# TD n°5.

## Géométrie algébrique

**Exercice 1.** Soient $F, G \in \mathbb{C}[X,Y]$ tels que $\text{pgcd}(F,G) = 1$.

a) Montrer qu'il existe $A, B \in \mathbb{C}[X,Y]$ tel que $AF + BG$ soit un polynôme non nul de $\mathbb{C}[X]$.

b) Montrer que $\mathcal{V}(F,G) := \{(x,y) \in \mathbb{C}^2, F(x,y) = G(x,y) = 0\}$ est un ensemble fini.

c) Montrer que $\mathbb{C}[X,Y]/(F,G)$ est un $\mathbb{C}$-espace vectoriel de dimension fini.

d) Décrire tous les idéaux premiers de $\mathbb{C}[X,Y]$.

**Exercice 2.** On dit qu'une sous-variété $V$ de $\mathbb{C}^n$ est irréductible si pour toutes sous-variétés $V_1, V_2$ de $\mathbb{C}^n$ telles que $V_1 \cup V_2 = V$, alors $V = V_1$ ou $V = V_2$.
Montrer que $V$ est irréductible si et seulement si $\mathcal{I}(V) := \{P \in \mathbb{C}[X_1,\ldots,X_n], \forall x \in V, P(x) = 0\}$ est un idéal premier (si $fg \in \mathcal{I}(V)$, on pourra montrer que $V = \mathcal{V}((\mathcal{I}(V), f)) \cup \mathcal{V}((\mathcal{I}(V), g))$).

**Exercice 3. Composantes irréductibles**
Soit $V$ une sous-variété de $\mathbb{C}^n$. Montrer qu'il existe des sous-variétés irréductibles $V_1, \cdots, V_n$ telles que $V = V_1 \cup \cdots \cup V_n$ (on pourra par l'absurde considérer un idéal maximal de $\mathbb{C}[X_1,\cdots,X_n]$ tel que $\mathcal{V}(I)$ n'admette pas de telle décomposition).
Montrer que si on suppose que $V_i \not\subseteq V_j$ pour $i \neq j$, alors cette décomposition est unique à réordonnement près des $V_i$ (on pourra commencer par montrer que si $W$ est une sous variété irréductible telle que $W \subset V_1 \cup \cdots \cup V_n$ alors il existe $i$ tel que $W \subset V_i$).

**Exercice 4.** Soit $A$ un anneau noethérien et $I$ un idéal réduit (c'est-à-dire $I = \sqrt{I}$). On veut montrer qu'il existe des idéaux premiers $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ de $A$ tels que $I = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$
Suppsons par l'absurde qu'il existe un idéal réduit qui n'est pas intersection fini d'idéaux premiers, $I_0$ maximal (justifier l'extistence d'un tel $I_0$).

a) Montrer qu'il existe $a, b \notin I_0$ tels que $ab \in I_0$. On note $J = I_0 + aA$ et $K = I_0 + bA$.

b) Montrer que $JK \subset I_0 \subset J \cap K$.

c) Montrer que $I_0 = \sqrt{J} \cap \sqrt{K}$.

d) En déduire une contradiction.

**Exercice 5. Topologie de Zariski** Montrer que l'ensemble $\{\mathbb{C}^n - V, V$ sous-variété algébrique fermé de $\mathbb{C}^{\}}$ est une topologie sur $\mathbb{C}^n$, moins fine que la topologie usuelle.

**Exercice 6.** Soit $\mathfrak{m}$ un idéal maximal de $A := \mathbb{R}[X_1,\cdots,X_n]$. Montrer que $A/\mathfrak{m}$ est isomorphe à $\mathbb{R}$ où $\mathbb{C}$.

**Exercice 7.** Soit $I$ un idéal maximal de $\mathbb{R}[X_1,\cdots,X_n]$. Montrer que $\mathcal{V}(I)$ est réduit à un point ou est vide. Donner un exemple où $\mathcal{V}(I)$ est vide.

**Exercice 8.** Soit $A = \mathbb{C}[X_1,\cdots,X_n]$. Soient $I, J$ deux idéaux de $A$. Si $x \in \mathbb{C}^n$, on note $\mathfrak{m}_x = \{P \in A, P(x) = 0\}$.

a) Montrer que $x \in V(I)$ si et seulement si $I \subset \mathfrak{m}_x$.

b) Montrer que $\mathcal{V}(I) = \emptyset$ si et seulement si $I = A$.

c) Montrer que $I + J = A$ si et seulement si $\mathcal{V}(I) \cap \mathcal{V}(J) = \emptyset$.

**Exercice 9.** Soit $I$ un idéal de $A := \mathbb{C}[X_1,\cdots,X_n]$. Soit $J = \mathcal{I}(\mathcal{V}(I))$.

a) Montrer que $\sqrt{I} \subset J$ et $\sqrt{J} = J$.

b) Soit $f \in J$. On considère l'idéal $J_0$ de $A[T]$ engendré par l'image de $I$ et $1 - fT$. Montrer que $\mathcal{V}(J_0) = \emptyset$.

c) En déduire que $1 - fT$ est inversible dans $A/I[T]$.

d) En déduire que $f \in \sqrt{I}$ (voir dm2).

