REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

Université Mohamed Boudiaf de M'sila
Faculté des Mathématiques et de l'Informatique
Département de Mathématiques

Mémoire de Master

Domaine : Mathématiques et Informatique
Filière : Mathématiques
Option : Algèbre et Mathématiques Discrétes

Thème

Le Nullstellensatz De Hilbert Et Quelques Applications

Présenté par :
Bouaziz Khalil

Devant le jury composé de :

M^r Amroune Abdelaziz	PROF,	Université de M'sila	**Président**.
M^r *Ladjelat Lahcene*	MAA,	Université de M'sila	**Encadreur**.
M^r *Dechoucha* Noureddine	MAA,	Université de M'sila	**Examinateur**.

Année universitaire 2020/2021

Le Nullstellensatz de Hilbert et Quelques Applications

Mr.M.A.A : LADJELAT LAHCENE ET BOUAZIZ KHALIL

29 juin 2021

Dédicaces

Je dédie ce travail ,

à mes chers parents,

à mon frère et mes sœurs,

à toute ma famille,

pour tous les petits de la famille,

à mes professeurs,

à tous ceux qui m'aiment,

à mes amis et à tous ceux que j'aime,

Bouaziz Khalil

Remerciment

Je tiens tout d'abord à remercier Dieu pour le don de la raison et pour avoir terminé ce travail.

En second lieu j'adresse mes remerciements à mon enseignant **Mr. Ladjelat Lahcene** pour son soutien continu avec ses conseils qui m'ont beaucoup aidé et sa patience tout au long de la période de recherche.

Je remercie le jury d'avoir lu et évalué mon mémo.

Je tiens à exprimer tout mes respects à mes parents mon père et ma mère, à mes sœurs , qui s'ont toujours encouragé.

J'exprime ici à toute la famille et mes amies.

Je remercie tous les professeure qui ont contribué à mon enseignement, notamment les professeure du département de mathématiques, sans oublier mes amis

Table des matières

INTRODUCTION GÉNÉRALE

Le théorème des points zéros de Hilbert, appelé "Nullstellensatz", est un théorème d'algèbre commutative. Il a été enoncé et démontré par le mathématicien allemand David Hilbert. Il est considérer parmi les resultats piliers dans les domaines d'Algebre commutative et Geométrie algébrique. Il constitut une extension du théoreme de Gauss D'Alembert connu par Le Théoreme Fondamental de l'Algebre; et realise un chemin de traduction entre la Geometrie et l'Algèbre, en construisant un lien entre les idéaux et les parties algébriques.

Dans ce mémoire, on s'intérèsse à l'étude du théorème des points zéros de Hilbert: D'abord on rappelle les notions de base nécéssaires à comprendre le théorème (anneau, idéal, partie algébrique d'un espace affine,...), ensuite on énonce le théorème dans ses deux formes: faible et forte avec les outils nécéssaires à la démonstration (lemme de Zariski, algèbre,...etc), enfin on cite quelques unes des applications du théorème dans les domaines d'Algèbre et Géométrie (idéaux maximaux, étude des parties algébriques ...etc).

Ce travail est composé de trois chapitre: Dans le premier chapitre, on rappelle les notions préliminaires fondamentales de l'Algèbre (anneaux, corps, ideaux d'un anneau, anneau noethériens,...etc), ces notions sont nécessaires pour comprendre les chapitres suivants de ce travail. On y mentionne quelques exemples pour expliquer mieux ces notions.

Le deuxième chapitre vise à présenter des concepts fondamentaux liés au théorème des points zéros et sa preuve. Pour cette raison on parle de sous-ensembles algébriques d'un éspace affines, et dun idéaux radicaux d'un anneau (en particulier anneau des polynômes), le théorème établit le liéu entre ces deux notions.

Enfin, le chapitre dernier énnonce le théorème des points zéros de Hilbert, en ses deux formes classique: Faible que répond à la question d'exestence de solution pour un système polynomial, et Forte qui permet de étudier des propriétes géométriques en s'aidant des notions algébriques et vise versa. On termine ce chpitre par la donnée de qulques applications des théorème de Hilbert en Géométrie et en Algèbre (détèrmination des idéaux maximaux de $k[X_1, ..., X_n]$, les zéros de l'ensemble vide,...,etc).

Chapitre 1

NOTIONS DE BASES

L'objectif de ce chapitre est de donner quelques notions d'algèbre commutative et élémentaire nécessaires par la suite.

1.1 Anneaux

Définition 1.1.1 *Un **anneau** est un ensemble non vide A muni de deux opérations internes " $+$ " et " $\cdot$ " tel que:*

1. $(A, +)$ *est un groupe commutatif.*
2. *La loi " $\cdot$ " est assosiative,i.e.* $\forall a, b, c \in A : a \cdot (b \cdot c) = (a \cdot b) \cdot c$
3. *La loi "$\cdot$" est distributive par rapport à "$+$": $a \cdot (b+c) = a \cdot b + a \cdot c$, et $(b+c) \cdot a = b \cdot a + c \cdot a$*

- Si de plus la loi " $\cdot$ "est commutative, on dit que *l'anneau* $(A, +, \cdot)$ est *commutatif.*
- Si A pussède un élément neutre pour la loi " $\cdot$ "on dit que A est **unitaire**, dans ce cas, on note 1_A ou simplement 1 cet élément et on l'appelle *unité de* A.

Exemple 1.1.1

1. $(\mathbb{Z}, +, \cdot)$ est un *anneau commutatif*.
2. $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un *anneau commutatif unitaire* d'élément *unité* $\overline{1}$.
3. $(M_n(\mathbb{R}), +, \cdot)$ l'ensemble des matrices carrés de type $n \times n$ sur $\mathbb{R}$ pour l'addition et la multiplication des matrices est un *anneau unitaire* d'unité
$$I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \vdots \\ \vdots & 0 & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$
non *commutatif.*
4. Les anneau des polynômes $\mathbb{Z}[X], \mathbb{Q}[X]$ et $\mathbb{R}[X]$ sont *anneaux.*

Définition 1.1.2 *Soit A anneau commutatif, on dit qu'un élément a de A est **inversible** dans A s'il existe un élément b de A tel que:*

$$a \cdot b = b \cdot a = 1$$

- On note par $\bigcup(A)$ l'ensemble dans éléments *inversibles* de A.

Exemple 1.1.2 *Les ensembles suivant possèdent des éléments inversibles*:

1. $\bigcup(\mathbb{Z}) = \{-1, 1\}$.
2. $\bigcup(\mathbb{Z}/n\mathbb{Z}) = \{\overline{x} \in \mathbb{Z}/n\mathbb{Z} : (x, n) = 1\}$.
3. $\bigcup(M_n(\mathbb{R})) = \{\mathrm{M} \in M_n(\mathbb{R}) : \det(\mathrm{M}) = 0\} = GL(n, \mathbb{R})$.
4. $\bigcup(\mathbb{C}) = \mathbb{C}^*$.

