Agrégation Interne. Le 04/01/2012

Anneaux euclidiens

On rappelle :
- que deux éléments a, b d'un anneau unitaire $\mathbb{A}$, sont dit associés s'il existe un élément inversible $u \in \mathbb{A}^\times$ tel que $b = ua$;
- qu'un anneau $\mathbb{A}$ est dit intègre s'il est commutatif, unitaire et n'admet pas de diviseur de 0, c'est-à-dire que pour a, b dans $\mathbb{A}$, on a :

$$a \cdot b = 0 \Leftrightarrow a = 0 \text{ ou } b = 0$$

- qu'un anneau $\mathbb{A}$ est principal s'il est intègre et si tout idéal de $\mathbb{A}$ est principal, c'est-à-dire de la forme $I = a_0 \cdot \mathbb{A}$;
- qu'un élément p d'un anneau commutatif, unitaire et intègre $\mathbb{A}$, est irréductible si $p \neq 0$, p n'est pas inversible et :

$$(p = uv) \Rightarrow (u \text{ ou } v \text{ est inversible})$$

(les seuls diviseurs de p sont les éléments inversibles ou les éléments de $\mathbb{A}$ associés à p) ;
- qu'un élément p d'un anneau commutatif, unitaire et intègre $\mathbb{A}$, est premier si $p \neq 0$, p n'est pas inversible et :

$$(p \text{ divise } uv) \Rightarrow (p \text{ divise } u \text{ ou } p \text{ divise } v)$$

Pour ce problème :
- $\mathbb{A}$ est un anneau intègre ;
- 0 et 1 sont les éléments neutres pour l'addition et la multiplication de $\mathbb{A}$, avec $0 \neq 1$;
- $\mathbb{A}^* = \mathbb{A} \setminus \{0\}$;
- $\mathbb{A}^\times$ est le groupe des éléments inversibles de $\mathbb{A}$;

On appelle stathme sur A une application $\varphi : \mathbb{A}^* \to \mathbb{N}$.

On dit que l'anneau $\mathbb{A}$ est euclidien, s'il existe un stathme φ sur $\mathbb{A}$ tel que pour tout couple (a, b) d'éléments de $\mathbb{A}$ avec $b \neq 0$, il existe un couple (q, r) dans $\mathbb{A}^2$ tel que :

$$a = bq + r \text{ avec } r = 0 \text{ ou } r \neq 0 \text{ et } \varphi(r) < \varphi(b)$$

Dans ces conditions, on dit que q est un quotient et r un reste dans la division euclidienne de a par b.

On notera $(\mathbb{A}, \varphi)$ un tel anneau euclidien.

– I – Généralités sur les anneaux euclidiens

1. Soit $(\mathbb{A}, \varphi)$ un anneau euclidien. Montrer que si le stathme φ est constant, $\mathbb{A}$ est alors un corps.
2. Montrer qu'un anneau euclidien est principal.
3. L'anneau $\mathbb{Z}[X]$ est-il euclidien ?
4. Soit $\mathbb{A}$ un anneau commutatif, unitaire et intègre qui n'est pas un corps. L'anneau $\mathbb{A}[X]$ est-il euclidien ?
5. Soit $\mathbb{A}$ un anneau principal. Montrer qu'un élément a de $\mathbb{A}$ est irréductible si, et seulement si, il est premier.
6. Étant donné un anneau euclidien $(\mathbb{A}, \varphi)$, on définit l'application $\overline{\varphi} : \mathbb{A}^* \to \mathbb{N}$ par :

$$\forall a \in \mathbb{A}^*,\ \overline{\varphi}(a) = \min_{x \in \mathbb{A}^*} \varphi(ax)$$

(a) Montrer que $\overline{\varphi}$ est bien définie et que :

$$\forall (a,b) \in \mathbb{A}^* \times \mathbb{A}^*,\ \overline{\varphi}(ab) \geq \overline{\varphi}(a)$$

Cette propriété se traduit en disant que le stathme $\overline{\varphi}$ est croissant dans le sens où : si a, c dans $\mathbb{A}^*$ sont tels que a divise c, on a alors $\overline{\varphi}(a) \leq \overline{\varphi}(c)$.

(b) Montrer que $(\mathbb{A}, \overline{\varphi})$ est un anneau euclidien.

7. Pour cette question, on suppose que $(\mathbb{A}, \varphi)$ est un anneau euclidien, que le stathme φ est croissant, c'est-à-dire que :

$$\forall (a,b) \in \mathbb{A}^* \times \mathbb{A}^*,\ \varphi(ab) \geq \varphi(a)$$

et on s'intéresse à quelques conséquences de la croissance de φ.

