Chapitre 4

Résultant, élimination, fonctions polynomiales

Une bonne partie de ce chapitre est traitée dans le “Tout-en-un pour la licence, niveau L2” de Ramis-Warusfel chez Dunod (chapitre II.7) ; voir aussi Lang et Briançon-Maisonobe.

4.1 Matrice de Sylvester et résultant

Soit R un anneau commutatif intègre de corps des fractions L. Soient $A := a_0 + \cdots + a_p X^p \in R[X]_p$ et $B := b_0 + \cdots + b_q X^q \in R[X]_q$. L'application linéaire :

$$\begin{cases} (Q,P) \mapsto AQ + BP, \\ R[X]_{q-1} \times R[X]_{p-1} \to R[X]_{p+q-1}, \end{cases}$$

a pour matrices, relativement aux bases “canoniques” $\big((1,0),\ldots,(X^{q-1},0),(0,1),\ldots,(0,X^{p-1})\big)$ de $R[X]_{q-1} \times R[X]_{p-1}$ et $(1,\ldots,X^{p+q-1})$ de $R[X]_{p+q-1}$, la matrice :

$$S_{p,q}(A,B) := \begin{pmatrix} a_0 & 0 & \ddots & 0 & b_0 & 0 & 0 & \ldots & 0 & 0 \\ a_1 & a_0 & \ddots & 0 & b_1 & b_0 & 0 & \ddots & 0 & 0 \\ \vdots & a_1 & \ddots & 0 & \vdots & b_1 & b_0 & \ddots & 0 & 0 \\ \vdots & \vdots & \ddots & a_0 & \vdots & \vdots & b_1 & \ddots & 0 & 0 \\ a_{p-1} & \vdots & \ddots & a_1 & b_q & \vdots & \vdots & \ddots & b_0 & 0 \\ a_p & a_{p-1} & \ddots & \vdots & 0 & b_q & \vdots & \ddots & b_1 & b_0 \\ 0 & a_p & \ddots & \vdots & 0 & 0 & b_q & \ddots & \vdots & b_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & 0 & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & a_{p-1} & \vdots & \vdots & \vdots & \ddots & b_q & \vdots \\ 0 & 0 & \ldots & a_p & 0 & 0 & 0 & \ldots & 0 & b_q \end{pmatrix} \in \mathrm{Mat}_{p+q}(R).$$

Les q premières colonnes sont formées avec les coefficients de A, les p suivantes avec les coefficients de B. Cette matrice est appelée *matrice de Sylvester*[1] de A et B. Nous noterons :

$$\mathrm{Res}_{p,q}(A,B) := \det S_{p,q}(A,B)$$

le *déterminant de Sylvester* ; c'est donc un polynôme en les a_i et b_j, à coefficients dans $\mathbf{Z}$.

Proposition 4.1.1 *Pour que $Res_{p,q}(A,B)$ soit nul, il faut, et il suffit, qu'il existe $P \in R[X]_{p-1}$ et $Q \in R[X]_{q-1}$ non tous deux nuls et tels que $AQ+BP=0$.*

Preuve. - On observe que $S_{p,q}(A,B)$ est la matrice dans la base canonique de $R[X]_{p+q-1}$ de la famille $(A,\dots,X^{q-1}A,B,\dots,X^{p-1}B)$. Si le déterminant de cette matrice est nul, la famille est liée, ce qui équivaut à la conclusion voulue. (On peut également raisonner sur le noyau de l'application linéaire associée, quitte à transposer au cas des R-modules libres les résultats connus pour les L-espaces vectoriels.) □

Proposition 4.1.2 *Il existe $P \in R[X]_{p-1}$ et $Q \in R[X]_{q-1}$ tels que $Res_{p,q}(A,B) = AQ+BP$.*

Preuve. - Notons $S := S_{p,q}(A,B)$ et $\tilde{S}$ la transposée de la matrice des cofacteurs de S. D'après les formules de Cramer, $S\tilde{S} = \mathrm{Res}_{p,q}(A,B)I_{p+q}$. Si l'on note $(\mu_0,\dots,\mu_{q-1},\lambda_0,\dots,\lambda_{p-1})$ la première colonne de $\tilde{S}$, alors $Q := \mu_0+\cdots+\mu_{q-1}X^{q-1}$ et $P := \lambda_0+\cdots+\lambda_{p-1}X^{p-1}$ conviennent. □

Exemple 4.1.3 Si $q=1$, on a $\mathrm{Res}_{p,q}(A,B) = a_0b_1^p - a_1b_0b_1^{p-1} + \cdots + (-1)^p a_p b_0^p = b_0^p A(-b_0/b_1)$.

