CODES ET RÉSEAUX

par

Anne Quéguiner-Mathieu

Résumé. — Ce texte, très largement inspiré du chapitre I du livre de Wolfgang Ebeling 'Lattices and codes', correspond à la première partie d'un cours de master donné à la Faculté des Sciences et Techniques de l'Université de Bamako, en mars 2007. L'objectif est d'introduire les notions de code et de réseau, et d'expliquer en partie les liens qui existent entre ces deux types d'objets.

Dans un deuxième temps, en visio-conférence, nous étudierons les réseaux de racines et leurs diagrammes de Dynkin.

Introduction

L'objectif de la théorie des codes correcteurs d'erreurs est de fabriquer des codes efficaces, c'est-à-dire permettant de transmettre l'information de façon à la fois fiable et relativement peu couteuse en mémoire, et donc en temps de transmission. Comme cela se produit souvent, certains problèmes de théorie des codes sont liés à des questions étudiées par ailleurs et de manière totalement indépendante dans d'autres branches des mathématiques. Ainsi, il existe des liens entre la théorie des codes et l'étude des réseaux, i.e. des sous-groupes discrets de $\mathbb{R}^n$ à quotient compact. Ce sont ces liens que nous souhaitons introduire dans ce document.

Table des matières

1. Formes quadratiques sur un corps

1.1. Définitions. — Dans tout ce qui suit, $\mathbb{K}$ désigne un corps commutatif, de caractéristique différente de 2.

1.1.1. Définition par les polynômes. — Les formes quadratiques peuvent être définis de différentes façons. Nous allons commencer par adopter le point de vue des polynômes.

Définition 1.1. — Une forme quadratique de dimension n sur le corps $\mathbb{K}$ est un polynôme homogène de degré 2 en les indéterminées $X_1, \dots, X_n$.

La forme générale d'un tel polynôme est $f(X_1, \dots, X_n) = \sum_{1 \leq i \leq j \leq n} \alpha_{i,j} X_i X_j$. On peut rendre l'écriture symétrique en écrivant, pour $i < j$,

$$\alpha_{i,j} X_i X_j = \frac{\alpha_{i,j}}{2}(X_i X_j + X_j X_i).$$

Ainsi, un tel polynôme s'écrit de façon unique sous la forme $f(X_1, \dots, X_n) = \sum_{i,j=1}^{n} a_{i,j} X_i X_j$, avec pour tout $i \neq j$, $a_{i,j} = a_{j,i}$. Autrement dit, f détermine une unique matrice symétrique $M_f = (a_{i,j})$ telle que

$$f(X_1, \dots, X_n) = (X_1, \dots, X_n) M_f \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}.$$

Exemple 1.2. — Ecrire la matrice M_f associée au polynôme $f(X_1, X_2, X_3) = X_1^2 + 2X_2^2 + 4X_3^2 + X_1X_2 + 2X_1X_3 + X_2X_3 + 3X_3X_2$.

1.1.2. Application polynôme associée. — Le polynôme f ci-dessus détermine une application $\tilde{f} : \mathbb{K}^n \to \mathbb{K}$, $x = (x_1, \dots, x_n) \mapsto f(x_1, \dots, x_n)$. Cette application possède les deux propriétés suivantes:
(a) $\forall \lambda \in \mathbb{K}$, $\tilde{f}(\lambda x) = \lambda^2 \tilde{f}(x)$.
(b) L'application $b_{\tilde{f}} : \mathbb{K}^n \times \mathbb{K}^n \to \mathbb{K}$ définie par $b_{\tilde{f}}(x, y) = \frac{1}{2}(\tilde{f}(x + y) - \tilde{f}(x) - \tilde{f}(y))$ est une forme bilinéaire.
La propriété (a) est une conséquence du fait que f est homogène de degré 2. La propriété (b) se démontre par un calcul direct. Si l'on utilise, par exemple, l'écriture matricielle, on observe que

$$\begin{aligned} b_{\tilde{f}}(x, y) = & \ \frac{1}{2}\Big((x_1, \dots, x_n) M_f \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} + (y_1, \dots, y_n) M_f \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}\Big) \\ & = \sum_{i,j=1}^{n} a_{i,j} x_i y_j = (x_1, \dots, x_n) M_f \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}. \end{aligned}$$

La forme $b_{\tilde{f}}$ est donc bien linéaire en x et en y.

Exemple 1.3. — Si f est le polynôme de l'exemple 1.2 ci-dessus, l'application $b_{\tilde{f}}$ associée est donnée par

$$b_{\tilde{f}}(x, y) = x_1y_1 + 2x_2y_2 + 4x_3y_3 + \frac{1}{2}(x_1y_2 + x_2y_1) + (x_1y_3 + x_3y_1) + 2(x_2y_3 + x_3y_2).$$

L'application associée à un polynôme est bien sur entièrement déterminé par le polynôme. En général, la réciproque est fausse. Ainsi, sur le corps fini $\mathbb{F}_q$, les polynômes $X^q - X$ et 0 sont distincts, et ont pourtant tous deux la fonction nulle comme fonction polynôme associée.

Dans le cas qui nous intéresse ici, pourtant, on peut retrouver le polynôme f à partir de l'application $\tilde{f}$. En effet, l'application $\tilde{f}$ détermine $b_{\tilde{f}}$, et celle-ci permet de retrouver la matrice $M_f = (a_{i,j})$, et donc les coefficients du polynôme f. Si $(e_1, \ldots, e_n)$ désigne la base canonique de $\mathbb{K}^n$, l'écriture matricielle ci-dessus montre que $a_{i,j} = b_{\tilde{f}}(e_i, e_j)$.

1.1.3. Une autre définition. — Ceci nous amène à une nouvelle définition de la notion de forme quadratique:

Définition 1.4. — Une forme quadratique sur le corps $\mathbb{K}$ est un couple (V, q) formé d'un $\mathbb{K}$-espace vectoriel de dimension finie V et d'une application $q : V \to \mathbb{K}$ telle que
(a) $\forall x \in V$ et $\lambda \in \mathbb{K}$, $q(\lambda x) = \lambda^2 q(x)$
(b) l'application $b_q : V \times V \to \mathbb{K}$ définie par $b_q(x, y) = \frac{1}{2}(q(x + y) - q(x) - q(y))$ est une forme bilinéaire.

Exemple 1.5. — Soit f un polynôme homogène de degré 2 en n variables. Le couple $(\mathbb{K}^n, \tilde{f})$ est une forme quadratique sur $\mathbb{K}$.

Remarque 1.6. — La nouvelle définition proposée ici est bien équivalente à la précédente. En effet, si $(e_1, \ldots, e_n)$ est une base de V, la linéarité de b_q implique que pour tout vecteur $x = x_1 e_1 + \cdots + x_n e_n$, on a $q(x) = b_q(x_1 e_1 + \cdots + x_n e_n, x_1 e_1 + \cdots + x_n e_n) = \sum_{i,j=1}^{n} x_i x_j b_q(e_i, e_j)$. La forme quadratique q est donc bien une application polynôme homogène de degré 2.

1.1.4. Forme polaire d'une forme quadratique. — L'application $(x, y) \mapsto b_q(x, y)$ est une forme bilinéaire symétrique sur V. On l'appelle la forme polaire de q. On peut retrouver la forme quadratique q à partir de b_q par $q(x) = b_q(x, x)$. Ceci établit une correspondance bijective entre les formes quadratiques et les formes bilinéaires symétriques.

Remarque 1.7. — L'hypothèse sur la caractéristique de $\mathbb{K}$ est ici essentielle. En caractéristique 2, on peut définir de manière analogue des formes quadratiques et des formes bilinéaires symétriques, mais ces deux notions ne sont pas équivalentes.

