *L'application $p \mapsto I_p$ est une bijection entre $S_1(K)$ et les idéaux différentiels premiers de $K\{X\}$.*

Démonstration. Par le lemme précédent, cette application est bien définie.

Montrons l'injectivité. Soient p et q deux types distincts de $S_1(K)$, montrons que $I_p \neq I_q$. Comme ces deux types sont distincts, il existe une $\mathcal{L}_K$-formule que nous pouvons supposer sans perdre de généralité, grâce à l'élimination des quantificateurs, sans quantificateur $\varphi(x,\overline{a}) \in p \setminus q$ avec $\overline{a} \in K$. Elle est de la forme

$$\varphi(x,\overline{a}) \equiv \bigvee_{i\in I} \Big(\bigwedge_{j\in J_i} f_{i,j}(x) = 0 \wedge g_i(x) \neq 0 \Big),$$

où I est fini et les $f_{i,j}$ et $g_i \in K\{X\}$. Mais $\varphi(x,\overline{a}) \in p$ si et seulement s'il existe un $i_0 \in I$ tel que les $f_{i_0,j} \in I_p$ et $g_{i_0} \notin I_p$. Comme $\varphi(x,\overline{a}) \notin q$, nous avons que $f_{i_0,j} \notin I_q$ ou $g_{i_0} \in I_q$, d'où $I_p \neq I_q$.

Reste à montrer la surjectivité. Soit I un idéal premier différentiel. Le quotient $K\{X\}/I$ est intègre. Prenons L son corps des fractions et grâce à V.38, plongeons-le dans un corps différentiellement clos M. Soit $p = \mathrm{tp}(\overline{X}/K)$ le type de l'image de X dans L. Alors $f(X) \in p$ si et seulement si $f(X+I) = 0$, ou encore en utilisant les propriétés du quotient, que $f(X)+I = 0$, i.e. $f(X) \in I$. Donc $I_p = I$. □

Nous arrivons finalement au résultat fondamental :

Corollaire V.45. *DCF_0 est ω-stable.*

Démonstration. Soient $\mathcal{M}$ un modèle de DCF_0 et $A \subseteq M$ un ensemble dénombrable de paramètres. Soit K le corps différentiel engendré par A, c'est un corps dénombrable car $K = \mathbb{Q}\langle A\rangle$ et à chaque étape de la construction, nous n'ajoutons qu'un nombre dénombrable de termes.

Nous allons montrer que $|S_1(A)| = |S_1(K)| = \aleph_0$. La première égalité est claire car K est l'ensemble des termes du langage $\mathcal{L}_A$. De plus, par la proposition précédente, nous avons que $|S_1(K)|$ est égal au nombre d'idéaux premiers de $K\{X\}$. Or $|K\{X\}| = |K| = \aleph_0$, d'où

$$|S_1(K)| \leqslant \aleph_0.$$

□

Théorème V.46 (Nullstellensatz différentiel de Seidenberg)**.** *Soit K un corps différentiellement clos. L'application $I \mapsto V_\delta(I)$ entre les idéaux différentiels radiciels premier de $K\{\overline{X}\}$ et les fermés de Kolchin de K^n est bijective.*

Démonstration. Si $Y \subseteq K^n$, nous pouvons facilement vérifier que

$$I_\delta(Y) := \{f(\overline{X}) \in K\{\overline{X}\} : \forall \overline{y} \in Y, f(\overline{y}) = 0\}$$

est un idéal différentiel radiciel. Alors si V est un fermé de Kolchin, nous avons que $V_\delta(I_\delta(V)) = V$ (comme pour Zariski).

Soient I et J deux idéaux radiciels distincts de $K\{\overline{X}\}$. Prenons $g \in J \setminus I$. Par le théorème de la base de Ritt-Raudenbush qui nous dit que la topologie de Kolchin est noethérienne, l'idéal I est l'intersection d'idéaux différentiels premiers. Il y a donc un idéal différentiel premier $P \supseteq I$ tel que $g \notin P$. Il nous suffit alors de montrer qu'il existe $x \in V_\delta(P)$ tel que $g(x) \neq 0$. Supposons que $P = \sqrt{\langle f_1, \ldots, f_m\rangle}$. Soit L un corps différentiellement clos qui contient $K\{\overline{X}\}/P$ et soit $x = (X_1 + P, \ldots, X_n + P)$. Alors comme pour les arguments de ce type, nous obtenons que $f(x) = 0$ pour tout $f \in P$ et $g(x) \neq 0$.

En particulier, le corps L vérifie que

$$L \models \exists v_1, \ldots, v_n, f_1(v_1, \ldots, v_n) = 0 = \ldots = f_m(v_1, \ldots, v_n) \wedge g(v_1, \ldots, v_n) \neq 0.$$

Par modèle complétude, le corps K vérifie cet énoncé. Ainsi, il existe $x \in K^n$ tel que $x \in V_\delta(P) \setminus V_\delta(J)$, d'où $V_\delta(I) \neq V_\delta(J)$.

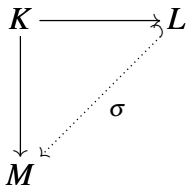
Pour la surjectivité, si $V = V_\delta(I)$, il suffit de prendre J le plus petit idéal radiciel différentiel de I. □

Remarque V.47. Le théorème de la base de Ritt-Raudenbush nous dit alors que tout fermé de Kolchin est définissable au premier ordre.

V.5 Modèles premiers et clôture différentielle

Soient (K, δ) un corps différentiel et C son corps des constantes.

Définition V.48. On dit que $L \supseteq K$ est une **clôture différentielle de** K si $L \models DCF_0$ et pour tout corps différentiellement clos M, si $M \supseteq K$, alors il existe un K-plongement $\sigma : L \hookrightarrow M$.



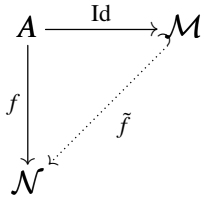
Nous allons montrer, modulo l'admission de résultats de théorie des modèles, l'existence de telles structures ainsi que leur unicité. Pour cela, nous allons utiliser des résultats classiques de théorie des modèles sur les théories ω-stables.

Rosenlicht a montré dans [11] que, contrairement au cas algébrique, la clôture différentielle n'est pas nécessairement minimale. Plus précisément, Rosenlicht, Kolchin et Shelah ont montré de façon indépendante que la clôture différentielle de $\mathbb{Q}$ se plongeait différentiellement dans un sous-corps propre d'elle-même. Nous donnerons dans le dernier chapitre de ce mémoire une preuve d'un résultat plus général (en admettant un certain théorème).

Pour utiliser nos outils de théorie des modèles, nous allons donner une généralisation des clôtures (qu'elles soient algébriques ou différentielles). Soit L un langage au plus dénombrable. Nous considérerons ici une T une théorie complète, ω-stable et admettant un modèle infini.

Définition V.49. Soient $\mathcal{M} \models T$ et $A \subseteq M$ une sous-structure. On dit que $\mathcal{M}$ est **premier sur** A si pour tout modèle $\mathcal{N}$ de T, toute application partielle élémentaire

$f : A \to \mathcal{N}$ s'étend en une extension élémentaire $\tilde{f} : \mathcal{M} \to \mathcal{N}$.



Exemple V.50. Pour la théorie des corps algébriquement clos, si A est un anneau intègre et K la clôture algébrique de son corps des fractions, alors K est premier sur A et donc n'importe quel plongement dans un corps algébriquement clos L s'étend en un plongement dans K. Ce plongement est élémentaire car ACF_0 est modèle complète. De la même façon, nous avons que :

Corollaire V.51. *Les modèles premiers de DCF_0 sur (K,δ) sont exactement les clôtures différentielles de K.*

Démonstration. Nous avons vu que DCF_0 est modèle-complète, par conséquent tout plongement est forcément un plongement élémentaire. □

Nous admettrons le résultat classique suivant qui nous assûre l'existence et l'unicité de *la* clôture différentielle de notre corps K.

Théorème V.52 ([2], Théorème 4.2.20 & Théorème 6.4.8)**.** *Soit T une théorie ω-stable et soient $\mathcal{M} \models T$ et $A \subseteq M$ une sous-structure. Il existe $\mathcal{M}_0 \prec \mathcal{M}$ un modèle premier de T sur A.*

De plus, s'il existe $\mathcal{M}_1$ un autre modèle de T premier sur A, alors il existe un isomorphisme entre $\mathcal{M}_0$ et $\mathcal{M}_1$ qui fixe A point par point.

Par conséquent, ce théorème utilisé à DCF_0 qui est ω-stable, comme les modèles premiers sur K sont exactement les clôtures différentielles de K :

Corollaire V.53. *Il existe une clôture différentielle de (K,δ). De plus, elle est unique à isomorphisme près.*

Lemme V.54. *Soit K un corps différentiel de cardinal κ. Alors sa clôture différentielle est aussi de cardinal κ*

Démonstration. La proposition V.38 nous dit que K se plonge dans un corps différentiellement clos de même cardinalité. Or la clôture différentielle de K s'y plonge aussi par définition et donc forcément doit être au plus de cardinal $|K|$. □

V.6 Théorie totalement transcendante

Le but de cette section sera de prouver la proposition 1 grâce aux outils de la théorie des modèles. Rappelons la proposition.

Proposition V.55. *Soit K un corps différentiel et L une clôture différentielle de K telle que $K \neq L$. Il existe un automorphisme différentiel de L/K non trivial.*

Tout le cheminement que nous allons faire fonctionnera également pour le même énoncé dans sa version algébrique. Nous tirons les prochains résultats de l'ouvrage [14], plus précisément de son cinquième chapitre.

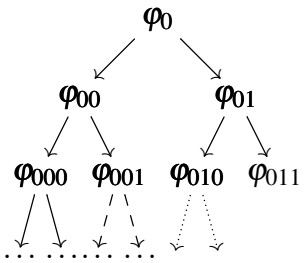
Pour arriver à nos fins, introduisons un nouveau type de théorie : les théories totalement transcendantes. Nous verrons un peu plus loin qu'en fait... nous les connaissons déjà. Nous fixons une théorie T complète dans un langage dénombrable qui admet des modèles infinis.

Introduisons d'abord la notion d'arbre binaire. Notons $2^{<\omega}$ l'ensemble des suites finies de $\mathbb{F}_2$

Définition V.56. Soit $(\varphi_s(\overline{x}))_{s\in 2^{<\omega}}$ une famille de $\mathcal{L}$-formules. On dit que cette famille de formules est un **arbre binaire de $\mathcal{L}$-formules** si elle satisfait pour tout $s \in 2^{<\omega}$:

- $T \vdash \forall \overline{x}, \big((\varphi_{s0}(\overline{x}) \vee \varphi s1(\overline{x})) \Rightarrow \varphi_s(\overline{x})\big)$;
- $T \vdash \forall \overline{x}, \neg\big(\varphi_{s0}(\overline{x}) \wedge \varphi s1(\overline{x})\big)$.

Sur un dessin, nous prenons comme convention d'ajouter 0 à la suite s de φ_s si nous allons à gauche, ou bien 1 dans le cas contraire.



Le premier axiome dit que si $\overline{x}$ réalise un nœud quelconque de l'arbre, alors il satisfait un chemin remontant jusqu'au sommet. Le deuxième axiome affirme que si $\overline{x}$ réalise un nœud quelconque de l'arbre, alors il ne satisfait aucun nœud de la même hauteur, et donc qu'il n'existe qu'un seul chemin vers le sommet.

Remarque V.57. Même si $\overline{x}$ réalise un nœud φ_s, il ne réalisera pas forcément φ_{s1} ou φ_{s2}, c'est-à-dire que $\varphi_s(\overline{x}) \nRightarrow \varphi_{s0}(\overline{x}) \vee \varphi_{s1}(\overline{x})$.

Définition V.58. On dit que T est **totalement transcendante** si T n'admet aucun modèle $\mathcal{M}$ avec un arbre binaire de $\mathcal{L}_M$-formules consistantes, c'est-à-dire un arbre binaire de $\mathcal{L}_M$-formules tel qu'en plus, pour tout $s \in 2^{<\omega}$,

$$T \vdash \exists \overline{x}, \varphi_s(\overline{x}).$$

Théorème V.59 ([14], Théorème 5.2.6)**.**

(i) Les théories ω-stables sont totalement transcendantes.

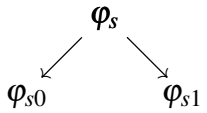
(ii) Les théories totalement transcendantes sont κ-stables pour tout $\kappa \geqslant |T|$.

Démonstration. Prouvons le premier point. Par contraposée, prenons une théorie T (avec un langage dénombrable) qui n'est pas totalement transcendante. Il existe donc un arbre binaire de $\mathcal{L}_M$ formules. Alors, le nombre de paramètres qui apparaissent dans cet arbre est au plus dénombrable car un arbre binaire n'a qu'un nombre dénombrable de nœuds, et chaque formule a un nombre fini de paramètres. De plus, chaque chemin de l'arbre correspond à un type différent car $T \vdash \forall \overline{x}, \neg\big(\varphi_{s0}(\overline{x}) \wedge \varphi s1(\overline{x})\big)$. Or, il existe $2^{\aleph_0}$ chemins dans l'arbre, c'est-à-dire $2^{\aleph_0}$ types distincts. Par conséquent, nous avons une infinité non dénombrable de types définis sur un même ensemble dénombrable de paramètres, d'où T n'est pas ω-stable.

Supposons maintenant que T est totalement transcendante. Supposons par l'absurde que T n'est pas κ-stable pour un certain $\kappa \geqslant |T|$, c'est-à-dire qu'il existe $> \kappa$ types (complets) sur un ensemble de paramètres A de cardinal κ. Nous allons distinguer deux types de formules, nous dirons qu'une $\mathcal{L}_A$-formule φ est :

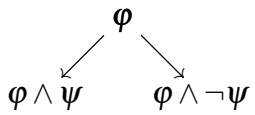
- **grande** si elle appartient à $> \kappa$ types ;
- **petite** sinon.

Nous allons construire un arbre binaire de $\mathcal{L}_A$-formules consistantes. Si nous montrons que nous pouvons *diviser* toute grande formule φ_s en deux grandes formules φ_{s0} et φ_{s1}, alors comme il en existe une, la formule $\varphi(x) \equiv x = x$ qui appartient à tous les types, nous pourrons construire un arbre binaire de L_A formule consistante.



Soit φ une grande formule. Comme $|A| = \kappa$, il existe κ $\mathcal{L}_A$-formules distinctes. De plus, par définition, chaque petite formule appartient à au plus κ types. Par conséquent, il existe au plus $\kappa.\kappa$ types contenant une petite formule. Or pour κ infini, nous avons que $\kappa.\kappa = \kappa$, d'où il existe seulement κ types contenant une petite formule. Ainsi φ appartient à au moins deux types distincts p et q qui n'abritent que des grosses formules. Comme p et q sont distincts, il existe une

formule $\psi \in p \setminus q$. Alors nous décomposons φ comme représenté sur le dessin :



Comme p et q sont complets nous avons que $\varphi \wedge \psi \in p$ et $\varphi \wedge \neg\psi \in q$ et donc que ce sont des grandes formules.

Prenons $\mathcal{M}$ n'importe quel modèle de T, il satisfait la formule $x = x$. Pour l'étape suivante, le théorème de compacité nous dit que tout type consistant est réalisé dans une extension élémentaire de $\mathcal{M}$, en particulier les formules $\varphi \wedge \psi \in p$ et $\varphi \wedge \neg\psi \in q$ sont réalisées dans une extension élémentaire de $\mathcal{M}$. Ainsi, nous obtenons un arbre binaire de $\mathcal{L}_A$ formules consistantes, une contradiction. □

Un corollaire immédiat de ce théorème est le suivant :

Corollaire V.60. *Une théorie dénombrable est totalement transcendante si et seulement si elle est ω-stable.*

En particulier, la théorie des corps différentiellement clos est totalement transcendante.

Nous allons utiliser des résultats classiques de la théorie des modèles sur les théories totalement transcendantes, mais avant ça : une définition.

Définition V.61. Soient $\mathcal{M} \models T$ un modèle, A un ensemble de paramètres dans M et $(c_i)_{i\in I}$ une famille d'éléments de M. On dit que les a_i sont **indiscernables sur** A si pour toute $\mathcal{L}_A$-formule φ et toutes suites finies $c_{j_1}, \ldots, c_{j_m}$ et $c_{k_1}, \ldots, c_{k_m}$,

$$\mathcal{M} \models \varphi(c_{j_1}, \ldots, c_{j_m}) \Leftrightarrow \varphi(c_{k_1}, \ldots, c_{k_m}).$$

Exemple V.62. Soit $K \models ACF_0$ un corps algébriquement clos. L'ensemble

$$\{\sqrt{2}, -\sqrt{2}\}$$

est indiscernable sur $\mathbb{Q}$ car ils partagent le même polynôme minimal.

Si $t_1, t_2, \ldots$ sont des éléments transcendants sur K et sont algébriquement indépendants, alors ils sont indiscernables sur $\mathbb{Q}$. En effet, deux sous-ensembles de taille n des t_i induisent un isomorphisme entre les corps des fonctions rationnelles de $\mathbb{Q}$ en n variables engendrés par ces éléments transcendants. Alors, nous pouvons voir, en utilisant l'élimination des quantificateurs, qu'ils vérifient le même type.

En fait, dans une théorie ω-stable, les modèles premiers sont assez simples dans le sens où il ne peut pas y avoir de trop grandes familles d'indiscernables. De plus, ils isolent tous les types sur lesquels ils sont premiers. Nous admettrons le résultat suivant :

Théorème V.63 (Shelah, [2] Théorème 9.2.1)**.** *Soit T une théorie totalement transcendante. Soient $\mathcal{M}$ un modèle de T et A une sous-structure de $\mathcal{M}$.*

Le modèle $\mathcal{M}$ est premier sur A si et seulement si $\mathcal{M}$ est atomique sur A et ne contient pas d'ensembles non dénombrables d'indiscernables sur A.

Corollaire V.64. *Soit K un corps différentiel et L sa clôture différentielle. Si $\overline{d} = (d_1, \ldots, d_n)$ est un n-tuple de $L \setminus K$, alors la clôture différentielle de $K\langle d_1, \ldots, d_n\rangle$ n'est rien d'autre que L.*

Démonstration. Nous écrirons simplement $K\langle\overline{d}\rangle$ pour $K\langle d_1, \ldots, d_n\rangle$.

Si nous montrons que L est premier sur $K\langle\overline{d}\rangle$, alors par unicité du modèle premier, nous devrons avoir que L est la clôture différentielle de $K\langle\overline{d}\rangle$. Par le théorème précédent, il suffit de montrer que L est atomique sur $K\langle\overline{d}\rangle$ et qu'il n'existe pas d'ensembles non dénombrables d'indiscernables de L sur $K\langle\overline{d}\rangle$. Cette dernière condition est claire : comme L est premier sur K, il n'existe pas d'ensembles non dénombrables d'indiscernables de L sur K, or regarder sur $K\langle\overline{d}\rangle$ est encore plus restrictif (les indiscernables doivent satisfaire plus de formules). Par conséquent, il nous suffit juste de montrer que L est atomique sur $K\langle\overline{d}\rangle$.

