1 Corps finis

1.1 Problème

L'objectif de cet exercice est de démontrer le théorème de Ax-Grothendieck dans des cas très particuliers, en utilisant les corps finis :

Théorème 1: Soit $P : \mathbb{C}^n \to \mathbb{C}^n$ une application polynomiale (*i.e.* toutes les coordonnées sont polynomiales). Si P est injective, alors P est bijective.

À l'avenir, on abrégera $(x_1, \dots, x_n)$ en $\vec{x}$, et de même pour $(y_1, \dots, y_n)$ qu'on écrira $\vec{y}$. Dans le même esprit, la lettre X désignera $(X_1, \dots, X_n)$, et Y désignera $(Y_1, \dots, Y_n)$.

Prérequis :
- anneaux-quotients, idéaux maximaux ;
- on admet que tout corps k admet une clôture algébrique, notée $\bar{k}$;
- $\mathbb{C}$ est un corps algébriquement clos.

1. Démontrer directement le cas où n égale 1 (Ce n'est pas nécessaire pour traiter l'exercice, et n'utilise pas les corps finis).
2. Démontrer le théorème en remplaçant $\mathbb{C}$ par un corps fini.
   À présent, on remplace $\mathbb{C}$ par $\bar{K}$ dans l'énoncé du théorème de Ax-Grothendieck, où $\bar{K}$ est la clôture algébrique d'un corps fini K.
3. Supposons que P est injective ; on veut prouver que P est surjective. Considérons $\vec{z_0}$ dans $\bar{K}^n$, et soit k le sous-corps de $\bar{K}$ engendré par les éléments de K, et par les coefficients de P et $\vec{z_0}$. Montrer que k est un corps fini, et en déduire le théorème « version $\bar{K}$ ».

   On se place enfin dans le cadre du théorème énoncé en introduction. Soit $P : \mathbb{C}^n \to \mathbb{C}^n$ une application polynomiale, qu'on suppose injective, et notons P_i ses coordonnées. On va traduire en termes algébriques le fait que P est injective : on veut montrer que pour tout $j \in [\![1, n]\!]$, il existe un entier $r_j \geqslant 1$ et des polynômes $Q_{ij} \in \mathbb{C}[X, Y]$ tel que :

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

   On aura besoin d'un lemme important :

   Lemme 2 (Théorème des zéros de Hilbert, ou *Nullstellensatz*): Soit J un idéal strict de $\mathbb{C}[X_1, \dots, X_n]$. Alors les polynômes de J ont une racine commune.

   Sa démonstration ne fait pas intervenir les corps finis, et fait l'objet des questions 4 à 6. On rappelle que pour tout idéal strict de $\mathbb{C}[X_1, \dots, X_n]$, il existe un idéal maximal $\mathfrak{M}$ de $\mathbb{C}[X_1, \dots, X_n]$ qui le contient. Posons $L = \mathbb{C}[X_1, \dots, X_n]/\mathfrak{M}$.
4. Montrer qu'il existe un morphisme de corps i de $\mathbb{C}$ dans L ; en particulier, i est injective, et quitte à remplacer $\mathbb{C}$ par $i(\mathbb{C})$ qui lui est isomorphe, on peut supposer $\mathbb{C} \subseteq L$. Montrer que la dimension de L en tant que $\mathbb{C}$-espace vectoriel est au plus dénombrable.
5. Montrer que les polynômes de $\mathfrak{M}$ ont au moins une racine commune dans L.
6. On veut montrer que $L = \mathbb{C}$. Justifier qu'il suffit de prouver que L est une extension algébrique de $\mathbb{C}$. En raisonnant alors par l'absurde, montrer que $L = \mathbb{C}$. En déduire que les polynômes de J ont au moins une racine commune (Indication : supposons qu'il existe un élément $x \in L$ transcendant sur $\mathbb{C}$; en considérant l'algèbre $\mathbb{C}(x)$, contredire la dénombrabilité de la dimension de L sur $\mathbb{C}$). On a donc prouvé le lemme.

