

G01. Algèbre commutative

Contrôle du 27 novembre 2006

Les trois exercices sont indépendants. Durée : 2 heures

1

Soit A un anneau (commutatif) et E un A -module. Pour un élément $a \in A$, on désigne par a_E l'homothétie de rapport a dans E , et par $\text{Ker}(a_E)$ son noyau; c'est donc le sous-module de E formé des $x \in E$ tels que $ax = 0$.

1.1. Dans cette question, $E = \mathbf{Z}/4\mathbf{Z}$, et $a = 2$. Déterminer $\text{Ker}(2_E)$, $E/2E$, ainsi que l'application composée $\text{Ker}(a_E) \rightarrow E \rightarrow E/aE$.

Le sous-groupe $\text{Ker}(2_E)$ est engendré par la classe de 2 laquelle classe dont l'image est nulle dans $E/2E \simeq \mathbf{Z}/2\mathbf{Z}$; l'application composée est donc nulle.

Dans la suite, a et b sont deux éléments de A tels que $aA + bA = A$, et E est un A -module tel que $abE = 0$.

1.2. Montrer que le morphisme canonique

$$E \longrightarrow E/aE \times E/bE$$

est un isomorphisme. Voyez-vous un rapport entre cette propriété et le théorème chinois ?

Par hypothèse, il existe des éléments $u, v \in A$ tels que

$$(\star) \quad au + bv = 1.$$

Montrons la surjectivité de l'application $E \longrightarrow E/aE \times E/bE$. Soient donc $\xi \in E/aE$ et $\eta \in E/bE$ deux éléments quelconques, et choisissons des représentants $x \in E$ pour ξ , et $y \in E$ pour η ; l'élément $z = auy + bvx$ est congru à $bvx = (1 - au)x \text{ mod. } aE$, soit finalement $z \equiv bvx \equiv x \text{ mod. } aE$. De même, $z \equiv auy = (1 - bv)y \equiv y \text{ mod. } bE$. Ainsi, l'image de z est $(\xi, \eta) \in E/aE \times E/bE$. Cela montre la surjectivité.

Injectivité : comme le noyau de l'application de passage au quotient $E \rightarrow E/aE$ est aE , le noyau de $E \rightarrow E/aE \times E/bE$ est égal à $aE \cap bE$; soit x un élément dans cette intersection. Comme $abE = 0$ et que $x \in aE$, on a $bx = 0$; de même, $ax = 0$; en utilisant la relation (\star) , on trouve $x = aux + bvx = 0$.

C'est une généralisation du théorème chinois qui correspond au cas où $E = A/abA$.

1.3. Montrer qu'on a une décomposition en somme directe

$$\text{Ker}(a_E) \oplus \text{Ker}(b_E) = E.$$

Expliquer comment retrouver, à partir de la décomposition précédente, le lemme des noyaux classique en algèbre linéaire sur un corps.

En utilisant de nouveau la relation (\star) , on obtient que tout $x \in E$ s'écrit

$$x = aux + bvx$$

Comme $abE = 0$, on a $aux \in \text{Ker}(b_E)$, et $bvx \in \text{Ker}(a_E)$, ainsi E est la somme des deux sous-espaces considérés. Montrons que cette somme est directe : si $x \in \text{Ker}(a_E) \cap \text{Ker}(b_E)$, alors la décomposition $x = aux + bvx$ montre que $x = 0$.

Dans la situation de l'algèbre linéaire sur un corps K , E est un K -espace vectoriel muni d'un endomorphisme φ ; on introduit l'anneau $A = K[X]$ et la structure de A -module sur E associée à φ , définie par $P.x = P(\varphi)(x)$ pour tout $x \in E$ et tout $P \in A[X]$. Les éléments a et b sont alors des polynômes en X , et l'homothétie a_E est l'endomorphisme $a(\varphi)$ de E ; ainsi, l'hypothèse $abE = 0$ signifie que l'endomorphisme $a(\varphi) \circ b(\varphi)$ est nul. Le lemme des noyaux classique dit que si a et b sont étrangers, l'espace E est somme directe de $\text{Ker}(a(\varphi))$ et $\text{Ker}(b(\varphi))$.