Soit $\overline{a} = (a_1, \ldots, a_m) \in L^n$. Montrons que $\mathrm{tp}(\overline{a}/K\langle\overline{d}\rangle)$ est isolé dans $\mathrm{Sn}(K\langle\overline{d}\rangle)$, c'est-à-dire qu'il existe une $\mathcal{L}_{K\langle\overline{d}\rangle}$-formule qui détermine $\mathrm{tp}(a/K\langle\overline{d}\rangle)$. Or la concaténation $\overline{ad} = (a_1, \ldots, a_m, d_1, \ldots, d_n)$ est un élément de L qui est atomique sur K. Par conséquent, le uple $\overline{ad}$ est isolé dans K, donc il existe une $\mathcal{L}$-formule $\varphi(\overline{x}, \overline{y}, \overline{z})$ et $\overline{e}$ des éléments de K qui satisfont

$$\varphi(\overline{x}, \overline{y}, \overline{e}) \Rightarrow \mathrm{tp}(\overline{ad}/K).$$

Notre objectif va être de transformer cette formule en une $\mathcal{L}_{K\langle\overline{d}\rangle}$-formule qui isole $\mathrm{tp}(\overline{a}/K\langle\overline{d}\rangle)$. Puisque $K\langle\overline{d}\rangle$ est le corps différentiel engendré par K et $\overline{d}$, les formules à paramètres dans $K\langle\overline{d}\rangle$ et les formules à paramètres dans $K \cup \{d_1, \ldots, d_n\}$ sont exactement les mêmes. En particulier $\mathrm{tp}(a/K\langle\overline{d}\rangle) = \mathrm{tp}(a/K \cup \{d_1, \ldots, d_n\})$. Comme $\varphi(\overline{x}, \overline{y}, \overline{e}) \in \mathrm{tp}(\overline{ad}/K)$, nous avons $L \models \varphi(\overline{a}, \overline{d}, \overline{e})$, d'où

$$\varphi(\overline{x}, \overline{d}, \overline{e}) \in \mathrm{tp}(\overline{a}/K\langle\overline{d}\rangle).$$

De plus, la formule $\varphi(\overline{x}, \overline{d}, \overline{e})$ isole bien $\mathrm{tp}(\overline{a}/K\langle\overline{d}\rangle)$. □

Notons que l'argument ne requiert rien sur la théorie des corps différentiels. L'argument se concentre sur les types isolés issus de la primalité du modèle sur K.

Démonstration de la proposition V.55. Soit $a \in L \setminus K$. Comme L est la clôture différentielle de K, le type de a sur K est isolé par une formule $\varphi(v)$ à paramètres dans K. Il Il existe $b \in L \setminus K$ et $b \neq a$ qui réalise φ car le type de a est en bijection

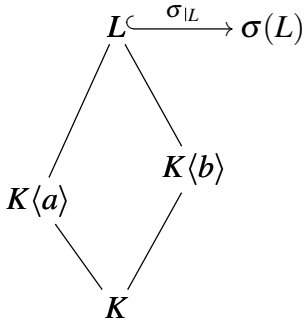
avec un polynôme différentiel dit *minimal*. Ce polynôme admettant plusieurs solutions (car $a \notin K$), une autre racine de ce polynôme réalise également φ. Alors a et b réalisent le même type sur K

En particulier, le corollaire précédent nous dit que L est une clôture différentielle de $K\langle b\rangle$.

Quitte à se plonger dans une extension élémentaire $\mathcal{M}$ de L, un résultat classique de la théorie des modèles (voir par exemple [2], proposition 4.1.5) nous donne un automorphisme

$$\begin{aligned}\sigma : \mathcal{M} &\to \mathcal{M}\\ a &\mapsto b\\ x &\mapsto x, \forall x \in K\end{aligned}$$

Alors, en considérant la restriction de σ à L et en regardant seulement l'image de L par σ à l'arrivée, nous obtenons un isomorphisme $\sigma_{|L} : L \to \sigma(L)$ fixant K et envoyant a sur b. Comme L et $\sigma(L)$ sont isomorphes, ce dernier est également la clôture différentielle de $K\langle b\rangle$.



Mais alors, par unicité de la clôture différentielle de $K\langle b\rangle$, il existe $\tau : \sigma(L) \to L$ qui fixe $K\langle b\rangle$. Alors, notre candidat pour notre automorphisme non triviale de L qui fixe K sera $\tau \circ \sigma_{|L}$. C'est bien un isomorphisme qui fixe K car τ et σ le fixent. De plus $(\tau \circ \sigma_{|L})(a) = \tau(b) = b$ car τ fixe $K\langle b\rangle$,. □

Cette proposition, encore une fois, ne tire pas grand chose de la théorie des corps différentiels : c'est une preuve assez générale qui se greffe complètement, par exemple, au cas des corps algébriquement clos.

Montrons un petit lemme qui nous donnera un lien entre les corps des constantes d'un corps différentiel et celui de sa clôture différentielle.

Lemme V.65. *Soit L la clôture différentielle de K. Alors C_L est algébrique sur C. En particulier, si C est algébriquement clos, alors $C_L = C$.*

Démonstration. Soit $a \in C_L$. Montrons que a est algébrique sur C. Comme L est atomique sur K, le type $p = \mathrm{tp}(a/K)$ est isolé. Or a est une constante, ainsi son type admet comme formule "$\delta(v) = 0$", d'où $I_p = \{f \in K\{X\} : "f(v) = 0" \in p\}$ est de rang différentiel $\leqslant 1$. Soit $\varphi(x) \equiv \bigwedge f_i(x) = 0 \wedge g(x) = 0$, où les f_i et $g \in K\{X\}$, la formule qui isole p.

Supposons que $\mathrm{RD}(I_p) = 1$. Le polynôme $\delta(X)$ est un polynôme minimal de I_p. Le corollaire V.37 nous dit que C_L est algébriquement clos, et donc il est fortement minimal dans le langage des anneaux. C'est un ensemble infini, donc les formules qu'il satisfait sont les "$h(x) \neq 0$", avec $h \in K[X]$. Par conséquent $\varphi(x)$ doit être de la forme $\varphi(x) \equiv \delta(x) = 0 \wedge g(x) \neq 0$ pour un certain $g \in K[X]$. Mais cette formule ne peut pas isoler p. En effet C est infini donc il existe $b \in C$ tel que $g(b) \neq 0$. Or $b \in K$ donc il est algébrique, d'où $\mathrm{tp}(b/K) \neq \mathrm{tp}(a/K)$, une contradiction avec φ qui isole p. Donc $\mathrm{RD}(I_p) = 0$.

Supposons que $\mathrm{RD}(I_p) = 0$. Soit $f(X) = \sum_{i=0}^{n} b_i X^i \in K[X]$ le polynôme minimal (algébrique) de a sur K. Comme $f(a) = 0$, nous avons que $\delta(f(a)) = 0$, c'est-à-dire

$$\delta(f(a)) = \delta(a) \sum_{i=0}^{n-1} (i+1) b_{i+1} a^i + \sum_{i=0}^{n} \delta(b_i) a^i = 0.$$

Comme $\delta(a) = 0$, le premier terme tombe à l'eau. Or $b_n = 1$ car f est monique, d'où $b_n' = 0$. Il reste donc

$$\sum_{i=0}^{n-1} \delta(b_i) a^i = 0.$$

Nous avons un nouveau polynôme qui annule a de degré strictement plus petit que celui du polynôme minimal de a. Par minimalité de f, ce polynôme doit être le polynôme nul. Nous en déduisons que les $\delta(b_i)$ sont tous nuls, c'est-à-dire que tous les b_n sont des constantes, i.e. le polynôme f est à coefficients dans C. Ainsi a est algébrique sur C. □

Et un dernier lemme pour la route qui nous dit qu'être algébrique au sens de la théorie des modèles et être algébrique au sens usuel coïncident encore dans les corps différentiels.

Lemme V.66. *Soit k un corps différentiel généré par un ensemble B. Soit x un élément dans une extension de k. Alors x est algébrique sur k si et seulement si $x \in acl(B)$, dans le sens modèle théorique.*

Démonstration. Si x est racine d'un polynôme dans $K[X]$, alors forcément il est algébrique au sens usuel car si p est le polynôme minimal de x, alors l'ensemble défini par la formule $\varphi(x) \equiv p(x) = 0$ est fini. C'est une formule définissable dans

le langage $\mathcal{L}_B$ car k est composé des termes engendrés par les éléments de B et du langage.

Réciproquement, supposons que x est algébrique sur B. Soit $I = I(x/k)$. Si $\mathrm{RD}(I) = 0$, alors x est fortement algébrique sur k car un polynôme minimal serait d'ordre 0. Supposons donc $\mathrm{RD}(I) > 0$. Soit K la clôture différentielle de k. Comme x est algébrique sur B et donc k, le type $\mathrm{tp}(x/k)$ est isolé. Soit $f(x) = 0 \wedge g(x) \neq 0$ une formule qui isole ce type, avec g d'ordre plus petit que f. Comme x est algébrique, il existe un nombre fini de réalisations $a_1, \ldots, a_n$ de $\mathrm{tp}(x/k)$ dans K. Mais K est différentiellement clos et donc il existe un $b \in K$ tel que

$$f(b) = 0 \wedge g(b)(x - a_1) \ldots (x - a_n) \neq 0.$$

Par conséquent b est une réalisation de $\mathrm{tp}(x/k)$ distincts des a_i, une contradiction. □

Chapitre VI

Étude des groupes algébriques

Nous allons dans ce chapitre étudier de plus près les groupes algébriques introduits avec les courbes elliptiques. Le contenu de cette section est tiré de [4] pour lequel nous avons étoffé les arguments. L'objectif de ce chapitre sera de *décrire* la fermeture de Kolchin du groupe de torsion d'une courbe elliptique au moyen d'un certain morphisme noté μ. Cet objet mathématique sera essentiel pour construire des exemples de corps différentiellement clos rigides.

Nous construisons notre théorie autour d'un corps différentiellement clos K de caractéristique nulle, avec comme dérivée $\delta : K \to K$. Relevons déjà que cette hypothèse de différentiellement clos ne sera pas nécessaire pour tous résultats énoncés. Nous noterons C le corps des constantes de K, c'est-à-dire l'ensemble

$$C = \{x \in K : \delta(x) = 0\}.$$

Pour $f \in K[X_1, \ldots, X_n]$, nous noterons f^δ le polynôme obtenu en dérivant uniquement les coefficients.

Exemple VI.1. Pour $K = \mathbb{C}(t)$, muni de la dérivée usuelle sur les polynômes, et $f(X) = t^2X^3 + tX + \frac{1}{t}$, nous avons que $f^\delta(X) = 2tX^3 + X - \frac{1}{t^2}$.

Soient $f \in K[X_1, \ldots, X_n]$ et $a = (a_1, \ldots, a_n) \in K^n$, nous pouvons écrire :

$$\delta(f(a_1, \ldots, a_n)) = \sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(a)\delta(a_i) + f^\delta(a).$$

En effet, cela découle de la règle de Leibnitz. Regardons sur un exemple. Soient $f(X,Y) = cXY^3 \in K[X,Y]$ et $(a,b) \in K^2$. Alors

$$\frac{\partial f}{\partial X}(a,b)\delta(a) = c\delta(a)b^3 \text{ et } \frac{\partial f}{\partial Y}(a,b)\delta(b) = ca3\delta(b)b^2.$$

En outre, par la formule de Leibnitz nous obtenons que

$$\begin{aligned}\delta(f(a,b)) &= \delta(cab^3)\\ &= \delta(c)ab^3 + c\delta(a)b^3 + ca3b^2\delta(b)\\ &= f^\delta(a,b) + \frac{\partial f}{\partial X}(a,b)\delta(a) + \frac{\partial f}{\partial Y}(a,b)\delta(b).\end{aligned}$$

La dérivée δ est celle associée à K tandis que ∂ est la dérivée partielle usuelle. Nous noterons $\delta(a)$ pour $(\delta(a_1),\dots,\delta(a_n))$.

Remarque VI.2. Un polynôme $f \in K[X_1,\dots,X_n]$ est à coefficients dans C si et seulement si $f^\delta = 0$.

VI.1 Prolongement de variétés algébriques

Soit $V \subseteq K^n$ une variété algébrique et $I(V) = (f_1,\dots,f_m)$ l'idéal engendré par V.

Définition VI.3. On appelle l'**espace tangent en** $a \in V$ le sous-ensemble de K^n défini par :

$$T_a(V) = \{u \in K^n : \forall f \in I(V), \sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(a)u_i = 0\}.$$

On définit alors le **fibré tangent de** V comme le sous-ensemble de K^{2n} donné par :

$$T(V) = \{(a,u) \in K^{2n} : a \in V, u \in T_a(V)\}.$$

Remarque VI.4. L'espace tangent est un ensemble algébrique de K^n car défini par des équations polynomiales. Par conséquent, le fibré tangent est un fermé de Zariski de K^{2n} car l'appartenance de $a \in V$ et $u \in T_a(V)$ sont aussi déterminés par des équations polynomiales.

Nous pouvons voir le fibré tangent comme la réunion disjointe :

$$T(V) = \bigcup_{a \in V} \{a\} \times T_a(V)$$

Le fibré tangent est l'ensemble des fibres $T_a(V)$ données par $a \in V$.

Une propriété immédiate de l'espace tangent est la suivante :

Lemme VI.5. *Soit $a \in V$. L'espace tangent de V en a est un K-espace vectoriel.*

Démonstration. Soient $u, v \in T_a(V)$ et $\lambda \in K$. Alors $\lambda u + v \in T_a(V)$ si et seulement si pour tout $f \in I(V)$,

$$\sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(a)(\lambda u_i + v_i) = 0.$$

Il nous suffit de distribuer pour en déduire que $\lambda u + v \in T_a(V)$. De plus, l'espace tangent en a contient le vecteur nul car pour tout $i \in \{1, \ldots, n\}$,

$$\frac{\partial f}{\partial X_i}(a).0 = 0.$$

□

Exemple VI.6. Soit E la courbe elliptique définie sur les constantes de K par $f(X,Y) = Y^2 - X^3 - 1$. Nous avons $(2,3) \in E$, regardons son espace tangent en ce point.

Soit $(u,v) \in K^2$, nous avons que $(u,v) \in T_{(2,3)}(E)$ si et seulement si $-3.2^2u + 2.3v = 0$, i.e. $v = 2u$. Nous obtenons que $T_{(2,3)}(E) = \{(u,2u) : u \in K\}$. C'est l'espace tangent au point $(2,3)$ de E, ramené à l'origine. Cet espace coïncide avec la droite tangente usuelle en un point d'une courbe dans le plan.

Quel est le fibré tangent de E ? Si $x = 0$, alors $y = \pm 1$ et si $y = 0$, forcément $x = -1$. Les espaces tangents aux points $(0,1)$ et $(0,-1)$ ne sont rien d'autres que la droite horizontale $y = 0$ et l'espace tangent en $(-1,0)$, la droite verticale $x = 0$. Si $x \neq 0$ et $y \neq 0$, alors $(u,v) \in T_{(x,y)}(E)$ si et seulement si $-3x^2u + 2yv = 0$, c'est-à-dire que $v = \frac{3x^2}{2y}u$. Par conséquent, le fibré tangent de E est donné par :

$$T(E) = \{(0,1,u,0), (0,-1,u,0), (-1,0,0,u)) : u \in K\} \cup \{(x,y,u, \frac{3x^2}{2y}u) : (x,y) \in E \wedge x \neq 0 \wedge y \neq 0 \wedge u \in K\}.$$

Exemple VI.7. Soient S le cercle unité défini par $f(X,Y) = X^2 + Y^2 - 1$ et $(x,y) \in S$. Un point du plan (u,v) appartient à l'espace tangent $T_{(x,y)}(S)$ si et seulement si $2xu + 2yv = 0$. Le fibré tangent de S s'écrit donc :

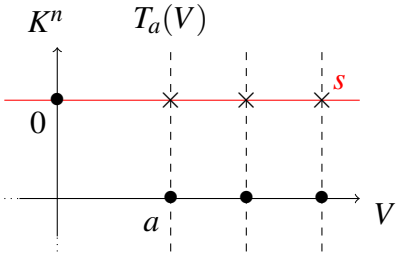
$$T(S) = \{(x,y,u,v) : (x,y) \in S, (u,v) \in K^2 \text{ et } xu + yv = 0\}.$$

Définition VI.8. Soit $f : A \to B$ une fonction. On dit que $g : B \to A$ est une **section** de f si $f \circ g = \mathrm{Id}_B$.

En particulier, si g est une section de f, alors g est injective car $g(a) = g(b)$ implique que $f(g(a)) = f(g(b)) = a = b$. La fonction g sélectionne un point dans chaque préimage de $b \in \mathrm{Im}(f)$.

Discussion VI.9. Soit $p : T(V) \to V$ la projection de $T(V)$ dans V. Nous avons une section naturelle s de p, donnée par $s(a) = (a,0)$. C'est bien une section de p car $(p \circ s)(a) = p(a,0) = a$ et $0 \in T_a(V)$ pour tout $a \in V$.

En représentant sur un dessin, cela donne :



La fonction s vient prendre un élément de chaque fibre. Une fibre est l'espace tangent en un point a de V, consistant en des vecteurs de K^n.

Lemme VI.10. *Pour tout $u \in T_a(V)$, nous avons $T_u(T_a(V)) = T_a(V)$.*

Démonstration. Un vecteur u appartient à $T_a(V)$ si et seulement si pour tout $f \in I(V)$, c'est un zéro de $g_f(Y_1,\dots,Y_n) = \sum_{i=1}^n \frac{\partial f}{\partial X_i}(a)Y_i$.

Par conséquent, en dérivant selon les variables Y_i, un vecteur v de K^n sera dans $T_u(T_a(V))$ si et seulement si pour tout $f \in I(V)$,

$$\sum_{j=1}^{n} \Big(\sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(a) \frac{\partial Y_i}{\partial Y_j}(u_i) \Big) v_j = 0.$$

Or $\frac{\partial Y_i}{\partial Y_j} \neq 0$ si et seulement si $i = j$, et si $i = j$, alors $\frac{\partial Y_i}{\partial Y_j} = 1$, ainsi nous pouvons réécrire cette expression comme

$$\sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(a) v_i = 0,$$

c'est-à-dire que $v \in T_a(V)$. □

Nous pouvons voir qu'en fait, c'est une conséquence que l'appartenance à $T_a(V)$ s'exprime par une équation *linéaire*. Ainsi, plus généralement, l'espace tangent d'un espace vectoriel n'est rien d'autre que lui-même.

Définition VI.11. On appelle le **torseur associé au plan tangent** $T_a(V)$ le sous-ensemble de K^n défini par :

$$\tau_a(V) = \{u \in K^n : \forall f \in I(V), f^\delta(a) + \sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(a) u_i = 0\}.$$

On définit alors le **prolongement de** V comme le sous-ensemble de K^{2n} donné par :

$$\tau(V) = \{(a,u) \in K^{2n} : a \in V, u \in \tau_a(V)\}.$$

On appelle aussi $\tau(V)$ le **fibré torseur associé à** V.

De la même manière que pour l'espace tangent et le fibré tangent, les torseurs et le prolongement de V sont des ensembles algébriques.

Proposition VI.12. *Soit $a \in V$. Les ensembles $T_a(V)$ et $\tau_a(V)$ sont des variétés algébriques.*

Démonstration. Notons $I(V) = (f_1, \ldots, f_m)$. Les ensembles $T_a(V)$ et $\tau_a(V)$ sont irréductibles car $u \in T_a(V)$ si et seulement si pour $f_1, \ldots, f_m$, le vecteur u est un zéro du polynôme

$$g_k(Y_1, \ldots, Y_n) = \sum_{i=1}^{n} \frac{\partial f_k}{\partial X_i}(a) Y_i.$$

Idem pour $\tau_a(V)$ en sommant en plus la constante $p^\delta(a)$. Comme ce sont des polynômes de degré 1, l'idéal engendré par ces polynômes est premier. Par conséquent $V(g_1, \ldots, g_m) = T_a(V)$ est irréductible et pareil pour $\tau_a(V)$. □

Remarque VI.13. En outre, puisque $K[X_1, \ldots, X_n]$ est noethérien, l'appartenance aux ensembles $T_a(V)$, $T(V)$, $\tau_a(V)$ et $\tau(V)$ est exprimable par un nombre fini d'équations polynomiales, et donc au premier ordre dans le langage des anneaux (le symbole δ n'est pas nécessaire car son image est toujours dans K).

