UNIVERSITÉ DE LORRAINE

L3 Mathématiques – Site Nancy, S5 – 2022-2023

Algèbre 2 – Feuille 6

Anneaux euclidiens, principaux, factoriels

Exercice 1. Soit $\Sigma = \{a^2 + b^2 \mid a, b \in \mathbb{N}\}$ et $\mathcal{P}$ l'ensemble des nombres premiers. Si $p \in \mathcal{P}$, on désigne par $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$. On pose ${}^2\mathbb{F}_p = \{x^2 \mid x \in \mathbb{F}_p\}$ et ${}^2\mathbb{F}_p^\times = \{x^2 \mid x \in \mathbb{F}_p^*\}$.

1. Soit $p \in \mathcal{P}$ tel que $p > 2$. On rappelle que le groupe des éléments inversibles de $\mathbb{Z} : p\mathbb{Z}$ est cyclique d'ordre $p - 1$.
   (a) Montrer que ${}^2\mathbb{F}_p^\times = \{x \in \mathbb{F}_p^\times \,:\, x^{\frac{p-1}{2}} = 1\}$.
   (b) Montrer que $\mathrm{card}({}^2\mathbb{F}_p) = \frac{p+1}{2}$ et $\mathrm{card}({}^2\mathbb{F}_p^*) = \frac{p-1}{2}$.
   (c) Montrer que $-1 \in {}^2\mathbb{F}_p$ si et seulement si $p \equiv 1[4]$, et que $-1 \notin {}^2\mathbb{F}_p$ si et seulement si $p \equiv 3[4]$.
2. On note $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$. On obtient ainsi un sous-anneau de $\mathbb{C}$, appelé l'anneau des *entiers de Gauss*.
   (a) On pose $\theta(x) = a^2 + b^2 = x\bar{x}$. Alors $\theta(xy) = \theta(x)\theta(y)$ pour $x, y \in \mathbb{Z}[i]$.
      (α) Déterminer le groupe $\mathbb{Z}[i]^\times$ des unités de $\mathbb{Z}[i]$.
      (β) Montrer que l'anneau $\mathbb{Z}[i]$ est euclidien pour le stathme θ.
   (b) Soit $p \in \mathcal{P}$.
      (α) Montrer que $p \in \Sigma$ si et seulement si p n'est pas irréductible dans $\mathbb{Z}[i]$.
      (β) Montrer que $p \in \Sigma$ si et seulement si $p = 2$ ou $p \equiv 1[4]$.
   (c) Montrer que les éléments irréductibles de $\mathbb{Z}[i]$ sont les éléments de l'une ou l'autre des formes suivantes :
      (α) $\pm ip$, $\pm p$, avec p premier tel que $p \equiv 3[4]$.
      (β) $a + ib$, avec $a, b \in \mathbb{Z}$ et $a^2 + b^2$ premier.
   (d) Soient $n \in \mathbb{N}^*$ et $n = \prod_{p \in \mathcal{P}} p^{a_p}$ sa décomposition en produit de facteurs premiers. Montrer que $n \in \Sigma$ si et seulement si a_p est pair pour tout $p \in \mathcal{P}$ tel que $p \equiv 3[4]$.
3. Déterminer dans l'anneau $\mathbb{Z}[i]$ la décomposition en facteurs irréductibles de $x = 69 + 45i$ et le pgcd de x et $y = 12 + 18i$.
4. Décomposer comme somme de deux carrés l'entier $n = 260$.
5. Si $x = a + ib$ est un élément irréductible de $\mathbb{Z}[i]$, avec $b \neq 0$. Peut-on avoir x et $\bar{x}$ associés ?

Exercice 2. On considère l'ensemble $\mathbb{Z}[i\sqrt{7}] = \{a + ib\sqrt{7}\ ;\ a, b \in \mathbb{Z}\}$.
(a) Montrer que $\mathbb{Z}[i\sqrt{7}]$ est un sous-anneau de $\mathbb{C}$.
(b) On pose pour tout $z \in \mathbb{Z}[i\sqrt{7}]$, $\theta(z) = z\bar{z} = |z|^2$. Montrer que $\mathbb{Z}[i\sqrt{7}]^\times = \{z \in \mathbb{Z}[i\sqrt{7}];\ \theta(x) = 1\}$, déterminer alors $\mathbb{Z}[i\sqrt{7}]^\times$.
(c) Montrer que 2, $1 + i\sqrt{7}$ et $1 - i\sqrt{7}$ sont irréductibles dans $\mathbb{Z}[i\sqrt{7}]$.
(d) Montrer que 2 n'est associé ni à $1 + i\sqrt{7}$ ni à $1 - i\sqrt{7}$ dans l'anneau $\mathbb{Z}[i\sqrt{7}]$.
(e) Montrer que 8 admet dans $\mathbb{Z}[\sqrt{-7}]$ deux décompositions en facteurs irréductibles. En déduire que l'anneau $\mathbb{Z}[i\sqrt{7}]$ n'est pas factoriel.

Exercice 3. On considère l'ensemble $\mathbb{Z}[\sqrt{10}] = \{a + b\sqrt{10};\ \ a, b \in \mathbb{Z}\}$.
(a) Montrer que $\mathbb{Z}[\sqrt{10}]$ est un sous-anneau de $\mathbb{R}$.
(b) Montrer que pour tout $x \in \mathbb{Z}[\sqrt{10}]$, il existe un unique couple d'entiers (a, b) tels que $x = a + b\sqrt{10}$. On note alors $\widetilde{x} = a - b\sqrt{10}$ et $\theta(x) = x\widetilde{x} = a^2 - 10b^2$.
(c) Montrer que $\forall x, y \in \mathbb{Z}[\sqrt{10}]$, on a $\theta(xy) = \theta(x)\theta(y)$.
(d) Montrer que $\mathbb{Z}[\sqrt{10}]^\times = \{x \in \mathbb{Z}[\sqrt{10}];\ \theta(x) = \pm 1\}$.
(e) Montrer que $2 + \sqrt{10}$ et $2 - \sqrt{10}$ et 3 sont irréductibles dans $\mathbb{Z}[\sqrt{10}]$.