1.1.5. Equivalence de formes quadratiques. —

Définition 1.8. — Soient (V, q) et (V', q') deux espaces quadratiques sur $\mathbb{K}$. Un morphisme métrique de (V, q) dans (V', q') est une application linéaire $f : V \to V'$ telle que $q' \circ f = q$.

On a alors $b_{q'}(f(x), f(y)) = b_q(x, y)$. Un morphisme métrique respecte donc également les formes polaires de q et de q'.

Définition 1.9. — Les espaces quadratiques (V, q) et (V', q') sont isométriques s'il existe un morphisme métrique bijectif (qu'on appellera isomorphisme ou isométrie) entre les deux.

L'objectif de la théorie des formes quadratiques est d'étudier les formes quadratiques à isométrie près. L'une des questions centrales est donc la suivante: étant données deux formes quadratiques, comment peut-on savoir si elles sont isomorphes. C'est une question très difficile en général, à laquelle le théorème de Milnor-Voevodsky, qui dépasse largement le cadre de ces notes, répond en partie. Sur certains corps, cependant, on dispose d'un

système complet d'invariants qui permet de répondre à cette question. C'est le cas par exemple sur $\mathbb{C}$, $\mathbb{R}$, les corps finis, les corps p-adiques et $\mathbb{Q}$.

1.2. Ecriture matricielle. —

1.2.1. Matrice d'une forme quadratique. —

Définition 1.10. — Soit $(e_1, \dots, e_n)$ une base de V. La matrice de q par rapport à cette base est la matrice symétrique $B = (b_q(e_i, e_j))$.

Exemple 1.11. — Soit $\tilde{f}$ une fonction polynôme homogène de degré 2. La matrice de $(\mathbb{K}^n, \tilde{f})$ par rapport à la base canonique est la matrice M_f introduite au § 1.1.1.

Proposition 1.12. — *Soit B la matrice de q par rapport à la base $(e_1, \dots, e_n)$, et X et Y les vecteurs colonnes correspondant dans cette base aux vecteurs x et $y \in V$. On a alors*

$$q(x) = {}^tXBX \quad et \quad b_q(x, y) = {}^tXBY.$$

Démonstration. — La première égalité est une conséquence évidente de la seconde, qui, quant à elle, découle de la bilinéarité de b_q et de la définition de B. En effet, si $x = x_1e_1 + \cdots + x_ne_n$ et $y = y_1e_1 + \cdots + y_ne_n$, alors $b_q(x, y) = \sum_{i,j=1}^n x_iy_jb_q(e_i, e_j)$. □

Remarque 1.13. — En réalité, ce calcul a déjà été fait au § 1.1.2 dans le cas d'une application polynomiale $\tilde{f}$. Comme toute forme quadratique est une application polynomiale, la proposition en découle.

1.2.2. Changement de base. — Soient $\mathcal{E}$ et $\mathcal{E}'$ deux bases de V. Rappelons que la matrice de passage P de $\mathcal{E}$ à $\mathcal{E}'$ est la matrice dont les colonnes donnent les coordonnées dans $\mathcal{E}$ des vecteurs $(e'_1, \dots, e'_n)$ de $\mathcal{E}'$. Si le vecteur $x \in V$ correspond respectivement aux vecteurs colonnes X et X' dans $\mathcal{E}$ et $\mathcal{E}'$, on a alors $X = PX'$. On en déduit:

Proposition 1.14. — *La matrice B' de q dans la base $\mathcal{E}'$ s'obtient à partir de la matrice B de q dans la base $\mathcal{E}$ par*

$$B' = {}^tPBP.$$

Démonstration. — On a en effet $b_q(x, y) = {}^tX'B'Y' = {}^tXBY = {}^tX'{}^tPBPY'$. Ainsi, quels que soient les vecteurs colonnes X' et Y', on a ${}^tX'B'Y' = {}^tX'{}^tPBPY'$. La proposition découle alors du lemme qui suit:

Lemme 1.15. — *Soient P et Q deux matrices de $M_n(\mathbb{K})$. Elles sont égales si et seulement si pour tous vecteurs colonnes X et Y on a ${}^tXPY = {}^tXQY$.*

Démonstration. — L'une des implications est claire. Pour montrer l'autre, il suffit d'appliquer l'égalité ${}^tXPY = {}^tXQY$ aux vecteurs de la base canonique de $\mathbb{K}^n$. On en déduit que les matrices P et Q ont les mêmes coefficients. □

Remarque 1.16. — Notons que comme B est symétrique, la matrice ${}^tPBP$ l'est également.

1.2.3. Isométries. — Dorénavant, (V, q) désigne un espace quadratique sur $\mathbb{K}$, et B est sa matrice dans une base donnée $\mathcal{E}$ de V. De même pour (V', q'), B' et $\mathcal{E}'$.

Proposition 1.17. — *Soit $f : V \to V'$ une application linéaire dont la matrice par rapport aux bases $\mathcal{E}$ et $\mathcal{E}'$ est notée A. Alors, f est un morphisme métrique si et seulement si $B = {}^tAB'A$.*

Démonstration. — L'application f est métrique si et seulement si pour tous vecteurs x et y de V, on a $b'(f(x), f(y)) = b(x, y)$. Matriciellement, ceci signifie que pour tous vecteurs colonnes X et Y, on a ${}^t(AX)B'(AY) = {}^tXBY$, soit ${}^tX({}^tAB'A)Y = {}^tXBY$. Par le lemme 1.15, ceci équivaut à ${}^tAB'A = B$. □

De cette proposition, on déduit maintenant le théorème qui suit:

Théorème 1.18. — *Il y a équivalence entre*
(i) Les espaces quadratiques (V, q) et (V', q') sont isométriques;
(ii) Les matrices de q et q' par rapport à des bases bien choisies sont égales;
(iii) Les matrices de q et de q' par rapport à des bases arbitraires sont congruentes.

Démonstration. — Soit $f : V \to V'$ une isométrie entre les deux espaces quadratiques. On se donne une base $\mathcal{E} = (e_1, \ldots, e_n)$ de V et on considère la base $(f(e_1), \ldots, f(e_n))$ correspondante de V'. On a alors $b_{q'}(f(e_i), f(e_j)) = b_q(e_i, e_j)$, ce qui prouve (ii).
L'implication (ii) $\Rightarrow$ (iii) est une conséquence immédiate de la proposition de changement de base du § 1.2.2.
Supposons finalement que les matrices B et B' sont congruentes, $B' = {}^tPBP$, pour une certaine matrice inversible P. Soit $f : V \to V'$ l'application linéaire bijective dont la matrice par rapport aux bases $\mathcal{E}$ et $\mathcal{E}'$ est P^{-1}. Par la proposition précédente, c'est un morphisme métrique entre q et q'. La matrice P^{-1} étant inversible, f est une isométrie. □

1.2.4. Groupe orthogonal. —

Définition 1.19. — On appelle groupe orthogonal de l'espace quadratique (V, q) le groupe des isométries de (V, q) dans lui-même. C'est un sous-groupe du groupe $GL(V)$ des applications linéaires bijectives de V dans lui-même.

Fixons une base $\mathcal{E}$ de V et notons B la matrice de b dans cette base. Le choix de $\mathcal{E}$ permet d'identifier $GL(V)$ au groupe $GL_n(\mathbb{K})$ des matrices inversibles de $M_n(\mathbb{K})$. Via cette identification, le groupe orthogonal $O(V, q)$ correspond à $\{P \in GL_n(\mathbb{K}),\ {}^tPBP = B\}$.

