Feuille d'exercices 4

1 Réseaux

Exercice 1. *Diverses propriétés des réseaux dans la suite K est l'un des corps $\mathbb{Q}$ ou $\mathbb{R}$ et V est un K-espace vectoriel de dimension finie $n > 0$. Une partie Γ de V est un sous-réseau s'il existe une famille libre $\mathbf{e} = (e_1, \cdots, e_r)$ de V telle que $\Gamma = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_r$. On dit que $\mathbf{e}$ est une $\mathbb{Z}$-base de Γ et r est son rang. On dit que Γ est un réseau si $r = n$.*

(i) $\mathbb{Z} + \sqrt{2}\mathbb{Z}$ *est-il un sous-réseau de* $\mathbb{R}$ *?*

(ii) Soit Γ *un réseau de* V*,* $\mathbf{e}$ *une* $\mathbb{Z}$*-base de* Γ *et* $\mathbf{v}$ *une base de* V*. Montrez que* $\mathbf{v}$ *est une* $\mathbb{Z}$*-base de* Γ *si et seulement si la matrice de passage de* $\mathbf{e}$ *à* $\mathbf{v}$ *appartient à* $GL_n(\mathbb{Z})$*.*

(iii) Soient Γ *un réseau de* V *et* $\Lambda \subset \Gamma$ *un sous-groupe. Montrez que* Λ *est un sous-réseau de* V *et qu'il existe une* $\mathbb{Z}$*-base* $(e_1, \cdots, e_n)$ *de* Γ*,* $1 \leq s \leq n$ *et* $a_1, \cdots, a_s \in \mathbb{Z}^\times$ *vérifiant:*

- $(a_1e_1, \cdots, a_se_s)$ *est une* $\mathbb{Z}$*-base de* Λ*,*
- *pour* $1 \leq i < s$*,* a_i *divise* a_{i+1}

En déduire une CNS pour que Γ/Λ *soit fini et calculez son cardinal en fonction des* a_i*.*

(iv) On suppose ici $K = \mathbb{Q}$*. Soient* Γ, Λ *des réseaux de* V*. Montrez que*

- *il existe* $d \in \mathbb{N}\backslash\{0\}$ *tel que* $d\Gamma \subset \Lambda$*,*
- $\Gamma + \Lambda$ *et* $\Gamma \cap \Lambda$ *sont des réseaux de* V*.*

(v) On suppose ici $K = \mathbb{R}$ *et on munit* V *de sa topologie canonique. Montrez que tout sous-groupe discret*[1] Γ *de* V *en est un sous-réseau.*

Indication: soit $(e_1, \cdots, e_r)$ *une famille libre maximale de* Γ *et* $\mathcal{K} = \{\lambda_1e_1 + \cdots + \lambda_re_r; \lambda_i \in [0,1]\}$*. En utilisant le fait que* $\mathcal{K} \cap \Gamma$ *est fini et en considérant pour* $j \in \mathbb{Z}$ *et* $x = l_1e_1 + \cdots + l_re_r \in \Gamma$*, les* $x_j = jx - ([jl_1]e_1 + \cdots + [jl_r]e_r)$[2]*, montrez que* $l_i \in \mathbb{Q}$ *et conclure.*

A quelles conditions est-ce un réseau?

Exercice 2. *On reprend les notations de l'exercice précédent avec* $K = \mathbb{R}$*. On note* μ *la mesure de Lebesgue de* $\mathbb{R}^n$*,* $(\epsilon_1, \cdots, \epsilon_n)$ *sa base canonique et* $(.|.)$ *le produit scalaire associé* $(\epsilon_i|\epsilon_j) = \delta_{i,j}$*. Pour* Γ *un réseau de* $\mathbb{R}^n$ *et* $\mathbf{e} = (e_1, \cdots, e_n)$ *une* $\mathbb{Z}$*-base de* Γ*, on pose*

- $P_{\mathbf{e},\Gamma} = \{\sum_{i=1}^n l_ie_i;\ l_1, \cdots, l_n \in [0,1]\}$*,*
- $D_{\mathbf{e},\Gamma} = \{\sum_{i=1}^n l_ie_i;\ l_1, \cdots, l_n \in [0,1[\}$*,*

