Module ACGA

Cours : Yongquan Hu

10 avril 2011

Table des matières

Chapitre 1

Algèbre et géométrie

Dans la **totalité** de ce cours, les anneaux seront supposés *unitaires*, *commutatifs* et *non triviaux.*

1.1 Rappels sur les idéaux

Définition 1.1.1 (Idéal)
Soit $\mathbb{A}$ un anneau et soit $\mathcal{I} \subset \mathbb{A}$.
Alors on dit que $\mathcal{I}$ est un idéal de $\mathbb{A}$ si :
(i) $(\mathcal{I}, +)$ *est un sous–groupe de* $(\mathbb{A}, +)$ *;*
(ii) $\forall a \in \mathbb{A}, \forall x \in \mathcal{I},\ ax \in \mathcal{I}$.

Remarques :
1. $\{0\}$ et $\mathbb{A}$ sont deux idéaux de $\mathbb{A}$, appelés *idéaux triviaux.*
2. Un idéal $\mathcal{I}$ de $\mathbb{A}$ est dit *propre* si $\mathcal{I} \subsetneq \mathbb{A}$.

Proposition 1.1.1
Soit $\mathbb{A}$ un anneau.
Alors :

$$\mathbb{A} \text{ est un corps } \Leftrightarrow \text{ ses idéaux sont triviaux}$$

Définition 1.1.2 (Morphisme d'anneaux)
Soient $\mathbb{A}$ et $\mathbb{B}$ deux anneaux.
On dit qu'une application $f : \mathbb{A} \to \mathbb{B}$ est un morphisme d'anneaux si elle vérifie que :
(i) f est un morphisme de groupes *de* $(\mathbb{A}, +)$ *dans* $(\mathbb{B}, +)$ *;*
(ii) $f(1_{\mathbb{A}}) = 1_{\mathbb{B}}$ *;*
(iii) $\forall x, y \in \mathbb{A},\ f(xy) = f(x)f(y)$.
On appelle noyau et image du morphisme f son noyau et son image en tant que morphisme de groupes.

Proposition 1.1.2
Soient $\mathbb{A}$ et $\mathbb{B}$ deux anneaux.
Soit $\varphi : \mathbb{A} \to \mathbb{B}$ un morphisme d'anneaux.
Alors :
(i) si J est un idéal de $\mathbb{B}$, $\varphi^{-1}(J)$ est un idéal de $\mathbb{A}$;
(ii) si φ est surjectif *et si I est un idéal de $\mathbb{A}$, $\varphi(I)$ est un idéal de $\mathbb{B}$.*

Proposition 1.1.3 (Intersection d'idéaux)
Soit $\mathbb{A}$ un anneau.
Soit $(I_j)_{j\in J}$ une famille (quelconque) d'idéaux de $\mathbb{A}$.
Alors :

$$\bigcap_{j\in J} I_j \text{ est un idéal de } \mathbb{A}$$

*En particulier, si $S \subset \mathbb{A}$, on peut définir l'*idéal engendré par *S comme étant l'intersection de tous les idéaux de $\mathbb{A}$ contenant S. Il s'agit de fait du plus petit idéal de $\mathbb{A}$ contenant S.*

Notations

- Si $S \subset \mathbb{A}$, on note $\langle S \rangle$ l'idéal engendré par S.
- Si I est un idéal de $\mathbb{A}$ et $\varphi : \mathbb{A} \to \mathbb{B}$ un morphisme d'anneaux, on note :

$$I^e := \langle \varphi(I) \rangle \subset \mathbb{B}$$

- Si J est un idéal de $\mathbb{B}$ et $\varphi : \mathbb{A} \to \mathbb{B}$ un morphisme d'anneaux, on note :

$$I^c := \varphi^{-1}(J) \subset \mathbb{A}$$

Proposition 1.1.4 (Somme d'idéaux)
Soit $\mathbb{A}$ un anneau.
Soit $(I_j)_{j\in J}$ une famille (quelconque) d'idéaux de $\mathbb{A}$.
Alors l'ensemble suivant est un idéal de $\mathbb{A}$:

$$\sum_{j\in J} I_j := \left\{ \sum_{j\in J} x_j \;\middle|\; \forall j \in J,\ x_j \in I_j,\ \ \textit{les } x_j \textit{ presque tous nuls} \right\}$$

Remarques :

1. Si $J = \{1 \ldots n\}$, la somme s'écrit :

$$\sum_{j=1}^{n} I_j = \left\{ \sum_{j=1}^{n} x_j \;\middle|\; \forall 1 \leq j \leq n,\ x_j \in I_j \right\}$$

2. Si $x_1, \ldots, x_n \in \mathbb{A}$, alors :

$$\sum_{j=1}^{n} \langle x_j \rangle = \langle x_1, \ldots, x_n \rangle$$

Proposition 1.1.5 (Produit d'idéaux)
Soit $\mathbb{A}$ un anneau.
*Soit $(I_i)_{1\leq i\leq n}$ une famille **finie** d'idéaux de $\mathbb{A}$.*
Alors l'ensemble suivant est un idéal de $\mathbb{A}$:

$$I_1 \ldots I_n := \left\{ \sum_{i=1}^{n} \prod_{k=1}^{n} x_{i,k} \;\middle|\; \forall 1 \leq i, k \leq n,\ x_{i,k} \in I_k \right\} = \left\langle \prod_{k=1}^{n} x_k \;\middle|\; \forall 1 \leq k \leq n,\ x_k \in I_k \right\rangle$$

Proposition 1.1.6
Soit $\mathbb{A}$ un anneau.
Soit $(I_i)_{1\leq i\leq n}$ une famille finie d'idéaux de $\mathbb{A}$.
Alors :

$$I_1 \ldots I_n \subset \bigcap_{i=1}^{n} I_i$$

Proposition 1.1.7 (Division d'idéaux)
Soit $\mathbb{A}$ un anneau.
Soient I, J deux idéaux de $\mathbb{A}$.
Alors l'ensemble suivant est un idéal de $\mathbb{A}$, appelé conducteur de J dans I :

$$(I : J) := \{x \in \mathbb{A} \mid \underbrace{x.J}_{:=\langle x\rangle .J} \subset I\}$$

Démonstration : Il est clair que $(I : J)$ est un sous–groupe additif de $\mathbb{A}$. De plus, si $a \in (I : J), b \in \mathbb{A}$, alors comme $a.J \subset I$, $a.b.J = b.a.J \subset b.I \subset b.I$, d'où le résultat.

Définition 1.1.3 (Idéal annulateur)
Soit $\mathbb{A}$ un anneau.
Soit J un idéal de $\mathbb{A}$.
Alors on appelle idéal annulateur de J l'idéal $((0) : J)$.

Construction d'anneaux quotients :
Soit $\mathbb{A}$ un anneau et soit I un idéal de $\mathbb{A}$. Alors I définit une relation d'équivalence sur $\mathbb{A}$, appelée relation d'équivalence modulo I :

$$a \equiv b[I] \Leftrightarrow a - b \in I$$

Pour $a \in \mathbb{A}$, on not $\mathrm{cl}_I(a)$ la classe de a modulo I. L'ensemble quotient A/I ainsi défini est muni d'une structure d'anneau via les opérations $(a, b \in \mathbb{A})$:

$$\mathrm{cl}_I(a) + \mathrm{cl}_I(b) := \mathrm{cl}_I(a+b)$$
$$\mathrm{cl}_I(a) \times \mathrm{cl}_I(b) := \mathrm{cl}_I(a \times b)$$

L'application $\mathrm{cl}_I : \mathbb{A} \to \mathbb{A}/I$ constitue donc un morphisme d'anneaux surjectif qui induit une bijection entre l'ensemble des idéaux de $\mathbb{A}$ contenant I et l'ensemble des idéaux de $\mathbb{A}/I$.

1.2 Lemme de Zorn

Définition 1.2.1 (Élément maximal, plus grand élément)
Soit $(E, \leq)$ un ensemble ordonné.
Soit $m \in E$.
Alors :

(i) on dit que m est un élément maximal de E si :

$$\nexists x \in E \setminus \{m\},\ m \leq x$$

1. on dit m est un plus grand élément de E si :

$$\forall x \in E,\ x \leq m$$

Définition 1.2.2 (Ensemble inductif)
Soit $(E, \leq)$ un ensemble ordonné.
Alors on dit que E est inductif si toute partie totalement ordonnée (on dit aussi chaîne) de E est majorée dans E.

Remarques :

1. Un ensemble inductif est non vide. En effet, $\emptyset$ est une chaîne de E donc y est majorée.
2. Si E est totalement ordoné, l'inductivité est équivalente à l'existence d'un plus grand élément.

Lemme 1.2.1 (Zorn)
Tout ensemble inductif admet un élément maximal.

Le lemme de Zorn est équivalent à l'axiome du choix, que nous utiliserons dans toute la suite de ce cours.

Axiome 1 (Axiome du choix)
Soit I un ensemble et soit $(E_i)_{i \in I}$ une famille d'ensembles tous non vides.
Alors :

$$\prod_{i \in I} E_i \neq \emptyset$$

1.3 Idéaux premiers, idéaux maximaux

Définition 1.3.1 (Idéal premier)
Soit $\mathbb{A}$ un anneau.
Soit $\mathfrak{P}$ un idéal de $\mathbb{A}$.
On dit que $\mathfrak{P}$ est un idéal premier si :

(i) $\mathfrak{P} \neq \mathbb{A}$;
(ii) pour tous $a, b \in \mathbb{A}$ tels que $ab \in \mathfrak{P}$, on a $a \in \mathfrak{P}$ ou $b \in \mathfrak{P}$.

Définition 1.3.2 (Idéal maximal)
Soit $\mathbb{A}$ un anneau.
Soit $\mathfrak{M}$ un idéal de $\mathbb{A}$.
On dit que $\mathfrak{M}$ est un idéal maximal si :

(i) $\mathfrak{M} \neq \mathbb{A}$ *;*

(ii) il n'existe aucun idéal I de $\mathbb{A}$ tel que $\mathfrak{M} \subsetneq I \subsetneq \mathbb{A}$ (i.e $\mathfrak{M}$ est un élément maximal pour l'inclusion).

Proposition 1.3.1
Soit $\mathbb{A}$ un anneau.
Soit I un idéal de $\mathbb{A}$.
Alors :

$$\begin{gathered} I \text{ est premier } \Leftrightarrow \mathbb{A}/I \text{ est intègre} \\ \text{et} \\ I \text{ est maximal } \Leftrightarrow \mathbb{A}/I \text{ est un corps} \end{gathered}$$

Proposition 1.3.2 (Krull)
Soit $\mathbb{A}$ un anneau.
Alors tout idéal propre de $\mathbb{A}$ est contenu dans un idéal maximal. En particulier, $\mathbb{A}$ possède des idéaux maximaux.

DÉMONSTRATION : Soit E l'ensemble des idéaux propres de $\mathbb{A}$, ordonné par l'inclusion. Alors E est un ensemble inductif. En effet, si C est une chaîne de E, alors :

Cas 1 : $C = \emptyset$. Alors $\{0\}$ majore C dans E.

Cas 2 : $C \neq \emptyset$. Alors, si on pose :

$$J := \bigcup_{\mathcal{I} \in C} \mathcal{I}$$

J est un idéal de $\mathbb{A}$ car C est totalement ordonnée pour l'inclusion, et est propre car $\forall \mathcal{I} \in C$, $1 \notin \mathcal{I}$ (car $\mathbb{A} \neq \{0\}$) donc $1 \notin J$.

Proposition 1.3.3
Soit $\mathbb{A}$ un anneau.
Soit $\mathfrak{P}$ un idéal premier de $\mathbb{A}$.
Soient I, J deux idéaux de $\mathbb{A}$.
Alors :

(i) si $I \cap J \subset \mathfrak{P}$, alors $I \subset \mathfrak{P}$ ou $J \subset \mathfrak{P}$;

(ii) si $I.J \subset \mathfrak{P}$, alors $I \subset \mathfrak{P}$ ou $J \subset \mathfrak{P}$.

DÉMONSTRATION : $I.J \subset I \cap J$ donc il suffit de montrer le point (ii). Supposons donc que $I.J \subset \mathfrak{P}$ mais que $I, J \subsetneq \mathfrak{P}$. Alors, il existe $a \in I, b \in J$ tels que $a, b \notin \mathfrak{P}$. Cependant, $ab \in I.J \subset \mathfrak{P}$, ce qui induit une contradiction sur la primalité de $\mathfrak{P}$.

Proposition 1.3.4
Soit $\mathbb{A}$ un anneau.
Soit I un idéal de $\mathbb{A}$.
Supposons qu'il existe des idéaux premiers $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$ de $\mathbb{A}$ tels que :

$$I \subset \bigcup_{i=1}^{n} \mathfrak{P}_i$$

Alors il existe $1 \leq k \leq n$ tel que $I \subset \mathfrak{P}_k$.

1.4 Nilradical, radical de Jacobson

Proposition 1.4.1 (Radical d'un idéal)
Soit $\mathbb{A}$ un anneau.
Soit I un idéal de $\mathbb{A}$.
Alors l'ensemble suivant est un idéal de $\mathbb{A}$ contenant I, appelé radical de I :

$$\sqrt{I} := \{a \in \mathbb{A} \,|\, \exists n \geq 1,\, a^n \in I\}$$

DÉMONSTRATION :
- Il est clair que $I \subset \sqrt{I}$.
- Si $a, b \in \mathbb{A}$ sont tels que $a^n, b^m \in I$, alors :

$$\begin{aligned}(a+b)^{n+m} &= \sum_{k=0}^{n+m} C_{n+m}^k a^k b^{n+m-k} \\ &= \sum_{k=0}^{n} C_{n+m}^k a^k b^{n+m-k} + \sum_{k=n+1}^{n+m} C_{n+m}^k a^k b^{n+m-k} \\ &= b^m \left(\sum_{k=0}^{n} C_{n+m}^k a^k b^{n-k} \right) + a^n \left(\sum_{k=n+1}^{n+m} C_{n+m}^k a^{k-n} b^{n+m-k} \right) \in I\end{aligned}$$

  Donc $a+b \in \sqrt{I}$.
- Si $a \in \sqrt{I}, b \in \mathbb{A}$, alors (si $a^n \in I$), $(ab)^n \in I$ et donc $ab \in \sqrt{I}$.

Définition 1.4.1 (Idéal radical)
Un idéal égal à son radical est dit radical.

Définition 1.4.2 (Nilradical)
Soit $\mathbb{A}$ un anneau.
On appelle nilradical de $\mathbb{A}$ l'ensemble $\mathrm{Nil}(\mathbb{A})$ *de ses éléments nilpotents, i.e :*

$$\mathrm{Nil}(\mathbb{A}) := \sqrt{(0)}$$

Définition 1.4.3 (Spectre premier)
Soit $\mathbb{A}$ un anneau.
On appelle spectre premier de $\mathbb{A}$ l'ensemble $\mathrm{Spec}(\mathbb{A})$ *de ses idéaux premiers.*

Proposition 1.4.2
Soit $\mathbb{A}$ un anneau.
Alors :

$$Nil(\mathbb{A}) = \bigcap_{\mathfrak{P} \in \mathrm{Spec}(\mathbb{A})} \mathfrak{P}$$

DÉMONSTRATION :
- Soit $\mathfrak{P} \in \mathrm{Spec}(\mathbb{A})$ et soit $a \in \mathrm{Nil}(\mathbb{A})$ tel que $a^n = 0$. Alors $a^n = 0 \in \mathfrak{P}$ et donc (récurrence triviale sur n) $a \in \mathfrak{P}$.
- On démontre de façon analogue à celle vue en démontrant le théorème de Krull (proposition 1.3.2) que l'ensemble des idéaux de $\mathbb{A}$ ne contenant pas un certain $a \in \cap_{\mathfrak{P} \in \mathrm{Spec}(\mathbb{A})} \mathfrak{P}$ non nilpotent est inductif et donc admet un élément maximal $\mathfrak{P}$. On montre alors que $\mathfrak{P}$ est premier (découle de la maximalité en raisonnant par l'absurde) et contient une puissance de a, ce qui est absurde.

