Concours Agrégation, Mathématiques générales

Leçon 22- Anneaux principaux. Applications.

Commentaires du jury 2015 :

C'est une leçon où les candidats ont tendance à se placer sur un plan trop théorique. Il est possible de présenter des exemples d'anneaux principaux classiques autres que $\mathbb{Z}$ et $K[X]$ (décimaux, entiers de Gauss ou d'Eisenstein), accompagnés d'une description de leurs irréductibles. Les applications en algèbre linéaire ne manquent pas, il serait bon que les candidats les illustrent. Par exemple, il est étonnant de ne pas voir apparaître la notion de polynôme minimal parmi les applications. Le candidat plus cultivé peut donner des exemples d'anneaux non principaux, mais aussi des exemples d'équations diophantiennes résolues à l'aide d'anneaux principaux. A ce sujet, il sera fondamental de savoir déterminer les unités d'un anneau, et leur rôle au moment de la décomposition en facteurs premiers. On a pu noter dans cette leçon l'erreur répandue que $1+i$ et $1-i$ sont des irréductibles premiers entre eux dans l'anneau factoriel $\mathbb{Z}[i]$.

Commentaires du jury 2016 :

Cette leçon n'est pas uniquement théorique, Il est possible de présenter des exemples d'anneaux principaux classiques autres que $\mathbb{Z}$ et $K[X]$ (décimaux, entiers de Gauss ou d'Eisenstein), accompagnés d'une description de leurs irréductibles. Les applications en algèbre linéaire ne manquent pas et doivent être mentionnées. Par exemple, les notions de polynôme minimal sont très naturelles parmi les applications. Les anneaux euclidiens représentent une classe d'anneaux principaux importante et l'algorithme d'Euclide a toute sa place dans cette leçon pour effectuer des calculs. S'ils le désirent, les candidats peuvent aller plus loin en s'intéressant à l'étude des réseaux, à des exemples d'anneaux non principaux, mais aussi à des exemples d'équations diophantiennes résolues à l'aide d'anneaux principaux. À ce sujet, il sera fondamental de savoir déterminer les unités d'un anneau, et leur rôle au moment de la décomposition en facteurs premiers. De même, le calcul effectif des facteurs invariants de matrices à coefficients dans certains anneaux peut être fait.

Remarque : Il faut savoir montrer qu'un anneau principal est factoriel. La preuve ne s'improvise pas, [Fr. F] p. 27. Le fait que $\mathbb{Z}$ est factoriel c'est le théorème fondamental de l'arithmétique et se montre facilement par récurrence.

Développements conseillés :

(1) Entiers de Gauss, somme de 2 carrés, [F. M. 1] $n°94$ p. 260 ou [Pe.] p. 57. Sur le même principe et pour changer on peut préferer étudier les entiers de la forme x^2+2y^2 et l'anneau $\mathbb{Z}[i\sqrt{2}]$, [F. M. 2] p. 197.

(2) L'anneau $\mathbb{Z}[i\sqrt{2}]$ et l'équation de Mordell, [F. M. 1] $n°98$ p. 269. Il faut savoir décrire les irréductibles de $\mathbb{Z}[i\sqrt{2}]$, [F. M. 2] p. 197.

(3) L'anneau principal $\mathbb{Z}[\sqrt{2}]$, [F. M. 2] p. 203.

(4) Le théorème des restes chinois généralisé, [F. M. 2] p. 189. Application du théorème des restes chinois au comptage des idempotents de l'anneau A/a où A est un anneau principal et $a \in A$, [F. M. 1] $n°93$ p. 257.

(5) La décomposition en éléments simples dans le corps des fractions rationnelles $K(X)$ sur le corps commutatif K, [F. M. 1] p. 308.

Bibliographie

[F. M. 1] Fresnel J., Matignon M. *Algèbre et Géométrie* (Hermann 2011)
Errata, https://www.math.u-bordeaux.fr/∼mmatigno/Errata-Alg-Géom.pdf
[F. M. 2] Fresnel J., Matignon M. *Algèbre et Géométrie-81 thèmes pour l'agrégation* (ellipses 2017)
Compléments et errata, https://www.math.u-bordeaux.fr/∼mmatigno/Errata-FM2.pdf
[Fr. A.] Fresnel J. *Algèbre des matrices* (Hermann 2011)
[Fr. F.] Fresnel J. *Anneaux* (Hermann 2001)

et
[Pe.] Perrin D. *Cours d'algèbre* (ellipses 1996)

Exercice 1 Soit $\mathbb{Z} \subset A \subset \mathbb{Q}$, un sous anneau. On se propose de montrer qu'il est principal.

