Université de Paris–Diderot
L3 de Mathématiques
Année 2014-2015

Algèbre II
Mathilde Herblot, Yongqi Liang,
Régis de la Bretèche

Partiel du 11 mars 2015 **Durée : 3 heures**

L'usage des calculatrices, téléphones et de tout document est strictement interdit. Une attention particulière sera apportée à la justification des arguments et à la qualité de la rédaction. Les trois exercices sont indépendants. On pourra traiter les questions en utilisant les résultats énoncés dans les questions qui les précèdent. Ne pas oublier de tourner la page pour faire le troisième exercice

Exercice I

Dans toute la suite de l'exercice nous considérons E un K-espace vectoriel de dimension n avec K un corps et $n \geqslant 1$.

Si F est un sous-espace stable d'un espace vectoriel E par un endomorphisme f, alors l'endomorphisme induit f_F $F \to F$ est défini par $f_F(x) = f(x)$ pour tout $x \in F$.

1- Montrer que le polynôme minimal de l'induit f_F divise le polynôme minimal de f.

2- Soit $f \in \mathcal{L}(E)$. Supposons que $E = F \oplus G$ où F et G sont des sous-espaces stables par f. Montrer alors que le polynôme minimal de f est le PPCM des polynômes minimaux de f_F et f_G.

3- Soient $f \in \mathcal{L}(E)$ et $P \in K[X]$. Redémontrer que $\mathrm{Ker}(P(f))$ et $\mathrm{Im}(P(f))$ sont stables par f.

4- Montrer que $\mathrm{Ker}(f) = \mathrm{Ker}(f^2)$ est équivalent à $\mathrm{Ker}(f) \cap \mathrm{Im}(f) = \{0_E\}$.

5- En utilisant le théorème du rang dont on rappelera l'énoncé, montrer que $\mathrm{Ker}(f)$ et $\mathrm{Im}(f)$ sont des supplémentaires dans E si et seulement si $\mathrm{Ker}(f) \cap \mathrm{Im}(f) = \{0_E\}$.

6- Nous supposons que f_F n'est pas bijective. Quel est le polynôme minimal de f_F lorsque $F = \mathrm{Ker}(f)$ et $F = \mathrm{Ker}(f^2)$? On donnera à chaque fois tous les cas possibles en exhibant un exemple dans les cas possibles.

Exercice II

1- Le nombre 2 est-il un carré dans $\mathbb{F}_5$?

2- Montrer que $P(X) = X^2 + X + 1$ est irréductible dans $\mathbb{F}_5[X]$.

3- Quelle est la caractéristique de $\mathbb{F}_{25}$?

4- Montrer que le quotient $\mathbb{F}_5[X]/(P)$ est isomorphe à $\mathbb{F}_{25}$ et que P a deux racines dans $\mathbb{F}_{25}$.

5- On note α une racine de P dans $\mathbb{F}_{25}$. Montrer que tout $\beta \in \mathbb{F}_{25}$ peut s'écrire de manière unique sous la forme $\beta = x\alpha + y$ avec x et y dans $\mathbb{F}_5$.

6- Soit $Q(X) = X^5 - X + 1$. Déterminer c et d dans $\mathbb{F}_5$ tels que $Q(\alpha) = c\alpha + d$.

7- En utilisant le résultat de la question 4, montrer que pour tout $\beta \in \mathbb{F}_{25}$, on a $Q(\beta) \neq 0$.

8- En déduire que Q est irréductible dans $\mathbb{F}_5[X]$. Le polynôme Q est-il irréductible dans $\mathbb{Q}[X]$?

Exercice III

Soit K un corps et P un polynôme à coefficients dans K irréductible sur K et de degré $n \geqslant 2$.

1- Montrer qu'il existe une extension finie L de K qui contienne une racine de P. On appelera dans la suite α une de ces racines.

2- Déterminer $[K(\alpha) : K]$.

3- Montrer que n divise $[L : K]$.