1.3. Orthogonalité, régularité et diagonalisation. —

1.3.1. Orthogonalité. —

Définition 1.20. — Les deux vecteurs x et $y \in V$ sont dits orthogonaux ($x \perp y$) si $b_q(x, y) = 0$.
Le vecteur x est orthogonal au sous-espace $U \subset V$ s'il est orthogonal à tout vecteur de U. Les deux sous-espaces U et $W \subset V$ sont dits orthogonaux ($U \perp W$) si tout vecteur de l'un est orthogonal à tout vecteur de l'autre.
Soit $U \subset V$ un sous-espace de V. On appelle orthogonal de U le sous-espace

$$U^\perp = \{x \in V,\ \forall u \in U\ b_q(x, u) = 0\}.$$

Définition 1.21. — Soient V_1 et V_2 deux sous-espaces vectoriels de V. On dit que V est la somme directe orthogonale de V_1 et V_2 ($V = V_1 \perp V_2$) si $V = V_1 \oplus V_2$ et $V_1 \perp V_2$.

Notons que pour tout sous-espace vectoriel $W \subset V$, la forme quadratique q induit par restriction une forme quadratique $q_W : W \to \mathbb{K}$. Si $V = V_1 \perp V_2$, et si l'on note q_i la restriction de q à V_i, on a $q(v_1 + v_2) = q_1(v_1) + q_2(v_2)$, quel que soit $v = v_1 + v_2 \in V$. On dit alors que l'espace quadratique (V, q) est la somme directe orthogonale des espaces (V_1, q_1) et (V_2, q_2).
Matriciellement, ceci signifie que si l'on se place dans une base de V formée de la réunion d'une base de V_1 et d'une base de V_2, la matrice de q est une matrice diagonale par blocs $B = \begin{pmatrix} B_1 & 0 \\ 0 & B_2 \end{pmatrix}$, où B_i désigne la matrice de q_i dans la base de V_i choisie.

1.3.2. Régularité. —

Définition 1.22. — L'espace quadratique (V, q) est dit régulier si $V^\perp = \{0\}$.

Autrement dit, (V, q) est régulier si et seulement si pour tout $x \in V$, $x \neq 0$, il existe $y \in V$ tel que $b_q(x, y) \neq 0$. Dans le cas contraire, on dit que (V, q) est dégénéré.

Proposition 1.23. — *L'espace quadratique (V, q) est régulier si et seulement si sa matrice dans une base quelconque de V est inversible.*

Démonstration. — Soit $V^\star = Hom_{\mathbb{K}}(V, \mathbb{K})$ le dual de V. A l'espace quadratique (V, q) on peut associer une application $\hat{b} : V \to V^\star$, $x \mapsto b(x, \ )$. Clairement, (V, q) est régulier si et seulement si $\hat{b}$ est injective (et donc bijective). Or la matrice de $\hat{b}$ par rapport à une base fixée de V et la base duale associée de $V^\star$ est la matrice B de la forme quadratique q. En effet, si $x = x_1e_1 + \cdots + x_ne_n = e_1^\star(x)e_1 + \cdots + e_n^\star(x)e_n$, alors $\hat{b}(e_i)(x) = b(e_i, x) = \sum_{j=1}^n b(e_i, e_j)e_i^\star(x)$. D'où $\hat{b}(e_i) = \sum_{j=1}^n b(e_i, e_j)e_i^\star$. □

Quand l'espace quadratique (V, q) n'est pas régulier, on peut toujours le décomposer en une somme directe d'un espace quadratique de forme nulle et d'un espace quadratique régulier (qu'on appelle la partie régulière de (V, q)). C'est l'objet du théorème qui suit:

Théorème 1.24. — *Soit (V, q) un espace quadratique. On considère un supplémentaire (quelconque) W de $V^\perp$. On a alors :*
(i) $V = V^\perp \perp W$;
(ii) L'espace W, muni de la forme induite q_W est régulier;
(iii) L'espace quadratique (W, q_W) est déterminé à isométrie près par (V, q).

Démonstration. — Le point (i) est clair.
Pour le point (ii), notons que tout vecteur de V est orthogonal à $V^\perp$. Si le vecteur $w \in W$ est orthogonal à tout vecteur de W, il est alors orthogonal à tout vecteur de $V^\perp \oplus W = V$. Il est donc en réalité dans $V^\perp$. Mais par hypothèse $V^\perp \cap W = \{0\}$. Ceci prouve que (W, q_W) est régulier.
Enfin, considérons un autre supplémentaire $W' \subset V$ de $V^\perp$ dans V. Comme $V = V^\perp \oplus W'$, tout vecteur $w \in W$ s'écrit de manière unique sous la forme $w = x + w'$, où $x \in V^\perp$ et $w' \in W'$. L'application $W \to W'$, $w \mapsto w'$ est en réalité la restriction à W de la projection sur W' parallèlement à $V^\perp$. C'est donc une application linéaire. Elle est clairement injective, donc bijective par un argument de dimension. Il reste à vérifier qu'elle préserve

la forme quadratique q. Mais $q(w) = q(x + w') = q(x) + 2b(x, w') + q(w') = q(w')$ puisque $x \in V^\perp$. □

Définition 1.25. — L'espace (W, q_W) est appelé la partie régulière de V.

Il découle du théorème que

Corollaire 1.26. — *Deux espaces quadratiques sont isomorphes si et seulement si ils ont la même dimension et des parties régulières isomorphes.*

Démonstration. — Deux espaces isomorphes ont clairement la même dimension et des parties régulières isomorphes. Montrons la réciproque.
Soient donc $V = V^\perp \perp W$ et $V' = V'^\perp \perp W'$ deux espaces décomposés comme ci-dessus. Par hypothèse, il existe un isomorphisme $\beta : W \to W'$. Par un argument de dimension, il existe une application linéaire bijective $\alpha : V^\perp \to V'^\perp$; la restriction des formes étant nulle dans les deux cas, c'est une isométrie. L'application $\alpha \oplus \beta$ est alors une isométrie entre (V, q) et (V', q'). □

Ainsi, si on souhaite classifier les formes quadratiques, il suffit en fait de considérer les formes régulières.

1.3.3. Sous-espaces réguliers. —

Remarque 1.27. — Notons qu'un sous-espace d'un espace quadratique régulier, muni de la forme induite, n'est pas nécessairement régulier. Il est facile, en effet, d'extraire une sous-matrice non inversible d'une matrice inversible. Considérons par exemple la forme quadratique q sur un espace de dimension 2 définie par la matrice $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Autrement dit, on a $q(e_1) = q(e_2) = 0$ et $b(e_1, e_2) = 1$. C'est une forme quadratique régulière. Pourtant, la restriction de cette forme à l'une des droites $\mathbb{K}e_1$ et $\mathbb{K}e_2$ est la forme nulle, qui elle, est non régulière (on dit aussi dégénérée).

On peut caractériser les sous-espaces réguliers d'un espace quadratique de la manière suivante:

Proposition 1.28. — *Soit $W \subset V$ un sous-espace vectoriel de l'espace quadratique (V, q). Il est régulier si et seulement si $W \cap W^\perp = \{0\}$.*

Démonstration. — Attention : la notation $W^\perp$ désigne l'ensemble des vecteurs orthogonaux à W dans l'espace vectoriel dans lequel on travaille. Ici, $W^\perp$ désigne donc l'ensemble des vecteurs de V qui sont orthogonaux à W. Par définition de la régularité, l'espace W muni de la forme induite est donc régulier si aucun de ces vecteurs n'est dans W, i.e. si $W \cap W^\perp = \{0\}$. □

Exemple 1.29. — Soit x un vecteur de V. Il est dit anisotrope si $q(x) \neq 0$. La droite $\mathbb{K}x$ est régulière si et seulement x est anisotrope.