(a) Montrer que pour tout $(a,b) \in \mathbb{A}^* \times \mathbb{A}^*$, on a $\varphi(ab) \geq \varphi(a)$, l'égalité étant réalisée si, et seulement si, b est inversible.
En particulier, on a $\varphi(-a) = \varphi(a)$ et $\varphi(ab) > \varphi(a)$ pour a, b non nuls avec b non inversible.

(b) Montrer que, pour tout $a \in \mathbb{A}^*$, on a :

$$\varphi(a) = \min_{x \in \mathbb{A}^*} \varphi(ax)$$

En particulier, on a :

$$\varphi(1) = \min_{x \in \mathbb{A}^*} \varphi(x)$$

(c) Montrer que :

$$\mathbb{A}^\times = \{a \in \mathbb{A}^* \mid \varphi(a) = \varphi(1)\}$$

8. On peut montrer, mais ce n'est pas élémentaire (voir le problème de Frédéric Dupré), qu'un anneau principal est factoriel et en conséquence il en est de même pour une anneau euclidien. La démonstration directe du fait qu'un anneau euclidien est factoriel est plus simple.
Précisément, étant donné un anneau euclidien $(\mathbb{A}, \varphi)$, montrer que :

(a) un élément non nul de $\mathbb{A}$ est soit inversible soit un produit fini d'éléments irréductibles ;

(b) si $a \in \mathbb{A}^* \setminus \mathbb{A}^\times$ s'écrit de deux manières :

$$a = \prod_{k=1}^{r} p_k = \prod_{j=1}^{s} q_j$$

où les p_k et q_j sont des éléments irréductibles de $\mathbb{A}$, on a alors $r = s$, chaque p_k est associé à un q_j et réciproquement.

– II – Exemples d'anneaux euclidiens

1.

(a) Soit α un réel. Montrer que pour tout couple d'entiers (a,b), avec $b \neq 0$, il existe un unique couple d'entiers (q,r) tel que $a = bq + r$ et $\alpha \leq r < \alpha + |b|$.

(b) Montrer que l'anneau $\mathbb{Z}$ des entiers relatifs est euclidien pour le stathme $\varphi : n \in \mathbb{Z}^* \mapsto |n|$.

(c) Soient $a \in \mathbb{Z}^*$ et $b \in \mathbb{N}^*$ ne divisant pas a.

i. Montrer que si $a = bq + r$ est une division euclidienne de a par b dans $(\mathbb{Z}, |\cdot|)$, il en existe une autre, et une seule, $a = bq' + r'$ avec $r \neq r'$ et $q \neq q'$.

ii. Montrer qu'il y a exactement deux divisions euclidiennes de a par b dans $(\mathbb{Z}, |\cdot|)$.

2. Montrer que l'anneau $\mathbb{K}[X]$ des polynômes à une indéterminée et à coefficients dans un corps commutatif $\mathbb{K}$ est euclidien pour le stathme deg : $P \in \mathbb{K}[X] \setminus \{0\} \mapsto \deg(P)$. A-t-on unicité du quotient et du reste pour la division euclidienne dans $(\mathbb{K}[X], \deg)$?

3. Soit $\mathbb{A}$ un anneau commutatif, unitaire et intègre. Montrer qu'on a les équivalences :

$$(\mathbb{A}[X] \text{ est euclidien}) \Leftrightarrow (\mathbb{A}[X] \text{ est principal}) \Leftrightarrow (\mathbb{A} \text{ est un corps})$$

4. Soit :

$$\mathbb{D} = \left\{ \frac{a}{10^m} \mid (a, m) \in \mathbb{Z} \times \mathbb{N} \right\}$$

l'anneau des nombres décimaux (on vérifie facilement que c'est un sous-anneau de $\mathbb{D}$).

(a) Montrer que tout nombre décimal non nul s'écrit de manière unique sous la forme $d = n2^p5^q$, où n, p, q sont des entiers relatifs avec $n \neq 0$ premier avec 10.
Une telle écriture d'un nombre décimale est appelée écriture canonique.

(b) Montrer que $\mathbb{D}$ est euclidien pour le stathme φ défini, en utilisant l'écriture canonique d'un nombre décimal, par :

$$\forall a = n2^p5^q \in \mathbb{D}^*,\ \varphi(a) = |n|$$

(c) A-t-on unicité du quotient et du reste pour la division euclidienne dans $(\mathbb{D}, \varphi)$?

5. On se donne un entier naturel $n \geq 1$ et on note :

$$\mathbb{Z}\left[i\sqrt{n}\right] = \mathbb{Z} + i\sqrt{n}\mathbb{Z} = \left\{a + ib\sqrt{n} \mid (a, b) \in \mathbb{Z}^2\right\}$$

Pour $n = 1$, il s'agit de l'ensemble $\mathbb{Z}[i]$ des entiers de Gauss.