Définition 1.1.3 *Un anneau commutatif $(A, +, \times)$ est un anneau **intégre** si A ne posséde pas de diviseurs de zéro, c'est a dire:*

$$si\ a \cdot b = 0\ alors\ a = 0\ ou\ b = 0$$

Exemple 1.1.3

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$et $\mathbb{C}$ sont *anneaux intégres*.
2. $M_2(\mathbb{R})$ non *intégre* car: $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

sous anneau

Définition 1.1.4 *Soit A un anneau et B une partie de A, On dit que B est un **sous-anneau** de l'anneau A si $(B, +, \cdot)$ est un anneau.*

Proposition 1.1.1 *Soit A un anneau et B un partie non vide de A.B est **sous-anneau** de A si,et seulement, si:*

$$1)\ \forall a, b \in B : a - b \in B$$

$$2)\ \forall a, b \in B : a \cdot b \in B$$

Exemple 1.1.4 *$\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$.*

Remarque 1.1.1 *Un sous-anneau d'un anneau intègre est intègre.*

1.2 Corps

Définition 1.2.1 *Un* ***corps*** $(K, +, \times)$ *est un ensemble muni de deux lois internes possédant les propriétes suivantes:*

1. $(K, +, \times)$ *est un anneau.*
2. $0_k \neq 1_k$.
3. *Tout élément de* $K \setminus \{0_k\}$ *admet un inverse pour la loi* " $\times$ ".

- Un *corps* (K,+,×) s'appelle *commutatif* si l'opération "×" est *commutative.*

Exemple 1.2.1 *pour* $K = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ *et* $\mathbb{C}$:
les anneaux sont des corps commutatifs .

sous-corps

Définition 1.2.2 *Soit* K *un corps et* L *un partie de* K. *On dit que* L *est un* ***sous-corps*** *de* K *si:*

1. L *est un sous-anneau* de K.
2. $\forall x \in L \setminus \{0\} : x^{-1} \in L$.

autrement dit:

a) $L \neq \emptyset$

b) $xy^{-1} \in L^* \forall x, y \in L^*$.

c) $x - y \in L^* \forall x, y \in L^*$.

Exemple 1.2.2

1. $\mathbb{Q}$ est un *sous-corps* de $\mathbb{R}$.
2. $\mathbb{R}$ est un *sous-corps* de $\mathbb{C}$.

1.2.1 Corps algébriquement clos

Définition 1.2.3 *On dit qu'un* ***corps algébriquement clos*** *si tout polynôme non constant de $K[x]$ a une racine dans K.*

Théorème 1.2.1 ***(Thérème de Gauss D'alembert)***. *Le corps $\mathbb{C}$ des nombres complexes est algébriquement clos.*

Preuve. Soit $P \in \mathbb{C}[x]$ polynôme non constant.

supposons qu'il n'est pas de racin dans $\mathbb{C}$.

$P = a_n x^n + ... + a_0$,donc $a_n \neq 0$ et $n \geq 1$.

alors,si $z \in \mathbb{C}$ est de module >1, on a:

$$\begin{aligned} |P(z)| &\geq |a_n|\,|z|^n - (|a_0| + ... + |a_n - 1|)|z|^{n-1} \\ &\geq |z|^n \left(|a_0| - \frac{1}{|z|}(|a_0| + ... + |a_n - 1|\right) \end{aligned}$$

si $z \to +\infty \Rightarrow |P(z)| \to +\infty$

Il en résulte que la fonction $\frac{1}{|P|}$est holomorphe sur $\mathbb{C}$ (P ne s'annule pas) et bornée donc P constante,contradiction. ■

1.3 Idéaux

Définition 1.3.1 *Soient $(A, +, \times)$ un anneau et I une partie non vide de A. I est appelé un* ***idéal*** *de A si:*

1. $\forall x, y \in I : x - y \in I$.

2. $\forall a \in A, \forall x \in I$,on a: $xa = ax \in I$.

- Un *idéal* I de A qui n'est pas *égal* à A est appelé un *idéal* **propre** de A.

- A et $\{0_A\}$ sont des *idéaux* de A appelés *idéaux* **triviaux** de A.

Exemple 1.3.1

1. A *anneau* et $x \in A$, l'ensemble $(x) = \{ax : a \in A\}$ est un *idéal* de A, appelé (x) l'*idéal engendré* par x.

2. (x^2+1) l'*idéal engendré* par (x^2+1) dans $\mathbb{R}[x]$.

Proposition 1.3.1 *si un idéal I contient un élément inversible $x \in A$,alors on a $I = A$.*

Preuve. Soit $x \in A, x^{-1} \in A$ donc $1 = xx^{-1} \in I$ et soit $a \in A$ on a: $a = a \cdot 1 \in I$, d'ou $A = I$. ■

Idéal engendré par une partie

Définition 1.3.2 *Soit S une partie d'un anneau commutatif A, l'idéal engendré par une partie S est alors,* $(S) = \left\{ \sum_{i=1}^{n} s_i a_i : n \in \mathbb{N}, s_i \in S, a_i \in A \right\}$.

Exemple 1.3.2 *Soit A un anneau commutatif et $S \subset A$.*

a) Si $A = \mathbb{Z}$ et $S = \{2\}$, alors $(S) = (2) = 2\mathbb{Z}$
$T = (4, 6)$, alors $(T) = 4\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z}$

b) Si $A = K[x, y]$ et $S = \{x, y\}$,
$(S) = (x, y) = \{xf(x, y) + yg(x, y) : f, g \in K[x, y]\}$

Définition 1.3.3 *Un idéal I est de* ***type fini*** *s'il exist $S \subset A$, S fini et $I = (S)$ .dit que I engendré par une partie fini de A.*

1.3.1 Idéal premier

Définition 1.3.4 *Soit I un idéal de A(anneau commutatife unitaire), $I \neq A$. on dit que l'idéal I est* ***premier*** *si:*

$$\textit{pour tout } a, b \in A, \textit{ si } a \cdot b \in I, \textit{ alors } a \in I \textit{ ou } b \in I$$

Exemple 1.3.3

1. Soit $p \in \mathbb{N}^*$ un entier premier,dans l'*anneau* $(\mathbb{Z}, +, \times)$,l'*idéal* $(p) = p\mathbb{Z}$ est un *idéal premier.*

2. (0) est un *idéal premier* dans tout *anneau intègre.*

Théorème 1.3.1 *Dans un anneau commutatif unitaire A un idéal $I \neq A$ alors:*

$$I \textit{ est premier si et seulement si } A/I \textit{ est un anneau intègre}$$

