**Université de Rennes 1 - 2011-2012 - Master 1 de mathématiques - Module ALGB - Corrigé du contrôle du 2/12/2011 - Durée : 1 heure**

**Les anneaux et morphismes d'anneaux sont supposés unitaires.**

**Exercice 1 -** (question de cours, 4 points) Donner les définitions : (a) d'un corps algébriquement clos ; (b) d'une clôture algébrique.

*Remarques :* on rappelle que toutes les notations utilisées doivent être définies. Si plusieurs définitions équivalentes sont possibles, on n'en demande qu'une.

(a) Réponse la plus fréquente : un corps $K$ est algébriquement clos si tout polynôme $P \in K[X]$ non constant a une racine dans $K$.

**Commentaire :** si l'on omet « non constant » (comme dans un grand nombre de réponses), il n'y a *pas* de corps algébriquement clos.

(b) Une clôture algébrique d'un corps $K$ est une extension algébrique de $K$ qui est un corps algébriquement clos.

**Commentaire :** « algébrique » a été le plus souvent oublié.

**Exercice 2 -** (5 points) On rappelle qu'un élément $u$ d'un anneau $A$ est *nilpotent* s'il existe un entier $r \geq 0$ tel que $u^r = 0$.
Soient $k$ un corps et $n \in \mathbb{N}$ (on pourra supposer $n > 0$). Définir une bijection entre :
(a) l'ensemble des classes de similitude de matrices nilpotentes de $\mathrm{M}_n(k)$ ;
(b) l'ensemble des suites *croissantes* $(r_1, \ldots, r_m)$ d'entiers strictement positifs vérifiant la condition $\sum_{i=1}^m r_i = n$.
(Indication : quels sont les invariants de similitude possibles pour une matrice nilpotente ?)

Si $n = 0$, il n'y a qu'une classe de similitude (la classe de la matrice vide, unique élément de $\mathrm{M}_0(k)$, qui est bien nilpotente) et une seule suite (b) (la suite vide, avec $m = 0$). Supposons $n > 0$ dans la suite.

Si $M \in \mathrm{M}_n(k)$ est nilpotente, elle est annulée par un polynôme de la forme $X^r$ ; son polynôme minimal est donc de la forme $X^j$, où $1 \leq j \leq r$ (on utilise le fait que $n > 0$ ici !). Ses invariants de similitude (qui divisent le polynôme minimal) sont donc de la même forme. La suite des invariants de similitude de $M$ est donc de la forme $(X^{r_1}, \ldots, X^{r_m})$ ; la condition de divisibilité impose que la suite $(r_1, \ldots, r_m)$ soit croissante, et la somme des degrés $r_i$ doit être égale à $n$. On associe donc à $M$ une suite d'entiers comme dans l'énoncé, qui caractérise $u$ à similitude près. Inversement, à une telle suite on peut associer le $k[X]$-module $E := \bigoplus_{i=1}^m k[X]/(X^{r_i})$ ; la matrice, dans n'importe quelle $k$-base de $E$, de la multiplication par $X$ est (par construction) une matrice dans $\mathrm{M}_n(k)$ ayant les invariants de similitude $(X^{r_1}, \ldots, X^{r_m})$, et en particulier nilpotente (son polynôme minimal est $X^{r_m}$).

**Exercice 3 -** (4 points) Soit $p$ un nombre premier. On note $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ le corps fini à $p$ éléments et on considère l'anneau $A = \dfrac{\mathbb{F}_p[x]}{(P)}$, où $P \in \mathbb{F}_p[x]$ est un polynôme non nul, de degré $n$, en l'indéterminée $x$.
On représente les éléments de $A$ (de façon unique) comme classes de polynômes de degré $< n$ à coefficients dans $\{0, 1, \ldots, p-1\}$.
A l'aide de maple, écrire (en utilisant, *par exemple*, les fonctions de division euclidienne et de réduction modulo $p$) trois procédures permettant respectivement d'additionner, de multiplier et d'inverser dans $A$. Les données d'entrée sont $p, P$ et les éléments à traiter.

```
# additionner dans A
    addA := proc(a,b,p,P)
    return (a+b) mod p;
    end:

# multiplier dans A
    mulA := proc(a,b,p,P)
    return rem(a*b,P,x) mod p;
    end:

# inverser dans A
    invA := proc(a,p,P)
    local d,u,v;
    d:=Gcdex(a,P,x,'u','v') mod p;
    if d=1 then
      return u
    else
      #print(‘pas inversible‘);
      return 0
    end if;
    end:
```

**Exercice 4 -** ($-2$ à $+6$ points) Soient $K \subset L \subset M$ trois corps, et soit $P \in K[X]$ un polynôme non nul. Pour chaque assertion ci-dessous, on répondra, *sans justifier la réponse*, V si elle est (toujours) vraie, F si elle est (parfois) fausse, et A en cas d'abstention.

**Barème :** 1 par réponse correcte, $-1$ par réponse incorrecte, 0 en cas d'abstention.

**Ne répondez qu'à coup sûr ! !**

1. Si $M$ est algébrique sur $K$, $L$ est algébrique sur $K$.

Vrai.

2. Si $M$ est transcendant sur $K$, $M$ est transcendant sur $L$.

Faux (exemple : $L = M$).

3. Si $M$ est transcendant sur $L$, $M$ est transcendant sur $K$.

Vrai.

4. Si $P$ est irréductible dans $L[X]$, il est irréductible dans $K[X]$.

Vrai.

5. Si $P$ est séparable sur $K$, il est séparable sur $L$.

Vrai.

6. Si $P$ est séparable sur $L$, il est séparable sur $K$.

Vrai.