On note $S_{\mathbf{e},\Gamma}$ *(resp.* $T_{\mathbf{e},\Gamma}$*) la matrice de terme général* $(e_i|e_j)$ *(resp.* $(\epsilon_i|e_j)$*).*

(a) Montrez que $S_{\mathbf{e},\Gamma} = {}^tT_{\mathbf{e},\Gamma}T_{\mathbf{e},\Gamma}$*. En utilisant la formule du jacobien pour le changement de variables dans les intégrales multiples, en déduire l'égalité* $\mu(P_{\mathbf{e},\Gamma}) = \sqrt{\det S_{\mathbf{e},\Gamma}}$*. Montrez ensuite que* $\mu(P_{\mathbf{e},\Gamma})$ *ne dépend que de* Γ *et non de* $\mathbf{e}$*; on dit que c'est la mesure du réseau et on la note* $\mu(\mathbb{R}^n/\Gamma)$*.*

(b) Une partie $\mathcal{D}$ *de* $\mathbb{R}^n$ *est un domaine fondamental de* Γ*, si* $\mathcal{D}$ *est* μ*-mesurable et si ses translatés par les vecteurs de* Γ *forment une partition de* $\mathbb{R}^n$*. Montrez que* $D_{\mathbf{e},\Gamma}$ *est un domaine fondamental et que* $\mu(\mathcal{D}) = \mu(\mathbb{R}^n/\Gamma)$ *pour tout domaine fondamental* $\mathcal{D}$ *de* Γ*.*

[1] i.e. tel que pour tout compact $\mathcal{K}$ de V, $\mathcal{K} \cap \Gamma$ est fini

[2] $[l]$ désigne la partie entière de l

(c) En utilisant le théorème de la base adaptée, montrez que si $\Lambda \subset \Gamma$ sont des réseaux alors Γ/Λ est fini et

$$\mu(\mathbb{R}^n/\Lambda) = \mathrm{card}(\Gamma/\Lambda)\mu(\mathbb{R}^n/\Gamma)$$

(d) (i) Soit $\psi : \mathbb{R}^n \longrightarrow \mathbb{R}^n/\Gamma$ la surjection canonique associé au réseau Γ et soit F une partie de $\mathbb{R}^n$, μ-mesurable vérifiant $\mu(F) > \mu(\mathbb{R}^n/\Gamma)$. Montrez que la restriction de ψ à F n'est pas injective.

(ii) Déduire de (i), le théorème de Minkowski: soient Γ un réseau de $\mathbb{R}^n$ et A une partie μ-mesurable, convexe, symétrique par rapport à O et vérifiant $\mu(A) > 2^n\mu(\mathbb{R}^n/\Gamma)$, alors $A \cap \Gamma \neq \{O\}$.

(iii) Montrez que si C est un convexe compact de $\mathbb{R}^n$, symétrique par rapport à O tel que $\mu(C) \geq 2^n\mu(\mathbb{R}^n/\Gamma)$ alors $C \cap \Gamma \neq \{O\}$.

(iv) Soit v_n le volume de la boule unité fermée de $\mathbb{R}^n$. Montrez qu'il existe $\gamma \in \Gamma$ différent de O et de norme inférieure ou égale à deux fois la racine n-ième de $v_n^{-1}\mu(\mathbb{R}^n/\Gamma)$.

Exercice 3. *Quelques applications arithmétiques (utiliser le point (iii) ci-dessus)*

(a) Soient $\epsilon > 0$ et $(\alpha_1, \cdots, \alpha_n) \in \mathbb{R}^n \backslash \mathbb{Q}^n$; montrez qu'il existe $p_1, \cdots, p_n \in \mathbb{Z}$ et $q \in \mathbb{N}$ non nul tels que pour tout $1 \leq i \leq n$, on ait $|\alpha_i - \frac{p_i}{q}| < \frac{\epsilon}{q}$.