Preuve. L'implication directe: on a

$$\begin{aligned}(a+I)(b+I) &= 0+I \Leftrightarrow ab+I = 0+I \\ &\Leftrightarrow ab \in I \\ &\Leftrightarrow a \in I \text{ ou } b \in I \\ &\Leftrightarrow a+I = I \text{ ou } b+I = I\end{aligned}$$

c'est-à-dire A/I est *intègre.*

L'implication inverse on a:

$$\begin{aligned}ab &\in I \Rightarrow ab+I = I = 0+I = (a+I)(b+I) \\ &\Rightarrow a+I = I \text{ ou } b+I = I \\ &\Rightarrow a \in I \text{ ou } b \in I \\ &\Rightarrow I \textit{ premier.}\end{aligned}$$

■

Exemple 1.3.4 *l'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre $\Leftrightarrow$ n premier.*

1.3.2 Idéal maximal

Définition 1.3.5 *Soit I un idéal de A non nul,$I \neq A$.on dit que l'idéal I est **maximal**,si pour tout J de A tel que: $I \subseteq J \subseteq A$, on a soit $J = I$ ou $J = A$*

Exemple 1.3.5

1. Soit $p \in \mathbb{N}^*$ un entier premier,dans l'*anneau* $(\mathbb{Z}, +, \times)$, l'*idéal* $p\mathbb{Z} = (p)$ est un *idéal maximal* .

2. Soient K *corps* et l'*anneau* $A = K[X]$, alors $I = (x)$ est un *idéal maximal* dans $K[X]$.
   Car: on a (x) *un idéal de* $A, (x) \neq A$ et $(x) \subseteq J \subseteq A, J$ *idéal* de A
   $A = K[X]$ *principal*,$J = (f(x))$ et $f \in K[X]$,

$$\begin{aligned}(x) \quad &\subseteq \quad (f(x)) \Longrightarrow f(x) \mid X \\ &\Longrightarrow \quad f(x) = X \text{ ou } f(x) = \lambda \in K^* \\ &\Longrightarrow \quad J = X, \text{ ou } J = (\lambda) = K[X](X = \lambda.(\lambda^{-1}.X) \ , X = X.1)\end{aligned}$$

Proposition 1.3.2 *Un idéal I d'un anneau A est maximal si,et seulement si,A/I est un corps.*

Preuve. Supposons que I est maximal,alors A/I est un anneau commutatif et unitaire.

si $\overline{a} \in A/I$ et $\overline{a} \neq \overline{0}$ i.e,$a \notin I$ alors l'idéal$(a) + I \neq I$,et $(a) + I = a$ car I maximal et $I \subsetneq (a) + I$,d'où $\exists r \in A, \exists i \in I$ tel que $1 = ra + i$,alors $\overline{1} = \overline{ra} = \overline{ra}$ dans A/I et ($\overline{i} = \overline{0}$ car $i \in I$)

ceci prouve que a est inversible dans A/I et que A/I est un corps.

D'autre part,si A/I est un corps,alors $A \neq I$.

soit J un idéal de A tel que $I \subsetneq J$ et soit $x \in J \setminus I$,alors, $\overline{x} \neq \overline{0}$ dans A/I d'où $\exists y \in A$ tel que $\overline{xy} = \overline{1}$ et donc $1 - xy \in I \subset J$ et $1 = (1 - xy) + xy \in J$ donc $J = A$. ■

Exemple 1.3.6

1. Tout idéal maximal est premier. Car: I maximal $\Rightarrow A/I$ corps $\Rightarrow A/I$ est un anneau integre $\Rightarrow I$ est premier.

2. Ia réciproque de 1) est engénéral fausse. Car par exemple:(0) est un idéal premier de $\mathbb{Z}$ mais n'pas maximal.

Exemple 1.3.7 *$I = n\mathbb{Z}$ idéal maximal de $\mathbb{Z} \Rightarrow \mathbb{Z}/n\mathbb{Z}$ corps $\Rightarrow$ n premier.*

1.4 Anneaux principaux

Définition 1.4.1 *Soit A anneau unitaire commutatif et intègre. l'idéal I est **principal** si:*

$$I = (a) : a \in A$$

Exemple 1.4.1 *Tout idéal $\mathbb{Z}$ de est principal.*

Définition 1.4.2 *On dit qu'un anneau est **principal** s'il est intègre et si tous ses idéaux sont principaux.*

Exemple 1.4.2

1. $\mathbb{Z}$ est un *anneau principal.*
2. *K* corps $\Leftrightarrow$ K$[X]$ est *principal.*

Définition 1.4.3 *Soit $p \in A$ un élément d'un anneau intègre A, $P \neq 0$. p est **irrédictible** si:*

a) $p \notin \sqcup(A) = A^*$.

b) Si $p = a \cdot b$,avec $a, b \in A$,alors $a \in A^*$ ou $b \in A^*$.

Théorème 1.4.1 *Soit $p \neq 0$ dans anneau principal A. p irrédictible si et selement si, l'idéal $pA = (p)$ est premier.*

Preuve. L'implication directe

si p irrédictible alors,pA maximal. Car $\exists a$ tel que $pA \subseteq aA, p = ab, a$ et b sont des élément inversibles et $aA = A$.

donc p premier

L'implication inverse

soit $p \neq 0$ et (p), si $p = bc$, alors $pc \in (p)$

supposons $c \in (p)$, donc $b \in (p)$ et $\exists d \in A$ tel que:

$b = dp$ donc $p = cdp$ comme A intègre,$cd = 1$ c'est-à-dire c et d sont des

éléments inversible donc p irrédictible. ■

Définition 1.4.4 ***(Anneau euclidiens)***

Soit A un anneau intègre et $\varphi : A \setminus \{0\} \longrightarrow \mathbb{N}$ un fonction tel que:

pour tout $a, b \in A \setminus \{0\}$, avec $b \neq 0$ il existe q et $r \in A$ tel que:

a) $a = bq + r$

b) $r = 0$ *ou* $\varphi(r) < \varphi(b)$.

alors, A est *euclidien.*

Exemple 1.4.3

1. l'anneau $\mathbb{Z}$ est *euclidien* avec $\varphi(x) = |x|$.
2. Si K un *corps*,alors $K[x]$ est un *anneau euclidien.*avec $\varphi(f) = \deg(f), f \in K[x]$.

Théorème 1.4.2 *Tout anneau euclidien est principal.*

Preuve. soit I un idéal non nul de l'anneau euclidien A $\exists a \in I$ tel que:

$\varphi(a) = \inf \{\varphi(y) \in \mathbb{N} \mid y \in I\}$, $\forall a \in I$ tel que :$x = aq + r$

si $r \neq 0 : \varphi(r) = \varphi(x - aq) < \varphi(a)$ impossible car $r \in I$

si $r = 0 : x = aq$ et $I = Aa = (a)$. ■

1.5 Anneau factoriel

Définition 1.5.1 *Soit A un anneau intègre. On dit que A est un anneau* ***factoriel*** *si:*

a) $\forall x \in A \backslash \sqcup(A)$ *non nul: x est le produit fini d'élément irrédictibles dans A:*
$x = p_1 p_2 ....p_k$,avec p_i *irrédictible* dans A $\forall i = \overline{1.k}$.

b) Si $x = q_1 q_2 ....q_s$:avec q_j *irrédictible* dans A $\forall j = \overline{1.s}$, alors $k = s$, et $\forall i = \overline{1.k}$,$\exists! j = \overline{1.k}$ tel que $q_j \sim p_i$.