(1) Soit $S := A^\times \cap \mathbb{Z}$, les entiers qui deviennent inversibles dans A. Montrer que $A = \mathbb{Z}[\frac{1}{s} \mid s \in S]$.
Preuve. Remarquer que si $s, s' \in S$ alors $ss' \in S$; ainsi $A \subset \mathbb{Z}[\frac{1}{s} \mid s \in S$. Pour l'autre inclusion on écrit $a = \frac{n}{d} \in A$ avec $n, d \in \mathbb{Z}$ et premiers entre eux. Ainsi $1 = un + vd$ avec $u, v \in \mathbb{Z}$ et donc $\frac{1}{d} = ua + v \in A$; il suit que $d \in S$. ///
(2) Conclure. Soit I un ideal de A. Soit $N(I) := I \cap \mathbb{Z}$, c'est un idéal $n\mathbb{Z}$ de $\mathbb{Z}$ et montrer que $I = nA$.
(3) Montrer que $A := \{\frac{n}{d}\}$ avec $n \in \mathbb{Z}$ et $d \in 2\mathbb{Z} - \{0\}$. Montrer que A est un anneau principal.

Exercice 2 Soit A un anneau principal dont le groupe $A^\times$ des inversibles est fini. Alors A est soit un corps fini, soit un anneau admettant une infinité d'idéaux maximaux, [F. M. 2] IV.14. p. 278.

Exercice 3 Si $A \subset \mathbb{C}$, on note $U(A) := \{z \in A \mid |z|^2 = z\sigma(z) = 1\}$. Structure des groupes $\mathbb{Q}^\times$, $U(\mathbb{Q})$ et $\mathbb{Q}[i]^\times$, $U(\mathbb{Q}[i])$ (utiliser la décomposition en irréductibles dans un anneau principal).

(1) Montrer que le groupe $\mathbb{Q}^\times$ est isomorphe au groupe $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \mathbb{Z}^{(\mathbb{N})}$ où $\mathbb{Z}^{(\mathbb{N})}$ est le sous-groupe des suites nulles à partir d'un certain rang i.e. la somme de copies de $\mathbb{Z}$ indexées par $\mathbb{N}$ et que le groupe multiplicatif $U(\mathbb{Q})$ est isomorphe au groupe additif $\frac{\mathbb{Z}}{2\mathbb{Z}}$.
Preuve. C'est une conséquence du théorème fondamental de l'arithmétique. Soit $\mathcal{P}$ l'ensemble des entiers premiers et considérons l'application $f : \mathbb{Q}^\times \to \frac{\mathbb{Z}}{2\mathbb{Z}} \times \mathbb{Z}^{\mathbb{N}}$ définie par $f(z) = (\epsilon \mod 2, (n_p)_{p\in\mathcal{P}})$ où $z = (-1)^\epsilon \prod_{p\in\mathcal{P}} p^{n_p}$ est la décomposition en irréductibles de z; c'est un homomorphisme de groupes qui est injectif (unicité de la décomposition) et son image est le sous-goupe $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \mathbb{Z}^{(\mathbb{N})}$ (les n_p sont nuls sauf au plus un nombre fini). ///
(2) Montrer que le groupe $\mathbb{Q}[i]^\times$ est isomorphe au groupe $\frac{\mathbb{Z}}{4\mathbb{Z}} \times \mathbb{Z}^{(\mathbb{N})}$ où $\mathbb{Z}^{(\mathbb{N})}$ est le sous-groupe des suites nulles à partir d'un certain rang i.e. la somme de copies de $\mathbb{Z}$ indexées par $\mathbb{N}$.
Preuve. On rappelle que $\mathbb{Z}[i]$ est un anneau principal, que le groupe des inversibles est le groupe cyclique engendré par i et donc isomorphe au groupe additif $\frac{\mathbb{Z}}{4\mathbb{Z}}$. Un système d'éléments irréductibles de $\mathbb{Z}[i]$ est indexé sur les premiers $\mathcal{P}$ de $\mathbb{N}$. Précisément si $p = 2$, on note $\pi_2 := 1 + i$, c'est l'unique irréductible à associés près avec $2\mathbb{Z} = \pi_2\mathbb{Z}[i] \cap \mathbb{Z}$. Si $p = 1 \mod 4$ alors $p = a^2 + b^2$ avec $0 < a < b$, on note $\pi_p := a + ib$ et $\overline{\pi}_p$ le conjugué, ce sont à associés près les seuls irréductibles π de $\mathbb{Z}[i]$ avec $p\mathbb{Z} = \pi\mathbb{Z}[i] \cap \mathbb{Z}$. Si $p = 3 \mod 4$, alors p est irréductible dans $\mathbb{Z}[i]$. Ainsi $\pi_2 \cup \{\pi_p, \overline{\pi}_p \mid p = 1 \mod 4\} \cup \{\pi_p \mid p = 3 \mod 4\}$ est un système Π de représentants à associé près des irréductibles de $\mathbb{Z}[i]$ (voir [F. M. 1] n° 94 p. 260). On construit comme dans la question précédente un homomorphisme injectif $f : \mathbb{Q}[i]^\times \to \frac{\mathbb{Z}}{4\mathbb{Z}} \times \mathbb{Z}^{\Pi}$ défini par $f(z) = (\epsilon \mod 4, (n_\pi)_{\pi\in\Pi})$ où $z = (i)^\epsilon \prod_{\pi\in\Pi} \pi^{n_\pi}$ est la décomposition en irréductibles de z; puisque l'image de f est le sous-groupe $\frac{\mathbb{Z}}{4\mathbb{Z}} \times \mathbb{Z}^{(\Pi)}$ qui puisque Π est dénombrable s'identifie au groupe $\frac{\mathbb{Z}}{4\mathbb{Z}} \times \mathbb{Z}^{(\mathbb{N})}$.
(3) *Montrer que le groupe $U(\mathbb{Q}[i])$ est isomorphe au groupe $\frac{\mathbb{Z}}{4\mathbb{Z}} \times \mathbb{Z}^{(\mathbb{N})}$ où $\mathbb{Z}^{(\mathbb{N})}$ est le sous-groupe des suites nulles à partir d'un certain rang i.e. la somme de copies de $\mathbb{Z}$ indexées par $\mathbb{N}$.*
Preuve. Il faut regarder plus dans le détail la décomposition en irréductibles. Comme vu précédemment si $z \in \mathbb{Q}[i]^\times$, alors $z = i^\epsilon \pi_2^{n_2} \prod_{p=1 \mod 4} \pi_p^{n_p}\overline{\pi}_p^{m_p} \prod_{p=3 \mod 4} p^{n_p}$ où $\epsilon \in \mathbb{Z}$ et $z \in U(\mathbb{Q}[i])$ si et seulement si $n_2 = 0$, $n_p + m_p = 0$ pour $p = 1 \mod 4$ et $n_p = 0$ pour $p = 3 \mod 4$. Soit donc $\mathcal{P}'$ l'ensemble des entiers premiers congrus à $1 \mod 4$, alors l'application $g : U(\mathbb{Q}[i]) \to \frac{\mathbb{Z}}{4\mathbb{Z}} \times \mathbb{Z}^{\mathcal{P}'}$ définie par $g(z) = (\epsilon \mod 4, (n_p)_{p\in\mathcal{P}'})$ pour $z = (i)^\epsilon \prod_{p\in\mathcal{P}'} (\frac{\pi}{\overline{\pi}})^{n_p}$ induit un isomorphisme du groupe $U(\mathbb{Q}[i])$ avec le groupe $\frac{\mathbb{Z}}{4\mathbb{Z}} \times \mathbb{Z}^{(\mathcal{P}')}$ qui est isomorphe au groupe $\frac{\mathbb{Z}}{4\mathbb{Z}} \times \mathbb{Z}^{(\mathbb{N})}$ où $\mathbb{Z}^{(\mathbb{N})}$ est le sous-groupe des suites nulles à partir d'un certain rang. ///