4- On choisit $k = \mathbb{Q}$, j une racine cubique de l'unité distincte de 1 et c une racine dans $\mathbb{C}$ du polynôme $X^5 - 2$.

4a- Montrer que le polynôme $X^5 - 2$ est irréductible sur $\mathbb{Q}$.

4b- Déterminer le degré $[\mathbb{Q}(j, c) : \mathbb{Q}]$.

4c- Montrer que $\mathbb{Q}(j, c) = \mathbb{Q}(j + c)$.

Corrigé du partiel du 11 mars 2015

Exercice I

1- On a $\mu_f(f)(x) = 0$ pour tout $x \in E$ et en particulier $x \in F$. Donc $\mu(f_F)(x) = \mu_f(f)(x) = 0$ pour $x \in F$. Ainsi μ_f est un polynôme annulateur de f_F donc divisible par le polynôme minimal de f_F.

2- Soit P le PPCM des polynômes minimaux de f_F et f_G noté respectivement P_1 et P_2. Pour tout $x \in F$, il existe $y \in F$ et $z \in G$ tels que $x = y + z$. On a $P(f)(x) = P(f)(y) + P(f)(z) = P(f_F)(y) + P(f_G)(z)$. Or $P_1 \mid P$ donc $P(f_F)(y) = 0$ et $P_2 \mid P$ donc $P(f_G)(z) = 0$. Ainsi $P(f) = 0$ et donc $\mu_f \mid P$.

D'autre part comme μ_f est un polynôme annulateur de f_F et f_G alors $P_1 \mid \mu_f$ et $P_2 \mid \mu_f$ donc P le PPCM de P_1 et P_2 divise μ_f. Ainsi $\mu_f = P$.

3- Redémontrons ce résultat. Si $x \in \mathrm{Ker}P(f)$, $P(f)(x) = 0_E$. Or

$$P(f)(f(x)) = f(P(f)(x)) = f(0) = 0$$

donc $f(x) \in \mathrm{Ker}(f)$. Si $y \in \mathrm{Im}(P(f))$, il existe $x \in E$ tel que $y = P(f)(x)$. Alors $f(y) = f\big(P(f)(x)\big) = P(f)(f(x))$ est donc un élément de $\mathrm{Im}(f)$.

Ainsi $\mathrm{Ker}P(f)$ et $\mathrm{Im}P(f)$ sont stables par f.

4- Supposons $\mathrm{Ker}(f) = \mathrm{Ker}(f^2)$ et prenons $x \in \mathrm{Ker}(f) \cap \mathrm{Im}(f)$. La relation $x \in \mathrm{Im}(f)$ impliqu'il existe $y \in E$ tel que $x = f(y)$. La relation $x \in \mathrm{Ker}(f)$ impliqu'il existe $y \in E$ tel que $f(x) = 0_E = f^2(y)$. Donc $y \in \mathrm{Ker}(f^2) = \mathrm{Ker}(f)$ Donc $f(y) = 0_E = x$. On a bien $\mathrm{Ker}(f) \cap \mathrm{Im}(f) = \{0_E\}$.

Supposons réciproquement que $\mathrm{Ker}(f) \cap \mathrm{Im}(f) = \{0_E\}$. L'implication $\mathrm{Ker}(f) \subset \mathrm{Ker}(f^2)$ est trivial. Montrons la relation $\mathrm{Ker}(f^2) \subset \mathrm{Ker}(f)$. Soit $x \in \mathrm{Ker}(f^2)$. Or $f^2(x) = 0$ donc $f(x) \in \mathrm{Ker}(f) \cap \mathrm{Im}(f) = \{0_E\}$. On a bien $x \in \mathrm{Ker}(f)$.

Nous avons donc montré l'égalité.