Exemple 1.5.1 $\mathbb{Z}$ *est factoriel.*

Théorème 1.5.1 *Tout anneau principal est factoriel.*

Preuve. Soit $x \in A \backslash \sqcup(A), x \neq 0$
supposons que x ne peut etre écrit sans la forme produit d'irréductibles dans A.
$\Rightarrow x$ n'est pas irréductible.en particulair $x = a_1 \cdot b_1 : a_1 \notin \sqcup(A)$ et $b_1 \notin \sqcup(A)$
a_1 ou $b_1$ne peut etre écrit sans la forme produit d'irréductibles.
supposons que c'est a_1, on a $x = a_1 \cdot b_2, (x) \subsetneq (a_1)$
on applique le meme raisonnement avec $a_1 (a_1 \neq 0, a_1 \notin \sqcup(A))$
$\exists a_2 \neq 0, a_2 \notin \sqcup(A), a_2 \neq$le produit d'élément *irrédictible*, et $(a_1) \subsetneq (a_2), a_1 = a_2 b_2$.
En précédant de cett manière,on construit $a_3, a_4, ...$
$(a_1) \subsetneq (a_2) \subsetneqq (a_3)$.....
Posons, $I = \bigcup_{i \geqslant 0} (a_i)$
I est un *idéal* de A *principal*, $\exists a \in A$ tel que $I = (a)$
on a: $a \in I \Rightarrow \exists k \geqslant 0, a \in (a_k)$,donc $(a) \subseteq (a_k)$
on particulair $(a_{k+1}) \subseteq (a_k) \subseteq (a_{k+1})$
donc $(a_k) = (a_{k+1})$ contredit $(a_k) \subsetneq (a_{k+1})$ ■

Exemple 1.5.2 *K corps,$K[x]$ principal donc factoriel.*

1.6 Anneaux noethériens

Définition 1.6.1 *Un anneau commutatif dont tout idéal et de type fini,est on appelé anneau* ***noethérien****.*

Proposition 1.6.1 *Les condition suivantes sont équivalentes:*

a) *A est un anneau noethérien.*

b) *Tout suite croissante* $I_1 \subset I_2 \subset .... \subset I_n \subset ....$d'*idéaux de A est stationnaire,c'est-à-dire* $\exists N \in \mathbb{N}, n \geqslant N \Longrightarrow I_n = I_N$.

c) *Tout ensemble non vide* d'*idéaux de A posséde un élément maximal pour lnclusion.*

Preuve.

1) $\Longrightarrow$ 2)

Comme la suite I_n est croissant,la réunion

$I = \bigcup_{n\in\mathbb{N}} I_n$ est un idéal de la forme $I = (a_1, ..., a_k)$

donc $\exists N \in \mathbb{N}$ tel que $a_1....a_k \in I_N$ alors on a $I = I_N$.

2) $\Longrightarrow$ 3)

Soit E un ensemble non vide d'idéaux, suppossons que E n'ait pas d'élément maximal, alors par récurrence une suite $(I_n)n \in \mathbb{N}$ qui contrasté avec 2):

on prend $I_1 \in E$ quelconque et comme $I_1 \in E$ avec $I_1 \subsetneq I_2$.

3) $\Longrightarrow$ 1)

Soit I un idéal et $E = \{$idéaux J de $A\backslash J \ \subset I$ de type fini$\}$

$E \neq \emptyset$ car $(0) \in E$,soit J élément maximal de E et,si $J \neq I$,soit $a \in I - J$,alors $I + (a)$ est encore de type fini, contenu dans I et contient strictement J.

on a donc $J = I$ et I est bien de type fini. ■

Exemple 1.6.1

1. Un *anneau principal* est *noethérien.* Car tous les *idéaux* sont principaux donc de type fini.

2. L'*anneau* des polynomes $A = K[x_1, ..., x_n, ...]$ n'pas *noethérien* . Car on a une suite croissante non stationnaire d'*idéaux:* $(x_1) \subset (x_1, x_2) \subset ...$

3. $K[x_1, ...x_n]$ est *noethérien* (voir chapitre II).

Chapitre 2

Parties Algébriques d'un éspace affine

2.1 Ensemble algébrique

Définition 2.1.1 ***(Espace affine de dimension*** n*).* *Soit* K *un corps et* $n \geq 1$ *un entier naturel, on appelé espace affine de dimension* n *sur* K *l'ensemble*

$$K^n = \{(a_1, ..., a_n)/a_1, ..., a_n \in K\}.$$

- Un élément $(a_1, ..., a_n)$ de K^n est appelé un *point.*
- L'espace K^1est appelé la *droit affine.*
- L'espace K^2est appelé le *plan affine.*

Soient $x_1, x_2, .., x_n$ des indétèrminées sur K.On considère l'anneau $K[X_1, ..., X_n]$ des polynômes en $x_1, x_2, .., x_n$ sur K.

Pour $S \subset K[X_1, ..., X_n]$ on définit

$$V(S) = \{(a_1, ..., a_n) \in K^n : \forall f \in S \ , f(a_1, ..., a_n) = 0\}$$

Exemple 2.1.1 *Pour $n = 1$:*

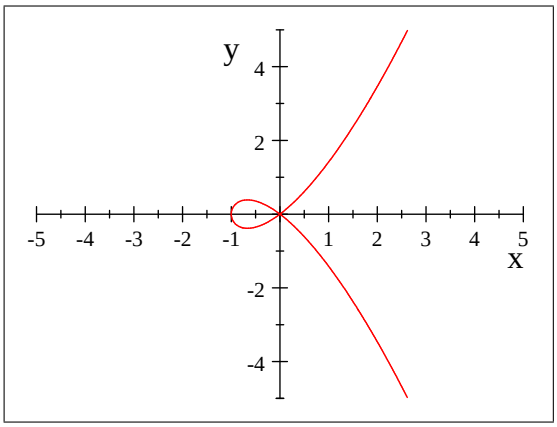
$$\begin{aligned} Si\ K &= \mathbb{R}, V(X^2+1) = 0 \\ Si\ K &= \mathbb{C}, V(X^2+1) = \{i, -i\} \end{aligned}$$

Définition 2.1.2 *Une partie $W \subset K^n$ est appelé une* ***partie algébrique*** *de K^n s'il existe $S \subset K[X_1, ..., X_n]$ tel que $W = V(S)$.*