**Exercice 10.** Soient $V \subset \mathbb{C}^n$ et $W \subset \mathbb{C}^m$ deux sous-variétés affines. Une fonction $f : V \to W$ est appelée application régulière de $V$ vers $W$ s'il existe $P_1, \cdots, P_m \in \mathbb{C}[X_1, \cdots, X_n]$ tels que $f(x_1, \cdots, x_n) = (P_1(x_1, \cdots, x_n), \cdots, P_m(x_1, \cdots, x_n)$ pour tout $(x_1, \cdots, x_n) \in V$. On note $\mathrm{Hom}_{\mathrm{Aff}}(V, W)$ l'ensemble des applications régulières de $V$ vers $W$.
On note $\mathcal{A}(V) = \mathbb{C}[X_1, \cdots, X_n]/\mathcal{I}(V)$.

a) Montrer que si $f : V_1 \to V_2$ et $g : V_2 \to V_3$ sont des applications régulières, alors $gf$ est une application régulière.

b) Montrer que $\mathrm{Hom}_{\mathrm{Aff}}(V, \mathbb{C})$, muni de la multiplication $(f \cdot g)(x) = f(x) \times g(x)$, est une $\mathbb{C}$-algèbre, isomorphe à $\mathcal{A}(V)$.

c) Construire une bijection $\mathrm{Hom}_{\mathrm{Aff}}(V, W) \to \mathrm{Hom}_{\mathbb{C}\text{-Alg}}(\mathcal{A}(W), \mathcal{A}(V))$.

**Exercice 11.** Soit $V = \{(t^3, t^4, t^5) \in \mathbb{C}^3, t \in \mathbb{C}\}$. Montrer que $V$ est une sous-variété irréductible de $\mathbb{C}^3$ (on pourra décrire $\mathcal{I}(V)$ comme le noyau d'un morphisme $\mathbb{C}[X, Y, Z] \to \mathbb{C}[T]$).

# Polynômes et extensions de corps

**Exercice 12.** Soit $p$ un nombre premier.

a) Donner la décomposition en facteurs irréductibles de $P = X^p - 1 \in \mathbb{Q}[X]$ (on pourra considérer $P(X+1)$).

b) Calculer $[\mathbb{Q}(\zeta_p) : \mathbb{Q}]$ où $\zeta_p$ est une racine primitive $p^{\mathrm{e}}$ de 1.

c) Calculer $[\mathbb{Q}(\cos(2\pi/p) : \mathbb{Q}]$.

**Exercice 13.** Soit $P$ le polynôme $X^3 + X^2 + X - 1 \in \mathbb{F}_3[X]$. On note $K$ l'anneau quotient $\mathbb{F}_3[X]/(P)$ et $\alpha$ la classe de $X$ modulo $(P)$.

a) Montrer que $K$ est un corps.

b) Quels sont les ordres multiplicatifs possibles des éléments de $K^*$ ?

c) On dit qu'un élément de $K$ est dit primitif s'il est générateur du groupe multiplicatif $K^*$.

   i) Montrer que $K$ admet un élément primitif.

   ii) Combien existe-t-il d'éléments primitifs de $K$ ?

   iii) Soit $x$ un élément de $K^*$ distinct de $-1$. Montrer que $x$ est primitif si et seulement si $x^{13} = -1$.

   iv) Soit $x$ est un élément de $K^*$ distinct de $-1$ et 1. Montrer que $x$ ou $-x$ est primitif.

d) On pose $\beta = \alpha(1 - \alpha)$.

   i) Vérifier que $\beta^2 = \alpha$.

   ii) Quel est l'ordre de $\alpha$ ? En déduire que $-\alpha$ est primitif.

**Exercice 14.** On pose $P = X^4 + X + 1 \in \mathbb{F}_2[X]$ et $K = \mathbb{F}_2[X]/(P)$. On note $\alpha$ la classe de $X$ modulo $(P)$.

a) Montrer que $K$ est un corps et déterminer son cardinal.

b) Montrer que $K$ admet un élément primitif.

c) Quel est l'ordre de $\alpha$ dans le groupe $K^*$ ?

d) On pose $\beta = 1 + \alpha^3$. Déterminer un polynôme irréductible à coefficients dans $\mathbb{F}_2$ dont $\beta$ soit racine.

e) Montrer que le polynôme $F = X^3 + X + 1$ est irréductible dans $K[X]$. Déterminer le cardinal de $K[X]/(F)$.

**Exercice 15.** Soit $\Omega$ une extension d'un corps $k$. Soient $K$ et $L$ deux sous-corps de $\Omega$ contenant $k$. On suppose que $m := [K : k]$ et $n := [L : k]$ sont finis. Soit $\Omega$ un corps contenant $K$ et $L$. On note $KL$ le composé de $K$ et $L$ dans $\Omega$ i.e. l'ensemble des sommes finies $\sum a_i b_i$ où $a_i \in K$ et $b_i \in L$.

a) Montrer que $KL$ est un corps et que c'est le sous-corps de $\Omega$ engendré par $K$ et $L$.

b) Montrer que $KL$ est une extension finie de $k$ de degré $\leq mn$.

c) Montrer que si $m$ et $n$ sont premiers entre eux, on a $[KL : k] = mn$.

d) Montrer qu'en général la conclusion de l'assertion 3 est fausse si $m$ et $n$ ne sont pas premiers entre eux.

