Université Claude Bernard LYON 1
Master MA Mathématiques générales
Algèbre et calcul formel

Corrigé de la fiche de TD 7

Exercice 1.
Soient $f_1, \cdots, f_r \in K[X_1, \cdots, X_n]$; on désigne par I l'idéal de $K[X_1, \cdots, X_n]$ engendré par $f_1, \cdots, f_r$ et $J = I \cap K[X_1, \cdots, X_{n-1}]$ l'idéal d'élimination. Montrer que :

$$Z(J) = \pi(Z(I)) \cup (Z(J) \cap Z(\varphi_1, \cdots, \varphi_r))$$

avec $\varphi_i = \mathrm{lc}_{X_n}(f_i) \in K[X_1, \cdots, X_{n-1}]$ pour $1 \leq i \leq n$.
Corrigé.
Comme f_1 n'est pas *constant*), il s'écrit :

$$f_1 = a_n(X_1, \cdots, X_{n-1})X_n^d + a_{n-1}(X_1, \cdots, X_{n-1})X_n^{d-1} + \cdots + a_0(X_1, \cdots, X_{n-1})$$

et l'on a $\varphi_1 = a_n$.
Supposons d'abord que $r = 1$. Pour tout $(x_1, \cdots, x_{n-1}) \in \Omega^{n-1} \setminus Z(\varphi_1)$le polynôme :

$$cX_n^d + a_{n-1}(x_1, \cdots, x_{n-1})X_n^{d-1} + \cdots + a_0(x_1, \cdots, x_{n-1}) \in \Omega[X_n]$$

où $c = a_n(x_1, \cdots, x_{n-1}) \neq 0$, a une racine $x_n \in \Omega$ et l'on a $(x_1, \cdots, x_{n-1}, x_n) \in Z(f_1)$ de sorte que :

$$\Omega^{n-1} = \pi(Z(f_1)) \cup Z(\varphi_1)$$

On suppose maintenant que $r = 2$. On a :

$$R = R_{X_n}(f_1, f_2) \in I \cap K[X_1, \cdots, X_{n-1}] = J$$

d'où :

$$R(x_1, \cdots, x_{n-1}) = 0 \text{ pour tout } x = (x_1, \cdots, x_n) \in Z(I)$$

de sorte que :

$$\pi(Z(I)) \subset Z(J) \subset Z(R)$$

Réciproquement, soit $(x_1, \cdots, x_{n-1}) \in Z(R) \setminus Z(\varphi_1, \varphi_2)$; on a par exemple :

$$R(x_1, \cdots, x_{n-1}) = 0 \text{ et } c = \varphi_1(x_1, \cdots, x_{n-1}) \neq 0$$

Le *théorème de spécialisation du résultant* s'applique (puisque f_1 est *quasi-unitaire*) *via* :

$$\begin{array}{rl} K[X_1, \cdots, X_{n-1}] & \longrightarrow \Omega \\ X_1 & \longrightarrow x_1 \\ & \vdots \\ X_{n-1} & \longrightarrow x_{n-1} \end{array}$$

si $\widetilde{R}$ est le résultant (relativement à X_n) des polynômes :

$$\left\{ \begin{array}{l} f_1(x_1, \cdots, x_{n-1}, X_n) \\ f_2(x_1, \cdots, x_{n-1}, X_n) \end{array} \right.$$

on a :

$$\widetilde{R} = R(x_1, \cdots, x_{n-1}) = 0$$

de sorte que les polynômes

$$\begin{cases} f_1(x_1, \cdots, x_{n-1}, X_n) \\ f_2(x_1, \cdots, x_{n-1}, X_n) \end{cases}$$

de $\Omega[X_n]$ ont *une racine commune* x_n.
Ainsi $x = (x_1, \cdots, x_n) \in Z(I)$; on a alors :

$$Z(J) = \pi(Z(I)) \cup (Z(J) \cap Z(\varphi_1, \varphi_2))$$

On suppose maintenant que $r \geq 3$.
On introduit une nouvelle indéterminée U et les polynômes

$$\begin{cases} g = f_1 \\ h = f_2 + U\, f_3 + \cdots + U^{r-2}\, f_r \end{cases}$$

On a :

$$g, h \in K[U, X_1, \cdots, X_{n-1}, X_n] \text{ et } R = R_{X_n}(g, h) \in K[U, X_1, \cdots, X_{n-1}]$$