Corollaire 1.4.2.1
Soit $\mathbb{A}$ un anneau.
Soit I un idéal de $\mathbb{A}$.
Alors :

$$\sqrt{I} = \bigcap_{I \subset \mathfrak{P} \in \mathrm{Spec}(\mathbb{A})} \mathfrak{P}$$

DÉMONSTRATION : On applique la proposition 1.4.2 à $\mathbb{A}/I$.

Définition 1.4.4 (Spectre maximal)
Soit $\mathbb{A}$ un anneau.
On appelle spectre maximal de $\mathbb{A}$ l'ensemble $\mathrm{Max}(\mathbb{A})$ *de ses idéaux maximaux.*

Définition 1.4.5 (Radical de Jacobson)
Soit $\mathbb{A}$ un anneau.
On appelle radical de Jacobson de $\mathbb{A}$ l'idéal de $\mathbb{A}$ défini par :

$$\mathrm{JacNil}(\mathbb{A}) := \bigcap_{\mathfrak{M} \in \mathrm{Max}(\mathbb{A})} \mathfrak{M}$$

Proposition 1.4.3
Soit $\mathbb{A}$ un anneau.
Alors :

$$\mathrm{Nil}(\mathbb{A}) \subset \mathrm{JacNil}(\mathbb{A})$$

Proposition 1.4.4
Soit $\mathbb{A}$ un anneau.
Alors :

$$\mathrm{JacNil}(\mathbb{A}) = \{a \in \mathbb{A} \,|\, \forall b \in \mathbb{A},\, 1 - ab \in \mathbb{A}^\times\}$$

DÉMONSTRATION :

- Soit $a \in \mathrm{JacNil}(\mathbb{A})$. Supposons qu'il existe $b \in \mathbb{A}$ tel que $1 - ab$ ne soit pas inversible. Ainsi, $\langle 1 - ab \rangle \subsetneq \mathbb{A}$ et donc il existe $\mathfrak{M} \in \mathrm{Max}(\mathbb{A})$ tel que $1 - ab \in \mathfrak{M}$ par théorème de Krull (1.3.2). Or, $a \in \mathfrak{M}$ donc $ab \in \mathfrak{M}$ d'où $1 \in \mathfrak{M}$, ce qui est impossible. Donc $a \in lbracea \in \mathbb{A} \,|\, \forall b \in \mathbb{A},\, 1 - ab \in \mathbb{A}^\times\}$.
- Réciproquement, si $a \in lbracea \in \mathbb{A} \,|\, \forall b \in \mathbb{A},\, 1 - ab \in \mathbb{A}^\times\}$ mais $a \notin \mathrm{JacNil}(\mathbb{A})$, alors il existe $\mathfrak{M} \in \mathrm{Max}(\mathbb{A})$ tel que $a \notin \mathfrak{M}$ et donc de facto $\mathbb{A} = \mathfrak{M} + \langle a \rangle$ (car $\mathfrak{M} \subsetneq \mathfrak{M} + \langle a \rangle$) donc 1 s'écrit $1 = x + ab$ avec $x \in \mathfrak{M}$ et $b \in \mathbb{A}$ et donc $1 - ab = x$, d'où $x \in \mathbb{A}^\times$, ce qui contredit la propreté [1] de $\mathfrak{M}$. D'où le résultat.

1.5 Ensembles algébriques, topologie de Zariski

On se donne dans toute section un corps *infini* k. On notera par la suite $\mathbb{A}_k^n := k^n$ l'espace affine de dimension $n \geq 1$.

Définition 1.5.1 (Ensemble algébrique)
On appelle ensemble algébrique sur $\mathbb{A}_k^n$ tout ensemble de la forme :

$$\mathcal{V}(S) := \{a \in \mathbb{A}_k^n \,|\, \forall f \in S,\, f(a) = 0\},\; S \subset k[X_1, \ldots X_n]$$

Exemples :

1. $V_1 := \{(x, y) \in \mathbb{C}^2 \,|\, x^2 + y^2 + 1 = 0\}$ est un ensemble algébrique (non vide) sur $\mathbb{A}_{\mathbb{C}}^2$.
2. $V_2 := \{(x, y) \in \mathbb{R}^2 \,|\, x^2 + y^2 + 1 = 0\}$ est un ensemble algébrique (vide) sur $\mathbb{A}_{\mathbb{R}}^2$.
3. $V_3 := \{(x, y, z) \in \mathbb{Q}^3 \,|\, x^n + y^n = z^n\}$ est un ensemble algébrique sur $\mathbb{A}_{\mathbb{Q}}^3$.

Lemme 1.5.1
Soient $S, S' \subset k[X_1 \ldots X_n]$.
Soit I un idéal de $k[X_1 \ldots X_n]$.

(i) Si $S \subset S'$, alors $\mathcal{V}(S') \subset \mathcal{V}(S)$.
(ii) $\mathcal{V}(S) = \mathcal{V}(\langle S \rangle)$. En particulier, un ensemble algébrique peut toujours être défini via un idéal de $k[X_1 \ldots X_n]$.
(iii) $\mathcal{V}(I) = \mathcal{V}(\sqrt{I})$. En particulier, un ensemble algébrique peut toujours être défini via un idéal radical de $k[X_1 \ldots X_n]$.

DÉMONSTRATION :

(i) Trivial.

1. Et Dieu sait que certaines personnes n'aiment pas que l'on contredise leur propreté ...

(ii) – $S \subset \langle S\rangle$ donc $\mathcal{V}(\langle S\rangle) \subset \mathcal{V}(S)$.
– Soit $a \in \mathcal{V}(S)$ et soit $f \in \langle S\rangle$. Alors, par définition, f s'écrit sous la forme :

$$f = \sum_{i=1}^{n} p_i f_i, \quad \text{les } f_i \in S \text{ et les } p_i \in k[X_1 \dots X_n]$$

Ainsi :

$$f(a) = \sum_{i=1}^{n} p_i(a) \underbrace{f_i(a)}_{=0} = 0$$

D'où le résultat.

(iii) – $I \subset \sqrt{I}$ donc $\mathcal{V}(\sqrt{I}) \subset \mathcal{V}(I)$.
– Soit $a \in \mathcal{V}(I)$ et soit $f \in \sqrt{I}$. Alors il existe $n \geq 1$ tel que $f^n \in I$ et donc $(f(a))^n = 0$. Par intègrité de k, on a de facto $f(a) = 0$ et donc $a \in \mathcal{V}(\sqrt{I})$.

Proposition 1.5.1
On a les propriétés suivantes :

(i) $\emptyset$ et $\mathbb{A}_k^n$ sont des ensembles algébriques ;

(ii) une intersection d'ensembles algébrique est un ensemble algébrique ;

(iii) une réunion finie d'ensembles algébrique est un ensemble algébrique.

DÉMONSTRATION :

(i) Immédiat car $\emptyset = \mathcal{V}(1)$ et $\mathbb{A}_k^n = \mathcal{V}(0)$.

(ii) Soit $(\mathcal{V}(S_i))_{i\in I}$ une famille d'ensembles algébriques. Montrons que :

$$\bigcap_{i\in I} \mathcal{V}(S_i) = \mathcal{V}\left(\bigcup_{i\in I} S_i\right)$$

On a :

$$\begin{aligned} a \in \bigcap_{i\in I} \mathcal{V}(S_i) &\Leftrightarrow \forall i \in I, \forall f \in S_i,\ f(a) = 0 \\ &\Leftrightarrow \forall f \in \bigcup_{i\in I} S_i,\ f(a) = 0 \\ &\Leftrightarrow a \in \mathcal{V}\left(\bigcup_{i\in I} S_i\right) \end{aligned}$$

D'où le résultat.

(iii) Démontrons le résultat pour deux [2] ensembles algébriques. Soient donc I et J deux idéaux de $k[X_1 \dots X_n]$. Montrons que :

$$\mathcal{V}(I) \cup \mathcal{V}(J) = \mathcal{V}(I.J)$$

– $I, J \subset I.J$ donc $\mathcal{V}(I.J) \subset \mathcal{V}(I), \mathcal{V}(J)$, soit, in fine, $\mathcal{V}(I.J) \subset \mathcal{V}(I) \cup \mathcal{V}(J)$.
– Soit $a \in \mathcal{V}(I) \cup \mathcal{V}(J)$, par exemple $a \in \mathcal{V}(I)$ et soit $f \in I.J$. On peut alors écrire f sous la forme suivante :

$$f = \sum_{k=1}^{n} f_{k,I} f_{k,J}, \quad \text{les } f_{k,I} \in I \text{ et les } f_{k,J} \in J$$

Ainsi :

$$f(a) = \sum_{k=1}^{n} \underbrace{f_{k,I}(a)}_{=0} f_{k,J}(a) = 0$$

D'où le résultat.

Corollaire 1.5.1.1 (Topologie de Zariski sur $\mathbb{A}_k^n$)
Les ensembles algébriques forment les fermés d'une topologie sur $\mathbb{A}_k^n$, appelée topologie de Zariski.

2. Le lecteur conclura par récurrence "comme un grand". Il faut savoir se prendre en main de temps en temps.

Intéressons nous désormais au problème suivant :

Problème 1
Un ensemble algébrique est–il toujours défini par un nombre fini de polynômes ?

Définition 1.5.2 (Idéal de type fini)
Soit $\mathbb{A}$ un anneau.
On dit qu'un idéal $\mathcal{I}$ de $\mathbb{A}$ est de type fini si il existe $x_1, \ldots, x_k \in \mathbb{A}$ tels que $\mathcal{I} = \langle x_1 \ldots x_k \rangle$.

On peut reformuler le problème 1 de la façon suivante : un idéal de $k[X_1 \ldots X_n]$ est–il toujours de type fini ?

1.6 Anneaux noethériens

Proposition 1.6.1 (Anneau noethérien)
Soit $\mathbb{A}$ un anneau.
Alors $\mathbb{A}$ est dit noethérien s'il vérifie l'une (et donc toutes) des propriétés équivalentes suivantes :

(i) *toute suite croissante d'idéaux de $\mathbb{A}$ est stationnaire ;*

(ii) *toute famille non vide d'idéaux de $\mathbb{A}$ admet un élément maximal ;*

(iii) *tout idéal de $\mathbb{A}$ est de type fini.*

DÉMONSTRATION :

$(i) \Rightarrow (ii)$ Découle immédiatement du fait que toute famille non d'idéaux sans élément maximal admet une sous–suite croissante non stationnaire.

$(ii) \Rightarrow (iii)$ Soit I un idéal de $\mathbb{A}$. On considère la famille $\mathcal{F}$ des idéaux de type fini contenus dans I. Par hypothèse, cette famille admet un élément maximal J. Si on suppose que $J \subsetneq I$, il existe $x \in I \subset J$ et donc $J + \langle x \rangle$ est un idéal de type fini contenant strictement J et inclus dans I, ce qui contredit la maximalité de J.

$(iii) \Rightarrow (i)$ Soit $(I_n)_n$ une suite croissante d'idéaux de $\mathbb{A}$. On pose :

$$I := \bigcup_{n \geq 0} I_n$$

Par hypothèse, I est de type fini . De plus, par croissance de I_n, il existe N tel que I_N contienne les générateurs de I et donc la suite précitée est stationnaire.

Exemples :

1. Tout anneau principal (et donc tout corps) est noethérien.
2. Si k est un corps, $k[X]$ est noethérien (car principal). À l'inverse $k[(X_n)_{n \geq 0}]$ ne l'est pas car la suite $(\langle X_0, \ldots, X_k \rangle)_k$ est non stationnaire.

Proposition 1.6.2
Soit $\mathbb{A}$ un anneau noethérien.
Soit I un idéal de $\mathbb{A}$.
Alors :

(i) *l'anneau quotient $\mathbb{A}/I$ est noethérien ;*

(ii) *il existe $r \geq 0$ tel que $\left(\sqrt{I}\right)^r \subset I$.*

DÉMONSTRATION :

(i) Soit $\pi : \mathbb{A} \to \mathbb{A}/I$ la projection canonique et soit J un idéal de $\mathbb{A}$ sur I. Comme $\pi^{-1}(J)$ est un idéal de $\mathbb{A}$, il est de type fini et donc J également, d'où le résultat.

(ii) $\sqrt{I}$ est de type fini donc il suffit, si $I =: \langle x_1 \ldots x_n \rangle$, de prendre $r := nk$, où k est l'entier tel que pour tout i, $x_i^r \in I$.

Lemme 1.6.1
Soit $\mathbb{A}$ un anneau noethérien.
Soit I un idéal de $\mathbb{A}[X]$.
Pour $k \geq 0$, on pose :

$$L_k(I) := \{0\} \bigcup \{a_k \in \mathbb{A} \,|\, \exists P \in I,\, P = a_k X^k + Q,\, \deg(Q) < k\}$$

Alors :

(i) $(L_k(I))_k$ *est une suite croissant d'idéaux de* $\mathbb{A}$ *;*

(ii) si J est un idéal de $\mathbb{A}[X]$ inclus dans I tel que $L_k(I) = L_k(J)$ alors $I = J$.

Théorème 1.6.3 (Théorème de la base de Hilbert)
Soit $\mathbb{A}$ un anneau noethérien.
Soit $n \geq 1$.
Alors l'annneau $\mathbb{A}[X_1, \ldots, X_n]$ est noethérien.

Corollaire 1.6.3.1
Soit k un corps.
Alors $k[X_1, \ldots, X_n]$ est noethérien.

Corollaire 1.6.3.2
Tout ensemble algébrique V de $\mathbb{A}_k^n$ est défini par un nombre fini d'équations.

Démonstration : On a vu qu'il existait un idéal I de $k[X_1, \ldots, X_n]$ tel que $V = \mathcal{V}(I)$. Par théorème de la base de Hilbert (1.6.3), $I =: \langle f_1, \ldots, f_k \rangle$ et donc $V = \mathcal{V}(f_1, \ldots, f_k)$.

Définition 1.6.1
Soit k un corps.
Soit V un ensemble algébrique de $\mathbb{A}_k^n$.
Alors on pose :

$$\mathcal{I}(V) := \{f \in k[X_1, \ldots, X_n] \,|\, \forall a \in V,\, f(a) = 0\}$$

Lemme 1.6.2
Soit k un corps.
Soit V un ensemble algébrique de $\mathbb{A}_k^n$.
Alors $\mathcal{I}(V)$ est un idéal radical de $k[X_1, \ldots, X_n]$.

