Université Paris 7 - Denis Diderot 2017-2018
UFR de Mathématiques M1 - Arithmétique

Feuille d'exercices 9

Exercice 1

1. Pour $k = -1, -2$ montrer que $\mathbb{Z}[\sqrt{k}]$ est euclidien.
2. Pour $k = -3, -7, -11$ montrer que $\mathbb{Z}[\frac{1+\sqrt{k}}{2}]$ est euclidien.

Exercice 2 Montrer que les seules solutions entières de l'équation $y^2 = x^3 - 2$ sont $(x, y) = (3, \pm 5)$. (Montrer d'abord que x, y doivent être impairs. En se plaçant dans $A = \mathbb{Z}[i\sqrt{2}]$, montrer que $y + i\sqrt{2}$ doit être un cube dans A et conclure en identifiant parties réelles et imaginaires.)

Exercice 3 On se propose de montrer que les $x, y \in \mathbb{Z}$ tels que $y^2 + y = x^3 - 2$ sont exactement $(x, y) = (2, 2)$ ou $(x, y) = (2, -3)$.

1. Montrer que $\sqrt{-7}$ est un élément premier dans $\mathbb{Z}[\alpha]$, où $\alpha = \frac{1+\sqrt{-7}}{2}$;
2. Montrer que si $y^2 + y = x^3 - 2$ alors $y + \alpha$ n'est pas divisible par $\sqrt{-7}$ dans $\mathbb{Z}[\alpha]$;
3. Conclure.

Exercice 4 Trouver toutes les solutions entières de $y^3 - x^2 = 1$ et de $x^2 - y^3 = 1$. (Travailler dans $\mathbb{Z}[i]$ pour la première équation et dans $\mathbb{Z}[\frac{1+i\sqrt{3}}{2}]$ pour la deuxième.)

Exercice 5 Soit $d \in \mathbb{Z}$. Montrer que le produit de deux nombres de la forme $a^3 + db^3 + dc^3 - 3abc$, avec $a, b, c \in \mathbb{Z}$, est encore de cette forme. On pourra d'abord supposer que d n'est pas un cube et considérer le corps $\mathbb{Q}(\sqrt[3]{d})$.

Exercice 6

1. Soient $m, n \in \mathbb{Z}$ avec $n \geq 1$ et soit L le réseau $L = \{(a, b) \in \mathbb{Z}^2 \mid a \equiv mb \bmod n\}$. Donner une $\mathbb{Z}$-base de L.
2. Montrer que $M = \{(a, b, c) \in \mathbb{Z}^3 \mid a \equiv b \bmod 5 \text{ et } b \equiv a+c \bmod 2\}$ est un réseau de $\mathbb{R}^3$. Calculer son covolume et en donner une $\mathbb{Z}$-base.
3. Monter que un élément $(a, b) \in \mathbb{Z}^2$ se complète en une $\mathbb{Z}$-base de $\mathbb{Z}^2$ si et seulement si a et b sont premiers entre eux.
4. Donner un exemple d'une famille génératrice du groupe $\mathbb{Z}$ dont on ne peut pas extraire aucune $\mathbb{Z}$-base.

Exercice 7 Soit $L \subset \mathbb{R}^n$ un réseau et soit $e_1, \ldots, e_n$ une famille d'éléments de L. Montrer que c'est une $\mathbb{Z}$-base de L si et seulement si $|\det(e_1, \ldots, e_n)| = \mathrm{covol}(L)$.

Exercice 8 On munit $\mathbb{R}^n$ du produit scalaire standard. On suppose que $L \subset \mathbb{R}^n$ soit un réseau de covolume 1 tel que $v \cdot w \in \mathbb{Z}$ pour tout $v, w \in L$ (réseau dit *entier*).

1. Montrer que si $n \geq 4$ alors il existe $v \in L$ tel que $v \cdot v = 1$.
2. On suppose qu'il existe $v \in L$ tel que $v \cdot v = 1$. Montrer que tout élément de L s'écrit de manière unique sous la forme $mv + u$ avec $m \in \mathbb{Z}$ et $u \in L \cap v^\perp$.
3. Montrer que $L \cap v^\perp$ est un réseau entier de covolume 1 dans l'espace euclidien $v^\perp$ (munit du produit scalaire induit par $\mathbb{R}^n$).

4. En déduire que si $n \geq 4$ il existe $g \in \mathrm{O}_n(\mathbb{R})$ tel que $L = g(\mathbb{Z}^n)$.

On peut démontrer que le même résultat reste vrai pour $n \leq 7$.

Exercice 9 Soit $D_8 = \{(x_1, \ldots, x_8) \in \mathbb{Z}^8 \mid \sum x_i \equiv 0 \bmod 2\}$ et soit $e \in \mathbb{R}^8$ le vecteur $e = \frac{1}{2}(1, \ldots, 1)$.

1. Montrer que D_8 est un réseau de $\mathbb{R}^8$ de covolume 2.
2. En déduire que $E_8 = \mathbb{Z}e + D_8$ est un réseau de $\mathbb{R}^8$ de covolume 1.
3. Vérifier que pour tout $v, w \in E_8$ on a $v \cdot v \in 2\mathbb{Z}$ et $v \cdot w \in \mathbb{Z}$.
4. En déduire que E_8 n'est pas de la forme $g(\mathbb{Z}^8)$ pour $g \in \mathrm{O}_8(\mathbb{R})$.

Exercice 10 Soit v_n le volume de la boule unité de $\mathbb{R}^n$. On définit, pour $s > 0$, la fonction $\Gamma(s) = \int_0^\infty e^{-t} t^{s-1}\, dt$.

1. Montrer que $\Gamma(1) = 1$ et $\Gamma(\frac{1}{2}) = \sqrt{\pi}$. Montrer que les valeurs de la fonction Γ aux entiers (resp. demi-entiers) positifs peuvent être calculés grâce à la formule $\Gamma(s+1) = s\Gamma(s)$.
2. En calculant de deux façons l'intégrale
$$\int_{\mathbb{R}^n} e^{-(x_1^2 + \cdots + x_n^2)}\, dx_1 \cdots dx_n,$$
montrer que
$$v_n = \frac{\pi^{n/2}}{\Gamma\left(\frac{n}{2} + 1\right)}.$$
3. En déduire que $v_{2m} = \pi^m / m!$ et $v_{2m+1} = \pi^m \alpha$ avec $\alpha \in \mathbb{Q}^*$ que l'on déterminera. Quoi vaut $\lim_{n\to\infty} v_n$?