Université Paris 7-Denis Diderot
M1 mathématiques

Algèbre
Année 2007-08
L. Merel - R. Mneinmé

**Corrigé de l'EXAMEN PARTIEL du 13 novembre 2007**

## Exercice I

**1.** On a $(x-1)(x^{n-1}+\cdots+x+1)=x^n-1$. Comme $A$ est intègre et que $x-1\neq 0$, on a $x^{n-1}+\cdots+x+1=0$, d'où la première égalité. On a donc $n=(1-x)+(1-x^2)+\cdots+(1-x^n)$. Comme $x-1$ divise chaque terme du second membre, il divise $n$.

**2.** Comme $x$ est d'ordre $n$, on a $(x^d)^{n/d}=1$ et $x^d\neq 1$. En appliquant la question 1., on trouve que $x^d-1$ divise $n/d$ dans $A$. Il divise donc $n/d$ dans $\mathbf{F}$. Comme $\mathbf{F}$ est de caractéristique $p$ et que $p$ ne divise pas $n/d$, $n/d$ est inversible dans $\mathbf{F}$. Donc $x^d-1$ est inversible dans $\mathbf{F}$.

**3.** Soit $x\in A$ un élément d'ordre $n$. L'image $\bar{x}$ de $x$ dans $\mathbf{F}$ vérifie $\bar{x}^n=1$. D'après la question 2., on a $\bar{x}^d-1\neq 0$ lorsque $d$ est diviseur de $n$, $d\neq n$.

**4.** On a $\Phi_9=(X^9-1)/(X^3-1)$. Les racines de $\Phi_9$ sont donc les racines 9-èmes de l'unité qui ne sont pas des racines cubiques. Ce sont bien les racines primitives 9-èmes de l'unité.

**5.** On a $\Phi_9(X+1)\equiv X^6+2^3X^3+1+X^3+1+1\equiv X^6 \pmod 3$ et $\Phi_9(X+1)$ a pour coefficient constant 3. On peut applique le critère d'irréductibilité d'Eisenstein pour établir que $\Phi_9(X+1)$, et donc aussi $\Phi_9(X)$, sont des polynômes irréductibles sur $\mathbf{Q}$. Comme le contenu de $\Phi_9$ est 1, c'est un polynôme irréductible sur $\mathbf{Z}$.

**6.** L'homomorphisme d'anneaux $\mathbf{Z}[X]\to\mathbf{Z}[\zeta]$ qui à $P$ associe $P(\zeta)$ est surjectif et a pour noyau $(\Phi_9)$, car tout polynôme de $\mathbf{Z}[X]$ qui annule $\zeta$ est un multiple rationnel de $\Phi_9$ et donc un multiple entier de $\Phi_9$, puisque $\Phi_9$ est de contenu 1.

**7.** L'élément $\zeta$ est dans $\mathbf{Z}[\zeta]^*$, car $\zeta^{-1}=\zeta^8\in\mathbf{Z}[\zeta]$. Il est d'ordre 9. Donc $-\zeta\in\mathbf{Z}[\zeta]^*$ est d'ordre 18.

**8.** Supposons que l'image $\phi_9$ de $\Phi_9$ dans $\mathbf{F}_2[X]$ est réductible. Elle a alors un facteur irréductible $P$ de degré 1, 2 ou 3. Le polynôme $P$ a alors une racine dans le corps $k=\mathbf{F}_2[X]/(P)$, qui possède 2, 4 ou 8 éléments. Donc $\phi_9$ a aussi une racine dans ce corps. Mais $k^*$ est un groupe d'ordre 1, 3 ou 7, il ne peut posséder de racine primitive 9-ème de l'unité.

**9.** Le groupe $\mathbf{F}_{19}^*$ des éléments inversibles de $\mathbf{F}_{19}$ est cyclique d'ordre 18. Il possède donc un sous-groupe cyclique d'ordre 9, et donc 6 éléments d'ordre 9. Ce sont précisément les racines de la réduction modulo 19 du polynôme $\Phi_9$. Soit $P$ un facteur irréductible de cette réduction. L'anneau $\mathbf{Z}_{19}[X]/(19,\Phi_9)$ a pour quotient le corps $\mathbf{F}_{19}[X]/(P)\simeq\mathbf{F}_{19}$.

**10.** On a montré en répondant à la question 4. que $\mathbf{Z}[\zeta]^*$ possède au moins 18 éléments d'ordre fini.

Soit $x$ un élément de $\mathbf{Z}[\zeta]^*$ d'ordre $n$. Posons $n=n'n_2n_{19}$, où $n'$ entier $>0$ premier à 2 et 19, $n_2$ est une puissance entière de 2 et $n_{19}$ est une puissance entière de 19. Les éléments $x^{n_2}$ et $x^{n_{19}}$ sont d'ordres $n'n_{19}$ (premier à 2) et $n'n_2$ (premier à 19) respectivement. D'après la question 3, l'image de $x^{n_2}$ dans $\mathbf{F}_2[X]/(\Phi_9)$ est d'ordre $n'n_{19}$. Donc $n'n_{19}$ divise 63. Donc $n_{19}=1$. De même, $n'n_2$ divise 18. Donc $n_2$ divise 2 et $n'$ divise 9. Donc $n'$ divise 18.