Indication: considérez le groupe Γ engendré par les vecteurs de la base canonique et le vecteur $(\alpha_1, \cdots, \alpha_n)$ et remarquez que Γ n'est pas un réseau et n'est donc pas discret.

(b) Montrez que si $p \equiv 1 \mod 4$, p premier, alors p est somme de deux carrés.

Indication: (-1) étant un carré modulo p, soit $u \in \mathbb{Z}$ tel que $u^2 + 1 \equiv 0 \mod p$ et soit $\Gamma = \{(a, b) \in \mathbb{Z}^2 \ / \ a \equiv ub \mod p\}$. Soit $\psi : \mathbb{Z}^2 \longrightarrow \mathbb{Z}/p\mathbb{Z}$ défini par $\psi(a, b) = \overline{a - ub}$. Montrez que Γ est un réseau de mesure p et utilisez le point (d) (iv) de l'exercice précédent.

(c) Montrez que tout nombre premier p est somme de quatre carrés.

Indication: montrez l'existence d'un couple $(u, v) \in \mathbb{Z}^2$ tel que $u^2 + v^2 + 1 \equiv 0 \mod p$. On fixe un tel couple et soit $\Gamma = \{(a, b, c, d) \in \mathbb{Z}^4 \ / \ ua + vb \equiv c \mod p$ et $ub - va \equiv d \mod p\}$. Soit $\psi : \mathbb{Z}^4 \longrightarrow (\mathbb{Z}/p\mathbb{Z})^2$ défini par $\psi(a, b, c, d) = (\overline{c - ua - vb}, \overline{d + va - ub})$. Montrez que Γ est un réseau de $\mathbb{R}^4$ de mesure p^2 et utilisez le point (d) (iv) de l'exercice précédent.

2 Codes correcteurs

Pour transmettre une information on utilise l'alphabet $\mathbb{F}_q$; on envoie des messages de n lettres. Le principe des codes correcteurs d'erreurs est de pouvoir corriger des erreurs de transmission (cf. les CD, les transmissions par satellite...). L'ensemble des mots $\mathbb{F}_q^n$ peut être muni de la distance de Hamming définie comme suit: pour $(x_1, \cdots, x_n)$ et $(x'_1, \cdots, x'_n)$ dans $\mathbb{F}_q^n$ alors

$$d(x, x') := \mathrm{card}\{i \in [1, n] \ / \ x_i \neq x'_i\}$$

On vérifie aisément qu'il s'agit bien d'une distance.

Un code est un sous-ensemble $\mathcal{C} \subset \mathbb{F}_q^n$ comportant au moins deux éléments de $\mathbb{F}_q^n$; on définit la distance d'un code comme

$$d(\mathcal{C}) := \min_{x \neq x' \in \mathcal{C}} d(x, x').$$

Le principe consiste, une fois choisi un code $\mathcal{C}$, à n'envoyer que des messages avec des mots appartenant à $\mathcal{C}$; on peut alors repérer jusqu'à $d(\mathcal{C}) - 1$ erreurs de transmission sur un mot en outre si le nombre d'erreurs commises t est tel que $2t + 1 \leq d(\mathcal{C})$, on voit qu'il existe un seul mot de $\mathcal{C}$ situé à une distance $\leq t$ du mot reçu. Le code permet donc de corriger $t := \lfloor \frac{d(\mathcal{C})-1}{t} \rfloor$ erreurs. On introduit le taux de corrections $\frac{t}{n}$ et le taux d'information $\log \mathrm{card}(\mathcal{C})/n \log q$. La théorie de l'information développée par Shannon, indique que si l'on accepte d'envoyer des messages de plus en plus long, il existe des codes aussi sûrs que l'on veut avec un taux d'information proche de 1: cependant le théorème de Shannon est un théorème d'existence, il ne dit pas comment construire les codes en question.

Exercice 1. *On considère des codes cycliques, i.e. $\mathcal{C} \subset \mathbb{F}_q^n$ est un sous-espace vectoriel. Pour tout $x \in \mathcal{C}$, on définit son poids $\omega(x)$ comme le nombre de composantes non nulles.*

(1) Montrer que $d(\mathcal{C}) = \min_{0 \neq x \in \mathcal{C}} \min \omega(x)$.