7. Pour $j \in [\![1, n]\!]$, soit J_j l'idéal de $\mathbb{C}[X, Y, Z]$ engendré par les $P_i(X) - P_i(Y)$ et par $1 - Z(X_j - Y_j)$. Montrer que les polynômes de J_j n'ont pas de racine commune. En déduire l'existence de polynômes S_{ij} et T_j tels que

$$1 = \sum_{i=1}^{n} (P_i(X) - P_i(Y)) S_{ij} + (1 - Z(X_j - Y_j)) T_j .$$

8. En déduire l'existence des polynômes Q_{ij} annoncés dans l'énoncé (Indication : poser $Z = \frac{1}{X_j - Y_j}$).

   De la même manière, on va traduire algébriquement le fait que P n'est pas surjective.

9. Raisonnons par l'absurde, et supposons que P soit injective, sans pour autant être surjective. Soit $\vec{z_0} = (\vec{z_0}_1, \ldots, \vec{z_0}_n) \in \mathbb{C}^n$ 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 :

$$\forall \vec{x} \in \mathbb{C}^n, \quad \sum_{i=1}^{n} (P_i(\vec{x}) - \vec{z_0}_i) \cdot R_i(\vec{x}) = 1. \tag{2}$$

   (Indication : s'inspirer de la question 7, en remplaçant $P_i(X) - P_i(Y)$ par $P_i(X) - \vec{z_0}_i$)
   Soit $\mathbb{Z}[\mathcal{C}]$ le sous-anneau de $\mathbb{C}$ engendré par les entiers, par les coefficients des P_i, Q_i, R_i et $\vec{z_0}$. Considérons $\mathfrak{M}$ un idéal maximal de $\mathbb{Z}[\mathcal{C}]$. L'objectif des prochaines questions est de montrer que le quotient $k = \mathbb{Z}[\mathcal{C}]/\mathfrak{M}$ est un corps fini.

10. 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 $p > 0$. On peut alors écrire $\mathbb{Z}/p\mathbb{Z} \subseteq k$.

11. Posons $\mathbb{Z}[\mathcal{C}] = \mathbb{Z}[\alpha_1, \ldots, \alpha_m]$, où les α_m sont des nombres complexes. Justifier l'existence d'un morphisme surjectif de $\overline{\mathbb{Z}/p\mathbb{Z}}[X_1, \ldots, X_m]$ dans $\bar{k}$, défini par $X_i \mapsto \alpha_i \mod \mathfrak{M}$.

12. Soit J le noyau du morphisme défini ci-dessus. Montrer que $\overline{\mathbb{Z}/p\mathbb{Z}}[X_1, \ldots, X_m]/J$ est un corps, et qu'il est isomorphe à $\overline{\mathbb{Z}/p\mathbb{Z}}$.

13. En déduire que les $\alpha_i \mod \mathfrak{M}$ sont algébriques sur $\mathbb{Z}/p\mathbb{Z}$, puis que k est un corps fini. En déduire le théorème de Ax-Grothendieck « version $\mathbb{C}^n$ ».

1.2 Corrigé

1. Dans le cas où n égale 1, on a affaire à un polynôme de $\mathbb{C}[X]$, et il est suffisamment simple à décrire pour qu'on puisse expliciter sa forme en cas d'injectivité. Le fait que P est une application polynomiale bijective en découlera alors facilement. Supposons P injective. On a, pour tout $z \in \mathbb{C}$: $P(z) = \prod_{i=1}^{k} (z - a_i)$, où les a_i sont les racines complexes de P, éventuellement comptées avec multiplicité. S'il existe deux racines distinctes, alors $P(z) = 0$ a deux solutions complexes et ne peut pas être injective.
   Écrivons donc $P(z) = (z-a)^k$, et montrons que $k = 1$: le cas des paraboles, par exemple, suggère qu'un polynôme n'est pas injectif s'il est de degré supérieur à 2. En fait, on peut montrer que l'image réciproque d'un élément par un polynôme de degré k a, en général, k éléments ; les exceptions sont des *points de ramification* (ici, 0 est un point de ramification pour $z \mapsto (z-a)^k$), et cette notion se généralise à bien d'autres applications que les polynômes complexes. Pour le polynôme P de cette question, on peut résoudre directement une équation du type $P(z) = b$ où $b \in \mathbb{C}$, puisqu'on trouve alors