Tout élément d'ordre fini de $\mathbf{Z}[\zeta]^*$ est d'ordre divisant 18. Or dans $\mathbf{C}$, qui est un corps, le polynôme $X^{18}-1$ a au plus 18 racines. Donc il y a au plus 18 éléments d'ordre divisant 18 dans $\mathbf{Z}[\zeta]^*$.

## Exercice II

**1.** Voir le cours pour le fait que la donnée de $A$ fait de $K^n$ un $K[X]$-module. L'application qui à $Q$ associe $Q(A)(e_1)$ est $K[X]$-linéaire. Son noyau est donc un sous-$K[X]$-module de $K[X]$, c'est-à-dire un idéal de $K[X]$.

**2.** Voir le cours pour cette matrice de Sylvester. C'est une matrice carrée d'ordre $n+1$ donnée ainsi

$$\begin{pmatrix} -T & 0 & 0 & \cdots & 0 & 0 & a_0 \\ 1 & -T & 0 & \cdots & 0 & 0 & a_1 \\ 0 & 1 & -T & \cdots & 0 & 0 & a_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & -T & 0 & a_{n-2} \\ 0 & 0 & 0 & \cdots & 1 & -T & a_{n-1} \\ 0 & 0 & 0 & \cdots & 0 & 1 & 1 \end{pmatrix}$$

Son déterminant est le résultant de $T-X$ et $P(X)$. On remarque que (a) en changeant le signe de la dernière colonne, (b) en ajoutant l'avant-dernière colonne à la dernière et (c) en développant par rapport à la dernière ligne (qui ne comprend qu'un seul coefficient non nul) on montre que le résultant de $T-X$ et $P$ est le déterminant de $-C_P(T)$, c'est-à-dire le polynôme caractéristique de $C_P$.
**3.** On a $c_P e_1 = e_2$, $c_P^2 e_1 = c_P e_2 = e_3, \cdots, c_P^{n-1} e_1 = c_P e_{n-1} = e_n$. Comme le $K[X]$-module engendré par $e_1$ contient, $e_1$, $X \cdot e_1 = e_2, \ldots, X^{n-1} \cdot e_1 = e_n$, il contient $K^n$.
**4.** Soit $Q = b_0 + \cdots + b_{n-1}X^{n-1} \in \mathcal{I}_1(c_P)$ de degré $< n$. On a $0 = Q(c_P)e_1 = b_0 e_1 + b_1 e_2 + \cdots + b_{n-1}e_n$. Comme $(e_1, \cdots, e_n)$ est une base du $K$-espace vectoriel $K^n$, on a $b_0 = b_1 = \cdots = b_{n-1} = 0$ et donc $P = 0$.
**5.** On a $P(c_P)e_1 = a_0 e_1 + a_1 e_2 + \cdots + a_{n-1}e_n - a_0 e_1 - a_{n-1}e_n = 0$.
**6.** Le polynôme minimal de $c_P$ est par définition le générateur unitaire de l'idéal de $K[X]$ formé par les polynômes $Q$ vérifiant $Q(c_P) = 0$. Il est de degré $\geq n$ d'après la question 4. Comme $K^n$ est engendré par $e_1$ comme $K[X]$-module, la question 5. entraîne que $P(c_P) = 0$. Donc $P$ est un multiple du polynôme minimal de $c_P$. C'est pourquoi $P$ est le polynôme minimal de $c_P$.
**7.** L'homomorphisme d'anneaux $K[X] \to \mathrm{M}_n(K)$ qui à $P$ associe $P(c_P)$ a pour image $K[c_P]$ et pour noyau $(P)$, puisque $P$ est le polynôme minimal de $c_P$. Comme $P$ est irréductible, l'anneau quotient $K[X]/(P)$ est un corps. Donc $K[c_P]$ est un corps.
**8.** Le polynôme $X^n - 2$ est irréductible d'après le critère d'Eisenstein.
**9.** Considérons le polynôme $P = X^n - 2 \in \mathbf{Q}[X]$. D'après les question 7. et 8., l'anneau $\mathbf{Q}[c_P]$ est un corps contenu dans $\mathrm{M}_n(\mathbf{Q})$ isomorphe à $\mathbf{Q}[X]/(X^n - 2)$. C'est donc un sous-espace vectoriel de dimension $n$ de $\mathrm{M}_n(\mathbf{Q})$. Donc $F \cap \mathbf{Q}[c_P]$ est un espace vectoriel de dimension $\geq 1$. Il contient un élément non nul, qui est inversible, puisque $\mathbf{Q}[c_P]$ est un corps.
**10.** C'est le cas de l'espace formé par les matrices dont la première colonne est nulle.