Ex.3 Berlekamp

Il s'agit de factoriser un polynôme Q en mettant en oeuvre l'algorithme de Berlekamp, donc sans utiliser des instructions toutes faites comme `factor(Q)` *. Vous pouvez cependant vérifier la pertinence de vos réponses avec les intructions évoluées de Sagemath tel* `factor()` *.*

Ex. On définit $Q \in \mathbb{Z}[X]$ par :

```
X=ZZ['X'].gen()
Q=X^15 + 3*X^14 + 13*X^13 + 33*X^12 + 72*X^11 + 124*X^10 + 188*X^9 + 242*X^8 + 273*X^7 + 264*X^6 + 223
*X^5 + 160*X^4 + 96*X^3 + 45*X^2 + 15*X + 3
```

a. Le polynôme Q a t-il des facteurs multiples ? Lesquels ? Quelle factorisation de Q en déduit on (ie sans utiliser `factor()`) ?

Attention : Sagemath considère le résultat de `Q/Q1` comme un élément du corps des fractions de l'anneau de polynômes, même si Q1 divise Q. Préférer l'instruction `Q//Q1`

```
print ((X^2-1)/(X-1)).parent()
print ((X^2-1)//(X-1)).parent()
Fraction Field of Univariate Polynomial Ring in X over Integer Ring
Univariate Polynomial Ring in X over Integer Ring
```

Rép. Q a des facteurs multiples (au moins dans $\mathbb{Q}[X]$ et en fait dans $\mathbb{Q}[X]$) si et seulement si son pgcd avec Q' (le polynôme dérivé de Q) est différent de ± 1, ce qui est le cas ici, et alors $Q \wedge Q'$ est un facteur non trivial de Q.

In [32]:
```
X=ZZ['X'].gen()
Q=X^15 + 3*X^14 + 13*X^13 + 33*X^12 + 72*X^11 + 124*X^10 + 188*X^9 + 242*X^8 + 273*X^7 + 264*X^
6 + 223*X^5 + 160*X^4 + 96*X^3 + 45*X^2 + 15*X + 3
Q0=gcd(Q,Q.derivative())
Q1=Q//Q0
print 'Q0 =',Q0
print 'Q1 =',Q1
print 'Q%Q0 =',Q%Q0
```

```
Q0 = X^2 + X + 1
Q1 = X^13 + 2*X^12 + 10*X^11 + 21*X^10 + 41*X^9 + 62*X^8 + 85*X^7 + 95*X^6 + 93*X^5 + 76*X^4 +
54*X^3 + 30*X^2 + 12*X + 3
Q%Q0 = 0
```

Si on connaît une décomposition en facteurs irréductibles (au moins dans $\mathbb{Q}[X]$), $Q \wedge Q' = \prod_i R_i^{\alpha_i}$, alors on peut dire un peu mieux : $\prod_i R_i^{\alpha_i+1}$ divise Q.
Ici X^2+X+1 est irréducible dans $\mathbb{Q}[X]$ car sans racines réelles donc $(X^2+X+1)^2$ divise Q.

In [69]:
```
print 'Vérification : Q%Q0^2 =',Q%Q0^2
print 'Q//Q0^2 =',Q//Q0^2
```

```
Vérification : Q%Q0^2 = 0
Q//Q0^2 = X^11 + X^10 + 8*X^9 + 12*X^8 + 21*X^7 + 29*X^6 + 35*X^5 + 31*X^4 + 27*X^3 + 18*X^2 +
9*X + 3
```

b. Quelles sont les racines de Q dans $\mathbb{F}_7$? et dans $\mathbb{F}_2$?

Q a t-il des racines dans $\mathbb{Z}$?

Quelle factorisation de Q dans $\mathbb{F}_7[X]$ déduit on de ce qui précède ?

★ Comment se compare le quotient $Q//Q1$ de la division euclidienne dans $\mathbb{Z}[X]$ de Q par un polynôme $Q1$ avec le quotient de la division euclidienne dans $\mathbb{F}_7[X]$?

In [70]:
```
print 'racines de Q dans F7 :',[x for x in GF(7) if Q(x)==0]
print 'racines de Q dans F2 :',[x for x in GF(2) if Q(x)==0]
```

```
racines de Q dans F7 : [2, 3, 4, 6]
racines de Q dans F2 : []
```

Une racine de Q dans $\mathbb{Z}$ serait aussi racine dans $\mathbb{F}_2$ donc Q est sans racine dans $\mathbb{Z}$.

Dans $\mathbb{F}_7[X]$ on a $\prod_{x\in\mathbb{F}_7, Q(x)=0}(X-x)$ divise Q donc $(X-2)(X-3)(X-4)(X-6)$ divise Q dans $\mathbb{F}_7[X]$.

Le quotient de la division euclidienne dans $\mathbb{F}_7[X]$ de Q par un polynôme $Q_2 \in \mathbb{Z}[X]$ est la classe de $Q//Q_2 \in \mathbb{Z}[X]$ dans $\mathbb{F}_7[X]$; il peut se calculer comme $(Q//Q_2)\%7$.