(f) Montrer que 6 admet dans $\mathbb{Z}[\sqrt{10}]$ deux décomposition en facteurs irréductibles. En déduire que l'anneau $\mathbb{Z}[\sqrt{10}]$ n'est pas factoriel.

Exercice 4. Soient $j = e^{\frac{2i\pi}{3}}$ et $\mathbb{Z}[j] = \{a + bj;\ a, b \in \mathbb{Z}\}$. On pose pour tout $z \in \mathbb{Z}[j]$, $\theta(z) = z\bar{z} = |z|^2$.

(a) Montrer que $\mathbb{Z}[j]$ est un sous-anneau de $\mathbb{C}$.

(b) Montrer que $(\mathbb{Z}[j])_* = \{z \in \mathbb{Z}[j];\ \theta(z) = 1\}$, déterminer alors $(\mathbb{Z}[j])_*$.

(c) Montrer que $\mathbb{Z}[j]$ est un anneau euclidien pour le stathme θ.

(d) On considère l'idéal I de $\mathbb{Z}[j]$ engendré par $1 - j$.

(α) Soient $a, b \in \mathbb{Z}$; montrer que $a + bj \in I \iff a + b \equiv 0 \mod (3)$.

(β) Montrer que 3 n'est pas irréductible dans $\mathbb{Z}[j]$.

(γ) Montrer que l'anneau quotient $\mathbb{Z}[j]/I$ est isomorphe à $\mathbb{Z}/3\mathbb{Z}$.

(δ) Montrer que l'idéal I est maximal.

Exercice 5.

1. Soit A un anneau euclidien et soit θ un stathme de A.
   (a) Montrer que θ' défini par $\theta'(x) = \min\{\theta(xu) \mid u \in A^\times\}$ 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 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.
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 note pour tout $z \in \mathbb{Z}[\alpha]$, $\theta(z) = z\bar{z} = |z|^2$.
   (a) Montrer que $\mathbb{Z}[\alpha]$ est un sous-anneau de $\mathbb{C}$.
   (b) 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 (1c), montrer que l'anneau $\mathbb{Z}[\alpha]$ n'est pas euclidien.
3. On montre maintenant que $\mathbb{Z}[\alpha]$ est principal.
   (a) Le critère de Dedekind-Hasse est la condition suivante : soient $z, w \in \mathbb{Z}[\alpha]$ 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
   $$pz - qw = r \text{ et } \theta(r) < \theta(w)\,.$$
   Montrer que ce critère 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 Dedekind-Hasse 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 l'anneau $\mathbb{Z}[\alpha]$ est principal.

Exercice 6. Montrer que les polynômes suivants sont irréductibles dans $\mathbb{Z}[X]$:
(a) $X^5 - 12X^3 + 36X - 12$;
(b) $2X^{15} - 7X^{12} + 35X^{10} - 84X^6 + 14X^4 + 7X^3 - 49X^2 + 210X - 21$;
(c) $X^{32} - 210$.

Exercice 7. Soit $p > 2$ un nombre premier et posons $K = \mathbb{Z}/p\mathbb{Z}$. Soient $P(X) = X^n(X^3 + 2X^2 + 2X + 2)^n + X^{4n} - X^4 - 1$ et $Q(X) = X^3 + X^2 + X + 1$ deux polynômes de $K[X]$. Montrer que Q divise P si et seulement si n est pair.

Exercice 8. (a) Donner la liste de tous les polynômes de degré 1, 2, ou 3 à coefficients dans le corps $K = \mathbb{Z}/2\mathbb{Z}$ et préciser pour chacun s'il est scindé, non-scindé, irréductible.
(b) Le polynôme $X^4 + X^2 + \bar{1}$ a-t-il des racines dans $K[X]$? Est-il irréductible ?
(c) Montrer que le polynôme $X^4 + X + \bar{1}$ est irréductible dans $K[X]$ et dans $\mathbb{Z}[X]$.

Exercice 9. Montrer que dans $\mathbb{Z}/17\mathbb{Z}$, les racines du polynôme $X^6 + X^4 + X^2 + \bar{1}$ sont toutes des carrés. Déterminer ces racines.

Exercice 10. Soit $\mathbf{a}(X) = a_0 + a_1X + \ldots + a_nX^n \in \mathbb{Z}[X]$, $a_n \neq 0$ $(n \geq 1)$.
(a) Soit $r = \frac{p}{q}$ une racine rationnelle de a $(p \wedge q = 1)$. Montrer que p divise a_0 et que q divise a_n.
(b) En déduire les racines rationnelles de $\mathbf{a}(X) = 2X^5 - 5X^4 - 21X^3 - 15X^2 - 23X - 10$, puis la décomposition de $\mathbf{a}$ en facteurs irréductibles.

Exercice 11. Soit le polynôme $\mathbf{a}(X) = X^4 - 10X^3 + 21X^2 - 10X + 11 \in \mathbb{Z}[X]$.
(a) Étudier l'irréductibilité de la réduction de $\mathbf{a}$ modulo 2, 3 et 5.
(b) $\mathbf{a}$ est-il irréductible dans $\mathbb{Z}[X]$?