Démonstration : Il est clair que $I := \mathcal{I}(V)$ est un idéal de $k[X_1, \ldots, X_n]$. De plus, si $f \in \sqrt{I}$, il existe n tel que $\forall a \in V$, $f^n(a) = 0$, ce qui implique (par intégrité de k) que $f(a) = 0$ et donc $f \in I$, d'où le résultat.
Par conséquent, l'application $V \mapsto \mathcal{I}(V)$ envoie l'ensemble des ensembles algébriques sur celui des idéaux radicaux de $k[X_1, \ldots, X_n]$, qui est lui–même renvoyé sur son collègue précité par l'application $I \mapsto \mathcal{V}(I)$.

Proposition 1.6.4
Soit k un corps.
Soient V et W deux ensembles algébriques sur $\mathbb{A}_k^n$.
Alors :

(i) si $V \subset W$, alors $\mathcal{I}(W) \subset \mathcal{I}(V)$;

(ii) $\mathcal{I}(V \cup W) = \mathcal{I}(V) \cap \mathcal{I}(W)$;

(iii) pour tout idéal I de $k[X_1 \ldots X_n]$, on a :

$$I \subset \mathcal{I}(\mathcal{V}(I))$$

(iv) $V = \mathcal{V}(\mathcal{I}(V))$.

En fait, on pourrait définir $\mathcal{I}(V)$ à l'identique pour tout $V \subset \mathbb{A}_k^n$. On aurait alors $\mathcal{V}(\mathcal{I}(V)) = \overline{V}$, où $\overline{V}$ est l'adhérence (au sens de Zariski) de V.

1.7 Rappels sur les corps algébriquements clos

Définition 1.7.1 (Extension de corps)
Soit k un corps.
On appelle alors extension de k toute k–algèbre qui est un corps.

✍ Désormais, on notera (si nulle ambiguité n'est à craindre) $\mathbb{K}/k$ une extension $\mathbb{K}$ d'un corps k.

Définition 1.7.2 (Éléments algébriques, transcendants)
Soit $\mathbb{K}/k$ une extension de corps.
Soit $\alpha \in \mathbb{K}$.
Alors on dit que α est ...

(i) ... algébrique si $\exists P \in \mathbb{K}[X] \setminus \{0\}$ tel que $P(\alpha) = 0$;

(ii) ... transcendant dans le cas contraire.

Définition 1.7.3 (Extensions algébrique, transcendante, finie)
Soit $\mathbb{K}/k$ une extension de corps.
Alors $\mathbb{K}$ est dite :

(i) algébrique si ses éléments sont algébriques sur k ;

(ii) transcendante sinon ;

(iii) finie si $\dim_k \mathbb{K} < \infty$. On appelle alors degré de $\mathbb{K}$ sur k la quantité suivante :

$$[\mathbb{K} : k] := \dim_k \mathbb{K}$$

Lemme 1.7.1
Toute extension finie est algébrique.

Proposition 1.7.1 (Lemme des bases téléscopiques)
Soient $\mathbb{K}/k$ et $\mathbb{L}/\mathbb{K}$ deux extensions de corps.
Alors $\mathbb{L}$ est une extension de k et :

$$[\mathbb{L} : k] = [\mathbb{L} : \mathbb{K}][\mathbb{K} : k]$$

Corollaire 1.7.1.1
Soient $\mathbb{K}/k$ et $\mathbb{L}/\mathbb{K}$ deux extensions finies.
Alors $\mathbb{L}/k$ est une extension finie.

Lemme 1.7.2
Soit k un corps.
Soit $\mathfrak{P}$ un idéal premier de $k[T]$.
Alors :

(i) $\mathfrak{P}$ est principal engendré par un polynôme irréductible ;

(ii) $\mathfrak{P}$ est un idéal maximal ;

(iii) le corps $k[T]/\mathfrak{P}$ est une extension finie de k.

DÉMONSTRATION :

(ii) Soit I un iéal contenant strictement $\mathfrak{P}$ et soit $P \in I \setminus \mathfrak{P}$. Alors P ne divise pas le générateur Q de et donc est premier avec lui. De facto, il existe $A, B \in k[T]$ tels que $AP + BQ = 1$ et donc $1 \in I$ d'où $I = k[T]$.

Proposition 1.7.2 (Corps algébriquement clos)
Soit k un corps.
Les assertions suivantes sont alors équivalentes :

(i) k n'admet pas d'extension algébrique non triviale ;

(ii) les polynômes irréductibles de $k[T]$ sont de degré 1 ;

(iii) tout polynôme de $k[T]$ de degré supérieur ou égal à 1 admet une racine sur k ;

(iv) tout polynôme de $k[T]$ de degré supérieur ou égal à 1 est scindé sur k.

Lorsque c'est le cas, on dit que k est un corps algébriquement clos.

Exemples :

1. $\mathbb{C}$ est algébriquement clos.
2. $\mathbb{R}$ n'est pas algébriquement clos.
3. $\mathbb{Q}$ n'est pas algébriquement clos.

Définition 1.7.4 (Clôture algébrique)
Un clôture algébrique d'un corps k est une extension algébrique *de k qui est un corps algébriquement clos.*

Exemples :

1. $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.
2. Le corps $\overline{\mathbb{Q}}$ des nombres complexes algébriques sur $\mathbb{Q}$ est une clôture algébrique de $\mathbb{Q}$.

Proposition 1.7.3 (Steinitz)
Soit k un corps.
Alors :

(i) k admet une clôture algébrique ;

(ii) deux clôtures algébriques de k sont k–isomorphes.

Démonstration : Admis (utilise le lemme de Zorn).

1.8 Algèbres de type fini

Définition 1.8.1 (Algèbre)
Soit $\mathbb{A}$ un anneau.
Une $\mathbb{A}$–algèbre est un couple $(\mathcal{A}, j)$ où :

(i) $\mathcal{A}$ est un anneau ;

(ii) $j : \mathbb{A} \to \mathcal{A}$ est un morphisme d'anneaux non nul (appelé morphisme structural).

Remarques :

1. La relative simplicité de cette définition s'explique par le fait que tous les anneaux considérés sont commutatifs.
2. Lorsque $\mathbb{A}$ est un corps, le morphisme structural j est nécessairement injectif.

Définition 1.8.2 (Sous–algèbre)
Soit $\mathbb{A}$ un anneau.
Soit $(\mathcal{A}, j)$ une $\mathbb{A}$–algèbre.
Soit $\mathcal{B} \subset \mathcal{A}$.
Alors on dit que $(\mathcal{B}, j_{|\mathcal{B}})$ est une sous–algèbre de $\mathcal{A}$ si :

(i) $\mathcal{B}$ est un sous–anneau de $\mathcal{A}$;

(ii) $j(\mathbb{A}) \subset \mathcal{B}$.

Proposition 1.8.1 (Sous–algèbre engendrée par une partie)
Soit $\mathbb{A}$ un anneau.
Toute intersection de sous–algèbre d'une de $\mathbb{A}$–algèbre donnée $\mathcal{A}$ est une sous–algèbre de $\mathcal{A}$. Par conséquent, on peut définir la sous–algèbre engendrée par une partie $S \subset \mathcal{A}$ comme étant l'intersection de toutes les sous–algèbres de $\mathcal{A}$ contenant S. C'est alors la plus petite sous–algèbre vérifiant cette propriété, et on la note $\mathbb{A}[S]$.

Définition 1.8.3 (Morphisme d'algèbres)
Soit $\mathbb{A}$ un anneau.
Soient $(\mathcal{A}, j)$ et $(\mathcal{A}', j')$ deux $\mathbb{A}$–algèbres.
On appelle morphisme d'algèbres tout morphisme d'anneaux $\varphi : \mathcal{A} \to \mathcal{A}'$ tel que :

$$\varphi \circ j = j'$$

Définition 1.8.4 (Algèbre de type fini)
Soit $\mathbb{A}$ un anneau.
On dit que $\mathcal{A}$ est de type fini si il existe une partie finie *$S \subset \mathcal{A}$ qui engendre $\mathcal{A}$ comme $\mathbb{A}$–algèbre.*

Lemme 1.8.1
Soit $\mathbb{A}$ un anneau.

(i) Tout anneau quotient d'une $\mathbb{A}$–algèbre de type fini est une $\mathbb{A}$–algèbre de type fini.

(ii) Si $\mathcal{A}$ est une $\mathbb{A}$–algèbre de type fini et que $\mathcal{B}$ est une $\mathcal{A}$–algèbre de type fini, alors $\mathcal{B}$ est une $\mathbb{A}$–algèbre de type fini.

DÉMONSTRATION : Si $\mathcal{A} = \mathbb{A}[S]$ et $\mathcal{B} = \mathcal{A}[F]$, alors $\mathcal{B} = \mathbb{A}[S \cup F]$.

Proposition 1.8.2
Soit k un corps.
Alors $k(X_1, \ldots, X_n)$ n'est pas de type fini en tant que k–algèbre.

DÉMONSTRATION : Supposons le contraire, i.e supposons que $k(X_1, \ldots, X_n) = k[y_1, \ldots, y_m]$, avec $y_i = \dfrac{f_i}{g_i}$, les $f_i, g_i \in k[X_1, \ldots X_n]$ avec les $g_i \neq 0$. Posons :

$$h := \prod_{i=1}^{n} g_i + 1 \in k[X_1, \ldots X_n]$$

Alors $\dfrac{1}{h} \in k(X_1, \ldots, X_n)$ et donc il existe $\lambda_1, \ldots, \lambda_k \in k$ et $r_{1,1}, \ldots, r_{k,m} \in \mathbb{N}$ tels que :

$$\frac{1}{h} = \sum_{i=1}^{k} \lambda_i \prod_{j=1}^{m} y_j^{r_{i,j}} = \sum_{i=1}^{k} \lambda_i \prod_{j=1}^{n} m \frac{f_j^{r_{i,j}}}{g_j^{r_{i,j}}}$$

Quitte à se livrer à des actes peu avouables sur $r_{1,1}, \ldots, r_{k,m}$, on peut écrire :

$$\frac{1}{h} = \frac{f}{\prod_{j=1}^{m} g_j^{r_j}}, \text{ avec } f \in k[X_1 \ldots X_n] \text{ et les } r_j \in \mathbb{N}$$

D'où :

$$fh = \prod_{j=1}^{m} g_j^{r_j}$$

Or $k[X_1 \ldots X_n]$ est factoriel (car k l'est) et comme $\deg(h) = \deg(g_1) + \ldots + \deg(g_n) \geq 1$, on peut trouver un polynôme irréductible non constant e tel que $e|h$. De facto, $e| \prod_j g_j^{r_j}$, ce qui implique par irréductibilité de e que e divise l'un des g_j. Ergo, $e|1$ (car $e|h$), ce qui est impossible.

Corollaire 1.8.2.1
Soit k un corps.
Soit $f \in k[X] \setminus \{0\}$.
Alors $k(X) \left[\dfrac{1}{f}\right]$ n'est pas un corps.

1.9 Extensions intègres

Définition 1.9.1 (Entier sur un anneau)
Soient $\mathbb{A} \subset \mathbb{B}$ deux anneaux.
On dit que $x \in \mathbb{B}$ est un entier sur $\mathbb{A}$ si il vérifie une équation de la forme :

$$x^n + \sum_{i=0}^{n-1} a_i x^i = 0, \text{ les } a_i \in \mathbb{A}$$

Une telle équation s'appelle relation de dépendance intégrale.

Remarque : Le fait que x vérifie une telle équation est équivalent au fait que x soit racine d'un polynôme *unitaire* de $\mathbb{A}[T]$.

Définition 1.9.2 (Module)
Soit $\mathbb{A}$ un anneau. Un $\mathbb{A}$–module à gauche est un triplet $(E, +, .)$ où :

(i) $(E, +)$ est un groupe abélien[3] *;*

(ii) . est une loi de composition externe (LCE), i.e une application de la forme $((\lambda, x) \in \mathbb{A}\times E) \mapsto (\lambda.x \in E)$ vérifiant :

  (a) $\forall x, y \in E, \forall \lambda \in \mathbb{A},\ \lambda.(x + y) = \lambda.x + \lambda.y$;

  (b) $\forall x \in E, \forall \lambda, \mu \in \mathbb{A},\ (\lambda + \mu).x = \lambda.x + \mu.x$;

  (c) $\forall x \in E,\ 1_{\mathbb{A}}.x = x$;

  (d) $\forall x \in E, \forall \lambda, \mu \in \mathbb{A},\ (\lambda \times \mu).x = \lambda.(\mu.x)$;

Proposition 1.9.1 (Sous–module engendré par une partie)
Soit $\mathbb{A}$ un anneau. Soit E un $\mathbb{A}$–module
Soit $S \subset E$.
Alors l'intersection de tous les sous–modules de E contenant S est le plus petit sous–module de E contenant S. On l'appelle sous–module engendré par S.
Il est de plus égal à :

$$\left\{ \sum_{i=1}^{n} \lambda_i s_i \;\middle|\; n \geq 1, (\lambda_i)_i \in \mathbb{A}^n, (s_i)_i \in S^n \right\}$$

En particulier, le sous–module engendré par la réunion de deux parties est égal à leur somme.

✍ On notera cet ensemble $\langle S \rangle_{\mathbb{A}}$, voire $\langle S \rangle$ si l'on a pas froid aux yeux.

Définition 1.9.3 (Module de type fini)
Soit $\mathbb{A}$ un anneau. Un $\mathbb{A}$–module est dit de type fini s'il est engendré par un ensemble fini.

Remarque : Une somme de modules de type fini est de type fini.

Proposition 1.9.2
Soient $\mathbb{A} \subset \mathbb{B}$ deux anneaux.
Soit $x \in \mathbb{B}$.
Alors :

$$\begin{gathered} x \text{ est entier sur } \mathbb{A} \\ \Leftrightarrow \\ \mathbb{A}[x] \text{ est un } \mathbb{A}\text{–module de type fini} \end{gathered}$$

Corollaire 1.9.2.1
Soient $\mathbb{A} \subset \mathbb{B}$ deux anneaux.
Soient $x_1 \ldots x_n \in \mathbb{B}$ des entiers sur $\mathbb{A}$.
Alors l'algèbre $\mathbb{A}[x_1, \ldots, x_n] \subset \mathbb{B}$ est un $\mathbb{A}$–module de type fini. En particulier, tout élément de $\mathbb{A}[x_1, \ldots, x_n]$ est un entier sur $\mathbb{A}$.

Corollaire 1.9.2.2
Soient $\mathbb{A} \subset \mathbb{B}$ deux anneaux.
Alors l'ensemble des éléments de $\mathbb{B}$ entiers sur $\mathbb{A}$ forme un sous–anneau de $\mathbb{B}$ contenant $\mathbb{A}$.

Définition 1.9.4 (Anneau entier)
Soient $\mathbb{A} \subset \mathbb{B}$ deux anneaux.
Alors $\mathbb{B}$ est dit entier sur $\mathbb{A}$ si tous ses éléments le sont.