Exercice 4 L'anneau $\mathbb{Z}[\sqrt{2}]$, [F. M. 2] p. 203. Déterminer la structure des groupes $\mathbb{Q}[\sqrt{2}]^\times$ et $U(\mathbb{Q}[\sqrt{2}])$. On pourra consulter en complément [F. M. 2] IV.8.1 p.246.

Exercice 5 Calcul des facteurs invariants d'une matrices de $M_{n,p}(A)$ avec $A = \mathbb{Z}$ ou $K[X]$, [Fr. A.] p. 57.

Exercice 6 Quotients d'anneaux principaux, [F. M. 1] $n°93$ p. 257.

Exercice 7 Soit A un anneau principal alors la première colonne des éléments de $GL_n(A)$ sont les n-uplets d'élements de A premiers entre eux dans leur ensemble, [Fr. F.] Ex. 5.3.3 p. 219 (Pour ii)$\rightarrow$ i) et iii) voir prop 5.11 p. 209). Construire une matrice de $GL_3(\mathbb{Z})$ dont la première ligne est $(6, 10, 15)$.

Exercice 8 $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ est un anneau principal mais pas euclidien, [Pe] p. 54 ou [Fr. F.] p. 221).

Exercice 9 Soit A un anneau commutatif. Montrer que l'anneau $A[X]$ est principal ssi A est un corps, [Fr. F.] ex. 1.9.9 p.47.

Exercice 10

(1) Ecrire la décomposition en éléments simples de $\frac{1}{X^p-X}$ dans $\mathbb{F}_p(X)$, (considérer la dérivée logarithmique de $X^p - X$).
(2) Ecrire la décomposition en éléments simples de $\frac{1}{X^q-X}$ dans $\mathbb{F}_p(X)$ avec $q = p^n$.
(3) Ecrire la décomposition en éléments simples de $\frac{1}{X^n-1}$ dans $\mathbb{Q}(X)$, (considérer le produit de X par la dérivée logarithmique de $X^n - 1$ et la décomposition en irréductibles de $X^n - 1$ avec les polynômes cyclotomiques). Pour en savoir plus voir [F. M. 2] IV.13. p. 275.