Définition 4.1.4 Le *résultant* des polynômes non nuls $A,B \in R[X]$ est $\mathrm{Res}(A,B) := \mathrm{Res}_{p,q}(A,B)$, où $p := \deg A$ et $q := \deg B$.

La principale difficulté de la théorie (et de la pratique) du résultant vient de ce que c'est bien cette définition qui est utile, mais que ce n'est pas une fonction simple (polynomiale ou même simplement continue) des coefficients : elle dépend explicitement du degré. Le problème est que, par exemple, le polynôme $a_0+\cdots+a_pX^p$ n'est pas nécessairement de degré p. Les exemples suivants illustrent cette non-régularité de la fonction résultant.

Exemple 4.1.5 On trouve :

$$\mathrm{Res}(aX^2+bX+c,\lambda X+\mu) = \begin{cases} a\mu^2 - b\lambda\mu + c\lambda^2 & \text{si } a\lambda \neq 0, \\ b\mu - \lambda c & \text{si } a=0, b\lambda \neq 0, \\ c & \text{si } a=b=0, c\lambda \neq 0. \end{cases}$$

Cas limites et des cas dégénérés.

$$\mathrm{Res}_{p,q}(A,B) = \begin{cases} 0 \text{ si } \deg A < p, \deg B < q, \\ \left((-1)^p a_p\right)^{q-\deg B}\mathrm{Res}(A,B) \text{ si } \deg A = p, \deg B < q, \\ b_q^{p-\deg A}\mathrm{Res}(A,B) \text{ si } \deg A < p, \deg B = q, \\ a^{\deg B} \text{ si } A = a \in R\setminus\{0\}, \\ b^{\deg A} \text{ si } B = b \in R\setminus\{0\}. \end{cases}$$

1. Dans certains ouvrages, c'est la transposée de $S_{p,q}$ qui est appelée matrice de Sylvester.

Proposition 4.1.6 *Pour que le résultant $Res(A,B)$ soit nul, il faut, et il suffit, que A et B aient un facteur commun non constant dans $L[X]$.*

Preuve. - D'après la proposition précédente, $\mathrm{Res}(A,B)=0$ équivaut à l'existence de $P,Q\in R[X]$ non tous deux nuls, tels que $AQ+BP=0$ et avec $\deg P<\deg A$, $\deg Q<\deg B$. On est alors ramené à un exercice facile sur la divisibilité dans l'anneau principal $L[X]$. □

Corollaire 4.1.7 *Supposons l'anneau R factoriel. Pour que le résultant $Res(A,B)$ soit nul, il faut, et il suffit, que A et B aient un facteur commun non constant dans $R[X]$.*

Calcul pratique du résultant. Il peut s'effectuer par un procédé analogue à l'algorithme d'Euclide de calcul du pgcd (divisions euclidiennes successives) , à l'aide des trois formules suivantes :

$$\begin{aligned}\mathrm{Res}(B,A)&=(-1)^{(\deg A)(\deg B)}\mathrm{Res}(A,B),\\ \mathrm{Res}(QB,B)&=0,\\ \mathrm{Res}(QB+A_1,B)&=b_q^{\deg A-\deg A_1}\mathrm{Res}(A_1,B)\quad (A_1\neq 0).\end{aligned}$$

Ces formules se prouvent par opérations élémentaires sur les colonnes de la matrice de Sylvester.

4.2 Résultant et élimination

4.2.1 Critères d'existence de racines communes

Les prochaines formules supposent que l'on dispose d'une factorisation, ce qui est rare : leur intérêt est donc théorique.

