Année universitaire 2012-2013 Licence 3 de mathématiques

Algèbre 4 - Devoir surveillé

Corrections

Tout anneau ci-dessous est commutatif. Si a et b sont des éléments d'un anneau A, on note par $\langle a, b\rangle$ l'idéal engendré par a et b.

Questions de cours

1. Soient A un anneau, $a, b \in A$. Rappeler la définition du $\mathrm{pgcd}(a, b)$.

   On appel $d \in A$ le $\mathrm{pgcd}(a, b)$ si d est diviseur commun de a et b (c'est à dire, $d \mid a$ et $d \mid b$) et tout autre diviseur commun de a et b divise d. Le $\mathrm{pgcd}(a, b)$ est bien défini à l'équivalence arithmétique près.

2. Supposons que l'anneau A est factoriel. Montrer l'existence du $\mathrm{pgcd}(a, b)$ pour tout $a, b \in A$.

   Supposons que $a, b \neq 0$. Soit $\{p_1, \dots, p_s\}$ l'ensemble de tous (à équivalence près) les diviseurs irréductibles de ab. Alors on factorise a et b comme $a = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ et $b = p_1^{\beta_1} \cdots p_s^{\beta_s}$, ou $\alpha_i, \beta_i \in \mathbb{Z}_{\geq 0}$. Alors $p_1^{\min\{\alpha_1,\beta_1\}} \cdots p_s^{\min\{\alpha_s,\beta_s\}} = \mathrm{pgcd}(a, b)$.
   Si, disons, $a = 0$ alors $\mathrm{pgcd}(a, b) = b$.

3. Supposons que l'anneau A est factoriel. Rappeler la définition du *contenu* d'un polynôme $P(t) \in A[t]$, et la définition d'un *polynôme primitif*.

   Le *contenu* d'un polynôme est le pgcd des ses coefficients. Un polynôme est dit *primitif* si son contenu est 1. Si d est le contenu du polynôme P alors $P = d\widetilde{P}$ où $\widetilde{P}$ est un polynôme primitif.

4. Quel lien y a-t-il entre les contenus de $P(t)$, de $Q(t)$ et de $P(t)Q(t)$? Démontrer cette propriété.

   Le « Lemme de Gauss » affirme que $\mathrm{cont}(PQ) = \mathrm{cont}(P)\,\mathrm{cont}(Q)$. Considérons d'abord le cas particulier où P et Q sont primitifs. Il faut montrer que PQ est primitif. Pour ceci, il suffit de montrer qu'aucun irréductible p ne divise tous les coefficients de PQ. Fixons un tel p et écrivons

   $$P(t) = a_0 + a_1 t + \dots, \quad Q(t) = b_0 + b_1 t + \dots, \quad P(t)Q(t) = c_0 + c_1 t + \dots,$$

   Puisque P est primitif il existe i tel que $p \nmid a_i$. Soit k le plus petit i avec ce propriété. De même, soit ℓ le plus petit j tel que $p \nmid b_j$. On a

   $$p \nmid a_k, \quad p \mid a_i \quad (i = 0, \dots, k-1); \qquad p \nmid b_\ell, \quad p \mid b_j \quad (j = 0, \dots, \ell-1).$$

   En écrivant

   $$c_{k+\ell} = \sum_{i=0}^{k-1} a_i b_{k+\ell-i} + a_k b_\ell + \sum_{i=k+1}^{k+\ell} a_i b_{k+\ell-i} = \sum_{i=0}^{k-1} a_i b_j + a_k b_\ell + \sum_{j=0}^{\ell-1} a_{k+\ell-j} b_j$$

   on observe que les deux sommes sont divisibles par p mais le terme $a_k b_\ell$ n'en est pas. Ceci montre que $p \nmid c_{k+\ell}$, ce qui achève la démonstration du lemme de Gausse pour les polynômes primitifs.
   Pour démontrer le cas général du lemme de Gauss on écrit $P = d\widetilde{P}$ et $Q = e\widetilde{Q}$, où $d = \mathrm{cont}(P)$, $e = \mathrm{cont}(Q)$ et $\widetilde{P}, \widetilde{Q}$ sont primitifs. Alors $PQ = de\widetilde{P}\widetilde{Q}$, où $\widetilde{P}\widetilde{Q}$ est primitif par le précédent, ce qui montre que $\mathrm{cont}(PQ) = de$.