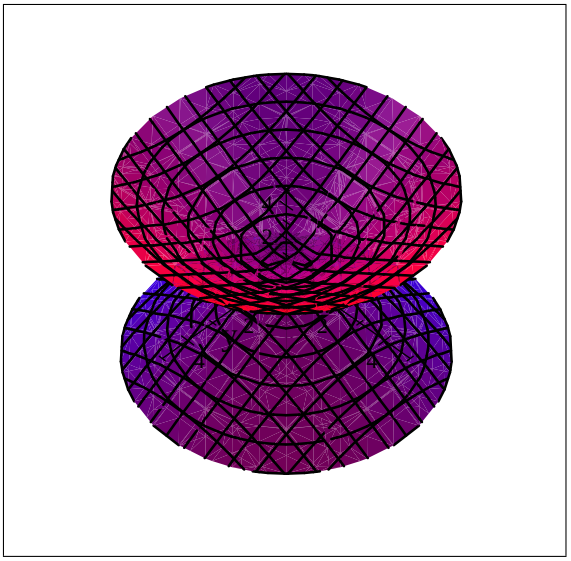
Exemple 2.1.2

1. $V(\{1\}) = \emptyset$ le vide est un *ensemble algébrique*.
2. $V(\{0\}) = K^n$ l'espace tout entier est un *ensemble algébrique*.
3. Si $K = \mathbb{R}$

a) $V(y^2 - x^2(x+1)) \subset \mathbb{R}^2$



b) $V(z^2 - (x^2 + y^2)) = 0 \subset \mathbb{R}^3$



Remarque 2.1.1

1. Soit S,$S^{'}$ deux parties de $K[X_1, ..., X_n]$. L'application :$S \mapsto V(S)$ est décroissante:

$$\text{Si } S \subset S^{'}, \text{ on a} V(S^{'}) \subset V(S).$$

2. Une intersection quelconque d'*ensembles algébriques* est un ensemble *algébrique*.
   En écrivant $\bigcap_i V(S_i) = V(\bigcup_i S_i)$

Proposition 2.1.1 *Pour tout $S \subset K[X_1, ..., X_n]$ on a:*

$$V(S) = V(\langle S \rangle)$$

Preuve. Est-ce que $V(S) \subset V(\langle S \rangle)$

On a $(a_1, ..., a_n) \in V(S)$ tel que $\forall f \in S, f(a_1, ..., a_n) = 0$ et soit $g \in \langle S \rangle$ qui s'écrit $\sum_{i=1}^{r} g_i f_i$ avec $f_i \in S$ et $g_i \in K[X_1, ..., X_n]$

est alors claire que $g(a_1, ..., a_n) = 0$

donc $(a_1, ..., a_n) \in V(\langle S \rangle)$.

Est-ce que$V(\langle S \rangle) \subset V(S)$

On a $\langle S \rangle \subset S$ par décroissante $V(\langle S \rangle) \subset V(S)$ ■

Proposition 2.1.2 *Une réunien finie d'ensembles algébriques est un ensemble algébrique.*

Preuve. Soit $V = V(I)$ et $V' = V(J)$, avec I, J deux idéaux

on a $V(I) \cup V(J) \subset V(IJ)$ clairement, soit $(a_1, ..., a_n) \in V(IJ)$, on suppose que $(a_1, ..., a_n) \notin V(I)$ et $\notin V(J)$, donc $\exists f \in I$ et $g \in J$ tel que $f(a_i) \neq 0$ et $g(a_i) \neq 0$, alors $(fg)(a_i) \neq 0$ mais $fg \in IJ$.contradiction. ■

2.2 Idéal d'un ensemble algébrique affine

Définition 2.2.1 *Soit X un ensemble de K^n .On appelé l'idéal de l'ensemble X l'ensemble:*

$$I(X) = \{f \in K[X_1, ..., X_n] : f(a_1, ..., a_n) = 0 \forall (a_1, ..., a_n) \in X\}$$

Exemple 2.2.1 *On a $I(\emptyset) = K[X_1, ..., X_n]$.*

Proposition 2.2.1 *L'ensemble $I(X)$ est un idéal.*

Preuve. L'ensemble $I(X)$ contient le polynômes nul, car il s'annule sur tous les points de K^n, donc en particulier sur tous les points de X.

soient f et g deux polynômes de $I(X)$ $\forall (a_1, ..., a_n) \in X$

on a:$(f+g)(a_1, ..., a_n) = f(a_1, ..., a_n) + g(a_1, ..., a_n) = 0+0 = 0$ et $f+g$ est un polynômes de $I(X)$,si de plus $h \in K[X_1, ..., X_n]$

$(hf)(a_1, ..., a_n) = h(a_1, ..., a_n)f(a_1, ..., a_n) = 0$,D'où $hf \in I(X)$

donc $I(X)$ est un idéal. ■

Proposition 2.2.2 *Si $f_1, ..., f_s$ sont des polynômes de $K[X_1, ..., X_n]$ alors,$\langle f_1, ..., f_s \rangle \subset I(V(f_1, ..., f_s))$.*

Preuve. Soit $f \in \langle f_1, ..., f_s \rangle$,alors $\exists$ une décomposition $f = h_1 f_1 + ... + h_s f_s$, où les h_i sont des polynômes de $K[X_1, ..., X_n]$

pour tout $(a_1, ..., a_n) \in V(f_1, ..., f_s)$

on a: $f_i(a_1, ..., a_n) = 0$,pour tout $i \in [1, s]$ par suite

$f(a_1, ..., a_n) = 0$,Ainsi f s'annule sur tous les points de $V(f_1, ..., f_s)$,ce que entraîne que $f \in I(V(f_1, ..., f_s))$. ■

Remarque 2.2.1

1. L'application :$X \mapsto I(X)$ est décroissante:

$$\text{Si } X \subset Y, \text{ ona } I(Y^{'}) \subset I(X).$$

2. Si V est un ensemble algebrique affine on a $V(I(V)) = V$.
   Car: il est clair que $V \subset V(I(V))$. Reciproquement, si $V = V(I)$, on a $I \subset I(V)$ et done $V = V(I) \supset V(I(V))$.

2.3 Le Radical d'un idéal

Définition 2.3.1 *Soit I un idéal d'un anneau commutatif $(A, +, \times)$. On définit le* ***radical*** *de I :*

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

Définition 2.3.2 *On dit que l'idéal I est un idéal radical si $\sqrt{I} = I$. C'est-à-dir:*

$$Si\ a^n \in I \Rightarrow I \in a.$$

Exemple 2.3.1

1. Dans $\mathbb{Z}$ si $I = 4\mathbb{Z}$ alors $\sqrt{I} = 2\mathbb{Z}$.

2. Dans $K[x]$ et K est *corps*,$I = (x^2)$ alors $\sqrt{I} = (x)$.

Proposition 2.3.1 *Soit I est un idéal de l'anneau A. Le radical de I est un idéal.*

Preuve. $\sqrt{I}$ contient I (prendre $n = 1$), donc n'est pas vide.

