Algèbre effective -- corps finis

F-X. Dehon - dehon@unice.fr - 7 nov 2019

0. K anneau de cardinal fini

L'application linéaire $\mathbb{Z} \to K, n \mapsto n1_K$ a un noyau non trivial $p\mathbb{Z}$ avec $p > 0$. Elle induit une inclusion de l'anneau $\mathbb{Z}/p\mathbb{Z}$ dans K.

Si K est intègre alors p est premier et l'inclusion $\mathbb{F}_p \to K$ fait de K une $\mathbb{F}_p$-algèbre de dimension finie comme $\mathbb{F}_p$ - espace vectoriel. En particulier le cardinal de K est une puissance de p : $\#K = p^{\dim_{\mathbb{F}_p} K}$.

Egalement pour chaque $x \in K$, la famille $(1, x, \ldots, x^{\dim_{\mathbb{F}_p} K})$ est liée sur $\mathbb{F}_p$, ce qui s'interprète comme :

$$\exists Q \neq 0 \in \mathbb{F}_p[X],\ \mathrm{d}^\circ Q \leq \dim_{\mathbb{F}_p} K \text{ et } Q(x) = 0\ .$$

Le polynôme minimal de x sur $\mathbb{F}_p$ est le polynôme à coefficients dans $\mathbb{F}_p$ unitaire de degré minimal annulant x.

Exemples :

- $K = \mathrm{M}_n(\mathbb{F}_p)$, l'algèbre des matrices de taille n à coefficients dans $\mathbb{F}_p$ est une $\mathbb{F}_p$-algèbre, non intègre si $n > 1$.
- $K = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ ne contient pas de corps.

Un élément d'un anneau fini est inversible pour la multiplication si et seulement si il est racine du polynôme $X^n - 1$ pour un certain n. $n = \#K^\times$ convient. ($K^\times$ désigne le groupe des éléments inversibles pour la multiplication, appelé aussi "groupe des unités".)

Prop. Soit K un anneau commutatif intègre ; alors tout sous-groupe fini de $K^\times$ est cyclique.

Le point clé est que si K est intègre, le nombre de racines dans K du polynôme $X^n - 1$ est majoré par n.

Prop. Soit K un corps fini ; alors $X^{\#K} - X = \prod_{x \in K}(X - x)$. Autrement dit $X^{\#K} - X$ est scindé à racines simples dans K et ses racines sont exactement les éléments de K.

Algèbre des matrices sur $\mathbb{F}_2$ dans Sagemath

In [8]:
```
M = MatrixSpace(GF(2),3,3) #QQ
A=M([0,1,1, 1,0,1, 1,1,1])
#A=matrix(GF(2),3,3,[0,1,1, 1,0,1, 1,1,1])
show('A =',A,', A^2 =',A^2)
N=span([vector(A^0),vector(A^1),vector(A^2),vector(A^3)]) #span([A^0,A^1,A
^2]) produit une erreur
print 'N:',N
print "dimension =", N.dimension()
```

Out[8]:

$$\mathtt{A} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \quad \mathtt{A\hat{}2} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

```
N: Vector space of degree 9 and dimension 3 over Finite Field of size 2
Basis matrix:
[1 0 0 0 1 0 0 0 1]
[0 1 0 1 0 0 0 0 1]
[0 0 1 0 0 1 1 1 0]
dimension = 3
```

L'implémentation de l'algèbre linéaire symbolique est lacunaire dans Sagemath (en nov. 2019), plus encore sur un corps fini ; chacune des trois dernières lignes ci-dessous produit une erreur.

```
A=matrix(GF(2),3,3,[0,1,1, 1,0,1, 1,1,1])
var('x y z')
solve([A^3==x*A^0+y*A^1+z*A^2],x,y,z)
solve([vector(A^3)==x*vector(A^0)+y*vector(A^1)+z*vector(A^2)],x,y,z)
solve([vector(A^3)[i]==x*vector(A^0)[i]+y*vector(A^1)[i]+z*vector(A^2)[i] for i i
n range(3)],x,y,z)
```

La dernière ligne fonctionne pour `A=matrix(QQ,3,3,[0,1,1, 1,0,1, 1,1,1])` ($\mathbb{Q}$ comme anneau de coefficients au lieu de $\mathbb{F}_2$)

