Université de Rennes 1 - 2010-2011 - Master 1 de mathématiques - Module ALGB - Corrigé de l'examen du 14/12/2010 - Durée : 2 heures

Documents, calculatrices et téléphones interdits. Barème indicatif.
Les anneaux sont supposés commutatifs (et unitaires).
Les réponses doivent être justifiées, sauf mention contraire.

Exercice 1 - (question de cours, 3 points) Soient K un corps, $n \geq 1$ un entier, a un élément non nul de K. À quelle(s) condition(s) sur n, K et a le polynôme $P = X^n - a \in K[X]$ est-il séparable ? Justifier la réponse.

Montrons que P est séparable si et seulement si n n'est pas divisible par $\mathrm{car}\,(K)$ (c'est-à-dire si $n1_K \neq 0$).

Si $\mathrm{car}\,(K)$ divise n, alors la dérivée $P' = nX^{n-1}$ de P est identiquement nulle. Donc P et P' ne sont pas premiers entre eux (puisque P n'est pas constant) et P n'est pas séparable (en fait, toutes les racines de P sont multiples).

Sinon, P' n'a pas de racine non nulle, et $P(0) = -a \neq 0$, donc P et P' n'ont pas de racine commune (dans une extension quelconque de K). Ils sont donc premiers entre eux et P est séparable.

Commentaires. Beaucoup de confusion et très peu de bonnes réponses, pour un résultat qui figurait dans le cours (avec démonstration laissée en exercice : ce n'était pas une figure de style !). Erreurs fréquentes :

– se contenter des cas « $\mathrm{car}\,(K) = n$ » et « $\mathrm{car}\,(K)$ ne divise pas n », comme si c'étaient les seuls ;
– croire que si $\mathrm{car}\,(K)$ divise n, alors $(x + y)^n = x^n + y^n$ dans K : essayez $n = 6$ par exemple ;
– traiter à part le cas où a n'est pas une puissance n-ième, alors qu'un polynôme (in)séparable le reste sur toute extension ;
– lorsque a n'est pas une puissance n-ième, croire que P est irréductible ;
– appliquer le critère d'Eisenstein sur K : qu'est-ce qu'un élément irréductible d'un corps ?

Exercice 2 - (2,5 points) Soient A un anneau, E un A-module, F un sous-module de E, $\pi : E \to E/F$ la surjection canonique. Soient S une partie de E et T une partie de F. On suppose que T engendre F (comme A-module) et que $\pi(S)$ engendre E/F. Montrer que $S \cup T$ engendre E.

Soit x un élément de E. Son image $\pi(x)$ peut s'écrire $\pi(x) = \sum_{s \in S} \lambda_s \pi(s)$ où les λ_s sont des éléments de A presque tous nuls. L'élément $x' := \sum_{s \in S} \lambda_s\, s$ vérifie donc $\pi(x') = \pi(x)$, et donc $y := x' - x \in \mathrm{Ker}\, \pi = F$. Donc y est combinaison linéaire finie d'éléments de T, et par suite $x = y + x'$ est combinaison linéaire finie d'éléments de $S \cup T$.

Autre démonstration : soit E' le sous-module de E engendré par $S \cup T$. Alors E' contient le sous-module engendré par T, qui est F. D'après le théorème sur les sous-modules d'un quotient, on a donc $E' = \pi^{-1}(\pi(E'))$. Or $\pi(E')$ contient $\pi(S)$ donc est égal à E/F, donc $E' = E$.

Commentaires. La notion de sous-module engendré semble à peu près comprise, celle de module quotient beaucoup moins. J'ai beaucoup vu « $E \cong F \oplus (E/F)$ », notamment. D'autre part, ceux qui s'acharnent à voir les éléments de E/F comme des classes d'équivalence ont le droit de le faire, mais le résultat est le plus souvent une rédaction lourde et confuse, mélangeant par exemple parties de E et éléments de E.