On peut dire mieux en tenant compte de la première factorisation et des multiplicités des racines :

In [35]:
```
#Racines de Q0 et Q1
print [x for x in GF(7) if Q0(x)==0]
print [x for x in GF(7) if Q1(x)==0]
print (Q1//prod((X-x) for x in [2,3,4,6]))%7
```

```
[2, 4]
[2, 3, 4, 6]
X^9 + 3*X^8 + 3*X^7 + 6*X^6 + 5*X^4 + 3*X^3 + 3*X^2 + 6
```

In [25]:
```
#Multiplicité des racines de Q1
for i in range(4):print [x for x in GF(7) if Q1.derivative(i)(x)==0]
```

```
[2, 3, 4, 6]
[2, 3]
[4]
[]
```

In [42]:
```
#Factorisation de Q1 en tenant compte des multiplicités
print Q1//((X-2)^2*(X-3)^2*(X-4)*(X-6))%7
print Q1%((X-2)^2*(X-3)^2*(X-4)*(X-6))%7
```

```
X^7 + X^6 + 2*X^5 + 3*X^4 + 3*X^3 + 2*X^2 + 2*X + 1
0
```

c. On pose $Q_1 = X^9 + 3*X^8 + 3*X^7 + 6*X^6 + 5*X^4 + 3*X^3 + 3*X^2 + 6$. Vérifier que Q_1 est un facteur de Q.

On définit l'anneau quotient $K = \mathbb{F}_7[X]/(Q_1)$ et on note x la classe de X dans K. $\mathbb{F}_7$ s'identifie aux classes des polynômes constants dans K.

```
Q1=X^9 + 3*X^8 + 3*X^7 + 6*X^6 + 5*X^4 + 3*X^3 + 3*X^2 + 6
K=GF(7)['X'].quotient(Q1,'x');x=K.gen()
print K
```

Pour a un élément de K l'instruction `a.list()` donne la liste des coordonnées de a dans la base canonique de K sur $\mathbb{F}_7$. De quelle base canonique s'agit il ?

On peut convertir cette liste en un vecteur par l'instruction `vector(a.list())` ou en une matrice par `matrix(a.list())` . Inversement on peut convertir une liste l de coefficients en un élément de K par l'instruction `K(l)` . Si C est une matrice (ligne ou colonne) de coordonnées ou un vecteur, on convertit préalablement C en liste : `K(C.list())` .
Essayer les instructions `print K([1,0,0,2,0])` , `print K([1,0,0,2,0]).list()` , `print K(matrix([1,0,0,2,0]).list())`

Combien y a t-il d'éléments dans K ? Pourquoi ?

Rép. On calcule $Q\%Q1$ et $Q\%Q1\%7$ dans $\mathbb{Z}[X]$. Le premier donne la divisibilité de Q par Q_1 dans $\mathbb{Z}[X]$, le second dans $\mathbb{F}_7[X]$.

Dans $\mathbb{F}_7[X]$, Q_1 divise Q si et seulement si $Q(x) = 0$ dans K.

In [44]:
```
Q1=X^9 + 3*X^8 + 3*X^7 + 6*X^6 + 5*X^4 + 3*X^3 + 3*X^2 + 6
print 'Q%Q1 =',Q%Q1
print 'Q%Q1%7 =',Q%Q1%7
K=GF(7)['X'].quotient(Q1,'x');x=K.gen()
print K
print 'Q(x)=',Q(x)
```

```
Q%Q1 = -777*X^8 - 147*X^7 - 1848*X^6 + 504*X^5 - 1323*X^4 - 546*X^3 - 1176*X^2 + 525*X - 1827
Q%Q1%7 = 0
Univariate Quotient Polynomial Ring in x over Finite Field of size 7 with modulus X^9 + 3*X^8 +
3*X^7 + 6*X^6 + 5*X^4 + 3*X^3 + 3*X^2 + 6
Q(x)= 0
```

Pour $a \in K$, l'instruction `a.list()` donne les coordonnées de a dans la base canonique $(1, x, x^2, \ldots, x^{\deg(Q_1)-1})$.

K est un $\mathbb{F}_7$-espace vectoriel de dimension $\deg(Q_1) = 9$ donc a 7^9 éléments.

In [47]:
```
print '7^9 =',7^9,'vérification K.cardinality() =',K.cardinality()
```

```
7^9 = 40353607 vérification K.cardinality() = 40353607
```

d. Calculer la matrice M_F du Frobenius $x \mapsto x^7$ relativement à la base canonique de K comme $\mathbb{F}_7$-espace vectoriel.

