

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**

On calcule le pgcd de F et sa dérivée :

```
> F1:=diff(F,x) mod 2;
                                F1 := x10 + x8 + x6 + x4 + x2 + 1
> Gcd(F,F1) mod 2;
                                1
```

Donc F est sans facteur multiple.

Attention de bien utiliser Gcd et non gcd pour calculer le pgcd modulo p .

On travaille dans l'espace vectoriel des polynômes de degré inférieur à 14.

On choisit pour base $1, x, x^2, \dots, x^{13}$ et on va écrire la matrice de l'application linéaire

$B(g(x)) = (g(x)^2 - g(x)) \bmod F(x)$ dans cette base.

Pour cela on calcule les images des vecteurs de base et on les met sous forme de vecteurs :

```
> for i from 0 to 13 do
    V[i] := PolyVect(Rem(x^(2*i) - x^i, F, x) mod 2, 14)
od;
```

$$V_0 := [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]$$

$$V_1 := [0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]$$

$$V_2 := [0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0]$$

$$V_3 := [0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0]$$

$$V_4 := [0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0]$$

$$V_5 := [0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0]$$

$$V_6 := [0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0]$$

$$V_7 := [1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0]$$

$$V_8 := [1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1]$$

$$V_9 := [1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1]$$

$$V_{10} := [0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0]$$

$$V_{11} := [0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1]$$

$$V_{12} := [0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0]$$

$$V_{13} := [1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0]$$

On voudrait construire la matrice qui a pour colonnes les vecteurs calculés, une solution est d'utiliser la fonction transpose de la librairie linalg :

```
> A := linalg[matrix]([seq(V[i], i=0..13)]);
```

```

A :=
[ 0 0 0 0 0 0 0 0 0 0 0 0 0 0
  0 1 1 0 0 0 0 0 0 0 0 0 0 0
  0 0 1 0 1 0 0 0 0 0 0 0 0 0
  0 0 0 1 0 0 1 0 0 0 0 0 0 0
  0 0 0 0 1 0 0 0 1 0 0 0 0 0
  0 0 0 0 0 1 0 0 0 0 1 0 0 0
  0 0 0 0 0 0 1 0 0 0 0 0 1 0
  1 1 0 1 0 1 0 0 0 1 0 1 1 0
  1 1 1 0 0 0 0 0 1 0 0 0 1 1
  1 0 0 0 0 1 1 1 1 0 1 1 0 1
  0 1 0 0 1 0 1 1 0 1 1 1 0 0
  0 0 0 1 0 0 1 0 1 1 0 0 0 1
  0 1 1 0 1 1 1 0 0 0 0 1 0 0
  1 1 0 0 1 1 1 0 1 1 0 1 1 0 ]

```

```
> B:=linalg[transpose](A);
```

```

B :=
[ 0 0 0 0 0 0 0 1 1 1 0 0 0 1
  0 1 0 0 0 0 0 1 1 0 1 0 1 1
  0 1 1 0 0 0 0 0 1 0 0 0 1 0
  0 0 0 1 0 0 0 1 0 0 0 1 0 0
  0 0 1 0 1 0 0 0 0 0 1 0 1 1
  0 0 0 0 0 1 0 1 0 1 0 0 1 1
  0 0 0 1 0 0 1 0 0 1 1 1 1 1
  0 0 0 0 0 0 0 0 0 1 1 0 0 0
  0 0 0 0 1 0 0 0 1 1 0 1 0 1
  0 0 0 0 0 0 0 1 0 0 1 1 0 1
  0 0 0 0 0 1 0 0 0 1 1 0 0 0
  0 0 0 0 0 0 0 1 0 1 1 0 1 1
  0 0 0 0 0 0 1 1 1 0 0 0 0 1
  0 0 0 0 0 0 0 0 1 1 0 1 0 0 ]

```

On peut maintenant calculer une base de son noyau dans $\mathbb{Z}/2\mathbb{Z}$.

```
[ > KerB:=Nullspace(B) mod 2;  
KerB := {[0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1], [0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0],  
[1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]}]
```

Le noyau est de dimension 3, **on sait donc que F est le produit de 3 polynômes irréductibles.**