Proposition 1.9.3
Soient $\mathbb{A} \subset \mathbb{B}$ deux anneaux intègres.
On suppose que $\mathbb{B}$ est entier sur $\mathbb{A}$.
Alors :

3. "+" n'est en général pas l'addition sur $\mathbb{A}$ (que l'on note pourtant de la même façon) !

$$\mathbb{A} \text{ est un corps} \\ \Leftrightarrow \\ \mathbb{B} \text{ est un corps}$$

DÉMONSTRATION :
- Supposons que $\mathbb{A}$ soit un corps. Soit $b \in \mathbb{B}^*$. Comme b est entier sur $\mathbb{A}$, il vérifie une relation de dépendance intégrale de la forme :

$$b^n + \sum_{i=0}^{n-1} a_i b^i = 0, \text{ les } a_i \in \mathbb{A}$$

Quitte à prendre n minimal, on peut supposer $a_0 \neq 0$ (car $\mathbb{B}$ est intègre). On a alors :

$$b\left(b^{n-1} + \sum_{i=0}^{n-1} a_i b^{i-1}\right) = -a_0 \in \mathbb{A}^\times = \mathbb{A}^*$$

Donc b est inversible.
- Réciproquement, si on suppose que $\mathbb{B}$ est un corps, tout élément $a \in \mathbb{A}^*$ admet un inverse b dans $\mathbb{B}$. De plus, b est entier sur $\mathbb{A}$ donc vérifie une relation de dépendance intégrale de la forme :

$$b^n + \sum_{i=0}^{n-1} a_i b^i = 0, \text{ les } a_i \in \mathbb{A}$$

Et donc :

$$b = b^n a^{n-1} = -\sum_{i=0}^{n-1} a_i a^{n-1-i} \in \mathbb{A}$$

D'où le résultat

1.10 Théorème des zéros de Hilbert

Théorème 1.10.1 (Théorème des zéros de Hilbert, énoncé 1)
Soit k un corps.
Soit $\mathbb{L}$ une k–algèbre de type fini.
Alors si $\mathbb{L}$ est un corps, l'extension $\mathbb{L}/\mathbb{K}$ est finie (et donc algébrique).

DÉMONSTRATION : Quand j'aurais le temps.

Théorème 1.10.2 (Théorème des zéros de Hilbert, énoncé 2)
Soit k un corps algébriquement clos.
Alors tout idéal maximal de $k[X_1, \ldots, X_n]$ est de la forme $\langle X_1 - a_1, \ldots, X_n - a_n \rangle$, avec les $a_i \in k$.

DÉMONSTRATION : Remarquons premièrement que les idéaux de la forme $\langle X_1 - a_1, \ldots, X_n - a_n \rangle$ sont bien maximaux. Inversement, si on se donne un idéal maximal $\mathfrak{M}$ alors l'extension $\mathbb{L} := k[X_1 \ldots X_n]/\mathfrak{M}$ est finie sur k d'après le théorème 1.10.1 et donc isomorphe à ce dernier (car il est algébriquement clos). De fait, il existe des éléments $a_i \in k$ tels que les $X_i - a_i \in \mathfrak{M}$ et donc $\mathfrak{M}$ contient l'idéal maximal $\langle X_1 - a_1, \ldots, X_n - a_n \rangle$ et est propre, donc y est égal.

Théorème 1.10.3 (Théorème des zéros de Hilbert, énoncé 3)
Soit k un corps algébriquement clos.
Soit I un idéal propre *de $k[X_1, \ldots, X_n]$.*
Alors :

$$\mathcal{V}(I) \neq \emptyset$$

DÉMONSTRATION : I est propre donc d'après le théorème de Krull (1.3.2), il existe un idéal maximal contenant I. De plus, par théorème 1.10.2, cet idéal est de la forme $\langle X_1 - a_1, \ldots, X_n - a_n \rangle$ et donc $\{a_1 \ldots a_n\} \subset \mathcal{V}(I)$, d'où le résultat.

Théorème 1.10.4 (Théorème des zéros de Hilbert, énoncé 4)
Soit k un corps algébriquement clos.
Soit I un idéal de $k[X_1, \ldots, X_n]$.
Alors :

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

DÉMONSTRATION :
- I est inclus dans l'idéal radical $\mathcal{I}(\mathcal{V}(I))$ donc $\sqrt{I} \subset \mathcal{I}(\mathcal{V}(I))$.
- Soit $f \in \mathcal{I}(\mathcal{V}(I))$. On considère l'idéal $J := \langle I, 1 - f.T \rangle \subset k[X_1 \ldots X_n, T]$. Remarquons tout d'abord que l'ensemble algébrique $\mathcal{V}(J) \subset \mathbb{A}_k^{n+1}$ est vide. En effet, si $(a_1 \ldots a_n, b) \in \mathcal{V}(J)$, alors $f(a_1 \ldots a_n, b) := f(a_1, \ldots, a_n) = 0$ et $1 - f(a_1, \ldots, a_n).b = 0$ et donc $1 = 0$.
  D'après le théorème 1.10.3, on a alors que $J = k[X_1 \ldots X_n, T]$ et donc $1 \in J$, i.e il existe $f_1, \ldots, f_k \in I$ et $g_0, \ldots, g_k \in k[X_1 \ldots X_n, T]$ tels que :

$$1 = \sum_{j=1}^{k} f_j g_j + (1 - f.T) g_0 \tag{1.1}$$

  On considère alors le morphisme :

$$\begin{aligned} \phi : k[X_1, \ldots, X_n, T] &\to k(X_1, \ldots, X_n) \\ X_i &\mapsto X_i \\ T &\mapsto \frac{1}{f} \end{aligned}$$

  En appliquant ϕ à l'équation 1.1, on obtient :

$$1 = \sum_{j=1}^{k} f_j g_j \left(X_1, \ldots, X_n, \frac{1}{f} \right)$$

  Posons à présent $d := \max_i \deg_T g_i$. On a alors $f^d \in I$ et donc $f \in \sqrt{I}$.

Corollaire 1.10.4.1
Soit k un corps algébriquement clos.
Alors les applications $V \mapsto \mathcal{I}(V)$ et $I \mapsto \mathcal{V}(I)$ sont des bijections réciproques reliant l'ensemble des ensembles algébriques de $\mathbb{A}_k^n$ et celui des idéaux radicaux *de $k[X_1, \ldots, X_n]$.*
En particulier, l'ensemble $\{\{a_1, \ldots, a_n\} \mid \forall 1 \leq i \leq n, \ a_i \in k\}$ est équipotent à $\mathrm{Max}(k[X_1 \ldots X_n])$ via l'application $(a_1, \ldots, a_n) \mapsto \langle X_1 - a_1, \ldots, X_n - a_n \rangle$.

Proposition 1.10.5
Soit k un corps algébriquement clos.
Soit V un ensemble algébrique de $\mathbb{A}_k^n$.
On note $\mathcal{A}(V) := k[X_1, \ldots, X_n]/\mathcal{I}(V)$. Alors :

(i) $\mathcal{A}(V)$ est une k-algèbre de type fini ;

(ii) l'anneau $\mathcal{A}(V)$ est réduit, i.e $\mathrm{Nil}(\mathcal{A}(V)) = \{0\}$.

1.11 Étude de la correspondance algèbre–géométrie

On se donne un corps algébriquement clos k.

Définition 1.11.1 (Ensemble algébrique irréductible)
Un ensemble algébrique non vide $V \subset \mathbb{A}_k^n$ est dit irréductible si pour tous (Zariski–)fermés V_1, V_2 tels que $V = V_1 \cup V_2$ alors $V_1 = V$ ou $V_2 = V$.

Proposition 1.11.1
Soit $V \subset \mathbb{A}_k^n$ un ensemble algébrique.
Alors :

$$\begin{gathered} V \textit{ est irréductible} \\ \Leftrightarrow \\ \mathcal{I}(V) \textit{ est premier} \\ \Leftrightarrow \\ \mathcal{A}(V) \textit{ est un corps} \end{gathered}$$

Proposition 1.11.2
Soit $V \subset \mathbb{A}_k^n$ un ensemble algébrique non vide.
Alors il existe une unique famille $V_1, \ldots, V_k$ d'ensembles algébriques irréductibles de $\mathbb{A}_k^n$ tels que :

(i)

$$V = \bigcup_{i=1}^{k} V_i$$

(ii) pour tous $i \neq j$, $V_i \not\subset V_j$.

Proposition 1.11.3
Soit $\mathbb{A}$ un anneau noethérien.
Soit I un idéal propre de $\mathbb{A}$.
Alors il existe une unique famille $\mathfrak{P}_1, \ldots, \mathfrak{P}_k$ d'idéaux premiers de $\mathbb{A}$ tels que :

(i)

$$I = \bigcap_{i=1}^{k} \mathfrak{P}_i$$

(ii) pour tous $i \neq j$, $\mathfrak{P}_i \not\subset \mathfrak{P}_j$.

Définition 1.11.2 (Espace topologique noethérien)
Un espace topologique est dit noethérien si toute suite décroissante *de fermés y est stationnaire.*

Proposition 1.11.4
Soit k un corps.
Alors l'espace $\mathbb{A}_k^n$ muni de la topologie de Zariski est noethérien.

DÉMONSTRATION : Découle du lemme 1.5.1 et du fait que $k[X_1 \ldots X_n]$ est un corps.

Définition 1.11.3 (Composantes irréductibles d'un ensemble algébrique)
Soit $V \subset \mathbb{A}_k^n$ un ensemble algébrique.
Alors les V_i de la proposition 1.11.2 sont appelés composantes irréductibles de V.

Proposition 1.11.5
Soit $V \subset \mathbb{A}_k^n$ un ensemble algébrique.
Alors les composantes irréductibles de V sont les fermés irréductibles maximaux contenus dans V. De plus, $\forall 1 \leq i \leq n$, $\mathcal{I}(V_i) \in \mathrm{Spec}(k[X_1 \ldots X_n])$ et est minimal parmi les idéaux premiers contenant $\mathcal{I}(V)$, i.e :

$$\mathcal{I}(V) = \bigcap_{i=1}^{n} \mathcal{I}(V_i)$$

Exemple : On considère l'idéal $I := \langle XY, YZ, XZ \rangle \subset k[X, Y, Z]$. Alors I est radical donc est égal à l'intersection des idéaux premiers minimaux le contenant. En fait :

$$I = \langle X, Y \rangle \cap \langle Y, Z \rangle \cap \langle X, Z \rangle$$

En effet, l'inclusion de gauche à droite est triviale et si on se donne $P \in k[X, Y, Z]$, alors :

$$P = \lambda + \sum_{i=1}^{d} a_i X^i + b_i Y^i + c_i Z^i + Q$$

Où λ et les a_i, b_i, c_i sont dans k et $Q \in I$. On remarque ensuite que si $P \in \langle X, Y \rangle$ (resp. $\langle Y, Z \rangle, \langle X, Z \rangle$, alors $\lambda = a_i = 0$ pour tout i (resp. $\lambda = b_i, c_i = 0$) et donc si $P \in \langle X, Y \rangle \cap \langle Y, Z \rangle \cap \langle X, Z \rangle$, $P = Q \in I$.

De plus, on a :

$$\mathcal{V}(I) = \{(0,0,z) \,|\, z \in k\} \cup \{(0,y,0) \,|\, y \in k\} \cup \{(x,0,0) \,|\, x \in k\} = \mathcal{V}(X,Y) \cup \mathcal{V}(X,Z) \cup \mathcal{V}(Y,Z)$$

Définition 1.11.4 (Dimension)
Soit V un ensemble algébrique de $\mathbb{A}_k^n$.
On appelle dimension de V l'entier suivant :

$$\dim(V) := \sup\{r \in \mathbb{N} \,|\, \exists V_0 \subsetneq \ldots \subsetneq V_r \subset V, \ \textit{les } V_i \textit{ irréductibles } \}$$

Proposition 1.11.6
Soient V, W deux ensembles algébriques de $\mathbb{A}_k^n$.

(i) Si $W \subset V$ alors $\dim(W) \leq \dim(V)$.

(ii) Si $V_1, \ldots, V_r$ sont les composantes irréductibles de V, alors :

$$\dim(V) = \max_{1 \leq i \leq r} \dim(V_i)$$

Démonstration :

(i) Trivial.

(ii) D'après le (i), $\dim V \geq \max \dim V_i$. Considérons à présent une chaîne $W_0 \subsetneq \subsetneq W_s$ de fermés irréductibles contenus dans V. Comme W_s est irréductible contenu dans $V = \cup V_i$, il existe un indice i_0 tel que $W_s \subset V_{i_0}$ et donc $W_0 \subsetneq \subsetneq W_s$ est une chaîne de fermés irréductibles contenus dans V_{i_0}, d'où $s \leq \dim V_{i_0} \leq \max \dim V_i$. La borne supérieure étant le plus petit majorant de l'ensemble considéré, on a donc $\dim(V) \leq \max \dim V_i$.

Proposition 1.11.7 (Produit de deux ensembles algébriques)
Soit $V = \mathcal{V}(I)$ un ensemble algébrique de $\mathbb{A}_k^n$, avec I radical dans $k[X_1, \ldots, X_n]$.
Soit $W = \mathcal{V}(J)$ un ensemble algébrique de $\mathbb{A}_k^m$, avec J radical dans $k[Y_1, \ldots, Y_m]$.
Alors :

$$V \times W = \mathcal{V}(I^e + J^e) = \mathcal{V}(\langle I, J \rangle_{k[X_1 \ldots X_n, Y_1 \ldots Y_m]}) \subset \mathbb{A}_k^{n+m}$$

Où la notation "e" est ici relative aux[4] *morphismes d'inclusion* $k[X_1 \ldots X_n] \hookrightarrow k[X_1 \ldots X_n, Y_1 \ldots Y_m]$ *et* $k[Y_1 \ldots Y_m] \hookrightarrow k[X_1 \ldots X_n, Y_1 \ldots Y_m]$.

Démonstration :

$$\begin{aligned}
(x, y) \in V \times W &\Leftrightarrow x \in \mathcal{V}(I), y \in \mathcal{V}(J) \\
&\Leftrightarrow \forall (f, g) \in I \times J,\ f(x) = g(y) = 0 \\
&\Leftrightarrow \forall (f, g) \in I^e \times J^e,\ f(x, y) = g(x, y) = 0 \text{ si on continue à noter } f \text{ et } g \text{ leurs images par l'inclusion} \\
&\Leftrightarrow (x, y) \in \mathcal{V}(I^e + J^e)
\end{aligned}$$

Exemples :

1. $\mathbb{A}_k^1 \times \mathbb{A}_k^1 = \mathbb{A}_k^2$.
2. $\mathbb{A}_k^1 \times \{0\} = \{(x, 0) \,|\, x \in \mathbb{A}_k^1\}$.

✗ Il existe des fermés de $\mathbb{A}_k^2$ qui ne sont pas produit de fermés de $\mathbb{A}_k^1$.

Définition 1.11.5 (Projection)
Soient $0 \leq s \leq n$.
Alors on définit l'application suivante, appelée projection de $\mathbb{A}_k^n$ sur $\mathbb{A}_k^s$:

$$\begin{aligned}
\pi_s : \mathbb{A}_k^n &\to \mathbb{A}_k^s \\
(a_1 \ldots a_n) &\mapsto (a_1 \ldots a_s)
\end{aligned}$$

4. Il y a donc deux sens à cette notation dans l'expression. Pour ceux qui trouvent ça déroutant, demandez vous ce qui signifie la phrase "la vieille garde le lit".

Exemple : On considère $V = \mathcal{V}(XY-1) \subset k[X,Y]$. On remarque alors que $V = \{(x, \frac{1}{x}) \mid x \in k^*\}$ et donc $\pi_1(v) = (Aa_k^1)^* \cong k^*$ et $\overline{\pi_1(V)} = \mathbb{A}_k^1 = \mathcal{V}(0)$. De plus, $\langle XY-1\rangle \cap k[X] = (0)$.

