TD n°1.

Exercice 1. Soit $S \subset k^n$ un ensemble quelconque et $I_S := \{f \in \mathcal{O}(k^n), \forall x \in S, f(x) = 0\}$. Montrer que V_{I_S} est l'adhérence de S pour la topologie de Zariski.

Exercice 2. Montrer que si $V \subset k^n$ et $W \subset k^m$ sont deux sous-ensembles algébriques, alors leur produit $V \times W \subset k^{n+m}$ est un sous-ensemble algébrique.

Exercice 3. Supposons k infini. Montrer que la topologie de Zariski sur k^{n+m} n'est pas la topologie produit de la topologie de Zariski sur k^n par celle sur k^m.

Solution. On doit trouver un ouvert U de k^{n+m} qui ne contient aucun ouvert produit non vide $U' \times U''$. On peut chercher U principal, i.e. $U = U_f$ avec $f \in \mathcal{O}(k^{n+m})$ et il suffira de montrer qu'il ne contient aucun produit d'ouverts principaux non vides $U_g \times U_h$. Passant aux fermés, on veut donc que V_f ne soit pas contenu dans un V_{gh} (où on voit g et h comme des fonctions sur k^{n+m} via les projections). L'hypothèse k infini nous permet d'identifier $\mathcal{O}(k^{n+m})$ avec $k[X_1, \cdots, X_{n+m}]$ qui est un anneau factoriel. Prenons $f = X_1 + X_{n+m}$ et supposons $V_f \subset V_{gh}$ avec $g \in k[X_1, \cdots, X_n]$ et $h \in k[X_{n+1}, \cdots, X_{n+m}]$. Alors $gh \in I_{V_f} = (f)$, donc f divise gh et, puisque f est irréductible, $f|h$ ou $f|g$. Cela implique $h = 0$ ou $g = 0$ et donc $U_h = \emptyset$ ou $U_g = \emptyset$. [Remarque : pour voir que $I_{V_f} = (f)$, on n'a pas besoin de supposer k algébriquement clos : en effet, si $p \in \mathcal{O}(k^{n+m})$ est la fonction nulle sur l'hyperplan V_f, alors $q := p(X_1, \cdots, X_{n+m-1}, -X_1)$ est le polynôme nul (k infini), donc $X_{n+m} + X_1$ divise $p = p - q$.]

Exercice 4. Soit $f \in \mathcal{O}(k^n)$ et $f = \prod_{i=1}^r f_i^{n_i}$ sa décomposition en facteurs irréductibles (avec les f_i deux à deux non associés). Montrer que $V_f = \bigcup_i V_{f_i}$. Est-il toujours vrai que les V_{f_i} sont des composantes irréductibles de V ?

Exercice 5. Supposons k algébriquement clos. Montrer qu'un sous-ensemble algébrique $V \subset k^n$ a un nombre fini de composantes connexes et que celles-ci sont en bijection avec les idempotents primitifs de $\mathcal{O}(V)$.

Solution. La finitude découle de celle du nombre de composantes irréductibles. Si e est idempotent non-trivial (i.e. $e \neq 0, 1$) alors $V = V_e \sqcup V_{1-e}$ avec $V_e, V_{1-e} \neq \emptyset$ (ici, pas besoin de algébriquement clos). Réciproquement, si V se décompose $V = V_1 \sqcup V_2$, et si on note $I_{V_i} \subset \mathcal{O}(V)$ les idéaux annulateurs, alors $I_{V_1} I_{V_2} = (0)$ et $V_{I_1+I_2} = \emptyset$ donc $I_1 + I_2 = \mathcal{O}(V)$ (k algébriquement clos). On peut donc écrire $1 = i_1 + i_2$ et en multipliant par i_1, on obtient $i_1 = i_1(i_1 + i_2) = i_1^2$, donc i_1 est idempotent et vaut 0 sur V_1 et 1 sur V_2. En posant $e := i_1$, on a donc $V_1 = V_e$ et $V_2 = V_{1-e}$. Remarquons maintenant que $\mathcal{O}(V_{1-e}) = \mathcal{O}(V)e$ (anneau dont l'unité est e) et que cet anneau possède un idempotent non trivial si et seulement si e est non primitif. On en déduit alors facilement que l'application $e \mapsto V_{1-e}$ est une bijection entre idempotents primitifs et composantes connexes.