Lemme 4.2.1 *Si $B=(X-\beta)B_1$, on a $Res(A,B)=A(\beta)Res(A,B_1)$.*

Preuve. - Cela se voit encore par des opérations élémentaires sur les colonnes de $S_{p,q}(A,B)$. □

Théorème 4.2.2 *Soient $A=a(X-\alpha_1)\cdots(X-\alpha_p)$ et $B=b(X-\beta_1)\cdots(X-\beta_q)$, $a,b\neq 0$. Alors :*

$$Res(A,B)=b^pA(\beta_1)\cdots A(\beta_q)=b^pa^q\prod_{\substack{1\le i\le p\\ 1\le j\le q}}(\beta_j-\alpha_i)=(-1)^{pq}B(\alpha_1)\cdots B(\alpha_p).$$

Preuve. - La première formule se prouve en appliquant q fois le lemme, puis l'une des formules relatives aux cas dégénérés ; la seconde en découle et la troisième découle de la seconde. □

Théorème 4.2.3 *On suppose le corps L algébriquement clos. Pour que le résultant $Res(A,B)$ soit nul, il faut, et il suffit, que A et B aient une racine commune dans L.*

Preuve. - On peut utiliser au choix le théorème précédent, ou la proposition 4.1.6. □

Exemple 4.2.4 On sait qu'un polynôme P a une racine multiple si, et seulement s'il a une racine commune avec P'. Considérons donc : $P:=X^d+c_1X^{d-1}+\cdots+c_d=(X-\lambda_1)\cdots(X-\lambda_d)$. Si le corps L est de caractéristique nulle (plus généralement, si d n'est pas multiple de la caractéristique), $\deg P'=d-1$ et $Res(P,P')=\mathrm{Res}_{d,d-1}(P,P')=P'(\lambda_1)\cdots P'(\lambda_d)=\prod_{\substack{1\le i,j\le d\\ i\neq j}}(\lambda_i-\lambda_j)$. Mais c'est un polynôme explicite $D(c_1,\cdots,c_d)$ à coefficients dans $\mathbf{Z}$, ce qui donne un critère d'existence de racines multiples vérifiable sans calcul des racines. Ce polynôme est (à un facteur conventionnel près) le *discriminant* de P.

4.2.2 Application à l'élimination

Soient K un corps algébriquement clos et $A, B \in K[X_0, \ldots, X_n]$ des polynômes où X_0 figure explicitement. On les écrit :

$$A = \sum_{i=0}^{p} a_i(X_1, \ldots, X_n) X_0^i, \quad B = \sum_{j=0}^{q} b_j(X_1, \ldots, X_n) X_0^j,$$

où $a_p, b_q \in K[X_1, \ldots, X_n]$ sont supposés non nuls. On considère A et B comme éléments de $R[X_0]$, où $R := K[X_1, \ldots, X_n]$. On peut donc définir :

$$F(X_1, \ldots, X_n) := \mathrm{Res}_{X_0}(A, B) \in R,$$

résultant obtenu par "élimination de X_0". C'est bien entendu un élément de R, donc un polynôme en $X_1, \ldots, X_n$; mais, plus précisément, ses coefficients sont eux-mêmes des polynômes en $a_0, \ldots, a_p, b_0, \ldots, b_q$ à coefficiente dans $\mathbf{Z}$.

Théorème 4.2.5 (d'extension, ou de relèvement) *Soit $(c_1, \ldots, c_n) \in K^n$. Alors :*

$$F(c_1, \ldots, c_n) = 0 \Longleftrightarrow \begin{cases} a_p(c_1, \ldots, c_n) = b_q(c_1, \ldots, c_n) = 0 \\ \text{ou} \\ \exists c_0 \in K \ , \ A(c_0, c_1, \ldots, c_n) = B(c_0, c_1, \ldots, c_n) = 0. \end{cases}$$

Preuve. - Soit $\phi : R[X_0] \to K[X_0]$ le morphisme d'anneaux défini par $P(X_0, X_1, \ldots, X_n) \mapsto P(X_0, c_1, \ldots, c_n)$. Sa restriction à R est le morphisme de R dans K défini par $P(X_1, \ldots, X_n) \mapsto P(c_1, \ldots, c_n)$; on note encore ϕ ce morphisme, qui envoie $\det S_{p,q}(A, B) \in R$ sur $\det S_{p,q}(\phi(A), \phi(B)) \in K$.
La condition à gauche de l'équivalence logique à démontrer dit que $\phi(F) = 0$, c'est-à-dire que $\det S_{p,q}(\phi(A), \phi(B)) = 0$, *i.e.* $\mathrm{Res}_{p,q}(\phi(A), \phi(B)) = 0$. c'est vrai soit si $\deg \phi(A) < p$ et $\deg \phi(B) < q$, autrement dit si $a_p(c_1, \ldots, c_n) = b_q(c_1, \ldots, c_n) = 0$; soit si $\phi(A)$ et $\phi(B)$ ont une racine commune c_0, autrement dit $A(c_0, c_1, \ldots, c_n) = B(c_0, c_1, \ldots, c_n) = 0$. □

