Exercice 1, polynôme à paramètre

Pour quelles valeurs de p le polynôme X^5+X^3-pX+1 admet-il une racine multiple ? Factoriser le polynôme pour cette valeur de p.

Exercice 2, système polynomial

Résoudre le système en éliminant successivement les variables grâce au résultant :

$$\left\{\begin{array}{rcl} a^3+b^3+c^3 & = & 8 \\ a^2+b^2+c^2 & = & 6 \\ a+b+2c & = & 4 \end{array}\right.$$

et en calculant le PGCD des équations obtenues par substitution.

Exercice 3, intersection de courbes

Déterminer l'intersection de $xy=4$ et $y^2=(x-3)(x^2-16)$, repésenter graphiquement les courbes. Discuter la multiplicité et le nombre d'intersections. Même question pour $(x-2)^2+y^2=4$ et $y^2=(x-3)(x^2-16)$.

Exercice 4, primitive

Déterminer

$$\int \frac{1-x^2}{1+x^4}\,dx$$

en utilisant le résultant pour calculer les termes logarithmiques.

Exercice 5, extension algébrique

Montrer que $\mathbb{Q}[\sqrt{2},\sqrt[3]{3}]$ est une extension de degré 6 de $\mathbb{Q}$ en déterminant le polynôme minimal de $\gamma=\sqrt{2}+\sqrt[3]{3}$ par un calcul de résultant et en vérifiant que ce polynôme est irréductible. Exprimer $\sqrt{2}$ puis $\sqrt[3]{3}$ en fonction de γ.

Exercice 6, paramétrisation rationnelle de coniques

Si on connait un point d'une conique, on peut paramétrer rationnellement la conique en cherchant la 2ème intersection d'une droite de pente t et passant par ce point avec la conique.

Le faire pour

$$x^2+4y^2+2xy=4, \quad x^2-3y^2+2xy=4$$

qui passent par le point $(2,0)$. Vérifier qu'on retrouve bien les équations cartésiennes en éliminant t sur les équations paramétriques obtenues.

Exercice 7, Bézout modulaire

Soient A et B des polynômes à coefficients entiers et U et V les polynômes de l'identité de Bézout

$$A=(X+1)^4(X-3), \quad B=(X-1)^4(X+2), \quad AU+BV=\text{resultant}(A,B)$$

1. Donner une majoration à priori des coefficients de U et V.
2. Combien de nombres premiers de taille 31 bits sont-ils nécessaires pour reconstruire U et V à partir du calcul de U et V dans $\mathbb{Z}/p\mathbb{Z}[X]$?
3. Que peut-on dire du coût de cet algorithme en fonction de A et B quelconques ?

TP exercice 1, courbe paramétrique dépendant d'un paramètre :

On considère la courbe C_m dépendant du réel m :

$$x(t)=\frac{t+m}{t^2+1+m^2}, \quad y(t)=\frac{t^2}{t-m}$$

1. Représenter la courbe pour quelques valeurs de m (on pourra utiliser dans un niveau de géométrie, le menu Edit, Ajouter un paramètre pour créer un curseur représentant m, puis utiliser la commande `plotparam`).
2. Donner une équation cartésienne de C_m en éliminant t
3. Déterminer les valeurs de m pour lesquelles la courbe admet un point singulier (i.e. $x'=y'=0$), représenter le graphe dans ce(s) cas.

TP Exercice 2, racines complexes, résultant, Sturm

Pour localiser les racines complexes $z = x + iy$ d'un polynôme $P(z)$, on peut écrire $P(z) = P(x+iy) = R(x,y) + iI(x,y)$ avec R et I les parties réelles et imaginaires de P, vus comme des polynômes en deux variables. Les parties réelles (resp. imaginaires) des racines sont alors racine réelles du résultant de R et I par rapport à y (resp. x) et on peut appliquer une méthode de localisation réelle, par exemple Sturm. Tester par exemple avec $P(z) = z^3 + z + 1$ puis avec un polynôme de degré quelques dizaines. Que peut-on dire du cout de cette méthode en fonction du degré n du polynôme P ?

TP Exercice 3, calcul du résultant modulaire par Euclide

On se donne un nombre premier p et deux polynômes $P, Q \in \mathbb{Z}/p\mathbb{Z}[X]$. Écrire un programme calculant le résultant de P et Q en utilisant l'algorithme d'Euclide : si R est le reste de P par Q, on calcule le résultant de Q et R et on multiplie par $\pm q^d \pmod p$, où q est le coefficient dominant de Q, d la différence entre le degré de P et de R et le signe $\pm$ est - si P et Q sont de degré pairs.

Comment peut-on se servir de ce programme pour calculer le résultant de deux polynômes de $\mathbb{Q}[X]$? Comparer le temps de calcul avec le déterminant de la matrice de Sylvester.

TP Exercice 4, calcul du résultant par interpolation

On se donne deux polynômes $P, Q \in \mathbb{Q}[X,Y]$, où la variable X est la variable principale et la variable Y est vue comme un paramètre. En utilisant l'interpolation polynomiale et le calcul du résultant en une variable, programmer le calcul du résultant de P et de Q.

TP Exercice 5, Bézout modulaire

Programmer l'algorithme de l'exercice 7.

TP Exercice 6, points cocycliques

On cherche une relation algébrique entre les coordonnées de 4 points A, B, C, D qui traduise le fait que ces 4 points sont cocycliques. Cette condition étant invariante par translation, on cherche une relation entre les 6 coordonnées des 3 vecteurs $v_1 = (x_1, y_1)$, $v_2 = (x_2, y_2)$ et $v_3 = (x_3, y_3)$ d'origine A et d'extrémité B, C et D. On peut supposer quitte à translater que le centre du cercle est l'origine, on a donc 5 paramètres : le rayon du cercle R et les 4 angles des points sur le cercle θ_0, θ_1, θ_2 et θ_3. La relation cherchée va s'obtenir en éliminant les 5 paramètres des expressions des 6 coordonnées en fonction de ces paramètres.

1. On paramètre les 4 points du cercle par $R\frac{1+ia}{1-ia}$, $R\frac{1+ib}{1-ib}$, ... Exprimer les 6 coordonnées $x_1, x_2, x_3, y_1, y_2, y_3$ en fonction de R et a, b, c, d. On obtient ainsi 6 équations, par exemple les deux premières sont de la forme
$$x_1 - F(R,a,b) = 0, \quad y_1 - G(R,a,b) = 0$$
où F et G sont deux fractions rationnelles.
2. En réduisant au même dénominateur, calculer 6 polynômes, fonction de $x_1, y_1, x_2, y_2, x_3, y_3, R, a, b, c, d$, qui doivent s'annuler pour que les points soient cocycliques (Vous pouvez utiliser l'instruction `numer` pour obtenir le numérateur d'une fraction rationnelle).
3. Éliminer b des polynômes contenant x_1 et y_1 et factoriser le polynôme obtenu, faire de même avec c, x_2 et y_2 et d, x_3 et y_3, en déduire (en supposant que les points sont tous distincts) 3 polynômes en $x_1, y_1, x_2, y_2, x_3, y_3, R, a$ qui s'annulent.
4. Éliminer R et a, en déduire la relation cherchée.
5. Vérifier que cette relation est équivalente à la nullité de la partie imaginaire du birapport des affixes $\alpha, \beta, \gamma, \delta$ des 4 points :
$$\Im\left(\frac{\alpha-\beta}{\alpha-\gamma}\frac{\delta-\gamma}{\delta-\beta}\right) = 0$$