Les sous-espaces réguliers d'un espace quadratique ont la propriété remarquable suivante:

Théorème 1.30. — *Soit (V, q) un espace quadratique et $W \subset V$ un sous-espace vectoriel. Si W est régulier, alors $V = W \perp W^\perp$. En particulier,* $\dim W^\perp = \dim V - \dim W$.

Démonstration. — Comme $W \perp W^\perp$, il suffit de montrer que $V = W \oplus W^\perp$.
On a déjà vu que $W \cap W^\perp = \{0\}$, de sorte que les deux sous-espaces sont en somme directe.
Il reste à montrer que $V = W + W^\perp$. Soit donc $v \in V$. Considérons la forme linéaire associée, $\hat{b}(v) : x \in V \mapsto b(v,x)$. Comme la restriction de b à W est non dégérérée, il existe un vecteur $w \in W$ tel que la restriction de $\hat{b}(v)$ à W est égale à $\hat{b}_W(w)$. Autrement dit, quel que soit $y \in W$, on a $\hat{b}(v)(y) = \hat{b}_W(w)(y)$ i.e. $b(v,y) = b_W(w,y)$. Le vecteur $v - w$ appartient donc à l'orthogonal de W et ceci prouve que $v = w + (v - w)$ appartient bien à $W + W^\perp$. □

1.3.4. Diagonalisation. — Le résultat précédent va nous permettre de montrer le résultat fondamental suivant:

Théorème 1.31. — *Soit (V,q) un espace quadratique. Il existe une base de V constituée de vecteurs deux à deux orthogonaux. Un telle base est appelée une base orthogonale de V. La matrice de q dans une base orthogonale de V est une matrice diagonale.*

Exemple 1.32. — On note $\mathbb{H}$ l'espace $\mathbb{K}^2$ muni de la forme quadratique dont la matrice dans la base canonique est $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Trouver une base orthogonale de $\mathbb{H}$.

Démonstration. — On procède par induction sur la dimension de l'espace vectoriel V. Si V est de dimension 1, le résultat est clair. Supposons le connu en dimension n et soit V un espace de dimension $n+1$ muni d'une forme quadratique q. Si q est la forme nulle, alors b est également nulle, et toute base est orthogonale. Sinon, il existe un vecteur $x \in V$ tel que $q(x) \neq 0$. La droite $W = \mathbb{K}x$ est alors régulière, et par le théorème précédent, on a $V = W \perp W^\perp$. Soit $(e_1, \ldots, e_n)$ une base orthogonale de $W^\perp$ muni de la forme quadratique induite par q. La base $(x, e_1, \ldots, e_n)$ de V est une base orthogonale de (V,q). □

Remarque 1.33. — Revenons un instant au point de vue des polynômes. Le théorème ci-dessus montre que tout polynôme f homogène de degré 2 peut se ramener, après un changement linéaire inversible de variables, à un polynôme 'diagonal', c'est-à-dire de la forme $a_1X_1^2 + \cdots + a_nX_n^2$. La forme quadratique correspondante de l'espace vectoriel $\mathbb{K}^n$ sera notée $\langle a_1, \ldots, a_n \rangle$.

Remarque 1.34. — On a en réalité montré un résultat plus précis. Quel que soit le vecteur $x \in V$ tel que $q(x) \neq 0$, il existe une base orthogonale de V qui commence par le vecteur x. La forme quadratique q admet donc une diagonalisation qui commence par $q(x)$.
Ainsi, par exemple, la forme quadratique $\langle 1, 1 \rangle$ admet une diagonalisation de la forme $\langle 2, a \rangle$. (Exercice : trouver la valeur de a).

2. Formes quadratiques sur $\mathbb{R}$ et $\mathbb{C}$

Dans tout ce paragraphe, on ne considère que des espaces quadratiques réguliers. On a vu que ceci était suffisant pour étudier les questions de classifications.

2.1. Rang et déterminant d'une forme quadratique. — On va ici introduire deux invariants classiques des formes quadratiques sur un corps $\mathbb{K}$ (de caractéristique différente de 2, mais pas nécessairement $\mathbb{R}$ ou $\mathbb{C}$ pour le moment).

Définition 2.1. — Soit (V, q) un espace quadratique.
Le rang de (V, q) est la dimension de l'espace vectoriel V.
Le déterminant de (V, q) est la classe dans $\mathbb{K}^\star/\mathbb{K}^{\star 2}$ du déterminant de la matrice de q dans une base quelconque de V.

Comme le déterminant de ${}^tPBP$ vaut $\det(B)\det(P)^2$, la classe dans $\mathbb{K}^\star/\mathbb{K}^{\star 2}$ du déterminant de la matrice de q ne dépend pas de la base choisie.
Deux formes quadratiques isométriques ont clairement le même rang et le même déterminant. On dit que le rang et le déterminant d'une forme quadratique sont des invariants. (Ils ne dépendent que de la classe d'isométrie de la forme quadratique).

2.2. Classification sur $\mathbb{C}$. —

Théorème 2.2. — *Deux formes quadratiques complexes sont isométriques si et seulement si elles ont le même rang.*

On dit que le rang est un *invariant complet* pour les formes quadratiques sur $\mathbb{C}$.

Démonstration. — Remarquons que le déterminant n'intervient pas ici. Ce n'est en fait pas étonnant. Le groupe $\mathbb{C}^\star/\mathbb{C}^{\star 2} = \{\bar{1}\}$; le déterminant est donc un invariant trivial.
Soit (V, q) un espace quadratique de dimension n sur $\mathbb{C}$ et $(e_1, \ldots, e_n)$ une base orthogonale de (V, q). Notons $a_i = q(e_i)$. Comme q est régulière, son déterminant est $a_1 \ldots a_n \neq 0$, de sorte que les a_i sont non nuls. Soit $\alpha_i \in \mathbb{C}^\star$ une racine carrée de a_i. La base $(\frac{e_1}{\alpha_1}, \ldots, \frac{e_n}{\alpha_n})$ est toujours orthogonale, et q correspond dans cette nouvelle base à la forme diagonale $\langle 1, \ldots, 1\rangle$. Cette diagonalisation ne dépend que du rang du la forme q. Par le théorème 1.18, ceci termine la preuve. □

2.3. Classification sur $\mathbb{R}$. —

Exemple 2.3. — On considère les formes quadratiques réelles $\langle 1, 1, 1, 1\rangle$ et $\langle 1, 1, -1, -1\rangle$. Elles ont même rang et même déterminant. Pourtant, elles ne sont pas isomorphes. (L'une d'entre elles est isotrope, c'est-à-dire prend la valeur 0 pour un vecteur non nul $x \in \mathbb{R}^4$ bien choisi, tandis que l'autre est anisotrope).

Pour distinguer les formes quadratiques réelles, on a besoin d'un invariant plus fin que le déterminant, à savoir la signature.

Définition 2.4. — L'espace quadratique réel (V, q) est dit positif (respectivement défini positif) si pour tout $x \in V$, $q(x) \geq 0$ (resp. pour tout x non nul de V, $q(x) > 0$).

Théorème 2.5. — *Soit (V, q) un espace quadratique réel (régulier). On peut décomposer V en une somme directe orthogonale $V = V^+ \perp V^-$ de telle sorte que V^+ muni de la forme induite est défini positif et V^- muni de la forme induite est défini négatif.*
Les dimensions r^+ et r^- de V^+ et V^- ne dépendent pas de la décomposition choisie.