Des exemples d'applications en géométrie algébrique sont donnés dans RW3 et dans le livre de Briançon-Maisonobe ; voir aussi certains exercices du TD.

4.3 Fonctions polynomiales

Proposition 4.3.1 *Soit K un corps commutatif. L'application $P \mapsto (x \mapsto P(x))$ de $K[X]$ dans la K-algèbre[2] $\mathcal{F}(K, K)$ des applications de K dans K est injective non surjective si K est infini, surjective non injective dans le cas contraire.*

Preuve. - Il est clair que l'application indiquée est un morphisme de K-algèbres (*i.e.* c'est un morphisme d'anneaux et elle est K-linéaire).
Supposons K infini. Alors un élément du noyau est un polynôme admettant une infinité de racines, donc nul, et l'application est injective. L'application "de Dirac" $x \mapsto \delta_{0,x}$ (on utilise le symbole de Kronecker) ne peut être définie par un polynôme car celui-ci aurait une infinité de racines donc

2. Une K-algèbre A est un anneau commutatif et un K-espace vectoriel, avec la condition de compatibilité suivante des deux structures : la multiplication interne de A doit être K-bilinéaire.

serait nul donc ne prendrait pas la valeur 1 en $x = 0$; elle n'appartient donc pas à l'image de notre morphisme, qui n'est donc pas surjectif.
Supposons K fini, ayant q éléments. Le polynôme $X^q - X = \prod_{a \in K} (X - a)$ admet pour racines tous les éléments de K, il appartient donc au noyau et notre morphisme n'est pas injectif. Pour tout $a \in K$, notons $P_a(X) := \frac{X^q - X}{X - a} = \prod_{b \in K \setminus \{a\}} \in K[X]$. Notons $p(a) := P_a(a) \neq 0$ (exercice : vérifier que c'est -1). Alors pour tout $f : K \to K$, le polynôme $P := \sum_{a \in K} \frac{f(a)}{p(a)} P_a$ est tel que $P(a) = f(a)$ pour tout $a \in K$ (c'est en fait le polynôme d'interpolation de Lagrange). Il a donc pour image f par le morphisme, qui est donc surjectif. □

Corollaire 4.3.2 *Supposons le corps K infini. Alors le morphisme de K-algèbres de $K[X_1, \ldots, X_n]$ dans $\mathcal{F}(K^n, K)$ qui, au polynôme P associe l'application $(c_1, \ldots, c_n) \mapsto P(c_1, \ldots, c_n)$, est injectif.*

Preuve. - On le déduit facilement de la proposition par récurrence sur n. □

Dorénavant, nous supposerons le corps K infini. On peut donc identifier le polynôme P à la *fonction polynomiale* $(c_1, \ldots, c_n) \mapsto P(c_1, \ldots, c_n)$. Les fonctions polynomiales forment une sous-algèbre (*i.e.* un sous-anneau et un sous-espace vectoriel) de $\mathcal{F}(K^n, K)$ isomorphe à $K[X_1, \ldots, X_n]$.

On veut maintenant définir la notion de fonction polynomiale sur un espace affine en s'affranchissant des coordonnées. La raison en est que l'on ne peut pas considérer une propriété comme vraiment géométrique si on n'en a pas une formulation "intrinsèque", indépendante des coordonnées. Cette idée figure sous une forme voisine dans le célèbre "Programme d'Erlangen" de Felix Klein, où il est dit, programmatiquement, qu'une géométrie se définit comme l'ensemble des propriétés invariantes sous un groupe : dans notre cas, il s'agit du groupe affine.