1.4. *Montrer que l'application composée*

$$\text{Ker}(a_E) \longrightarrow E \longrightarrow E/aE$$

est un isomorphisme. Expliquer la différence avec la question 1.1.

Pour $x \in E$, reprenons l'égalité $x = aux + bvx$. Elle entraîne la relation $x - bvx \in aE$; comme $abE = 0$, on a $bvx \in \text{Ker}(a_E)$; tout élément de E est donc congru à un élément de $\text{Ker}(a_E)$ modulo aE ; en d'autres termes, l'application composée $\text{Ker}(a_E) \rightarrow E \rightarrow E/aE$ est surjective. Vérifions qu'elle est aussi injective, c'est-à-dire que $aE \cap \text{Ker}(a_E) = 0$: or, si ax est annulé par a , on a $ax = a^2ux + abvx = 0$.

Pour relier les questions **1.2** et **1.3** on aurait pu aussi remarquer que $bE = \text{Ker}(a_E)$: en effet, l'inclusion $bE \subset \text{Ker}(a_E)$ provient de l'hypothèse $abE = 0$; réciproquement, si $ax = 0$, la relation (\star) montre que l'on a $x = bvx \in bE$.

Dans la question **1.1**, où $E = \mathbf{Z}/4\mathbf{Z}$ et $a = 2$, si b est élément étranger (ou comaximal) à a , alors b est impair, donc $bE = E$; la relation $abE = 0$ impliquerait donc $aE = 0$, ce qui n'est pas le cas.

2

Dans cet exercice A désigne un anneau intègre.

2.1. *Donner la définition d'élément irréductible. Soit $p \in A$ un élément non nul tel que l'idéal pA soit premier; montrer que p est irréductible.*

Un élément $a \in A$ est dit irréductible non inversible et si toute relation de la forme $a = bc$ entraîne que b ou c est inversible.

Soit $p \in A$ un élément non nul tel que l'idéal pA soit premier. Il n'est pas inversible sinon $pA = A$, ce qui s'oppose à la définition d'idéal premier. Si, d'autre part, $p = bc$, alors on a, bien sûr, $bc \in pA$, donc, par exemple, $b \in pA$ puisque l'idéal pA est premier; cela s'écrit $b = pb'$ d'où $p(1 - b'c) = 0$; mais A est supposé intègre, et p est non nul, donc $1 = b'c$ et c est inversible.

On rappelle que, dans un anneau factoriel, tout élément irréductible engendre un idéal premier.

2.2. *(Cette question, plus difficile que les suivantes, propose simplement des exemples, et ne sera pas utilisée dans la suite) Soit K le corps des fractions de A . Soit t un élément de A . Montrer que $X^2 - t$ est irréductible dans $A[X]$ si et seulement si t n'est pas le carré d'un élément de A .*

Si $t = u^2$ est le carré d'un élément $u \in A$, alors $X^2 - t = (X - u)(X + u)$ est réductible. Réciproquement, supposons que $X^2 - t$ soit réductible dans $A[X]$; on a donc une égalité de la forme

$$X^2 - t = (aX + b)(cX + d).$$

Elle entraîne $ac = 1$; par suite, a et c sont inversibles dans A , et l'égalité ci-dessus s'écrit aussi $X^2 - t = (X + b/a)(X + d/c)$; l'élément $u = -b/a$ est dans A et est une racine du polynôme ; on a donc $u^2 = t$.

Montrer que $X^2 - t$ engendre un idéal premier de $A[X]$ si et seulement si t n'est pas le carré d'un élément de K (Montrer d'abord que la condition est nécessaire ; pour montrer qu'elle est suffisante, on pourra utiliser la division euclidienne par $X^2 - t$).