(a) Montrer que $\mathbb{Z}[i\sqrt{n}]$ est un sous anneau de $\mathbb{C}$ stable par l'opération de conjugaison complexe.

(b) Déterminer l'ensemble $\mathbb{Z}[i\sqrt{n}]^\times$ des éléments inversibles de $\mathbb{Z}[i\sqrt{n}]$.

(c) Soient u, v dans $\mathbb{Z}[i\sqrt{n}]$ avec $v \neq 0$ et $(x, y) \in \mathbb{Q}^2$ tel que $\dfrac{u}{v} = x + iy\sqrt{n}$.

i. Montrer qu'il existe un unique couple (a, b) d'entiers relatifs tel que :

$$(x, y) \in \left[a - \frac{1}{2}, a + \frac{1}{2}\right[\times \left[b - \frac{1}{2}, b + \frac{1}{2}\right[$$

ii. En déduire qu'il existe $q \in \mathbb{Z}[i\sqrt{n}]$ tel que $|u - qv| \leq \dfrac{\sqrt{n+1}}{2}|v|$.

(d) Montrer que, pour $n = 1$ ou $n = 2$, l'anneau $\mathbb{Z}[i\sqrt{n}]$ est euclidien pour le stathme :

$$\varphi : u = a + ib\sqrt{n} \in \mathbb{Z}\left[i\sqrt{n}\right] \mapsto |u|^2 = a^2 + nb^2 \in \mathbb{N}$$

(le stathme est aussi défini en 0).

(e) A-t-on unicité du quotient et du reste pour la division euclidienne dans $(\mathbb{Z}[i], \varphi)$?

(f) Effectuer la division euclidienne de $u = 11 + 7i$ par $v = 18 - i$ dans $\mathbb{Z}[i]$.

6. On utilise les notations de **II.5** avec $n \geq 3$.

(a) Montrer que $i\sqrt{n}$, est irréductible dans $\mathbb{Z}[i\sqrt{n}]$.

(b) On suppose que n est pair, soit que $n = 2m$ avec $m \geq 2$. Montrer que $i\sqrt{n}$ divise $2\left(m + i\sqrt{n}\right)$ et en déduire que $\mathbb{Z}\left[i\sqrt{n}\right]$ n'est pas euclidien.

(c) Montrer que 2 est irréductible dans $\mathbb{Z}\left[i\sqrt{n}\right]$.

(d) On suppose que n est impair, soit que $n = 2m + 1$ avec $m \geq 1$. En utilisant le fait que 2 divise $1 + n$, montrer que $\mathbb{Z}\left[i\sqrt{n}\right]$ n'est pas euclidien.

7. Soient $\omega = x + iy$ un nombre complexe non réel (i. e. avec $x \in \mathbb{R}$ et $y \in \mathbb{R}^*$) et :

$$\mathbb{Z}[\omega] = \mathbb{Z} + \mathbb{Z}\omega = \left\{a + b\omega \mid (a, b) \in \mathbb{Z}^2\right\}$$

(a) Montrer que $\mathbb{Z}[\omega]$ est un anneau si, et seulement si, ω est un entier quadratique, c'est-à-dire racine d'un polynôme de degré 2, $P(X) = X^2 - \alpha X - \beta$ à coefficients entiers.
Dans ce cas, montrer que $\mathbb{Z}[\omega]$ est stable par l'opération de conjugaison complexe $z \mapsto \overline{z}$, que l'application $\varphi : u \mapsto |u|^2$ définit un stathme sur $\mathbb{Z}[\omega]$, que $\mathbb{Z}[\omega] = \mathbb{Z}[\overline{\omega}]$, que pour tout entier relatif n, on a $\mathbb{Z}[\omega] = \mathbb{Z}[n + \omega]$ et qu'il existe un nombre complexe $\omega' = x' + iy'$ tel que $x' \in [0, 1[$, $y' > 0$ et $\mathbb{Z}[\omega] = \mathbb{Z}[\omega']$.
Pour la suite de cette question, on suppose que $\omega = x + iy$ est un entier quadratique avec $x \in [0, 1[$, $y > 0$.

(b) Montrer que l'on soit $\omega = i\sqrt{n}$, soit $\omega = \dfrac{1}{2} + i\dfrac{\sqrt{4n-1}}{2}$ où $n \in \mathbb{N}^*$.

(c) Soient u, v dans $\mathbb{Z}[\omega]$ avec $v \neq 0$.

i. Montrer qu'il existe $(r, s) \in \mathbb{Q}^2$ tel que $\dfrac{u}{v} = r + s\omega$.

ii. Montrer qu'il existe $q \in \mathbb{Z}[\omega]$ tel que $|u - qv|^2 \leq \dfrac{1 + y^2}{4}|v|^2$.