On reconnaît en dernier les constantes qui ne nous intéressent pas, on a donc deux polynômes intéressants

```
[ > g1:=VectenPoly(KerB[1],14);g2:=VectenPoly(KerB[2],14);  
g1 := x3+x4+x7+x13  
g2 := x+x2+x7+x8+x11+x12]
```

Comme F divise $g1^2 - g1 = g1(g1 - 1)$ on va calculer les pgcd(F,g1) et pgcd(F,g1-1)

```
[ > F1:=Gcd(F,g1) mod 2;F2:=Gcd(F,g1-1) mod 2;  
F1 := x9+x8+x7+x6+x5+x4+1  
F2 := x5+x4+x3+x+1]
```

On a bien une décomposition de F mais pas en 3 facteurs

```
[ > expand(F1*F2) mod 2;  
x14+x12+x11+x9+x7+x5+x3+x+1]
```

L'un des facteurs n'est pas irréductible .

On essaie g2 et F1

```
[ > F3:=Gcd(F1,g2) mod 2;F4:=Gcd(F1,g2-1) mod 2;  
F3 := x5+x3+1  
F4 := x4+x3+1]
```

On a eu de la chance

```
[ > expand(F2*F3*F4) mod 2;  
x14+x12+x11+x9+x7+x5+x3+x+1]
```

Donc la décomposition de F en facteurs irréductibles est

$$F = (x^4 + x^3 + 1)(x^5 + x^3 + 1)(x^5 + x^4 + x^3 + x + 1) .$$

On vérifie

```
[ > Factor(F) mod 2;  
(x5+x4+x3+x+1)(x5+x3+1)(x4+x3+1)]
```

– 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;
      FI := x^8 + 5 x^7 + 2 x^4 + 4 x^6 + 5 x^3 + 1
```

Que remarque-t-on ?

Solution

```
> FactIrrModp:=proc(F0,p)
  local an,d,F,MB,KerMB,NbFactIrr,ListFact,V,Vpol;
  global NbFactActuel;

  if Gcd(F0,diff(F0,x)) mod p <>1
  then ERROR('F a un facteur multiple') fi;

  an:=lcoeff(F0);d:=degree(F0);
  if an<>1 then F:=F0/an mod p
  else F:=F0 fi;

  MB:=MatriceBerlekamp(F,p);
  KerMB:=Nullspace(MB) mod p;
  NbFactIrr:=nops(KerMB);

  if NbFactIrr=1 then RETURN(an,F) fi;
  ListFact:=[F];NbFactActuel:=1;
  for V in KerMB do
    Vpol:=VectenPoly(V,d);
    if degree(Vpol)>0 then
      ListFact:=map(Decomp,ListFact,Vpol,p,NbFactIrr)
      fi;
    if NbFactActuel=NbFactIrr then RETURN(an,ListFact) fi;
  od;
end;
```

On commence par quelques tests :

- Si le polynôme P n'est pas sans facteur multiple on déclenche une erreur.
- S'il n'est pas unitaire on extrait le coefficient principal a_n et on factorise le polynôme

unitaire $\frac{P}{a_n}$.

Ensuite on calcule la matrice de Berlekamp MB et une base de son noyau. On connaît désormais le nombre de facteurs irréductibles de P : c'est la dimension du noyau . On choisit la stratégie d'utiliser les différents vecteurs de cette base jusqu'à avoir le bon nombre de facteurs. Pour cela on va utiliser une variable globale $NbFactActuel$ qui est augmentée chaque fois qu'on décompose un facteur (voir la procédure `Decomp`).

- Si le nombre de facteurs irréductibles de P est 1 on retourne directement a_n, P .
- Sinon on fait une boucle sur les vecteurs V de la base de $\text{Ker}(MB)$.
- Si le vecteur correspond à un polynôme constant on saute l'itération : elle ne décomposera rien.

- Sinon on essaie de décomposer les différents facteurs déjà obtenus.
- A la fin de chaque itération on teste et on arrête si on a le nombre de facteurs souhaité.

La procédure retourne $a_n, [P_1, \dots, P_k]$ où les P_i sont les facteurs irréductibles de P .

Le calcul de la matrice.

