TP8 : Méthodes d'élimination : pivot de Gauss et résultant

Références :
— *Algèbre linéaire*, J. Grifone.
— *Calcul mathématique avec SAGE*, multi-auteurs.
— *Cours de calcul formel*, Ph. Saux-Picard.

Ce TP gravite autour de deux méthodes d'élimination pour des systèmes d'équations linéaires (pivot de Gauss) ou polynomiales (résultant). Le pivot de Gauss est un procédé d'échelonnement qui permet, notamment, de calculer efficacement le déterminant d'une matrice carrée. On étudie ensuite les propriétés d'un déterminant en particulier : le résultant de deux polynômes. Celui-ci jouit de propriétés permettant d'être calculé plus efficacement qu'un déterminant quelconque. Enfin, nous utiliserons le résultant comme méthode d'élimination dans le cas de systèmes d'équations polynomiales. En particulier, nous déterminerons les points d'intersection de courbes algébriques.

1 Calcul du déterminant via le pivot de Gauss

Une méthode brutale

1. Rappeler la formule explicite du déterminant d'une matrice $M = (m_{i,j})_{1\leq i,j\leq n}$ via le groupe symétrique S_n.
2. Implémenter l'algorithme associé `det_naif(M)`. Le tester sur des matrices aléatoires de taille $n \times n$ (commencer avec n=3) ; comparer avec la fonction `det` de SAGE.
3. Pour quelle valeur de n ce calcul requiert-il plus d'une seconde ? Exprimer la complexité de l'algorithme en nombre d'opérations $(+, \times)$ sur les scalaires.

Pivot de Gauss pour des matrices à coefficients dans un corps

4. Rappeler comment est modifié le déterminant d'une matrice si l'on :
   — ajoute à une ligne une combinaison linéaire des autres lignes.
   — multiplie une ligne par un scalaire.
   — échange deux lignes.

Une matrice est dite *échelonnée* si le nombre de zéros à gauche augmente strictement de ligne en ligne. La position du premier coefficient non nul est alors appelée *pivot*. L'algorithme du pivot de Gauss consiste à produire, grâce aux trois types d'opération ci-dessus, une matrice échelonnée. Dans le cas d'une matrice carrée, il s'agit donc d'une matrice triangulaire supérieure, dont le déterminant se lit sur la diagonale. Ainsi, pour obtenir le déterminant de la matrice originelle, il suffit de se souvenir des opérations qui l'ont modifié en cours de route.

5. A la main, exécuter l'algorithme sur les matrices M_1 et M_2 :

$$M_1 = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \qquad M_2 = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 2 & 2 & 1 & 0 \\ 1 & 2 & -1 & 1 \\ -1 & 0 & -1 & -3 \end{pmatrix}.$$

6. Ecrire un premier algorithme `det_pivot(M)`, où M est une matrice à coefficients dans un corps (vous avez donc le droit de diviser).
7. Le tester sur les matrices rationnelles M_1 et M_2. Pour des matrices M_3 rationnelles aléatoires de taille 10, calculer `det(M)` puis `det_pivot(M)`.
   On pose :
$$M_4 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$
8. [Pour les curieux.] Calculer `det(M4)`, `det_pivot(M4)`, puis de nouveau `det(M4)`. Tester sur d'autres matrices. D'où proviennent ces erreurs ?
9. Tester votre algorithme sur M_5, vue tour-à-tour comme matrice de $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/7\mathbb{Z}$:
$$M_5 = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 3 \\ 3 & 8 & -1 \end{pmatrix}.$$
10. Jusqu'à quelle taille de matrice peut-on calculer le déterminant pour un délai inférieur à une seconde ? Exprimer la complexité de l'algorithme.
    Tester les temps d'exécution sur d'autres corps que $\mathbb{Q}$.

Pivot de Gauss pour des matrices à coefficients dans un anneau

11. Justifier que le déterminant d'une matrice à coefficients dans un anneau A est encore dans A.
12. Exécuter, à la main, le pivot de Gauss sur la matrice M_6 en vous interdisant de recourir aux fractions :
$$M_6 = \begin{pmatrix} 1 & 3 & 0 \\ 0 & 7 & 3 \\ 0 & 3 & 2 \end{pmatrix}.$$
13. Réécrire un algorithme général `det_pivot_general(M)` valable dans un anneau (division interdite). Le tester sur les matrices précédentes, vues comme matrices à coefficients dans $\mathbb{Z}$.
14. [Remarque.] Dans quels anneaux (et comment) peut-on définir et calculer le *pgcd* et le *ppcm* : euclidiens, principaux, factoriels, intègres ?