Supposons qu'il existe $a, b \in A, a \neq 0$ tels que, dans le corps des fractions K de A , on ait $t = b^2/a^2$; alors, dans $A[X]$, on a

$$a^2(X^2 - t) = (aX - b)(aX + b).$$

Si a est inversible dans A le polynôme $X^2 - t$ est réductible. Si a n'est pas inversible, l'égalité ci-dessus entraîne que l'idéal engendré par $X^2 - t$ n'est pas premier, puisqu'il ne contient pas $aX \pm b$ (regarder les degrés).

Supposons, enfin, que l'idéal de $A[X]$ engendré par $X^2 - t$ ne soit pas premier ; on a donc, dans $A[X]$, un relation de la forme

$$P(X)Q(X) = (X^2 - t)R(X),$$

où ni P ni Q ne sont multiples de $X^2 - t$. Par division euclidienne, on obtient

$$P = (X^2 - t)P_1 + aX + b, \quad Q = (X^2 - t)Q_1 + cX + d.$$

Les polynômes $aX + b$ et $cX + d$ ne sont pas dans l'idéal $(X^2 - t)$, c'est-à-dire, sont non nuls, et on a

$$(aX + b)(cX + d) = (X^2 - t)R_1(X).$$

En regardant les degrés, on constate que R_1 est constant, et qu'il est égal à ac en particulier $ac \neq 0$; on a aussi $ad + bc = 0$ et $bd = -tac$. Dans K , ces égalités s'écrivent $b/a = -d/c$ et $-t = (b/a)(d/c)$; ainsi $t = (b/a)^2$ est un carré dans K .

Il y a une façon plus directe, et un peu plus savante, de démontrer cela : le morphisme

$$A[X]/(X^2 - t) \longrightarrow K[X]/(X^2 - t)$$

est injectif : car, en désignant par x , resp. y , la classe de X dans l'anneau de gauche, resp. de droite, la A -base $\{1, x\}$ est envoyée sur la K -base $\{1, y\}$. Par suite, si t n'est pas un carré dans K , le polynôme $X^2 - t$ est irréductible dans l'anneau principal $K[X]$, donc le quotient est un corps ; par suite le sous-anneau $A[X]/(X^2 - t)$ est intègre.

Réciproquement, si cet anneau est intègre, il en est de même de son anneau de fractions à dénominateurs dans $S = A - \{0\}$

$$S^{-1}(A[X]/(X^2 - t)) = K[X]/(X^2 - t).$$

2.3. *Soit A un anneau principal et p un élément non nul de A . Montrer que si p engendre un idéal premier de A , alors cet idéal est même maximal. Donner un exemple d'anneau factoriel (non principal!) contenant un élément irréductible qui n'engendre pas un idéal maximal.*

Soit I un idéal de A contenant strictement pA ; il faut montrer que $I = A$. Or, comme A est principal, $I = uA$ pour un élément $u \in I$; la relation $pA \subset I$ s'écrit $p = uv$; mais p est irréductible, donc u ou v est inversible ; dans ce dernier cas $pA = uA$ contrairement à l'hypothèse ; donc u est inversible, et $uA = A$.

La question qui suit concerne la réciproque de la précédente. On suppose que A est factoriel et que tout élément irréductible de A engendre un idéal maximal ; il s'agit de montrer que A est principal.

2.4. Montrer que si a et b n'ont pas de diviseur commun, alors $aA + bA = A$ (on pourra raisonner par récurrence sur le nombre de diviseurs irréductibles de a).

L'énoncé aurait dû contenir l'hypothèse $a \neq 0$ et $b \neq 0$.

Soit n le nombre de diviseurs de a (supposé non nul). Si $n = 0$, alors a est inversible et $aA = A$. Soit a un élément produit de n éléments irréductibles ne divisant pas b , et soit p un élément irréductible ne divisant pas non plus b . L'hypothèse de récurrence entraîne l'égalité $aA + bA = A$, d'où $pA = paA + pbA \subset paA + bA$; l'inclusion est stricte puisque p ne divise pas b , c'est-à-dire $b \notin pA$; mais, par hypothèse, l'idéal pA est maximal, donc $paA + bA = A$.