Démonstration. — Montrons tout d'abord l'existence d'une telle décomposition. Pour cela, on diagonalise la forme quadratique q. Quitte à ré-ordonner la base, on peut supposer que $q(e_1), \dots, q(e_i)$ sont strictement positifs et $q(e_{i+1}), \dots, q(e_n)$ sont strictement négatifs. Les sous-espaces $V^+ = \mathbb{R}e_1 \oplus \cdots \oplus \mathbb{R}e_i$ et $V^- = \mathbb{R}e_{i+1} \oplus \cdots \oplus \mathbb{R}e_n$ conviennent.
Supposons maintenant que $V = W^+ \oplus W^-$ est une autre décomposition satisfaisant les mêmes conditions. Clairement, vues les valeurs de la forme q sur ces sous-espaces, on a $W^+ \cap V^- = \emptyset$. D'où $\dim(W^+) \leq \dim(V) - \dim(V^-) = \dim(V^+)$. Mais le même argument fonctionne aussi dans l'autre sens, et on en déduit $\dim(V^+) = \dim(W^+)$. □

Définition 2.6. — On appelle signature de (V, q) l'entier relatif $s = r^+ - r^-$. Il est compris entre $-n$ et n et il a même parité que n.

Théorème 2.7. — *Deux espaces quadratiques réels sont isomorphes si et seulement si ils ont même rang et même signature.*

On dit que le rang et la signature forment un *système complet d'invariants* pour les formes quadratiques sur $\mathbb{R}$.

Démonstration. — Soit (V, q) un espace quadratique de dimension n et de signature s. Par le même raisonnement que dans le cas complexe, on montre qu'il existe une base orthogonale de V dans laquelle q est la forme diagonale $\langle 1, \dots, 1, -1, \dots, -1\rangle$, où le nombre de 1 est $\frac{n-s}{2}$ et le nombre de -1 est $\frac{n+s}{2}$. □

2.4. Espaces euclidiens. —

2.4.1. Définition. —

Définition 2.8. — Un espace euclidien est un espace vectoriel V de dimension finie sur $\mathbb{R}$ muni d'une forme quadratique définie positive.

Exemple 2.9. — L'espace $\mathbb{R}^n$ muni de la forme unité $\langle 1, \dots, 1\rangle$ est un espace euclidien.

2.4.2. Norme et produit scalaire. — Rappelons l'inégalité de Cauchy-Schwarz:

Proposition 2.10. — *Soient $x, y \in V$ deux vecteurs non nuls. On a*

$$|b_q(x, y)| \leq q(x)q(y),$$

et il y a égalité si et seulement si les vecteurs x et y sont colinéaires.

Démonstration. — Soit $\lambda \in \mathbb{R}$ et considérons le vecteur $v = x + \lambda y$. Il vérifie
$q(v) = b_q(x + \lambda y, x + \lambda y) = \lambda^2 q(y) + 2\lambda b_q(x, y) + q(x)$.
Considérons cette quantité comme un trinôme du second degré en λ. Comme q est définie positive, $q(v) \geq 0$, et $q(v) = 0 \Leftrightarrow v = 0$. Le discriminant $\Delta' = b_q(x, y)^2 - q(x)q(y)$ est donc supérieur ou égal à zéro. Ceci prouve l'inégalité requise. De plus, il y a égalité si et seulement si il existe $\lambda \in \mathbb{R}$ tel que $x + \lambda y = 0$, ce qui équivaut bien à dire que x et y sont colinéaires. □

Ceci permet de montrer que l'application $x \mapsto ||x|| = \sqrt{q(x)}$ est une norme, qu'on appelle la norme euclidienne. En effet, elle vérifie bien les trois axiomes des normes:
(a) $||\lambda x|| = |\lambda|\, ||x||$;
(b) $||x + y|| \leq ||x|| + ||y||$;
(c) $||x|| = 0 \Leftrightarrow x = 0$.

La forme polaire associée à q est appelée un produit scalaire et est notée $x \cdot y$. On a donc $||x||^2 = x \cdot x$.

2.4.3. Dualité. — Rappelons tout d'abord la définition de l'espace dual:

Définition 2.11. — L'espace dual de V est l'espace vectoriel $V^\star = Hom_{\mathbb{R}}(V, \mathbb{R})$ des formes linéaires de V dans $\mathbb{R}$.

Tout espace vectoriel de dimension finie est isomorphe à son espace dual, mais par un isomorphisme non canonique, c'est-à-dire qui dépend du choix d'une base de V.
Dans le cas euclidien qui nous intéresse ici, le produit scalaire permet de définir un isomorphisme *canonique* (c'est-à-dire qui ne dépend pas du choix d'une base) entre V et $V^\star$:

Théorème 2.12. — *L'application $V \to V^\star$, $v \mapsto (x \mapsto v \cdot x)$ est un isomorphisme. En particulier, quel que soit $\varphi \in V^\star$, il existe un unique $v_\varphi \in V$ tel que $\varphi(x) = v_\varphi \cdot x$ pour tout $x \in V$.*

Démonstration. — Le produit scalaire étant défini positif, il est régulier. Le résultat en découle d'après la démonstration de la proposition 1.23. □

Corollaire 2.13. — *Soit $(\varepsilon_1, \ldots, \varepsilon_n)$ une base de V. Il existe une unique base $(\check{\varepsilon}_1, \ldots, \check{\varepsilon}_n)$ telle que pour tous $i, j \in \{1, \ldots, n\}$, $\varepsilon_i \cdot \check{\varepsilon}_j = \delta_{ij}$. On l'appelle la base duale euclidienne de $\mathcal{E}$.*

Démonstration. — Soit $(\varphi_1, \ldots, \varphi_n)$ la base de $V^\star$ duale de $(\varepsilon_1, \ldots, \varepsilon_n)$. Pour tout i, φ_i est la $i$ème forme coordonnée définie, par $\varphi_i(x_1\varepsilon_1 + \cdots + x_n\varepsilon_n) = x_i$. On a donc $\varphi_i(\varepsilon_j) = \delta_{ij}$. La base duale euclidienne est alors l'image de la base duale par l'isomorphisme du théorème, i.e. $\check{\varepsilon}_i = v_{\varphi_i}$. □

2.4.4. Bases orthonormales. —

Définition 2.14. — Une base orthonormale de l'espace euclidien E est une base orthogonale $(e_1, \ldots, e_n)$ dont tous les vecteurs sont de norme 1.

Autrement dit, la base $\mathcal{E}$ est orthonormale si et seulement si la matrice de q par rapport à cette base est I_n. Ceci revient également à dire que la base $(e_1, \ldots, e_n)$ coïncide avec sa base duale euclidienne.
Il découle du théorème de classification des formes quadratiques sur $\mathbb{R}$ que tout espace euclidien admet des bases orthonormales.
D'après les formules de changement de base, une matrice de passage entre deux bases orthonormales vérifie ${}^tPP = I_n$. Une telle matrice est appelée une matrice orthogonale. Elle vérifie $P^{-1} = {}^tP$. Elle est de déterminant ± 1.
Si l'on rapporte l'espace à une base orthonormale, la forme q devient la forme diagonale $\langle 1, \ldots, 1 \rangle$. On peut ainsi identifier (V, q) à l'espace vectoriel $\mathbb{R}^n$ muni de la forme $(x_1, \ldots, x_n) \mapsto x_1^2 + \cdots + x_n^2$. On a alors $||x|| = \sqrt{x_1^2 + \cdots + x_n^2}$ et $x \cdot y = x_1y_1 + \cdots + x_ny_n$.

2.4.5. Sous-espaces d'un espace euclidien. — Tout sous-espace d'un espace vectoriel euclidien est régulier. (Ceci est vrai, de façon plus générale, pour tout sous-espace d'un espace quadratique anisotrope. En effet, un sous-espace non régulier contient, en particulier, un vecteur isotrope.) Ainsi, pour tout sous-espace W de $(\mathbb{R}^n, \cdot)$, on a $\mathbb{R}^n = W \perp W^\perp$.