Soit a, b des éléments de $\sqrt{I}, n_0$ et m_0 deux indices tels que $a^n \in I$ et $b^0 \in I$,l'anneau étant commutatif,$(a-b)^{n_0+m_0} = \sum_{k=0}^{n_0+m_0} \binom{n_0+m_0}{K}(-1)^{n_0+m_0-k}a^k b^{n_0+m_0-k}$

Si $K \geq n_0, a^k b^{n_0+m_0-k} = a^{n_0}a^{k-n_0}b^{n_0+m_0-k} \in I$

Si $K < n_0$,alors $n_0 + m_0 - k > m_0$, donc de même $a^k b^{n_0+m_0-k} \in I$,

comme I est un *sous-groupe* de $(A, +)$, et $(a-b)^{n_0+m_0} \in I$ et donc $a - b \in I$.

Si $c \in A, (a \times c)^{n_0} = a^{n_0} \times c^{n_0} \in I$,donc $a \times b \in \sqrt{I}$

donc $\sqrt{I}$ est un idéal. ■

Proposition 2.3.2 *Soit I un idéal premier de A, alors I est radical.*

Preuve. Soit $x \in I$,pour n entier strictement positif,soit P_n la propriété:"*si* $x^n \in I$,*alors* $x \in I$ ". P_1 est vérifiée.

soit $n \geq 1$ un entier tel que P_n est vérifiée et on montre que P_{n+1} est vérifiée,

supposons $x^{n+1} \in I$,comme $x = x^n.x$ et I est un idéal premier,on a $x \in I$ ou $x^n \in I$:

dans le premier cas $(x \in I)$, P_{n+1} est vérifiée.

dans le second cas $(x^n \in I)$,d'après P_n ,P_{n+1} est vérifiée.

donc par récurrence,P_n est vraie pour tout n.

donc I radical. ■

Remarque 2.3.1

1. Soit I un *idéal*, $I \subset \sqrt{I}$. Car:on a $x^1 = x$ donc $x^1 \in I$ et donc $x \in \sqrt{I}$.
2. $\sqrt{\sqrt{I}} = \sqrt{I}$. Car: si $a^n \in \sqrt{I} \Longrightarrow a^{n\ s} = (a^n)^s \in I$, $\forall s$.

Théorème 2.3.1 *Soit I, J des idéaux radicaux de A, alors $I \cap J$ est un idéal radical de A.*

Preuve. On montre que $\sqrt{I \cap J} \subset I \cap J$

Soit $x \in \sqrt{I \cap J}$ et $n \in \mathbb{N}\backslash\{0\}$ tel que $x^n \in I \cap J$

En particulier on a: $x^n \in I$ donc $x \in \sqrt{I}$ et $\sqrt{I} = I$, donc $x \in I$, et $x^n \in J$ donc $x \in \sqrt{J}$ et $\sqrt{J} = J$, donc $x \in J$

alors $I \cap J$ est un idéal radical de A. ■

Exemple 2.3.2

1. $15\mathbb{Z} = 3\mathbb{Z} \cap 5\mathbb{Z}$ est un *idéal radical.*
   car: $3, 5$ sont premier, $3\mathbb{Z}$ et $5\mathbb{Z}$ sont des *idéaux* premier
   donc, $3\mathbb{Z} \cap 5\mathbb{Z}$ est un *idéal radical.*
2. $\{0\}$ est un *idéal radical.*
3. $\sqrt{I}$ est un *idéal radical* $(\sqrt{\sqrt{I}} = \sqrt{I})$.

2.4 Théorème de base de Hilbert

Théorème 2.4.1 ***(de base de Hilbert).*** *Si A est un anneau noethérien, alors l'anneau des polynômes $A[X]$ est noethérien.*

Preuve. Soit I un idéal de $A[X]$, il s'agit de montrer que I est de type fini.

Soit E l'ensemble des coefficients des termes de plus haut degré des éléments de I. Alors E est clairement un idéal de A, donc de type fini.

Soient $\{a_1, ..., a_n\}$ un système de générateurs et considérons les $f_i = a_i X^{r_i} + (\text{ termes de degré } < r_i) \in I$ qui ont donné naissance aux a_i. Soit encore $r = max\ r_i$ et $J \subset I$ l'idéal de $A[X]$ engendré par $f_1, ..., f_n$.

Montrons que, $\forall f \in I,\ \ f = g + h$ où $h \in J$ et $g \in I$ de degré $< r$. Si $\deg f < r$, il n'y a rien à démontrer. On peut donc supposer $m = \deg f \geq r$. Alors $f = ax^m + (\deg < m)$. Or $a \in E$, donc $a = \sum_i a_i u_i$.

Posons alors $g_1 = f - \sum_i u_i f_i X^{m-r_i}$. Ainsi $g_1 \in I$ et son degré $\deg g1 < m$, d'où, par récurrence descendante sur m, on peut écrire $f = g_j + h$ où $h \in J$ et $\deg g_j < r$. Il suffit alors de poser $g = g_j$.

Soit $M = A + AX + AX^2 + ... + AX^{r-1}$; c'est un A-module de type fini, donc noethérien et on a $I = J + I \cap M$. Or J est de type fini, donc I est de type fini. ■

Corollaire 2.4.1 *Si A est noethérien, alors $A[X_1, ..., X_n]$ noethérien.*

Chapitre 3

LE NULLSTELLENSATZ DE HILBERT ET APPLICATIONS

Dans ce chapitre, nous étudions le théorème des points zéros de Hilbert (dans ces deux formes: forme faible et forme forte) en commençant par la donnée de la preuve, citant quelques exemples, et enfin quelques applications du théorème qui nous permer de créer un pont entre l'algèbre et la géométrie.

3.1 Le Nullstellensatz de Hilbert

3.1.1 Théorème des points zéros(forme faible)

Lemme 3.1.1 ***(de zariski).*** *Soient k et K deux corps algébriquement clos et $k \subset K$. Si K est un k-algèbre de type fini, alors K est algébrique sur k, donc $K = k$.*

Preuve. Voir[8] ■

Théorème 3.1.1 *Soit k un corps algébriquement clos.*
Si J est un idéal propre de l'anneau $k[X_1, ..., X_n]$, alors $V(J) \neq \emptyset$.

- C.à.d. tout idéal propre J dans $k[X_1, ..., X_n]$ possède un zéro dans k^n.

Preuve. Soit un point $P = (a_1, ..., a_n) \in k^n$.on définit l'homomorphisme d'évalution en P

$ev_P : k[X_1, ..., X_n] \to k$

$f(X_1, ..., X_n) \mapsto f(P)$

Si $P \in V(J)$, alors $J \subset \ker ev_P$.

Eneffet.$P \in V(J)$ equivant à $f(P) = 0$ pour tout polynôme $f \in J$. Et comme

$$\begin{aligned} \ker ev_P &= \{g \in k[X_1, ..., X_n] : ev_P(g) = 0\} \\ &= \{g \in k[X_1, ..., X_n] : g(P) = 0\} \end{aligned}$$

il est clair que $J \subset \ker ev_P$.