Exercice 3 - (2,5 points) Donner un exemple d'un anneau A et d'un sous-A-module de A qui n'est pas libre.

Soient x_1 et x_2 deux éléments d'un anneau non nul A. Alors la famille (x_1, x_2) n'est pas libre : c'est clair si $x_1 = x_2 = 0$, et sinon on a la relation non triviale $x_2x_1 - x_1x_2 = 0$. Donc, si un sous-module (c'est-à-dire un idéal) de A est libre il est de rang ≤ 1, donc engendré par un élément. Il suffit donc de prendre pour A un anneau intègre non principal (par exemple $\mathbb{Z}[X]$) et pour I un idéal non principal de A, comme $(2, X)$.

Autre exemple : soit A non nul et non intègre (par exemple $\mathbb{Z}/4\mathbb{Z}$) et $I = xA$ où x est non nul et non régulier (par exemple $x = 2$). Soit $y \neq 0$ tel que $xy = 0$: alors $yI = 0$ donc I n'a aucune famille libre non vide. Comme il n'est pas nul il n'est donc pas libre.

Commentaire. Contrairement à ce que semblent croire une bonne moitié des candidats, $\mathbb{Z}/2\mathbb{Z}$ n'est pas un sous-$\mathbb{Z}$-module de $\mathbb{Z}$.

Exercice 4 - (2 points) Soit E le $\mathbb{Q}$-espace vectoriel $\mathbb{Q}^{10}$, et soit f l'endomorphisme de E de matrice diag $(J_2(1), J_1(1), J_3(2), J_3(2), J_1(2))$ (où $J_n(\lambda)$ désigne le bloc de Jordan de taille n et de valeur propre λ). Quels sont les facteurs invariants du $\mathbb{Q}[X]$-module E_f ?

De façon générale, le bloc de Jordan $J_n(\lambda)$ correspond au $\mathbb{Q}[X]$-module $\mathbb{Q}[X]/(X-\lambda)^n$. Donc

$$\begin{aligned} E_f &\simeq \mathbb{Q}[X]/(X-1)^2 \oplus \mathbb{Q}[X]/(X-1) \oplus \mathbb{Q}[X]/(X-2)^3 \oplus \mathbb{Q}[X]/(X-2)^3 \oplus \mathbb{Q}[X]/(X-2) \\ &\simeq \mathbb{Q}[X]/(X-1)^2(X-2)^3 \oplus \mathbb{Q}[X]/(X-1)(X-2)^3 \oplus \mathbb{Q}[X]/(X-2) \quad \text{(lemme chinois).} \end{aligned}$$

Comme $(X-2) \mid (X-1)(X-2)^3 \mid (X-1)^2(X-2)^3$, la suite des facteurs invariants est $\big((X-2),\ (X-1)(X-2)^3,\ (X-1)^2(X-2)^3\big)$.

Commentaire. Souvent, le résultat a bien été trouvé mais très mal (ou pas du tout) justifié.

Exercice 5 - (2 points) Que fait ce programme Maple ? Quelles sont les conditions sur L pour qu'il fonctionne ?
(Ne pas justifier les réponses).

```
f :=proc(L)
local n,d,s,t,g ;
n :=nops(L) ;
if n=2 then
d :=igcdex(L[1],L[2],'s','t') ;
RETURN(d,[s,t]) ;
else
d :=f(L[2..n]) ;
g :=igcdex(L[1],d[1],'s','t') ;
RETURN(g,[s,op(t*d[2])]) ;
fi ;
end ;
```

Conditions : L est une liste (c-à-d une suite entre crochets) d'au moins deux éléments. Les éléments de L sont des entiers relatifs.

Le programme renvoie le pgcd des éléments de L ainsi que des coefficients de Bézout : si $L = [a_1, \cdots, a_n]$, le résultat est $d, [t_1, \cdots, t_n]$ où $d = \text{pgcd}(a_1, \cdots, a_n)$ et où $d = a_1 t_1 + \cdots + a_n t_n$.

