Agrégation Externe et Interne

Anneaux principaux

[1]Ce problème est en relation avec les leçons d'oral suivante :
– 122 : Anneaux principaux. Applications ;

On pourra consulter les ouvrages suivants.

P. Boyer, J. J. Risler : *Algèbre pour la licence 3. Groupes, anneaux, corps.* Dunod (2006).

F. Combes — *Algèbre et géométrie.* Bréal (2003).

S. Francinou, H. Gianella, S. Nicolas : *Exercices de mathématiques. Oraux X-ENS. Algèbre 1.* Cassini (2001).

S. Francinou, H. Gianella. *Exercices de mathématiques pour l'agrégation. Algèbre 1.* Masson (1994).

D. Perrin. *Cours d'algèbre.* Ellipses (1996).

A. Szpirglas. *Mathématiques L3. Algèbre.* Pearson (2009).

1. Le 05/10/2013

1 Énoncé

Pour ce problème, $\mathbb{A}$ désigne un anneau commutatif, unitaire, intègre et on note :
– 0 et 1 les éléments neutres pour l'addition et la multiplication de $\mathbb{A}$, avec $0 \neq 1$;
– $\mathbb{A}^* = \mathbb{A} \setminus \{0\}$ l'ensemble des éléments non nuls de $\mathbb{A}$;
– $\mathbb{A}^\times$ le groupe multiplicatif des éléments inversibles (ou des unités) de $\mathbb{A}$.

– I – Anneaux principaux

1. Soit $\mathbb{A}$ un anneau principal.
   (a) Montrer qu'un élément $p \in \mathbb{A}^* \setminus \mathbb{A}^\times$ est irréductible si, et seulement si, il est premier.
   (b) Montrer que, pour tout $p \in \mathbb{A}^* \setminus \mathbb{A}^\times$, on a :
   $$((p) \text{ premier}) \Leftrightarrow (p \text{ premier}) \Leftrightarrow (p \text{ irréductible}) \Leftrightarrow ((p) \text{ maximal})$$
2. Montrer que, pour $n \geq 3$, l'anneau $\mathbb{Z}[i\sqrt{n}]$ n'est pas principal.
3. Soient $\mathbb{A}$ un anneau principal et $I = (a)$ un idéal non trivial de $\mathbb{A}$ (i. e. $I \neq \{0\}$ et $I \neq \mathbb{A}$). Montrer que tous les idéaux de $\dfrac{\mathbb{A}}{I}$ sont principaux de la forme $\left(\overline{b}\right)$ où $b \in \mathbb{A}$ est un diviseur de a.
   L'anneau $\dfrac{\mathbb{A}}{I}$ est-il principal ?
4. On désigne par $\mathbb{K}[[X]]$ l'anneau des séries formelles à une indéterminée et à coefficients dans un corps commutatif $\mathbb{K}$.
   (a) Soient $S = \sum_{n\in\mathbb{N}} a_n X^n$ et $T = \sum_{n\in\mathbb{N}} b_n X^n$ deux séries formelles avec $\mathrm{val}(T) = 0$ (soit $b_0 \neq 0_\mathbb{K}$). Montrer que, pour tout entier naturel n, il existe un unique couple $(Q_n, R_n) \in \mathbb{K}_n[X] \times \mathbb{K}[[X]]$ tel que $S = TQ_n + X^{n+1}R_n$.
   (b) Montrer que $(\mathbb{K}[[X]])^\times = \mathbb{K}[[X]] \setminus (X)$.
   (c) Montrer que les idéaux non réduit à $\{0\}$ de $\mathbb{K}[[X]]$ sont de la forme $(X^n) = X^n \cdot \mathbb{K}[[X]]$. Donc $\mathbb{K}[[X]]$ est principal.
5. On se donne deux réels $a < b$ et $\mathbb{A} = \mathcal{C}^0([a,b], \mathbb{R})$ est l'anneau des fonctions continues de $[a,b]$ dans $\mathbb{R}$.
   (a) L'anneau $\mathbb{A}$ est-il intègre ?
   (b) Montrer que, pour tout réel $x \in [a,b]$ l'ensemble :
   $$I_x = \{f \in \mathbb{A} \mid f(x) = 0\}$$
   est un idéal maximal de $\mathbb{A}$.
   (c) Montrer que les idéaux I_x ne sont pas principaux.