Lemme 1.11.1
Soit $S \subset \mathbb{A}_k^n$.
On définit $\mathcal{I}(S)$ de la même façon que si S était un ensemble algébrique.
Alors

(i) $\mathcal{I}(S) = \mathcal{I}(\overline{S})$ et $\overline{S}$ est l'unique Zariski–fermé vérifiant cette condition ;

(ii) $\overline{S} = \mathcal{V}(\mathcal{I}(S))$.

DÉMONSTRATION :

(i) – $S \subset \overline{S}$ donc $\mathcal{I}(\overline{S}) \subset \mathcal{I}(S)$.
– Soit $f \in \mathcal{I}(S)$. Alors $S \subset \mathcal{V}(f)$ qui est fermé donc $\overline{S} \subset \mathcal{V}(f)$ donc $f \in \mathcal{V}(\overline{S})$.
– Donnons nous à présent un fermé V tel que $\mathcal{I}(V) = \mathcal{I}(S)$. Alors $\mathcal{I}(\overline{S}) = \mathcal{I}(V)$ et donc $\mathcal{V}(\mathcal{I}(V)) = \mathcal{V}(\mathcal{I}(\overline{S}))$, i.e $\overline{S} = V$.

(ii) Découle du (i).

Proposition 1.11.8
Soit $V = \mathcal{V}(I)$ un ensemble algébrique de $\mathbb{A}_k^n$.
Alors :

$$\forall s \leq n,\ \overline{\pi_s(V)} = \mathcal{V}(I_s),\ \textit{où } I_s := I \cap k[X_1 \dots X_s]$$

DÉMONSTRATION : D'après le lemme 1.11.1, il nous suffit de démontrer que $\mathcal{I}(\pi_s(V)) = \mathcal{I}(\mathcal{V}(I_s))$. Or, par théorème 1.10.4, $\mathcal{I}(\mathcal{V}(I_s)) = \sqrt{I_s}$. De plus,

$$\begin{aligned} f \in \mathcal{I}(\pi_S(V)) &\Leftrightarrow f \in k[X_1 \dots X_s] \text{ et } f_{|_{\pi_s(V)}} = 0 \\ &\Leftrightarrow f \in k[X_1 \dots X_s] \text{ et } f_{|_V} = 0 \text{ via inclusion} \\ &\Leftrightarrow f \in k[X_1 \dots X_s] \text{ et } \exists r \geq 1,\ f^r \in I \\ &\Leftrightarrow f \in \sqrt{I_s} \end{aligned}$$

Corollaire 1.11.8.1
Soit V un ensemble algébrique de $\mathbb{A}_k^n$.
Alors si V est irréductible, $\overline{\pi_s(V)}$ l'est également pour tout $s \leq n$.

Chapitre 2

Base de Gröbner et division

Dans ce chapitre, k désigne un corps.

2.1 Algorithme de division

✍ Dans la suite, on notera un polynôme $f \in k[X_1 \dots X_n]$ sous la forme :

$$f = \sum_{\alpha \in \mathbb{N}^n} a_\alpha X^\alpha$$

Où les $a_\alpha \in k$ sont presque tous nuls et où la notation X^α désigne, si $\alpha = (\alpha_1, \dots, \alpha_n)$ le monôme $X_1^{\alpha_1} \dots X_n^{\alpha_n}$. On dira également qu'un tel monôme X^α *apparait* dans f si $a_\alpha \neq 0$. Enfin, si $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$, on pose :

$$|\alpha| := \sum_{i=1}^{n} \alpha_i$$

Définition 2.1.1 (Ordre monomial)
Une relation d'ordre $\geq$ sur $\mathbb{N}^n$ est dite monomiale si elle vérifie les conditions suivantes :

(i) $\forall \alpha, \beta \in \mathbb{N}^n$, *si* $\alpha \geq \beta$ *alors* $\forall \gamma \in \mathbb{N}^n$, $\alpha + \gamma \geq \beta + \gamma$ *;*

(ii) $\geq$ *est un bon ordre, i.e toute partie non vide possède un plus petit élément.*

☞ La condition (ii) est équivalente au fait que toute suite décroissante soit stationnaire. De plus, toute partie finie admet alors un plus grand élément.

Exemples :

1. Le seul ordre monomial sur $\mathbb{N}$ est l'ordre usuel.
2. Si $n \geq 2$, on peut définir plusieurs ordres monomiaux sur $\mathbb{N}^n$.
   - L'ordre lexicographique : $\alpha \geq \beta$ si le premier coefficient non nul de $\alpha - \beta$ est positif.
   - L'ordre lexicographico–bizarre : $\alpha \geq \beta$ si le dernier coefficient non nul de $\alpha - \beta$ est positif.
   - L'ordre lexicographique gradué : $\alpha \geq \beta$ si $|\alpha| > |\beta|$ *ou bien* $|\alpha| = |\beta|$ et le premier coefficient non nul de $\alpha - \beta$ est positif.

Dans toute la suite, on fixe un ordre monomial $\geq$ sur $\mathbb{N}^n$.

Définition 2.1.2
Soit $f = \sum_{\alpha \in \mathbb{N}^n} a_\alpha X^\alpha \in k[X_1 \dots X_n]$.

(i) On appelle multi–degré de f le multi-entier :

$$\text{multdeg}(f) := \max_{\geq} \{\alpha \in \mathbb{N}^n \mid a_\alpha \neq 0\}$$

(ii) On appelle coefficient dominant de f la quantité :

$$LC(f) := a_{\text{multdeg}(f)}$$

(iii) On appelle monôme dominant de f la quantité :

$$LM(f) := X^{\mathrm{multdeg}(f)}$$

(iv) On appelle terme dominant de f la quantité :

$$LT(f) := a_{\mathrm{multdeg}(f)} X^{\mathrm{multdeg}(f)} = LC(f)LM(f)$$

Exemple : Posons $f := 4XY^2Z + 4Z^2 - 5X^3 + 7X^2Z^2 \in \mathbb{Q}[X, Y, Z]$.

1. Pour l'ordre lexicographique, on a :
   - $LT(f) = -5X^3$;
   - $\mathrm{multdeg}(f) = (3, 0, 0)$.
2. Pour l'ordre lexicographique gradué, on a :
   - $LT(f) = 7X^2Z^2$;
   - $\mathrm{multdeg}(f) = (2, 0, 2)$.

Algorithme 2.1.1 (Division de polynômes à plusieurs variables)
Soient $f, f_1, \ldots, f_s \in k[X_1 \ldots X_n]$.
L'algorithme suivant renvoie $a_1, \ldots, a_s, r \in k[X_1 \ldots X_n]$ tels que :

$$f = \sum_{i=1}^{s} a_i f_i + r$$

Avec $r = 0$ ou bien r est une combinaison linéaire de monômes qui ne sont divisibles par aucun des $LT(f_i)$. De plus, $\forall 1 \leq i \leq s$, $\mathrm{multdeg}(a_i f_i) \leq \mathrm{multdeg}(f)$.
ALGORITHME :

- Initialisation. *$\forall 1 \leq i \leq s$, $a_i \leftarrow 0$; $r \leftarrow 0$; $g \leftarrow f$.*
- Tant que *$g \neq 0$, on exécute le test conditionnel ci–après.*
  - Si *cela est possible, on trouve le premier indice $1 \leq i_0 \leq s$ tel que $LT(f_i)|LT(g)$.* Alors *:*

$$a_{i_0} \leftarrow a_{i_0} + \frac{LT(g)}{LT(f_{i_0})} \quad ; \quad g \leftarrow g - \frac{LT(g)}{LT(f_{i_0})} f_{i_0}$$

  - Sinon *:*

$$g \leftarrow g - LT(g) \quad ; \quad r \leftarrow r + LT(g)$$

✗ ***ATTENTION !*** L'ordre des f_i affecte le résultat.

Exemple : Soit $f := X^2Y + XY^2 + Y^2 \in \mathbb{Q}[X, y]$ (ordre lexicographique). On pose $f_1 := XY - 1$ et $f_2 = Y^2 - 1$.

- Effectuons la division de f par (f_1, f_2).

$X^2Y + XY^2 + Y^2$	$XY - 1$	$Y^2 - 1$	r
$XY^2 + X + Y^2$	$X + Y$	1	$X + Y + 1$
$X + Y^2 + Y$			
$Y^2 - 1$			
$Y + 1$			

  Ainsi : $f = (X + Y)f_1 + f_2 + (X + Y + 1)$.
- Effectuons à présent la division de f par (f_2, f_1).

$X^2Y + XY^2 + Y^2$	$Y^2 - 1$	$XY - 1$	r
$XY^2 + X + Y^2$	$X + 1$	X	$2X + 1$
$2X + 1$			
Y^2			
1			

  Ainsi : $f = (X + 1)f_2 + Xf_1 + (2X + 1)$.

2.2 Bases de Gröbner

Définition 2.2.1 (Idéal monomial)
Un idéal de $k[X_1 \dots X_n]$ est dit monomial si il est engendré par des monômes.

Lemme 2.2.1
Soit $I = \langle X^\alpha \mid \alpha \in A \subset \mathbb{N}^n \rangle$ un idéal monomial.
Alors :

(i) $\forall \beta \in \mathbb{N}^n$, $X^\beta \in I \Leftrightarrow \exists \alpha \in A$, $X^\alpha | X^\beta$;

(ii) $\forall f \in k[X_1 \dots X_n]$, *$f \in I$ si et seulement si tous les monômes apparaissant dans f sont des éléments de I.*

Lemme 2.2.2 (Dickson)
Soit $I = \langle X^\alpha \mid \alpha \in A \subset \mathbb{N}^n \rangle$ un idéal monomial.
Alors, il existe $\alpha_1 \dots \alpha_s \in A$ tel que $I = \langle X^{\alpha_1} \dots X^{\alpha_s} \rangle$.

Démonstration : D'après le théorème de la base de Hilbert (1.6.3), I est de type fini, soit $I = \langle f_1 \dots f_t \rangle$. De fait, chaque monôme apparaissant dans l'un des f_i est de la forme $X^\nu X^\alpha$, avec $\nu \in \mathbb{N}^n$ et $\alpha \in A$. Posons à présent :

$$S := \{X^\alpha \in I \mid \exists \nu \in \mathbb{N}^n \text{ tel que } X^\nu X^\alpha \text{ apparaisse dans l'un des } f_i\}$$

Par construction, S est un ensemble fini qui engendre I, d'où le résultat.

Définition 2.2.2
Soit I un idéal non nul de $k[X_1 \dots X_n]$.
On définit alors l'ensemble suivant :

$$LT(I) := \{LT(f) \mid f \in I\}$$

Proposition 2.2.1
Soit I un idéal non nul de $k[X_1 \dots X_n]$.
Alors $\langle LT(I) \rangle$ est un idéal monomial.

☞ Le lemme de Dickson (2.2.2) implique alors qu'il existe $g_1 \dots g_t \in I$ tels que :

$$\langle LT(I) \rangle = \langle LM(g_1) \dots LM(g_t) \rangle = \langle LT(g_1) \dots LT(g_t) \rangle$$

Définition 2.2.3 (Base de Gröbner)
Soit I un idéal non nul de $k[X_1 \dots X_n]$.
Une famille $(g_1, \dots, g_t)$ de polynômes de I est appelée base de Gröbner de I si :

$$LT(I) := \langle LT(g_1) \dots LT(g_t) \rangle$$

☞ Tout idéal non nul de $k[X_1 \dots X_n]$ admet une base de Gröbner. Il n'y a cependant pas en général unicité.

Proposition 2.2.2
Soit I un idéal non nul de $k[X_1 \dots X_n]$.
Soit $(g_1, \dots, g_t)$ une base de Gröbner de I.
Alors :

$$I = \langle g_1, \dots, g_t \rangle$$

Démonstration : Découle de l'algorithme 2.1.1.

Proposition 2.2.3
Soit I un idéal non nul de $k[X_1 \dots X_n]$.
Soit $(g_1, \dots, g_t)$ une base de Gröbner de I.
Soit $f \in k[X_1 \dots X_n]$.
Alors il existe un unique $r \in k[X_1 \dots X_n]$ tel que :

(i) $f - r \in I$;

(ii) aucun monôme de r n'est divisible par l'un des $LT(g_i)$.

Corollaire 2.2.3.1
Soit I un idéal non nul de $k[X_1 \dots X_n]$.
Soit $(g_1, \dots, g_t)$ une base de Gröbner de I.
Soit $f \in k[X_1 \dots X_n]$.
Alors :

(i) le reste r de la division (algorithme 2.1.1) de f par $(g_1, \dots, g_t)$ est uniquement déterminé par f (il ne dépend donc pas de l'ordre des g_i) ;

(ii) $f \in I \Leftrightarrow r = 0$.

Exemple : On considère l'idéal $I \subset k[X, Y]$ engendré par $g_1 := 2XY + Y$ et $g_2 := Y^2 - 1$. Alors (g_1, g_2) n'est pas une base de Gröbner de I car $LT(\frac{Y}{2}g_1 - Xg_2) \notin \langle LT(g_1), LT(g_2)\rangle$.

Proposition 2.2.4
Soit $I := \langle g_1 \dots g_t\rangle \subset k[X_1 \dots X_n]$.
Alors :

$$(g_1 \dots g_t) \text{ n'est pas une base de Gröbner de } I$$
$$\Leftrightarrow$$
$$\text{il existe } f \in I \text{ tel qu'aucun } LT(g_i) \text{ ne divise } LT(f).$$

Définition 2.2.4 (Plus petit commun multiple (ppcm))
Soient $\alpha, \beta \in \mathbb{N}^n$.
On appelle ppcm de X^α et X^β le monôme X^ν, où $\nu = (\nu_1 \dots \nu_n) \in \mathbb{N}^n$ avec $\forall 1 \leq i \leq n$, $\nu_i = \max(\alpha_i, \beta_i)$.

Définition 2.2.5 (S–polynôme)
Soient $f, g \in k[X_1 \dots X_n] \setminus \{0\}$.
On appelle S–polynôme de f et g le polynôme suivant :

$$S(f, g) := \frac{\text{ppcm}(LM(f), LM(g)}{LT(f)} f - \frac{\text{ppcm}(LM(f), LM(g)}{LT(g)} g$$

Remarques : Soient $f, g \in k[X_1 \dots X_n] \setminus \{0\}$. Alors :
- $S(f, g) = -S(g, f)$;
- $S(f, f) = 0$.

Proposition 2.2.5
Soient $c_1 \dots c_t \in k^*$ et $\alpha_1 \dots \alpha_t \in \mathbb{N}^n$.
Soient $g_1 \dots g_t \in k[X_1 \dots X_n]$.
On considère le polynôme :

$$f := \sum_{i=1}^{t} c_i X^{\alpha_i} g_i$$

On suppose qu'il existe $\delta \in \mathbb{N}^n$ tel que :
- $\forall 1 \leq i \leq t$, $\text{multdeg}(g_i) + \alpha_i = \delta$;
- $\text{multdeg}(f) < \delta$.

Alors il existe une famille $(c_{i,j})_{1 \leq i,j \leq t}$ d'éléments de k tels que :

$$f = \sum_{i<j} c_{i,j} X^{\delta - \nu_{i,j}} S(g_i, g_j)$$

Avec les $X^{\nu_{i,j}} = \text{ppcm}(X^{\text{multdeg}(g_i)}, X^{\text{multdeg}(g_j)}$. Notons qu'on a $\nu_{i,j} \leq \delta$ par construction.