*(2) **exemple du bit de parité:** pour transmettre $(x_1, \cdots, x_{n-1}) \in \mathbb{F}_2^{n-1}$ on envoie $x = (x_1, \cdots, x_{n-1}, x_1 + \cdots + x_{n-1}) \in \mathbb{F}_2^n$. Montrer qu'il s'agit d'un code cyclique qui permet de repérer une erreur mais pas de la corriger.*

*(3) **Code de Hamming:** prenons l'ensemble des mots de sept chiffres binaires, $q = 2$, $n = 7$ et $\mathcal{C}$ le code ayant pour base*

$$e_0 = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad e_1 = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad e_3 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix},$$

Pour transmettre un message $m = (m_0, m_1, m_2, m_3)$, on transmet $x = m_0e_0 + m_1e_1 + m_2e_2 + m_3e_3$. Expliquez le décodage dans le cas où une erreur au plus est commise.

Toujours en utilisant l'exemple précédent, montrer comment il est possible de retrouver un entier entre 0 et 15 à partir d'un élément de $\mathbb{F}_2^7$ si au plus une erreur est commise.

(4) Une matrice génératrice A d'un code $\mathcal{C}$ est une matrice dont les lignes forment une base. Une matrice vérificatrice B d'un code $\mathcal{C}$ est une matrice dont les lignes forment une base des formes linéaires s'annulant sur $\mathcal{C}$. Montrer que $A^tB = 0$ et que la distance du code $\mathcal{C}$ est le plus petit nombre d tel qu'il existe d vecteurs colonnes de B distincts et liés.

(5) Supposons un code $\mathcal{C}$ donné avec une matrice vérificatrice B et supposons que le code est 1-correcteur. Soit alors un message x' reçu différant du message envoyé x en au plus une coordonée: on note $\epsilon = x' - x$ l'erreur commise. Montrer comment calculer ϵ à l'aide de B.

(6) Soit $\mathcal{C}$ un code de longueur n sur $\mathbb{F}_q$. Donnez la distance et des matrices génératrices et vérificatrices des codes suivants:

*(i) **Code raccourci**: soit $d(\mathcal{C}) \leq l \leq n$, on pose $\mathcal{C}^{(l)} := \{x \in \mathbb{F}_q^l \ / \ (x; 0, \cdots, 0) \in \mathcal{C}\}$.*

*(ii) **Code étendu**: $\bar{\mathcal{C}} := \{(x_1, \cdots, x_{n+1}) \in \mathbb{F}_q^{n+1} \ / \ (x_1, \cdots, x_n) \in \mathcal{C} \text{ et } x_1 + \cdots + x_{n+1} = 0\}$.*

*(iii) **Code dual**: $\mathcal{C}^* := \{x' \in \mathbb{F}_q^n \ / \ \forall x \in \mathcal{C}, \ < x, x' >= 0\}$ où $<,>$ est le produit scalaire canonique.*

(7) Soit $\mathcal{C}$ un code de dimension k et de longueur n sur $\mathbb{F}_q$, montrer que $d(\mathcal{C}) \leq n + 1 - k$ et que si $\mathcal{C}$ est t-correcteur alors

$$1 + C_n^1(q-1) + C_n^2(q-1)^2 + \cdots + C_n^t(q-1)^t \leq q^{n-k}$$

Un code tel que $d(\mathcal{C}) = n + 1 - k$ sera dit MDS maximal distance separable. Un code t-correcteur tel que $\mathcal{C} = \bigcup_{x \in \mathcal{C}} B(x, t)$ est dit t-correcteur parfait.

Montrer que le code de Hamming de longueur 7 est 1-correcteur parfait mais qu'il n'est pas MDS.