Inversement, A tout homomorphisme de k-algèbres $\varphi : k[X_1, ..., X_n] \to k$ verifiant $J \in \ker \varphi$.on assosie un point $P = (\varphi(X_1), ..., \varphi(X_n))$ dans$V(J)$.

Pour démontre le Théorème,il suffit de prouver qu'il existe un homomorphisme de k-algébre $k[X_1, ..., X_n] / J \to k$ .....(1)

Si J idéal,$J \subset m$ (maximal).il suffit de prouver pour un idéal maximal m. $k \subset K = k[X_1, ..., X_n] / m$ est un corps,k-algébre de type fini engendré par $(X_1 + m, ..., X_n + m)$ alors K algébrique d'apres zariski $k = K$.donc (1) devenir

$$\begin{aligned} k[X_1, ..., X_n] / J &\to k[X_1, ..., X_n] / m \\ f + J &\mapsto f + m \end{aligned}$$

contient J dans son noyau. ■

3.1.2 Théorème des points zéros(la forme forte)

Théorème 3.1.2 *Soit k un corps algébriquement clos.*
Pour tout idéal J de $k[X_1, ..., X_n]$, alors $I(V(J)) = \sqrt{J}$.

- En particular. $I(V(J)) = J$ si J est *radical*.

Preuve. L'inclusion direct: montrons que $\sqrt{J} \subset I(V(J))$

Soit $h \in \sqrt{J}$, alors il existe un entier $s \in \mathbb{N}^*$ tel que $h^s \in J$. Pour $P \in V(J)$, on a $h^s(P) = 0$, et $h^s(P) = \underbrace{h(P).h(P)...h(P)}_{s \text{ fois}} = 0$. Comme k est un corps, cela entraîne que $h(P) = 0$.

Donc $\forall P \in V(J)$, $h(P) = 0$. C'est à dire $h \in I(V(J))$.

L'inclusion inverse: montrons que $I(V(J)) \subset \sqrt{J}$

On a $h \in I(V(J))$ c'est à dire $(h(p) = 0, \forall p \in V(J))$. Est ce qu'il existe un entier $N \geq 1$ tel que $h^N \in J$.

Supposons que $h \neq 0, J = (g_1, ..., g_m)$

considérons $\begin{cases} g_1(X_1, ..., X_n) = 0 \\ g_2(X_1, ..., X_n) = 0 \\ \vdots \\ g_m(X_1, ..., X_n) = 0 \\ 1 - yh(X_1, ..., X_n) = 0 \end{cases}$ $\begin{cases} m+1 \text{ equations} \\ n+1 \text{ inconnies} \end{cases}$

si $(a_1, .., a_n, b)$ verifie les m equations,alors $(a_1, .., a_n) \in V(J)$ donc $h(a_1, .., a_n) = 0$, et $(a_1, .., a_n, b)$ ne verifie pas la dernière equations. d'apre le théorème de point zéros(form faible) $\exists f_i \in k[X_1, ..., X_n]$ tel que $1 = \sum_{i=1}^{m} f_i g_i + f_{m+1}(1 - yh)$ dans l'anneau $k[X_1, ..., X_n]$.

En regardant cette indentité dans $k[X_1, ..., X_n][y]$ et en remplaçant y par h^{-1} on trouve

$$1 = \sum_{i=1}^{m} f_i(X_1, ..., X_n, h^{-1}) g_i(X_1, ..., X_n) .....(*)$$

dans $k[X_1, ..., X_n]$, $f_i(X_1, ..., X_n, h^{-1}) = \frac{\textbf{polynomial en } X_1,...,X_n}{h^{N_i}}$

soit $N = \max_{1 \leq i \leq m} \{N_i\}$

en mullipliant $(*)$ par h^N,on obtient

$$h^N = \sum_{i=1}^{m} (\text{polynomial en } X_1, ..., X_n) g_i(X_1, ..., X_n)$$

que montre $h^N \in J$. ■

Exemple 3.1.1 *Si $J = (X, Y^2)$ on a $I(V(J)) = (X, Y)$.*

3.1.3 Quelques Applications du Théorème Nullstellensatz

Proposition 3.1.1 *Pour tout partie $X \subset A^n$,l'ensemble $VI(X)$ est la plus petite partie algébrique contenant X. en particulaire $VI(X) = X \Leftrightarrow X$ est algébrique.*

Preuve. Soit V une partie algébrique contenant X.

On a: $V = V(J)$,J idéal de $k[X_1, ..., X_n]$ alors $J \subset I(X)$, d'où $V = V(J) \supset VI(X)$. ■

Théorème 3.1.3 *L'application $V : J \mapsto V(J)$ est une bijection (décroissante) de l'ensemble des idéaux radicaux de $k[X_1, ..., X_n]$ sur l'ensemble des parties algébriques de $k^n = A^n$.son inverse est l'application $I : X \longmapsto I(X)$.*

Preuve. On a:

$$\begin{aligned} IV(J) &= J \Leftrightarrow J \text{ idéal radical} \\ VI(X) &= X \Leftrightarrow X \text{ algébrique} \end{aligned}$$

donc V est une application bijective et $I = V^{-1}$. La décroissance de V est claire. ■

Remarque 3.1.1 *Les idéaux maximaux de $k[X_1, ..., X_n]$ sant exactement les idéaux de la form $(X_1 - a_1, ..., X_n - a_n)$.*

Soit $C = \{m \mid m \text{ idéal maximal de } k[X_1, ..., X_n] \text{ et } J \subset m\}$

Corollaire 3.1.1 *Si J est un idéal de $k[X_1, ..., X_n]$, alors*

$$\sqrt{J} = \bigcap_{m \in C} m$$

Preuve. J idéal de $k[X_1, ..., X_n]$

si m maximal,alors m est radical ($m = \sqrt{m}$)

si $J \subset m \Rightarrow \sqrt{J} \subset m$

$$\Rightarrow \sqrt{J} \subset \bigcap_{m \subset C} m \quad \ldots\ldots\ldots (1)$$

soit $P = (a_1, ..., a_n) \in K^n$, $m_P = (X_1 - a_1, ..., X_n - a_n)$ est un idéal maximal

$$f \in m_P \Leftrightarrow f(P) = 0$$

donc

$$J \subset m_P \Leftrightarrow P \in V(J)$$

.

si $f \in m_P$,pour tout $P \in V(J)$, alors $f \equiv 0$ sur $V(J)$,

d'où $f \in IV(J) = \sqrt{J}$,donc $\sqrt{J} \supset \bigcap_{P \subset V(J)} m_P \supset \bigcap_{m \subset C} m \quad \ldots\ldots\ldots (2)$

d'où l'egalité. ■

Application 1:

Soient A et B deux parties algébriques.