5- Le théorème du rang affirme lorsque $f \in \mathcal{L}(E)$ et $n = \dim(E)$ alors

$$\dim\big(\mathrm{Ker}(f)\big) + \dim\big(\mathrm{Im}(f)\big) = n.$$

L'implication $\mathrm{Ker}(f)$ et $\mathrm{Im}(f)$ sont des supplémentaires dans E entraîne $\mathrm{Ker}(f) \cap \mathrm{Im}(f) = \{0_E\}$ est évidente. Supposons $\mathrm{Ker}(f) \cap \mathrm{Im}(f) = \{0_E\}$, alors $\mathrm{Ker}(f)$ et $\mathrm{Im}(f)$ sont en somme directe et

$$\dim\big(\mathrm{Ker}(f) \oplus \mathrm{Im}(f)\big) = \dim\big(\mathrm{Ker}(f)\big) + \dim\big(\mathrm{Im}(f)\big) = n.$$

Par comparaison des dimensions, nous obtenons

$$\mathrm{Ker}(f) \oplus \mathrm{Im}(f) = E.$$

6- f_F n'est pas bijective donc $\mathrm{Ker}(f) \neq \{0\}$ et $\mathrm{Ker}(f^2) \neq \{0\}$. Lorsque $F = \mathrm{Ker}(f)$, X est un polynôme annulateur de f_F donc le polynôme minimal de f_F est X. Lorsque $F = \mathrm{Ker}(f^2)$, X^2 est un polynôme annulateur de f_F donc le polynôme minimal de f_F est soit X, soit X^2.

Si c'est X, cela veut dire que $f_F = 0_{\mathcal{L}(F)}$ et donc $\mathrm{Ker}(f) = \mathrm{Ker}(f^2)$. Un exemple correspond à l'endomorphisme associé à la matrice de $\mathcal{M}_2(K)$ définie par

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Sinon c'est X^2. Un exemple correspond à l'endomorphisme associé à la matrice de $\mathcal{M}_2(K)$ définie par

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \qquad A^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Exercice II

1- les carrés de $\mathbb{F}_5$ sont 0, 1 ou 4. Donc 2 n'est pas un carré.

2- $P(0) = 1$, $P(1) = 3$, $P(2) = 2$, $P(3) = 3$, $P(4) = 1$ donc P n'a pas de racine dans $\mathbb{F}_5$ et il est de degré 2, donc il est irréductible dans $\mathbb{F}_5[X]$.

3- La caractéristique de $\mathbb{F}_{25}$ est 5.

4- $\mathbb{F}_5[X]$ est principal donc P irréductible entraine (P) maximal et ainsi $\mathbb{F}_5[X]/(P)$ est un corps. Il est de cardinal $5^{\deg P} = 25$. Il est donc isomorphe à $\mathbb{F}_{25}$. Le polynôme P a une racine dans ce corps donc dans $\mathbb{F}_{25}$. Si on la note α , sa deuxième racine est $-1-\alpha \neq \alpha$ (relation entre somme des racines et coefficients).

5- Un élément β de $\mathbb{F}_{25}$ s'écrit sous la forme $A(\alpha)$ avec $A \in \mathbb{F}_5[X]$. On fait la division euclidienne de A par P. Il existe un polynôme $R \in \mathbb{F}_5[X]$ de degré $\leqslant 1$ et $B \in \mathbb{F}_5[X]$ tels que $A = BP + R$. Il vient $\beta = R(\alpha)$ ce qui fournit le résultat demandé en prenant $R(X) = xX + y$.

6- On a $Q(\alpha) = \alpha^5 - \alpha + 1 = \alpha(-\alpha - 1)^2 - \alpha + 1 = \alpha^2 - \alpha + 1 = -2\alpha$, où on a utilisé à plusieurs reprises $P(\alpha) = 0$ [autre méthode faire la division euclidienne de Q par P i.e. $Q = (X^3 - X^2 + 1)P - 2X$].

7- On écrit $\beta = x\alpha + y$. Comme la caractéristique est 5 et que x et y sont dans $\mathbb{F}_5$, on a

$$Q(x\alpha + y) = x\alpha^5 + y - (x\alpha + y) + 1 = x(P(\alpha) - 1) + 1 = -2x\alpha - x + 1.$$

Si on avait $Q(\beta) = 0$, alors $2x = 0$ et $1 - x = 0$ ce qui serait impossible.