Rappelons qu'à tout espace affine E est associé un espace vectoriel sous-jacent $\vec{E}$ et que, pour tout choix d'une origine $O \in E$ et d'une base $\mathcal{B} := (e_1, \ldots, e_n)$ de $\vec{E}$, on obtient une bijection :

$$\begin{cases} K^n \to E, \\ (x_1, \ldots, x_n) \mapsto O + x_1 e_1 + \cdots + x_n e_n, \end{cases}$$

où l'expression $O + x_1 e_1 + \cdots + x_n e_n$ désigne l'unique point $M \in E$ tel que $\overrightarrow{OM} = x_1 e_1 + \cdots + x_n e_n$. La donnée d'une origine et d'une base définit un repère affine $\mathcal{R}$. On notera $\phi_{\mathcal{R}}$ la bijection ci-dessus.

À tout application $F : E \to K$ on associe son écriture dans le repère affine $\mathcal{R}$, qui est l'application de K^n dans K définie par : $(x_1, \ldots, x_n) \mapsto F(O + x_1 e_1 + \cdots + x_n e_n)$, autrement dit l'application $P := F \circ \phi_{\mathcal{R}}$.

Lemme 4.3.3 *La propriété : "l'écriture de F dans le repère $\mathcal{R}$ est une fonction polynomiale" est indépendante du choix du repère $\mathcal{R}$.*

Preuve. - Soient $\mathcal{R}_1$ et $\mathcal{R}_2$ deux repères affines, et notons P_1 et P_2 les deux fonctions de K^n dans K associées. Alors $P_2 = P_1 \circ \psi$, où $\psi := \phi_{\mathcal{R}_1}^{-1} \circ \phi_{\mathcal{R}_2}$ est un automorphisme affine de K^n, c'est-à-dire

une application de la forme $X \mapsto AX + B$, où $A \in \mathrm{GL}_n(K)$ et où $B \in K^n$. Il est alors évident que P_2 est une fonction polynomiale si, et seulement si, P_1 l'est. □

Notons aussi que le degré total de P_2 est alors égal à celui de P_1.

Définition 4.3.4 On dit que F est une *fonction polynomiale* sur E si l'une quelconque de ses écritures dans un repère affine l'est. Le *degré* de F est alors le degré total de l'une quelconque de ces écritures.

On notera $K[E]$ la K-algèbre des fonctions polynomiales sur E. C'est une sous-algèbre de $\mathcal{F}(E,K)$ isomorphe à $K[X_1,\ldots,X_n]$, chaque repère $\mathcal{R}$ fournissant un isomorphisme $F \mapsto F \circ \phi_{\mathcal{R}}$.

Définition 4.3.5 On dit qu'une partie $A \subset E$ est *Zariski-dense* si le morphisme de restriction $F \mapsto F_{|A}$ de $K[E]$ dans $\mathcal{F}(A,K)$ est injectif.

Il est clair que c'est bien un morphisme de K-algèbres. La propriété de Zariski-densité dit que si deux fonctions polynomiales sont égales sur A alors elles sont égales. Il suffit de vérifier que si une fonction polynomiale s'annule sur A, elle est nulle partout.

Exemples 4.3.6
1. Si $K = \mathbf{R}$ ou $\mathbf{C}$, toute partie dense de K^n est Zariski-dense : cela tient à la continuité des fonctions polynomiales.
2. Toute partie qui contient une partie Zariski-dense est Zariski-dense (immédiat).
3. Une partie infinie n'est pas nécessairement Zariski-dense (sauf si $n = 1$) : voir une droite ou un cercle dans le plan. Mais, si $A_1,\ldots,A_n$ sont des parties infinies de K, alors $A_1 \times \cdots \times A_n$ est une partie Zariski-dense de K^n. Cela se prouve facilement par récurrence, mais il est chaudement recommandé d'en rédiger la démonstration.

La terminologie "Zariski-dense" sera justifiée au chapitre suivant par l'introduction de la "topologie de Zariski". L'intérêt de cette notion apparaîtra bientôt, mais on donne déjà à la fin du TD quelques applications amusantes fondées sur l'important principe suivant.

