

COURS DE CALCUL FORMEL EN M1 : TP 11

DES RÉSULTANTS PARTICULIERS : LES SOMMES ET PRODUITS COMPOSÉS

1. CALCUL DE SOMMES ET DE PRODUITS COMPOSÉS

Pour deux polynômes $f, g \in \mathbb{Z}[X]$, on définit la *somme composée* $f \oplus g$ comme l'unique polynôme unitaire de $\mathbb{Q}[X]$ dont les racines sont les sommes $\alpha + \beta$, où $\alpha \in \mathbb{C}$ est une racine de f et $\beta \in \mathbb{C}$ est une racine de g .

- (1) Écrire une fonction `ComposedSumByResultant(f, g, x)` qui calcule $f \oplus g$ à l'aide d'un résultant. Vérifier que cette fonction sur des polynômes linéaires et sur les polynômes $f = X^2 - 2$ et $g = X^2 - 3$ renvoie bien le polynôme souhaité.

Le *produit composé* $f \otimes g$ de f et g est défini comme l'unique polynôme unitaire de $\mathbb{Q}[X]$ dont les racines sont les produits $\alpha\beta$, où $\alpha \in \mathbb{C}$ est une racine de f et $\beta \in \mathbb{C}$ est une racine de g .

- (2) Écrire une fonction `ComposedProductByResultant(f, g, x)`, qui calcule $f \otimes g$ à l'aide d'un résultant. Vérifier cette fonction sur les mêmes polynômes.

2. GROUPE DE GALOIS DU POLYNÔME DE CARTIER-TRINKS

Le groupe projectif spécial linéaire $PSL(2, 7)$ est un groupe simple à 168 éléments, ayant de nombreuses applications importantes en algèbre, géométrie et théorie des nombres. Par exemple, c'est le groupe des symétries du plan projectif à sept points de Fano.

Des arguments théoriques montrent qu'un polynôme f de degré 7 et irréductible dans $\mathbb{Q}[X]$ admet $PSL(2, 7)$ comme groupe de Galois, si et seulement si les conditions suivantes sont simultanément satisfaites :

- (i) le discriminant de f est un carré parfait.
- (ii) le polynôme f_{21} est irréductible dans $\mathbb{Q}[X]$.
- (iii) $f_{35}(X)$ se factorise comme produit de deux polynômes irréductibles sur \mathbb{Q} , de degrés 7 et 28.

Ici, f_{21} et f_{35} sont les polynômes unitaires de degrés $\binom{7}{2} = 21$, resp. $\binom{7}{3} = 35$, dont les racines sont toutes les sommes de 2, resp. 3, racines distinctes de f . Cet exercice montre comment le calcul de ces polynômes se ramène à des résultants.

Soit $f(X) = X^7 - 7X + 3$. En théorie de Galois, ce polynôme est appelé de Cartier-Trinks ; ce qui suit permet de prouver que son groupe de Galois vaut $PSL(2, 7)$.

- (3) Montrer que f est irréductible dans $\mathbb{Q}[X]$ et calculer son discriminant.
- (4) Déterminer f_{21} à l'aide d'un calcul de somme composée et vérifier qu'il est irréductible dans $\mathbb{Z}[X]$.
- (5) Calculer le polynôme f_{35} et le factoriser. On pourra utiliser les formules

$$f \oplus f \oplus f = \prod_{\alpha} (X - 3\alpha) \cdot \prod_{\alpha \neq \beta} (X - (\alpha + 2\beta))^3 \cdot \prod_{\alpha \neq \beta \neq \gamma \neq \alpha} (X - (\alpha + \beta + \gamma))^6,$$

$$\prod_{\alpha} (X - 3\alpha) = f \otimes (X - 3) \quad \text{et} \quad \prod_{\alpha \neq \beta} (X - (\alpha + 2\beta)) = \frac{f \oplus (f \otimes (X - 2))}{f \otimes (X - 3)}.$$

3. CALCUL DE POLYNÔMES DE SWINNERTON-DYER

Les polynômes de Swinnerton-Dyer à une variable sont définis par

$$T_n(X) = \prod (X \pm \sqrt{p_1} \pm \cdots \pm \sqrt{p_n}),$$

où le produit est pris sur toutes les 2^n combinaisons possibles des signes \pm et $(p_n)_{n \geq 1}$, avec $p_1 = 2, p_2 = 3, \dots$, est la suite des nombres premiers. Ces polynômes sont irréductibles dans $\mathbb{Z}[X]$, mais réductibles modulo tout nombre premier p .

- (6) Calculer T_n pour $n = 1, \dots, 7$ à partir de la formule ci-dessus.
- (7) Factoriser les 6 premiers sur \mathbb{Q} et modulo un nombre premier (par exemple le plus grand nombre premier inférieur à 2^{32}).

Pour $n \geq 8$, cette façon de calculer T_n devient trop coûteuse.

- (8) Calculer T_{10} à l'aide de sommes composées itérées.