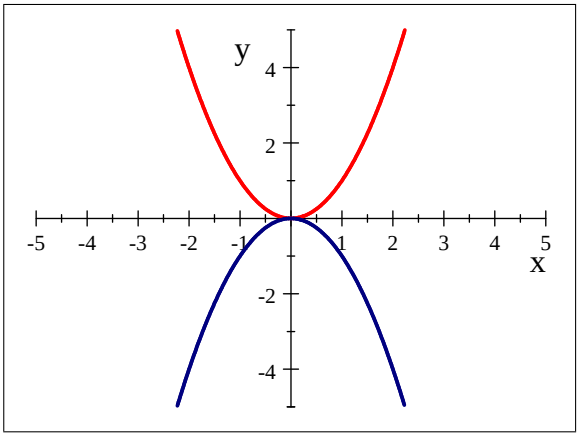
comme $A \cap B$ est la plus grande partie algébrique contenue dans A et B, l'ideal $I(A \cap B)$ doit être le plus petit idéal radical contenant à la foit $I(A)$ et $I(B)$:

c'est à dire

$$I(A \cap B) = \sqrt{I(A) + I(B)}$$

Exemple 3.1.2 *Soit $A = V(X^2 - Y)$ et $B = V(X^2 + Y)$ alors,$I(A \cap B) = \sqrt{(X^2, Y)} = (X, Y)$.*

$V(X^2 - Y) \cap V(X^2 + Y)$



En supposant la caractéristique$\neq$ 2, notez que $A \cap B = \{(0,0)\}$,mais lorsqu'il est rélisé comme l'intersection de $Y = X^2$ et $Y = -X^2$, il a la multiplicité 2.

Application 2:

$V(0) = k^n$

car: $I(k^n) = IV(0) = \sqrt{0} = 0$

Application 3:

on a $I(\{a_1, ..., a_n\}) = (X_1 - a_1, ..., X_n - a_n)$.

Preuve. L'inclusion $\supset$ est claire. Inversement, si on a $P(a_1, ..., a_n) = 0$ on divise P successivement par les $X_i - a_i$ et écrit ainsi: $P = (X_1 - a_1)\varphi_1 + ... + (X_n - a_n)\varphi_n + c$ avec $c \in k$ .mais c n'est autre que $P(a_1, ..., a_n)$,que est nul, donc $P \in (X_1 - a_1, ..., X_n - a_n)$. ■

Application 4:

Si $V(J) = \emptyset \Leftrightarrow J = k[X_1, ..., X_n]$.

Preuve. On a:

$$\begin{aligned} V(J) &= \emptyset \Leftrightarrow IV(J) = \sqrt{J} = I(\emptyset) = k[X_1, ..., X_n]. \\ &\Leftrightarrow 1 \in \sqrt{J} \Leftrightarrow 1 \in J \\ &\Leftrightarrow J = k[X_1, ..., X_n] \end{aligned}$$

■

Conclusion

Dans ce travail, on a essayé de faire une étude sur le théorème des points zéros de Hilbert, en expliquant les notions fondamentales nécéssaires pour l'établir. On conclut que ce théorème constitue une généralisation du théorème de Gauss-D'alembert pour un polynôme non constant sur $\mathbb{C}$*, et d'autre part représente un pont reliant l'algèbre et la géométrie.*

Bibliographie

[1] A. Chambert-Loir. Algebre commutative, lecture notes, 2001.

[2] A. Chambert-Loir, Algèbre corporelle, Ecole Polytechnique, 2005.

[3] C. Boulonne, M301 _ Algèbre commutative, 2009.

[4] C. Brookes, D. Mehrle, Commutative Algebra, Cambridge University Mathematical Tripos, Part III, Michaelmas 2016.

[5] D. Perrin, Cours d'algèbre, Ellipses Marketing, 1998.

[6] D. Perrin. Géométrie algébrique,Une introduction,Edp Sciences, 1995.

[7] D. Schaub, Elements d'algebre commutative, 2005.

[8] J. BOCHNAK, SUR LE THEOREME DES ZEROS DE HILBERT DIFFERENTIABLE, Topology Vol. 12, pp. 417-424. Pergamon Press. 1973. Printed in Great Britain.

[9] J. Querre, Cours d'algebre, Masson, 1976.

[10] J. S. Milne, Algebraic Geometry, (v6.02), 2017.

[11] Hilberts Nullstellensatz, https://en.wikipedia.org/wiki/Hilbert%27s_Nullstellensatz

[12] Hilberts Nullstellensatz and the Beginning of Algebraic Geometry https://www.ias.ac.in/public/Volumes/reso/004/08/0036-0057.pdf

[13] L. Ladjelat , Cours 1^{e} Master Discrète "courbe Algèbrique", Université M'sila , 2019 2020.

[14] R. Taillefer, Algèbre Commutative, 2012.

[15] S. Axler, F.W. Gehring, K.A. Ribet, Graduate Texts in Mathematics 211, Serge Lang Algebra, Springer-Verlag, New York, 2002.

ملخص

في هذه المذكرة، قمنا بتقديم دراسة عن نظرية هيلبرت للنقاط الصفرية في شكليها الضعيف والقوي. قمنا أولا بتذكير حول خصائص البنى الجبرية: الحلقة، الحقل، الحقل المغلق جبريا و المثالية، بعد ذلك قدمنا تعريف المجموعات الجبرية في فضاء تالفي على حقل تبديلي والمثاليات الجذرية (الراديكالية) لحلقة. واخبرا تأتي نظرية هيلبرت للربط بين المفهومين السابقين مع ذكرنا لبعض التطبيقات لهذه الأخيرة.

كلمات مفتاحية: الحلقة، الحقل المغلق جبريا، المثاليات الجذرية (الراديكالية)، المجموعات الجبرية.

Résumé

Dans ce mémoire, nous présent une étude sur le théorème des points zéros de Hilbert sous ses deux formes faible et forte. Nous commençons par rappeler des propriétes de quelques structures algébriques :anneau, corps, corps algébriquement clos et idéaux. Ensuite nous donnons les définitions et les propriétés des parties algébriques d'un espace affine et les idéaux radicaux d'un anneau. Enfin, le théorème de Hilbert est énoncé pour lier les deux notions précédentes, accompagné de quelques applications.

Mots clés : Anneau, Corps algébriquement clos, Les Idéaux radicaux et Les ensembles algébriques.

Abstract

In this memory, We present a study of The Hilbert's zeros points Theorem in its two forms: the weak and the strong. We start by recalling some properties of algebraic structures like: rings, fields, algebraically closed fields and radical ideals. After that we give definitions and properties of the algebraic subsets in affine space and the radical ideals in a ring. Finally, we state the Hilbert's theorem in order to built a link between the two precedent notions. In last we finish this work by giving some applications.

Key words: ring, algebraically closed fields, radical ideals and algebraic sets.