– II – Anneaux euclidiens

Définition 1 *On appelle stathme sur $\mathbb{A}$ une application $\varphi : \mathbb{A}^* \to \mathbb{N}$.*

Définition 2 *On dit que l'anneau $\mathbb{A}$ est euclidien, s'il est intègre et s'il existe un stathme φ sur $\mathbb{A}$ tel que pour tout couple (a,b) d'éléments de $\mathbb{A} \times \mathbb{A}^*$, il existe un couple (q,r) dans $\mathbb{A}^2$ tel que :*
$$a = bq + r \text{ avec } r = 0 \text{ ou } r \neq 0 \text{ et } \varphi(r) < \varphi(b)$$

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

1. Montrer qu'un anneau euclidien est principal.
2. **L'anneau** $(\mathbb{Z}, |\cdot|)$.

   (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 $\alpha \leq r < \alpha + |b|$.
   Pour $\alpha = 0$, on retrouve le théorème classique de division euclidienne avec un reste positif.
   Pour $\alpha = -\dfrac{|b|}{2}$, le reste est dans $\left[-\dfrac{|b|}{2}, \dfrac{|b|}{2}\right[$ et c'est le reste de plus petite valeur absolue.

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

3. **Les anneaux** $\mathbb{K}[X]$.
   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 $(\mathbb{K}[X], \deg)$?

4. **L'anneau** $\mathbb{D}$ **des nombres décimaux.**
   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 $\mathbb{Q}$).

   (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. **Les anneaux** $\mathbb{Z}[i\sqrt{n}]$.

   (a) 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 $|u - qv| \leq \dfrac{\sqrt{n+1}}{2}|v|$.

   (b) 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).

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

   (d) Montrer que, pour $n \geq 3$, $\mathbb{Z}[i\sqrt{n}]$ n'est pas euclidien.

6. 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.

7. **Un anneau principal non euclidien.**

Pour cette question, $\omega = \dfrac{1 + i\sqrt{19}}{2}$ (cas $n = 5$ du deuxième cas de figure de **II.6b**) et on se propose de montrer que l'anneau $\mathbb{Z}[\omega]$ est principal, mais non euclidien.

(a) Montrer que :

$$(\mathbb{Z}[\omega])^\times = \{-1, 1\}$$

(b) On suppose qu'il existe un stathme $\varphi : \mathbb{A}^* \to \mathbb{N}$ qui fasse de $\mathbb{Z}[\omega]$ un anneau euclidien.

i. Justifier l'existence de $u \in \mathbb{Z}[\omega] \setminus \{0\}$ tel que :

$$\varphi(u) = \min\{\varphi(v) \mid v \in \mathbb{Z}[\omega] \setminus \{-1, 0, 1\}\}$$

ii. Montrer que pour tout $v \in \mathbb{Z}[\omega] \setminus \{0\}$, l'entier $|u|^2$ divise l'un des entiers $|v|^2$, $|v-1|^2$ ou $|v+1|^2$ dans $\mathbb{N}$.

iii. Montrer qu'on aboutit à une contradiction et conclure.

(c) Montrer que pour tout $z \in \mathbb{C}$, il existe $u \in \mathbb{Z}[\omega]$ tel que :

$$|z - u| < 1 \text{ ou } |2z - u| < 1$$

(d) Montrer que l'anneau $\mathbb{Z}[\omega]$ est principal.

– III – Anneaux factoriels

Définition 3 *On dit que l'anneau $\mathbb{A}$ est factoriel s'il est intègre et si tout élément a non nul et non inversible s'écrit de manière unique (à permutation et association près) comme produit d'éléments irréductibles.*

1. On se propose de montrer que l'anneau intègre $\mathbb{A}$ est factoriel si, et seulement si, les deux propriétés suivantes sont vérifiées :
   (1) toute suite croissante d'idéaux principaux de $\mathbb{A}$ est stationnaire ;
   (2) tout élément irréductible de $\mathbb{A}$ est premier.

   (a) Montrer que si $\mathbb{A}$ est factoriel, les propriétés (1) et (2) sont alors vérifiées.