Exemple VI.14. Soit $\pi : \tau(V) \to V$, la projection de $\tau(V)$ sur ses n premières coordonnées. La fonction $\nabla : V \to \tau(V)$ qui envoie un élément $a \in V$ sur $(a, \delta(a))$ est une section de π. L'élément $\delta(a) \in \tau_a(V)$ car pour tout $f \in I(V)$, nous savons que $p(a) = 0$ et par conséquent,

$$\delta(p(a)) = f^\delta(a) + \sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(a) \delta(a_i) = 0.$$

Discussion VI.15 (Liens entre le prolongement et le fibré tangent)**.** Si V est défini sur les constantes, alors $f^\delta = 0$, ainsi pour tout $a \in V$, les ensembles $T_a(V)$ et $\tau_a(V)$ coïncident. Il en résulte que $T(V) = \tau(V)$.

En général, les ensembles $\tau(V)$ et $T(V)$ ne sont pas isomorphes en tant que variétés algébriques, mais l'application

$$\begin{aligned} \sigma : T(V) &\to \tau(V) \\ (a,u) &\mapsto (a, u + \delta(a)) \end{aligned}$$

est un isomorphisme algébrique différentiel, dans le sens où nous le décrivons dans le langage des anneaux munis du symbole de dérivation δ.

En effet, notons déjà que σ est bien définie : l'élément $(a, u+\delta(a)) \in \tau(V)$ si et seulement si pour tout $f \in I(V)$,

$$f^{\delta}(a) + \sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(a)(u_i + \delta(a_i)) = 0.$$

Or en distribuant $(u_i + \delta(a_i))$, comme $a \in V$ et ∇ est une section de $\tau(V)$, le terme

$$f^{\delta}(a) + \sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(a)\delta(a_i)$$

est nul, et donc, puisque $u \in T_a(V)$,

$$f^{\delta}(a) + \sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(a)(u_i + \delta(a_i)) = \sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(a)u_i = 0.$$

Supposons que $(a, u+\delta(a)) = (b, v+\delta(b))$, alors $a = b$, d'où $\delta(a) = \delta(b)$ et donc $u = v$, ainsi σ est injective. Si $(a,u) \in \tau(V)$, considérons l'élément $(a, u - \delta(a)$, alors $\sigma(a, u-\delta(a)) = (a,u)$. Notons que que $u - \delta(a)$ est bien dans $T(V)$ car

$$\begin{aligned}\sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(a)(u_i - \delta(a_i)) &= f^{\delta}(a) - f^{\delta}(a) + \sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(a)(u_i - \delta(a_i)) \\ &= \big(f^{\delta}(a) + \sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(a)u_i\big) - \big(f^{\delta}(a) + \sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(a)\delta(a_i)\big) \\ &= 0.\end{aligned}$$

En fait, pour tous $u, v \in \tau_a(V)$, leur différence $u - v$ est dans $T_a(V)$ par le même argument. Nous profitons juste ici de la section de π donnée par ∇. Quoi qu'il en soit, nous avons montré que σ est bien bijective.

Définition VI.16. Soient deux fonctions f et g définies vers un même ensemble comme représentés sur le diagramme suivant.

$$\begin{array}{ccc} & & Y \\ & & \downarrow g \\ X & \xrightarrow{f} & Z \end{array}$$

On définit le **produit fibré** [1] de X et Y sur Z, noté $X \times_Z Y$, comme l'ensemble des couples (x,y) dont les composantes ont la même image, c'est-à-dire que $f(x) = g(y)$.

1. Le produit fibré est parfois appelé *pullback* sous l'influence des travaux anglophones.

Exemple VI.17. Si $f = p : T(V) \to V$ et $g = \pi : \tau(V) \to V$, alors le produit fibré $T(V) \times_V \tau(V)$ est l'ensemble des éléments $((a,u),(a,v))$ avec $u \in T_a(V)$ et $v \in \tau_a(V)$.

Définition VI.18. Soient G un groupe et E un ensemble tels que G agit sur E. On dit que l'action de G sur E est **simplement transitive** si elle est libre et transitive, c'est-à-dire que pour tous $x, y \in E$, il existe un unique $g \in G$ tel que $y = g \cdot x$.

Exemple VI.19. Un groupe G agit sur lui-même par translations $G \times G \to G$: $(g,h) \mapsto gh$. C'est une action simplement transitive car pour tous $g, \tilde{g} \in G$, nous avons que $g = \tilde{g}h$ si et seulement si $h = \tilde{g}^{-1}g$.

Définition VI.20. Soient X, Y et V des ensembles algébriques et $f : X \to V$ et $g : Y \to V$ des applications régulières telles que pour tout $a \in V$, l'ensemble $f^{-1}(a)$ soit un groupe. On dit que Y **est un torseur sous** X s'il existe une application $q : X \times_V Y \to Y$ tel que q induit une action de groupe simplement transitive de $f^{-1}(a)$ sur $g^{-1}(a)$ pour tout $a \in V$.

Exemple VI.21. Le prolongement $\tau(V)$ est un torseur sous $T(V)$ avec les applications $f = p$ et $g = \pi$ (comme définis précédemment). Nous avons bien que $p^{-1}(a)$ est un groupe car $p^{-1}(a) = \{(a,u) : u \in T_a(V)\} \cong T_a(V)$ est un K-espace vectoriel. Nous avons aussi $\pi^{-1}(a) = \tau_a(V)$. Nous définissons alors comme fonction sur le produit fibré $T(V) \times_V \tau(V)$:

$$\begin{aligned} q : T(V) \times_V \tau(V) &\to \tau(V) \\ ((a,u),(a,v)) &\mapsto (a, u+v) \end{aligned}$$

Des calculs analogues à ceux qui précédent montrent que q est bien défini : $u+v$ est bien dans $\tau_a(V)$. Pour $a \in V$, nous avons l'action de $T_a(V)$ sur $\tau_a(V)$:

$$\begin{aligned} q_a : T_a(V) \times \tau_a(V) &\to \tau_a(V) \\ (u,v) &\mapsto u+v \end{aligned}$$

Montrons que cette action est simplement transitive, c'est-à-dire que deux éléments quelconques de $\tau_a(V)$ sont envoyés l'un sur l'autre par un unique élément de $T_a(V)$.

Soient $v, w \in \tau_a(V)$. Prenons $u = w - v \in T_a(V)$. Alors $q_a(u,v) = w - v + v = w$. De plus, c'est forcément le seul car $u + v = w$ si et seulement si $u = w - v$.

Proposition VI.22. *Soit $a \in V$. Si V est lisse, alors $T_a(V)$, $T(V)$, $\tau_a(V)$ et $\tau(V)$ le sont aussi.*

Démonstration. Supposons que V est de dimension d et $V(I)$ avec $I = (f_1, \dots, f_m)$. Dire que V est lisse, c'est dire que la matrice

$$J_a(V) = \begin{pmatrix} \frac{\partial f_1}{\partial X_1}(a) & \dots & \frac{\partial f_1}{\partial X_n}(a) \\ \vdots & \ddots & \vdots \\ \frac{\partial f_m}{\partial X_1}(a) & \dots & \frac{\partial f_m}{\partial X_n}(a) \end{pmatrix}$$

est une matrice de rang $n-d$ (voir proposition IV.49). Or, l'espace tangent de V au point a n'est rien d'autre que le noyau de cette matrice, qui est de dimension d. Par conséquent $\dim_K(T_a(V)) = d$. Par le lemme VI.10, l'espace tangent en tout point n'est rien d'autre que lui-même, ainsi ils ont la même dimension, d'où pour tout $a \in V$, la variété $T_a(V)$ est lisse.

Montrons que $T(V)$ est lisse. Comme $T(V)$ est déterminé par les polynômes

$$\tilde{f}_i(X_1, \dots, X_n, Y_1, \dots, Y_n) = f_i(X_1, \dots, X_n)$$

et

$$g_{f_i}(X_1, \dots, X_n, Y_1, \dots, Y_n) = \sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(X_1, \dots, X_n) Y_i$$

pour tout $1 \leqslant i \leqslant m$, l'espace tangent de $T(V)$ au point $(a,u) \in T(V)$, noté $T_{(a,u)}(T(V))$, est le noyau de l'application linéaire

$$J = \begin{pmatrix} \frac{\partial f_1}{\partial X_1}(a) & \dots & \frac{\partial f_1}{\partial X_n}(a) & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \frac{\partial f_m}{\partial X_1}(a) & \dots & \frac{\partial f_m}{\partial X_n}(a) & 0 & \dots & 0 \\ \sum_{j=1}^n \frac{\partial^2 f_1}{\partial X_j \partial X_1}(a) u_j & \dots & \sum_{j=1}^n \frac{\partial^2 f_1}{\partial X_j \partial X_n}(a) u_j & \frac{\partial f_1}{\partial X_1}(a) & \dots & \frac{\partial f_1}{\partial X_n}(a) \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \sum_{j=1}^n \frac{\partial^2 f_m}{\partial X_j \partial X_1}(a) u_j & \dots & \sum_{j=1}^n \frac{\partial^2 f_m}{\partial X_j \partial X_n}(a) u_j & \frac{\partial f_m}{\partial X_1}(a) & \dots & \frac{\partial f_m}{\partial X_n}(a) \end{pmatrix}.$$

Ainsi pour montrer que $T(V)$ est lisse, puisque $T(V)$ est de dimension $2d$ (c'est la $\dim(V) + \dim(T_a(V))$ pour n'importe quel $a \in V$), il faut et il suffit de montrer que la jacobienne J en (a,u) de $T(V)$ est de rang $2n-2d$.

Les n dernières colonnes sont de rang $n-d$ car V est lisse. En outre, la dimension de l'espace vectoriel engendré par les n premiers vecteurs colonnes est minorée par $n-d$ car les m premières lignes sont de rang $n-d$ (V est encore lisse), ainsi en regardant une concaténation avec les m dernières lignes, les vecteurs colonnes ne peuvent devenir que plus libres. De plus, nous pouvons montrer que cette dimension est majorée par $n-d$ car une dépendance linéaire sur les

m premières lignes (des n premières colonnes) se transmet sur l'intégralité des n premières colonnes. Ceci prouvé, nous aurons montré que l'espace vectoriel engendré par les n premiers vecteurs colonnes est de dimension $n-d$.

Supposons donc qu'il existe des λ_i non tous nuls tels que

$$\sum_{i=1}^{n} \lambda_i \big(\frac{\partial f_1}{\partial X_i}(a), \dots, \frac{\partial f_m}{\partial X_i}(a)\big) = 0.$$

Montrons que

$$\sum_{i=1}^{n} \lambda_i \big(\frac{\partial f_1}{\partial X_i}(a), \dots, \frac{\partial f_m}{\partial X_i}(a), \sum_{j=1}^{n} \frac{\partial^2 f_1}{\partial X_j \partial X_i}(a) u_j, \dots, \sum_{j=1}^{n} \frac{\partial^2 f_m}{\partial X_j \partial X_i}(a) u_j\big) = 0.$$

Les n premières composantes sont égales 0 par hypothèse. Regardons composante par composante. Pour tout $k \in \{1, \dots, m\}$, nous avons :

$$\begin{aligned}
\sum_{i=1}^{n} \lambda_i \sum_{j=1}^{n} \frac{\partial^2 f_k}{\partial X_j \partial X_i}(a) u_j &= \sum_{j=1}^{n} \sum_{i=1}^{n} \lambda_i \frac{\partial^2 f_k}{\partial X_j \partial X_i}(a) u_j \\
&= \sum_{j=1}^{n} \frac{\partial}{\partial X_j} \big(\sum_{i=1}^{n} \lambda_i \frac{\partial f_k}{\partial X_i}(a) \big) u_j \\
&= \sum_{j=1}^{n} u_j \frac{\partial}{\partial X_j} \big(\sum_{i=1}^{n} \lambda_i \frac{\partial f_k}{\partial X_i}(a) \big) \\
&= \sum_{j=1}^{n} u_j \frac{\partial 0}{\partial X_j} \\
&= 0.
\end{aligned}$$

Par conséquent, cette famille de vecteurs colonnes est au plus de rang $n-d$.

Au final, nous avons que le rang de la matrice jacobienne J est majorée par $2n-2d$ car l'image de la matrice est engendré par deux familles de vecteurs de dimension $n-d$ chacune. Il nous reste à montrer l'autre inégalité.

C'est une conséquence du lemme suivant :

Lemme VI.23. *Soit* $M = \begin{pmatrix} A & 0 \\ B & C \end{pmatrix}$ *une matrice. Alors* $Rang(M) \geqslant Rang(A) + Rang(C)$.

Démonstration. Considérons la matrice $N = \begin{pmatrix} A & 0 \\ 0 & C \end{pmatrix}$. Nous pouvons voir qu'elle est de rang $\mathrm{Rang}(A) + \mathrm{Rang}(C)$. Nous affirmons que le rang de cette matrice est inférieure à celle de M. En effet, une dépendance linéaire sur les vecteurs de $0.C$ (où . est la concaténation) peut se retranscrire en une dépendance linéaire sur les

vecteurs $B.C$ en prenant les scalaires sur B égaux à 0. Alors, une dépendance linéaire sur les vecteurs colonnes de $\begin{matrix} A.0 \\ 0.C \end{matrix}$ se transfert sur ceux de $\begin{matrix} A.0 \\ B.C \end{matrix}$, d'où notre affirmation. □

Or, notre jacobienne J admet un bloc de 0 sur la partie supérieure droite de la matrice. Le lemme nous dit dans notre contexte, avec $M = J$ et $A = C$ est la matrice de $T_a(V)$ qui est de rang $n-d$, que $\text{Rang}(J) \geqslant 2n-2d$. En conclusion, le rang J est donné par $2n-2d$ et donc $T(V)$ est bien lisse.

Un argument similaire pour $\tau_a(V)$ et $\tau(V)$ permet de déduire qu'ils sont lisses. □

Nous admettrons le résultat suivant sur ces ensembles, pour une preuve nous pourrons consulter la proposition 1.5 de [3].

Proposition VI.24. *Si V est lisse, alors $T(V)$ et $\tau(V)$ sont irréductibles.*

Énonçons un résultat dont nous aurons besoin. Il généralise la règle de dérivation d'une fonction composée dans le cadre de l'analyse réelle aux polynômes sur des anneaux différentiels.

Proposition VI.25 (Bourbaki IV.§1.4, Proposition 4, Corollaire)**.** *Soient A un anneau commutatif muni d'une dérivée D, $g \in A[X_1,\dots,X_m]$ et $f_i \in A[Y_1,\dots,Y_n]$ pour $1 \leqslant i \leqslant m$. Posons $h = g(f_1,\dots,f_m)$. Alors pour tout $1 \leqslant j \leqslant n$,*

$$\frac{\partial h}{\partial Y_j} = \sum_{i=1}^{m} D_i g(f_1,\dots,f_m)\frac{\partial f_i}{\partial Y_j}.$$

Avec $D_i(g) = \frac{\partial g}{\partial X_i}$, nous obtenons le résultat classique.

Discussion VI.26. Soient $W \subseteq K^m$ une variété algébrique et $\varphi : V \to W$ une application régulière. Alors nous pouvons définir une fonction qui envoie les vecteurs tangents de V sur ceux de W.

Supposons que $\varphi(x) = (\varphi_1(x),\dots,\varphi_m(x))$ avec $\varphi_i : K^n \to K$. Pour $a \in V$, considérons l'application :

$$\begin{aligned} d_a\varphi : T_a(V) &\to T_{\varphi(a)}(W) \\ u &\mapsto \left(\sum_{i=1}^{n} \frac{\partial \varphi_1}{\partial X_i}(a)u_i, \dots, \sum_{i=1}^{n} \frac{\partial \varphi_m}{\partial X_i}(a)u_i\right) \end{aligned}$$

C'est l'application linéaire associée à la matrice jacobienne : $K^n \to K^m$ de la fonction φ au point a, restreinte à $T_a(V)$. Avons-nous bien que son image est dans $T_{\varphi(a)}(W)$?

Pour cela, nous devons avoir que $d_a\varphi(u)$ est un zéro de la différentielle de tout $g \in I(W)$ en $\varphi(a)$, c'est-à-dire,

$$\sum_{j=1}^{m} \frac{\partial g}{\partial X_j}(\varphi(a))(d_a\varphi(u))_j = 0,$$

ou encore, en utilisant les mêmes notations pour la différentielle de g en $\varphi(a)$,

$$d_{\varphi(a)}g(\varphi(a))(d_a\varphi(u)) = 0.$$

Notons bien que les différentielles $d_{\varphi(a)}g : K^m \to K$ et $d_a\varphi : K^n \to K^m$ sont bien définies sur leur domaine. Le seul problème nous préoccupant est de voir si la restriction à $T_a(V)$ de $d_a\varphi$ nous garantit une image dans $T_{\varphi(a)}(W)$. Par la formule de dérivation de la composée de deux fonctions, nous obtenons que

$$\sum_{j=1}^{m} \frac{\partial g}{\partial X_j}(\varphi(a))(d_a\varphi(u))_j = d_a(g\circ\varphi)(u).$$

Or, le morphisme φ est une application polynomiale qui envoie un élément de V sur un élément de W, ainsi $g\circ\varphi \in I(V)$ pour tout $g \in I(W)$. Par conséquent, comme $u \in T_a(V)$, c'est un zéro de la différentielle de $g\circ\varphi$ au point a, donc

$$d_a(g\circ\varphi)(u) = 0,$$

c'est-à-dire que $d_a\varphi(u) \in T_{\varphi(a)}(W)$.

Nous pouvons étendre cette différentielle aux fibrés $T(V)$ et $\tau(V)$. Notons $\varphi^\delta(x) = (\varphi_1^\delta(x), \ldots, \varphi_m^\delta(x))$. Nous définissons alors les applications

$$\begin{aligned} T(\varphi) : T(V) &\to T(W) \\ (a,u) &\mapsto (\varphi(a), d_a\varphi(u)) \end{aligned}$$

et

$$\begin{aligned} \tau(\varphi) : \tau(V) &\to \tau(W) \\ (a,u) &\mapsto (\varphi(a), d_a\varphi(u) + \varphi^\delta(a)) \end{aligned}$$

Notons que puisque ce sont des applications linéaires, ce sont des applications régulières. En outre, nous voyons facilement que l'application $T(\varphi)$ est bien définie. Vérifions que $\tau(\varphi)$ l'est aussi. Soit $(a,u) \in \tau(V)$. Nous voulons montrer que $d_a\varphi(u) + \varphi^\delta(a) \in \tau_{\varphi(a)}(W)$, c'est-à-dire que $g^\delta(\varphi(a)) + d_{\varphi(a)}g\big(d_a\varphi(u) + \varphi^\delta(a)\big) = 0$. Comme $g\circ\varphi \in I(V)$, nous avons $g(\varphi(a)) = 0$, d'où $\delta(g(\varphi(a))) = 0$. Or, nous avons que

$$\begin{aligned} \delta((g\circ\varphi)(a)) &= \sum_{j=1}^{m} \frac{\partial(g\circ\varphi)}{\partial X_j}(a)\delta(a_j) + (g\circ\varphi)^\delta(a) \\ &= d_a(g\circ\varphi)\delta(a) + (g\circ\varphi)^\delta(a) \\ &= 0, \end{aligned}$$

mais aussi

$$\begin{aligned}\delta(g(\varphi(a))) &= \sum_{j=1}^{m} \frac{\partial g}{\partial X_j}(\varphi(a))\delta(\varphi_j(a)) + g^{\delta}(\varphi(a)) \\ &= d_{\varphi(a)}g\big(\delta(\varphi(a))\big) + g^{\varphi}(\varphi(a)) \\ &= d_{\varphi(a)}g\big(d_a\varphi(\delta(a)) + \varphi^{\delta}(a)\big) + g^{\varphi}(\varphi(a)).\end{aligned}$$

Et donc par linéarité de la différentielle et la règle de dérivation de la composée,

$$\delta(g(\varphi(a))) = d_a(g\circ\varphi)\delta(a) + d_{\varphi(a)}g(\varphi^{\delta}(a)) + g^{\varphi}(\varphi(a)).$$

En comparant les deux expressions, nous obtenons que

$$(g\circ\varphi)^{\delta}(a) = d_{\varphi(a)}g(\varphi^{\delta}(a)) + g^{\varphi}(\varphi(a)).$$

Au final, nous avons qu'un vecteur u est dans $\tau_{\varphi(a)}(W)$ si et seulement si

$$\begin{aligned}g^{\delta}(\varphi(a)) + d_{\varphi(a)}g\big(d_a\varphi(u) + \varphi^{\delta}(a)\big) &= d_a(g\circ\varphi)(u) + (g\circ\varphi)^{\delta}(a) \\ &= 0,\end{aligned}$$

ce qui est toujours vrai pour $u \in \tau_a(V)$ puisque $g\circ\varphi \in I(V)$.

