TD n°7.

1 Nullstellensatz

Exercice 1. Soient $f_1, \cdots f_m \in \mathbb{C}[X_1, \cdots, X_n]$.

a) Montrer que si l'idéal $I := (f_1, \cdots, f_m)$ de $\mathbb{C}[X_1, \cdots, X_n]$ est propre, alors le système d'équations $f_i(z) = 0$, $i = 1, \cdots, m$ admet une solution $z = (z_1, \cdots, z_n)$ dans $\mathbb{C}^n$.

b) Soit $V \subset \mathbb{C}^n$ l'ensemble des solutions comme ci-dessus. On dit qu'une fonction $V \longrightarrow \mathbb{C}$ est *polynômiale* si c'est la restriction à V d'une fonction polynômiale sur $\mathbb{C}^n$ (donc donnée par évaluation d'un polynôme $g \in \mathbb{C}[X_1, \cdots, X_n]$). Notons $\mathcal{O}(V)$ la $\mathbb{C}$-algèbre des fonctions polynômiales sur V. Montrer que $\mathcal{O}(V) \simeq \mathbb{C}[X_1, \cdots, X_n]/\sqrt{I}$.

c) Soit $V' \subset \mathbb{C}^{n'}$ un autre ensemble algébrique. On dit qu'une application $V \longrightarrow V'$ est polynômiale si elle est restriction d'une application $\mathbb{C}^n \longrightarrow \mathbb{C}^{n'}$ polynômiale. Montrer que

$$\{\text{App. Pol. } V \longrightarrow V'\} \simeq \mathrm{Hom}_{\mathbb{C}-\mathrm{alg}}(\mathcal{O}(V'), \mathcal{O}(V)).$$

Exercice 2 (Normalisation de Noether)**.** Soit k un corps et A une k-algèbre de type fini. On veut montrer qu'il existe une sous-k-algèbre A' de A telle que

— A est un module de type fini sur A'.
— A' est isomorphe à une algèbre de polynômes $k[X_1, \cdots X_d]$ sur k.

a) Soit $f \in k[Y_1, \cdots, Y_m]$ un polynôme non nul. Montrer que pour $r \in \mathbb{N}$ assez grand, le polynôme

$$\widetilde{f}(Y_m) = f(Y_1 + Y_m^{r^{m-1}}, Y_2 + Y_m^{r^{m-2}}, \cdots, Y_{m-1} + Y_m^r, Y_m) \in k[Y_1, \cdots, Y_{m-1}][Y_m]$$

est unitaire à un facteur inversible près.

b) Soient $y_1, \cdots, y_m$ des générateurs de la k-algèbre A. Si A n'est pas isomorphe à une algèbre de polynôme, montrer qu'il existe $f \in k[Y_1, \cdots, Y_m]$ tel que $f(y_1, \cdots, y_m) = 0$ dans A. Prenons alors r comme dans la question précédente et posons $z_i := y_i - y_1^{r^{m-i}}$ pour $i = 1, \cdots, m-1$. Montrer que A est un module de type fini sur la sous-algèbre $A_1 := k[z_1, \cdots, z_{m-1}]$ engendrée par $z_1, \cdots, z_{m-1}$.

c) Prouver l'énoncé souhaité.

2 Quelques extensions non algébriques

Exercice 3. Soit k un corps et $K = k(X)$.

a) Montrer que K n'est pas de type fini en tant que k-algèbre.

b) Soit $F \in K \backslash k$. On écrit $F = \frac{P(X)}{Q(X)}$, avec $P, Q \in k[X]$ premiers entre eux.

i) Montrer que X est algébrique sur $k(F)$ (on pourra considérer $R(T) := P(T) - FQ(T) \in k(F)[T]$).

ii) En déduire que F est transcendant sur k.

iii) Montrer que $[K : k(F)] = \max(\deg(P), \deg(Q))$ (on pourra montrer que $R(T)$ est irréductible dans $k[F][T]$).

c) Soit $\phi : \mathrm{GL}_2(k) \to \mathrm{Aut}_k(K)$ le morphisme de groupe défini par

$$\phi \begin{pmatrix} a & b \\ c & d \end{pmatrix} (R) = R\left(\frac{aX + b}{cX + d}\right).$$

Montrer que ϕ est surjectif, et que $\mathrm{Ker}(\phi) = k^\times$.