8- On vérifie que le polynôme Q n'a pas de racine dans les extensions de $\mathbb{F}_5$ de degré $\leqslant \deg(Q)/2 = 5/2$. La seule extension de $\mathbb{F}_5$ de degré 1 est $\mathbb{F}_5$ de degré 2 est $\mathbb{F}_{25}$. Le polynôme P est donc irréductible dans $\mathbb{F}_5[X]$. Il est donc irréductible dans $\mathbb{Z}[X]$. Comme il est unitaire et qu'il est irréductible dans $\mathbb{Z}[X]$, la classification des irréductibles dans $\mathbb{Z}[X]$ permet d'affirmer qu'il est irréductible dans $\mathbb{Q}[X]$.

Exercice III

Soit K un corps et P un polynôme à coefficients dans K irréductible sur K et de degré $n \geqslant 2$.

1- On choisit L le corps de rupture de P sur K. D'après le cours, il contient bien une racine de P et $[L : K] = \deg(P)$.

2- $K(\alpha)$ est isomorphe à $K[X]/(P)$ donc $[K(\alpha) : K] = \deg(P) = n$.

3- Le théorème de la base téléscopique fournit

$$[L : K] = [L : K(\alpha)] \times [K(\alpha) : K] = [L : K(\alpha)]n,$$

ce qui fournit bien le résultat.

4- On choisit $k = \mathbb{Q}$, j une racine cubique de l'unité distincte de 1 et c une racine dans $\mathbb{C}$ du polynôme $X^5 - 2$.

4a- Pour montrer que le polynôme $X^5 - 2$ est irréductible sur $\mathbb{Q}$, on applique le critère d'Eisenstein en prenant $p = 2$ ce qui fournit le résultat.

4b- D'après 4a, on a $[\mathbb{Q}(c) : \mathbb{Q}] = 5$. L'élément j annule $X^2 + X + 1$ qui est irréductible sur $\mathbb{Q}$ (pas de racines dans $\mathbb{Q}$ et de degré 2). Donc $[\mathbb{Q}(j) : \mathbb{Q}] = 2$. Ainsi 2 et 5 sont des diviseurs $[\mathbb{Q}(j, c) : \mathbb{Q}]$. Donc 10 divise $[\mathbb{Q}(j, c) : \mathbb{Q}]$. Or la famille $\{j^n c^m\}_{0 \leqslant n \leqslant 1, 0 \leqslant m \leqslant 4}$ est une famille génératrice du $\mathbb{Q}$ espace vectoriel $\mathbb{Q}(j, c)$ donc $[\mathbb{Q}(j, c) : \mathbb{Q}] \leqslant 10$ puis $[\mathbb{Q}(j, c) : \mathbb{Q}] = 10$.

4c- On a $\mathbb{Q}(b) \subset \mathbb{Q}(j, c)$ avec $b = j + c$. Montrons que $j \in \mathbb{Q}(b)$. On a

$$\begin{aligned}(b - j)^5 - 2 &= b^5 - 5jb^4 + 10j^2b^3 - 10j^3b^2 + 5j^4b - j^5 \\ &= j(5b - 5b^4 - 10b^3 + 1) + (b^5 - 10b^3 - 10b^2 + 1) = c^5 - 2 = 0,\end{aligned}$$

où nous avons ici utilisé les relations $j^3 = 1$ et $j^2 = -j - 1$. On a donc $j = -(b^5 - 10b^3 - 10b^2 + 1)/(5b - 5b^4 - 10b^3 + 1) \in \mathbb{Q}(b)$ et donc $\mathbb{Q}(j, c) \subset \mathbb{Q}(b)$. Nous avons ici vérifié que $b^5 - 10b^3 - 10b^2 + 1 \neq 0$ et $5b - 5b^4 - 10b^3 + 1 \neq 0$. En effet sinon b annule un polynôme de degré < 5 alors $[\mathbb{Q}[b, j] : \mathbb{Q}] < 5 \times 2 = 10$ ce qui est absurde.