$$P^{-1}(\{b\}) = \{a + |b|^{1/k} e^{i\frac{2\pi l + \mathrm{Arg}(b)}{k}} ; l \in \mathbb{N}^*\},$$

   où $\mathrm{Arg}(b) \in]-\pi, \pi]$ est l'argument principal de b. Dès que b est non nul, cet ensemble a k éléments, donc l'injectivité de P impose $k = 1$. Ainsi, P est un polynôme du premier degré, et il devient clair qu'il définit une application polynomiale bijective.

2. Si $P : k^n \to k^n$ est injective, alors elle est bijective en tant qu'application entre deux ensembles finis de même cardinal. La nature polynomiale de P n'intervient pas ici.

3. Les coefficients de P et $\vec{z_0}$ sont dans $\bar{K}$, donc algébriques sur K. Si α est un de ces coefficients, alors $\dim_K(K(\alpha))$ est fini. Notons p_i les coefficients de P et $\vec{z_0}$. Alors, par la formule de multiplicativité des degrés et l'inégalité $\dim_L L(\alpha) \leqslant \dim_K K(\alpha)$ pour $K \subseteq L$ (à vérifier !), on a :

$$\dim_K(k) = \prod_{i=1}^{l} \dim_{K(p_1,\ldots,p_{i-1})}(K(p_1, \ldots, p_{i-1})(p_i)) \leqslant \prod_{i=1}^{l} \dim_K(K(p_i)),$$

où le terme $i = 1$ du premier produit est $\dim_K(K(p_1))$. Donc k est de dimension finie sur K, isomorphe en tant qu'espace vectoriel à $K^{\dim_K(k)}$, ce qui prouve que k est fini.

On a montré, en substance, qu'un corps de dimension finie (en tant qu'espace vectoriel) sur un corps fini est lui-même fini. Ce même argument permet de prouver que si L est une extension algébrique de K et M une extension algébrique de L, alors M est une extension algébrique de L.

À présent, considérons la restriction de P à ce corps k. Il est aisé de vérifier que son image est dans k^n, car un corps est stable par les différentes opérations intervenant dans un polynôme : addition et multiplication. L'application $P_{|k^n} : k^n \to k^n$ est toujours injective, donc bijective d'après la question 2. Ainsi, il existe $x \in k^n$ tel que $P(x) = z_0$, et comme k^n est inclus dans $\bar{K}^n$, on a prouvé la surjectivité de P.

En toute généralité, quand on travaille avec la clôture algébrique d'un corps fini, ou avec une extension algébrique d'un corps fini (éventuellement infinie), il est très efficace de se ramener à des corps finis en remarquant qu'il y a un nombre fini de quantités algébriques à manipuler, et c'est ce qu'illustre cette question. Ici, ces quantités sont les différents coefficients des polynômes en jeu, et z_0.

