

TP9 : Décomposition en facteurs irréductibles dans $\mathbb{Z}/p\mathbb{Z}[x]$

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

– Un plus gros exemple toujours dans $\mathbb{Z}/2\mathbb{Z}[x]$

Pour bien comprendre la méthode expliquée en cours on va traiter un plus gros exemple pas à pas en utilisant Maple.

Comme on aura souvent besoin de passer d'un polynôme au vecteur formé par la liste de ses coefficients et vice-versa ces deux fonctions seront utiles :

```
> VectenPoly:=proc(V,dim)
  local i;
  add(V[i]*x^(i-1),i=1..dim)
end:

> VectenPoly([1,2,3,4,5],5);
      1+2x+3x2+4x3+5x4

> PolyenVect:=proc(P,dim)
  local i;
  [seq(coeff(P,x,i),i=0..dim-1)]
end:

> PolyenVect(1+2*x+3*x2+4*x3+5*x4,5);
      [1,2,3,4,5]
```

Les polynômes sont en la variable x.

Comme les polynômes ne sont pas forcément de degré maximal il faut donner la dimension de l'espace vectoriel dans lequel on travaille quand on convertit un polynôme en vecteur :

```
> PolyenVect(1+2*x+3*x2+4*x3+5*x4,8);
      [1,2,3,4,5,0,0,0]
```

On veut décomposer en facteurs irréductibles dans $\mathbb{Z}/2\mathbb{Z}[x]$ le polynôme :

```
> F:=x14+x12+x11+x9+x7+x5+x3+x+1;
      F := x14 + x12 + x11 + x9 + x7 + x5 + x3 + x + 1
```

- Vérifier que F est sans facteur multiple
- Calculer la matrice de l'application linéaire B puis son noyau
- En calculant des pgcd de F avec les polynômes du noyau de B décomposer F en facteurs irréductibles.

Fonctions utiles : **Gcd** , **Rem** , **Nullspace** , **linalg[matrix]** , **linalg[transpose]**

+ *Solution*

– Un programme

Ecrire maintenant un programme qui prenne en entrée un polynôme F et un modulo p et rende, si F est sans facteur multiple, la décomposition de F en facteurs irréductibles dans $\mathbb{Z}/p\mathbb{Z}[x]$.

Pour la lisibilité et la recherche d'erreurs il est souhaitable de décomposer ce programme en

plusieurs fonctions : calcul de la matrice, décomposition par un des polynômes du noyau, ...
Fonctions utiles : **nops** pour le nombre d'éléments d'un ensemble.

- Vérifier sur l'exemple précédent que vous trouvez bien les mêmes facteurs modulo 2,
- décomposer ce polynôme modulo 3, modulo 5 et modulo 7,
- que peut-on remarquer ?
- Peut-on en déduire la décomposition dans $\mathbb{Z}[x]$?

puis sur le polynôme suivant modulo 3 et modulo 5.

[> F1 := x^8+5*x^7+2*x^4+4*x^6+5*x^3+1;

[$F1 := x^8 + 5x^7 + 2x^4 + 4x^6 + 5x^3 + 1$

Que remarque-t-on ?