Feuille 10 – Théorème des zéros de Hilbert

Dans tous les exercices de cette feuille, K désigne un corps **algébriquement clos**.

Exercice 1. (Formulations équivalentes du *Nullstellensatz*) Démontrer l'équivalence entre les propositions suivantes :

— les idéaux maximaux de $K[X_1, \ldots, X_n]$ sont les $(X_1 - a_1, \ldots, X_n - a_n)$, où $(a_1, \ldots, a_n) \in K^n$;

— si J est un idéal strict de $K[X_1, \ldots, X_n]$, alors tous les polynômes de J ont une racine commune ;

— soient P_1, …, P_m des polynômes de $K[X_1, \ldots, X_n]$ et Q un polynôme s'annulant sur le lieu des zéros communs des P_i ; alors $Q \in \sqrt{(P_1, \ldots, P_m)}$ (voir la définition et les propriétés élémentaires du radical d'un idéal dans la feuille 1).

Exercice 2. (Anneaux de Jacobson) Un anneau A est dit de Jacobson si pour tout idéal I de A, le radical $\sqrt{I}$ est égal à l'intersection des idéaux maximaux de A qui contiennent I. L'objectif de l'exercice est de montrer que les anneaux $k[X_1, \ldots, X_n]$ et $k[\alpha_1, \ldots, \alpha_n]$ sont de Jacobson. Notons K la clôture algébrique du corps k.

1. (a) Montrer que $K[X_1, \ldots, X_n]$ est un anneau de Jacobson.
   (b) Soit $\mathfrak{m}$ un idéal maximal de $K[X_1, \ldots, X_n]$. Montrer que l'idéal $\mathfrak{m} \cap k[X_1, \ldots, X_n]$ est maximal dans $k[X_1, \ldots, X_n]$.
   (c) Montrer que $k[X_1, ..., X_n]$ est un anneau de Jacobson.
2. Soit $A = k[\alpha_1, \ldots, \alpha_n]$ un anneau de type fini sur k. Montrer que A est un anneau de Jacobson.

Exercice 3. (Ensembles algébriques affines) On appelle ensemble algébrique affine de K^n un ensemble de la forme :

$$\mathrm{V}(S) = \{\vec{x} \in K^n \mid \forall P \in S, P(\vec{x}) = 0\},$$

où S est un sous-ensemble de $K[X_1, \ldots, X_n]$. Si $V \subseteq K^n$ est un ensemble quelconque, on appelle idéal de V l'idéal :

$$\mathrm{I}(V) = \{P \in K[X_1, \ldots, X_n] \mid \forall \vec{x} \in V, P(\vec{x}) = 0\}.$$

Enfin, pour tout ensemble $V \subseteq K^n$, on pose $\Gamma(V) = K[X_1, \ldots, X_n]/\mathrm{I}(V)$.

1. Montrer que les applications $V \mapsto \mathrm{I}(V)$ et $S \mapsto \mathrm{V}(S)$ sont décroissantes.
2. Montrer que si V est un ensemble algébrique affine, on a $\mathrm{V}(\mathrm{I}(V)) = V$, et en déduire que l'application I est injective. A-t-on $\mathrm{I}(\mathrm{V}(I)) = I$ en général ?
3. Montrer que I définit une bijection décroissante, de réciproque V, entre les ensembles algébriques affines de K^n et les idéaux radicaux de $K[X_1, \ldots, X_n]$ (c'est-à-dire les idéaux J tels que $J = \sqrt{J}$).
4. Montrer qu'un ensemble algébrique affine V est un singleton si, et seulement si $\mathrm{I}(V)$ est un idéal maximal, si et seulement si $\Gamma(V) = K$.

Exercice 4. (Théorème d'Ax-Grothendieck) L'objectif de cet exercice est de démontrer qu'une application polynomiale $P : \mathbb{C}^n \to \mathbb{C}^n$ (c'est-à-dire dont toutes les coordonnées sont polynomiales) est injective si, et seulement si elle est bijective. On abrégera $(x_1, \ldots, x_n)$ en $\vec{x}$, et de même pour $(y_1, \ldots, y_n)$ qu'on écrira $\vec{y}$. Dans le même esprit, la lettre X désignera $(X_1, \ldots, X_n)$, et Y désignera $(Y_1, \ldots, Y_n)$.

