UPMC PARIS UNIVERSITAS

Modélisation et résolutions numérique et symbolique de problèmes via les logiciels Maple et MATLAB (MODEL)

TD-TME n°8 - Résolution de systèmes polynomiaux

1. TD

Exercice 1 (Polynômes)**.** On dit qu'un polynôme $f \in \mathbb{Q}[X_1,\dots,X_n]$ est homogène si

$$f(\lambda X_1,\dots,\lambda X_n) = \lambda^d f(X_1,\dots,X_n)$$

où d est le degré total de f.

1. Les polynômes ci-dessous sont-ils homogènes ?

$$X^2+Y^2+1, XY+X^2+Y^2, X^3+XYZ+X^2$$

2. Quel est le nombre de monômes de degré 1 dans $\mathbb{Q}[X_1,\dots,X_n]$?

3. Quel est le nombre de monômes de degré 2 dans $\mathbb{Q}[X_1,\dots,X_n]$?

4. Étant donné le nombre de monômes de degré $d-1$, déduire le nombre de monômes de degré d dans $\mathbb{Q}[X_1,\dots,X_n]$.

5. Quel est le nombre de monômes de degré inférieur ou égal à d dans $\mathbb{Q}[X_1,\dots,X_n]$

6. Montrer que l'ensemble des polynômes homogènes de $\mathbb{Q}[X_1,\dots,X_n]$ de degré fixé D est un espace vectoriel.

7. Cet ensemble est-il un anneau ? Même question pour l'ensemble des polynômes homogènes de $\mathbb{Q}[X_1,\dots,X_n]$.

8. Montrer que tout polynôme $f \in \mathbb{Q}[X_1,\dots,X_n]$ se décompose de manière unique en somme de polynômes homogènes.

Exercice 2 (Idéaux)**. 1.** Rappeler le Nullstellensatz. En déduire une méthode pour prouver qu'un système de polynômes dans $\mathbb{Q}[X_1,\dots,X_n]$ admet des solutions dans $\mathscr{C}^n$.
Indication : essayez de ramener le problème à la résolution d'un système linéaire en interprétant les polynômes comme des vecteurs de coefficients.

2. Que faut-il pour faire de cette méthode un algorithme ? Quelle serait la complexité de cet algorithme ?

3. Montrer que pour tout idéal I, $I \subset \sqrt{I}$

4. L'idéal $\langle X^2+bX+c, b^2-4c\rangle$ de $\mathbb{Q}[X,b,c]$ est-il radical ? Si ce n'est pas le cas, quel est son radical ?

5. On dit qu'un idéal I est premier si et seulement si $\forall (f,g) \in A\times A, fg \in I \Longrightarrow f \in I$ ou $g \in I$.
Tous les idéaux premiers sont-ils radicaux ? Tous les idéaux radicaux sont-ils premiers ?

6. Montrer que $V(I\cap J) = V(I)\cup V(J)$.

7. Montrer que $I \subset J \Longrightarrow V(J) \subset V(I)$ et que $V(J)\subset V(I) \Longrightarrow \sqrt{I}\subset\sqrt{J}$.

Exercice 3 (Anneaux-quotients)**. 1.** Soit I un idéal de $\mathbb{Q}[X_1,\dots,X_n]$. Montrez proprement que $\frac{\mathbb{Q}[X_1,\dots,X_n]}{I}$ est un $\mathbb{Q}$-espace vectoriel.

2. Montrer que $\frac{\mathbb{Q}[X_1,\dots,X_n]}{I}$ est engendré par l'image des monômes de $\mathbb{Q}[X_1,\dots,X_n]$ dans $\frac{\mathbb{Q}[X_1,\dots,X_n]}{I}$.

3. Décrire l'anneau-quotient $\mathbb{Q}[X,Y]/\langle X,Y\rangle$. Est-il de dimension finie ? Si oui, quelle est sa dimension ?

4. Décrire l'anneau-quotient $\mathbb{Q}[X,Y]/\langle X^2,Y\rangle$. Est-il de dimension finie ? Si oui, quelle est sa dimension ?

