MAT4111

Premier Semestre — 2018-2019

Premier Contrôle Continu

1	
2	
3	
4	
5	

1. Soit $I \subseteq \mathbb{Z}[i]$ un idéal non nul. Montrer que l'anneau $\mathbb{Z}[i]/I$ est fini.
Indication : *Utiliser le fait (qu'il ne faut pas démontrer) que* $\mathbb{Z}[i]$ *est euclidien.*

Solution. Comme $\mathbb{Z}[i]$ est euclidien, il est principal. Cela implique que I est un idéal principal, *i.e.* il existe $z_0 = a + ib \in A \setminus \{0\}$ tel que $I = (z_0)$. Soit $N = \lfloor |z_0| \rfloor + 1 \in \mathbb{N}$. C'est clair que le cardinal de l'ensemble $A_N = \{z \in A : |z| < N\}$ est inférieur ou égal à $(2N-1)^2$. En effet, $a + ib \in A_N$ implique que $|a| < N$ et $|b| < N$, ce qui nous dit que $a, b \in \{-N+1, \dots, N-1\}$.

Par ailleurs, comme $\mathbb{Z}[i]$ est euclidien, pour tout $z \in A$ il existe $q_z \in A$ et $r_z \in A$ uniques tels que $z = q_z z_0 + r_z$ et $|r_z| < |z_0|$. Comme $|z_0| \leq N$, la dernière condition nous dit que $r_z \in A_N$. On définit alors l'application $\phi : A/I \to A_N$ via $\phi([z]) = r_z$, où $[z] \in A/I$ dénote la classe de $z \in A$. Cette application est bien définie, puisque si $z' - z = wz_0$ et $z = q_z z_0 + r_z$ avec $|r_z| < |z_0|$, alors $z' = (q_z + w)z_0 + r_z$, *i.e.* $\phi([z']) = \phi([z]) = r_z$. En plus c'est clair que ϕ est injectif, parce que $r_z = 0$ équivaut à $z \in I$, *i.e.* $[z] = 0$. Comme ϕ est injectif, $\#(A/I) \leq \#(A_N) \leq (2N-1)^2$.

2. Soit A un anneau commutatif intègre. Une *dérivation* de A est une application $d : A \to A$ satisfaisant que $d(a+b) = d(a) + d(b)$ et $d(ab) = d(a)b + ad(b)$, pour tous $a, b \in A$. On note $\mathsf{Der}(A)$ l'ensemble formé de toutes les dérivations de A.

(a) Étant donné $d \in \mathsf{Der}(A)$, on définit $A^d = \{a \in A : d(a) = 0\}$. Montrer que A^d est un sous-anneau de A.

(b) Montrer qu'il existe une unique dérivation $\bar{d} \in \mathsf{Der}(\mathsf{Fr}(A))$ telle que $\bar{d} \circ i = i \circ d$, où $i : A \to \mathsf{Fr}(A)$ est l'inclusion canonique. En déduire que l'image du morphisme canonique $\bar{j} : \mathsf{Fr}(A^d) \to \mathsf{Fr}(A)$ induit par l'inclusion $j : A^d \to A$ est incluse dans $\mathsf{Fr}(A)^{\bar{d}}$.

Solution.

(a) Comme d est un morphisme de groupes abéliens, $d(0) = 0$, *i.e.* $0 \in A^d$. En plus, si $a, b \in A^d$, alors $d(a+b) = d(a) + d(b) = 0$ et $d(-a) = -d(a) = 0$, ce qui nous dit que A^d est sous-groupe de A pour l'opération $+$. En outre, comme $d(1) = d(1 \cdot 1) = 1 \cdot d(1) + d(1) \cdot 1 = d(1) + d(1)$, on conclut que $d(1) = 0$, *i.e.* $1 \in A^d$. Si $a, b \in A^d$, $d(ab) = d(a)b + ad(b) = 0 \cdot b + a \cdot 0 = 0$, *i.e.* $ab \in A^d$. Cela implique que A^d est un sous-anneau de A.