Proposition 2.2.6 (Critère de Buchberger)
Soit I un idéal non nul de $k[X_1 \dots X_n]$.
Soit $(g_1 \dots g_t)$ un système de générateurs de I.
Alors :

$$(g_1 \dots g_t) \text{ est une base de Gröbner de } I$$
$$\Leftrightarrow$$

Pour tous $i \leq j$, le reste de la division de $S(g_i, g_j)$ par $\{g_1 \dots g_t\}$ pris dans un certain ordre est nul.

Remarque : L'éventuelle nullité du reste de la division précitée est en fait indépendante de la façon dont on ordonne les g_i.

2.3 Algorithme de Buchberger

Algorithme 2.3.2 (Buchberger)
Soit I un idéal non nul de $k[X_1 \dots X_n]$.
Soit $(g_1 \dots g_t)$ un système de générateurs de I.
L'algorithme suivant renvoie une base de Gröbner G de l'idéal I.

- Initialisation. $G \leftarrow \{g_1 \dots g_t\}$.
- Pour *tous $i \neq j$, calculer le reste r de la division de $S(g_i, g_j)$ par G.* Si $r \neq 0$ alors $G \leftarrow G \cup \{r\}$.
- *On itère l'étape précédente jusqu'à ne plus trouver que des restes nuls.*

Exemple : On considère l'idéal I engendré par $g_1 := 2XY + Y$ et $g_2 := Y^2 - 1$.

- $S(g_1, g_2) = X + \frac{1}{2}Y^2 = \frac{1}{2}g_2 + X + \frac{1}{2}$. Ainsi $G \leftarrow \{g_1, g_2, g_3 := X + \frac{1}{2}\}$.
- Par définition, le reste de la division de $S(g_1, g_2)$ par G est à présent nul. $S(g_1, g_3) = 0$, il n'y a donc rien à faire de ce côté–ci. $S(g_2, g_3) = X + \frac{1}{2}Y^2 = \frac{1}{2}g_2 + g_3$. Ainsi, l'algorithme termine en deux itérations et renvoie $\{g_1, g_2, g_3\}$.

Remarquons que $g_1 = 2Yg_3$, donc g_1 n'est pas "nécessaire" à notre base de Gröbner (nous y reviendrons).

2.4 Bases de Gröbner réduites

Soit I un idéal non nul de $k[X_1 \dots X_n]$, de base de Gröbner G. Supposons qu'il existe $g \in G$ tel que $LT(g) \in \langle LT(G \setminus \{g\}) \rangle$. Alors $G \setminus \{g\}$ est également une base de Gröbner de I.

Définition 2.4.1 (Base de Gröbner minimale)
Une base de Gröbner G est dite minimale si :

(i) $\forall g \in G,\ LC(g) = 1$;

(ii) $\forall g \in G,\ LT(g) \notin \langle LT(G \setminus \{g\}) \rangle$.

Remarque : Tout idéal non nul de $k[X_1 \dots X_n]$ admet une base de Gröbner minimale. Il n'y a pas en général unicité.

Proposition 2.4.1
Soit I un idéal non nul de $k[X_1 \dots X_n]$.
Soient G et H deux bases de Gröbner minimales de I.
Alors $LT(G) = LT(H)$ et donc $\operatorname{card} G = \operatorname{card} H$.

DÉMONSTRATION : Soit $g \in G$. H est une base de Gröbner de I donc il existe $h \in H$ tel que $LT(h)|LT(g)$. De plus, G est une base de Gröbner de I donc il existe $f \in G$ tel que $LT(f)|LT(h)$. Ainsi, par transitivité, $LT(f)|LT(g)$. Or, G est minimale donc $f = g$ et comme $LC(g) = LC(h) = 1$ alors $LT(g) = LT(h)$ et $LT(G) \subset LT(H)$. Les rôles de G et H étant symétriques, on obtient le résultat voulu.

Définition 2.4.2 (Base de Gröbner réduite)
Une base de Gröbner G est dite réduite si :

(i) $\forall g \in G,\ LC(g) = 1$;

(ii) $\forall g \in G$, *aucun des monômes de g n'appartient à* $\langle LT(G \setminus \{g\}) \rangle$.

Remarque : Une base de Gröbner réduite est minimale.

Exemple : On considère l'idéal I engendré par $g_1 := 2XY + Y$ et $g_2 := Y^2 - 1$. On pose $g_3 := X + \frac{1}{2}$. Alors (g_2, g_3) est une base de Gröbner réduite de I mais pas $(g_2, g_2 + g_3)$ (qui est "pourtant" minimale).

Proposition 2.4.2
Soit I un idéal non nul de $k[X_1 \dots X_n]$.
Alors I admet une unique base de Gröbner réduite.

Chapitre 3

Algèbre commutative

On considère dans ce chapitre un anneau $\mathbb{A}$ et un corps k.

3.1 Anneau des fractions

Définition 3.1.1 (Partie mutliplicative)
Soit $S \subset \mathbb{A}$.
On dit que S est multiplicative si :

(i) $1 \in S$;

(ii) $\forall x, y \in S$, $xy \in S$.

Lemme 3.1.1
Soit S une partie multiplicative de $\mathbb{A}$.
On définit alors une relation d'équivalence $\sim$ sur $\mathbb{A} \times S$ comme suit :

$$\forall (a,s),(b,t) \in \mathbb{A} \times S \ (a,s) \sim (b,t) \Leftrightarrow \exists r \in S,\ r(at - bs) = 0$$

✘ La relation $\sim$ suivante n'est pas en général une relation d'équivalence :

$$\forall (a,s),(b,t) \in \mathbb{A} \times S \ (a,s) \sim (b,t) \Leftrightarrow at = bs$$

En effet, si $\mathbb{A}$ n'est pas intègre, on peut trouver a et $s \neq t$ tels que $sa = ta$ et donc $(1,s) \sim (a,sa) \sim (1,t)$ mais $(1,s) \nsim (1,t)$.

Définition 3.1.2 (Localisé par rapport à une partie multiplicative)
Soit S une partie multiplicative de $\mathbb{A}$.
On appelle localisé de $\mathbb{A}$ par rapport à S le quotient $\mathbb{A}[S^{-1} := \mathbb{A} \times S/\sim$.

✍

- On note parfois cet anneau $S^{-1}\mathbb{A}$.
- La classe de $(a,s) \in \mathbb{A} \times S$ modulo $\sim$ est notée $\dfrac{a}{s}$.

Proposition 3.1.1
Soit S une partie multiplicative de $\mathbb{A}$.
Alors le localisé $\mathbb{A}[S^{-1}]$ est un anneau pour les opérations suivantes :

(i) $+ : (\dfrac{a}{s}, \dfrac{b}{t}) \mapsto \dfrac{at + bs}{st}$, *de neutre* $\dfrac{0}{1}$;

(ii) $\times(\dfrac{a}{s}, \dfrac{b}{t}) \mapsto \dfrac{ab}{st}$,*de neutre* $\dfrac{1}{1}$.

Proposition 3.1.2
Soit S une partie multiplicative de $\mathbb{A}$.
Alors :

(i) on dispose d'un morphisme d'anneaux :

$$\ell_S : \mathbb{A} \to \mathbb{A}[S^{-1}]$$
$$a \mapsto \frac{a}{1}$$

(ii) ℓ_S *est injective* $\Leftrightarrow$ S *ne contient aucun diviseur de* 0 *;*

(iii) $\mathbb{A}[S^{-1}] \cong \{0\} \Leftrightarrow 0 \in S$ *;*

(iv) $\ell_S(S) \cong S$ *et* $\ell_S(S) \subset \mathbb{A}[S^{-1}]^\times$ *;*

(v) $\mathbb{A}[S^{-1}] \cong \mathbb{A} \Leftrightarrow S \subset \mathbb{A}^\times$ *;*

DÉMONSTRATION :

(i) Clair.

(ii) Soit $a \in \mathbb{A}$. Alors :

$$a \in \mathrm{Ker}(\ell_S) \Leftrightarrow \exists s \in S\,, as = 0$$

D'où le résultat.

(iii) $\Rightarrow$ est triviale. Réciproquement, si $0 \in S$ alors $\sim$ est triviale, d'où le résultat.

(iv) La restriction de ℓ_S à S est clairement injective par multiplicativité de S et les points (ii) et (iii). L'inclusion de $\ell_S(S)$ dans $\mathbb{A}[S^{-1}]^\times$ découle du fait que $\forall s \in S$, $\dfrac{s}{1} \times \dfrac{1}{s} = \dfrac{1}{1}$.

(v)
- Si $S \subset \mathbb{A}^\times$, ℓ_S est injective par (i). De plus, $\forall \dfrac{a}{s} \in \mathbb{A}[S^{-1}]$, $\dfrac{a}{s} = \ell_S(as^{-1})$, donc ℓ_S est un isomorphisme.
- Réciproquement, si $\mathbb{A}[S^{-1}] \cong \mathbb{A}$ alors d'après (iii) tout élément de $\ell_S(S) \cong S$ est inversible dans $\mathbb{A}[S^{-1}] \cong \mathbb{A}$, d'où le résultat

Exemples :

1. Si $\mathbb{A}$ est intègre, alors $S := \mathbb{A}^*$ est multiplicative et $\mathbb{A}[S^{-1}]$ s'identifie au corps des fractions de $\mathbb{A}$.
2. Soit $\mathfrak{P} \in \mathrm{Spec}(\mathbb{A})$. Alors $S := \mathbb{A} \setminus \mathfrak{P}$ est multiplicative car si $a, b \notin \mathfrak{P}$ alors par primalité $ab \notin \mathfrak{P}$. On note alors $\mathbb{A}_{\mathfrak{P}}$ le localisé de $\mathbb{A}$ par rapport à S. Cet anneau est appelé *localisé de* $\mathbb{A}$ *en* $\mathfrak{P}$.

Définition 3.1.3 (Anneau local)
Un anneau est dit local s'il admet un unique idéal maximal.

Exemple "idiot" : un corps est local, d'idéal (0).

Proposition 3.1.3
$\mathbb{A}$ *est local* $\Leftrightarrow \mathbb{A} \setminus \mathbb{A}^\times$ *est un idéal de* $\mathbb{A}$.
Si c'est le cas, $\mathbb{A} \setminus \mathbb{A}^\times$ *est alors l'unique idéal maximal de* $\mathbb{A}$.

DÉMONSTRATION :

$(\Rightarrow)$ Soit $x \notin \mathbb{A}^\times$. Alors $\langle x \rangle$ est un idéal propre de $\mathbb{A}$ donc est contenu dans un idéal maximal (théorème de Krull – 1.3.2 –). Par localité de $\mathbb{A}$, il n'existe qu'un seul tel idéal, qui ne peut contenir d'inversible (un idéal maximal est propre). Ergo, cet idéal contient et est contenu dans $\mathbb{A} \setminus \mathbb{A}^\times$.

$\Leftarrow$ $\mathbb{A} \setminus \mathbb{A}^\times$ est un idéal propre de $\mathbb{A}$ car 1 est inversible. De plus, si I est un idéal contenant strictement $\mathbb{A} \setminus \mathbb{A}^\times$, alors $I \cap \mathbb{A}^\times \neq \emptyset$ et donc $I = \mathbb{A}$. Donc $\mathbb{A} \setminus \mathbb{A}^\times$ est maximal. L'unicité provient du fait que tout idéal propre est inclus dans $\mathbb{A} \setminus \mathbb{A}^\times$ (un idéal propre ne peut contenir d'inversible).

Corollaire 3.1.3.1
Soit $\mathfrak{P} \in \mathrm{Spec}(\mathbb{A})$.
Alors $\mathbb{A}_{\mathfrak{P}}$ *est local, d'idéal maximal* $\mathfrak{M} := \left\{ \dfrac{a}{s} \,\middle|\, a \in \mathfrak{P},\, s \notin \mathfrak{P} \right\}$.

Démonstration : $\mathfrak{M}$ est clairement un idéal car $\mathbb{A}\backslash\mathfrak{P}$ est multiplicative. De plus, $\frac{a}{s} \notin \mathfrak{M} \Leftrightarrow \frac{a}{s} \notin \mathbb{A}_{\mathfrak{P}}^{\times}$, d'où le résultat.

Proposition 3.1.4 (Propriété universelle du localisé)
Soit S une partie multiplicative de $\mathbb{A}$.
Alors pour tout anneau $\mathbb{B}$ et pour tout morphisme d'anneau $\phi : \mathbb{A} \to \mathbb{B}$ tel que $\varphi(S) \subset \mathbb{B}^{\times}$, il existe un unique morphisme d'anneaux $\psi : \mathbb{A}[S^{-1}] \to \mathbb{B}$ tel que $\phi = \psi \circ \ell_S$.

Démonstration : On vérifie que $\psi : \frac{a}{s} \mapsto \phi(a)\phi(s)^{-1}$ est bien définie et convient. L'unicité provient du fait que si $f \circ \ell_S = \phi$ alors nécessairement $\forall \frac{a}{s} \in \mathbb{A}[S^{-1}]$, $f\left(\frac{a}{S}\right) = \phi(a)\phi(s)^{-1}$.

Un petit diagramme commutatif ?

$$\begin{tikzcd}
\mathbb{A} \arrow[r, "\phi"] \arrow[d, "\ell_S"'] \arrow[dr, phantom, "\circlearrowleft"] & \mathbb{B} \\
\mathbb{A}[S^{-1}] \arrow[ur, "\exists!\psi"'] &
\end{tikzcd}$$

Proposition 3.1.5
Soient $S \subset T$ deux parties multiplicatives de $\mathbb{A}$. Alors :

(i) on dispose d'un morphisme d'anneaux injectif :

$$\begin{aligned} \mathbb{A}[S^{-1}] &\hookrightarrow \mathbb{A}[T^{-1}] \\ \frac{a}{s} &\mapsto \frac{a}{s} \end{aligned}$$

(ii) $\ell_S(T)$ est une partie multiplicative de $\mathbb{A}[S^{-1}]$;

(iii) $\mathbb{A}[S^{-1}][\ell_S(T)^{-1} \cong \mathbb{A}[T^{-1}]$.

3.2 Idéaux du localisé

Lemme 3.2.1
Soit S une partie multiplicative de $\mathbb{A}$.
Soit I un idéal de $\mathbb{A}$.
Alors :

$$(I^e)^c = \bigcup_{s \in S} (I : s)$$

Où les notations ^{e} et ^{c} sont entendues par rapport à ℓ_S.

Proposition 3.2.1 (Idéaux du localisé)
Soit S une partie multiplicative de $\mathbb{A}$.
Alors (les notations ^{e} et ^{c} sont entendues par rapport à ℓ_S) :

(i) tout idéal de $\mathbb{A}[S^{-1}$ est de la forme I^e, avec I idéal de $\mathbb{A}$;

(ii) les ensembles $\{\mathfrak{P} \in Spect = (\mathbb{A}) \,|\, \mathfrak{P} \cap S = \emptyset\}$ et $\mathrm{Spec}\mathbb{A}[S^{-1}]$ sont équipotents, via $\mathfrak{P} \mapsto \mathfrak{P}^e$ et $\mathfrak{Q} \mapsto \mathfrak{Q}^c$.

Démonstration : Démontrons le (i). Soit J un idéal de $\mathbb{A}[S^{-1}]$. On pose $I = J^c$. Alors par définition $I^e \subset J$ et si $\frac{a}{s} \in J$ alors $\frac{a}{1} = \frac{a}{s} \times \frac{s}{1} \in J$ et comme $\frac{a}{1} = \ell_S(a)$ on a $a \in J^c = I$. D'où le résultat.