(d) Montrer que, pour $x \in [0, 1[$ et $y \in \left]0, \sqrt{3}\right[$, l'anneau $\mathbb{Z}[\omega]$ est euclidien pour le stathme :

$$\varphi : u = a + b\omega \in \mathbb{Z}[\omega] \mapsto |u|^2$$

Préciser les valeurs possibles de ω, sont $\omega = i\sqrt{n}$, ou $n = \dfrac{1}{2} + i\dfrac{\sqrt{4n-1}}{2}$ avec $n \in \mathbb{N}^*$.

– III – Anneaux euclidiens pour lesquels il y a unicité de la division

Pour cette partie, $(\mathbb{A}, \varphi)$ est un anneau euclidien.

1. Montrer que le quotient et le reste sont uniquement déterminés pour la division euclidienne dans $(\mathbb{A}, \varphi)$ si, et seulement si, le stathme φ est tel que :

$$\forall (a, b) \in \mathbb{A}^* \times \mathbb{A}^*,\ \varphi(ab) \geq \varphi(a) \tag{1}$$

et :

$$\forall (a, b) \in \mathbb{A}^* \times \mathbb{A}^*,\ a \neq b \Rightarrow \varphi(a - b) \leq \max(\varphi(a), \varphi(b)) \tag{2}$$

La propriété (1) est vérifiée pour les exemples classiques d'anneaux euclidiens : $\mathbb{K}[X]$, $\mathbb{Z}$, $\mathbb{D}$ et $\mathbb{Z}[i]$ (question **III.2**).
En fait, on peut toujours se ramener à un stathme croissant (question **I.6**), ce qui est intéressant pour caractériser les éléments inversibles de $\mathbb{A}$ (question **I.7c**) et montrer facilement qu'un anneau euclidien est factoriel (question **I.8**).

2. Les propriétés (1) et (2) sont-elles vérifiées pour $\varphi = \deg$ sur $\mathbb{K}[X]$? pour $|\cdot|$ sur $\mathbb{Z}$? pour φ défini en **II.4b** sur $\mathbb{D}$? pour φ défini en **II.5d** sur $\mathbb{Z}[i]$?

   On suppose, pour la suite de cette partie que le quotient et le reste sont uniquement déterminés pour la division euclidienne dans $(\mathbb{A}, \varphi)$, c'est-à-dire que :

$$\forall (a,b) \in \mathbb{A} \times \mathbb{A}^*,\ \exists ! (q,r) \in \mathbb{A}^2 \mid a = bq + r \text{ avec } r = 0 \text{ ou } r \neq 0 \text{ et } \varphi(r) < \varphi(b)$$

   ce qui équivaut à dire que les propriétés (1) **et** (2) **sont vérifiées.**

3. Montrer que $\mathbb{K} = \mathbb{A}^\times \cup \{0\}$ est un corps. On en déduit alors que $\mathbb{A}$ est un $\mathbb{K}$-espace vectoriel.

4. Soient $a \neq b$ dans $\mathbb{A}^*$. Montrer que si $\varphi(a) < \varphi(b)$, on a alors $\varphi(b-a) = \varphi(b)$.

   On suppose maintenant que A n'est pas un corps. On a donc $\mathbb{K} \subsetneqq \mathbb{A}$ et il existe $x \in \mathbb{A} \setminus \mathbb{K}$ tel que :

$$\varphi(x) = \min_{y \in \mathbb{A} \setminus \mathbb{K}} \varphi(y)$$

5.

   (a) Montrer que $\varphi(x) > \varphi(1)$.

   (b) Montrer que la suite $(\varphi(x^n))_{n \in \mathbb{N}}$ est strictement croissante dans $\mathbb{N}$.

   (c) Montrer que la famille $\mathcal{B}_x = (x^n)_{n \in \mathbb{N}}$ est libre dans le $\mathbb{K}$-espace vectoriel $\mathbb{A}$.

   (d) Montrer que pour tout $a \in \mathbb{A}^*$, il existe un unique entier naturel n tel que $\varphi(a) = \varphi(x^n)$.

   (e) Montrer que $\mathcal{B}_x$ est une base de $\mathbb{A}$, c'est-à-dire que pour tout $a \in \mathbb{A}$, il existe un unique entier naturel n et une unique suite $(a_k)_{0 \leq k \leq n}$ d'éléments de $\mathbb{K}$ telle que $a = \sum_{k=0}^{n} a_k x^k$, les a_k étant dans $\mathbb{K}$ avec $a_n \in \mathbb{A}^\times$. Ce que l'on peut noter $\mathbb{A} = \mathbb{K}[x]$.

   (f) En déduire que l'anneau $\mathbb{A}$ est isomorphe à l'anneau $\mathbb{K}[X]$ des polynômes à une indéterminée et à coefficients dans le corps commutatif $\mathbb{K}$.