(b) Étant donné $a, b \in A$ avec $b \neq 0$, on définit

$$\bar{d}(a/b) = \frac{d(a)b - ad(b)}{b^2} \tag{1}$$

Soient $a', b' \in A$ avec $b' \neq 0$ des éléments tels que $a/b = a'/b'$, *i.e.* $ab' = a'b$. Il faut montrer que

$$\bar{d}(a/b) = \bar{d}(a'/b'), \text{ i.e. } (b')^2\big(d(a)b - ad(b)\big) = b^2\big(d(a')b' - a'd(b')\big).$$

Or, on sait que $d(a)b' + ad(b') = d(ab') = d(a'b) = d(a')b + a'd(b)$, ce qui implique que

$$bb'\big(d(a)b' - a'd(b)\big) = bb'\big(d(a')b - ad(b')\big).$$

Si l'on utilise $a'b = ab'$, on voit bien que le membre de gauche coïncide avec $d(a)b(b')^2 - a(b')^2d(b) = (b')^2(d(a)b - ad(b))$, tandis que le membre de droite est égal à $d(a')b^2b' - a'b^2d(b') = b^2(d(a')b' - a'd(b'))$, comme on voulait démontrer.

C'est facile à vérifier que

$$\begin{aligned}\bar{d}\left(\frac{a}{b} + \frac{a'}{b'}\right) = \bar{d}\left(\frac{ab' + a'b}{bb'}\right) &= \frac{d(ab' + a'b)bb' - (ab' + a'b)d(bb')}{(bb')^2} \\ &= \frac{d(a)b(b')^2 + d(a')b'b^2 - ad(b)(b')^2 - a'd(b')b^2}{(bb')^2} \\ &= \frac{d(a)b - ad(b)}{b^2} + \frac{d(a')b' - a'd(b')}{(b')^2} = \bar{d}\left(\frac{a}{b}\right) + \bar{d}\left(\frac{a'}{b'}\right)\end{aligned}$$

et

$$\begin{aligned}\bar{d}\left(\frac{a}{b}\frac{a'}{b'}\right) = \bar{d}\left(\frac{aa'}{bb'}\right) &= \frac{d(aa')bb' - aa'd(bb')}{(bb')^2} \\ &= \frac{d(a)ba'b' + d(a')b'ab - ad(b)a'b' - a'd(b')ab}{(bb')^2} \\ &= \frac{d(a)b - ad(b)}{b^2}\frac{a'}{b'} + \frac{d(a')b' - a'd(b')}{(b')^2}\frac{a}{b} = \bar{d}\left(\frac{a}{b}\right)\frac{a'}{b'} + \frac{a}{b}\bar{d}\left(\frac{a'}{b'}\right),\end{aligned}$$

pour tous $a, b, a', b' \in A$ tels que $b, b' \neq 0$. Cela nous dit que $\bar{d} \in \mathrm{Der}(\mathrm{Fr}(A))$. Pour l'unicité de $\bar{d}$, noter que si $\tilde{d} \in \mathrm{Der}(\mathrm{Fr}(A))$ satisfait que $\tilde{d}(a/1) = d(a)$, alors $\tilde{d}(a/b) = d(a)/b + a\tilde{d}(1/b)$ pour $a = b$ nous dit que $\tilde{d}(1/b) = -d(b)/b^2$ (puisque $\tilde{d}(1) = 0$), ce qui implique que $\tilde{d}(a/b) = (d(a)b - ad(b))/b^2 = \bar{d}(a/b)$, pour tout $a/b \in \mathrm{Fr}(A)$.

Par ailleurs, on sait que $\bar{j}(a/b) = a/b$, pour tout $a, b \in A^d$, avec $b \neq 0$. L'expression (1) nous dit que $\bar{d}(a/b) = (d(a)b - ad(b))/b^2 = 0/b^2 = 0$, si $a, b \in A^d$, avec $b \neq 0$, ce qui implique que l'image de $\bar{j} : \mathrm{Fr}(A^d) \to \mathrm{Fr}(A)$ est incluse dans $\mathrm{Fr}(A)^{\bar{d}}$.

3. Soient $z_1, z_2, z_3, z_4 \in \mathbb{C}$ tels que

$$\sum_{h=1}^{4} z_h = \sum_{h=1}^{4} z_h^3 = 0.$$

Montrer qu'il existe $i, j \in \{1, \dots 4\}$ tels que $i \neq j$ et $z_i + z_j = 0$.