Exercice 2. ***Codes linéaires cycliques; DEVOIR A RENDRE*** *Un code linéaire cyclique est un code $\mathcal{C}$ linéaire de longueur n, stable par la permutation $T(a_1, \cdots, a_n) = (a_n, a_1, \cdots, a_{n-1})$.*

(1) En utilisant l'isomorphisme naturel d'espace vectoriel $\psi : \mathbb{F}_q^n \simeq \mathbb{F}_q[X]/Q(X)$ où $Q = X^n - 1$, montrer que $\mathcal{C} \subset \mathbb{F}_q^n$ est stable par T si et seulement si son image par ψ est un idéal. En déduire alors qu'il existe une bijection entre les codes cycliques de longueur n et les polynômes unitaires divisant $X^n - 1$.

(2) Rappeler la factorisation en irréductibles des polynômes cyclotomiques Φ_n dans $\mathbb{F}_q$, et en déduire une bijection entre les codes cycliques de longueur n et les parties $I \subset (\mathbb{Z}/n\mathbb{Z})^\times$ stables par la multiplication par q.

(3) *Soit C un code linéaire cyclique de longueur n sur $\mathbb{F}_q$ associé à $I \subset (\mathbb{Z}/n\mathbb{Z})^\times$ et supposons qu'il existe i et s tels que $\{i+1, i+2, \cdots, i+s\} \subset I$. Montrer alors que $d(\mathcal{C}) \geq s+1$.*

(4) ***Codes de Hamming**: soit $n = \frac{q^r-1}{q-1}$ et $I := \{1, q, q^2, \cdots, q^{r-1}\}$. Montrer que $d(\mathcal{C}) = 3$ ou 4 et qu'il est parfait 1-correcteur.*

Remarque: Pour $r = 3$, $q = 2$ et $n = 7$ on retrouve le code étudié précédemment.

En construisant une matrice vérificatrice montrer qu'en fait on a $d(\mathcal{C}) = 3$.

(5) ***Codes de Reed-Solomon**: ce code est utilisé dans les CD. Soit $n = q-1$ et soit α un générateur de $\mathbb{F}_q^\times$. Pour k fixé on pose*

$$g(X) := \prod_{i=1}^{q-1-k} (X - \alpha^i)$$

Montrer que le code linéaire cyclique correspondant est MDS et que pour $q = 2^f$, on a $2t+1 \leq d(\mathcal{C}) = q-k$.

(6) ***Code ternaire de Golay**: on a $3^5 - 1 = 11.23$; on choisit $q = 3$, $n = 11$ et la partie de$(\mathbb{Z}/11\mathbb{Z})^\times$ engendrée par 3, i.e. $i = \{1, 3, 4, 5, 9\}$. On note $\mathcal{G}_{11}$ le code linéaire cyclique correspondant. Montrer que $d(\mathcal{G}_{11}) = 4, 5$ puis que $\mathcal{G}_{11}$ est 2-correcteur parfait (il n'est pas MDS).*

(7) ***Code binaire de Golay**: on a $2^{11} - 1 = 23.89$, on choisit $q = 2$, $n = 23$ et $I = (2) \subset (\mathbb{Z}/23\mathbb{Z})^\times$.On note $\mathcal{G}_{23}$ le code linéaire cyclique correspondant. Montrer que $d(\mathcal{G}_{2^n}) = 5, 6, 7$ puis que $\mathcal{G}_{23}$ est "-correcteur parfait.*

3 Quelques équations diophantiennes

Exercice 1. *On considère l'équation $y^2 = x^3 + 7$:*

(i) *Montrez qu'il n'y a pas de solutions avec x pair;*

(ii) *En écrivant l'équation sous la forme $y^2 + 1 = x^3 + 8 = (x+2)(x^2 - 2x + 4)$ et en utilisant l'exercice 1 b, déduisez en qu'il n'existe pas de solutions entières.*

Exercice 2. *Soit $A = \mathbb{Z}[i\sqrt{2}] = \{a + ib\sqrt{2} \ / \ (a,b) \in \mathbb{Z}^2\}$. On définit pour $z = a + ib\sqrt{2} \in A$, $N(z) = a^2 + 2b^2$.*

