L3 Mathématiques – Site Nancy, S5 – 2022-2023

Algèbre 2 – Feuille 6

Anneaux euclidiens, principaux, factoriels

Exercice 1. Le but de cet exercice est de donner un exemple d'un anneau non euclidien mais principal (contre-exemple à la réciproque de l'implication euclidien ⇒ principal).

1. Soit A un anneau euclidien et soit θ un stathme euclidien de A (ie, $\forall z, w \in A$ avec $w \neq 0$, il existe $q, r \in A$ tels que $z = wq + r$ et $\theta(r) < \theta(w)$).
   (a) Montrer que θ' défini par $\theta'(x) = \min\{\theta(xu) \,|\, u \in A^\times\}$ munit A d'un nouveau stathme euclidien.
   (b) Montrer qu'on a $\forall x \in A, \forall u \in A^\times, \theta'(x) = \theta'(xu)$.
   (c) Montrer que si $u \in A^\times$, alors $\theta'(u) = \theta'(1)$. On note $n_{\mathrm{inv}} = \theta'(1)$.
   (d) Montrer que pour $x \in A$, on a l'implication $\theta'(x) < n_{\mathrm{inv}} \Longrightarrow x = 0$.
   (On pourra considérer x non nul tel que $\theta'(x) = \min\{\theta'(y) \,|\, y \in A \setminus \{0\}\}$, et utiliser la division euclidienne de 1 par x pour montrer que x est inversible).
   (e) Montrer qu'il existe $x \in A$ non inversible, tel que la restriction de la projection canonique $p : A \to A/xA$ à $A^\times \cup \{0\}$ soit surjective.
   (f) Etant donné un anneau A et une fonction $\theta : A \to \mathbb{N}$, le critère de Dedekind-Hasse est la condition suivante : soient $z, w \in A$ tels que $w \neq 0$ et $\theta(z) \geq \theta(w)$. Alors, soit w divise z, soit il existe $p, q, r \in \mathbb{Z}[\alpha]$ tels que
   $$pz - qw = r \neq 0 \text{ et } \theta(r) < \theta(w)\,.$$
   Montrer que si θ est un stathme euclidien, alors ce critère est vérifié.
   (g) Montrer qu'un anneau intègre muni d'une fonction $\theta : A \to \mathbb{N}$ satisfaisant le critère de Dedkind-Hasse est principal (on pourra s'inspirer de la preuve donnée en cours dans le cas euclidien).
2. On pose $\alpha = \frac{1+i\sqrt{19}}{2}$ et on considère l'ensemble $\mathbb{Z}[\alpha] = \{a + b\alpha;\ a, b \in \mathbb{Z}\}$. On montre dans cette question que $\mathbb{Z}[\alpha]$ n'est pas un anneau euclidien.
   (a) Montrer que $\mathbb{Z}[\alpha]$ est un sous-anneau de $\mathbb{C}$.
   (b) On note pour tout $z \in \mathbb{Z}[\alpha]$, $\theta(z) = z\bar{z} = |z|^2$.
   Calculer $\theta(a + b\alpha)$. Montrer que si $z \in \mathbb{Z}[\alpha]$ n'est pas réel, alors $\theta(z) \geq 5$.
   (c) En utilisant θ, montrer que $\mathbb{Z}[\alpha]^\times = \{\pm 1\}$.
   (d) En utilisant θ, montrer que 2 et 3 sont irréductibles dans $\mathbb{Z}[\alpha]$.
   (e) En utilisant la question (1e), montrer que l'anneau $\mathbb{Z}[\alpha]$ n'est pas euclidien.
3. On montre maintenant que $\mathbb{Z}[\alpha]$ est un anneau principal.
   (a) Montrer que le critère de Dedekind-Hasse pour A muni de θ est impliqué par la condition : soit $z, w \in \mathbb{Z}[\alpha]$ tels que $0 < \theta(w) < \theta(z)$. Alors, soit w divise z, soit il existe $p, q \in \mathbb{Z}[\alpha]$ tels que $0 < \theta(pz/w - q) < 1$.
   (b) Soient $z, w \in \mathbb{Z}[\alpha]$ tels que $w \neq 0$. Montrer qu'il existe $a, b \in \mathbb{Q}$ tels que $z/w = a + b\alpha$.
   Pour x un rationnel, on note $[x]$ sa partie entière, et $\{x\}$ l'entier le plus proche de x (avec la convention $\{n + 1/2\} = n$). Pour $z = a + b\alpha \in \mathbb{Q}[\alpha]$, on note $\{z\} = \{a\} + \{b\}\alpha$.
   (c) On montre maintenant le critère de la question (3)(a) dans tous les cas :
      i. Lorsque $b \in \mathbb{Z}$, montrer que le critère est satisfait avec $p = 1$ et $q = \{pz/w\}$.
      ii. Lorsque $a \in \mathbb{Z}$ et $5b \notin \mathbb{Z}$, montrer que le critère est satisfait avec $p = \overline{\alpha}$ et $q = \{pz/w\}$.

