UNIVERSITÉ DE RENNES 1

Théorie des nombres

Feuille n°3 : Réseaux

Sur les réseaux

Exercice 1

1. Rappeler la définition d'un réseau.
2. Rappeler la caractérisation des réseaux en termes de sous-groupes de $\mathbb{R}^n$.
3. Rappeler la définition d'un domaine fondamental pour un réseau.
4. Montrer que deux domaines fondamentaux d'un réseau ont même volume.
5. Représenter quelques points du réseau $\mathscr{R}$ de base $(1,2),(2,2)$.
6. Donner deux domaines fondamentaux de $\mathscr{R}$.
7. Donner un vecteur non nul de plus petite norme dans $\mathscr{R}$.

Exercice 2

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 $\mathscr{R}$ 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.

Théorème de Minkowski

Exercice 3

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 4

Théorème de Minkowski :
Soit C un convexe de $\mathbb{R}^n$ symétrique par rapport à 0, 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 on a $A_u \subset D$, et que $\mathrm{Vol}(A) = \sum_{u \in \mathbb{Z}^n} \mathrm{Vol}(A_u)$.
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 $u_0 = x_0 - y_0 \in C \cap \mathbb{Z}^n \setminus \{0\}$.

Exercice 5

Soit Λ un réseau de $\mathbb{R}^n$, de volume V_Λ. Soit C un convexe symétrique compact de $\mathbb{R}^n$, de volume V_C. On suppose que $V_C \geqslant 2^n V_\Lambda$. Montrer que $C \cap \Lambda$ n'est pas réduit à 0.

Applications du théorème de Minkowski

Exercice 6

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 $\mathscr{R}$ 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 7

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 8

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 $\mathscr{R}$ 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 $n = x^2 + 2y^2$.

Exercice 9

Soit p un nombre premier.

1. Montrer que s'il existe $(x, y) \in \mathbb{Z}^2$ tels que $p \mid (x^2 + 5y^2)$, alors p divise x ou -5 est un carré dans $\mathbb{F}_p$.
2. Montrer que si $p \neq 5$ et si -5 est un carré modulo p, alors il existe un couple d'entiers $(x, y) \in \mathbb{Z}^2$ tel que $x^2 + 5y^2 \in \{p, 2p\}$.
3. Trouver un nombre premier p qui s'écrive sous la forme $p = x^2 + 5y^2$, avec x et y entiers, et tel que $2p$ ne peut pas s'écrire sous cette forme.
4. Trouver un nombre premier p tel qu'il existe des entiers x et y vérifiant $2p = x^2 + 5y^2$, et tel que p ne s'écrive pas sous cette forme.
5. Montrer qu'il existe un couple $(x, y) \in \mathbb{Z}^2$ tel que $x^2 + 5y^2 \in \{p, 2p\}$ si et seulement si $p = 5$ ou $p \equiv 1, 3, 7$ ou $9 \pmod{20}$.

Exercice 10

On rappelle que tout nombre premier congru à 1 modulo 4 est somme de deux carrés. On considère l'équation $x^2 + y^2 = pz^2$ où p est un nombre premier impair.

1. Vérifier qu'elle possède une solution dans $\mathbb{Q}^3$ si et seulement si elle en possède une dans $\mathbb{Z}^3$.
2. Montrer que si elle admet une solution dans $\mathbb{Z}^3 \setminus \{(0, 0, 0)\}$, -1 est un carré dans $\mathbb{F}_p$ et donc p est congru à 1 modulo 4.
3. La réciproque est-elle vraie ?
4. Lorsqu'elle en possède, décrire toutes les solutions dans $\mathbb{Q}^3$ de l'équation.