2.4.6. Groupe orthogonal d'un espace euclidien. — Le groupe orthogonal de E est l'ensemble des applications linéaires bijectives de E dans E qui vérifient $f(x)\cdot f(y) = x\cdot y$ pour tout $x, y \in E$, ou encore, de façon équivalente, $||f(x)|| = ||x||$ pour tout $x \in E$ (cf. § 1.2.4).
Si l'on rapporte l'espace E à une base orthonormale, il correspond à l'ensemble des matrices orthogonales $O_n(\mathbb{R}) = \{P \in M_n(\mathbb{R}),\ {}^tPP = I_n\}$.

3. Réseaux

On se place dans l'espace vectoriel euclidien $V = \mathbb{R}^n$, muni de son produit scalaire canonique. Les réseaux sont des sous-groupes discrets de $\mathbb{R}^n$. Avant d'en donner une définition, on commence par quelques résultats préliminaires sur les groupes.

3.1. Groupes abéliens libres de type fini. —

Définition 3.1. — Un groupe est de type fini s'il admet un système générateur fini.

Tous les groupes considérés ci-dessous sont supposés abéliens et de type fini. La loi est donc notée additivement. De plus, pour tout $\ell \in \mathbb{N}$ et $a \in A$, on note $\ell.a = a + \cdots + a$ la somme de ℓ fois le terme a; si $\ell \in \mathbb{Z}$ est négatif, $\ell.a = -((-\ell).a)$.

Définition 3.2. — Soit A un groupe (abélien de type fini) et B et C deux sous groupes de A. Le groupe A est somme directe des sous groupes B et C ($A = B \oplus C$) si tout élément de A s'écrit de manière unique comme somme d'un élément de B et d'un élément de C.

Remarque 3.3. — On a $A = B \oplus C$ si et seulement si $A = B + C$ et $B \cap C = \{0\}$.

Définition 3.4. — Soit A un groupe (abélien de type fini) et $(\varepsilon_1, \ldots, \varepsilon_n)$ une famille non vide d'éléments de A. On dit que c'est une base de A si $A = \mathbb{Z}\varepsilon_1 \oplus \cdots \oplus \mathbb{Z}\varepsilon_n$.

Autrement dit, $(\varepsilon_1, \ldots, \varepsilon_n)$ est une base de A si et seulement si tout élément de A s'écrit de manière unique sous la forme $\ell_1\varepsilon_1 + \cdots + \ell_n\varepsilon_n$.

Remarque 3.5. — Notons tout de suite que la plupart des groupes abéliens n'ont pas de base. Ainsi, par exemple, l'élément $\bar{1}$ est bien un générateur de $\mathbb{Z}/7\mathbb{Z}$. Mais ce n'est pas une base puisque $\bar{0} = 7.\bar{1} = 14.\bar{1}$.

Définition 3.6. — Le groupe (abélien de type fini) A est dit libre s'il admet une base.

Théorème 3.7. — *Soit A un groupe abélien libre de type fini. Toutes les bases de A ont le même cardinal n, appelé le rang de A. Le groupe A est (non canoniquement) isomorphe à $\mathbb{Z}^n$.*

Démonstration. — Soit $(\varepsilon_1, \ldots, \varepsilon_n)$ une base de A. On fixe un entier p, et on considère le morphisme $A = \mathbb{Z}\varepsilon_1 \oplus \cdots \oplus \mathbb{Z}\varepsilon_n \to (\mathbb{Z}/p\mathbb{Z})^n$ défini par $(\ell_1\varepsilon_1 + \cdots + \ell_n\varepsilon_n) \mapsto (\bar{\ell}_1, \ldots, \bar{\ell}_n)$. C'est clairement un morphisme surjectif de groupes dont le noyau est le sous-groupe $pA = \{pa,\ a \in A\} = p\mathbb{Z}\varepsilon_1 \oplus \cdots \oplus p\mathbb{Z}\varepsilon_n \subset A$. Ainsi, le groupe A/pA est un groupe fini de cardinal p^n. Ceci prouve que l'entier n ne dépend pas du choix d'une base de A.
L'application $A = \mathbb{Z}\varepsilon_1 \oplus \cdots \oplus \mathbb{Z}\varepsilon_n \to \mathbb{Z}^n$, $\ell_1\varepsilon_1 + \cdots + \ell_n\varepsilon_n \mapsto (\ell_1, \ldots, \ell_n)$ est alors un isomorphisme de groupe. □

Soient $A = \mathbb{Z}\varepsilon_1 \oplus \cdots \oplus \mathbb{Z}\varepsilon_n$ un groupe abélien libre, et supposons que $(e_1, \ldots, e_n)$ en est une autre base. La matrice de passage P de $\mathcal{E} = (\varepsilon_1, \ldots, \varepsilon_n)$ à $(e_1, \ldots, e_n)$ donne les coordonnées des vecteurs des vecteurs e_i dans la base $\mathcal{E}$; elle est donc à coefficients entiers. Son inverse, qui donne les coefficients des vecteurs ε_i dans la base $(e_1, \ldots, e_n)$ est également dans $M_n(\mathbb{Z})$. La matrice P est donc une matrice inversible de $M_n(\mathbb{Z})$, $P \in GL_n(\mathbb{Z})$.
Notons $e_1 = k_1\varepsilon_1 + \cdots + k_n\varepsilon_n$, de sorte que $k_1, \ldots, k_n$ sont les coefficients de la première colonne de P. Il découle de $P^{-1} \times P = I_n$ que $\lambda_1 k_1 + \cdots + \lambda_n k_n = 1$, où $(\lambda_1, \ldots, \lambda_n)$ est la première ligne de P^{-1}. D'où on déduit que les entiers $(k_1, \ldots, k_n)$ sont premiers entre eux dans leur ensemble (i.e. leur plus grand diviseur commun est 1). La proposition qui suit montre que réciproquement, tout vecteur qui s'écrit ainsi fait partie d'une base de A:

Proposition 3.8. — *Soit $v = \ell_1\varepsilon_1 + \cdots + \ell_n\varepsilon_n \in A$. Si les entiers $(\ell_1, \ldots, \ell_n)$ sont premiers entre eux dans leur ensemble, alors il existe des vecteurs $v_2, \ldots, v_n \in A$ tels que $(v, v_2, \ldots, v_n)$ est une base de A.*

Démonstration. — Pour toute base $\mathcal{B}$ de A, on note $s_\mathcal{B}$ la somme des valeurs absolues des coordonnées de v dans la base $\mathcal{B}$. Ainsi, $s_\mathcal{E} = |\ell_1| + \cdots + |\ell_n|$.
Supposons tout d'abord que $s_\mathcal{E} = 1$. Comme les ℓ_i sont des entiers, on a $v = \pm\varepsilon_i$ pour un certain entier i, et la famille $(v, \varepsilon_1, \ldots, \varepsilon_{i-1}, \varepsilon_{i+1}, \ldots, \varepsilon_n)$ est une base de A. Ainsi, pour montrer la proposition, il suffit de prouver qu'il existe une base $\mathcal{B}$ de A telle que $s_\mathcal{B} = 1$.
Plaçons nous maintenant dans le cas général, où $s_\mathcal{E} \geq 2$. Comme les ℓ_i sont premiers entre eux dans leur ensemble, deux au moins d'entre eux sont non nuls. Quitte à réordonner la base $\mathcal{E}$, et à remplacer si nécessaire les vecteurs ε_1 et ε_2 par leurs opposés, on peut supposer que $\ell_1 \geq \ell_2 \geq 1$. Plaçons nous alors dans la base $\mathcal{E}' = (\varepsilon_1, \varepsilon_1 + \varepsilon_2, \varepsilon_3, \ldots, \varepsilon_n)$. Les coordonnées de v sont $(\ell_1 - \ell_2, \ell_2, \ell_3, \ldots, \ell_n)$, de sorte que $s_{\mathcal{E}'} = |\ell_1 - \ell_2| + |\ell_2| + \cdots + |\ell_n| = s_\mathcal{E} - \ell_2 < s_\mathcal{E}$.
En itérant le processus, on peut construire une base $\mathcal{B}$ de A telle que $s_\mathcal{B} = 1$, et ceci prouve la proposition. □

Pour terminer ce paragraphe, on démontre le théorème suivant, très utile pour étudier les réseaux.