De plus :

$$R = \sum_{k=0}^{s} R_k U^k \text{ avec } R_k \in K[X_1, \cdots, X_{n-1}] \text{ pour tout } 0 \leq k \leq s$$

Alors, la *formule de Bezout sans dénominateur* :

$$R = S\, g + T\, h \text{ où } S, T \in K[U, X_1, \cdots, X_{n-1}, X_n]$$

montre, *par identification des coefficients en* U, que l'on a :

$$R_k \in I \cap K[X_1, \cdots, X_{n-1}] = J \text{ pour tout } 0 \leq k \leq s$$

En particulier on a :

$$R_k(x_1, \cdots, x_{n-1}) = 0 \text{ pour tout } 0 \leq k \leq s \text{ et pour tout } x = (x_1, \cdots, x_n) \in Z(I)$$

de sorte que :

$$\pi(Z(I)) \subset Z(J) \subset Z(R_0, \cdots, R_s)$$

Réciproquement, soit $(x_1, \cdots, x_{n-1}) \in Z(R_0, \cdots, R_s) \setminus Z(\varphi_1, \cdots, \varphi_r)$ on a par exemple :

$$R_k(x_1, \cdots, x_{n-1}) = 0 \text{ pour } 0 \leq k \leq s \text{ et } c = \varphi_1(x_1, \cdots, x_{n-1}) \neq 0$$

Pour tout $u \in \Omega$, le *théorème de spécialisation du résultant* s'applique (puisque $c \neq 0$) *via* :

$$\begin{aligned} K[U, X_1, \cdots, X_{n-1}] &\longrightarrow \Omega \\ U &\longrightarrow u \\ X_1 &\longrightarrow x_1 \\ &\vdots \\ X_{n-1} &\longrightarrow x_{n-1} \end{aligned}$$

si $\widetilde{R}$ est le résultant (relativement à X_n) des polynômes :

$$\begin{cases} f_1(x_1, \cdots, x_{n-1}, X_n) \\ f_2(x_1, \cdots, x_{n-1}, X_n) + u f_3(x_1, \cdots, x_{n-1}, X_n) \cdots + u^{r-2} f_r(x_1, \cdots, x_{n-1}, X_n)) \end{cases}$$

on a :

$$\widetilde{R} = R(u, x_1, \cdots, x_{n-1}) = \sum_{k=0}^{s} R_k(x_1, \cdots, x_{n-1}) u^k = 0$$

Il en résulte que, pour tout $u \in \Omega$, les polynômes

$$\begin{cases} f_1(x_1, \cdots, x_{n-1}, X_n) \\ f_2(x_1, \cdots, x_{n-1}, X_n) + u f_3(x_1, \cdots, x_{n-1}, X_n) \cdots + u^{r-2} f_r(x_1, \cdots, x_{n-1}, X_n) \end{cases}$$

de $\Omega[X_n]$ ont *une racine commune*.
Comme cette *racine commune* ne peut prendre qu'un nombre fini de valeurs, il existe une racine x_n du polynôme $f_1(x_1, \cdots, x_{n-1}, X_n) \in \Omega[X_n]$ qui est racine du polynôme

$$f_2(x_1, \cdots, x_{n-1}, X_n) + u f_3(x_1, \cdots, x_{n-1}, X_n) \cdots + u^{r-2} f_r(x_1, \cdots, x_{n-1}, X_n) \in \Omega[X_n]$$

pour une infinité d'entiers de $u \in \Omega$. Finalement le polynôme :

$$f_2(x_1, \cdots, x_{n-1}, x_n) + f_3(x_1, \cdots, x_{n-1}, x_n) U \cdots + f_r(x_1, \cdots, x_{n-1}, x_n) U^{r-2} \in \Omega[U]$$

est *nul*. Ainsi, il existe $x_n \in \Omega$ tel que $x = (x_1, \cdots, x_n) \in Z(I)$. Finalement on obtient que :

$$Z(J) = \pi(Z(I)) \cup (Z(J) \cap Z(\varphi_1, \cdots, \varphi_r))$$

Exercice 2.
On considère des polynômes $f_i \in \mathbb{Z}[X_1, \cdots, X_n]$ pour $1 \leq i \leq r$. On désigne par $Z_{\mathbb{C}}(f_1, \cdots, f_r)$ (*resp.* $Z_{\overline{\mathbb{Q}}}(f_1, \cdots, f_r)$) l'ensemble des zéros de $f_1, \cdots, f_r$ dans $\mathbb{C}^n$ (*resp.* dans $\overline{\mathbb{Q}}^n$). Pour tout entier premier p, soit $\pi_p : \mathbb{Z} \longrightarrow \mathbb{F}_p$ le morphisme canonique ; on désigne par $Z_{\overline{\mathbb{F}_p}}(f_1, \cdots, f_r)$ l'ensemble des zéros de $\pi_p(f_1), \cdots, \pi_p(f_r)$ dans $\overline{\mathbb{F}_p}^n$.