4. Il suffit de poser $i(z) = z$ pour $z \in \mathbb{C}$, et il est clair qu'on tient là un morphisme de corps bien défini de $\mathbb{C}$ dans L. Un morphisme de corps est toujours injectif, donc $\mathbb{C} \simeq i(\mathbb{C}) \subseteq L$. Comme un isomorphisme de corps conserve tous les résultats en rapport avec la structure de corps, on peut raisonner indifféremment sur $i(\mathbb{C})$ ou $\mathbb{C}$. On peut donc supposer que $\mathbb{C} \subseteq L$. Comme $\mathbb{C}[X_1, \dots, X_n]$ est de dimension au plus dénombrable [*], il est clair que L aussi : si on projette une base de $\mathbb{C}[X_1, \dots, X_n]$ sur $\mathbb{C}[X_1, \dots, X_n]/\mathfrak{M}$ grâce au morphisme surjectif qui s'impose (qui envoie X_i sur $X_i + \mathfrak{M}$), on obtient une famille génératrice de L.
5. L'élément $(X_1+\mathfrak{M}, \dots, X_n+\mathfrak{M}) = \pi(X_1, \dots, X_n)$ (π est le morphisme surjectif de la question précédente) est une racine de tout polynôme de $\mathfrak{M}$: en effet, si f est un tel polynôme, alors $f(X_1+\mathfrak{M}, \dots, X_n+\mathfrak{M}) = f(\pi(X_1, \dots, X_n)) = \pi(f(X_1, \dots, X_n) = 0$, l'avant-dernière égalité étant due à la définition d'un morphisme de corps, et la dernière égalité provenant du fait que $f \in \mathfrak{M} = \ker(\pi)$.
6. Comme $\mathbb{C}$ est algébriquement clos, toute extension algébrique de $\mathbb{C}$ lui est égale. Supposons qu'il existe un élément de $x \in L$ transcendant sur $\mathbb{C}$. L'application $\varphi_x : \begin{cases} \mathbb{C}[X] & \to & L \\ R & \mapsto & R(x) \end{cases}$ est un morphisme d'anneaux injectif, car x est transcendant, et on en déduit que $\mathbb{C}[X] \simeq \varphi_x(\mathbb{C}[X]) \subseteq L$, donc L contient une $\mathbb{C}$-algèbre isomorphe à $\mathbb{C}[X]$ et même à $\mathbb{C}(X)$ puisque L est un corps, et que $\mathbb{C}(X)$ est le corps de fractions de $\mathbb{C}[X]$, donc le plus petit corps au sens de l'inclusion à contenir $\mathbb{C}[X]$. Or $\mathbb{C}(X)$ est une $\mathbb{C}$-algèbre de dimension infinie : la famille $\left(\frac{1}{X-a}\right)_{a\in\mathbb{C}}$ est indénombrable et libre. En effet, pour toute somme finie vérifiant

$$\sum_{j=1}^{n} \frac{\lambda_j}{X - a_j} = 0,$$

il suffit de multiplier cette égalité par $X - a_{j_0}$ puis de l'évaluer en a_{j_0} pour obtenir $\lambda_{j_0} = 0$. Ainsi, L ne peut pas être de dimension au plus dénombrable, ce qui est absurde. Donc L est une extension algébrique de $\mathbb{C}$, puis $L = \mathbb{C}$.
7. Soit $(\vec{x}, \vec{y}, z)$ une racine commune des polynômes $P_i(X) - P_i(Y)$ et $1 - Z(X_j - Y_j)$. On a alors $P(\vec{x}) = P(\vec{y})$ et $1 = z(x_j - y_j)$. Mais, comme P est injective, la première égalité implique $\vec{x} = \vec{y}$ puis $x_j = y_j$, donc $1 = 0$: absurde. Donc l'idéal engendré par ces deux polynômes n'est pas strict, par le lemme, et égale $\mathbb{C}[X, Y, Z]$. En particulier, 1 appartient à cet idéal, et

∗. L'ensemble $\bigcup_{i\geqslant 0} B_i$, où B est l'ensemble des produits de monômes dont les puissances n'excèdent pas i, engendre cet espace vectoriel et est dénombrable comme union dénombrable d'ensembles finis.

comme il est engendré par les $P_i(X) - P_i(Y)$ et $1 - Z(X_j - Y_j)$, il existe des S_{ij} et T_j dans $\mathbb{C}[X, Y, Z]$ tels que

$$1 = \sum_{i=1}^{n} (P_i(X) - P_i(Y)) S_{ij} + (1 - Z(X_j - Y_j))\, T_j.$$

8. En posant $Z = \frac{1}{X_j - Y_j}$ comme indiqué, j'obtiens l'égalité suivante dans $\mathbb{C}[X, Y]$:

$$1 = \sum_{i=1}^{n} (P_i(X) - P_i(Y)) S_{ij} \left(X, Y, \frac{1}{X_j - Y_j} \right).$$

