

TP8 : Décomposition d'un polynôme en produit de polynômes sans facteur multiple

N'oubliez pas d'exécuter (valider avec la touche Entrée) les commandes Maple (texte en rouge) avant de les utiliser.

– Dans $\mathbf{Q[x]}$

On veut écrire un programme qui prenne en entrée un polynôme P de $\mathbf{Q[x]}$ et rende une liste de polynômes Q_i tels que :

- $P = Q_1 Q_2^2 \dots Q_k^k$,
- chaque Q_i soit sans facteur multiple,
- si $i \neq j$ alors $\text{pgcd}(Q_i, Q_j) = 1$,

Remarque : Q_i n'est pas forcément irréductible, c'est le produit des facteurs irréductibles apparaissant avec une puissance i dans P .

On utilise l'algorithme exposé en cours :

Initialisation

On calcule

$$A_1 = \text{pgcd}(P, P') \text{ et } B_1 = \frac{P}{A_1}$$

$$\text{(donc } A_1 = Q_2 Q_3^2 \dots Q_k^{(k-1)} \text{ et } B_1 = Q_1 Q_2 \dots Q_k \text{)}$$

Boucle

On calcule

$$A_2 = \text{pgcd}(A_1, A_1') \text{ et } B_2 = \frac{A_1}{A_2}$$

$$\text{(donc } A_2 = Q_3 Q_4^2 \dots Q_k^{(k-2)} \text{ et } B_2 = Q_2 Q_3 \dots Q_k \text{)}$$

$$\text{et } Q_1 = \frac{B_1}{B_2}, \text{ on a extrait le premier des } Q_i$$

et on recommence jusqu'à ...

- Trouvez un test d'arrêt.
- Faites des tests de votre fonction. Vous pouvez commencer par un polynôme test simple du genre :

```
[ > p:=mul((x-i)^i, i=1..5); p:=expand(p);
```

Fonctions utiles : **diff** pour calculer la dérivée, **gcd** pour calculer le pgcd, **quo** pour calculer

le quotient (a besoin du nom de la variable).

– Dans $\mathbb{Z}/p\mathbb{Z}[x]$

On se demande si on peut utiliser cet algorithme dans $\mathbb{Z}/p\mathbb{Z}[x]$.

Faites un test dans $\mathbb{Z}/3\mathbb{Z}[x]$ sur le polynôme suivant

```
> P :=  
x^19+2*x^18+x^17+x^16+2*x^15+x^12+2*x^11+x^10+x^8+2*x^7+x^6+x  
^5+x^3+x^2+2;
```

en calculant à la main les polynômes A_i, B_i dans $\mathbb{Z}/3\mathbb{Z}[x]$.

Fonctions utiles : pour calculer modulo p vous devez utiliser les fonctions **Gcd** et **Quo**.

- Comprenez-vous d'où vient le problème ?
- Pour mieux comprendre ce qui se passe vous pouvez utiliser la fonction **Factor** pour décomposer le polynôme P et les polynômes A_i, B_i dans $\mathbb{Z}/3\mathbb{Z}[x]$.
- Ecrire une fonction moins exigeante qui décompose le polynôme P en produit $Q_1 Q_2 \dots Q_k$ de polynômes sans facteur multiple.