**Exercice 16.** a) Montrer que l'équation $a^2 + 5b^2 = 2$ avec $(a, b) \in \mathbb{Z}^2$ n'a pas de solution.
Soit $K$ le corps $\mathbb{Q}(\sqrt{-5})$.

b) i) Quel est de degré de l'extension $K/\mathbb{Q}$, donner une base de $K$ sur $\mathbb{Q}$. Soit $x$ un élément de $K$ qui n'est pas dans $\mathbb{Q}$, montrer que $K = \mathbb{Q}(x)$.

ii) Déterminer les automorphismes $\mathbb{Q}$-linéaires du corps $K$ tel que si $x \in \mathbb{Q}$, on a $\sigma(x) = x$. On note $G$ cet ensemble d'automorphismes et pour $x \in K$, on définit

$$N_{K/\mathbb{Q}}(x) = \prod_{\sigma \in G} \sigma(x).$$

c) i) En écrivant $x = a + b\sqrt{-5}$ avec $a$ et $b$ dans $\mathbb{Q}$, calculer $N_{K/\mathbb{Q}}(x)$ et montrer que $N_{K/\mathbb{Q}}(x) \in \mathbb{Q}$.

ii) Notons $m_x : K \to K$ la multiplication par $x$. Montrer que $N_{K/\mathbb{Q}}(x) = \det(m_x)$.
Notons $A$ le sous-anneau $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$ de $K$.

d) Montrer que $A$ est isomorphe à $\mathbb{Z}[X]/(X^2 + 5)$.

e) Soit $x$ un élément non nul de $A$.

i) Montrer que l'idéal $(x)$ est un $\mathbb{Z}$-module libre de rang 2 et qu'il existe une $\mathbb{Z}$-base $(e_1, e_2)$ de $A$ et des éléments $(c_1, c_2) \in \mathbb{N}^2$ tels que $(c_1 e_1, c_2 e_2)$ est une $\mathbb{Z}$-base de $(x)$.

ii) Montrer que l'anneau $A/(x)$ est fini et déterminer son cardinal que l'on le notera $N(x)$.

f) Considérons l'application $\mathbb{Z}$-linéaire $u : A \to (x)$ définie par $u(e_i) = c_i e_i$ qui est inversible d'inverse $u^{-1} : (x) \to A$ défini par $u^{-1}(c_i e_i) = e_i$. Considérons maintenant l'application $\mathbb{Z}$-linéaire $v : (x) \to (x)$ définie par $v = m_x \circ u^{-1}$ où $m_x : A \to (x)$ est la multiplication par $x$.

i) Montrer que dans la base $(c_1 e_1, c_2 e_2)$, la matrice de $v$ est à coefficients dans $\mathbb{Z}$.

ii) Montrer que $v$ est surjective et en déduire que $\det(v) = \pm 1$.

iii) En calculant $\det(m_x)$ de deux manières, montrer que $N(x) = N_{K/\mathbb{Q}}(x)$.

g) Soit $I$ un idéal non nul de $A$

i) Montrer que $A/I$ est un ensemble fini. On définit $N(I) = \mathrm{Card}(A/I)$ pour tout idéal $I$ non nul de $A$.

ii) Calculer $N(I)$ pour $I = (2, 1 + \sqrt{-5})$.

iii) Montrer que l'anneau $A$ n'est pas principal.

## Complément

**Exercice 17.** Soit $K$ un espace topologique compact et soit $x \in K$. Soit $A = \mathbb{C}^0(K, \mathbb{R})$. On admet le théorème de prolongement de Tietze : Si $K'$ est un fermé de $K$ et $f : K' \to \mathbb{R}$ est une fonction continue, alors il existe $f' \in A$ telle que $f'_{|K'} = f$.

a) Soit $\mathfrak{m}_x = \{f \in A, f(x) = 0\}$. Montrer que $M$ est un idéal maximal de $A$.

b) Soit $J = \{f \in A, \exists U \text{ voisinage ouvert de } x, f(U) = 0\}$. Montrer que $J$ est un idéal de $A$

c) Soit $S = A - \mathfrak{m}_x$. Montrer que $S$ est une partie multiplicative de $A$.

d) Montrer que si $f \in J$, il existe $t \in S$ telle que $tf = 0$. En déduire un morphisme $\phi : A/J \to S^{-1}A$ de $A$-algèbres.

e) Montrer que si $s \in S$, il existe $s' \in A$ telle que $ss' - 1 \in J$. En déduire un morphisme $\psi : S^{-1}A \to A/J$ de $A$-algèbres.

f) Montrer que $\phi$ et $\psi$ sont des isomorphismes inverses l'un de l'autre.