Théorie des nombres

Feuille de TD n°4

1. Sur les réseaux

Exercice 1

1 Rappeler la définition d'un réseau. Rappeler la caractérisation des réseaux en termes de sous-groupes de $\mathbb{R}^n$.

2 Quels sont les entiers n tels que l'anneau des entiers du corps quadratique $\mathbb{Q}(\sqrt{n})$ admet un plongement complexe dont l'image est un réseau de $\mathbb{R}^2$? Calculer alors le volume de ce réseau.

Exercice 2

1 Rappeler la définition d'un domaine fondamental pour un réseau.

2 Montrer que deux domaines fondamentaux d'un réseau ont même volume.

3 Représenter quelques points du réseau $\mathcal{R}$ de base $(1,2)$, $(2,2)$. Donner deux domaines fondamentaux de $\mathcal{R}$. Donner un vecteur non nul de plus petite norme dans $\mathcal{R}$.

4 Représenter quelques points du réseau des entiers de $\mathbb{Q}(\sqrt{-3})$.

Exercice 3

1 Énoncer le théorème de la base adaptée pour les modules sur des anneaux principaux.

2 Donner l'exemple d'un sous-module d'un $\mathbb{Z}$-module qui n'a pas de supplémentaire.

3 Soit $\mathcal{R}$ un sous-réseau de $\mathbb{Z}^2$ dans $\mathbb{R}^2$. Montrer que son volume est égal au nombre de points de $\mathbb{Z}^2$ dans un domaine fondamental.

Exercice 4

Pour $x \in \mathbb{R}$, on note $E(x)$ sa partie entière et $\{x\} = x - E(x)$ sa partie fractionnaire. Soit α un nombre réel irrationnel.

1 Montrer que les nombres $\{k\alpha\}$, $k \in \mathbb{N}$, de $[0,1[$, sont deux à deux distincts.

2 Soit Q un entier strictement positif. À l'aide du principe des tiroirs, en déduire qu'il existe des entiers i et j tels que $0 \leq i < j \leq Q$ et $|\{i\alpha\} - j\alpha| \leq 1/Q$.

3 Montrer qu'il existe, pour tout entier $Q > 0$, une fraction irréductible p/q telle que

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{qQ}.$$

4 Donner l'exemple d'un nombre réel β et de deux entiers naturels strictement positifs q et Q tels qu'il n'existe aucune fraction irréductible p/q telle que $\left|\beta - \frac{p}{q}\right| \leq \frac{1}{qQ}$.

5 **Théorème de Dirichlet.** Soit θ un nombre irrationnel. Montrer qu'il existe une infinité d'entiers p, q premiers entre eux tels que $|\theta - \frac{p}{q}| < \frac{1}{q^2}$.

2. Théorème de Minkowski

Exercice 5

On cherche les nombres p premiers s'écrivant sous la forme $p = x^2 + y^2$.

1 Montrer que si $p = 3 \mod 4$, alors p n'est pas somme de deux carrés.
On supposera dans la suite que $p = 1 \mod 4$. (Le cas $p = 2$ est simple)
2 Montrer qu'il existe $u_0 \in \mathbb{Z}$ tel que $u_0^2 = -1 \mod p$. Montrer que pour tout $x \in \mathbb{Z}$, $x^2 + (u_0 x)^2 = 0 \mod p$.
3 On considère l'ensemble

$$E = \{u_0 x - y \mid 0 \leq x < \sqrt{p}, 0 \leq y < \sqrt{p}\}.$$

Montrer qu'il existe z_1 et z_2 dans E tels que $z_1 = z_2 \mod p$.
4 En déduire qu'il existe x et y dans $\mathbb{N}$ tels que $x^2 + y^2 = p$.

Exercice 6

Théorème de Minkowski. Soit C un convexe de $\mathbb{R}^n$ symétrique par rapport à 0 et de volume strictement supérieur à 2^n. Alors il existe $u_0 \neq 0$ tel que $u_0 \in C \cap \mathbb{Z}^n$.
1 Notons $D = [0, 1[^n$. Vérifier que $\mathbb{R}^n = \bigcup_{u \in \mathbb{Z}^n} (D + u)$.
2 Soit $A \subset \mathbb{R}^n$ un ensemble de volume strictement supérieur à 1. Pour $u \in \mathbb{Z}^n$, on note $A_u = (A \cap (D + u)) - u$. Montrer que pour tout u, $A_u \subset D$ et que $Vol(A) = \sum_{u \in \mathbb{Z}^n} Vol(A_u)$.
3 En déduire qu'il existe $u, v \in \mathbb{Z}^n$, $u \neq v$ tels que $A_u \cap A_v \neq \emptyset$.
4 Posons $C' = \frac{1}{2} C$. Montrer qu'il existe $x_0, y_0 \in C'$ tels que $x_0 - y_0 \in \mathbb{Z}^n \setminus \{0\}$.
5 Montrer que $C = \{x - y \mid x, y \in C'\}$. En déduire que $u_0 = x_0 - y_0 \in C \cap \mathbb{Z}^n \setminus \{0\}$.

3. Applications du théorème de Minkowski

Exercice 7

1 Soit $p = 13$. On remarque que pour $a = 5$, on a $a^2 + 1 = 0 \mod p$. Montrer que tous les éléments du réseau $\mathcal{R}$ de $\mathbb{Z}^2$ engendré par $(1, a)$ et $(0, p)$ ont une norme multiple de p. Trouver deux entiers x et y tels que $p = x^2 + y^2$.
2 Même question pour $p = 61$ et $a = 11$.

Exercice 8

1 Écrire $2425 = 5^2 \cdot 97$ et $754 = 2 \cdot 13 \cdot 29$ comme sommes de deux carrés.
2 Tous les entiers naturels sont-ils sommes de trois carrés ?
3 Écrire l'identité qui exprime le fait que la norme du produit de deux quaternions est égale au produit de leurs normes.
4 Écrire $323 = 17 \cdot 19$ et $1265 = 5 \cdot 11 \cdot 23$ comme sommes de quatre carrés.

Exercice 9

On cherche les nombres premiers p s'écrivant sous la forme $p = x^2 + 2y^2$.
1 Montrer que pour un tel p, -2 est un carré dans $\mathbb{F}_p$.
2 Supposons que -2 est un carré dans $\mathbb{F}_p$. Il existe donc un entier a tel que $a^2 = -2 \mod p$. En considérant le réseau $\mathcal{R}$ de $\mathbb{Z}^2$ engendré par $(a, 1)$ et $(p, 0)$ et l'ellipse définie pour un certain r par $x^2 + 2y^2 = r^2$ (le volume défini par une telle ellipse est $V_r = \frac{\pi r^2}{\sqrt{2}}$), montrer qu'il existe deux entiers x et y tels que $x^2 + 2y^2 = p$.
3 Écrire 323 sous la forme $n = x^2 + 2y^2$.