5. Décrire l'anneau-quotient $\mathbb{Q}[X,Y]/\langle X^2, XY, Y^2\rangle$; Est-il de dimension finie ? Si oui, quelle est sa dimension ?

6. Décrire l'anneau-quotient $\mathbb{Q}[X,Y]/\langle XY\rangle$; Est-il de dimension finie ? Si oui, quelle est sa dimension ?

7. Soit I un idéal de dimension 0 dans $\mathbb{Q}[X_1,\ldots,X_n]$. Montrez que si I est radical alors la dimension de $\frac{\mathbb{Q}[X_1,\ldots,X_n]}{I}$ est égale au nombre de points dans $V(I)$.

2. TME

Exercice 4 (Le module `PolynomialIdeals`)**.** Le module `PolynomialIdeals` de MAPLE permet de manipuler les idéaux. Les questions ci-dessous ont pour but de vous familiariser à la manipulation des fonctionnalités de base disponibles dans ce module pour résoudre des systèmes polynomiaux.

1. Chargez le module `PolynomialIdeals`.

2. Que font les fonctions `HilbertDimension` et `IsZeroDimensional` et `NumberOfSolutions` ? Que font les fonctions `UnivariatePolynomial` et `EliminationIdeal` ? Que font les fonctions `IdealMembership`, et `PrimaryDecomposition`.

3. Déclarez les idéaux engendrés par les deux familles de polynômes ci-dessous considérées comme des polynômes à coefficients rationnels dans un premier temps, puis comme des polynômes à coefficients dans $\mathbb{Z}/65521\mathbb{Z}$.

```
cyclic5 := [x*y+y*z+z*t+t*u+u*x,
            x*y*z+y*z*t+z*t*u+t*u*x+u*x*y,
            x+y+z+t+u,
            x*y*z*t+y*z*t*u+z*t*u*x+t*u*x*y+u*x*y*z,
            x*y*z*t*u-1];
katsura4:=[1*x0+2*x3*x2+2*x2*x1-2*x1*x0-4*x3*x0-4*x2*x0-4*x0^2,
           x1-2*x3*x1+2*x2*x0-4*x2*x1-4*x1^2-4*x1*x0+x0^2,
           x2+2*x3*x0-4*x3*x2-4*x2^2-4*x2*x1-4*x2*x0+2*x1*x0,
           -2*x3-2*x2-2*x1-2*x0+6*x3^2+6*x2^2+6*x1^2+6*x0^2+
              8*x3*x1+8*x2*x0+8*x3*x2+8*x2*x1+8*x1*x0+8*x3*x0]
```

4. Ces idéaux sont-ils de dimension zéro, radicaux, premiers ? Combien ont-ils de solutions ?

5. Comment procéder pour vérifier qu'une forme linéaire est séparante lorsque ces idéaux sont radicaux. Trouvez un élément séparant pour ces idéaux.

6. Calculez les valeurs numériques prises par ces éléments séparants en les solutions. Essayez d'en déduire une "méthode" pour obtenir des approximations des solutions.

Exercice 5 (PGCD)**. 1.** Soit A et B deux polynômes de $\mathbb{Q}[X]$. Implantez une fonction qui renvoie Q et R dans $\mathbb{Q}[X]$ tels que $A = BQ + R$ avec $\deg(R) < \deg(B)$.

2. Quelle est la complexité de votre algorithme ? Mettez en place des benchmarks pour "vérifier" expérimentalement votre complexité.

3. Déduisez de votre implantation de la division euclidienne, une implantation de l'algorithme d'Euclide.

4. Quelle est la complexité de l'algorithme d'Euclide ? Mettez en place des benchmarks pour "vérifier" expérimentalement votre complexité.

5. Est-il nécessaire de modifier vos implantations lorsque A et B sont des polynômes de $(\mathbb{Z}/p\mathbb{Z})[X]$ (où p est premier) ? Pourquoi ? Si oui, procédez à ces modifications.

6. Comparez les temps de calcul pour des polynômes A et B dont les coefficients sont vus dans un premier temps dans $\mathbb{Q}$ puis dans $\mathbb{Z}/p\mathbb{Z}$. Que pouvez-vous en déduire ?