Exercice 6. On suppose k algébriquement clos.
i) Soit $C \subset k^3$ l'image de l'application $t \mapsto (t, t^2, t^3)$. Montrer que C est algébrique, calculer I_C et montrer que $\mathcal{O}(C) \simeq k[X]$.
ii) Soit $C \subset k^2$ l'image de l'application $t \mapsto (t^2, t^3)$. Montrer que C est algébrique, calculer I_C et montrer que $\mathcal{O}(C)$ n'est pas isomorphe à $k[X]$.

Solution. i) Manifestement $C = V_I$ avec $I = (Y - X^2, Z - X^3)$. Le morphisme canonique $k[X] \longrightarrow k[X, Y, Z]/I$ est un isomorphisme d'inverse le morphisme $k[X, Y, Z]/I \longrightarrow k[X]$ qui envoie X sur X, Y sur X^2 et Z sur X^3. En particulier $k[X, Y, Z]/I$ est réduit donc $I = I_C$.
ii) C est manifestement inclus dans $V_{Y^2-X^3}$. Réciproquement, soit $(x, y) \in k^2$ tel que $x^3 = y^2$. Si t est une racine carrée de x, on a $t^3 = \pm y$, donc il existe une unique telle racine carrée telle que $t^3 = y$. D'où $C = V_{Y^2-X^3}$. Montrons que $I_C = (Y^2 - X^3)$. Pour cela, il suffit de voir que $Y^2 - X^3$ est un élément irréductible de $k[X, Y]$, ce qui est clair puisque X^3 n'a pas de racine carrée dans $k(X)$. Enfin, regardons le corps des fractions

$\mathrm{Frac}(\mathcal{O}(C)) = k(X)[Y]/(Y^2 - X^3)$. L'élément $T = YX^{-1}$ vérifie $T^2 = X$ et $TX = Y$, donc cet élément engendre $\mathrm{Frac}(\mathcal{O}(C))$ comme extension de k, i.e. $\mathrm{Frac}(\mathcal{O}(C)) = k(T)$. Or T n'est pas dans $\mathcal{O}(C)$, bien qu'il soit entier sur $\mathcal{O}(C)$. Donc $\mathcal{O}(C)$ n'est pas intégralement clos, donc pas isomorphe à une k-algèbre de polynômes $k[X]$. Alternativement, on peut aussi montrer que l'idéal (X, Y) de $\mathcal{O}(C)$ n'est pas principal, où encore montrer que l'élément X de $\mathcal{O}(C)$ est irréductible mais pas premier, ou encore vérifier que X et Y sont irréductibles et en conclure que l'égalité $Y^2 = X^3$ montre que $\mathcal{O}(C)$ n'est pas factoriel.

Exercice 7. Soit $V \subset k^n$ un sous-ensemble algébrique et $f \neq 0$ une fonction polynomiale sur V. On note U_f l'ouvert de V associé. Montrer que l'application $U_f \longrightarrow k^{n+1}$, $x \mapsto (x, f(x)^{-1})$ est injective et que son image W_f est un sous-ensemble algébrique de k^{n+1}. Calculer $\mathcal{O}(W_f)$ (on pourra commencer par le cas $V = k^n$).

Exercice 8. Montrer que l'image de l'application $(x, y) \mapsto (x, xy)$, $k^2 \longrightarrow k^2$ n'est ni fermée ni ouverte.

Exercice 9. Dans k^3 soit V le sous-ensemble algébrique défini par l'idéal $(X^2 - YZ, XZ - X)$. Trouver les composantes connexes de V et leurs idéaux premiers associés.

Solution. C'est l'intersection du cône Q d'équation $x^2 = yz$ avec la réunion des plans P_1 d'équation $x = 0$ et P_2 d'équation $z = 1$. On voit que $P_1 \cap Q$ est la réunion des deux axes de coordonnées y et z, et que $P_2 \cap Q$ est la parabole d'équation $y = x^2$ dans le plan $z = 1$. On a donc trois composantes irréductibles d'idéaux associés (X, Z), (X, Y) et $(Z - 1, Y - X^2)$. Pour voir que le dernier est bien irréductible, on peut calculer son algèbre de fonction $k[X, Y, Z]/(Z - 1, Y - X^2) \xrightarrow{\sim} k[X]$ qui est intègre.