(a) *Montrez que B est euclidien et donc factoriel.*

(b) *Soient $(x, y) \in \mathbb{Z}^2$, vérifiant l'équation $y^2 + 2 = x^3$. Montrez que x est impair puis que dans B, $y + i\sqrt{2}$ et $y - i\sqrt{2}$ sont premiers entre eux. En déduire qu'il existe $(a, b) \in \mathbb{Z}^2$ tels que $x = a^2 + 2b^2$ et $y + i\sqrt{2} = (a + ib\sqrt{2})^3$, puis décrire les solutions de l'équation précédente.*

(c) *Étudiez comme dans l'exercice précédent l'ensemble $S = \{n \in \mathbb{N} \ / \ \exists (x, y) \in \mathbb{Z}^2, \ n = x^2 + 2y^2\}$.*
Indication: on utilisera que -2 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $p \equiv 1, 3 \mod 8$.

(d) *Étudiez de même l'ensemble $\{n \in \mathbb{Z} \ / \ \exists (x, y) \in \mathbb{Z}^2, \ n = x^2 - 2y^2\}$.*

Exercice 3. *Étude de l'équation de Pell-Fermat: $x^2 - Ny^2 = 1$.*

(i) *Traitez le cas $N \leq 0$.*

(ii) *Montrez que dans le cas où N est un carré parfait, les solutions triviales $x = \pm 1, y = 0$ sont les seules.*

(iii) *On suppose donc $N > 1$ et N n'est pas un carré parfait. En utilisant l'anneau $\mathbb{Z}[\sqrt{N}]$, montrez l'égalité:*

$$(x_1^2 - Ny_1^2)(x_2^2 - Ny_2^2) = (x_1x_2 + Ny_1y_2)^2 - N(x_1y_2 + x_2y_1)^2$$

En déduire que s'il existe un solution non triviale (x_0, y_0) à l'équation de Pell-Fermat, alors il en existe une infinité (x_n, y_n) définie par récurrence:

$$\begin{cases} x_{n+1} = x_0x_n + Ny_0y_n \\ y_{n+1} = x_0y_n + x_ny_0 \end{cases}$$

Calculez par exemple pour $N = 2$, les 3 premiers termes de cette suite en remarquant que $(3, 2)$ est solution.

(iv) Montrez que pour (x_1, y_1) et (x_2, y_2) des solutions positives de l'équation, les équivalences

$$x_1 < x_2 \Leftrightarrow y_1 < y_2 \Leftrightarrow (x_1 + y_1\sqrt{N}) < (x_2 + y_2\sqrt{N})$$

En déduire que s'il existe des solutions non triviales alors il existe une solution minimale (x_0, y_0) pour une relation d'ordre que l'on définira. Montrez ensuite que l'ensemble des solutions sont les (x_n, y_n) définis ci-dessus.

(v) On veut montrer l'existence d'une solution non triviale. Montrez qu'il existe une infinité de rationnels p/q tels que $|\sqrt{N} - p/q| < 1/q^2$.

Indication: commencez par remarquer que p ou $p-1$ est la partie entière de $q\sqrt{N}$, puis appliquez le principe des chaussettes et des tiroirs ($n+1$ chaussettes rangées dans n tiroir, implique qu'un tiroir contient au moins deux chaussettes), où les chaussettes sont les $n\sqrt{N} - [n\sqrt{N}]$ pour $0 \leq n \leq q$ et les tiroirs sont les intervalles $[k/q, (k+1) : q]$ pour $0 \leq k < q$.

En déduire qu'il existe une infinité de couples $(p, q) \in \mathbb{N}^2$ premiers entre eux tels que $-1-2\sqrt{N} < p^2 - Nq^2 < 1+2\sqrt{N}$. En utilisant à nouveau le principe des tiroirs, montrez qu'il existe un entier $l < 1+2\sqrt{N}$, $p_1 \equiv p_2 \mod l$, $q_1 \equiv q_2 \mod l$ tels que $p_1^2 - Nq_1^2 = p_2^2 - Nq_2^2 = \pm l$, et en déduire l'existence d'une solution non triviale.