Théorème 3.9. — *Soient A un groupe abélien libre de rang n, et A' un sous-groupe de A distinct de $\{0\}$. Il existe une base $(e_1, \ldots, e_n)$ de A et des entiers non nuls $d_1, \ldots, d_k$, avec $0 < k \leq n$ tels que $(d_1e_1, \ldots, d_ke_k)$ est une base de A'. En particulier, A' est également un groupe abélien libre, et son rang est $\leq n$.*

Démonstration. — On procède par induction sur le rang n de A. Si A est de rang 1, le choix d'une base e_1 permet d'identifier A à $\mathbb{Z}$; il existe alors un entier non nul d_1 tel que $A' = d_1\mathbb{Z}$ et le théorème est démontré dans ce cas. Supposons maintenant qu'il est vrai pour tout groupe abélien libre de rang $n-1$, et considérons un groupe $A = \mathbb{Z}\varepsilon_1 \oplus \cdots \oplus \mathbb{Z}\varepsilon_n$, et un sous-groupe $A' \subset A$.
On note f' la restriction à A' de l'application $f : A \to \mathbb{Z}$, $x_1\varepsilon_1 + \cdots + x_n\varepsilon_n \mapsto x_n$. Si l'image de f' est $\{0\}$, alors A' est contenu dans le noyau de f, $\ker f = \mathbb{Z}\varepsilon_1 \oplus \cdots \oplus \mathbb{Z}\varepsilon_{n-1}$ et l'hypothèse de récurrence permet de conclure dans ce cas.

Sinon, il existe un entier non nul k tel que l'image de f' est $k\mathbb{Z}$. Le groupe A' contient donc un élément $e'_n \in A'$ tel que $f'(e'_n) = k$, i.e. $e'_n = x_1\varepsilon_1 + \cdots + x_{n-1}\varepsilon_{n-1} + k\varepsilon_n$. Soit d_n le plus grand diviseur commun de $(x_1, \ldots, x_{n-1}, k)$ et posons $e_n = \frac{1}{d_n}e'_n \in A$.

Lemme 3.10. — *L'intersection $A' \cap \mathbb{Z}e_n$ est $\mathbb{Z}e'_n$.*

Démonstration. — L'inclusion $\mathbb{Z}e'_n \subset A' \cap \mathbb{Z}e_n$ découle du fait que $e'_n = d_n e_n$ appartient à A' et à $\mathbb{Z}e_n$.
Réciproquement, soit $x \in \mathbb{Z}$ tel que $xe_n \in A'$. On a alors $f'(xe_n) = x\frac{k}{d_n} \in k\mathbb{Z}$. L'entier x est donc nécessairement multiple de d_n, de sorte que $xe_n = \frac{x}{d_n}e'_n \in \mathbb{Z}e'_n$. Ceci prouve l'inclusion réciproque. □

Pour terminer la démonstration du théorème, nous allons utiliser la proposition précédente. Par construction, les coordonnées $(\frac{x_1}{d_n}, \ldots, \frac{x_{n-1}}{d_n}, \frac{k}{d_n})$ de e_n sont des entiers premiers entre eux dans leur ensemble. Il existe donc des vecteurs $e_1, \ldots, e_{n-1}$ tels que $(e_1, \ldots, e_n)$ est une base de A. Le sous-groupe A' se décompose alors en une somme directe

$$A' = A' \cap (\mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_{n-1}) \oplus A' \cap \mathbb{Z}e_n.$$

En appliquant l'hypothèse de récurence à $A' \cap (\mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_{n-1})$ et le lemme ci-dessus à $A' \cap \mathbb{Z}e_n$, on obtient, après une permutation éventuelle, une base ayant la forme requise.

3.2. Généralités. —

3.2.1. Définition d'un réseau. —

Définition 3.11. — Un réseau est un sous-ensemble $\Gamma \subset \mathbb{R}^n$ tel qu'il existe une base $(e_1, \ldots, e_n)$ de $V = \mathbb{R}^n$ telle que $\Gamma = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n$.

C'est donc un sous-groupe de $\mathbb{R}^n$ qui est un groupe abélien libre de rang n.

Exemple 3.12. — $\mathbb{Z}^n$ est un réseau de $\mathbb{R}^n$. On notera Γ_1 le réseau $\mathbb{Z}^2 \subset \mathbb{R}^2$.

Exemple 3.13. — Tracer le réseau $\Gamma_2 = \mathbb{Z}\begin{pmatrix}1\\0\end{pmatrix} \oplus \mathbb{Z}\begin{pmatrix}1\\2\end{pmatrix}$.

Exemple 3.14. — Dans $\mathbb{R}^2$ rapporté à un repère orthonormal $(O, \vec{i}, \vec{j})$, on considère le cercle $\mathcal{C}$ de centre O et de rayon r, $r > 0$. On note A et B les points du cercles tels que les angles $(\vec{i}, \vec{OA})$ et $(\vec{i}, \vec{OB})$ mesurent respectivement 0 et 60 degrés, de sorte que OAB est un triangle équilatéral. On note $\Gamma_3(r)$ le réseau $\mathbb{Z}\vec{OA} \oplus \mathbb{Z}\vec{OB}$.
Tracer le réseau $\Gamma_3(r)$. Tracer un pavage du plan par des hexagones réguliers dont les centres et les sommets sont des points de $\Gamma_3(r)$. Dans ce document, le réseau $\Gamma_3(r)$ sera appelé 'réseau hexagonal de rayon r'.

3.2.2. Bases d'un réseau. —

Définition 3.15. — On appelle base du réseau $\Gamma \subset \mathbb{R}^n$ toute base $(e_1, \ldots, e_n)$ de $\mathbb{R}^n$ telle que $\Gamma = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n$.

Les bases du réseau Γ sont donc des bases de Γ au sens du § 3.1

Exemple 3.16. — Les vecteurs $\begin{pmatrix}2\\0\end{pmatrix}$ et $\begin{pmatrix}0\\2\end{pmatrix}$ sont deux vecteurs de $\Gamma_1 = \mathbb{Z}^2$ qui forment une base de $\mathbb{R}^2$. Pourtant, ils ne forment pas une base de Γ_1. En effet, $\begin{pmatrix}1\\0\end{pmatrix} \in \Gamma_1$ s'écrit $\begin{pmatrix}1\\0\end{pmatrix} = \frac{1}{2}\begin{pmatrix}2\\0\end{pmatrix}$. Il n'appartient donc pas à $\mathbb{Z}\begin{pmatrix}2\\0\end{pmatrix} \oplus \mathbb{Z}\begin{pmatrix}0\\2\end{pmatrix}$.

Exemple 3.17. — Deux des trois couples suivants sont des bases du réseau Γ_2. Lesquels?
$\left(\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\2\end{pmatrix}\right)$; $\left(\begin{pmatrix}1\\2\end{pmatrix}, \begin{pmatrix}-1\\2\end{pmatrix}\right)$; $\left(\begin{pmatrix}1\\2\end{pmatrix}, \begin{pmatrix}0\\-2\end{pmatrix}\right)$.