5. Déterminer le contenu du polynôme

   $$P(t) = (t + 2)(2t + 3)(3t + 4) \cdots (2011t + 2012) \in \mathbb{Z}[t].$$

   Le polynôme $nt + n + 1$ est primitif : son contenu divise $n + 1 - n = 1$. Le polynôme $P(t)$ est donc primitif comme produit de polynômes primitifs.

Exercice 1

1. Démontrer que le polynôme $F(t, u) = (t + 2)^3 - (u + 3)^2$ est irréductible dans l'anneau $\mathbb{R}[t, u]$.

   Si $F(t, u)$ est réductible, alors le polynôme $G(t, u) = F(t - 2, u - 3) = t^3 - u^2$ est également réductible. Il est clair que G n'est pas divisible par un polynôme non-constant appartenant à $\mathbb{R}[t]$. Donc $G = H_1 H_2$ avec $\deg_u H_1 = \deg_u H_2 = 1$, ce qui signifie que G, considéré comme polynôme en u sur $\mathbb{R}(t)$, doit avoir une racine dans le corps $\mathbb{R}(t)$. Mais il n'en a pas.

2. Soit S un ensemble infini de nombres réels et soit I l'ensemble des polynômes $P(t, u) \in \mathbb{R}[t, u]$ vérifiant

   $$P(a^2 - 2, a^3 - 3) = 0 \quad \text{pour tout } a \in S.$$

   Montrer que I est un idéal de l'anneau $\mathbb{R}[t, u]$. Vérifier que $F(t, u) \in I$.

   Si $P_1(a^2 - 2, a^3 - 3) = P_2(a^2 - 2, a^3 - 3) = 0$ alors $(P_1 + P_2)(a^2 - 2, a^3 - 3) = 0$, et si $P(a^2 - 2, a^3 - 3) = 0$ alors pour tout $Q \in \mathbb{R}[t, u]$ on a $(QP)(a^2 - 2, a^3 - 3) = 0$. Ceci démontre que I est un idéal.
   Pour tout $a \in \mathbb{R}$ on a $F(a^2 - 2, a^3 - 3) = a^6 - a^6 = 0$, ce qui montre que $F \in I$.

3. Vérifier que l'application

$$f: \begin{array}{rcl} R[t,u] & \to & \mathbb{R}[x] \\ P(t,u) & \mapsto & P(x^2-2, x^3-3) \end{array}$$

est un morphisme d'anneaux. Préciser la relation entre le noyau de ce morphisme, l'idéal I et l'idéal $\langle F(t,u)\rangle$.

La vérification que f est un morphisme est immédiate.

Si $P \in \ker f$ alors $P(a^2-2, a^3-3) = 0$ pour tout $a \in \mathbb{R}$, ce qui implique $P \in I$. Réciproquement, si $P \in I$ alors le polynôme $P(x^2-2, x^3-3) \in \mathbb{R}[x]$ admet comme racine tout élément de l'ensemble infini S, ce qui n'est possible que si $P(x^2-2, x^3-3)$ est polynôme nul, ce qui signifie que $P \in \ker f$. On a montré que $\ker f = I$.

Notons $\tilde{I}$ l'idéal de l'anneau $\mathbb{R}(t)[u]$ engendré par I. C'est un idéal principal (parce que l'anneau est principal comme l'anneau de polynômes d'une seule variable sur un corps) propre contenant F. Puisque F est irréductible dans $\mathbb{R}(t)[u]$, on a $\tilde{I} = \langle F\rangle$, ce qui implique que pour tout $P \in I$ le polynôme F divise P dans $\mathbb{R}(t)[u]$. Puisque F est primitif comme polynôme en u sur $\mathbb{R}[t]$, il divise P dans $\mathbb{R}[t][u]$. Ceci montre que $I = \langle F\rangle$.

Exercice 2

1. Le polynôme $t^3 - t - 30$ est-il réductible dans $\mathbb{Q}[t]$? dans $\mathbb{Z}[t]$? Mêmes questions sur le polynôme $t^3 + t + 30$.

   Si le polynôme primitif $at^3 + bt^2 + ct + d \in \mathbb{Z}[t]$ de degré 3 est réductible dans $\mathbb{Z}[t]$ alors il admet un facteur linéaire $\alpha t + \beta \in \mathbb{Z}[t]$, et il est clair que $\alpha \mid a$ et $\beta \mid d$. En particulier, si $a = 1$ alors f admet une racine entière qui divise d.

   En vérifiant tous les diviseurs de 30, on trouve que $t^3 + t + 30$ admet la racine -3, donc réductible, mais $t^3 - t - 30$ n'admet pas de racine parmi les diviseurs de 30, donc irréductible.