iii. Lorsque $a \in \mathbb{Z}$ et $5b \in \mathbb{Z}$, montrer que le critère est satisfait avec $p = 1$ et $q = \{pz/w\}$ (observer que $|b - \{b\}| \leq 2/5$).
iv. Lorsque $a, b \notin \mathbb{Z}$ et $2a, 2b \in \mathbb{Z}$, montrer que le critère est satisfait avec $p = \alpha$ et $q = \{pz/w\}$.
v. Montrer que le critère est satisfait avec $p = 1$ et $q = \{pz/w\}$ lorsque $b \notin [[b] + 1/3, [b] + 2/3]$.
vi. Montrer que le critère est satisfait avec $p = 2$ et $q = \{pz/w\}$ lorsque $b \in [[b] + 1/3, [b] + 2/3]$ et $2a \notin \mathbb{Z}$ ou $2b \notin \mathbb{Z}$.
vii. Montrer que le critère de Dedekind-Hasse est toujours satisfait.

(d) Montrer que $\mathbb{Z}[\alpha]$ est un anneau principal.

Solution : (1)(a) Il s'agit de montrer que pour tout a, b de A avec b non nul, il existe $q, r \in A$ tels que $a = bq + r$ et $\theta'(r) < \theta'(b)$. Soit d'abord $u \in A^\times$ tel que $\theta(bu) = \theta'(b)$. Soit ensuite q et r un quotient et un reste de la division de a par bu pour θ : $a = buq + r$ et $\theta(r) < \theta(bu)$. Alors on a $\theta'(r) \leq \theta(r) < \theta'(b)$, de sorte que $q' = qu$ et $r' = r$ sont un quotient et un reste de la division de a par b pour le stathme θ'.

(1)(b) Soit $x \in A$ et $u \in A^\times$. On a

$$\theta'(x) = \min\{\theta(xv) \,|\, v \in A^\times\} \text{ et } \theta'(xu) = \min\{\theta(xuv) \,|\, v \in A^\times\}$$

Or, l'application $v \mapsto uv$ réalise une bijection de $A^\times$ dans lui-même, de bijection réciproque $v \mapsto u^{-1}v$, de sorte que l'ensemble des uv dans la deuxième égalité est l'ensemble $A^\times$, donc on en déduit que $\theta'(x) = \theta'(xu)$.

(1)(c) On applique la question précédente à $x = 1$ et $u \in A^\times$: on obtient $\theta'(1) = \theta'(1u) = \theta'(u)$.

(1)(d) Soit x non nul tel que $\theta'(x) = \min\{\theta'(y) \,|\, y \in A \setminus \{0\}\}$, Soit q et r le quotient et le reste de la division euclidienne de 1 par x : $1 = qx + r$ avec $\theta'(r) < \theta'(x)$. Or, par le choix de x, ceci implique que $r = 0$. On a donc $1 = qx$, donc x est inversible (d'inverse q). On a donc $\theta'(x) = n_{\text{inv}}$ et, par définition de x encore, on a l'implication $\theta'(y) < n_{\text{inv}} \implies y = 0$.

(1)(e) On prend x tel que $\theta'(x) = \min\{\theta'(y) \,|\, y \notin A^\times \text{ et } y \neq 0\}$. Soit $p : A \to A/xA$. Montrons que tout élément de A/xA admet un antécédent dans $A^\times \cup \{0\}$. Soit donc $\beta \in A/xA$ quelconque et $y \in A$ tel que $\overline{y} = \beta$. Soit q et r le quotient et le reste de la division euclidienne de y par x : $y = qx + r$ avec $\theta'(r) < \theta'(x)$. La définition de x implique que $r \in A^\times$ ou $r = 0$. De plus, on a $\overline{y} = \overline{r}$, donc $p(r) = \beta$, montrant la surjectivité voulue.