3.3 Localisation d'un module

Lemme 3.3.1
Soit M un $\mathbb{A}$–module.
Soit S une partie multiplicative de $\mathbb{A}$.
On définit alors une relation d'équivalence $\sim$ sur $M \times S$ comme suit :

$$\forall (a,s),(b,t) \in M \times S \ (a,s) \sim (b,t) \Leftrightarrow \exists r \in S,\, r(at - bs) = 0$$

Définition 3.3.1 (Localisé d'un module)
Soit M un $\mathbb{A}$–module.
Soit S une partie multiplicative de $\mathbb{A}$.
On appelle localisé de M par rapport à S le quotient $M[S^{-1} := \mathbb{A} \times S/\sim$.

✍ La classe de $(a,s) \in M \times S$ modulo $\sim$ est notée $\dfrac{a}{s}$.

Proposition 3.3.1
Soit M un $\mathbb{A}$–module.
Soit S une partie multiplicative de $\mathbb{A}$.
Alors le localisé $M[S^{-1}]$ est un $\mathbb{A}[S^{-1}]$–module pour les opérations suivantes :

(i) $+ : (\dfrac{a}{s}, \dfrac{b}{t}) \mapsto \dfrac{at+bs}{st}$*, de neutre* $\dfrac{0}{1}$ *;*

(ii) $\times((\dfrac{a}{s}, \dfrac{b}{t}) \in \mathbb{A}[S^{-1}] \times M[S^{-1}]) \mapsto \dfrac{ab}{st}$*,de neutre* $\dfrac{1}{1}$.

☞ $M[S^{-1}]$ hérite de fait d'une structure de $\mathbb{A}$–module.

Proposition 3.3.2
Soit M un $\mathbb{A}$–module.
Soit S une partie multiplicative de $\mathbb{A}$.
Alors on dispose d'un morphisme de $\mathbb{A}$–modules :

$$\begin{aligned} \ell_S : M &\to M[S^{-1}] \\ a &\mapsto \frac{a}{1} \end{aligned}$$

Proposition 3.3.3 (Propriété universelle du localisé d'un module)
Soit M un $\mathbb{A}$–module.
Soit S une partie multiplicative de $\mathbb{A}$.
Alors pour tout $\mathbb{A}$–module N et pour tout morphisme de $\mathbb{A}$–modules $\phi : M \to N$, il existe un unique morphisme de $\mathbb{A}[S^{-1}]$–modules $\psi : M[S^{-1}] \to N[S^{-1}]$ tel que $\phi = \psi \circ \ell_S$.

Proposition 3.3.4 (Exactitude de la localisation)
Soient M et N deux $\mathbb{A}$–modules.
Soit $\phi : M \to N$ une application $\mathbb{A}$–linéaire.
Alors l'application suivante est $\mathbb{A}[S^{-1}]$–linéaire :

$$\begin{aligned} \phi[S^{-1}] : M[S^{-1}] &\to N[S^{-1}] \\ \frac{m}{s} &\mapsto \frac{\phi(m)}{s} \end{aligned}$$

Si de plus ψ est une application $\mathbb{A}$–linéaire partant de N alors :

$$(\psi \circ \phi)[S^{-1}] = \psi[S^{-1}] \circ \phi[S^{-1}]$$

Définition 3.3.2 (Suite exacte courte de $\mathbb{A}$–modules)
On appelle suite exacte courte de $\mathbb{A}$–modules un diagramme de la forme :

$$0 \to M' \xrightarrow{\phi} M \xrightarrow{\psi} M'' \to 0$$

Où :

- *ϕ est injective ;*

– *ψ est surjective ;*
– *$\Im\psi = \operatorname{Ker}\phi$.*

Remarquons que ces trois conditions sont équivalentes (dans leur ensemble) à la suivante : $M' \hookrightarrow M$ et $M'' \cong M/M'$.

Proposition 3.3.5

Pour toute suite exacte courte de $\mathbb{A}$–modules $0 \to M' \xrightarrow{\phi} M \xrightarrow{\psi} M'' \to 0$, la suite de $\mathbb{A}[S^{-1}]$–modules suivante est exacte :

$$0 \to M'[S^{-1}] \xrightarrow{\phi[S^{-1}]} M[S^{-1}] \xrightarrow{\psi[S^{-1}]} M''[S^{-1}] \to 0$$

Pour ceux qui parlent le langage des catégories, cette proposition signifie que le foncteur de localisation $\mathcal{F} : \mathbb{A}-\mathrm{Mod} \to \mathbb{A}[S^{-1}]-\mathrm{Mod}$ est exact.

Si I est un idéal de $\mathbb{A}$, il est naturellement muni d'une structure de $\mathbb{A}$–module et donc on peut définir $I[S^{-1}]$. Si la notation "^{e}" est relative à l'application canonique ℓ_S, on a même :

$$I^e = I[S^{-1}]$$

3.4 Idéaux primaires, irréductibles

Définition 3.4.1 (Idéal primaire)

Un idéal propre *$\mathfrak{Q}$ de $\mathbb{A}$ est dit primaire si $\forall a, b \in \mathbb{A}$ tels que $ab \in \mathfrak{Q}$ tel que $a \notin \mathfrak{Q}$ soit $b \in \sqrt{\mathfrak{Q}}$.*

Proposition 3.4.1

Soit $\mathfrak{Q}$ un idéal propre de $\mathbb{A}$.
Alors :

(i)

$$\begin{aligned} \mathfrak{Q} \text{ est primaire } &\Leftrightarrow \mathbb{A}/\mathfrak{Q} \neq \{0\} \text{ et tout diviseur de } 0 \text{ dans } \mathbb{A}/\mathfrak{Q} \text{ est nilpotent} \\ &\Leftrightarrow (0) \text{ est primaire dans } \mathbb{A}/\mathfrak{Q} \end{aligned}$$

(ii) si $\mathfrak{Q}$ est primaire, alors $\sqrt{\mathfrak{Q}}$ est premier. On dit alors que $\mathfrak{Q}$ est $\sqrt{\mathfrak{Q}}$–primaire.

Démonstration :

(i) La seconde équivalence est triviale. Soient $a, b \in \mathbb{A}$. Alors :

$$\begin{aligned} ab \in \mathfrak{Q} &\Leftrightarrow \overline{a}\overline{b} = 0 \text{ dans } \mathbb{A}/\mathfrak{Q} \\ a \notin \mathfrak{Q} &\Leftrightarrow \overline{a} \neq 0 \text{ dans } \mathbb{A}/\mathfrak{Q} \\ b \in \sqrt{\mathfrak{Q}} &\Leftrightarrow \overline{b} \in \mathrm{Nil}(\mathbb{A}/\mathfrak{Q}) \end{aligned}$$

D'où le résultat.

(ii) Soient $a, b \in \mathbb{A}$ tels que $ab \in \sqrt{\mathfrak{Q}}$. Alors, si $a \notin \sqrt{\mathfrak{Q}} \supset \mathfrak{Q}$, $b \in \sqrt{\mathfrak{Q}}$ par primalité. D'où le résultat.

✘ La réciproqie du point (ii) est **FAUSSE** ! Considérer l'idéal $\mathfrak{Q} := (X) \cap (X^2, Y^2) \subset k[X, Y]$ de racine $\sqrt{\mathfrak{Q}} = \sqrt{(X)} \cap \sqrt{(X^2, Y^2)} = (X)$. En effet, $X.Y^2 \in \mathfrak{Q}$, $X \notin \mathfrak{Q}$ et $Y^2 \notin \sqrt{\mathfrak{Q}}$.

Proposition 3.4.2

Un idéal premier est primaire.

Proposition 3.4.3

Soit $\mathfrak{Q}$ un idéal de $\mathbb{A}$ tel que $\sqrt{\mathfrak{Q}}$ soit un idéal maximal.
Alors $\mathfrak{Q}$ est primaire.

Démonstration : Un diviseur de 0 dans $\mathbb{A}/\mathfrak{Q}$ est toujours contenu dans un idéal maximal (Krull). Or il n'existe qu'un seul tel idéal car $\mathrm{Max}(\mathbb{A}/\mathfrak{Q})$ est équipotent à l'ensemble des idéaux maximaux de $\mathbb{A}$ contenu $\mathfrak{Q}$ (si $\mathfrak{M}$ est un tel idéal, alors comme $\mathfrak{Q} \subset \mathfrak{M}$, $\sqrt{\mathfrak{M}} \subset \mathfrak{Q}$ et donc $\mathfrak{M} = \sqrt{\mathfrak{Q}}$). Ainsi, tout diviseur de 0 dans $\mathbb{A}/\mathfrak{Q}$ est contenu dans l'idéal $\sqrt{\mathfrak{Q}}\mathfrak{Q} \subset \mathrm{Nil}(\mathbb{A}/\mathfrak{Q})$.

Exemple : (X^2, Y^2) est primaire dans $k[X,Y]$ car sa racine (X,Y) y est maximale.

Proposition 3.4.4
Toute puissance finie d'un idéal primaire est primaire.

Lemme 3.4.1
Soit $\mathfrak{P} \in \mathrm{Spec}(\mathbb{A})$.
Alors toute intersection d'idéaux $\mathfrak{P}$*–primaire est un idéal* $\mathfrak{P}$*–primaire.*

Définition 3.4.2 (Idéal irréductible)
Un idéal propre I *des* $\mathbb{A}$ *est dit irréductible si pour tous idéaux* I_1, I_2 *de* $\mathbb{A}$ *tels que* $I = I_1 \cap I_2$ *on a* $I = I_1$ *ou* $I = I_2$.

✍ I est irréductible (resp. primaire) dans $\mathbb{A}$ si et seulement si (0) est irréductible (resp. primaire) dans $\mathbb{A}/I$. Ainsi, on peut toujours se ramener au cas $I = (0)$.

Proposition 3.4.5
On suppose $\mathbb{A}$ *noethérien.*
Alors tout idéal irréductible de $\mathbb{A}$ *est primaire.*

Dans toute la suite du chapitre, on suppose l'anneau $\mathbb{A}$ noethérien.

3.5 Décomposition primaire

Définition 3.5.1 (Décomposition primaire)
Soit I *un idéal* propre *de* $\mathbb{A}$.
On appelle décomposition primaire de I *toute égalité de la forme suivante :*

$$I = \bigcap_{i=1}^{n} \mathfrak{Q}_i$$

Où les $\mathfrak{Q}_i$ *sont des idéaux primaires de* $\mathbb{A}$.

Proposition 3.5.1
Tout idéal propre de $\mathbb{A}$ *admet une décomposition primaire.*

Définition 3.5.2 (Décomposition primaire minimale)
Soit I *un idéal propre de* $\mathbb{A}$.
On se donne une décomposition primaire de I *:*

$$I = \bigcap_{i=1}^{n} \mathfrak{Q}_i$$

Alors cette décomposition est dite minimale si :
 (i) $\forall 1 \leq i \leq n,\ I \not\subset \cap_{j \neq i} \mathfrak{Q}_j$ *(i.e* $\cap_{j\neq i}\mathfrak{Q}_j \not\subset \mathfrak{Q}_i$*)* ;
 (ii) pour tous indices $i \neq j$, $\sqrt{\mathfrak{Q}_i} \neq \sqrt{\mathfrak{Q}_j}$.

Proposition 3.5.2
Tout idéal propre de $\mathbb{A}$ *admet une décomposition primaire minimale.*

✗ Il n'y a pas en général unicité !

3.6 Unicité

Soit I un idéal propre de $\mathbb{A}$.
On se donne une décomposition primaire minimale de I :

$$I = \bigcap_{i=1}^{n} \mathfrak{Q}_i$$

Pour tout indice i, on pose $\mathfrak{P}_i := \sqrt{\mathfrak{Q}_i}$. Alors :
- les $\mathfrak{P}_i$ sont appelés *idéaux premiers associés à* I ;
- si $\mathfrak{P}_i$ est minimal parmi les idéaux premiers de $\mathbb{A}$ contenant I, il est dit *isolé* ;
- dans le cas contraire, $\mathfrak{P}_i$ est dit immergé.

Exemple : Dans $k[X,Y]$, la décomposition $I = (X) \cap (X^2, Y^2)$ est minimale.
- Les idéaux premiers associés à I sont (X) et (X,Y).
- (X) est isolé.
- (X,Y) contient strictement (X) donc est immergé.

Proposition 3.6.1
Soit $\mathfrak{P} \in \mathrm{Spec}(\mathbb{A})$.
Sont alors équivalentes :

(i) il existe un indice i tel que $\mathfrak{P} = \mathfrak{P}_i$;

(ii) il existe $a \in \mathbb{A}$ tel que $\mathfrak{P} = (I : a)$.

Corollaire 3.6.1.1
Les $\mathfrak{P}_i$ sont indépendants de la décomposition, i.e si il existe deux décompositions primaires minimales de I $I = \cap_{i=1}^{n} \mathfrak{Q}_i = \cap_{i=1}^{m} \mathfrak{Q}'_i$ alors :

(i) $m = n$;

(ii) $\exists \sigma \in \mathfrak{S}_n$, $\forall 1 \leq i \leq n$, $\sqrt{\mathfrak{Q}_i} = \sqrt{\mathfrak{Q}'_{\sigma(i)}}$.

Remarque : Soit $\mathfrak{P} \in \mathrm{Spec}(\mathbb{A})$ et soit $\mathfrak{Q}$ un idéal $\mathfrak{P}$–primaire. Alors :

$$\forall a \in \mathbb{A},\ (\mathfrak{Q} : a) = \begin{cases} \mathbb{A} & \text{si } a \in \mathfrak{Q} \\ I \text{ idéal } \mathfrak{P}\text{–primaire} & \text{si } a \in \mathfrak{P} \setminus \mathfrak{Q} \\ \mathfrak{Q} & \text{si } a \notin \mathfrak{P} \end{cases}$$

Proposition 3.6.2
Soit $1 \leq i \leq n$. Si $\mathfrak{P}_i$ est un idéal premier isolé alors :

(i) il existe $s \notin \mathfrak{P}_i$ tel que $\mathfrak{Q}_i = (I : s)$;

(ii) $\mathfrak{Q}_i$ est le plus petit idéal $\mathfrak{P}_i$–primaire contenant I.

Corollaire 3.6.2.1
Soient $I = \cap_{i=1}^{n} \mathfrak{Q}_i = \cap_{i=1}^{n} \mathfrak{Q}'_i$ deux décompositions primaires de I telles que :

$$\forall 1 \leq i \leq n\, \mathfrak{P}_i := \sqrt{\mathfrak{Q}_i} = \sqrt{\mathfrak{Q}'_i}$$

Alors pour tout i tel que $\mathfrak{P}_i$ soit isolé on a :

$$\mathfrak{Q}_i = \mathfrak{Q}'_i$$

Exemple : On considère l'idéal $I = (X^2, XY^2) \subset k[X,Y]$. Une décomposition primaire minimale de I est :

$$I = (X) \cap (X^2, Y^2)$$

Pour $n \geq 2$, on pose $\mathfrak{Q}(n) = (X^2, XY^2, Y^n)$. Ces idéaux sont (X,Y)–primaires et :

$$\forall n \geq 2,\ I = (X) \cap \mathfrak{Q}(n) \text{ est une décomposition polaire minimale de } I$$

I admet donc une infinité de décompositions polaires minimales distinctes.