2 Résultant et applications

Construction, propriétés

Soit A un anneau commutatif intègre, F son corps des fractions, et $P, Q \in A[X]$ deux polynômes non constants, de degrés p et q respectivement :
$$P = \sum_{i=0}^{p} a_i X^i \qquad Q = \sum_{j=0}^{q} b_j X^j.$$

On considère :
$$\begin{array}{rccc} \psi : & A_{q-1}[X] \times A_{p-1}[X] & \longrightarrow & A_{p+q-1}[X] \\ & (U, V) & \longmapsto & PU + QV. \end{array}$$

15. Montrer qu'il s'agit d'un morphisme de modules, et exprimer sa matrice de la base $((X^{q-1}, 0), (X^{q-2}, 0), ...,$ vers la base $(X^{p+q-1}, ..., X, 1)$.

On appelle la transposée de cette (grosse) matrice : *matrice de Sylvester de P et Q*. Le *résultant de P et Q*, Res(P,Q), est son déterminant. C'est donc un élément de l'anneau A, qui peut aussi être vu comme polynôme en a_i, b_j, à coefficients dans $\mathbb{Z}$.

16. Déterminer à la main le résultant des polynômes $P = aX^2 + bX + c$ et $Q = dX + e$. L'évaluer pour $(a, b, c, d, e) = (1, 2, 0, -1, 4)$ puis $(a, b, c, d, e) = (0, 1, 2, 4, -1)$. Vérifier vos résultats avec SAGE via `P.resultant(Q)`. D'où vient votre erreur ?

17. [Propriété de spécialisation.] Soit à présent B un autre anneau commutatif intègre, et φ un morphisme de A dans B, que l'on étend en un morphisme de $A[X]$ dans $B[X]$. Montrer que :
$$\varphi(Res(P,Q)) = (-1)^{q'(p-p')}\varphi(a_p)^{q-q'}\varphi(b_{q'})^{p-p'}Res(\varphi(P),\varphi(Q)),$$
où p' et q' désignent respectivement les degrés de $\varphi(P)$ et $\varphi(Q)$. Que dire du cas particulier $p = p'$ et $q = q'$?

18. [Cas d'annulation.] On suppose dans cette question que l'anneau A est factoriel. Montrer que : $Res(P,Q) = 0 \Leftrightarrow \exists U \in A_{q-1}[X], V \in A_{p-1}[X]$, non simultanément nuls, tels que $PU + QV = 0$. En déduire que le résultant de P et Q (rappel : ils sont supposés non constants) s'annule si, et seulement si, ils ont un facteur commun non constant dans $A[X]$. Quels sont les avantages du résultant sur le PGCD pour la recherche de facteur(s) commun(s) de polynômes ?

19. [Expression en fonction des racines.] Soit K un surcorps de F dans lequel P et Q sont scindés. Démontrer que leur résultant peut s'écrire :
$$Res(P,Q) \;=\; a_p^q b_q^p \prod_{i,j}(\alpha_i - \beta_j)\,,$$
où α_1,...,α_p et β_1,...,β_q sont les racines de P et Q dans K.

Calcul du résultant via le déterminant

20. Ecrire une fonction `Sylvester(P,Q)` qui, pour deux polynômes P et Q non constants, exhibe leur matrice de Sylvester.

21. En déduire une fonction `resultant-pivot(P,Q)` qui calcule le résultant de deux polynômes non constants via les algorithmes que vous avez construits en partie I. A partir de quel ordre de grandeur de $p \times q$ l'éxécution sur deux polynômes à coefficients dans $\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$ prend-elle plus d'une seconde ? Estimer la complexité (en temps) de l'algorithme. Quel autre problème devinez-vous ?