In [3]:
```
A=matrix(QQ,3,3,[0,1,1, 1,0,1, 1,1,1])
var('x y z')
solve([vector(A^3)[i]==x*vector(A^0)[i]+y*vector(A^1)[i]+z*vector(A^2)[i]
for i in range(3)],x,y,z)
```

Out[3]:
```
[[x == 1, y == 3, z == 1]]
```

Les méthodes matricielles fonctionnent dans tous les cas, cf [cette page (https://ask.sagemath.org/question/33574/solve-linear-system-in-gf7/)](https://ask.sagemath.org/question/33574/solve-linear-system-in-gf7/).

In [17]:
```
var('x y z')
A=matrix(GF(2),3,3,[0,1,1, 1,0,1, 1,1,1]);show('A=',A,LatexExpr(r"\in"),A.
parent())
M=Matrix(GF(2),[vector(A^0),vector(A^1),vector(A^2)]).transpose()
show('(x,y,z)=',M.solve_right(vector(A^3)))
show('# M*(x,y,z)=vector(A^3)')
```

Out[17]:
$$\mathtt{A=}\begin{pmatrix}0 & 1 & 1\\ 1 & 0 & 1\\ 1 & 1 & 1\end{pmatrix} \in \mathrm{Mat}_{3\times 3}(\mathbf{F}_2)$$

Out[17]: $\mathtt{(x,y,z)=}(1,\ 1,\ 1)$

Out[17]: `# M*(x,y,z)=vector(A^3)`

La notion de polynôme minimal est implémenté dans Sagemath

```
A.minpoly()
x^3 + x^2 + x + 1
```

1. Algorithme de division euclidienne dans l'anneau de polynôme $k[X]$

k anneau (commutatif ?), $A, B \in k[X]$. Algorithme :

initiation $(Q, R) := (0, A)$

tant que $\mathrm{d}^\circ R \geq \mathrm{d}^\circ B$: $(Q, R) \to (Q + \frac{cd(R)}{cd(B)} X^{\mathrm{d}^\circ R - \mathrm{d}^\circ B}, R - B\frac{cd(R)}{cd(B)} X^{\mathrm{d}^\circ R - \mathrm{d}^\circ B})$

La réécriture diminue $\mathrm{d}^\circ R$ et conserve $BQ + R$ qui vaut initialement A.

Applications :

- Tout idéal de $k[X]$ admet un générateur (est de la forme $mk[X]$ pour un m dans l'idéal).
- Le polynôme minimal d'un élément x d'une $\mathbb{F}_p$-algèbre finie est le générateur unitaire de l'idéal $\{Q \in \mathbb{F}_p[X],\ Q(x) = 0\}$.
- Algorithme d'Euclide de calcul d'un pgcd (générateur, noté $A \wedge B$, de l'idéal engendré par deux polynômes A, B) et d'une relation de Bezout.

Ex. $X^k - 1 \wedge X^l - 1 = X^{k \wedge l} - 1$ avec relation de Bezout dans $\mathbb{Z}[X]$.

Conséquences : pour chaque entier n, $(n^k - 1) \wedge (n^l - 1) = n^{k \wedge l} - 1$ dans $\mathbb{Z}$ et $(X^{n^k - 1} - 1) \wedge (X^{n^l - 1} - 1) = X^{n^{k \wedge l} - 1} - 1$ dans tout anneau de polynôme.

2. Anneau quotient $\mathbb{F}_p[X]/(Q)$

$Q \in \mathbb{F}_p[X]$ de degré $n \geq 0$ (*i.e.* $Q \neq 0$).

$K = \mathbb{F}_p[X]/(Q)$ est une $\mathbb{F}_p$-algèbre (commutative) de dimension $\mathrm{d}^\circ Q$ comme $\mathbb{F}_p$ - espace vectoriel, de base canonique $(1, x, \ldots, x^{\mathrm{d}^\circ Q - 1})$, où x désigne la classe de X modulo Q. Le polynôme minimal sur $\mathbb{F}_p$ de $x = X \bmod Q$ est Q.