1. Montrer que si $Z_{\mathbb{C}}(f_1, \cdots, f_r) = \emptyset$, il existe $N \geq 1$ tel que pour tout entier premier $p > N$ on a $Z_{\overline{\mathbb{F}_p}}(f_1, \cdots, f_r) = \emptyset$.
2. On suppose que $Z_{\mathbb{C}}(f_1, \cdots, f_r) \neq \emptyset$.
   (a) Montrer que $Z_{\overline{\mathbb{Q}}}(f_1, \cdots, f_r) \neq \emptyset$
   (b) Montrer qu'il existe une solution $x = (x_i)_{1 \leq i \leq n}$ avec x_i, $1 \leq i \leq n$, entier sur l'anneau $A = \mathbb{Z}[\frac{1}{D}]$ avec $D \geq 1$.
   (c) Montrer que l'anneau $A = \mathbb{Z}[\frac{1}{D}]$ est principal.
   (d) Montrer que $B = A[x_1, \cdots, x_n]$ est un A-module libre de type fini.
   (e) Montrer que pour p premier, $p > D$, $B \neq pB$ et que si $\mathfrak{m} \supset pB$ est un idéal maximal de B contenant pB alors $K_p = B/\mathfrak{m}$ est une $\mathbb{F}_p$-extension de degré fini.
   (f) En déduire que $Z_{\overline{\mathbb{F}_p}}(f_1, \cdots, f_r) \neq \emptyset$ pour $p > D$.
   (g) En conclure que $Z_{\mathbb{C}}(f_1, \cdots, f_r) = \emptyset$ si et seulement si $Z_{\overline{\mathbb{F}_p}}(f_1, \cdots, f_r) = \emptyset$ pour $p >> 0$.

Corrigé.

1. Par le th des zéros de Hilbert, il existe des polynômes $h_i \in \mathbb{Q}[X_1, \cdots, X_n]$ tels que $\sum_{i=1}^{r} h_i f_i = 1$; soit $N \geq 1$ un dénominateur commun des coefficients des polynômes h_i, $1 \leq i \leq r$; on a $\sum_{i=1}^{r} (N h_i) f_i = N$ avec $N h_i \in \mathbb{Z}[X_1, \cdots, X_n]$ pour $1 \leq i \leq r$. On a alors pour tout entier

premier $p > N$, $\sum_{i=1}^{r} \pi_p(d)^{-1}\pi_p(dh_i)\pi_p(f_i) = \pi_p(1)$ avec $\pi_p(dh_i) \in \mathbb{F}_p[X_1, \cdots, X_n]$ de sorte que $Z_{\overline{\mathbb{F}_p}}(f_1, \cdots, f_r) = \emptyset$.

2. a. On a $Z_{\mathbb{C}}(f_1, \cdots, f_r) \neq \emptyset$. Soit I l'idéal de $\mathbb{Q}[X_1, \cdots, X_n]$ engendré par les polynômes $f_1, \cdots, f_r$. On a donc $I \neq \mathbb{Q}[X_1, \cdots, X_n]$ et par suite $Z_{\overline{\mathbb{Q}}}(f_1, \cdots, f_r) \neq \emptyset$.

b. Soit $x = (x_i)_{1 \leq i \leq n} \in \overline{\mathbb{Q}}$ une solution. Comme les x_i, $1 \leq i \leq n$, sont algébriques sur $\mathbb{Q}$, en prenant pour $D \geq 1$ le dénominateur commun des coefficients des polynômes minimaux des x_i, on a que les x_i sont entiers sur l'anneau $A = \mathbb{Z}[\frac{1}{D}]$.