Exercice 4. Soit $f \in \mathbb{C}[T]$ unitaire de degré 3, de racines $z_1, z_2, z_3 \in \mathbb{C}$.

a) Montrer que $K = K_{z_1,z_2,z_3} := \mathbb{C}(X)[T]/(X^2 - f(T))$ est un corps de degré de transcendance 1 sur $\mathbb{C}$. Calculer $[K : \mathbb{C}(X)]$ et $[K : \mathbb{C}(T)]$.

b) Si $z_1 = z_2$, montrer que K est transcendant pur engendré par $\frac{X}{T-z_1}$.

c) Supposons les z_i distincts deux à deux. Montrer qu'il existe $\lambda \in \mathbb{C} \setminus \{0, 1\}$ tel que $K_{z_1,z_2,z_3} \simeq K_{0,1,\lambda}$.

d) Montrer que $K_{0,1,\lambda}$ n'est pas transcendant pur, si $\lambda \neq 0, 1$.

Exercice 5. Soit p un nombre premier, et notons $K := \mathbb{F}_p(X, Y)$.

a) Montrer que $K^p := \{x^p, x \in K\}$ est un sous corps de K et que $[K : K^p] = p^2$.

b) Montrer que pour tout $x \in K$, le degré du polynôme minimal de x sur K^p est inférieur à p. En déduire que l'extension $K^p \subset K$ n'est pas monogène.

3 Quelques polynômes irréductibles

Exercice 6. Soit $n \in \mathbb{N}^*$. Soit $\Phi_n = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} (X - e^{2i\pi k/n}) \in \mathbb{C}[X]$.

a) Montrer que $X^n - 1 = \prod_{d|n} \Phi_d$. En déduire que $\Phi_n \in \mathbb{Z}[X]$.

b) Soit ζ une racine primitive n^{e}de 1 et p un nombre premier premier à n. Soit f et g les polynômes minimaux unitaire sur $\mathbb{Q}$ de ζ et $\zeta' = \zeta^p$. On suppose $f \neq g$. Montrer que $fg|\Phi_n$ et $f|g(X^p)$.

c) Montrer que l'image de Φ_n dans $\mathbb{F}_p[X]$ a un facteur irréductible ayant multiplicité au moins deux, et en déduire une contradiction.

d) En déduire que Φ_n est un polynôme irréductible dans $\mathbb{Q}[X]$.

Exercice 7. Soit p un nombre premier et $a \in \mathbb{F}_p$. Soit $P = X^p - X - a \in \mathbb{F}_p[X]$.

a) Si $a = 0$, donner la décomposition en facteur irréductible de P. On suppose dorénavant $a \neq 0$.

b) Montrer que $P(X + 1) = P(X)$.

c) Soit Q un facteur irréductible de P. Montrer que $Q(X + 1)$ est aussi un facteur irréductible de P.

d) Montrer que $Q(X + 1) = Q(X)$ (on pourra considérer une action de $\mathbb{Z}/p\mathbb{Z}$ sur l'ensemble des facteurs irréductibles de P).

e) Montrer que si $R \in \mathbb{F}_p[X]$ est de degré $\leqslant p - 1$ et $R(X + 1) = R(X)$, alors R est un polynôme constant.

f) En déduire que P est irréductible.

g) Soit $b \in \mathbb{Z}$ premier à p. Montrer que $X^p - X - b$ est un polynôme irréductible de $\mathbb{Q}[X]$.