Exercice 10. Soient $f, g \in k[X, Y]$ irréductibles et non associés.

a) Montrer qu'il existe $d \in k[X]$ et $a, b \in k[X, Y]$ tels que $af + bg = d$ dans $k[X, Y]$.
b) En déduire que l'image de $V_{(f,g)}$ par la première projection $k^2 \longrightarrow k$ est finie, puis que $V_{(f,g)}$ est fini.
c) En utilisant la théorie du résultant (cf exercice suivant), montrer qu'on peut choisir d de degré $\leqslant \deg(f)\deg(g)$.
d) Montrer finalement que $|V_{(f,g)}| \leqslant \deg(f)\deg(g)$.

Solution. a) Rappel : si A est un anneau factoriel, $A[Y]$ est factoriel et ses éléments irréductibles f sont de deux types :

i) soit $f \in A$ et f est irréductible dans A,
ii) soit f est irréductible dans $\mathrm{Frac}(A)[Y]$ et de contenu (1) (le contenu est l'idéal de A engendré par un pgcd des coefficients).

Ainsi, un élément irréductible de type i) devient inversible dans $\mathrm{Frac(A)}[Y]$ et deux éléments irréductibles de type ii) qui sont non associés dans $A[Y]$ restent non associés dans $\mathrm{Frac}(A)[Y]$ (car $\mathrm{Frac}(A)[Y]^\times = \mathrm{Frac}(A)^\times$, donc si f, g sont associés dans $\mathrm{Frac}(A)[Y]$, il existe $a, b \in A \setminus \{0\}$ tels que $af = bg$ d'où $(a) = (b)$ en prenant les contenus, puis $\frac{a}{b} \in A^\times$).
Application : dans l'anneau de polynômes $k(X)[Y]$, on a deux cas possibles :
— soit l'un des deux éléments, par exemple f, devient inversible, auquel cas on a $f \in k[X]$ et il suffit de prendre $d = f$, $a = 1$, $b = 0$.
— soit les deux éléments f et g restent irréductibles et non associés. Mais alors, puisque $k(X)[Y]$ est principal, il existe $A, B \in k(X)[Y]$ tels que $Af + Bg = 1$. Réduisant au même dénominateur, on trouve a, b et d.

b) Si $(x, y) \in V_{f,g}$, alors $d(x) = 0$, donc l'image par la première projection est contenue dans l'ensemble fini des racines de d. De même, l'image par la seconde projection est finie, et finalement $V_{f,g}$ est fini.

c) Homogénéisons f et g en des polynômes homogènes $F, G \in k[X, Y, T]$. D'après le b) l'exercice suivant, le résultant $\mathrm{Res}_X(F, G) \in k[Y, T]$ est homogène de degré $\deg(F)\deg(G) = \deg(f)\deg(g)$. Or, on trouve $\mathrm{Res}_X(f, g) \in k[Y]$ en déshomogénéisant $\mathrm{Res}_X(F, G)$ (ie en faisant $T = 1$), donc $\deg(\mathrm{Res}_X(f, g)) \leqslant \deg(f)\deg(g)$. On conclut grâce au a) de l'exercice suivant.

d) Si la première projection est injective sur $V_{f,g}$ alors on a directement la majoration souhaitée. Sinon, il nous suffit de trouver $a \in k$ tel que l'application $V_{f,g} \longrightarrow k$, $(x, y) \mapsto y + ax$ soit injective et d'appliquer la question c) après changement de variable $Y + aX \mapsto Y$. Puisque $V_{f,g}$ est fini, l'existence de a est claire si k est infini. En général, on peut plonger k dans un corps algébriquement clos $\bar{k}$ et obtenir la majoration voulue pour $V_{f,g}(\bar{k})$, qui implique celle cherchée.

Exercice 11 (Résultant)**.** Soit A un anneau commutatif et $f, g \in A[X]$ de degrés respectifs p et q. Notons $A[X]_{<n}$ le A-module libre des polynômes de degré $< n$ et considérons l'application A-linéaire

$$A[X]_{<q} \times A[X]_{<p} \longrightarrow A[X]_{<p+q} : (u, v) \mapsto uf + vg.$$

On note $\mathrm{Res}_X(f, g)$ son déterminant dans les bases $\{1, \cdots, X^{p-1}\} \sqcup \{1, \cdots, X^{q-1}\}$ et $\{1, \cdots, X^{p+q-1}\}$.

a) Montrer qu'il existe u, v dans $A[X]_{<q} \times A[X]_{<p}$ tels que $uf + vg = \mathrm{Res}_X(f, g)$.

b) Supposons que $A = k[X_1, \cdots, X_n]$ et que f et g soient *homogènes* de degrés p et q, en tant que polynômes en $X, X_1, \cdots, X_n$. Alors montrer que $\mathrm{Res}_X(f, g)$ est homogène de degré pq.