Les fonctions T et τ vérifient :

Proposition VI.27. *Soient $\varphi : U \to V$ et $\psi : V \to W$ des applications régulières. Alors $T(\psi\circ\varphi) = T(\psi)\circ T(\varphi)$ et $\tau(\psi\circ\varphi) = \tau(\psi)\circ\tau(\varphi)$.*

Cette proposition nous dit que T et τ sont des foncteurs de la catégorie des variétés affines munie des applications régulières dans cette même catégorie.

Démonstration. Nous avons que

$$\begin{aligned}(T(\psi)\circ T(\varphi))(u) &= T(\psi)(\varphi(a), d_a\varphi(u)) \\ &= \big(\psi(\varphi(a)), d_{\varphi(a)}\psi(d_a\varphi(u))\big) \\ &= \big((\psi\circ\varphi)(a), d_a(\psi\circ\varphi)(u)\big) \\ &= T(\psi\circ\varphi).\end{aligned}$$

Pour τ, puisque $\tau(\psi)\big(\varphi(a), d_a\varphi(u) + \varphi^{\delta}(a)\big) = \big((\psi\circ\varphi)(a), d_{\varphi(a)}\psi\big(d_a\varphi(u) + \varphi^{\delta}(a)\big) + \psi^{\delta}(\varphi(a))\big)$,

il suffit de montrer que $(\psi\circ\varphi)^{\delta}(a) = d_{\varphi(a)}\psi(\varphi^{\delta}(a)) + \psi^{\delta}(\varphi(a))$. Or par un argument similaire au précédent (en remplaçant g par ψ), nous avons ce résultat, ainsi $\tau(\psi\circ\varphi) = \tau(\psi)\circ\tau(\varphi)$. □

Rappelons-nous que $\nabla_V : V \to \tau(V) : a \mapsto (a, \delta(a))$.

Proposition VI.28. *Soit $\varphi : V \to W$ une application régulière. Alors*

$$\tau(\varphi) \circ \nabla_V = \nabla_W \circ \varphi.$$

Démonstration. Soit $a \in V$. D'un côté nous avons

$$\tau(\varphi)(a, \delta(a)) = \big(\varphi(a), d_a\varphi(\delta(a)) + \varphi^\delta(a)\big),$$

et de l'autre

$$\nabla_W(\varphi(a)) = \big(\varphi(a), \delta(\varphi(a))\big) = (\varphi(a), d_a\varphi(\delta(a)) + \varphi^\delta(a)\big).$$

□

Lemme VI.29. *Soient $V \subseteq K^n$ et $W \subseteq K^m$ des variétés algébriques, alors $T(V \times W)$ est naturellement isomorphe à $T(V) \times T(W)$. De même, nous avons que $\tau(V \times W) \cong \tau(V) \times \tau(W)$.*

Démonstration. Considérons la fonction très naturelle suivante :

$$\begin{aligned} \sigma : T(V) \times T(W) &\to T(V \times W) \\ \big((a,u),(b,v)\big) &\mapsto (a,b,u,v) \end{aligned}$$

Du premier coup d'œil, si σ est bien définie, nous pouvons nous apercevoir que c'est un morphisme de variétés injectif. Si nous montrons que l'espace tangent $T_{(a,b)}(V \times W)$ se décompose en $T_a(V) \times T_b(W)$, alors l'application sera bien définie, et surjective.

Or $(a,b) \in V \times W$ si et seulement si pour tout $f(X_1, \ldots, X_n) \in I(V)$ et pour tout $g(Y_1, \ldots, Y_m) \in I(W)$, nous avons $f(a) = 0 = g(b)$. En modifiant des indéterminées des polynômes f et g, nous pouvons voir $V \times W$ comme une variété définie sur K^{n+m} engendrés par les polynômes $\tilde{f}(X_1, \ldots, X_n, Y_1, \ldots, Y_m) = f(X_1, \ldots, X_n)$ et $\tilde{g}(X_1, \ldots, X_n, Y_1, \ldots, Y_m) = g(Y_1, \ldots, Y_m)$. Nous identifions alors V sur les n premières coordonnées et W sur les m dernières. Ainsi les zéros des différentielle de $\tilde{f}$ ou $\tilde{g}$ en un point $(a,b) \in V \times W$ se font composante par composante, et donc nous avons bien la décomposition.

L'argument se transmet très bien au cas $\tau(V \times W)$ et donc nous avons fini. □

VI.2 Prolongement de groupes algébriques

Nous allons maintenant nous intéressant au cas particulier où V est un groupe algébrique. Soit $G \subseteq K^n$ un groupe algébrique muni de la loi de groupe m, noté multiplicativement. Nous écrirons juste gh à la place de $m(g,h)$ pour $g, h \in G$. Remarquons que puisque G est un groupe algébrique, la fonction m est un morphisme de variétés entre $G \times G$ et G, ainsi nous avons la proposition suivante :

Proposition VI.30. *Les fibrés $T(G)$ et $\tau(G)$ sont des groupes algébriques munis respectivement de l'opération $T(m)$ et de l'opération $\tau(m)$.*

Démonstration. Il découle du fait que T et τ soient des foncteurs de la catégorie des variétés affines muni des applications régulières, que $T(m)$ et $\tau(m)$ sont bien des applications régulières, et idem pour la fonction inverse.

Nous avons que $T(m) : T(G \times G) \to T(G)$. Or le lemme VI.29 nous dit que $T(G \times G) \cong T(G) \times T(G)$, par conséquent l'application $T(m)$ définit bien une opération binaire sur $T(G)$.

Pour montrer l'associativité, considérons le diagramme suivant :

$$\begin{array}{ccc} (a,b,c) & \longrightarrow & (ab,c) \\ \downarrow & & \downarrow \\ (a,bc) & \longrightarrow & abc \end{array}$$

C'est un diagramme commutatif car m vérifie l'associativité. Nous pouvons voir les flèches comme des applications régulières (elles fusionnent deux composantes en appliquant m), ainsi en lui appliquant les foncteurs T et τ et en utilisant encore que $T(G^k) = T(G)^k$, nous obtenons que $T(m)$ et $\tau(m)$ sont associatifs.

Soit inv la fonction inverse de G. Comme G est un groupe algébrique, c'est un endomorphisme de variétés de G.

$$\begin{array}{ccc} g & \xrightarrow{\text{inv}} & g^{-1} \\ & \searrow^{\text{Id}} & \downarrow{\scriptstyle \text{inv}} \\ & & g \end{array}$$

En appliquant les foncteurs T et τ à ce diagramme, nous obtenons un morphisme $T(\text{inv}) : T(G) \to T(G) : (g,u) \mapsto (\text{inv}(g), d_g\text{inv}(u))$. Ce morphisme vérifie que $T(\text{inv}) \circ T(\text{inv}) = \text{Id}$. En particulier il est bijectif, ainsi il donne un et un seul inverse pour chaque élément de $T(G)$.

De plus, si $x \in T(V)$, alors $T(m)\big(x, T(\text{inv})(x)\big) = 0$ car l'application correspondante dans G est le morphisme nul. □

Discussion VI.31. Décrivons plus en détail la loi de groupe du fibré tangent de G. Nous prenons la notation multiplicative $(G, \cdot, 1_G)$. Pour $g \in G$, posons les fonctions $\lambda^g(h) = gh$, $\rho^g(h) = hg$ et $i^g(h) = g^{-1}hg$ respectivement les multiplications à gauche, à droite et la conjugaison par g. Notons pour $T(m)(g,u)(h,v) = (g,u)(h,v)$ pour des éléments (g,u) et $(h,v) \in T(G)$.

Alors la loi de groupe sur $T(G)$ est donnée par :

$$(g,u)(h,v) = (gh, d_h\lambda^g(v) + d_g\rho^h(u)).$$

En effet, soit $(g,h) \in G \times G$ et $(u,v) \in T_g(G) \times T_h(G)$. Nous avons

$$T(m)((g,h),(u,v)) = (m(g,h), d_{(g,h)}m(u,v)).$$

Notons $w = (u,v)$ la concaténation de u et v. La différentielle de m en (g,h) évaluée en (u,v) est donnée par $\sum_{i=1}^{2n} \frac{\partial m}{\partial X_i}(g,h)w_i$, que nous pouvons décomposer en $\sum_{i=1}^{n} \frac{\partial m}{\partial X_i}(g,h)w_i + \sum_{i=n+1}^{2n} \frac{\partial m}{X_i}(g,h)w_i$. Comme h est considérée comme une constante sur les n premières coordonnées et g sur les n-dernières, ceci n'est rien d'autre que :

$$\begin{aligned}\sum_{i=1}^{n} \frac{\partial \rho^h}{\partial X_i}(g)u_i + \sum_{i=n+1}^{2n} \frac{\partial \lambda^g}{\partial X_i}(h)v_i &= d_g\rho^h(u) + d_h\lambda^g(v) \\ &= d_h\lambda^g(v) + d_g\rho^h(u),\end{aligned}$$

nous en déduisons la loi de groupe de $T(G)$.

Remarque VI.32. Notons e l'inverse de G. Nous avons une action naturelle de G sur $T_e(G)$ qui envoie $(g,u) \in G \times T_e(G)$ sur $g * u = d_e i^g(u)$. En effet, nous avons que $i^g(e) = g^{-1}eg = e$, ainsi par VI.26, cette application est bien définie.

Nous avons une application $\eta : T(G) \to T_e(G)$ défini par $\eta(g,u) = d_g\lambda^{g^{-1}}u$ induite par l'action $*$. Cette fonction envoie donc un vecteur tangent à n'importe quel point de G sur un vecteur tangent en l'élément neutre.

Puisque $\lambda^{g^{-1}}(g) = e$, la différentielle $d_g\lambda^{g^{-1}}$ va de $T_g(G)$ dans $T_e(G)$. Remarquons qu'avec les notations en λ, nous avons que $\lambda^g \circ \lambda^h = \lambda^{gh}$.

$$\begin{aligned}\eta\big((g,u),(h,v)\big) &= \eta\big(gh, d_h\lambda^g(v) + d_g\rho^h(u)\big) \\ &= d_{gh}\lambda^{(gh)^{-1}}(d_h\lambda^g(v) + d_g\rho^h(u)) \\ &= d_{gh}\lambda^{(gh)^{-1}}(d_h\lambda^g(v)) + d_{gh}\lambda^{(gh)^{-1}}(d_g\rho^h(u)) \\ &= d_h(\lambda^{(gh)^{-1}} \circ \lambda^{g^1})(v) + d_g(\lambda^{(gh)^{-1}} \circ \rho^h)(u) \\ &= \eta(h,v) + d_g(\lambda^{(gh)^{-1}} \circ \rho^h)(u)\end{aligned}$$

Mais $\lambda^{(gh)^{-1}} \circ \rho^h = i^h \circ \lambda^{g^{-1}}$, d'où

$$\begin{aligned}\eta\big((g,u),(h,v)\big) &= \eta(h,v) + d_g(i^h \circ \lambda^{g^{-1}})(u) \\ &= \eta(h,v) + d_e i^h(d_g\lambda^{g^{-1}})(u) \\ &= \eta(h,v) + d_e i^h(\eta(g,u)) \\ &= \eta(h,v) + h * \eta(g,u).\end{aligned}$$

Une application vérifiant une telle propriété s'appelle un **produit croisé**.

Proposition VI.33. *Si G est commutatif, alors $\eta : T(G) \to T_e(G)$ est un morphisme de groupes et $T(G) \cong G \oplus T_e(G)$.*

Démonstration. C'est immédiat que η est un morphisme de groupes car i^h est l'identité. Ainsi sa différentielle est aussi l'identité.

L'isomorphisme entre $T(G)$ et $G \oplus T_e(G)$ est donné par $(g,u) \mapsto (g, \eta(g,u))$. Soient (g,u) et $(h,v) \in T(G)$, leur image par l'isomorphisme est donnée par :

$$\begin{aligned}(g,u)(h,v) &= \big(gh, d_h\lambda^g(v) + d_g\rho^h(u)\big) \\ &\mapsto \big(gh, \eta(gh, d_h\lambda^g(v) + d_g\rho^h(u))\big) \\ &= \big(gh, \eta(h,v) + d_e i^h(\eta(g,u))\big)\end{aligned}$$

Mais comme G est commutatif, la fonction i^h est l'identité elle-même, d'où

$$\begin{aligned}(g,u)(h,v) &= \big(gh, \eta(h,v) + \eta(g,u)\big) \\ &= (g, \eta(g,u))(h, \eta(h,v)),\end{aligned}$$

selon la loi de $G \oplus T_e(G)$ définie composante par composante, donc c'est bien un morphisme de groupes.

Pour montrer l'injectivité, considérons un vecteur (g,u) tel que son image $(g, \eta(g,u))$ soit l'élément neutre $(e,0)$ de $G \oplus T_e(G)$. Alors nous devons forcément avoir $g = e$ d'un part et $\eta(g,u) = \eta(e,u) = d_e\lambda^e(u) = 0$ de l'autre. Or la multiplication à gauche par l'élément neutre n'est rien d'autre que l'identité, et donc $u = 0$.

Montrons maintenant la surjectivité. Soit $(g,u) \in G \oplus T_e(G)$. Prenons $h = g$. Nous voulons trouver un $v \in T_g(G)$ tel que $\eta(g,v) = u$, c'est-à-dire que

$$d_g\lambda^{g^{-1}}(v) = u.$$

Prenons $v = d_e\lambda^g(u)$, c'est bien dans $T_g(G)$ car $\lambda^g(e) = g$. Alors

$$d_g\lambda^{g^{-1}}(v) = d_g\lambda^{g^{-1}}(d_e\lambda^g(u)) = d_e(\lambda^{g^{-1}} \circ \lambda^g)(u) = d_e(\mathrm{Id})(u) = u.$$

□

Nous pouvons donc, dans le cas commutatif, totalement nous cantonner à l'espace tangent au point e.

Proposition VI.34. *La section différentielle $\nabla : G \to \tau(G)$ est un morphisme de groupes.*

Démonstration. En notant $m : G \times G \to G$ la multiplication de G, nous obtenons par VI.28 que

$$\tau(m) \circ \nabla_{G\times G} = \nabla_G \circ m.$$

□

Attention, un groupe algébrique n'est pas forcément un groupe topologique.

VI.3 La dérivée logarithmique

En analyse, la dérivée logarithmique d'une fonction f dérivable ne s'annulant pas est donnée par

$$L(f) = \frac{f'}{f}.$$

Si f est à valeurs dans $\mathbb{R}^{>0}$, alors $L(f)$ coïncide avec la dérivée de $\ln \circ f$ car

$$(\ln \circ f)' = \ln'(f)f' = \frac{1}{f}f' = L(f).$$

De plus, elle vérifie pour toutes fonctions dérivables u et v, les propriétés $L(uv) = L(u) + L(v)$, $L(u/v) = L(u) - L(v)$ et $L(u^\alpha) = \alpha L(u)$.

Dans notre cadre de variétés définies sur un corps K différentiellement clos, nous supposons que G est un groupe algébrique commutatif de dimension d défini sur les corps des constantes C de K. Dans ce cas, puisque G est défini sur les constantes, les fibrés tangent et torseur coïncident, et donc ∇ est une section non triviale de $T(G)$ (en supposant ∇ non triviale...).

Définition VI.35. On définit la **dérivée logarithmique** $l : G \to T_e(G)$ par $l = \eta \circ \nabla$.

Remarque VI.36. C'est un morphisme de groupes de G dans $T_e(G)$ car ∇ et η sont des morphismes de groupes.

Exemple VI.37. Soit G le groupe additif $(K, +, 0)$. Nous le noterons $\mathbb{G}_a$. Plus généralement nous noterons $\mathbb{G}_a^n$ le groupe algébrique $(K^n, +, 0)$. Dans le cas $n = 1$, la différentielle de $\lambda^g(X) = g + X$ au point h, avec $g, h \in K$, est donnée par $\frac{\partial \lambda^g}{\partial X}(h) = 1$ et donc $d_h\lambda^g(u) = u$.

Par conséquent, nous obtenons pour tout $g \in G$ que

$$l(g) = \eta(\nabla(g)) = \eta(g, \delta(g)) = d_g\lambda^{g^{-1}}(\delta(g)) = \delta(g).$$

Exemple VI.38. Soit G le groupe multiplicatif $(K^\times, \cdot, 1)$. C'est un groupe algébrique vu dans K^2 par l'isomorphisme $K^\times \cong K[X,Y]/(XY-1)$. Nous le noterons $\mathbb{G}_m$. Ici, la différentielle de $\lambda^g(X) = gX$ au point h pour $g,h \in K$ est donnée par $\frac{\partial \lambda^g}{\partial X}(h) = g$.

Par conséquent, nous obtenons pour tout $g \in G$ que

$$l(g) = d_g \lambda^{g^{-1}}(\delta(g)) = \frac{\delta(g)}{g}.$$

Nous retrouvons ici la dérivée logarithmique habituelle.

Nous admettrons le théorème suivant qui donne une axiomatisation de DCF_0 en termes de variétés algébriques avec le prolongement $\tau(V)$. Cette axiomatisation est due à D. Pierce et A. Pillay, dans [9].

Théorème VI.39 (Axiomatisation géométrique de DCF_0, [6] Théorème 1.3)**.** *Soit K un corps différentiel algébriquement clos. Alors K est différentiellement clos si et seulement si K vérifie :*

Pour toute variété algébrique V définie sur K, si W est une sous-variété de $\tau(V)$ telle que la projection de W sur V est Zariski dense dans V, alors il existe un $a \in V$ tel que $\nabla(a) \in W$.

Dans notre cas bien précis, comme V est définie sur les constantes, $\tau(V) = T(V)$.

Proposition VI.40. *La dérivée logarithmique l est surjective.*

Démonstration. Nous avons que $l : G \to T_e(G)$. Soit $\alpha \in T_e(G)$.

Posons $W = \{(g,u) \in T(G) : d_g \lambda^{g^{-1}}(u) = \alpha\}$, c'est un ensemble K-définissable car ce ne sont que des polynômes différentiels à coefficients dans K. Nous savons que W est non vide car $(e,\alpha) \in W$. De plus, comme $W \subseteq T(G) \cong G \oplus T_e(G)$, l'ensemble W se plonge génériquement dans G, d'où par l'axiomatisation géométrique de DCF_0, il existe un $g \in G$, tel que $\nabla(g) = (g, \delta(g)) \in W$, c'est-à-dire que $d_g \lambda^{g^{-1}}(\delta(g)) = \alpha$, ou encore que $l(g) = (\eta \circ \nabla)(g) = \alpha$. Nous avons donc bien que l est surjective. □

Proposition VI.41. *Soient $s_1, \ldots, s_d : T_e(G) \to K$ des formes linéaires linéairement indépendantes sur K. Posons $\chi_i = s_i \circ l$ pour tout $1 \leqslant i \leqslant d$. Les χ_i sont des morphismes de G dans $\mathbb{G}_a$ linéairement indépendants sur K.*

Démonstration. Soient $a_1, \ldots, a_d \in K$ tels que pour tout $g \in G$, nous avons

$$\sum_{i=1}^{d} a_i \chi_i(g) = 0.$$

Cela revient à dire que $\sum_{i=1}^{d} a_i s_i(l(g)) = 0$. Comme l est surjective, et les s_i sont linéairement indépendants sur K, nous obtenons pour tout $u \in T_e(G)$ que

$$\sum_{i=1}^{d} a_i s_i(u) = 0,$$

et donc que les a_i sont tous nuls. □

Définition VI.42. Une **forme différentielle** ω sur une variété algébrique W est une application qui envoie un point $a \in W$ sur une forme linéaire du K-espace vectoriel $T_a(W)$, notée ω_a.