```
> MatriceBerlekamp:=proc(F,p)
  local d,i,Xpk,C,k;
  d:=degree(F,x);C[0]:=[seq(0,i=1..d)];Xpk:=1;
  for k from 1 to d-1 do
    Xpk:=Rem(Xpk*x^p,F,x) mod p; C[k]:=PolyenVect(Xpk,d);
    C[k][k+1]:=C[k][k+1]-1 mod p
  od;
  linalg[transpose](matrix([seq(C[k],k=0..d-1)]))
end;
```

Une optimisation : on ne calcule pas brutalement $x^{(p^{(k+1)})} \bmod P(x)$, ayant calculé $x^{(p^k)} \bmod P(x)$ on multiplie celui-ci par x^p et on le réduit modulo $P(x)$. Les polynômes sont ainsi de degré maximal $p+d-1$ au lieu de kp . C'est particulièrement intéressant si p et d sont grands.

On retranche ensuite x^k au vecteur représentant $x^{(p^k)} \bmod P(x)$. Attention au décalage : $C[k]$ est la colonne $k+1$ de la matrice.

On essaie de décomposer un des facteurs.

```
> Decomp:=proc(Pol,Vpol,p,NbFactIrr)
  local i,LFact,Pgcd;
  global NbFactActuel;
  if degree(Pol)=1 or NbFactActuel=NbFactIrr then
    RETURN(Pol) fi;
  LFact:=NULL;
  for i from 0 to p-1 do
    Pgcd:=Gcd(Pol,Vpol-i) mod p;
    if degree(Pgcd)>0 then LFact:=LFact,Pgcd fi
  od;
  NbFactActuel:=NbFactActuel+nops([LFact])-1;
  LFact
end;
```

Si le degré du facteur est 1 ou si l'on a déjà le bon nombre de facteurs on ne fait rien, on retourne le facteur tel quel.

Sinon on calcule les pgcds avec le vecteur du noyau moins i et on stocke ceux qui ne sont pas des constantes.

Après la boucle on augmente le nombre de facteurs actuel du nombre de facteurs de Pol moins 1 et on rend la séquence des facteurs.

Une optimisation possible : on arrête la boucle des pgcds dès que la somme des degrés des facteurs dans $LFact$ vaut le degré de $Lpol$.

Les tests :

```
> FactIrrModp(F,2);
1, [x^5+x^3+1, x^4+x^3+1, x^5+x^4+x^3+x+1]
```

On retrouve bien les mêmes facteurs.

On essaie maintenant modulo 3, 5 et 7.

```
[ > FactIrrModp(F, 3);  
1, [x12 + 2x10 + x9 + 2x8 + 2x7 + 2x6 + 2x4 + x3 + 2x2 + 2x + 2, x + 2, x + 1]
```

On a encore trois facteurs mais qui n'ont rien à voir : deux de degré 1 et un de degré 12.

```
[ > FactIrrModp(F, 5);  
1, x14 + x12 + x11 + x9 + x7 + x5 + x3 + x + 1
```

F est irréductible modulo 5.

```
[ > FactIrrModp(F, 7);  
1, [x12 + 6x10 + x9 + 2x8 + 6x7 + 3x6 + 3x5 + x4 + 2x3 + 5x2 + 4x + 4, x2 + 2]
```

F a deux facteurs modulo 7.

On peut remarquer que la décomposition de F en facteurs irréductibles dépend fortement du $\mathbb{Z}/p\mathbb{Z}$: le nombre et le degré des facteurs changent.

Si un polynôme unitaire a des facteurs irréductibles dans $\mathbb{Z}[x]$ on retrouve ces facteurs dans $\mathbb{Z}/p\mathbb{Z}[x]$ mais ils ne sont plus forcément irréductibles, ils peuvent encore se décomposer. Du fait que F est irréductible modulo 5 on peut déduire que F est irréductible dans $\mathbb{Z}[x]$.

Un autre test :

```
[ > FactIrrModp(F1, 3);  
Error, (in FactIrrModp) F a un facteur multiple  
[ > FactIrrModp(F1, 5);  
1, [x + 3, x + 2, x3 + 3x2 + x + 2, x3 + 2x2 + x + 3]
```

Le fait d'être sans facteur multiple dépend aussi du $\mathbb{Z}/p\mathbb{Z}$:

```
[ > Factor(F1) mod 3;  
  
1, (x + 2)2 (x3 + 2x2 + 2x + 2)2  
[ >
```