En déduire que tout idéal engendré par deux éléments est principal.

Soient d le pgcd de a et b , de sorte que $a = da'$, $b = db'$ et a' et b' n'ont pas de diviseurs communs; on a donc $a'A + b'A = A$, et par suite $aA + bA = dA$.

2.5. (Facultatif, mais apporte des points supplémentaires à ceux qui auraient regardé le corrigé du contrôle précédent) Montrer que si tout idéal de A engendré par deux éléments est principal, alors A est principal.

Voir le corrigé du contrôle précédent.

3

3.1. Soit I un idéal d'un anneau (commutatif) A . Soit E un A -module de type fini tel que $E = IE$. Le but de cette question est de montrer qu'il existe un élément $a \in I$ tel que $(1 + a)E = 0$.

Soit $\{x_1, \dots, x_n\}$ un système générateur du module E . Traduire la relation $E = IE$ en n égalités :

$$\begin{array}{ccccccc} x_1 & = & c_{11}x_1 & + & c_{12}x_2 & + & \cdots & + & c_{1n}x_n \\ & & \vdots & & \vdots & & & & \vdots \\ x_n & = & c_{n1}x_1 & + & c_{n2}x_2 & + & \cdots & + & c_{nn}x_n \end{array}$$

où les coefficients c_{ij} sont dans I ; soit $C = (c_{ij})$ la matrice carrée correspondante. Montrer que $\det(1_n - C)$ annule E (penser à la matrice des cofacteurs). Conclure.

Le module IE est formé des sommes finies d'éléments de la forme ax , avec $a \in I$ et $x \in E$; chaque x s'exprime comme combinaison linéaire à coefficients dans A des x_i , donc chaque ax s'exprime comme combinaison linéaire des x_i à coefficients dans I , puisque $ab \in I$ pour tout $b \in A$. L'égalité $E = IE$ se traduit donc par le tableau des relations indiqué.

Soit $X \in E^n$ le vecteur colonne des générateurs x_i . Le tableau est résumé dans la relation

$$(1_n - C)X = 0.$$

Soit $D \in M_n(A)$ la transposée de la matrice des cofacteurs de $(1_n - C)$; on a donc

$$D.(1_n - C) = \det((1_n - C)).1_n.$$

Posons $\delta = \det(1_n - C)$. On a donc

$$0 = D.(1_n - C)X = \delta X,$$

ou encore, pour tout i , $\delta x_i = 0$; mais les x_i forment un système générateur de E , donc $\delta E = 0$.

Vérifions que $\delta \in 1 + I$: un déterminant est une expression polynomiale en les coefficients d'une matrice carré $M \in M_n(A)$; un morphisme d'anneaux $f : A \rightarrow B$ respectant les produits et sommes, on voit que

$$\det(f(M)) = f(\det(M)).$$

Appliquant cette remarque à la matrice $(1_n - C)$ et à son image $1_n \in M_n(A/I)$, on voit que

$$\delta \equiv 1 \pmod{I}$$

3.2. Soit F un A -module, et $f : F \rightarrow F$ une application A -linéaire. Expliquer pourquoi on définit une structure de $A[X]$ -module sur F en posant $P.x = P(f)(x)$ pour tout $x \in F$ et tout $P \in A[X]$.

Soit $I = (X)$ l'idéal de $A[X]$ engendré par X . Quel est le sous-module $IF \subset F$?

On suppose maintenant que F est un A -module de type fini, et que f est surjective. Montrer que f est un isomorphisme en utilisant la propriété établie en **3.1**.

Le sous-module IF est exactement l'image $f(F)$ de f . Si f est surjective, donc si $F = f(F)$, la question précédente montre qu'il existe un polynôme dans I , donc de la forme $XP(X)$ tel que $(1 + P(X)X)F = 0$, soit, pour tout $y \in F$,

$$y + P(f)(f(y)) = 0.$$

Si $f(y) = 0$, on a donc $y = 0$; autrement dit, f est injective.