   (b) On suppose que les propriétés (1) et (2) sont vérifiées et on se donne $a \in \mathbb{A}^* \setminus \mathbb{A}^\times$.

      i. Montrer que a admet un diviseur irréductible.

      ii. On construit des diviseurs irréductibles de a comme suit :
      si a est irréductible, on pose $p_1 = a$ et c'est terminé ;
      supposant construits, pour $n \geq 1$, des diviseurs irréductibles $p_1, \cdots, p_n$ de a, si $a_n = \dfrac{a}{p_1 \cdot \cdots \cdot p_n}$ est inversible c'est terminé, sinon p_{n+1} est un diviseur irréductible de a_n.
      Montrer que cet algorithme s'arrête nécessairement au bout d'un nombre fini d'étapes et en déduire l'existence d'une décomposition de a en facteurs irréductibles.

      iii. Montrer l'unicité d'une telle décomposition.

2. Montrer que, pour $n \geq 3$, l'anneau $\mathbb{Z}\left[i\sqrt{n}\right]$ n'est pas factoriel.

3. Montrer qu'un anneau principal est factoriel.

– IV – Anneaux à pgcd

Définition 4 *Soient $r \in \mathbb{N} \setminus \{0, 1\}$ et $a_1, \cdots, a_r$ dans $\mathbb{A}^*$. On dit que ces éléments admettent un plus grand commun diviseur s'il existe $\delta \in \mathbb{A}^*$ tel que :*

$$\begin{cases} \forall k \in \{1, \cdots, r\}, \ \delta \text{ divise } a_k \\ \text{tout diviseur commun à } a_1, \cdots, a_r \text{ divise } \delta \end{cases} \tag{1}$$

Définition 5 *On dit que $\mathbb{A}$ est un anneau à* pgcd *si deux éléments quelconques a, b de $\mathbb{A}^*$ admettent un plus grand commun diviseur.*

1. En cas d'existence, montrer que deux plus grands communs diviseurs d'une famille $\{a_1, \cdots, a_r\}$ de $r \geq 2$ éléments de $\mathbb{A}^*$ sont associés.
   On note $\text{pgcd}\,(a_1, \cdots, a_r)$ ou $a_1 \wedge \cdots \wedge a_r$ un plus grand commun diviseur de $a_1, \cdots, a_r$, c'est un élément de $\mathbb{A}^*$ défini à association près (ou modulo $\mathbb{A}^\times$).
   Si $\{a_1, \cdots, a_r\}$ est une famille d'éléments non tous nuls de $\mathbb{A}$, on définit $\text{pgcd}\,(a_0, a_1, \cdots, a_n)$ comme le pgcd des coefficients a_k qui sont non nuls.
   Dans le cas où $\text{pgcd}\,(a_1, \cdots, a_r)$ est inversible, on dit que $a_1, \cdots, a_r$ sont premiers entre eux et on note :
   $$\text{pgcd}\,(a_1, \cdots, a_r) = 1$$
   (c'est une égalité modulo $\mathbb{A}^\times$).

2. Montrer que $\mathbb{A}$ est un anneau à pgcd si, et seulement si, toute famille $\{a_1, \cdots, a_r\}$ de $r \geq 2$ éléments de $\mathbb{A}^*$ admet un pgcd et que dans ce cas :

   (a) pour $r \geq 3$, on a :
   $$\text{pgcd}\,(a_1, \cdots, a_r) = \text{pgcd}\,(\text{pgcd}\,(a_1, \cdots, a_{r-1}), a_r)$$
   (associativité du pgcd) ;

(b) pour toute permutation σ de $\{1,\cdots,r\}$, on a :

$$\text{pgcd}\,(a_1,\cdots,a_r)=\text{pgcd}\left(a_{\sigma(1)},\cdots,a_{\sigma(r)}\right)$$

(commutativité du pgcd) ;

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

$$\text{pgcd}\,(c\cdot a_1,\cdots,c\cdot a_r)=c\cdot\text{pgcd}\,(a_1,\cdots,a_r)$$

(homogénéité du pgcd) ;

(d) $\delta=\text{pgcd}\,(a_1,\cdots,a_r)$ si, et seulement si, il existe des éléments $a'_1,\cdots,a'_r$ premiers entre eux dans $\mathbb{A}^*$ tels que $a_k=\delta a'_k$ pour tout k compris entre 1 et r.