On peut ainsi représenter les éléments de $\mathbb{F}_p[X]/(Q)$ par des n-uplets d'éléments de $\mathbb{F}_p$, addition et multiplication par un scalaire coordonnée par coordonnée, produit via le reste de la division euclidienne par Q du produit dans $\mathbb{F}_p[X]$.

In [9]:
```
K.<X>=PolynomialRing(GF(3),'X')
print 'K:',K
P=X^3+X+1
print '[P] =',P.list()
print 'P_[1, 1, 0, 1] =',K([1, 1, 0, 1])
# P.list() est une donnée de P qu'on ne peut extraire de la fonction polyn
omiale P(x) si l'anneau de coefficient est un corps fini.
#K([1, 1, 0, 1]) peut être facilement codée :
l=[1, 1, 0, 1];P=sum(l[i]*X^i for i in range(len(l)));print P,P.parent()
```

```
K: Univariate Polynomial Ring in X over Finite Field of size 3
[P] = [1, 1, 0, 1]
P_[1, 1, 0, 1] = X^3 + X + 1
X^3 + X + 1 Univariate Polynomial Ring in X over Finite Field of size 3
```

La notion d'anneau quotient $\mathbb{F}_p[X]/(Q)$ est déjà implémentée dans Sagemath :

In [38]:
```
A.<X>=PolynomialRing(GF(3),'X')
Q=X^3+X+1
K=A.quotient(Q,'x');x=K.gen()
print 'Q(x) =',Q(x)
print 'Q(X) =',Q(X)
```

```
Q(x) = 0
Q(X) = X^3 + X + 1
```

x désignant toujours la classe de X modulo Q, soit $A \in \mathbb{F}_p[X]$, alors $A(x) = 0$ si et seulement si Q divise A dans $\mathbb{F}_p[X]$.

Prop. $\mathbb{F}_p[X]/(Q)$ est un corps si et seulement si Q est irréductible ($\neq 0$)

Supposons Q irréductible de degré n ; alors $x^{p^n} - x = 0$ donc Q divise $X^{p^n} - X$ dans $\mathbb{F}_p[X]$. Inversement si Q est un facteur irréductible de $X^{p^m} - X$ pour un certain entier m alors :

- Tous les éléments de $\mathbb{F}_p[X]/(Q)$ sont racines de $X^{p^m} - X$ donc $m \geq n$
- Q divise $(X^{p^m} - X) \wedge (X^{p^n} - X) = X^{p^{m \wedge n}} - X$ donc $m \wedge n \geq n$ donc n divise m.

Comme $X^{p^m} - X$ est premier avec son polynôme dérivé dans $\mathbb{F}_p[X]$ on obtient :

Prop. $X^{p^m} - X = \prod_{Q \text{ irréductible unitaire, } \mathrm{d}^\circ Q | m} Q$

Notons $\psi(d)$ le nombre de polynômes irréductibles de degré $d \geq 1$. En observant les degrés dans la formule ci-dessus on obtient

$$p^m = \sum_{d|n} d\psi(d) \ .$$

Affirmation : $\psi(n) > 0$ pour chaque entier $n \geq 1$. Comment le prouver ?

Soit K une $\mathbb{F}_p$-algèbre et $\varphi : \mathbb{F}_p[X]/(Q) \to K$ un homomorphisme d'anneaux ; alors φ est déterminé par l'image de $x = X \bmod Q$ et $Q(\varphi(x)) = 0$. Réciproquement soit y une racine de Q dans K ; alors l'application $\mathbb{F}_p[X] \to K$, $P \mapsto P(y)$ induit un homomorphisme d'anneaux $\mathbb{F}_p[X]/(Q) \to K$.

Lemme chinois : l'application $\mathbb{F}_p[X]/(Q_1 Q_2) \to \mathbb{F}_p[X]/(Q_1) \times \mathbb{F}_p[X]/(Q_2)$,
$P \mapsto (P \bmod Q_1, P \bmod Q_2)$ est un isomorphisme de $\mathbb{F}_p$-algèbres si $Q_1 \wedge Q_2 = 1$.

TP Racines de $X^p - X$ et algorithme de Berlekamp

3. Corps intermédiaire, générateurs, polynôme minimal

In [0]:
```
```