Proposition 4.3.7 (Principe de prolongement des identités algébriques) *Soit $F \in K[E]$ une application polynomiale non triviale. Alors $E \setminus F^{-1}(0)$ est Zariski-dense.*

Preuve. - Soit $G \in K[E]$ nulle sur $E \setminus F^{-1}(0)$. La fonction polynomiale FG est donc identiquement nulle : $FG = 0$. Mais $K[E]$ est intègre puisqu'isomorphe à $K[X_1,\ldots,X_n]$. Comme $F \neq 0$, on a bien $G = 0$. □

Exemples 4.3.8
1. Le groupe linéaire $\mathrm{GL}_n(K)$ est Zariski-dense dans l'espace affine $\mathrm{Mat}_n(K)$. En effet, c'est le complémentaire de $\det^{-1}(0)$ et det est une fonction polynomiale non triviale sur $\mathrm{Mat}_n(K)$. (Pour une application, voir l'exercice 4.4.14.)
2. On suppose K algébriquement clos. Alors l'ensemble des matrices diagonalisables est Zariski-dense dans l'espace affine $\mathrm{Mat}_n(K)$. En effet, il contient le complémentaire du lieu d'annulation de la fonction $D(M)$, qui désigne le discriminant du polynôme caractéristique χ_M : c'est une fonction polynomiale des coefficients de χ_M d'après la section 4.2, donc des coefficients de M ; quand $D(M) \neq 0$, la matrice M a n valeurs propres distinctes donc est diagonalisable ; enfin, K étant infini, il y a des matrices diagonales dont les n coefficients diagonaux sont distincts, donc qui n'annulent pas $D(M)$, donc D est non triviale. (Pour une application, voir l'exercice 4.4.15.)

4.4 Exercices sur le chapitre 4

Exercice 4.4.1 Vérifier que, si $A = a_0 + a_1 X$, on a $\mathrm{Res}_{p,q}(A,B) = a_0 b_1^p - a_1 b_0 b_1^{p-1} + \cdots + (-1)^p a_p b_0^p = b_0^p A(-b_0/b_1)$ et que $\mathrm{Res}_{p,q}(A,B) = AQ + BP$ s'obtient facilement par division euclidienne de A par B.

Exercice 4.4.2 Vérifier et compléter les calculs donnant $\mathrm{Res}(aX^2 + bX + c, \lambda X + \mu)$.

Exercice 4.4.3 1) Vérifier les formules donnant $\mathrm{Res}_{p,q}(A,B)$ lorsque $\deg A < p$ ou $\deg B < q$.
2) Vérifier la formule $\mathrm{Res}(B,A) = (-1)^{\deg A \deg B}\mathrm{Res}(A,B)$.
3) Prouver la formule $\mathrm{Res}(QB + A_1, B) = b_p^{\deg A - \deg A_1}\mathrm{Res}(A_1,B)$.
4) Prouver la formule $\mathrm{Res}(A,(X-\beta)C) = A(\beta)\mathrm{Res}(A,C)$.

Exercice 4.4.4 Compléter la preuve de la proposition 4.1.6.

Exercice 4.4.5 1) On suppose L de caractéristique nulle. On appelle *discriminant* du polynôme A de degré p :

$$\mathrm{Dis}(A) := \frac{(-1)^{p(p-1)/2}}{a_p}\mathrm{Res}(A,A').$$

Vérifier que c'est un polynôme à coefficients entiers en les a_i.
2) Démontrer la formule :

$$\mathrm{Dis}(A) := a_p^{2p-2}\prod_{i\neq j}(\alpha_i - \alpha_j).$$

3) Calculer les discriminants de $aX^2 + bX + c$ et de $X^3 + pX + q$ en fonction des coefficients et en fonction des racines.
4) Démontrer la formule : $\mathrm{Dis}(AB) = \mathrm{Dis}(A)\mathrm{Dis}(B)\big(\mathrm{Res}(A,B)\big)^2$.

Exercice 4.4.6 1) Etudier les zéros communs de $A := XY^2 - 1$ et $B := XY - 1$.
2) Etudier les zéros communs de $A := X^2 + Y^2 - 4$ et $B := XY - 1$.
3) Etudier les zéros communs de $A := X^2Y^2 - 1$ et $B := XY - 1$.
4) Etudier les zéros communs de $A := X^2Y^2 - 2$ et $B := XY - 1$.

Exercice 4.4.7 Soient $A := a_0 + \cdots + a_p X^p$ ($a_p \neq 0$) et $B := \lambda X + \mu$ ($\lambda \neq 0$). Démontrer la formule : $\mathrm{Res}(A,B) = \sum_{i=0}^{p}(-1)^i a_i \lambda^{p-i}\mu^i$.