Calcul du résultant via un algorithme d'Euclide

22. [Cas d'arrêt.]Calculer le résultant de deux polynômes constants non nuls. Ecrire la matrice de Sylvester de P et Q, où $degP \geq 1$ et $degQ = 0$ (indication : réécrire le morphisme ψ et adapter les bases) ; puis déterminer leur résultant.

23. [Propriétés de calcul.] Montrer que, pour P et Q non constants :
(1) $Res(P,Q) = (-1)^{pq}Res(Q,P)$.
(2) $Res(PQ,Q) = 0$, dès lors que Q n'est pas constant.
(3) Si $P_2 \neq 0$, $Res(P_1Q + P_2, Q) = (-b_q)^{degP - degP_2}Res(P_2,Q)$, où $P = P_1Q + P_2$.

24. Déduire des deux questions précédentes un algorithme `resultant-euclide(P,Q)` qui calcule le résultant de P et Q sans passer par le déterminant.

25. Comparer ses performances avec `resultant-pivot(P,Q)` et la fonction `P.resultant(Q)` de SAGE. Estimer sa complexité.

Application à la résolution de systèmes polynomiaux

Exemple 1 : recherche de points d'intersection de courbes algébriques planes

Etant donné un polynôme multivarié à coefficients rationnels $P \in \mathbb{Q}[X,Y]$, la *courbe algébrique plane associée à* P, notée $\mathcal{C}_P$, est l'ensemble des points rationnels du plan qui annulent P :

$$\mathcal{C}_P := \{(x,y) \in \mathbb{Q}^2 : P(x,y) = 0\}.$$

Soient P et $Q \in \mathbb{Q}[X,Y]$. On veut calculer l'intersection des courbes $\mathcal{C}_P$ et $\mathcal{C}_Q$, c'est-à-dire résoudre le système polynomial $S = \{P = 0; Q = 0\}$.

On commence par remarquer que si $(a,b) \in \mathcal{C}_P \cap \mathcal{C}_Q$, alors b est une racine commune aux polynômes univariés $P(a,Y)$ et $Q(a,Y) \in \mathbb{Q}[Y]$. Par conséquent, leur résultant s'annule : $Res_Y(P(a,Y), Q(a,Y)) = 0$; ce qui signifie si l'on désigne par $\bar{P}$ et $\bar{Q}$ les classes de P et Q dans l'anneau quotient $A = \mathbb{Q}[X,Y]/(X-a)$, $Res_Y(\bar{P},\bar{Q}) = 0$. Or, si les degrés de $\bar{P}$ et $\bar{Q}$ sont égaux à ceux de P et Q respectivement, on sait, par la propriété de spécialisation, que :

$$Res_Y(\bar{P},\bar{Q}) = \overline{Res_Y(P,Q)}.$$

Autrement-dit, les abscisses des points d'intersection des courbes $\mathcal{C}_P$ et $\mathcal{C}_Q$ sont les racines de $R = Res_Y(P,Q)$; auxquelles s'ajoutent éventuellement des racines des coefficients dominants de P et $Q \in (\mathbb{Q}[X])[Y]$.

26. Sur SAGE, tracer les courbes d'équation cartésienne $x^2 + y^2 = 1$ et $(x-2)^2 + y^2 = 1$. Combien de points d'intersection comptez-vous ?
27. Par le calcul, commencer par déterminer leurs abscisses, puis dresser la liste de leurs coordonnées. Vos résultats s'accordent-ils avec vos observations ?
28. Même questions pour $\mathcal{C}_1 = \{(x,y) \in \mathbb{Q}^2 : x^4 + y^4 = 1\}$ et $\mathcal{C}_2 = \{(x,y) \in \mathbb{Q}^2 : x^5y^2 - 4x^3y^3 + x^2y^5 = 1\}$. Chercher ensuite les points d'intersection à coordonnées réelles.

Exemple 2 : intersection de surfaces : la fenêtre de Viviani

La *fenêtre de Viviani* est l'intersection de la sphère d'équation $x^2+y^2+z^2 = 1$ et du cylindre d'équation $x^2 - x + y^2 = 0$.

29. Tracer ces deux surfaces sur SAGE.
30. Expliciter puis tracer les projections de la fenêtre selon chacun des axes du repère. (Indication : éliminer une variable puis étudier la courbe obtenue.)