2. Mêmes questions sur le polynôme $t^{2012} + 21t^{49} + 49t^{21} + 70$.

   Ce polynôme est irréductible d'après le critère d'Eisenstein avec $p = 7$.

3. (a) Déterminer tous les polynômes irréductibles de degré 2 dans l'anneau $\mathbb{F}_2[t]$, où $\mathbb{F}_2$ désigne le corps de 2 éléments.

   Si $t^2 + bt + c \in \mathbb{F}_2[t]$ est irréductible alors $c = 1$. Il n'y a que 2 polynômes avec cette propriété : $t^2 + 1 = (t+1)^2$, qui est réductible, et $t^2 + t + 1$, qui n'admet pas de racine dans $\mathbb{F}_2$, donc irréductible.

   (b) Le polynôme $t^5 + t^2 + 1$ est-il réductible dans $\mathbb{F}_2[t]$?

   Si ce polynôme est réductible alors il doit admettre soit une racine dans $\mathbb{F}_2$, soit un facteur irréductible de degré 2, qui est forcement $t^2 + t + 1$. On voit immédiatement qu'il n'y a pas de racine, et la division euclidienne montre que $t^2 + t + 1$ ne divise pas $t^5 + t^2 + 1$. Donc ce dernier est irréductible.

   (c) Le polynôme

   $$2007t^5 + 2008t^4 + 2010t^3 + 2011t^2 + 2012t + 2013 \tag{1}$$

   est-il réductible dans $\mathbb{Z}[t]$?

   L'image de ce polynôme par le morphisme $\mathbb{Z}[t] \to \mathbb{F}_2[t]$ (réduction modulo 2) est $t^5 + t^2 + 1$, qui est irréductible dans $\mathbb{F}_2[t]$. Ceci implique que le polynôme (1) est irréductible dans $\mathbb{Z}[t]$.

Exercice 3

1. Déterminer la décomposition en facteurs irréductibles du polynôme $t^4 - t$ dans $\mathbb{Z}[t]$.

   $t^4 - t = t(t-1)(t^2+t+1)$

2. Soit p un nombre premier et $\mathbb{F}_p$ le corps de p éléments. Montrer que les anneaux $\mathbb{Z}[t]/\langle t^4 - t + p, t^2 + t + 1\rangle$ et $\mathbb{F}_p[t]/\langle t^2 + t + 1\rangle$ sont isomorphes.

   On utilise la propriété générale suivante. Soient A un anneau, I et J des idéaux de A et $\bar{J}$ l'image de J dans A/I. Alors

   $$A/(I+J) \cong (A/I)/\bar{J}. \tag{2}$$

   (Pour la démontrer on considère les morphismes naturels $A \to A/I \to (A/I)/\bar{J}$ et montre que le noyau du morphisme composé est $I + J$.)

   Dans notre cas $A = \mathbb{Z}[t]$. Puisque $(t^2+t+1) \mid (t^4 - t)$, on a

   $$\langle t^4 - t + p, t^2 + t + 1\rangle = \langle p, t^2 + t + 1\rangle = I + J, \qquad I = \langle p\rangle, \quad J = \langle t^2 + t + 1\rangle,$$

   et donc $A/I = \mathbb{F}_p[t]$ et $\bar{J} = \langle t^2 + t + 1\rangle$, ce qui achève le résultat.

3. Montrer que l'anneau $\mathbb{R}[t,u]/\langle t^4 - t + u, t^2 + t + 1\rangle$ est isomorphe à $\mathbb{C}$.

   De même, $A = \mathbb{R}[t,u]$,

   $$\langle t^4 - t + u, t^2 + t + 1\rangle = \langle u, t^2 + t + 1\rangle = I + J, \qquad I = \langle u\rangle, \quad J = \langle t^2 + t + 1\rangle,$$

   et donc $A/I = \mathbb{R}[t]$ et $\bar{J} = \langle t^2 + t + 1\rangle$, ce qui démontre que

   $$\mathbb{R}[t,u]/\langle t^4 - t + u, t^2 + t + 1\rangle \cong \mathbb{R}[t]/\langle t^2 + t + 1\rangle.$$

   Puis, le morphisme $\mathbb{R}[t] \to \mathbb{C}$ définie par $t \mapsto \frac{-1+\sqrt{-3}}{2}$ est surjectif et son noyau est $\langle t^2 + t + 1\rangle$, ce qui démontre que $\mathbb{R}[t]/\langle t^2 + t + 1\rangle \cong \mathbb{C}$.