Exemple VI.43. Si f est une application régulière $V \to K$, alors l'application qui associe pour tout $a \in V$ la différentielle $d_a f$ est une forme différentielle.

Exemple VI.44. Soit $f : V \to W$ une application régulière entre les variétés V et W. Si ω est une forme différentielle sur W, alors l'application $f * \omega$ qui envoie $a \in V$ sur la forme linéaire l'application définie par

$$(f * \omega)_a(u) = \omega_{f(a)}\big(d_a f(u)\big),$$

pour tout $u \in T_a(V)$, est une forme linéaire sur V.

Définition VI.45. Une forme différentielle ω est appelée une **forme différentielle invariante** si pour tout $g \in G$, elle vérifie $\lambda^g * \omega = \omega$.

Soit $g \in G$. Dire que $\lambda^g * \omega = \omega$, c'est dire que pour tout $h \in G$,

$$(\lambda_g * \omega)_h = \omega_h,$$

ou encore que $\omega_{gh} \circ d_h \lambda^g = \omega_h$. Or $d_{gh}\lambda^{g^{-1}}$ est la fonction inverse de $d_h \lambda^g$, ainsi en l'appliquant sur les deux membres de l'égalité, cela revient à dire que

$$\omega_{gh} = \omega_h \circ d_{gh}\lambda^{g^{-1}},$$

pour tout g et $h \in G$, et puisque G est commutatif, cela donne aussi que

$$\omega_{gh} = \omega_h \circ d_{gh}\lambda^{g^{-1}} = \omega_g \circ d_{gh}\lambda^{h^{-1}}.$$

Proposition VI.46. *Soit ω une forme différentielle invariante sur G, posons $\chi_\omega : G \to K$ défini par $\chi_\omega(g) = \omega_g \nabla(g)$. Alors χ_ω est un caractère du groupe additif $(K, +, 0)$.*

Démonstration. Puisque $T(G) = \tau(G)$, nous savons par la proposition VI.34 et la description de la loi de groupe de $T(G)$, que

$$\nabla(gh) = d_g\lambda^h\nabla(g) + d_h\nabla^g\nabla(h).$$

Par conséquent,

$$\begin{aligned}\chi_\omega(gh) &= \omega_{gh}\nabla(gh)\\ &= \omega_{gh}\big(d_g\lambda^h\nabla(g)\big) + \omega_{gh}\big(d_h\lambda^g\nabla(h)\big),\end{aligned}$$

et par invariance de ω, en remplaçant ω_{gh}, nous obtenons que

$$\begin{aligned}\chi_\omega(gh) &= \omega_g\big(d_{gh}\lambda^{h^{-1}}(d_g\lambda^h\nabla(g))\big) + \omega_h(d_{gh}\lambda^{g^{-1}}\big(d_h\lambda^g\nabla(h))\big)\\ &= \omega_g\nabla(g) + \omega_h\nabla(h)\\ &= \chi_\omega(g) + \chi_\omega(h).\end{aligned}$$

□

Proposition VI.47. *Soient $s_1,\dots,s_d : T_e(G) \to K$ des formes linéaires linéairement indépendantes sur K et $\chi_i = s_i \circ l$ pour tout $1 \leqslant i \leqslant d$. Posons ω^i la forme différentielle définie pour $g \in G$,*

$$\omega^i_g(u) = s_i(d_g\lambda^{g^{-1}}(u)).$$

Alors ω^i est une forme différentielle invariante. De plus, pour tout $1 \leqslant i \leqslant d$, nous avons que $\chi_i = \chi_{\omega^i}$ et les $\chi_1,\dots,\chi_d$ engendrent l'espace dual de $T_e(G)$.

Démonstration. Soient $g,h \in G$. Nous avons que

$$\begin{aligned}\omega^i_{gh} &= s_i \circ d_{gh}\lambda^{(gh)^{-1}}\\ &= s_i \circ \big(d_g\lambda^{g^{-1}} \circ d_{gh}\lambda^{h^{-1}}\big)\\ &= \big(s_i \circ d_g\lambda^{g^{-1}}\big) \circ d_{gh}\lambda^{h^{-1}}\\ &= \omega^i_g \circ d_{gh}\lambda^{h^{-1}},\end{aligned}$$

ainsi ω^i est bien une forme différentielle invariante.

Montrons maintenant que $\chi_i = \chi_{\omega^i}$. Nous avons

$$\chi_i(g) = s_i(l(g)) = s_i(d_g\lambda^{g^{-1}}\nabla(g)) = \omega^i_g(\nabla(g)) = \chi_{\omega^i}(g).$$

Nous savons par la proposition VI.41 que les χ_i sont linéairement indépendants sur K, ainsi l'espace vectoriel engendré par ceux-ci est de dimension d. Or l'espace dual de $T_e(G)$ est de dimension $T_e(G)$ qui est de dimension d. □

VI.4 Noyaux de Manin de variétés abéliennes

Soit G un groupe algébrique. Précédemment, nous avons travaillé avec l'hypothèse que G était défini sur le corps des constantes de K. Ainsi, pour notre groupe G nous avions $T(G) = \tau(G)$. Par conséquent, $\nabla : G \to T(G) : g \mapsto (g, \delta(g))$ était une section non triviale du fibré tangent $T(G)$.

Pour un groupe algébrique qui n'est pas défini sur le corps des constantes, cela se complique. Nous pouvons nous en sortir dans le cas où G est une variété abélienne :

Définition VI.48. Une **variété abélienne** sur un corps K est une variété projective qui satisfait une structure de groupe algébrique.

Exemple VI.49. Une courbe elliptique est une variété abélienne.

Commençons par certaines définitions qui nous seront nécessaires pour énoncer le théorème qui nous sauvera la mise.

Définition VI.50. Soit V un groupe algébrique. On dit que V est un groupe vectoriel si $\mathbb{G}_m$ agit sur V tel qu'il existe un isomorphisme de groupes algébriques entre V et $\mathbb{G}_a^n$ une certaine puissance du groupe additif pour lequel l'action de $\mathbb{G}_m$ sur V correspond à l'action naturelle de $\mathbb{G}_m$ sur $\mathbb{G}_a^n$.

$$\begin{array}{ccc} \mathbb{G}_m \times V & \longrightarrow & V \\ \uparrow & & \uparrow \\ \mathbb{G}_m \times \mathbb{G}_a^n & \longrightarrow & \mathbb{G}_a^n \end{array}$$

Pour rappel, $\mathbb{G}_m$ est isomorphe, en tant que groupe, au groupe multiplicatif $(K^\times, \cdot, 1)$ et $\mathbb{G}_a^n$ au groupe additif $(K^n, +, 0)$.

Aussi, l'action naturelle de $\mathbb{G}_m$ sur $\mathbb{G}_a^n$ n'est rien d'autre que la multiplication par un scalaire.

Exemple VI.51.

- Le groupe additif $\mathbb{G}_a^n$ est un groupe de vectoriel (il est isomorphe à lui-même).
- Tout groupe algébrique V qui vérifie en plus d'être un espace vectoriel de dimension fini est un groupe vectoriel. En effet, en échangeant des éléments de la base nous avons un isomorphisme entre V et $\mathbb{G}_m^n$ où n est la dimension de V. De plus, il vérifie les axiomes de la multiplication scalaire.

Définition VI.52. Soient A et E deux groupes algébriques commutatifs. On dit que E est une extension de A par un groupe vectoriel s'il existe un morphisme de groupes algébriques surjectif

$$p : E \longrightarrow A$$

tel que son noyau est isomorphe à un groupe vectoriel.

En d'autres termes, si E est une extension de A par le groupe vectoriel V, nous avons la suite exacte :

$$0 \longrightarrow V \longrightarrow E \xrightarrow{p} A \longrightarrow 0.$$

Exemple VI.53.

- Si G est un groupe algébrique, la projection

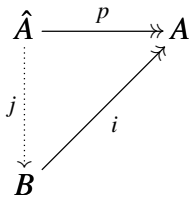
  $$p : T(G) \to G : (g,u) \mapsto g$$

  est une extension de G par un groupe vectoriel.
  En effet, le noyau de p est donné, en notant e le neutre de G, par $\{(e,u) : u \in T_e(G)\}$ qui est isomorphe à $T_e(G)$. Or nous avons vu précédemment que c'était un K-espace vectoriel, et donc un groupe vectoriel.
- La projection $\pi : \tau(G) \to G : (g,u) \mapsto g$ est aussi une extension de G par un groupe vectoriel. Rappelons-nous que nous avons une action simplement transitive $T_e(G) \times \tau_e(G) \to \tau_e(G)$ qui envoie un élément (u,v) sur $u+v$. Cette action induit pour tout $v_0 \in \tau_e(G)$ un morphisme bijectif $T_e(G) \to \tau_e(G)$ défini par $\varphi_{v_0}(u) = u + v_0$. Le morphisme φ_{v_0} a comme morphisme inverse $\varphi_{-v_0} : \tau_e(G) \to T_e(G)$ donnée par $\varphi_{-v_0}(u) = u - v_0$. C'est bien défini car pour tout couple (u, v_0) de vecteurs de $\tau_e(G)$ il existe un $w \in T_e(G)$ tel que $w + v_0 = u$, c'est-à-dire que $w = u - v_0$. Ainsi φ_{v_0} est bien un isomorphisme, d'où $\tau(G)$ est aussi un groupe vectoriel.
- Pour n'importe quel groupe algébrique G et n'importe quel groupe vectoriel V, nous pouvons construire une extension triviale de G par un groupe vectoriel en définissant $G \times V \to G : (g,v) \mapsto g$.

Prenons maintenant A une variété abélienne de dimension d (la dimension de A en tant que variété algébrique). Nous admettrons le théorème suivant :

Théorème VI.1 (Rosenlicht, [10] Proposition 11)**.** *Il existe un groupe algébrique $\hat{A}$ et un morphisme surjectif $p : \hat{A} \twoheadrightarrow A$ tels que $\hat{A}$ est une extension de A par un groupe vectoriel. De plus, s'il existe un groupe algébrique commutatif B et $i : B \twoheadrightarrow A$ formant une autre extension de A par un groupe vectoriel, alors il existe un unique morphisme de groupes algébriques $j : \hat{A} \to B$ tel que $p = i \circ j$.*

*Le groupe algébrique $\hat{A}$ est appelé l'**extension universelle de** A par un groupe vectoriel. Sa dimension est $2d$. Nous pouvons illustrer ce théorème avec le diagramme commutatif ci-dessous.*



Soit $\hat{A}$ l'extension universelle de A par un groupe vectoriel avec p. Soit $\pi : \tau(\hat{A}) \to \hat{A}$ la projection de $\tau(\hat{A})$ sur ses $2d$ premières coordonnées.

Lemme VI.54. *Il existe une section $j : \hat{A} \to \tau(\hat{A})$ de π.*

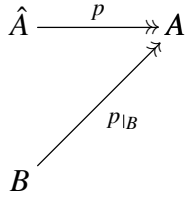
Démonstration. Nous avons que $p \circ \pi : \tau(\hat{A}) \to A$ est une extension de A par un groupe vectoriel. En effet, les morphismes p et π sont surjectifs et donc leur composée aussi. De plus, nous avons que $\mathrm{Ker}(p \circ \pi) = \{(\hat{a}, \hat{u}) \in \tau(\hat{A}) : \hat{a} \in \mathrm{Ker}(p)\} = \pi^{-1}(\mathrm{Ker}(p))$. Comme $\mathrm{Ker}(p)$ est isomorphe à un groupe vectoriel, il en est tout autant de $\pi^{-1}(\mathrm{Ker}(p))$. Par la propriété universelle de $\hat{A}$, il existe *unique* $j : \hat{A} \to \tau(\hat{A})$ tel que $p = (p \circ \pi) \circ j$.

Nous avons donc $p = p \circ (\pi \circ j)$, mais aussi $p = p \circ \mathrm{Id}$. Par unicité de j, nous avons que $\pi \circ j = \mathrm{Id}$, c'est-à-dire que j est une section de π. □

Nous garderons la notation j pour cette section de π pour ce chapitre.

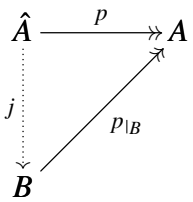
Proposition VI.55. *Soit B un sous-groupe algébrique propre de $\hat{A}$. Alors $p(B)$ est une sous-groupe algébrique propre de A.*

Démonstration. Raisonnons par l'absurde et supposons au contraire que $p(B)$ n'est pas un sous-groupe propre de A, c'est-à-dire que $p(B) = A$. Nous avons que $\mathrm{Ker} p_{|B}$ est un sous-groupe vectoriel de $\mathrm{Ker}(p)$, c'est-à-dire que :



Dire cela c'est dire que B est une extension de A par un groupe vectoriel car $\mathrm{Ker}(p_{|B})$ est un sous-groupe vectoriel de $\mathrm{Ker}(p)$ et la restriction $p_{|B}$ est un morphisme surjectif puisque nous supposons que $p(B) = A$.

Par la propriété universelle de $\hat{A}$, nous avons un morphisme de groupes algébriques $j : \hat{A} \to B$ et le diagramme commutatif :



Comme $\mathrm{Ker}(p)$ est isomorphe à $\mathbb{G}_a^m$ pour un certain naturel m, nous pouvons trouver un sous-groupe vectoriel V de $\mathrm{Ker}(p)$ tel que

$$\mathrm{Ker}(p) = V \oplus \mathrm{Ker}p_{|B}.$$

Le groupe vectoriel V est le supplémentaire de $\mathrm{Ker}(p_{|B})$. Soit $\hat{a} \in \hat{A}$. Par surjectivité de $p_{|B}$, nous pouvons trouver un $b \in B$ tel que $p(b) = p(\hat{a})$. Alors, comme p est un morphisme de groupes, nous avons aussi $p(\hat{a}) - p(b) = 0 = p(\hat{a} - b)$, d'où $\hat{a} - b \in \mathrm{Ker}(p)$. En outre, puisque V et $\mathrm{Ker}(p_{|B})$ sont des supplémentaires dans $\mathrm{Ker}(p)$ et $\hat{a} - b \in \mathrm{Ker}(p)$, pouvons trouver deux uniques éléments $v \in V$ et $\tilde{b} \in B$ tel que $\hat{a} - b = v + \tilde{b}$. Nous obtenons alors que $\hat{a} = (b + \tilde{b}) + v$, c'est-à-dire que $\hat{A} = B + V$. De plus, comme B est un sous-groupe propre de $\hat{A}$, nous devons avoir que $V \neq \varnothing$.

Nous affirmons que $\hat{A} = B \oplus V$. Pour avoir ce résultat, il suffit de montrer que $B \cap V = \{0\}$. Nous savons que $V \subseteq \mathrm{Ker}(p)$ et $\mathrm{Ker}(p_{|B}) = \mathrm{Ker}(p) \cap B$, mais aussi que $\mathrm{Ker}(p) = V \oplus \mathrm{Ker}p_{|B}$ et donc en particulier $V \cap \mathrm{Ker}(p_{|B}) = \{0\}$, d'où

$$\{0\} = \mathrm{Ker}(p_{|B}) \cap V = \mathrm{Ker}(p) \cap B \cap V = B \cap V.$$

En outre, le diagramme nous dit que $p_{|B} \circ j = p$. Or, l'image de j est dans B et donc ce n'est rien d'autre que $p \circ j = p$. Pour arriver à une contradiction, nous allons exhiber un morphisme de groupes algébriques $\tilde{j} \neq j$ tel que $p_{|B} \circ \tilde{j} = p$, et ainsi obtenir que j n'est pas unique, une contradiction avec la propriété universelle de $\hat{A}$.

Comme $\hat{A} = V \oplus B$ et V n'est pas vide, V est au moins de dimension 1 en tant que K-espace vectoriel, et par conséquent, nous pouvons définir un isomorphisme de groupes algébriques sur V (par exemple prendre une homothétie). Soit σ un automorphisme de $\hat{A}$ qui fixe B mais agit comme un automorphisme non trivial sur V, alors en prenant $\tilde{j} = j \circ \sigma \neq j$, nous obtenons que

$$p_{|B} \circ (j \circ \sigma) = p \circ \tilde{j} = p,$$

une contradiction. □

Discussion VI.56. Nous allons nous intéresser aux points de torsion de la variété abélienne $\hat{A}$, plus tard nous nous restreindrons au cas où A est une courbe elliptique.

Définissons quelques outils que nous allons utiliser. Considérons les fonctions définies par :

$$\begin{aligned}\varphi : \tau(\hat{A}) &\to \mathrm{Ker}(\pi)\\ x &\mapsto x - j(\pi(x))\end{aligned}$$

et

$$\begin{aligned}\psi : \hat{A} &\to \mathrm{Ker}(\pi)\\ x &\mapsto \varphi(\nabla(x))\end{aligned}$$

Notons que ces applications sont bien définies sur leur domaine. En effet, si on applique π à l'image de φ, alors nous obtenons pour $(\hat{a},u) \in \tau(\hat{A})$,

$$\pi((\hat{a},u) - j(\pi(\hat{a},u))) = \pi(\hat{a},u) - \pi(j(\pi(\hat{a},u))),$$

par linéarité de π. Alors puisque j est une section de π, c'est-à-dire que $\pi \circ j = \mathrm{Id}$, nous obtenons $\hat{a} - \hat{a} = 0$.

Par ailleurs, le noyau de l'application ψ est donné par :

$$\begin{aligned}\mathrm{Ker}(\psi) &= \{\hat{a} \in \hat{A} : \varphi(\hat{a}, \delta(\hat{a})) = 0_A\}\\ &= \{\hat{a} \in \hat{A} : (\hat{a}, \delta(\hat{a})) - j(\pi(\hat{a}, \delta(\hat{a})) = 0_A\}\\ &= \{\hat{a} \in \hat{A} : \nabla(\hat{a}) = j(\hat{a})\}.\end{aligned}$$

Le noyau de ψ est donc l'ensemble des éléments de $\hat{A}$ dont les images par j et par ∇ coïncident. De plus, c'est un fermé de Kolchin de $\hat{A}$ car défini par l'équation différentiel $\nabla(\overline{X}) - j(\overline{X}) = 0$. En effet, puisque j est un morphisme de variétés et ∇ est juste une application de la dérivée composante par composante, en prenant pour chaque coordonnée le polynôme différentiel $f_i(\overline{X}) = \nabla(\overline{X})_i - j(\overline{X})_i$, nous obtenons que $\mathrm{Ker}(\psi) = V_\delta(f_1, \ldots, f_{2n})$.

Proposition VI.57. *Le noyau de ψ est Zariski dense dans $\hat{A}$.*

Démonstration. En effet, soit U un ouvert de $\hat{A}$ pour sa topologie de Zariski et soit $V = j(U) \subseteq \tau(\hat{A})$. Nous avons que V se projette sur U car $\pi(V) = (\pi \circ j)(U) = U$ puisque j est une section de π. Alors par les axiomes algébriques de DCF_0, il existe un $a \in U$ tel que $\nabla(a) \in V$.

Or dire que $\nabla(a) \in V = j(U)$ c'est dire que qu'il existe un $b \in U$ tel que $j(b) = \nabla(a)$. En outre, puisque j est une section de π, nous savons que $(\pi \circ j)(b) = b$,

et donc en particulier que $j(b) \in \tau(\hat{A})$ est de la forme (b, u_b) avec $u_b \in \tau_b(\hat{A})$. Par conséquent, de $\nabla(a) = j(b)$, nous déduisons que $a = b$, et donc que $\nabla(a) = j(a)$, d'où $a \in \mathrm{Ker}(\psi)$. Ainsi nous obtenons que $\mathrm{Ker}(\psi) \cap U \neq \varnothing$, d'où $\mathrm{Ker}(\psi)$ est Zariski dense dans $\hat{A}$. □

Rappelons-nous qu'un groupe G est dit **divisible** si pour tout naturel $k > 0$, nous avons $G = kG$, i.e. pour tout $g \in G$, il existe $h \in G$ tel que $g = kh$.