1. Montrer que le théorème est vrai si l'on remplace $\mathbb{C}$ par un corps fini.
2. Notons P_i les coordonnées de P, supposée injective. À l'aide du *Nullstellensatz*, montrer que pour tout $j \in [\![1, n]\!]$, il existe un entier $r_j \geqslant 1$ et des polynômes $Q_{ij} \in \mathbb{C}[X, Y]$ tels que :

$$\forall (\vec{x}, \vec{y}) \in (\mathbb{C}^n)^2, \quad \sum_{i=1}^{n} (P_i(\vec{x}) - P_i(\vec{y})) \cdot Q_{ij}(\vec{x}, \vec{y}) = (x_j - y_j)^{r_j}.$$

3. Raisonnons par l'absurde, et supposons que P soit injective, sans pour autant être surjective. Soit $\vec{z_0} = (z_{01}, \dots, z_{0n}) \in \mathbb{C}^n$ tel que $P(\vec{x}) = \vec{z_0}$ n'ait pas de solution sur $\mathbb{C}^n$. Montrer qu'il existe des polynômes $R_i \in \mathbb{C}[X]$ tels que : $\forall \vec{x} \in \mathbb{C}^n, \quad \sum_{i=1}^{n} (P_i(\vec{x}) - z_{0i}) \cdot R_i(\vec{x}) = 1.$

   Soit $\mathbb{Z}[\mathcal{C}]$ le sous-anneau de $\mathbb{C}$ engendré par les coefficients des P_i, Q_{ij}, R_i et $\vec{z_0}$. Considérons $\mathfrak{M}$ un idéal maximal de $\mathbb{Z}[\mathcal{C}]$, et soit $k = \mathbb{Z}[\mathcal{C}]/\mathfrak{M}$.
4. On suppose que k est de caractéristique nulle. Montrer que sous cette hypothèse, $\mathbb{Q}$ doit avoir un nombre fini de générateurs. En déduire que k est de caractéristique $p > 0$.
5. Posons $\mathbb{Z}[\mathcal{C}] = \mathbb{Z}[\alpha_1, \dots, \alpha_m]$, où les α_m sont des nombres complexes. Soit J le noyau du morphisme surjectif $\overline{\mathbb{Z}/p\mathbb{Z}}[X_1, \dots, X_m] \to \bar{k}$, défini par $X_i \mapsto \alpha_i \bmod \mathfrak{M}$. Montrer que $\overline{\mathbb{Z}/p\mathbb{Z}}[X_1, \dots, X_m]/J$ est un corps isomorphe à $\overline{\mathbb{Z}/p\mathbb{Z}}$.
6. En déduire que les $\alpha_i \bmod \mathfrak{M}$ sont algébriques sur $\mathbb{Z}/p\mathbb{Z}$, puis que k est un corps fini. Conclure.

Exercice 5. On veut démontrer qu'une application polynomiale $P : \mathbb{C}^n \to \mathbb{C}^n$ involutive (c'est-à-dire : qui vérifie $P \circ P = \mathrm{Id}_{\mathbb{C}^n}$) admet nécessairement un point fixe.

1. Soient k un corps fini de caractéristique impaire et $\bar{k}$ sa clôture algébrique.
   (a) Montrer qu'une application polynomiale $P : k^n \to k^n$ involutive admet un point fixe.
   (b) Soit $P : \bar{k}^n \to \bar{k}^n$ involutive. En raisonnant sur une extension finie convenable de k, montrer que P admet un point fixe.
2. Raisonnons par l'absurde : soit $P = (P_1, \dots, P_n) : \mathbb{C}^n \to \mathbb{C}^n$ une application polynomiale involutive et sans point fixe. Montrer qu'il existe des polynômes $R_i \in \mathbb{C}[X_1, \dots, X_n]$ tels que :

$$\forall \vec{x} = (x_1, \dots, x_n) \in \mathbb{C}^n, \quad \sum_{i=1}^{n} (P_i(\vec{x}) - x_i) \cdot R_i(\vec{x}) = 1.$$

   Soit Λ le sous-anneau de $\mathbb{C}$ engendré par les coefficients des P_i et R_i. Considérons $\mathfrak{M}$ un idéal maximal de Λ, et soit $k_0 = \Lambda/\mathfrak{M}$.
3. Montrer que quitte à remplacer Λ par un anneau le contenant strictement, on peut supposer que la caractéristique de k_0 est impaire.
4. En déduire le résultat désiré.