Exercice 4.4.8 Déterminer l'équation cartésienne de la courbe paramétrée :

$$\begin{cases} x = \dfrac{2t}{1+t^2}, \\ y = \dfrac{1-t^2}{1+t^2}. \end{cases}$$

(Mettre ces relations sous forme polynomiale et éliminer t.)

Exercice 4.4.9 On appelle *fenêtre de Viviani* l'intersection de la sphère $x^2 + y^2 + z^2 = 1$ et du cylindre $x^2 - x + y^2 = 0$. Décrire ses projections sur les trois plans de coordonnées. (Il s'agit d'éliminer x, d'où une courbe dans le plan des y,z ; et ainsi de suite.)

Exercice 4.4.10 Déterminer l'équation cartésienne de la surface paramétrée : $x = uv$, $y = v$, $z = u^2$ (*parapluie de Whitney*). (Il s'agit d'éliminer u et v. On doit trouver $x^2 - y^2 z = 0$.) Tous les points qui satisfont à l'équation cartésienne proviennent-ils de la surface de départ ?

Exercice 4.4.11 Éliminer t dans les équations $x = t^n$, $y = t^p$, où $n, p \in \mathbf{N}^*$.

Exercice 4.4.12 1) Soient a, b deux rationnels. En éliminant x entre les relations $x^3 - a = 0$ et $(\gamma - x)^3 - b = 0$, montrer que le réel $\sqrt[3]{a} + \sqrt[3]{b}$ est algébrique.
2) Démontrer par élimination que la somme et le produit de deux nombres algébriques sont algébriques. Appliquer à $\sqrt{3} + \sqrt{2}$ et $\sqrt{3} - \sqrt{2}$ (ainsi, la vérification sera aisée).

Exercice 4.4.13 1) Soient $P, Q \in \mathbf{Z}[X]$ unitaires. Montrer que $\mathrm{Res}_X(P(X+Y), Q(X))$ est un élément unitaire de $\mathbf{Z}[Y]$.
2) On dit que $x \in \mathbf{C}$ est un *entier algébrique* s'il existe $P \in \mathbf{Z}[X]$ unitaire tel que $P(x) = 0$. Montrer que la somme de deux entiers algébriques est un entier algébrique.
3) Proposer une démonstration du fait que le produit de deux entiers algébriques est un entier algébrique.

Exercice 4.4.14 Démontrer la formule $\chi_{MN} = \chi_{NM}$, *i.e.* les polynômes caractéristiques de MN et de NM sont égaux, où $M, N \in \mathrm{Mat}_n(K)$. (Si M ou N est inversible, les matrices MN et NM sont conjuguées et la formule en découle. En général, on fixe M et on dit que les n coefficients non triviaux de $\chi_{MN} - \chi_{NM}$ sont des fonctions polynomiales de N, nulles sur $\mathrm{GL}_n(K)$, donc partout d'après le principe de prolongement des identités algébriques.)

Exercice 4.4.15 Démontrer le théorème de Cayley-Hamilton, *i.e.* $\chi_M(M) = 0$. (C'est facile pour une matrice diagonale, et plus généralement pour une matrice diagonalisable Comme les n^2 coefficients de la matrice $\chi_M(M)$ sont des fonctions polynomiales de M, le cas général en découle par le principe de prolongement des identités algébriques.)

Exercice 4.4.16 (i) Soient $N \in \mathbf{N}^*$ un entier et K un corps de caractéristique nulle (donc tel que les images des entiers $1, \ldots, N \in \mathbf{N}$ dans K sont distinctes). Soit $P \in K[X]$ un polynôme non nul de degré $d \geq 1$. Démontrer que le nombre de points d'annulation de $\tilde{P}$ dans le pavé $[1, N]^n \subset K^n$ est majoré par dN^{d-1}.
(ii) On propose l'algorithme suivant pour tester si un polynôme $P \in K[X_1, \ldots, X_n]$ de degré inférieur ou égal à d est nul : on choisit $a_1, \ldots, a_n \in [1, N]$ et l'on calcule $P(a_1, \ldots, a_n) \in K$. Si l'on trouve 0, on déclare P nul, sinon, on le déclare non nul. Que pensez-vous de cette méthode ?