(1)(f) Soit $z, w \in A$ avec $w \neq 0$. Supposons que w ne divise pas z et montrons qu'il existe $p, q, r \in A$ tels que $0 \neq r = pz + qw$ et $\theta(r) < \theta(w)$ (si $w|z$ il n'y a rien à montrer). Soit q et r le quotient et le reste de la division euclidienne de z par w : on a $z = qw + r$ et $\theta(r) < \theta(w)$. De plus, r ne peut pas être nul car sinon $z = qw$ donc w divise z. Ainsi, en posant $p = 1$, le triplet (p, q, r) convient.

(1)(g) Il s'agit de montrer que tout idéal est principal. Soit donc $I \subset A$ un idéal. Si $I = \{0\}$, alors $I = 0A$ est principal. Sinon, soit x un élément de I tel que $\theta(x) = \min\{\theta(y) \,|\, y \in I, y \neq 0\}$. Montrons que $I = xA$. On a $I \supset xA$ car $x \in I$ et I est un idéal. Réciproquement, soit $y \in I$. On a donc deux cas possibles, par la condition de Dedekind-Hasse : soit $x|y$, soit il existe $p, q, r \in A$ avec $r = px + qy$, $r \neq 0$, et $\theta(r) < \theta(x)$. Par définition de x, cette deuxième alternative est impossible (on ne peut avoir $r \neq 0$ et $\theta(r) < \theta(x)$). C'est donc la première alternative qui se produit, donc $x|y$.

Attention : certains étudiants écrivent que dans la deuxième alternative, $r = 0$ donc $px + qy = 0$ donc $-qy = px$ donc y divise x, mais c'est faux car on a seulement y divise px dans ce cas de figure.

(2)(a) Il s'agit de montrer que $\mathbb{Z}[\alpha]$ est un sous-groupe de $\mathbb{C}$, ce que je ne détaille pas, et que $\mathbb{Z}[\alpha]$ est stable par produits. Soit donc $a + b\alpha, c + d\alpha$ deux éléments de $\mathbb{Z}[\alpha]$. Alors

$$(a + b\alpha)(c + d\alpha) = ac + (ad + bc)\alpha + bd(\alpha - 5) = (ac - 5bd) + (ad + bc)\alpha\,,$$

la première égalité résultant de l'égalité $\alpha^2 = \alpha - 5$. On en déduit que ce produit est bien dans $\mathbb{Z}[\alpha]$.

(2)(b) On a $a + b\alpha = (a + \frac{b}{2}) + bi\frac{i\sqrt{19}}{2}$, donc

$$\theta(a + b\alpha) = (a + \frac{b}{2})^2 + \frac{19}{4}b^2 = a^2 + ab + 5b^2 \tag{1}$$

Si $z = a + b\alpha$ n'est pas réel, alors $b \neq 0$, donc $\theta(z) \geq \frac{19}{4}b^2 \geq \frac{19}{4}$. Puisque, de plus, $\theta(z)$ est entier, alors $N(z) \geq 5$.

(2)(c) On a clairement $\{-1, 1\} \subset A^\times$. Réciproquement, soit $x \in A^\times$, et donc $y \in A$ tel que $xy = 1$. On a alors $1 = \theta(1) = \theta(xy) = \theta(x)\theta(y)$. Or $\theta(x), \theta(y) \in \mathbb{N}$, donc $\theta(x) = \theta(y) = 1$. La deuxième partie de la question (2b) implique alors que x et y sont réels, donc entiers relatifs, et donc dans $\mathbb{Z}^\times = \{-1, 1\}$.

(2)(d) Ecrivons $2 = xy$ et montrons que $x \in A^\times$ ou $y \in A^\times$. On a alors $4 = \theta(2) = \theta(xy) = \theta(x)\theta(y)$. De nouveau, l'inégalité de la question (2b) implique que x et y sont réels, donc entiers relatifs. Comme 2 est un nombre premier, ceci implique que $x = \pm 1$ ou $y = \pm 1$. La démonstration de l'irréductibilité de 3 est exactement identique.

(2)(e) Si $\mathbb{Z}[\alpha]$ est euclidien, soit x comme à la question (1)(e). Alors $p(2) \in \{p(-1), p(0), p(1)\}$. Donc x divise 1, 2, ou 3. Comme x n'est pas inversible, et que 2 et 3 sont irréductibles, $x = \pm 2$ ou $x = \pm 3$. Mais x doit aussi diviser $\alpha, \alpha - 1$, ou $\alpha + 1$, ce qui produit une contradiction.

