École Normale Supérieure, Année 2021-2022

1e année, Algèbre 1

TD nº 10 : Arithmétique des anneaux

`À faire en priorité : 1 - 2 - 3 - 4 - 5 - 6`

Exercice 1. Échauffement

Factoriser $-3+15i$ et $4+7i$ en irréductibles dans $\mathbb{Z}[i]$.

Exercice 2. Entiers d'Eisenstein

On pose $j = e^{2\pi/3}$ et $\mathbb{Z}[j] = \mathbb{Z} + \mathbb{Z}j$.

1. Montrer que $\mathbb{Z}[j]$ est un sous-anneau de $\mathbb{C}$.
2. Montrer $\mathbb{Z}[j]^\times = \{\pm 1, \pm j, \pm j^2\} = \mu_6$.
3. Montrer que $\mathbb{Z}[j]$ est euclidien pour $z \mapsto |z|^2$.
4. Soit p un nombre premier $\equiv 1 \bmod 3$. Montrer que[1] l'on a $p = \pi\overline{\pi}$ avec π et $\overline{\pi}$ des irréductibles non associés de $\mathbb{Z}[j]$.
5. `(suite)` En déduire qu'il existe exactement 12 couples $(a,b) \in \mathbb{Z}^2$ tels que $p = a^2 - ab + b^2$.
6. `(suite)` Montrer qu'il existe un unique $(a,b) \in \mathbb{N}^2$ avec $p = a^2 + 3b^2$.
7. Trouver tous les $(x,y) \in \mathbb{Z}^2$ tels que $y^2 = x^3 - 1$.

Exercice 3.

1. Montrer que le plus petit réel > 1 de la forme $x + y\sqrt{2}$ avec $x, y \in \mathbb{Z}_{>0}$ et $x^2 - 2y^2 = \pm 1$ est $1 + \sqrt{2}$.
2. En déduire $\mathbb{Z}[\sqrt{2}]^\times = \langle -1 \rangle \times \langle 1 + \sqrt{2} \rangle$.

Exercice 4. Noethérianité de $\mathbb{Z}[\sqrt{d}]$

Soient $d \in \mathbb{Z}$ non carré et $A = \mathbb{Z}[\sqrt{d}]$.

1. Montrer que tout idéal non nul I de A contient un entier $n \in \mathbb{Z}_{>0}$.
2. Montrer qu'il n'y a qu'un nombre fini de sous-groupes de A contenant un entier $n \in \mathbb{Z}_{>0}$ donné.
3. Montrer que A est noethérien, et que tout idéal non nul y est d'indice fini.
4. Soit $d \equiv 1 \pmod 4$, montrer que A_d est noethérien, et que tout idéal non nul y est d'indice fini.

Exercice 5. Unités de $\mathbb{Z}[\sqrt{d}]$ avec $d > 0$

Soit $d > 0$ un entier non carré. On se propose de montrer $\mathbb{Z}[\sqrt{d}]^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.

1. Soit $\varepsilon = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]^\times$. Rappeler pourquoi on a $\varepsilon > 1 \iff x, y > 0$.
2. On suppose $\mathbb{Z}[\sqrt{d}]^\times \neq \{\pm 1\}$. Montrer qu'il existe un plus petit réel $\eta \in \mathbb{Z}[\sqrt{d}]^\times$ avec $\eta > 1$.
3. `(suite)` En déduire $\mathbb{Z}[\sqrt{d}]^\times = \{\pm 1\} \times \langle \eta \rangle$.
4. Montrer le *principe de Dirichlet* que pour tout $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, et tout entier $N \geq 1$, il existe $p \in \mathbb{Z}$ et $1 \leq q \leq N$ tels que $|q\alpha - p| < 1/N$.
5. Montrer qu'il existe une suite d'éléments $x_n \in \mathbb{Z}[\sqrt{d}]$ non nuls avec $x_n \to 0$ dans $\mathbb{R}$ et $(\mathrm{N}(x_n))_{n \geq 1}$ bornée.
6. `(suite)` Montrer que, quitte à extraire une sous-suite de x_n, on peut supposer qu'il existe $k \in \mathbb{Z}$ tel que $\mathrm{N}(x_n) = k$ et $x_n\overline{x_m} \in k\mathbb{Z}[\sqrt{d}]$, pour tout $n, m \geq 1$.
7. `(suite)` En déduire que $\mathbb{Z}[\sqrt{d}]^\times$ est infini.
8. Conclure.