3.7 Décomposition polaire dans les anneaux localisés

$\boxed{\text{On se donne désormais une partie multiplicative } S \text{ de } \mathbb{A}.}$

Proposition 3.7.1
L'anneau $\mathbb{A}[S^{-1}]$ est noethérien.

Lemme 3.7.1
Soit $\mathfrak{Q}$ un idéal $\mathfrak{P}$–primaire de $\mathbb{A}$.
Alors :

(i) $\mathfrak{Q} \cap S = \emptyset \Leftrightarrow \mathfrak{P} \cap S = \emptyset$;

(ii) *Si* $\mathfrak{Q} \cap S = \emptyset$*, alors* $\mathfrak{Q}^e$ *est un idéal* $\mathfrak{P}^e$*–primaire de* $\mathbb{A}[S^{-1}]$ *(la notation "*^{e}*" est ici relative à l'application* ℓ_S*) ;*

(iii) *Si* $\mathfrak{Q} \cap S \neq \emptyset$*, alors* $\mathfrak{Q}^e = \mathbb{A}[S^{-1}]$.

Lemme 3.7.2
Soient $\mathbb{A}$ *et* $\mathbb{B}$ *deux anneaux.*
Soit $\phi : \mathbb{A} \to \mathbb{B}$ *un morphismes d'anneaux.*
Soit $\mathfrak{Q}$ *un idéal primaire de* $\mathbb{B}$.
Alors $\mathfrak{Q}^c$ *est un idéal primaire de* $\mathbb{A}$.

Démonstration : ϕ induit une injection de $\mathbb{A}/\mathfrak{Q}^c$ dans $\mathbb{B}/\mathfrak{Q}$ donc il est aisé de démontrer que les diviseurs de 0 de $\mathbb{A}/\mathfrak{Q}^c$ sont nilpotents.

Proposition 3.7.2
Les applications $\mathfrak{Q} \mapsto \mathfrak{Q}^e$ *et* $\mathfrak{Q} \mapsto \mathfrak{Q}^c$ *(les notation "*^{e}*" et "*^{c}*" sont ici relatives à l'application* ℓ_S*) sont des bijections réciproques entre l'ensemble des idéaux de primaires de* $\mathbb{A}$ *disjoints de* S *et celui des idéaux primaires de* $\mathbb{A}[S^{-1}]$.

Proposition 3.7.3
Soit I *un idéal propre de* $\mathbb{A}$ *tel que* $I \cap S = \emptyset$.
On se donne une décomposition primaire minimale de I *:*

$$I = \bigcap_{i=1}^{n} \mathfrak{Q}_i$$

Alors la relation suivante est une décomposition primaire minimale de I^e *dans* $\mathbb{A}[S^{-1}]$ *(la notation "*^{e}*" est ici relative à l'application* ℓ_S*) :*

$$I^e = \bigcap_{\mathfrak{Q}_i \cap S = \emptyset} \mathfrak{Q}_i^e$$

3.8 Applications

Lemme 3.8.1
On suppose $\mathbb{A}$ *réduit (i.e* $\mathrm{Nil}(\mathbb{A}) = (0)$*).*
Alors l'ensemble $\mathrm{Div}(\mathbb{A})$ *des diviseurs de zéro dans* $\mathbb{A}$ *vérifie :*

$$\mathrm{Div}(\mathbb{A}) = \bigcup_{\mathfrak{P} \in \mathrm{Spec}(\mathbb{A}) \ \textit{minimaux}} \mathfrak{P}$$

Proposition 3.8.1
Soient I, J *deux idéaux propres de* $\mathbb{A}$.
Alors :

$$(I : J) = I \Leftrightarrow J \textit{ n'est contenu dans aucun idéal premier associé à } I$$

Proposition 3.8.2
On rappelle que $\mathbb{A}$ *est supposé noethérien.*
Alors :

$$\mathrm{Div}(\mathbb{A}) = \bigcup_{\mathfrak{P} \in \mathrm{Spec}(\mathbb{A}) \ \textit{associés à } (0)} \mathfrak{P}$$

Théorème 3.8.3 (Lemme de Nakayama)
Soit $\mathbb{A}$ *un anneau (non nécessairement noethérien).*
Soit M *un* $\mathbb{A}$*–module de type fini.*
Soit I *un idéal de* $\mathbb{A}$ *tel que* $I \subset \mathrm{JacNil}(\mathbb{A})$.
Alors :

$$(M = I.M) \Rightarrow (M = 0)$$

Corollaire 3.8.3.1
Soit $\mathbb{A}$ *un anneau local d'idéal maximal* $\mathfrak{M}$.
Soit M *un* $\mathbb{A}$*–module de type fini.*
Alors :

$$(M = \mathfrak{M}.M) \Rightarrow (M = 0)$$

Corollaire 3.8.3.2
Soit $\mathbb{A}$ un anneau[1] *intègre.*
Soit I un idéal propre de $\mathbb{A}$.
Soit $\mathfrak{A}$ un idéal de $\mathbb{A}$.
Alors :

$$(\mathfrak{A} = I.\mathfrak{A}) \Rightarrow (\mathfrak{A} = 0)$$

Lemme 3.8.2
Soit I un idéal propre de $\mathbb{A}$.
Alors :

$$I.\left(\bigcap_{k\geq 1} I^k\right) = \bigcap_{k\geq 1} I^k$$

Proposition 3.8.4
Soit I un idéal propre de $\mathbb{A}$.

(i) *Si $I \subset \mathrm{JacNil}(\mathbb{A})$ alors $\cap_{k\geq 1} I^k = (0)$.*
(ii) *Si $\mathbb{A}$ est intègre alors $\cap_{k\geq 1} I^k = (0)$.*

3.9 Dimension

On suppose désormais le corps k algébriquement clos.

Définition 3.9.1 (Suite de rang r)
Soit V un ensemble algébrique de $\mathbb{A}_k^n$.
Pour $r \geq 1$, on appelle suite de rang r[2] *toute suite d'ensembles algébriques irréductibles V_i de $\mathbb{A}_k^n$ vérifiant :*

$$V_0 \subsetneq V_1 \subsetneq \ldots \subsetneq V_r \subset V$$

✍ Une telle suite induit de fait une suite d'idéaux dans $k[X_1 \ldots X_n]$:

$$\mathcal{I}(V) \subset \mathcal{I}(V_r) \subsetneq \ldots \subsetneq \mathcal{I}(V_0)$$

Et donc on a, dans l'algèbre $\mathcal{A}(V) := k[X_1, \ldots, X_n]/\mathcal{I}(V)$:

$$(0) \subset \mathcal{I}(V_r)/\mathcal{I}(V) \subsetneq \ldots \subsetneq \mathcal{I}(V_0)/\mathcal{I}(V)$$

On rappelle à tout hasard la définition suivante :

Définition 3.9.2 (Dimension)
Soit V un ensemble algébrique de $\mathbb{A}_k^n$.
On appelle dimension de V l'entier suivant :

$$\dim(V) := \sup\{r \in \mathbb{N} \,|\, \exists V_0 \subsetneq \ldots \subsetneq V_r \subset V, \ \textit{les } V_i \textit{ irréductibles } \}$$

Définition 3.9.3 (Dimension de Krull)
On appelle dimension de Krull de l'anneau $\mathbb{A}$ l'entier suivant :

$$\dim(\mathbb{A}) := \sup\{r \in \mathbb{N} \,|\, \exists \mathfrak{P}_0 \subsetneq \ldots \subsetneq \mathfrak{P}_r \subset \mathbb{A}, \ \textit{les } \mathfrak{P}_i \in \mathrm{Spec}(\mathbb{A}) \ \}$$

Proposition 3.9.1
Soit V un ensemble algébrique de $\mathbb{A}_k^n$.
Alors :

$$\dim(V) = \dim \mathcal{A}(V)$$

Définition 3.9.4 (Hauteur d'un idéal premier)
Soit $\mathfrak{P} \in \mathrm{Spec}(\mathbb{A})$.
On appelle hauteur de $\mathfrak{P}$ l'entier suivant :

$$\mathrm{ht}(\mathfrak{P}) := \sup\{r \in \mathbb{N} \,|\, \exists \mathfrak{P}_0 \subsetneq \ldots \subsetneq \mathfrak{P}_r = \mathfrak{P}, \ \textit{les } \mathfrak{P}_i \in \mathrm{Spec}(\mathbb{A}) \ \}$$

1. Noethérien à nouveau !
2. Les esprits chagrins auront remarqués qu'une suite de rang r possède $r+1$ termes ...

✍ On remarquera que :

$$\dim \mathbb{A} = \sup\{\mathrm{ht}(\mathfrak{P}) \mid \mathfrak{P} \in \mathrm{Spec}\mathbb{A}\} = \sup\{\mathrm{ht}(\mathfrak{M}) \mid \mathfrak{M} \in \mathrm{Max}\mathbb{A}\}$$

Proposition 3.9.2
Soit $\mathfrak{P} \in \mathrm{Spec}(\mathbb{A})$.
Alors :

$$\mathrm{ht}(\mathfrak{P}) = 0 \Leftrightarrow \mathfrak{P} \textit{ est un idéal premier isolé associé à } (0)$$

De fait, si $\mathbb{A}$ *est intègre on a :*

$$\mathrm{ht}(\mathfrak{P}) = 0 \Leftrightarrow \mathfrak{P} = (0)$$

Lemme 3.9.1
Soient $\mathfrak{P}_1, \mathfrak{P}_2 \in \mathrm{Spec}\mathbb{A}$ *tels que* $\mathfrak{P}_1 \subsetneq \mathfrak{P}_2$.
Si $\mathrm{ht}(\mathfrak{P}_2) - \mathrm{ht}(\mathfrak{P}_1) = 1$ *alors il n'existe aucun idéal premier strictement compris entre* $\mathfrak{P}_1$ *et* $\mathfrak{P}_2$.

Exemples :

1. Au sens de Krull, $\dim k[X] = 1$ car $k[X]$ est un anneau principal intègre donc toute suite d'idéaux premiers y est de la forme $(0) \subsetneq \langle f \rangle$, avec f irréductible.
2. $\dim k[X_1 \ldots X_n] \geq n$ car on a la suite $(0) \subsetneq \langle X_1 \rangle \subsetneq \ldots \subsetneq \rangle$.
3. Considérons l'idéal $I := \langle X^2Y, X^3 \rangle \subset k[X,Y]$ et l'ensemble algébrique $V := \mathcal{V}(I)$. Alors on a :

   $$V = \mathcal{V}(X^2Y) \cap \mathcal{V}(X^3) = \mathcal{V}(X)$$

   V est donc une droite vectorielle. De plus :

   $$\dim(V) = \dim \mathcal{A}(V) = \dim k[X,Y]/\sqrt{I} = \dim k[Y] = 1$$

   Et donc $\dim V = \dim_k V$.

Proposition 3.9.3
Soit $n \geq 1$.
Alors $\dim \mathbb{A}^n_k = n$.

Corollaire 3.9.3.1
Soit V *un ensemble algébrique de* $\mathbb{A}^n_k$.
Alors $\dim V \leq n$.

Proposition 3.9.4
Soit S *une partie multiplicative de* $\mathbb{A}$.
Alors :

(i) S *est (modulo inclusion) une partie multiplicative de* $\mathbb{A}[X]$ *;*

(ii) si $\mathbb{K}$ *est le corps des fractions de* $\mathbb{A}$ *alors on a dans* $\mathbb{K}(X)$ *l'égalité suivante :*

$$\mathbb{A}[S^{-1}][X] = \mathbb{A}[X][S^{-1}]$$

Corollaire 3.9.4.1
Si $\mathfrak{P} \in \mathrm{Spec}(\mathbb{A})$, *alors :*

$$\mathbb{A}_{\mathfrak{P}}[X] = \mathbb{A}[X][\mathbb{A} \setminus \mathfrak{P}] \textit{ dans } \mathbb{K}(X)$$

En particulier, comme $\mathbb{A}_{(0)} = \mathbb{K}$, *on a :*

$$\mathbb{K}[X] = \mathbb{A}[X][\mathbb{A}^*]$$

☞ De fait, comme $\mathbb{K}[X]$ est principal et que les idéaux premiers de $\mathbb{A}[X][\mathbb{A}^*]$ sont en bijection avec les idéaux premiers de $\mathbb{A}[X]$ disjoints de $\mathbb{A}^*$, on a que si $\mathfrak{P} \subsetneq \mathfrak{Q}$ sont deux tels idéaux alors $\mathfrak{P} = (0)$.

Proposition 3.9.5
Soit $\mathfrak{Q} \in \mathrm{Spec}(\mathbb{A})$.
Soit $\mathfrak{P}' \subsetneq \mathfrak{Q}[X]$ *un idéal premier de* $\mathbb{A}[X]$.
On pose $\mathfrak{P} := \mathbb{A} \cap \mathfrak{P}' \subsetneq \mathfrak{Q}$.
Si il n'existe aucun idéal premier strictement compris entre $\mathfrak{P}$ *et* $\mathfrak{Q}$ *alors :*

$$\mathfrak{P}' = \mathfrak{P}[X]$$

Théorème 3.9.6 (Théorème de l'idéal principal de Krull)
Soit $\mathbb{A}$ *un anneau (noethérien) intègre.*
Soit $I = \langle a \rangle$ *un idéal principal non nul de* $\mathbb{A}$.
Alors tout idéal premier isolé de I *est de hauteur* 1.

3.10 Calculs de dimension

Définition 3.10.1 (Ordre monomial gradué)
On dit qu'un ordre monomial sur $\mathbb{N}^n$ *est dit gradué si* $\forall \alpha, \beta \in \mathbb{N}^n$ *on a :*

$$(|\alpha| > |\beta|) \Rightarrow (\alpha > \beta)$$

Exemple : L'ordre lexicographique gradué est ... gradué ! ✌

On fixe à présent un ordre monomial gradué $\geq$.

Proposition 3.10.1
Soit I *un idéal propre de* $k[X_1 \dots X_n]$.
Alors :

$$\dim \mathcal{V}(I) = \dim \mathcal{V}(\langle LT(I) \rangle)$$

Exemple : On considère l'idéal $I := \langle X^5 Z^4, X^2 Y Z^2, Y^2 Z^3 \rangle \subset k[X, Y, Z]$. Remarquons alors que $\sqrt{I} = \langle XZ, YZ \rangle$ et donc que :

$$\mathcal{V}(I) = \mathcal{V}(\sqrt{I}) = \mathcal{V}(XZ) \cap \mathcal{V}(YZ) = \{Z = 0\} \cup \{X = Y = 0\}$$

Donc $\dim \mathcal{V}(I) = 2$.

Algorithme 3.10.3 (Calcul de dimension)
Soit I *un idéal propre de* $k[X_1 \dots X_n]$.

- *Calculer une base de Gröbner de* I *pour l'ordre* gradué $\geq$. *On obtient ainsi une base de* $\langle LT(I) \rangle$.
- *Calculer* $\dim \mathcal{V}(\langle LT(I) \rangle)$.
-

Proposition 3.10.2
Soit $I := \langle X^{\alpha_1} \dots X^{\alpha_r} \rangle$ *un idéal de* $k[X_1 \dots X_n]$.
Alors :

$$\dim \mathcal{V}(I) = n - \min\{\mathrm{card}\, J \mid J \subset \{X_1, \dots X_n\}, \forall 1 \leq i \leq r, \exists X_\ell \in J, X_\ell | X^{\alpha_i}\}$$