Par exemple, le K-espace vectoriel $(K^n, +, 0)$ est divisible car pour un naturel $k > 0$ et $v = (v_1, \ldots, v_n)$, alors en prenant $w = (k^{-1}v_1, \ldots, k^{-1}v_n) \in K^n$, nous avons que $v = kw$.

Proposition VI.58. *Soient $\alpha \in \hat{A}$ et $a, b \in A$ tels que $p(\alpha) = a$ et $kb = a$, où $kb = b + \ldots + b$ est b sommé k fois, pour un certain naturel k. Alors il existe $\beta \in \hat{A}$ tel que $k\beta = \alpha$ et $p(\beta) = b$.*

Démonstration. Par surjectivité de p, nous avons un $\gamma \in \hat{A}$ tel que $p(\gamma) = b$. Puisque p est un morphisme de groupes, nous avons que $p(k\gamma) = kp(\gamma) = kb = a$, d'où $p(\alpha - k\gamma) = 0$, c'est-à-dire que $\alpha - k\gamma \in \mathrm{Ker}(p)$ qui est un groupe vectoriel.

Alors, puisque $\mathrm{Ker}(p) \cong \mathbb{G}_a^m$ pour un certain m, et que $(K^m, +, 0)$ est divisible, il existe un $\varepsilon \in \mathrm{Ker}(p)$ tel que $k\varepsilon = \alpha - k\gamma$. Prenons comme candidat pour β l'élément $\varepsilon + \gamma$. Nous avons en isolant α dans l'égalité que $k\varepsilon + k\gamma = k(\varepsilon + \gamma) = k\beta = \alpha$. Nous avons aussi que $p(\beta) = p(\varepsilon + \gamma) = b$. □

Nous allons maintenant continuer la théorie en considérant uniquement le cas où A est une courbe elliptique. Les résultats restent vrais dans le cadre général des variétés abéliennes (se référer à [3]) mais nécessitent des propriétés des variétés abéliennes chronophages.

Considérons donc désormais E, une courbe elliptique définie sur K.

Corollaire VI.59. *Le groupe algébrique $\hat{E}$ est divisible.*

Démonstration. Soit $\alpha \in \hat{E}$ est $k > 0$ un naturel. Avec $a = p(\alpha)$, la proposition III.28 nous dit que E est divisible, et donc par la proposition précédente, il existe un $b \in E$ tel que $a = kb$, nous avons un $\beta \in \hat{E}$ tel que $\alpha = k\beta$. □

Notons $\mathrm{Tor}(\hat{E})$ le groupe de torsion de $\hat{E}$. Une courbe elliptique définie sur un corps algébriquement clos a un groupe de torsion infini.

Corollaire VI.60. *Le groupe de torsion de $\hat{E}$ est infini.*

Démonstration. Puisque p est un morphisme de groupes, nous avons que $p(0_{\hat{E}}) = 0_E$. Or, il existe pour chaque nombre premier $p > 0$ un point de p-torsion P. Par la proposition précédente, il existe une infinité de couples distincts (p, P) tels que $pP = 0_{\hat{E}}$, c'est-à-dire un point de p-torsion de $\hat{E}$. □

Définition VI.61. Soit G un groupe algébrique. On dit que G est **connexe** s'il n'admet aucun sous-groupe normal propre d'indice fini.

Nous pouvons reformuler ça en disant que tout quotient fini de G est trivial.

Lemme VI.62. *Le noyau de ψ est connexe.*

Démonstration. Par un corollaire précédent, nous savons que $\hat{E}$ est divisible. Soit $\alpha \in \hat{E}$. Si $\psi(\alpha) = 0$, alors puisqu'il existe pour tout naturel $k > 0$ un $\beta \in \hat{E}$ tel que $\alpha = k\beta$, nous avons aussi que $0 = \psi(\alpha) = \psi(k\beta) = k\psi(\beta)$, d'où $\beta \in \mathrm{Ker}(\psi)$ est un diviseur de α. Par conséquent, le noyau de ψ est divisible.

Montrons maintenant que $\mathrm{Ker}(\psi)$ est connexe. Posons $G = \mathrm{Ker}(\psi)$. Par l'absurde, supposons que G n'est pas connexe c'est-à-dire qu'il existe $H \subseteq G$ un sous-groupe normal propre de G d'indice fini k. Alors il existe $g_1, \ldots, g_k \in G$ tels que $G = (g_1 + H) + \ldots + (g_k + H)$ est une partition de G en classes latérales de H. Comme H est un sous-groupe propre, il existe $h \in G \setminus H$. Alors, avec $h \in G$ et $k \in \mathbb{N} \setminus \{0\}$, nous avons qu'il n'existe pas de $g \in G$ tel que $h = kg$. En effet, soit $g \in G$, nous avons que $g + H \in g_i + H$ pour un certain g_i. Puisque G/H est d'ordre k, par le théorème de Lagrange nous devons avoir que $0 = k(g + H) = kg + H$, par conséquent $kg \in H$, et donc forcément $kg \neq h$, ce qui est absurde car $\mathrm{Ker}(\psi)$ est divisible. □

Proposition VI.63. *Le corps des fonctions rationnelles différentielles sur $Ker(\psi)$ se plonge dans le corps des fonctions rationnelles sur $\hat{E}$.*

Démonstration. Comme nous nous trouvons dans $\mathrm{Ker}(\psi)$, nous savons que pour tout $x \in \mathrm{Ker}(\psi)$, l'égalité $\nabla(x) = j(x)$ se vérifie, avec j algébrique. Ainsi, si $f : \mathrm{Ker}(\psi) \to K$ est une fonction rationnelle différentielle, nous pouvons trouver sur cet ensemble une fonction rationnelle *algébrique* g, telle que pour tout $x \in \mathrm{Ker}(\psi)$, nous avons $f(x) = g(x)$. Pour cela, il suffit de remplacer l'indéterminée $X_i^{(k)}$ par la bonne coordonnée de $j^k(X)$ car $j(X) = \nabla(X) = (X, \delta(X))$. Dès lors, comme la section j est définie sur tout $\hat{E}$, la fonction rationnelle g est définie sur tout $\hat{E}$. □

Il faut bien faire attention ici au fait que nous ne travaillons pas avec une topologie séparée. Ainsi nous n'avons pas forcément l'unicité d'une extension de $f : D \subseteq X \to X$ sur X même si D est dense dans X.

Corollaire VI.64. *L'ensemble $Ker(\psi)$ est un fermé de Kolchin qui est Zariski dense dans $\hat{E}$. De plus, c'est un fermé de Kolchin minimal pour la propriété de Zariski densité dans $\hat{E}$.*

Démonstration. Supposons qu'il existe V un fermé de Kolchin de $\hat{E}$ inclus strictement dans $\mathrm{Ker}(\psi)$, tel que V est Zariski dense. Alors, il existe un élément $a \in$

$\mathrm{Ker}(\psi) \setminus V$, c'est-à-dire qu'il existe un polynôme différentiel qui s'annule sur V mais pas sur a, et donc qui ne s'annule pas sur $\mathrm{Ker}(\psi)$.

Mais par la proposition précédente, l'équation différentielle est équivalente à une équation algébrique sur $\hat{E}$ qui s'annule sur V, mais pas sur a et donc $\hat{E}$, une contradiction avec V étant Zariski dense. En effet, notons $\overline{V}$ la fermeture de Zariski (au sens projectif ici). Alors nous avons vu dans le chapitre sur la topologie de Zariski projective que $\overline{V} = V_p(I(V)$. Dire que V est dense c'est dire que $\overline{V} = \hat{E}$ et donc que $\hat{E}$ s'annule sur tout polynôme qui s'annule sur V : une contradiction. □

Nous allons maintenant définir ce qu'est le noyau de Manin de la courbe elliptique E. Rappelons-nous les outils à disposition :

- $\pi : \tau(\hat{E}) \to \hat{E}$
- $p : \hat{E} \to E$, d'où $\mathrm{Ker}(p) \subseteq \hat{E}$
- $\psi : \hat{E} \to \mathrm{Ker}(\pi) \subseteq \tau(\hat{E})$

Puisque p est surjective, nous avons que $\hat{E}/\mathrm{Ker}(p) \cong E$. En notant q la projection canonique de $\hat{E}$ dans $\hat{E}/\mathrm{Ker}(p)$, nous obtenons

$$\hat{E} \xrightarrow{q} \hat{E}/\mathrm{Ker}(p) \cong E \xrightarrow{\tilde{\psi}} \mathrm{Ker}(\pi)/\psi(\mathrm{Ker}(p)),$$

où $\tilde{\psi}$ est la fonction ψ appliquée sur les classes latérales de $\mathrm{Ker}(p)$ dans $\hat{E}$.

Le quotient $\mathrm{Ker}(\pi)/\psi(\mathrm{Ker}(p))$ n'est pas forcément bien défini car $\psi(\mathrm{Ker}(p))$ n'est pas forcément un sous-groupe normal de $\mathrm{Ker}(\pi)$. Si ψ est surjectif, alors l'image de $\mathrm{Ker}(p)$ par ψ sera normal dans $\mathrm{Ker}(\pi)$ car $\mathrm{Ker}(p)$ est normal dans $\hat{E}$. En effet, soient $g,h \in \hat{E}$ avec $g \in \mathrm{Ker}(p)$ et $h \in \mathrm{Ker}(\pi) = \mathrm{Im}(\psi)$, nous avons $\psi(h) + \psi(g) - \psi(h^{-1}) = \psi(hgh^{-1})$ et donc, puisque le noyau est normal, nous obtenons que $hgh^{-1} \in \mathrm{Ker}(p)$, i.e. $\psi(hgh^{-1}) \in \psi(\mathrm{Ker}(p))$.

Pour palier le problème, il suffit de considérer la fonction ψ dont l'image est restreinte à $\mathrm{Im}(\psi)$, qui est trivialement surjective. Par conséquent, en posant

$$H = \mathrm{Im}(\psi)/\psi(\mathrm{Ker}(p)),$$

nous obtenons un morphisme induit par ψ dans le groupe quotient H,

$$\mu : E \to H.$$

C'est donc l'application induite de ψ de $\hat{E} \to \psi(\hat{E})$ aux groupes quotients $E \cong \hat{E}/\mathrm{Ker}(p) \to \psi(\hat{E})/\psi(\mathrm{Ker}(p))$. C'est donc un morphisme de groupes algébriques différentiels (dans le sens où nous utilisons le symbole de la dérivée).

Définition VI.65. On appelle le noyau de μ le **noyau de Manin de** E.

Proposition VI.66. *Le noyau de Manin de E vérifie que* $Ker(\mu) = p(Ker(\psi))$.

Démonstration. Soit $\alpha \in \mathrm{Ker}(\psi)$. Nous voulons montrer que $\mu(p(\alpha)) = 0$. Or si a est l'image de α par p, alors a s'identifie à $\alpha+\mathrm{Ker}(p)$ dans $E \cong \hat{E}/\mathrm{Ker}(p)$. Appliquer μ sur $p(\alpha)$ revient à appliquer ψ sur la classe $\alpha+\mathrm{Ker}(p)$. Or $\psi(\alpha) = 0$, d'où $\psi(\alpha) \in \mathrm{Ker}(p)$. Nous avons donc que $\mu(p(\alpha)) = 0$.

Réciproquement, soit $a \in E$ tel que $\mu(a) = 0$. Par surjectivité de p, il existe un $\alpha \in \hat{E}$ tel que $p(\alpha) = a$, c'est-à-dire que a s'identifie à $\alpha+\mathrm{Ker}(p)$ dans $E \cong \hat{E}/\mathrm{Ker}(p)$. Appliquer μ sur a revient à appliquer ψ sur la classe $\alpha+\mathrm{Ker}(p)$. Or, dire que $\mu(a) = 0$ c'est dire que $\psi(\alpha) \in \psi(\mathrm{Ker}(p))$, d'où il existe $\beta \in \mathrm{Ker}(p)$ tel que $\psi(\beta) = \psi(\alpha)$. Comme ψ est un morphisme de groupes, nous avons que $\alpha - \beta \in \mathrm{Ker}(\psi)$, avec $p(\alpha-\beta) = p(\alpha) - p(\beta) = a - 0 = a$, car $\beta \in \mathrm{Ker}(p)$. Par conséquent, nous avons bien que $a \in p(\mathrm{Ker}(\psi))$. □

Notons $E^{\#}$ la fermeture de Kolchin de $\mathrm{Tor}(E)$.

Lemme VI.67. *Nous avons l'inclusion $E^{\#} \subseteq E$*

Démonstration. Comme E est une courbe elliptique, c'est un fermé de Zariski. Or $\mathrm{Tor}(E) \subseteq E$, ainsi sa clôture pour la topologie de Kolchin doit être plus petite que celle de E. Mais la fermeture de Kolchin de E n'est rien d'autre que lui-même puisque c'est l'ensemble des zéros d'un système d'équations polynomiales différentielles d'ordre 0, d'où le résultat. □

Rappelons un résultat classique de topologie :

Lemme VI.68. *Si $f : X \to Y$ est une fonction continue, et S est un sous-ensemble de X, alors $f(\overline{S}) \subseteq \overline{f(S)}$ où $\overline{A}$ désigne l'adhérence de A pour la topologie concernée.*

Démonstration. Soit $S \subseteq X$. Nous savons que $S \subseteq f^{-1}(f(S)) \subseteq f^{-1}(\overline{f(S)})$.

Puisque $\overline{f(S)}$ est un fermé et f est continue, nous avons que $f^{-1}(\overline{f(S)})$ est un fermé (et donc égal à son adhérence). En appliquant l'opération de clôture nous obtenons que $\overline{S} \subseteq f^{-1}(\overline{f(S)})$, et en rappliquant f que $f(\overline{S}) \subseteq \overline{f(S)}$. □

Théorème VI.69. *Le noyau de Manin n'est rien d'autre que $E^{\#}$.*

Démonstration. Montrons que $\mathrm{Tor}(\hat{E}) \subseteq p^{-1}(E^{\#}) \cap \mathrm{Ker}(\psi)$. Si $\alpha \in \hat{E}$ est un point de torsion, alors il existe un naturel $k > 0$ tel que $k\alpha = 0$, d'où $p(k\alpha) = 0 = kp(\alpha)$, c'est-à-dire que $p(\alpha)$ est un point de torsion de E, et donc $\alpha \in p^{-1}(E^{\#})$. De plus, nous avons que $\psi(k\alpha) = \psi(0) = 0$.

Nous affirmons maintenant que $p^{-1}(E^{\#}) \cap \mathrm{Ker}(\psi)$ est Zariski dense dans $\hat{E}$. Soit B la clôture de Zariski de $\mathrm{Tor}(\hat{E})$. Si nous montrons que $B = \hat{E}$, alors comme $\mathrm{Tor}(\hat{E}) \subseteq p^{-1}(E^{\#}) \cap \mathrm{Ker}(\psi)$, nous aurons notre affirmation. Nous savons que $p(B)$ contient les points de torsion de E car si $ka = 0$ pour un naturel $k > 0$ et $a \in E$, alors la proposition VI.58 nous donne un $\alpha \in \hat{E}$ tel que $k\alpha = 0$ et $p(\alpha) = a$,

et donc il existe $\alpha \in B$ tel que $p(\alpha) = a$. Notons $\overline{p(B)}$ la clôture de Zariski de $p(B)$ dans E. La proposition III.33 nous dit que l'ensemble des points de torsion de E est dense dans E, et donc comme $p(B) \supseteq \mathrm{Tor}(E)$, nous avons que $\overline{p(B)} = E$. Mais par le lemme précédent, nous savons que $p(\overline{B}) \subseteq \overline{p(B)} = E$. La proposition VI.55 nous dit alors que $\overline{B} = \hat{E}$, c'est-à-dire que $B = \hat{E}$ puisque B est un fermé.

Par conséquent, l'intersection $p^{-1}(E^{\#}) \cap \mathrm{Ker}(\psi)$ est Zariski dense dans $\hat{E}$. De plus, c'est un fermé de Kolchin car $\mathrm{Ker}(\psi)$ est un fermé de Kolchin et $p^{-1}(E^{\#})$ est l'image réciproque d'un fermé de Kolchin par une application continue pour la topologie de Kolchin. En outre, cette intersection est contenue dans $\mathrm{Ker}(\psi)$. Le corollaire VI.64 nous affirme que $\mathrm{Ker}(\psi)$ est minimal parmi les fermés de Kolchin pour la propriété *être Zariski dense dans* $\hat{E}$, nous devons donc avoir que

$$p^{-1}(E^{\#}) \cap \mathrm{Ker}(\psi) = \mathrm{Ker}(\psi),$$

c'est-à-dire que $\mathrm{Ker}(\psi) \subseteq p^{-1}(E^{\#})$.

En appliquant p sur cette inclusion, nous obtenons que $p(\mathrm{Ker}(\psi)) \subseteq E^{\#}$. Or, la proposition VI.66 nous dit que $\mathrm{Ker}(\mu) = p(\mathrm{Ker}(\psi))$, nous obtenons donc

$$\mathrm{Ker}(\mu) \subseteq E^{\#}.$$

Montrons que $\mathrm{Tor}(E) \subseteq p(\mathrm{Ker}(\psi))$. Si $ka = 0$ pour un naturel $k > 0$ et $a \in E$, alors nous savons qu'il existe $\alpha \in \hat{E}$ tel que $p(\alpha) = a$ et $k\alpha = 0$ par la proposition VI.58. Ainsi $0 = \psi(0) = \psi(k\alpha) = k\psi(\alpha)$, d'où $\alpha \in \mathrm{Ker}(\psi)$ avec $p(\alpha) = a$. Ainsi, nous avons que $\mathrm{Tor}(E) \subseteq \mathrm{Ker}(\mu)$.

Or μ est un morphisme de groupes algébriques différentiels, et donc μ est défini composante par composante par un polynôme différentiel. Par conséquent $\mathrm{Ker}(\mu)$ est un fermé de E pour la topologie de Kolchin. Puisque $\mathrm{Tor}(E) \subseteq \mathrm{Ker}(\mu)$, en passant à la clôture de Kolchin nous obtenons que

$$E^{\#} \subseteq \mathrm{Ker}(\mu).$$

□

Proposition VI.70. *L'ensemble $E^{\#}$ est Zariski dense dans E. De plus, il est minimal pour cette propriété parmi les sous-groupes de E.*

Démonstration. Premièrement notons que c'est bien un sous-groupe de E par le théorème précédent qui nous dit que c'est le noyau de μ.

Supposons maintenant qu'il existe $\Sigma \subseteq E^{\#} = \mathrm{Ker}(\mu)$ un sous-groupe de E qui est Zariski dense. Posons $\Gamma = p^{-1}(\Sigma) \cap \mathrm{Ker}(\psi) \subseteq \hat{E}$. Alors,

$$p(\Gamma) = \Sigma \cap p(\mathrm{Ker}(\psi)) = \Sigma,$$

car $\Sigma \subseteq E^{\#} = \mathrm{Ker}(\mu) = p(\mathrm{Ker}(\psi))$. Comme Σ est Zariski dense dans E, en notant $\overline{\Gamma}$ l'adhérence pour la topologie de Zariski, nous obtenons que $\overline{p(\Gamma)} = \overline{\Sigma} = E$.

Mais par le dernier lemme, nous savons que $p(\overline{\Gamma}) \subseteq \overline{p(\Gamma)} = E$. En utilisant la proposition VI.55, nous obtenons que $\overline{\Gamma} = E$, c'est-à-dire que Γ est un sous-ensemble de Kolchin qui est Zariski dense dans $\hat{E}$. Par conséquent, par minimalité de $\mathrm{Ker}(\psi)$, nous devons avoir que $\Gamma = \mathrm{Ker}(\psi)$. En appliquant p sur cette égalité, nous obtenons que $\Sigma = p(\mathrm{Ker}(\psi))$, c'est-à-dire que $\Sigma = \mathrm{Ker}(\mu) = E^{\#}$. □

Chapitre VII

Aboutissement

Ce dernier chapitre se concentrera sur la présentation des constructions que Marker a annoncé dans son récent article [4].

VII.1 Les ensembles de Rosenlicht

Considérons K un corps différentiellement clos. Nous noterons C son corps des constantes. Nous allons construire des corps différentiellement clos rigides.