---

[1] On rappelle que -3 est un carré modulo p.

Exercice 6.

Soit $d < -2$ un entier. On se propose de montrer que l'anneau $\mathbb{Z}[\sqrt{d}]$ est non principal. On pose $\alpha = \sqrt{d}$ si d est pair, $\alpha = 1 + \sqrt{d}$ sinon.

1. Traiter directement les cas $d = -3, -4$. On suppose désormais $d < -4$.
2. Vérifier que les seuls éléments de $\mathbb{Z}[\sqrt{d}]$ de norme 4 sont ± 2.
3. Montrer $(2, \alpha) = 2\mathbb{Z} + \alpha\mathbb{Z}$.
4. En déduire que l'idéal $(2, \alpha)$ n'est pas principal.

Exercice 7.

1. Montrer $\mathrm{A}_{-3}^{\times} = \mu_6$ et $\mathrm{A}_d^{\times} = \{\pm 1\}$ pour $d < 0$.
2. Montrer que A_{-3}, A_{-7} et A_{-11} sont euclidiens pour N.
3. Montrer que A_d est principal pour $d = -43, -67$ et -163.

Exercice 8.

On se propose de montrer que l'anneau A_{-19} est principal.

1. Montrer que pour tout $a, b \in \mathrm{A}_{-19}$ non nuls, avec b ne divisant pas a, on a soit $a = bq + r$ avec $\mathrm{N}(r) < \mathrm{N}(b)$, soit $2a = bq + r$ avec $\mathrm{N}(r) < \mathrm{N}(b)$.
2. Montrer que l'idéal (2) est maximal dans A_{-19}, et que l'élément 2 est premier.
3. En déduire que A_{-19} est principal.

Exercice 9.

On veut montrer que A_d n'est pas euclidien pour $d < -11$.

1. Soit A un anneau euclidien pour le stathme φ. On suppose que A n'est pas un corps. Montrer qu'il existe $x \in A$ non zero ou unité, tel que l'application naturelle $\{0\} \sqcup A^{\times} \to A/xA$ est surjective.
2. Montrer que pour $d < -11$, A_d ne possède aucun élément de norme 2 ou 3.
3. Conclure.

Exercice 10. Lemme du *contenu* de Gauss

Soit A un anneau factoriel de corps de fractions K. Si $P \in A[X]$ est non nul, on note $\mathrm{c}(P)$ le pgcd des coefficients de P, c'est un élément de A bien défini aux unités près. On dit que P est primitif si $\mathrm{c}(P)$ est une unité.

1. Montrer $A[X]^{\times} = A^{\times}$.
2. Montrer que si $P, Q \in A[X]$ sont primitifs alors PQ est primitif.
3. En déduire que si $P, Q \in A[X]$ sont non nuls, on a $\mathrm{c}(PQ) = \mathrm{c}(P)\mathrm{c}(Q)$ (aux unités près).
4. Montrer que si $P \in A[X]$ est non constant, alors P est irréductible dans $A[X]$ si et seulement si $\mathrm{c}(P) = 1$ et P est irréductible dans $K[X]$.
5. En déduire que les irréductibles de $A[X]$ sont les irréductibles de A et les polynômes primitifs non constant.
6. Montrer que $A[X]$ est factoriel. On en déduit que $\mathbb{Z}[X_1, \ldots, X_n]$ et $k[X_1, \ldots, X_n]$ sont factoriels si $n \geq 1$ et si k est un corps.
7.

Notations 0.1. Pour $d \in \mathbb{Z}$ non carré et $d \equiv 1 \bmod 4$, on note $\tau_d = \frac{1+\sqrt{d}}{2}$ et $\mathrm{A}_d = \mathbb{Z} + \mathbb{Z}\tau_d$. La relation $\tau_d^2 = \tau_d + \frac{d-1}{4} \in \mathbb{Z} + \tau\mathbb{Z}$ montre que c'est un sous-anneau de $\mathbb{Q}[\sqrt{d}]$ contenant strictement $\mathbb{Z}[\sqrt{d}]$. Par exemple, on a $\tau_{-3} = -e^{4i\pi/3}$ et donc $\mathrm{A}_{-3} = \mathbb{Z}[j]$ est l'anneau des entiers d'Eisenstein.