Solution. a) Il suffit d'utiliser la formule $M.\mathrm{com}(M) = \det(M)\,\mathrm{id}$ où M est la matrice de l'application linéaire $(u, v) \mapsto uf + vg$ dans les bases choisies, et $\mathrm{com}(M)$ est sa “comatrice” (transposée de la matrice des mineurs de taille $p + q - 1$).

b) On doit montrer que $\mathrm{Res}_X(f, g)(\lambda X_1, \cdots, \lambda X_n) = \lambda^{pq}.\mathrm{Res}_X(f, g)(X_1, \cdots, X_n)$. Écrivons

$$f(X) = F(X_1, \cdots, X_n, X) \text{ et } g(X) = G(X_1, \cdots, X_n, X).$$

On a $F(\lambda X_1, \cdots, \lambda X_n, X) = \lambda^p F(X_1, \cdots, X_n, X/\lambda)$ et $G(\lambda X_1, \cdots, \lambda X_n, X) = \lambda^q G(X_1, \cdots, X_n, X/\lambda)$, donc $\mathrm{Res}_X(f, g)(\lambda X_1, \cdots, \lambda X_n) = \mathrm{Res}_X(\lambda^p f(X/\lambda), \lambda^q g(X/\lambda)) = \lambda^{2pq}\mathrm{Res}_X(f(X/\lambda), g(X/\lambda))$. Il nous reste donc à montrer que

$$\mathrm{Res}_X(f(X/\lambda), g(X/\lambda)) = \lambda^{-pq}\mathrm{Rex}_X(f, g).$$

Or, la matrice de l'application linéaire $(u, v) \mapsto uf(X/\lambda) + vg(X/\lambda)$ dans les bases $\{1, \cdots, (X/\lambda)^{p-1}\} \sqcup \{1, \cdots, (X/\lambda)^{q-1}\}$ et $\{1, \cdots, (X/\lambda)^{p+q-1}\}$ est la même que celle de l'application linéaire $(u, v) \mapsto uf + vg$ dans les bases $\{1, \cdots, X^{p-1}\} \sqcup \{1, \cdots, X^{q-1}\}$ et $\{1, \cdots, X^{p+q-1}\}$. Donc on a

$$\mathrm{Res}_X(f(X/\lambda), g(X/\lambda)) = \mathrm{Rex}_X(f, g) D_p(\lambda) D_q(\lambda) D_{p+q}(\lambda)^{-1}$$

où $D_n(\lambda)$ est le déterminant de la matrice de passage de la base $\{1, \cdots, (X/\lambda)^{n-1}\}$ à la base $\{1, \cdots, X^{n-1}\}$. Ce déterminant étant $D_n(\lambda) = \lambda^{1+\cdots+n} = \lambda^{n(n+1)/2}$, on conclut avec un petit calcul.

Exercice 12. Soit $f \in k[X, Y]$ irréductible de degré $\leqslant 2$ avec k algébriquement clos de caractéristique $\neq 2$. Montrer que $\mathcal{O}(V_f)$ est isomorphe à $k[T]$ ou à $k[T, T^{-1}]$.

Solution. La forme générale de f est $aX^2 + bXY + cY^2 + dX + eY + f$. Après changement linéaire de coordonnées, on peut se ramener à l'une des formes suivantes : $X + f$, $X^2 + dX + eY + f$ ou $XY + dX + eY + f$. Après translations et homothéties, on peut alors se ramener à l'une des formes X, $X^2 - Y$ ou $XY - 1$ (il y a d'autres formes possibles, mais pas irréductibles). Dans les deux premiers cas, l'anneau des fonctions est isomorphe à $k[T]$. Dans le dernier cas, il est isomorphe à $k[X, Y]/(XY - 1) = k[X, X^{-1}]$.