Exercice 6 - (8 points) Soit ζ le nombre complexe $e^{i\pi/6} = \frac{\sqrt{3}+i}{2}$. On pose $K = \mathbb{Q}(\zeta)$.
1- Trouver un polynôme $P \in \mathbb{Z}[X]$ unitaire et de degré 4 tel que $P(\zeta) = 0$. Quelles sont ses racines dans $\mathbb{C}$? dans K ?

On a $(2\zeta - \sqrt{3})^2 = -1 = 4\zeta^2 - 4\sqrt{3}\zeta + 3$, d'où : $\sqrt{3}\zeta = \zeta^2 + 1$. En élevant au carré, on obtient : $3\zeta^2 = \zeta^4 + 2\zeta^2 + 1$, donc $\zeta^4 - \zeta^2 + 1 = 0$. Le polynôme $P = X^4 - X^2 + 1$ est donc le polynôme cherché. (Autre démonstration : $\zeta^2 = -j^2$ donc $-\zeta^2$ est racine de $1 + X + X^2$).

Comme le polynôme P est pair et à coefficients réels, les racines de P dans $\mathbb{C}$ sont $\{\zeta, -\zeta, \overline{\zeta}, -\overline{\zeta}\}$ (elles sont toutes distinctes). Comme $\overline{\zeta} = \frac{1}{\zeta} \in K$, ce sont aussi les racines dans K.

Dans la suite, on admet que P est le polynôme minimal de ζ sur $\mathbb{Q}$.
2- Montrer que l'extension K est galoisienne sur $\mathbb{Q}$.

K est le corps de décomposition sur $\mathbb{Q}$ du polynôme P, qui est séparable (ses racines dans $\mathbb{C}$ sont simples) : l'extension $\mathbb{Q} \subset K$ est donc galoisienne.

On note G le groupe de Galois de K sur $\mathbb{Q}$. On admet qu'il est abélien.
3- Quel est le cardinal de G ? En déduire (en utilisant par exemple un théorème de structure) que $G \simeq \mathbb{Z}/4\mathbb{Z}$ ou $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Comme K est galoisienne, on a $|G| = [K : \mathbb{Q}] = 4$ car le polynôme minimal de ζ est de degré 4.

Le groupe G est donc abélien d'ordre 4. D'après le théorème de structure des groupes abéliens finis, il est produit de groupes cycliques ; il est immédiat que les seules possibilités sont (à isomorphisme près) $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

4- Montrer que K contient au moins deux sous-corps distincts de degré 2 sur $\mathbb{Q}$ (on remarquera que $\sqrt{3} \in K$ et $i \in K$).

D'après les calculs de la première question, on a $\sqrt{3} = \zeta + \frac{1}{\zeta} \in K$, puis $i = 2\zeta - \sqrt{3} \in K$. On a donc $\mathbb{Q}(\sqrt{3}) \subset K$ et $\mathbb{Q}(i) \subset K$. Ces deux sous-corps sont distincts puisque $i \notin \mathbb{R}$ et $\mathbb{Q}(\sqrt{3}) \subset \mathbb{R}$, et de degré 2 sur $\mathbb{Q}$ (immmédiat).

5- Que peut-on déduire de la question précédente en termes de sous-groupes de G ?

Par la correspondance de Galois, les deux sous-corps $\mathbb{Q}(\sqrt{3})$ et $\mathbb{Q}(i)$ correspondent à deux sous-groupes distincts de G, d'indice 2 et donc d'ordre 2.

6- En déduire que $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Comme le groupe $\mathbb{Z}/4\mathbb{Z}$ ne possède qu'un sous-groupe d'ordre 2 (à savoir $2\mathbb{Z}/4\mathbb{Z}$), le groupe G ne peut pas lui être isomorphe. On a donc nécessairement $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, d'après la question 3.