c. Soit $\mathfrak{a}$ un idéal *non nul* de A ; alors $\mathfrak{a} \cap \mathbb{Z}$ est un idéal *non nul* de $\mathbb{Z}$. On a donc $\mathfrak{a} \cap \mathbb{Z} = \mathbb{Z}c$; soit $\delta = \text{pgcd}(c, D)$ et $c' = \frac{c}{\delta}$. On a $c' = \frac{D'}{D} \in A$ où $D' = \frac{D}{\delta}$ de sorte que $\mathfrak{a} = Ac'$.

d. Puisque les x_i, $1 \leq i \leq n$ sont entiers sur A, la A-algèbre $B = A[x_1, \cdots, x_n]$ est un A-module de type fini.

e. Comme $B \subset \overline{\mathbb{Q}}$, le A-module B de type fini est sans torsion donc est *libre de type fini*. On a donc un isomorphisme de A-modules $B \simeq A^r$.

Par ailleurs les éléments irréductibles de A sont les entiers premiers p qui *ne divisent pas* D et l'on a $A/Ap \simeq \mathbb{Z}/\mathbb{Z}p$. Par suite B/Bp est *fini*.

Pour tout entier premier p avec $p > D$ (donc qui est irréductible dans A), on a donc $Bp \subsetneq B$.

Il existe donc un idéal maximal $\mathfrak{m}$ de B contenant Bp ; comme le morphisme canonique $B/Bp \longrightarrow K_p = A/\mathfrak{m}$ est *surjectif* et K_p est corps fini de caractéristique p. Il existe un $\mathbb{F}_p$-morphisme $K_p \longrightarrow \overline{\mathbb{F}_p}$.

f. On note $\overline{x_i}$ l'image de x_i par le morphisme composé $B \longrightarrow \overline{\mathbb{F}_p}$ et comme $f_i(x_1, \cdots, x_n) = 0$ pour $1 \leq i \leq r$, on a finalement $\overline{x} = (\overline{x_i})_{1 \leq i \leq n} \in Z_{\overline{\mathbb{F}_p}}(f_1, \cdots, f_r)$.

g. On a montré que si $Z_{\mathbb{C}}(f_1, \cdots, f_r) \neq \emptyset$ alors il existe un entier $D \geq 1$ tel que pour tout entier premier p, $p > D$ on a $Z_{\overline{\mathbb{F}_p}}(f_1, \cdots, f_r) \neq \emptyset$. Il en résulte que si $Z_{\mathbb{C}}(f_1, \cdots, f_r) \neq \emptyset$ alors pour tout entier $N \geq 1$ il existe p premier tel que $p > N$ et $Z_{\overline{\mathbb{F}_p}}(f_1, \cdots, f_r) \neq \emptyset$ ou encore s'il existe N tel que $Z_{\overline{\mathbb{F}_p}}(f_1, \cdots, f_r) = \emptyset$ pour $p > N$, on a $Z_{\mathbb{C}}(f_1, \cdots, f_r) = \emptyset$.

Complément. On a vu que si $Z_{\mathbb{C}}(f_1, \cdots, f_r) \neq \emptyset$ alors il existe un entier $D \geq 1$ tel que pour tout entier premier $p > D$ on a $Z_{\overline{\mathbb{F}_p}}(f_1, \cdots, f_r) \neq \emptyset$.

Réciproquement supposons l'on a $Z_{\overline{\mathbb{F}_p}}(f_1, \cdots, f_r) \neq \emptyset$ pour $p > D$.

Considérons l'anneau $\mathcal{A} = \prod_{p>D} \overline{\mathbb{F}_p}$; le noyau $\mathfrak{m}_p$ de la projection canonique $\mathcal{A} \longrightarrow \overline{\mathbb{F}_p}$ est un idéal maximal de $\mathcal{A}$ et l'on a $\mathcal{A}/\mathfrak{m}_p \simeq \overline{\mathbb{F}_p}$.

Par ailleurs l'ensemble $\mathcal{I}$ des éléments de $\mathcal{A}$ de *support fini* est un idéal de $\mathcal{A}$. Par le th de Krull il existe un idéal maximal $\mathcal{M}$ de $\mathcal{A}$ *contenant* $\mathcal{I}$. On a $\mathcal{M} \neq \mathfrak{m}_p$ pour tout p.

On peut alors montrer que le corps $\mathcal{A}/\mathcal{M}$ est de caractéristique nulle, algébriquement clos, de cardinal Card(C) *donc est isomorphe à* $\mathbb{C}$. Il en résulte que $Z_{\mathbb{C}}(f_1, \cdots, f_r) \neq \emptyset$.