3. Montrer que dans $\mathbb{A}=\mathbb{Z}\left[i\sqrt{5}\right]$, $a=6$ et $b=4+2i\sqrt{5}$ n'ont pas de pgcd.
4. Soit $\mathbb{A}$ un anneau à pgcd et a,b dans $\mathbb{A}^*$. Montrer que a et b sont premiers entre eux si, et seulement si, pour tout $c\in\mathbb{A}^*$, on a :

$$(a\text{ divise }bc)\Leftrightarrow(a\text{ divise }c)$$

(lemme de Gauss).

5. Montrer que dans un anneau à pgcd $\mathbb{A}$, un élément est irréductible si, et seulement si, il est premier.
6. Montrer qu'un anneau principal $\mathbb{A}$ est un anneau à pgcd.
7. Soient $\mathbb{A}$ un anneau factoriel et a,b deux éléments non nuls et non inversibles de $\mathbb{A}$. En notant :

$$a=u\prod_{k=1}^{r}p_k^{m_k},\ b=v\prod_{k=1}^{r}P_k^{n_k}$$

les décompositions de a et b en facteurs irréductibles, où u,v sont inversibles, les p_k sont irréductibles deux à deux non associés et les n_k, m_k sont des entiers naturels (certains de ces entiers pouvant être nuls), montrer que :

$$(a\text{ divise }b)\Leftrightarrow(\forall k\in\{1,\cdots,r\},\ m_k\leq n_k)$$

8. Montrer qu'un anneau factoriel $\mathbb{A}$ est un anneau à pgcd.

– V – L'anneau $\mathbb{A}[X]$ des polynômes à coefficients dans $\mathbb{A}$

On suppose connues les principales propriétés de l'anneau $\mathbb{K}[X]$ des polynômes à coefficients dans un corps commutatif $\mathbb{K}$.

Définition 6 *Si $P(X)=\sum_{k=0}^{n}a_kX^k$ est un polynôme non nul à coefficients dans un anneau factoriel $\mathbb{A}$, son contenu est :*

$$c(P)=\text{pgcd}\,(a_0,a_1,\cdots,a_n)$$

On dit que P est primitif si son contenu est inversible dans $\mathbb{A}$.

1. Soit $\mathbb{A}$ un anneau commutatif, unitaire. Montrer que les assertions suivantes sont équivalentes :
   (a) l'anneau $\mathbb{A}[X]$ est intègre ;
   (b) l'anneau $\mathbb{A}$ est intègre ;

(c) pour tous polynômes P, Q dans $\mathbb{A}[X]$, on a :

$$\deg(PQ) = \deg(P) + \deg(Q)$$

2. On suppose à nouveau, que l'anneau $\mathbb{A}$ est intègre. Montrer que le groupe des éléments inversibles de l'anneau $\mathbb{A}[X]$ est $\mathbb{A}^\times$.
3. Montrer que :

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

Dans les questions qui suivent, l'anneau $\mathbb{A}$ est supposé factoriel.

4. Montrer que le produit de deux polynômes primitifs dans $\mathbb{A}[X]$, où $\mathbb{A}$ est factoriel, est primitif.
5. Soient P, Q deux polynômes non nuls dans $\mathbb{A}[X]$. Montrer que $c(PQ) = c(P)\,c(Q)$.
On désigne par $\mathbb{K}$ le corps des fractions de $\mathbb{A}$.
6. Soit $P \in \mathbb{A}[X]$ non nul et non inversible. Montrer que P est irréductible dans $\mathbb{A}[X]$ si, et seulement si il est constant et irréductible dans $\mathbb{A}$, ou non constant et primitif dans $\mathbb{A}[X]$ et irréductible dans $\mathbb{K}[X]$.
7. Montrer que si $\mathbb{A}$ est factoriel, alors dans $\mathbb{A}[X]$, un polynôme est irréductible si, et seulement si, il est premier.
8. Montrer que si $\mathbb{A}$ est factoriel, alors $\mathbb{A}[X]$ est factoriel (théorème de Gauss).
On en déduit que si $\mathbb{A}$ est un anneau factoriel qui n'est pas un corps, l'anneau $\mathbb{A}[X]$ est factoriel non principal.