In [52]:
```
print (x^2).list()
```

```
[0, 0, 1, 0, 0, 0, 0, 0, 0]
```

In [56]:
```
MF=matrix([(x^(7*i)).list() for i in range(9)]).transpose()
show(MF)
```

Out[56]:
$$\begin{pmatrix} 1 & 0 & 2 & 3 & 6 & 2 & 4 & 3 & 4 \\ 0 & 0 & 3 & 4 & 1 & 5 & 1 & 5 & 4 \\ 0 & 0 & 0 & 6 & 0 & 3 & 1 & 5 & 2 \\ 0 & 0 & 5 & 1 & 4 & 3 & 0 & 0 & 4 \\ 0 & 0 & 2 & 4 & 1 & 3 & 6 & 0 & 2 \\ 0 & 0 & 6 & 1 & 2 & 2 & 2 & 3 & 5 \\ 0 & 0 & 5 & 1 & 0 & 5 & 5 & 1 & 6 \\ 0 & 1 & 1 & 5 & 1 & 0 & 6 & 1 & 0 \\ 0 & 0 & 3 & 3 & 5 & 0 & 6 & 6 & 5 \end{pmatrix}$$

e. Comment s'interprète les colonnes de la matrice N définie par l'instruction ci-dessous ?

```
N=matrix((MF-identity_matrix(Q1.degree())).right_kernel().basis()).transpose()
```

In [57]:
```
N=matrix((MF-identity_matrix(Q1.degree())).right_kernel().basis()).transpose()
show(N)
```

Out[57]:
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 4 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 6 & 6 & 2 \\ 0 & 6 & 0 & 1 \\ 0 & 0 & 6 & 1 \\ 0 & 6 & 3 & 1 \end{pmatrix}$$

Il s'agit de la matrice des coordonnées (dans la base canonique de K) des vecteurs d'une base de $\mathrm{Ker}(MF - I)$, c'est à dire de l'espace propre du Frobenius pour la valeur propre 1 (l'espace des points fixes du Frobenius).

On donne

```
N=matrix(GF(7),9,4,[1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 4, 0, 0, 0, 0, 1, 0, 6, 6, 2, 0, 6, 0,
 1, 0, 0, 6, 1, 0, 6, 3, 1])
```

Que dit le rang de N sur le polynôme Q_1 ?

Quels sont les éléments de $\mathbb{F}_7 \subset K$ parmi $\mathrm{Im}(N)$?

Exhiber un élément P de Im(N) qui ne soit pas dans $\mathbb{F}_7$? Combien y a t-il de tels éléments ?

Pouvez vous exhiber un $a \in \mathbb{F}_7$ tel que Q_1 et $P - a$ aient un facteur commun non trivial dans $\mathbb{F}_7[X]$?

In [58]:
```
N=matrix(GF(7),9,4,[1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 4, 0, 0, 0, 0, 1, 0, 6, 6, 2, 0,
6, 0, 1, 0, 0, 6, 1, 0, 6, 3, 1])
show(N)#comparer avec le calcul de N ci-dessus
```

Out[58]:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 4 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 6 & 6 & 2 \\ 0 & 6 & 0 & 1 \\ 0 & 0 & 6 & 1 \\ 0 & 6 & 3 & 1 \end{pmatrix}$$

N est de rang 4 puisque ses vecteurs colonnes forment une base. L'espace des points fixes du Frobenius $K \to K, y \mapsto y^7$ est de dimension 4 ce qui indique que Q_1 a quatre facteurs premiers.

$\mathbb{F}_7$ s'identifie aux classes dans K des polynômes constants, donc aux éléments de K dont les coordonnées dans la base canonique sont des multiples du vecteur $(1, 0 \ldots, 0)$. Cela correspond au sous-espace engendré par la première colonne de N.

Toute combinaison linéaire des quatre colonnes de N autres que les multiples de la première colonne donne un élément de $\mathrm{Im}(N) \setminus \mathbb{F}_7$; il y en a $\mathrm{card}(\mathrm{Im}(N)) - \mathrm{card}(\mathrm{Vect}((1, 0, \ldots, 0))) = (7^9)^4 - 7$.

La deuxième colonne fournit les coordonnées d'un tel élément.

In [63]:
```
P=K((N*vector([0,1,0,0])).list());print 'P =',P
```

```
P = 6*x^8 + 6*x^6 + 6*x^5 + x^3 + x
```

In [67]:
```
L=GF(7)['X']
print L(P.list())#représentant de P\in K dans F_7[X]
print [(a,gcd(Q1,L(P.list())-a)) for a in GF(7)]
```

```
6*X^8 + 6*X^6 + 6*X^5 + X^3 + X
[(0, 1), (1, X^2 + 2*X + 6), (2, 1), (3, 1), (4, 1), (5, 1), (6, X^7 + X^6 + 2*X^5 + 3*X^4 + 3*
X^3 + 2*X^2 + 2*X + 1)]
```

$Q1 \wedge (P - 1) = X^2 + 2X + 6$ est un facteur non trivial de Q_1 (On remplace ici $P - 1$ qui est une classe modulo Q_1 par un représentant dans $\mathbb{F}_7[X]$).

f. ★ Calculer la décomposition de Q en facteurs irréductibles.

g. ★★ Quelles sont les racines de Q dans $\mathbb{F}_7[X]/(Q)$?

f.rép. On décompose $X^2 + 2X + 6$ en facteurs premiers dans $\mathbb{F}_7[X]$ en cherchant ses racines dans $\mathbb{F}_7$; on recommence l'algorithme de Berlekamp pour $Q1//(X^2 + 2X + 6)$ jusqu'à ce que chaque facteur soit irréductible.