Pour cela, considérons le polynôme $f(X) = \frac{X}{1+X}$ à coefficients dans C.

Définition VII.1. Soit a un élément non nul de K, on définit l'**ensemble de Rosenlicht associé à** a, noté X_a le sous-ensemble de K donné par

$$X_a(K) = \{x \in K \setminus \{0\} : x' = af(x)\}.$$

Remarque VII.2 (Fondamental)**.** Si b est un élément de $X_a(K)$, alors $K(b) = K\langle b\rangle$ car $b' = a\frac{b}{1+b}$, d'où b' est un un terme de $K(b)$.

Nous admettrons le (gros) théorème suivant, dû au mathématicien éponyme, qui nous donnera des propriétés cruciales sur les ensembles de Rosenlicht. Une preuve complète de ce théorème peut être trouvée dans la section II.6 de [5].

Théorème VII.3 (Rosenlicht)**.** *Soient $k \subseteq K$ des corps différentiels tels que C_K est algébrique sur C_k. Posons $C = C_k$.*

Soient $f \in C(X)$, $c_1, \ldots, c_n \in C$ et $u_1, \ldots, u_v, v \in C(X)$ tels que

$$\frac{1}{f(X)} = \frac{\partial v}{\partial X} + \sum_{i=1}^{n} c_i \frac{\frac{\partial u_i}{\partial X}}{u_i}.$$

Soient x_1 et x_2 des éléments de K solutions de l'équation $X_i' = a_i f(X_i)$ où a_1 et a_2 sont dans k. Dans ce cas :

si x_1 et x_2 sont algébriquement dépendants sur k, alors les x_i sont algébriques sur k ou alors $a_2 v(x_1)' = a_1 v(x_2)'$.

Un exemple important est celui où $f(X) = \frac{X}{1+X}$. Nous pouvons écrire

$$\frac{1}{f(X)} = \frac{1}{X} + 1 = \frac{\frac{\partial}{\partial X}(X)}{X} + \frac{\partial}{\partial X}(X).$$

Par conséquent, en prenant $f(X) = \frac{X}{1+X}$ dans le théorème de Rosenlicht, avec $c_1 = 1$, $u_1(X) = X$ et $v(X) = X$, nous obtenons :

Corollaire VII.4. *Soient $k \subseteq K$ des corps différentiels tels que C_K est algébrique sur C_k. Soient $a, b \in K \setminus \{0\}$. Si $x \in X_a(K)$ et $y \in X_b(K)$ sont algébriquement dépendants sur k, alors x et y sont algébriques sur k ou $x = y$.*

Ce théorème est l'un des piliers de la démonstration de la non minimalité de la clôture différentielle. Faisons un pas sur le côté pour explorer cet aspect du théorème. Nous allons démontrer un théorème qui nous donne l'existence d'une infinité de corps différentiels dont la clôture différentielle n'est pas minimale.

VII.2 Non minimalité de la clôture différentielle

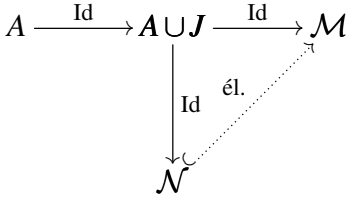
Cette section reprend les arguments de la section II.6 de [5] qui est tiré lui-même du travail de Rosenlicht dans [11].

Prouvons d'abord un résultat général sur les théories ω-stables (rappelons-nous que DCF_0 en est une) qui sera notre critère de non minimalité.

Lemme VII.5. *Soient T une théorie ω-stable dans un langage $\mathcal{L}$, un modèle $\mathcal{M}$ de T et A une sous-structure de M telle que $\mathcal{M}$ est premier sur A.*

Si $\mathcal{M}$ est minimal sur A, alors tout ensemble d'indiscernables de $\mathcal{M}$ sur A est fini.

Démonstration. Supposons que M est minimal sur A, et par l'absurde qu'il existe $I \subseteq M$ un ensemble infini d'indiscernables sur A. Soit $b \in I$ et posons $J = I \setminus \{b\}$ L'ensemble J est non vide car I est infini. Par le théorème V.52, il existe un modèle premier $\mathcal{N} \models T$ premier sur $A \cup J$. En particulier, nous avons une application élémentaire (l'identité) de $A \cup J$ dans $\mathcal{M}$.



Comme $\mathcal{N}$ est premier sur $A \cup J$, l'identité s'étend en un plongement élémentaire $\mathcal{N} \hookrightarrow \mathcal{M}$ qui fixe $A \cup J$ point par point. Mais $\mathcal{M}$ est minimal sur A, et donc $\mathcal{M} = \mathcal{N}$. Comme le théorème V.63 nous dit que $\mathcal{N}$ est atomique sur $A \cup J$, nous en déduisons que $\mathcal{M}$ l'est aussi.

Posons $p = \operatorname{tp}(b/A \cup J)$ le type de b sur $A \cup J$. Comme $\mathcal{M}$ est atomique sur $A \cup J$, il existe une $\mathcal{L}_{A\cup J}$-formule qui isole p, c'est-à-dire une $\mathcal{L}$-formule φ avec $a_1, \dots, a_n \in A$ et $c_1, \dots, c_m \in J$ telle que

$$\mathcal{M} \models \varphi(x, \overline{a}, \overline{c}) \Rightarrow p(x).$$

Soit $d \in J \setminus \{c_1, \dots, c_n\}$. Un tel élément existe car I est infini. Considérons la formule $\psi(x) \equiv x \neq d$. C'est une $\mathcal{L}_{A\cup J}$-formule qui appartient à p car $b \neq d$, donc en particulier $\varphi(x, \overline{a}, \overline{c})$ isole ψ, d'où

$$\mathcal{M} \models \forall v, \varphi(v, \overline{a}, \overline{c}) \Rightarrow v \neq d,$$

et comme b est une réalisation de son type, nous avons aussi

$$\mathcal{M} \models \varphi(b, \overline{a}, \overline{c}).$$

Les éléments b et d étant indiscernables sur A, ils le sont aussi sur $A \cup \{c_1, \dots, c_n\}$ car les c_i sont dans le même ensemble d'indiscernables que d et b. Par conséquent, puisque b est une réalisation de φ, nous devons avoir que d en est une aussi. Mais alors d doit réaliser ψ, c'est-à-dire $d \neq d$, une contradiction. □

Ce lemme nous dit alors, par contraposée, que pour montrer qu'une structure $\mathcal{M}$ n'est pas minimale, il *suffit* d'exhiber une famille infinie d'éléments indiscernables.

Nous considérons toujours le polynôme $f(X) = \frac{X}{1+X}$.

Proposition VII.6. *Soient C le corps des constantes de k et K la clôture différentielle de C. Si $x_1, \dots, x_n \in K$ sont des solutions non constantes de $X_i' = a_i f(X_i)$ avec les $a_i \in C \setminus \{0\}$, alors les $x_1, \dots, x_n$ sont algébriquement indépendants sur C.*

Démonstration. Dire que x_i n'est pas une constante et est une solution de $X_i' = a_i f(X_i)$, c'est dire que

$$x' = a_i \frac{x}{1+x} \neq 0.$$

Quitte à renuméroter les x_i, soit m un naturel minimal tel que les $x_1, \dots, x_m$ sont algébriquement dépendants sur C. Si $m = 0$, c'est terminé. Montrons que les autres scénarios sont impossibles.

Si $m = 1$, alors par hypothèse x_1 est algébrique sur C. Le lemme V.36 nous dit alors que $x_1 \in C$, une contradiction.

Sinon $m > 1$. Dans ce cas, nous avons que x_m et x_{m-1} sont algébriquement dépendants sur $C(x_1,\dots,x_{m-2})$. Par minimalité de m, ni x_m ni x_{m-1} ne sont algébriques sur $C(x_1,\dots,x_{m-2})$. En effet, car sinon nous pouvons écrire x_m ou x_{m-1} comme une combinaison des $x_1,\dots,x_{m-2}$ et obtenir une liste plus petite de solutions algébriquement dépendantes sur C. Mais alors, comme le lemme V.65 nous dit que C_K est algébrique sur C, nous pouvons utiliser le corollaire VII.4 qui nous affirme alors que $x_m = x_{m-1}$, une contradiction. □

Un dernier lemme avant d'obtenir un exemple de clôture différentielle non minimale...

Lemme VII.7. *Soit K un corps différentiellement clos et $p(X) \in K\{X\}$ un polynôme différentielle d'ordre > 0. Alors il existe une infinité de solutions dans K de l'équation différentielle $p(X) = 0$.*

Démonstration. Supposons par l'absurde que K n'abrite qu'un nombre fini de solutions de $p(X) = 0$, disons $s_1,\dots,s_n$. Alors en considérant les polynômes $f(x) = p(x)$ d'ordre > 0 et $g(x) = (x-s_1)\dots(x-s_n)$ d'ordre 0, comme K est différentiellement clos, il existe une racine de f qui n'annule pas g, c'est-à-dire une solution de p qui est différente des s_i, une contradiction. □

Remarque VII.8. Pour une équation différentielle de la forme $p(x) = x'$, avec p d'ordre 0, il n'existe qu'un nombre fini de solutions constantes : le degré de p. En effet, si a est une solution constante de cette équation alors il doit satisfaire $p(a) = 0$. Par conséquent, il existe une infinité de solutions non constantes.

Théorème VII.9. *Soit C le corps des constantes de k et K la clôture différentielle de C. Alors K n'est pas minimale sur C.*

Démonstration. Comme K est différentiellement clos, par le lemme précédent et quitte à multiplier par le dénominateur, il existe dans K une infinité de solution de $x' = f(x)$ qui est d'ordre 1. Soient $x_1, x_2, \dots \in K$ une infinité de solutions non constantes. Nous allons montrer que ces éléments forment un ensemble infini d'indiscernables de K sur C. Soient $x_{j_1},\dots,x_{j_m}$ une sous-famille quelconque finie des x_i. Par la proposition VII.6, les $x_{j_1},\dots,x_{j_m}$ sont algébriquement indépendants sur C. De plus, comme $x'_{j_i} = f(x_{j_i})$ et $f(X) \in C(X)$, le corps différentiel engendré par les x_{j_i} dans C et le corps engendré par les x_{j_i} dans C coïncident, c'est-à-dire que

$$C\langle x_{j_1},\dots,x_{j_m}\rangle = C(x_{j_1},\dots,x_{j_m}).$$

En effet, nous pouvons écrire la dérivée de x comme une expression algébrique dans C. Alors, le type de $x_{j_1},\dots,x_{j_m}$ est déterminé algébriquement. Comme ils

sont algébriquement indépendant sur C, le type de $x_{j_1},\dots,x_{j_m}$ est donné par l'ensemble des $\mathcal{L}_C$-formules du type

$$\bigwedge_{i=1}^{m}(v_i' = f(v_i) \wedge v_i' \neq 0) \wedge p(v_1,\dots,v_m) \neq 0,$$

où p est un polynôme non nul dans $C[X]$. Mais les $x_1, x_2, \dots$ sont algébriquement indépendants sur C, et donc forcément pour n'importe quel polynôme p non nul, nous aurons $p(x_{k_1},\dots,x_{k_m}) \neq 0$. Ainsi n'importe quelle sous-famille des x_i satisfait ce type (complet). Par conséquent, les $x_1, x_2, \dots$ forment un ensemble infini d'indiscernables de K sur C. Par notre critère VII.5, nous en déduisons que K n'est pas minimal sur C. □

Nous avons en particulier pour $\mathbb{Q}$ sur lequel toute dérivée est triviale :

Corollaire VII.10. *La clôture différentielle de $\mathbb{Q}$ n'est pas minimale.*

Remarque VII.11. Soit K_0 est la clôture différentielle de $\mathbb{Q}$. Elle se plonge dans un sous-corps propre différentiellement clos $K_1 \subseteq K_0$. Mais K_1 est à son tour une clôture différentielle de $\mathbb{Q}$, qui n'est pas minimale, et donc nous pouvons trouver $K_2 \subseteq K_1$, un sous corps différentiellement clos propre de K_1 et ainsi de suite.

Nous construisons une suite strictement décroissante de clôtures différentielles de $\mathbb{Q}$:

$$K_0 \supseteq K_1 \supseteq K_2 \supseteq \dots$$

VII.3 Orthogonalité

Revenons à nos moutons. Nous aurons besoin de quelques propriétés supplémentaires sur les ensembles de Rosenlicht. Pour ce qui est de cette section, nous tirons nos résultats de la section II.7 de [5]. Les résultats y sont énoncés en termes de types, mais nous ne nous engagerons pas dans cette terminologie ici.

Soient X et Y des ensembles fortement minimaux dans la théorie DCF_0.

Définition VII.12. On dit que X et Y sont **orthogonaux**, si pour tout corps différentiel k tels que X et Y sont définissables sur k, et si x est un point générique de X sur k et y un point générique de Y sur k, alors x et y sont algébriquement indépendants sur k. Nous écrirons alors $X \perp Y$.

Dire que x et y sont algébriquement dépendants sur k, c'est le dire au sens de la théorie des modèles : $y \in acl(x/k)$ et $x \in acl(y/k)$. Cela revient à dire que $acl(k\langle x\rangle) = acl(k\langle y\rangle)$ dans le cadre de DCF_0 car ce sont exactement les termes du langage $\mathcal{L}_{k\cup\{x\}}$.

Moralement, dire que $X \perp Y$, c'est dire qu'ils sont *"indépendants"*, alors que $X \not\perp Y$, c'est dire qu'ils sont *"liés"*.

Théorème VII.13 (Rosenlicht, [4])**.** *Soit K un corps différentiel et soient $a, b \in K^\times$.*

(a) L'ensemble X_a est fortement minimal.

(b) Si $x \in X_a(K)$, alors $C(K) = C(K\langle x\rangle)$.

(c) Si $a \neq b$, alors $X_a \perp X_b$.

Nous donnons une démonstration du point (c).

Démonstration du point (c). Soient x et y des points génériques (distincts) respectivement de X_a et de X_b sur un corps différentiel K. Supposons par l'absurde qu'ils sont algébriquement dépendants sur K (au sens modèle théorique), c'est-à-dire que $acl(K\langle x\rangle) = acl(K\langle y\rangle)$.

Comme DCF_0 a l'élimination des quantificateurs et qu'un polynôme d'ordre > 0 a une infinité de solutions, la fonction acl envoie un ensemble A sur la clôture algébrique du corps différentiel engendré par A. En outre, par la remarque fondamental sur les ensembles de Rosenlicht, nous avons que si $x \in X_a$, alors $K(x) = K\langle x\rangle$. Par conséquent x et y sont en fait algébriquement dépendants au sens usuel des corps algébriques.

Mais le corollaire VII.4 nous dit que x et y sont tous les deux algébriques sur K, donc ils ne peuvent pas être générique, une contradiction. □

Nous admettrons le résultat suivant qui nous permettra de s'assurer de ne pas augmenter le nombre de réalisations d'un ensemble de Rosenlicht d'une étape à l'autre de notre construction.

Proposition VII.14 ([5], Lemme 7.2)**.** *Supposons que $K \models DCF_0$. Soient X et Y des ensembles orthogonaux et $a \in X$. Posons F la clôture différentielle de $K\langle a\rangle$. Alors :*

$$Y(F \setminus K) = \varnothing.$$

Cette proposition nous dit qu'en fait, si X et Y sont orthogonaux, ajouter un élément de X à K et prendre la clôture différentielle du corps ainsi engendré n'ajoute aucun point à Y. Ce résultat sera fondamental dans nos constructions. Nous pouvons reformuler l'assertion de cette proposition comme :

$$Y(F) = Y(K).$$

Dans notre cas particulier, en combinant le théorème VII.13 et cette dernière proposition, nous obtenons que :

Corollaire VII.15. *Soit $K \models DCF_0$. Soient $a, b \in K^\times$ deux éléments distincts. Soit $x \in X_a(K)$. Soit F la clôture différentielle de $K\langle x\rangle$. Alors :*

$$X_b(K) = X_b(F).$$

VII.4 Une première construction

Nous avons vu dans la section IV.5 ce qu'étaient les cardinaux inaccessibles. Pour construire notre premier type de corps différentiellement clos rigide, nous allons avoir besoin d'un cardinal inaccessible. Rappelons qu'un tel cardinal κ vérifie $\kappa = \aleph_\kappa$. En particulier, c'est un ordinal limite.

Théorème VII.16. *Il existe pour tout cardinal inaccessible κ un corps différentiellement clos rigide de cardinal κ.*

Démonstration. Nous allons construire un corps différentiellement clos K de cardinal κ tel que pour tous $a, b \in K$ non nuls, nous avons $|X_a(K)| \neq |X_b(K)|$. Si nous arrivons à construire un tel corps K, alors il n'y aura pas d'automorphisme envoyant $a \mapsto b$.

En effet, soit $\varphi(x,y) \equiv x' = yf(x)$. Alors $c \in X_a(K)$ si et seulement si $K \models \varphi(x,a)$. Ainsi, si $\sigma : K \to K$ est un isomorphisme de K qui envoie a sur b, alors $c \in X_a(K)$, c'est-à-dire que $K \models \varphi(c,a)$, si et seulement si $K \models \varphi(\sigma(c), \sigma(a))$, ce qui revient à dire que $K \models \varphi(\sigma(c), b)$, ou encore que $\sigma(c) \in X_b(K)$. Pour une question de cardinal, nous devons avoir que $a = b$. En outre, comme $0 \mapsto 0$, il n'existera pas d'automorphisme non trivial de K.

Prenons $K_0 = \mathbb{Q}^{\mathrm{dcl}}$ et $a_0 \in K_0$. Nous allons construire une chaîne de corps différentiellement clos

$$K_0 \subseteq K_1 \subseteq \ldots \subseteq K_\alpha \subseteq \ldots$$

avec $|K_\alpha| = \aleph_\alpha$ pour $\alpha < \kappa$. En parallèle, nous construisons $a_0, a_1, \ldots, a_\alpha, \ldots$ une énumération injective du groupe multiplicatif $K^\times$ où

$$K = \bigcup_{\alpha < \kappa} K_\alpha.$$

Pour passer de K_0 à K_1, nous ajoutons $\aleph_1$ nouveaux éléments de X_{a_0} algébriquement indépendants sur K_0. Pourquoi pouvons-nous en trouver autant ?

Lemme VII.17. *Soit k un corps différentiel. Soient α un cardinal infini quelconque et $f(X)$ un polynôme d'ordre > 0 dans $k\{X\}$. Alors il existe un modèle $\mathbb{U}$ de DCF_0 qui admet α racines de $f(X)$, algébriquement indépendantes sur k.*

Démonstration. Considérons le langage augmenté $\mathcal{L}$, le langage $\{+,\cdot,0,1\}$ auquel nous avons ajouté un nombre α de constantes c_i. Considérons la $\mathcal{L}$-théorie T composée des énoncés suivants :

(1) DCF_0 ;

(2) pour tout $i \in \alpha$, l'énoncé $f(c_i) = 0$;

(3) pour tout $i, j \in \alpha$ des cardinaux différents, l'énoncé $(c_i - c_j) \neq 0$;

(4) pour tout naturel $k > 0$, pour tout polynôme $q \in k[X_1, \ldots, X_k]$, pour toutes constantes $c_1, \ldots, c_k$, l'énoncé $q(c_1, \ldots, c_k) \neq 0$.

Montrons que cette théorie est finiment consistante. Soit $\Sigma \subseteq T$ un sous-ensemble fini d'axiomes de T. Soit K la clôture différentielle de k. Montrons que K peut être vu comme un modèle de Σ. Le corps K satisfait forcément DCF_0. S'il existe des axiomes du type (2), alors comme K est différentiellement clos, nous pouvons trouver une solution x de $f(X) = 0$, qui est d'ordre 1, telle que

$$q_1(x, c_{j_1}, \ldots, c_{j_n}) \ldots q_k(x, c_{k_1}, \ldots, c_{k_r})(x - c_{p_1}) \ldots (x - c_{p_s}) \neq 0,$$

où les q_i sont les polynômes qui apparaissent dans les axiomes de la forme (4) et les c_{p_i} dans ceux de la forme (3). Alors, nous posons $c = x$ pour un symbole de constante c non interprété. Nous répétons l'argument un nombre fini de fois (le nombre d'axiomes du type (2) dans Σ).