Je fixe un entier r qui dépasse le degré en Z des polynômes S_{ij}. Si on écrit $S_{ij} = \sum_{k=0}^{r} S_{ijk}(X, Y) Z^j$, alors multiplier l'égalité ci-dessus par $(X_j - Y_j)^r$ donne :

$$(X_j - Y_j)^r = \sum_{i=1}^{n} (P_i(X) - P_i(Y)) \cdot \sum_{k=0}^{r} S_{ijk}(X, Y)\, (X_j - Y_j)^{r-k},$$

et poser $Q_{ij} = \sum_{k=0}^{r} S_{ijk}(X, Y)\, (X_j - Y_j)^{r-k}$ pour tout $i \in [\![1, n]\!]$ permet de répondre à la question.

Ainsi, de l'information géométrique suivante : « P est injective », qui dit que le lieu commun des zéros des polynômes de $\mathbb{C}[X, Y]$ définis par les $X_j - Y_j$ contient le lieu commun des zéros des polynômes $P_i(X) - P_i(Y)$, on a obtenu un énoncé algébrique, *via* un système d'équations, qui traduit précisément l'obstruction géométrique à la non injectivité de P. Ce genre de résultat est typique de ce qu'on peut rencontrer en *géométrie algébrique*.

9. On peut répondre à la question en reproduisant le schéma des questions précédentes. Il suffit de considérer l'idéal engendré par les $P_i(X) - \vec{z_0}_i$: il n'y a pas de zéro commun à ces polynômes, sinon $P(\vec{x}) = \vec{z_0}$ aurait une solution. Par le lemme, cet idéal égale tout l'anneau, et en particulier 1 appartient à cet idéal, et on en déduit l'égalité de l'énoncé.

10. Si k est de caractéristique nulle, il existe alors un morphisme injectif de $\mathbb{Q}$ dans k, et $\mathbb{Q}$ est isomorphe à un sous-corps de k. Comme l'algèbre $\mathbb{Z}[\mathcal{C}]$ a clairement un nombre fini de générateurs sur $\mathbb{Z}$ (par construction), on en déduit que k, puis $\mathbb{Q}$ aussi. Mais ce qu'on sait être faux ; on en déduit une contradiction. Bref, notre assertion de départ étant fausse, on en déduit que k est de caractéristique strictement positive p, et ceci équivaut à l'inclusion $\mathbb{Z}/p\mathbb{Z} \subseteq k$.
11. (Rédaction à venir)
12. (Rédaction à venir)
13. La question précédente montre que les $\alpha_i \mod \mathfrak{M}$ appartiennent à la clôture algébrique de $\mathbb{Z}/p\mathbb{Z}$, donc sont algébriques sur $\mathbb{Z}/p\mathbb{Z}$. Comme ils engendrent $\mathbb{Z}[\mathcal{C}]/\mathfrak{M} = k$, on en déduit que k est un corps fini par le même raisonnement que dans la question 3. Voici comment on peut, finalement, démontrer le théorème de Ax-Grothendieck : on a vu que si $P : \mathbb{C}^n \to \mathbb{C}^n$ est injective et non surjective, elle induit des relations (1) et (2) qui sont en fait valables dans $\mathbb{Z}[\mathcal{C}]$ par définition de cet anneau, puis dans k par passage au quotient. Grâce à ces mêmes relations, on est assuré que $P : k^n \to k^n$ est injective (relation (1)) et non surjective (relation (2)), ce qui contredit le résultat de la question 2. Par l'absurde, $P : \mathbb{C}^n \to \mathbb{C}^n$ est injective et surjective, ce qu'énonce le théorème désiré.