Voici un autre argument possible (trouvé dans des copies d'étudiants). On pose de nouveau x comme à la question (1)(e). Comme $A^\times = \{-1, 1\}$, la définition de x implique que la restriction de p à $\{-1, 0, 1\}$, de cardinal 3, est surjective. Donc $|A/xA| \leq 3$. De plus, puisque $A^\times$ est par définition constitué d'éléments inversibles, $p(A^\times \cup \{0\})$ est un corps. Ainsi, A/xA est un corps à deux ou trois éléments, soit donc $\mathbb{Z}/2\mathbb{Z}$ ou $\mathbb{Z}/3\mathbb{Z}$. De plus, il contient $\overline{\alpha}$, qui vérifie l'équation $\overline{\alpha}^2 = \overline{\alpha} - 5$. On trouve alors une contradiction en observant que $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$ ne contiennent pas d'élément x tel que $x^2 = x - 5$.

(3)(a) Supposons que A vérifie la condition de l'énoncé, et vérifions le critère de Dedekind-Hasse. Soit $z, w \in A$. Si $w|z$, il n'y a rien à montrer. Sinon, soit p, q tels que $0 < \theta(pz/w - q) < 1$. En multipliant par w, on obtient $0 < \theta(pz - qw) < \theta(w)$. Ainsi, $pz - qw \neq 0$, et on a bien $\theta(pz - qw) < \theta(w)$.

(3)(b) Soit $z = a + b\alpha$ et $w = c + d\alpha$ avec $w \neq 0$. On multiplie numérateur et dénominateur de $\frac{z}{w}$ par la quantité conjuguée pour faire apparaître une fraction avec un dénominateur entier. Plus précisément, puisque $\overline{\alpha} = 1 - \alpha$, on a

$$\frac{a + b\alpha}{c + d\alpha} = \frac{(a + b\alpha)(c + d\overline{\alpha})}{(c + d\alpha)(c + d\overline{\alpha})} = \frac{(a + b\alpha)(c + d(1 - \alpha))}{\theta(c + d\alpha)}.$$

Le numérateur de cette fraction est clairement dans $\mathbb{Z}[\alpha]$, et le dénominateur est un entier (non nul), donc ce quotient est bien dans $\mathbb{Q}[\alpha]$.

(3)(c) On adopte dans tous les cas la notation $\frac{pz}{w} = a + b\alpha$, avec $a, b \in \mathbb{Q}$ d'après la question précédente.

(i) Dans ce cas, b est entier, de sorte que $\frac{pz}{w} - q = a - \{a\}$. Si a est aussi entier, $\frac{z}{w}$ est dans $\mathbb{Z}[\alpha]$, donc w divise z. S'il n'est pas entier, $0 < \theta(\frac{pz}{w} - q) \leq (\frac{1}{2})^2 < 1$.

(ii) $(a+b\alpha)\overline{\alpha} = a(-\alpha+1)+5b = (a+5b) - a\alpha$. Dans ce cas, $\theta(\frac{pz}{w} - q) = (5b - \{5b\})^2 \leq \frac{1}{4}$ (et $(5b - \{5b\} \neq 0)$.

(iii) Dans ce cas, $\theta(\frac{pz}{w} - q) = 5(b - \{b\})^2 \leq 5\frac{4}{25} < 1$.

(iv) On a dans ce cas $(a + b\alpha)\alpha = -5b + (a + b)\alpha$, avec $a + b \in \mathbb{Z}$ et $-5b \notin \mathbb{Z}$. Donc $\theta(\frac{pz}{w} - q) = (\frac{1}{2})^2$.

(v) Alors $\theta((a - \{a\}) + (b - \{b\})\alpha) = (a - \{a\})^2 + (a - \{a\})(b - \{b\}) + 5(b - \{b\})^2 \leq 1/4 + 1/6 + 5/9 = 35/36$, en utilisant (1) et $|b - \{b\}| \leq \frac{1}{3}$.

(vi) Dans ce cas $2z/w$ vérifie la condition précédente.

(vii) Les points (i) à (iii) traitent tous les cas avec $a \in \mathbb{Z}$ ou $b \in \mathbb{Z}$. On peut donc supposer que ni a ni b ne sont entiers. Les cas (v) et (vi) traitent tous les cas, sauf si a et b sont tous les deux des demi-entiers, cas traité par (iv).

(3)(d) Dans la question (3)(c), on a montré le critère de la question (3)(a). Cette question montre que le critère de Dedekind-Hasse est vérifié par $\mathbb{Z}[\alpha]$. Par la question (1)(g), $\mathbb{Z}[\alpha]$ est donc principal.