Indication : *Utiliser les identités de Newton* $S_\ell + \sum_{i=1}^{\ell-1}(-1)^i \sigma_i S_{\ell-i} + (-1)^\ell \ell \sigma_\ell = 0$*, pour* $1 \leq \ell \leq n$.

Solution. Si $z_1 = z_2 = z_3 = z_4 = 0$, il n'y a rien à démontrer. On suppose désormais qu'il y a au moins une racine non nulle. On écrit le polynôme $P = \prod_{h=1}^{4}(X - z_h) = X^4 + c_3X^3 + c_2X^2 + c_1X + c_0$. Par définition des polynômes symétriques élémentaires, on sait que $c_\ell = (-1)^\ell \sigma_\ell(z_1, z_2, z_3, z_4)$, pour tout $\ell \in \{1, \dots, 4\}$. Par hypothèse, on sait que $S_1(z_1, z_2, z_3, z_4) = S_3(z_1, z_2, z_3, z_4) = 0$. D'après les identités de Newton, on voit bien

$$c_1 = -\sigma_1(z_1, z_2, z_3, z_4) = -S_1(z_1, z_2, z_3, z_4) = 0$$

et

$$c_3 = -\sigma_3(z_1, z_2, z_3, z_4) = -\frac{1}{3}\Big(S_3 - \sigma_1 S_2 + \sigma_2 S_1\Big)\Big|_{X_i = z_i, i=1,\dots,4} = 0.$$

Cela implique que $P = X^4 + c_2X^2 + c_0$ est un polynôme biquadratique, et en particulier, si $r \in \{z_1, z_2, z_3, z_4\}$ est une racine non nulle de P, $-r$ ($\neq r$, vu que $r \neq 0$) est aussi une racine de P.

4. Soit A un anneau commutatif noethérien et soit $f : A \to A$ un morphisme d'anneaux. Montrer que f est surjectif si et seulement si f est bijectif.
Indication : *Étudier le noyau de* $f^{(n)} = f \circ \cdots \circ f$*, pour* $n \in \mathbb{N}^*$.

Solution. Il suffit de démontrer que tout morphisme surjetif d'anneaux est injectif. On suppose que f n'est pas injectif, *i.e.* $I = \mathrm{Ker}(f) \neq 0$. Pour tout $n \in \mathbb{N}^*$, on considère le morphisme d'anneaux $f^{(n)} = f \circ \cdots \circ f$ (où il y a $n-1$ compositions). Soit $I_n = \mathrm{Ker}(f^{(n)})$, pour $n \in \mathbb{N}^*$, et $I_0 = 0$. On note que I_n est un idéal de A pour tout $n \in \mathbb{N}$ et que $I_1 = I$. C'est clair que $I_n \subseteq I_{n+1}$, pour $n \in \mathbb{N}$. En effet, le cas $n = 0$ est immédiat et, si $a \in I_n$ avec $n \geq 1$, alors $f^{(n+1)}(a) = f \circ f^{(n)}(a) = f(0) = 0$, *i.e.* $a \in I_{n+1}$. D'ailleurs, comme A est noethérien, il existe $N \in \mathbb{N}^*$ tel que $I_n = I_N$, pour tout $n \geq N$. Soit n_0 le plus petit entier non négatif tel que $I_n = I_{n_0}$, pour tout $n \geq n_0$. Par définition, $n_0 \in \mathbb{N}^*$ et $I_{n_0-1} \subsetneq I_{n_0}$. Soit $a \in I_{n_0} \setminus I_{n_0-1}$. Comme f est surjectif, il existe $b \in A$ tel que $f(b) = a$. Or, $a \in I_{n_0}$ nous dit que $0 = f^{(n_0)}(a) = f^{(n_0+1)}(b)$, *i.e.* $b \in I_{n_0+1}$. Comme $I_{n_0+1} = I_{n_0}$ et $b \in I_{n_0+1}$, $f^{(n_0-1)}(a) = f^{(n_0)}(b) = 0$, *i.e.* $a \in I_{n_0-1}$, ce qui est absurde.

5. Soit A un anneau commutatif intègre.

(a) Rappeler la définition d'élément irréductible et d'élément premier.

(b) Démontrer que tout élément premier de A est irréductible. Donner un contre-exemple pour prouver que la réciproque n'est pas vraie.

Solution. Il s'agit des résultats du cours.