Ainsi, par compacité, nous avons notre modèle $\mathbb{U}$. □

Par conséquent, nous pouvons prendre $\aleph_1$ nouveaux éléments de $X_{a_0}(\mathbb{U})$ algébriquement indépendants sur K_0. Nous posons alors K_1, la clôture différentielle du corps différentiel engendré par ces nouveaux éléments dans K_0 et posons $a_1 \in K_1$ de sorte que $a_0 \neq a_1$.

De façon plus générale, si α est un …

- ordinal successeur, étant donné K_α, nous construisons $K_{\alpha+1}$, la clôture différentielle du corps différentiel engendré par $\aleph_{\alpha+1}$ éléments de X_{a_α} algébriquement indépendants sur K_α et posons $a_{\alpha+1} \in K_{a_{\alpha+1}}$ de sorte que $a_{\alpha+1}$ soit distincts des a_β choisi jusqu'à cette étape ;
- ordinal limite, nous prenons juste

$$K_\alpha = \bigcup_{\beta<\alpha} K_\beta.$$

Nous nous arrêtons quand $\alpha = \aleph_\kappa$.

Cette construction nous donne alors un corps différentiellement clos K de cardinal $\aleph_\kappa$. En effet, par récurrence transfinie, montrons que pour tout $\alpha < \kappa$, nous avons $|K_\alpha| = \aleph_\alpha$. En outre, nous avons une injection $i : \kappa \hookrightarrow K^\times : \alpha \mapsto a_\alpha$.

Pour $\alpha = 0$, c'est bon car $\mathbb{Q}$ est de cardinal $\aleph_0$ et donc sa clôture différentielle aussi, c'est le résultat V.54. Pour $\alpha + 1$, même raisonnement : nous regardons la clôture différentielle du corps engendré par K_α et $\aleph_{\alpha+1}$ éléments, qui est donc de cardinal $\aleph_{\alpha+1}$. Pour β un ordinal limite, la réunion de tous les K_β pour $\beta < \alpha$ est de cardinal $\sup\{\beta : \beta < \alpha\} = \alpha$.

Avons-nous que K satisfait, comme nous le voulons, que pour tous $a \neq b \in K^\times$, les ensembles $X_a(K)$ et $X_b(K)$ sont de cardinaux différents ?

Cela se déduit du fait que les X_a et X_b sont orthogonaux pour $a \neq b$. En fait, à chaque étape, nous n'ajoutons aucune nouvelle solution de l'équation $X' = a_\alpha f(X)$, c'est-à-dire d'éléments de X_{a_α}. Soit $\alpha < \kappa$, montrons par récurrence transfinie sur β que pour tout $\alpha < \beta \leqslant \kappa$, nous avons $|X_{a_\alpha}(K_\beta)| = \aleph_{\alpha+1}$.

- Pour $\beta = \alpha + 1$, comme le corps $K_{\alpha+1}$ est de cardinal $\aleph_{\alpha+1}$ nous devons forcément avoir que $|X_{a_\alpha}(K_{\alpha+1})| = \aleph_{\alpha+1}$.
- Pour un ordinal successeur $\beta + 1$, le corps $K_{\beta+1}$ est construit en ajoutant $\aleph_{\beta+1}$ éléments de $X_{a_\beta}(\mathbb{U})$ algébriquement indépendants sur K_β. Mais pour $\beta > \alpha$, nous avons que $X_{a_\alpha}(K_\beta) \perp X_{a_\beta}(K_\beta)$ car $a_\alpha \neq a_\beta$. Par conséquent, le résultat VII.15 nous dit que $X_{a_\alpha}(K_\beta) = X_{a_\alpha}(K_{\beta+1})$.
- Pour β un ordinal limite, c'est immédiat car pour chacun des $\alpha < \gamma < \beta$, nous avons que $|X_{a_\alpha}(K_\gamma)| = \aleph_{\alpha+1}$.

Ainsi K forme bien un corps différentiellement clos avec la propriété voulue : il n'existe donc pas d'automorphisme non trivial de K, i.e. K est rigide. □

Remarque VII.18. Soit B_α l'ensemble de toutes les réalisations indépendantes de X_{a_α} ajouté à l'étape α. Alors bien que par construction K soit la clôture différentielle de $k = \mathbb{Q}\langle B_\alpha : \alpha < \kappa\rangle$, cela ne contredit pas la proposition V.55. En effet, montrons que nous avons $k = K$.

Si $a \in K^\times$, alors il existe un β tel que $a = a_\beta$ grâce à notre énumération. Soit $b \in X_a$, alors comme $b = a\frac{b}{1+b}$, nous avons que $a = \frac{b'(1+b)}{b} \in \mathbb{Q}\langle b\rangle \subseteq k$.

VII.5 Les noyaux de Manin

Soient k un corps différentiel et $a \in k$. Nous noterons E_a la courbe elliptique définie sur k par l'équation de Weierstrass

$$E_a \equiv Y^2 = X(X-1)(X-a).$$

Posons $E_a^\#$ la clôture dans la topologie de Kolchin de $\mathrm{Tor}(E_a)$. Souvenons-nous que $E_a^\#$ n'est rien d'autre que le noyau de l'application μ, et qu'ainsi $E_a^\#$ est un sous-groupe définissable de E_a Zariski dense minimal dans E_a.

Nous utilisons les notions des prégéométries de la section IV.3.

Théorème VII.19 (Hrushovski-Sokolovic, [4])**.**

(a) Si a n'est pas une constante, alors $E_a^\#$ est un ensemble fortement minimal localement modulaire non trivial.

(b) Les ensembles $E_a^\#$ et $E_b^\#$ sont non orthogonaux si et seulement si E_a et E_b sont isogéniques. En particulier, si a et b sont algébriquement indépendants sur $\mathbb{Q}$, alors $E_a^\#$ et $E_d^\#$ sont orthogonaux.

En particulier, les noyaux de Manin sont orthogonaux au corps des constantes.

En plus de ça, les noyaux de Manin vérifie une propriété plutôt forte :

Théorème VII.20 (Buium, [1])**.** *Soit $E^\#$ un noyau de Manin. Soient k un corps différentiel et Y un ensemble fortement minimal. Si pour tout $x \in Y$, le degré de transcendance de $k\langle x\rangle$ sur k est < 2, alors $Y \perp E^\#$.*

Corollaire VII.21. *Les ensembles de Rosenlicht et les noyaux de Manin sont orthogonaux.*

Démonstration. Si $x \in X_a \setminus k$, alors par la remarque fondamentale, nous obtenons que $k\langle x\rangle = k(x)$. Or, ce corps est de degré de transcendance au plus 1 sur k. □

Pour construire nos corps différentiellement clos rigides dénombrables, nous introduisons certaines notions. Rappelons-nous de la notion de solution générique, vu en V.27. Comme $E_b^\#$ est un fermé de Kolchin, c'est l'ensemble des zéros d'un système d'équations différentielles polynomiales.

Nous dirons que $x \in L \supseteq k$ est une réalisation du **type générique de $E_b^\#$ sur k**, si x est un point générique de $E_b^\#(k)$. Un tel élément est forcément transcendant.

Définition VII.22. Soit $b \notin C_k$. On pose $\dim E_b^\#(k)$ le nombre de réalisations indépendantes de k du type générique de $E_b^\#$ sur $\mathbb{Q}\langle b\rangle$.

Notons que cette dimension est majorée par le degré de transcendance de k sur $\mathbb{Q}\langle b\rangle$.

Remarque VII.23. Le corollaire V.29 nous dit que si x est algébrique sur $\mathbb{Q}\langle b\rangle$, alors x n'est pas un point générique de $E_b^\#(\mathbb{Q}\langle b\rangle)$.

Soit L un corps différentiellement clos. Pour chaque $a \in L^\times$, nous lui associons le nombre $n_a = \max_{d \in X_a(L)} \dim E_d^\#(L)$.

Nous allons construire K un corps différentiellement clos (dénombrable) tel que pour chaque $a, b \in K^\times$, si $a \neq b$ alors $n_a \neq n_b$. Si nous arrivons à construire un tel K, alors il n'y aura pas d'automorphisme qui envoie $a \mapsto b$. Mais avant cela, nous allons avoir besoin de quelques résultats pour s'assurer que notre construction se passe sans accroc. Pour un corps différentiel k, nous noterons k^{dcl} sa clôture différentielle et k^{acl} sa clôture algébrique (que ce soit au sens modèle théorique ou algébrique, elles coïncident ici).

Les b que nous considérerons seront dans des ensembles de Rosenlicht, ainsi nous aurons que $\mathbb{Q}\langle b\rangle = \mathbb{Q}(b)$.

Lemme VII.24. *Si b n'est pas une constante, alors $\dim E_b^\#(\mathbb{Q}\langle b\rangle^{dcl}) = 0$.*

Démonstration. Soit $x \in E_b^{\#}(\mathbb{Q}\langle b\rangle^{\mathrm{dcl}})$. Pour un naturel $m > 0$, un point de m-torsion n'est rien d'autre qu'un élément du noyau de l'isogénie $[m] : E(\mathbb{Q}(b)) \to E(\mathbb{Q}(b))$. Or la proposition III.30 nous dit que ce groupe est fini. Tous les points de torsion de E_b sont donc des éléments algébriques sur $\mathbb{Q}(b)$. Ainsi, nous pouvons supposer sans perdre de généralité que x n'est pas un point de torsion car un élément algébrique ne peut pas être générique.

Puisque la clôture différentielle $\mathbb{Q}\langle b\rangle^{\mathrm{dcl}}$ est atomique sur $\mathbb{Q}\langle b\rangle$, il existe une formule ψ à paramètre dans $\mathbb{Q}\langle b\rangle$ qui isole le type de x sur $\mathbb{Q}\langle b\rangle$. Aucun point de torsion ne peut satisfaire ψ car x satisfait les formules *ne pas être un point de k-torsion* pour tout naturel $k > 0$. De plus, comme b est non constant, le noyau de Manin de E_b est fortement minimal. Par conséquent, comme les points de torsion forment un ensemble infini dans $\mathbb{Q}\langle b\rangle^{\mathrm{dcl}}$, le nombre de réalisations de ψ est fini et donc x est algébrique sur $\mathbb{Q}(b)$. Nous en déduisons que x ne satisfait pas le type générique de $E_b^{\#}$ sur $\mathbb{Q}\langle b\rangle$. □

Lemme VII.25. *Supposons que K est différentiellement clos. Soient $b, d \in K$ et E_b et E_d des courbes elliptiques isogéniques. Alors dim $E_b^{\#}(K)$ = dim $E_d^{\#}(K)$.*

Démonstration. Soit $f : E_d \to E_b$ une isogénie entre E_d et E_b. Par le théorème de Hrushovski-Sokolovic, les éléments d et b sont algébriquement dépendants sur $\mathbb{Q}$, d'où $\mathbb{Q}(d)^{\mathrm{alg}} = \mathbb{Q}(b)^{\mathrm{alg}}$, ainsi f est définissable sur $\mathbb{Q}(b)^{\mathrm{alg}}$.

En particulier f est un morphisme de courbes et donc surjective par le théorème III.26. De plus, comme f est compatible avec la loi de groupe et est surjective, sa restriction au groupe de torsion de E_d est à image dans le groupe de torsion de E_b car un point de torsion de E_d est envoyé sur un point de torsion de E_b. De plus, si y est un point de k-torsion de E_b, alors par surjectivité de f il existe un $x \in E_d$ tel que $f(x) = y$. Alors $f(kx) = kf(x) = ky = 0$ et donc $kx \in \mathrm{Ker}(f)$. Mais f est une isogénie, donc son noyau est d'ordre fini, disons m, d'où $mkx = 0$. Ainsi la restriction de f aux groupes des points de torsion est toujours surjective.En outre, comme $E_d^{\#}$ et $E_b^{\#}$ sont les clôtures de Kolchin respectives de $\mathrm{Tor}(E_d)$ et $\mathrm{Tor}(E_b)$, nous pouvons *dé*-restreindre f sur ces ensembles et obtenir $f : E_d^{\#} \to E_b^{\#}$ car $f(A) \subseteq f(\overline{A}) \subseteq \overline{f(A)}$.

Nous affirmons que dim $E_d^{\#}(K) \leqslant$ dim $E_b^{\#}(K)$. Montrons que si x et y sont deux réalisations indépendantes du type générique de $E_d^{\#}(K)$ sur $\mathbb{Q}\langle b\rangle$, alors $f(x)$ et $f(y)$ sont envoyés sur deux réalisations indépendantes sur $\mathbb{Q}\langle b\rangle$ du type générique de $E_b^{\#}(K)$. Si elles ne sont pas indépendantes sur $\mathbb{Q}\langle b\rangle$, il existe un polynôme p à coefficients dans $\mathbb{Q}\langle b\rangle$ tel que $p(f(x), f(y)) = 0$. Mais f est une application rationnelle définie sur $\mathbb{Q}(b)^{\mathrm{alg}}$, d'où a et b sont algébriquement dépendants sur $\mathbb{Q}(b)^{\mathrm{alg}}$.

Comme $E_d^{\#}(K)$ et $E_b^{\#}(K)$ sont isogéniques, il existe une isogénie dans l'autre sens (voir par exemple le théorème III.6.1 de [12]), à savoir $g : E_b \to E_d$. En répétant le même argument, nous obtenons l'autre inégalité. □

VII.6 Une construction de modèles rigides dénombrables

Nous allons maintenant construire un corps différentiellement clos rigide, dénombrable.

Théorème VII.26. *Il existe un corps différentiellement clos rigide de cardinalité dénombrable.*

Démonstration. Prenons $K_0 = \mathbb{Q}^{\mathrm{dcl}}$, c'est un corps différentiellement clos dénombrable. Nous allons construire

$$K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n \subseteq \ldots,$$

une chaîne croissante de corps différentiellement clos dénombrables et une énumération injective $a_0, a_1, \ldots$ de $K^\times = \cup_{n\in\mathbb{N}} K_n^\times$ qui vérifient :

(1) $C(K_i) = C(K_0)$;

(2) $X_{a_i}(K) = X_{a_i}(K_{i+1})$;

(3) si $b \in X_{a_i}(K)$, alors $E_b^\#(K) = E_b^\#(K_{i+1})$;

(4) $n_{i+1} = \max_{d\in X_{a_i}(K)} \dim E_b^\#(K) := n_{a_i}$.

Nous avons $K_0 = \mathbb{Q}^{\mathrm{dcl}}$. Pour passer à l'étape suivante, nous prenons un $a_0 \in K_0^\times$. Posons b_0 un nouvel élément de X_{a_0} générique sur K_0, c'est-à-dire que b_0 est un point générique de $X_{a_0}(K_0)$. Par convention, nous avons $n_0 = 0$. Prenons x_0 une (n_0+1) réalisation du type générique de $E_{b_0}^\#$ sur $K_0\langle b_0\rangle = K_0(b_0)$ (car $b_0 \in X_{a_0}$). Nous définissons alors $K_1 = K_0\langle b_0, x_0\rangle^{\mathrm{dcl}}$.

Plus généralement, à l'étape s, nous posons b_s un élément générique de X_{a_s} sur K_s. Nous choisissons alors, $n_{s-1}+1$ réalisations indépendantes, que l'on note $\bar{x}_s$, du type générique de $E_{b_s}^\#$ sur $K_s\langle b_s\rangle = K_s(b_s)$ et posons $K_{s+1} = K_s\langle \bar{x}_s, b_s\rangle^{\mathrm{dcl}}$.

Nous pouvons voir, comme la clôture différentielle est de même cardinalité que le corps de base, que le corps ainsi construit est dénombrable.

Vérifions les différentes propriétés mentionnées plus tôt :

(1) À chaque étape, nous ajoutons un élément b_s de X_{a_s} (dans une extension) et d'éléments de $E_{b_s}^\#$ où $b_s \in X_{a_s}$. Le théorème VII.14 et le fait que les noyaux de Manin soient orthogonaux au corps des constantes nous dit que

$$C(K_{s+1}) = C(K_s\langle b, x_1, \ldots, x_{n_s}\rangle^{\mathrm{dcl}}) = C(K_s).$$

(2) Idem, par les résultats VII.21 et VII.15, nous ne faisons ajouter qu'à chaque étape des éléments d'ensembles orthogonaux à X_{a_s}. Nous en déduisons l'assertion par la proposition VII.14.

(3) Encore pareil, le théorème de Hrushovski–Sokolovic nous dit qu'à chaque étape, nous n'ajoutons que des éléments d'un ensemble orthogonal à $E_b^{\#}(K)$, nous concluons par le résultat VII.14.

Pour montrer (4), nous voulons avoir qu'à l'étape s l'existence un n_s tel que

$$n_s = \max_{d \in X_{a_s}} \dim E_d^{\#}(K).$$

Par construction, nous avons que si n_s existe, alors $n_s > n_{s-1}$ (nous ajoutons toujours au moins un élément en plus).

Pour terminer sa construction, D. Marker utilise le résultat suivant qui découle des lemmes VII.25 et VII.24.

Lemme VII.27 ([4], Lemme 3.4)**.** *Si $d \in K \setminus C$, alors $\dim E_d^{\#}(K) = n_i$ pour un certain i.*

Pour une preuve complète de la construction nous pourrons consulter [4].

Alors, si éléments a_i et a_j sont deux éléments distincts de $K^\times$, par injectivité de l'énumération, nous avons que $i \neq j$. Par conséquent $n_{a_i} \neq n_{a_j}$. Or, nous avons que $0 = n_0 < n_1 < \ldots$, par conséquent un automorphisme ne peut pas envoyer a_i sur a_j.

□

En fait, Marker a montré qu'il existe $2^{\aleph_0}$ corps différentiellement clos rigides dénombrables non isomorphes, chacun n'étant pas la clôture différentielle d'un sous-corps propre. Sa construction repose sur celle que nous venons réaliser.

Considérations ultérieures

Dans notre première construction de corps différentiellement clos rigides, nous nous sommes servis d'un cardinal inaccessible, quant à la seconde, nous nous sommes efforcés de rester dans un corps de cardinal dénombrable. Nous pouvons nous interroger sur l'existence de corps différentiellement clos rigides de cardinal $> \aleph_0$, par exemple, $\aleph_1$.

Bibliographie

[1] A. Buium, Differential Algebra and Diophantine Geometry, Actualité Mathématiques, Hermann, Paris (1994).

[2] D. Marker, Model Theory : An Introduction, Springer (2002).

[3] D. Marker, Manin Kernels, Connections between Model Theory and Algebraic and Analytic Geometry, quaderni di matematica, Vol. 6 (2000) : 1-21.

[4] D. Marker, Rigid Differentially Closed Fields, arXiv (2022).

[5] D. Marker, M. Messmer & A. Pillay, Model Theory of Fields (1995).

[6] D. Marker, Model Theory of Differential Fields, Model Theory, Algebra, and Geometry, MSRI Publications, Volume 39 (2000).

[7] D. Perrin, Géométrie algébrique : Une introduction, InterEditions-CNRS (1995).

[8] D. Perrin, Cours d'algèbre, Éditions Ellipses (1996).

[9] D. Pierce & A. Pillay, A note on the axioms for differentially closed fields of characteristic zero, J. of algebra 204 (1998) :108–115.

[10] M. Rosenlicht, Extensions of Vector Groups by Abelian Varieties, American Journal of Mathematics 80, No. 3 (1958) : 685–714.

[11] M. Rosenlicht, The Nonminimality of the Differential Closure, Pacific Journal of Mathematics Vol. 52, No. 2 (1974).

[12] J. H. Silverman, The Arithmetic of Elliptic Curves, Second Edition, Springer (2009).

[13] J. H. Silverman & J. T. Tate, Rational Points on Elliptic Curves, Second Edition, Springer (2015).

[14] K. Tent & M. Ziegler, A Course in Model Theory, Cambridge University Press (2012).