Comme on l'a vu au § 3.1, la matrice de passage entre deux bases du réseau Γ est une matrice à coefficients entiers, dont l'inverse est également à coefficients entiers. C'est donc un élément de $GL_n(\mathbb{Z})$. Rappelons à ce propos le résultat suivant:

Lemme 3.18. — *Une matrice $P \in M_n(\mathbb{Z})$ est inversible dans $M_n(\mathbb{Z})$ si et seulement si son déterminant vaut ± 1.*

Démonstration. — Supposons que P est inversible dans $M_n(\mathbb{Z})$, c'est-à-dire admet un inverse $P^{-1} \in M_n(\mathbb{Z})$. On a alors $\det(P) \times \det(P^{-1}) = 1$, ce qui prouve que $\det(P)$ est un inversible de $\mathbb{Z}$, et vaut donc ± 1.
Réciproquement, si $\det(P) = \pm 1$, alors P est inversible dans $M_n(\mathbb{Q})$ et son inverse $\frac{1}{\det(P)}{}^t(com(P))$ est à coefficients entiers. Elle est donc bien inversible dans $M_n(\mathbb{Z})$. □

Ceci permet de caractériser les bases d'un réseau:

Théorème 3.19. — *Soit Γ un réseau et $\mathcal{E} = (\varepsilon_1, \ldots, \varepsilon_n)$ une base de Γ. La famille $(e_1, \ldots, e_n)$ de vecteurs de Γ est une base de Γ si et seulement si la matrice de passage de $\mathcal{E}$ à $(e_1, \ldots, e_n)$ a pour déterminant ± 1.*

Démonstration. — L'implication directe découle de ce qui précède. Supposons maintenant que la matrice de passage a pour déterminant ± 1. Elle est inversible dans $M_n(\mathbb{Z})$, de sorte que les ε_i s'expriment comme combinaisons linéaires à coefficients entiers des e_i. Ainsi, ils appartiennent au sous-groupe $\Gamma' = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_n \subset \Gamma$. D'où on déduit que $\Gamma' = \Gamma$, et ceci prouve que $(e_1, \ldots, e_n)$ est une base de Γ. □

3.2.3. Réseaux équivalents. —

Définition 3.20. — Les deux réseaux Γ et $\Delta \subset \mathbb{R}^n$ sont équivalents s'il existe un automorphisme orthogonal $f \in O_n(\mathbb{R})$ tel que $f(\Gamma) = \Delta$.

Ainsi, l'image d'un réseau Γ par une rotation de centre O ou une réflexion d'axe passant par O est un réseau équivalent. En revanche, son image par une similitude de rapport différent de ± 1 est un réseau non équivalent.

Remarque 3.21. — Le produit scalaire de l'espace euclidien $\mathbb{R}^n$ munit le réseau Γ d'une forme $\mathbb{Z}$-bilinéaire symétrique $b_\Gamma : \Gamma \times \Gamma \to \mathbb{R}$, $(x, y) \mapsto x \cdot y$. Notons cependant que cette forme n'est généralement pas à valeurs entières.
Si Γ et Δ sont deux réseaux équivalents, et $f \in O_n(\mathbb{R})$ vérifie $f(\Gamma) = \Delta$, la restriction de f à Γ est un isomorphisme de $\mathbb{Z}$-modules qui préserve les formes bilinéaires, i.e. tel que $b_\Delta(f(x), f(y)) = b_\Gamma(x, y)$.

3.3. Invariants d'un réseau. —

3.3.1. Matrice de Gram et déterminant. —

Définition 3.22. — Soit $\mathcal{E} = (\varepsilon_1, \ldots, \varepsilon_n)$ une $\mathbb{Z}$-base du réseau Γ. La matrice de Gram de Γ par rapport à cette base est la matrice $B = (\varepsilon_i \cdot \varepsilon_j)$.

Il découle de la proposition analogue dans le cas des corps que si $\mathcal{E}' = (\varepsilon'_1, \ldots, \varepsilon'_n)$ est une autre base de Γ, et si P est la matrice de changement de base, alors la matrice de Gram de Γ dans $\mathcal{E}'$ est $B' = {}^tPBP$.
On a vu au § 3.2.2 que la matrice de passage entre deux bases d'un réseau a pour déterminant ± 1. Le déterminant de la matrice B ne dépend donc pas du choix de la base.

Définition 3.23. — On appelle déterminant du réseau Γ le déterminant d'une matrice de Gram de Γ.

La proposition qui suit montre que le déterminant est un invariant:

Proposition 3.24. — *Deux réseaux équivalents ont le même déterminant.*

Démonstration. — Soit f un automorphisme de $\mathbb{R}^n$ qui transforme Γ en un réseau équivalent Γ'. Les vecteurs $(f(\varepsilon_1), \ldots, f(\varepsilon_n))$ forment une base de Γ', de sorte que la matrice $(f(\varepsilon_i) \cdot f(\varepsilon_j))$ est une matrice de Gramm de Γ'. Comme f est une isométrie de E, $f(\varepsilon_i) \cdot f(\varepsilon_j) = \varepsilon_i \cdot \varepsilon_j$ et la proposition en découle. □

Exemple 3.25. — Calculer le déterminant des réseaux Γ_1, Γ_2 et $\Gamma_3(r)$.

3.3.2. Déterminant d'un sous-réseau. — Soient Γ et Γ' deux réseaux de $\mathbb{R}^n$, et supposons que $\Gamma' \subset \Gamma$.
D'après le paragraphe préliminaire sur les groupes abéliens libres, il existe une base $(\varepsilon_1, \ldots, \varepsilon_n)$ de Γ et des entiers $d_1, \ldots, d_n$ tels que $(d_1\varepsilon_1, \ldots, d_n\varepsilon_n)$ est une base de Γ'. On a alors $\Gamma/\Gamma' \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z}$, et l'indice de Γ' dans Γ vaut $d_1 \ldots d_n$.

Exemple 3.26. — Montrer que l'indice de Γ_2 dans $\Gamma_1 = \mathbb{Z}^2$ est 2.

Proposition 3.27. — *Si* $\Gamma' \subset \Gamma$, *alors* $\det(\Gamma') = \det(\Gamma)[\Gamma : \Gamma']^2$.

Démonstration. — Il suffit de comparer les déterminants des matrices de Gram des deux réseaux, $(\varepsilon_i \cdot \varepsilon_j)$ et $(d_i\varepsilon_i \cdot d_j\varepsilon_j)$. □

Exemple 3.28. — Retrouver la valeur de l'indice de Γ_2 dans Γ_1 à l'aide de la formule ci-dessus.

3.3.3. Minimum. —

Définition 3.29. — On appelle minimum de Γ la valeur

$$Min(\Gamma) = Min\{x \cdot x, x \in \Gamma, x \neq 0\}.$$

L'existence d'un tel minimum découle du fait que Γ est un sous-groupe discret de $\mathbb{R}^n$.

Exemple 3.30. — Déterminer le minimum des réseaux Γ_1, Γ_2 et $\Gamma_3(r)$.

Proposition 3.31. — *Deux réseaux équivalents ont le même minimum.*

A nouveau, ceci découle du fait qu'une équivalence entre deux réseaux préserve le produit scalaire.

3.4. Dual d'un réseau. — Soit $\Gamma = \mathbb{Z}\varepsilon_1 \oplus \cdots \oplus \mathbb{Z}\varepsilon_n$ un réseau. Le dual du $\mathbb{Z}$-module libre Γ est le $\mathbb{Z}$-module $Hom_{\mathbb{Z}}(\Gamma, \mathbb{Z})$ des applications $\mathbb{Z}$-linéaires de Γ dans $\mathbb{Z}$.

Proposition 3.32. — *On peut identifier le dual de Γ à un sous-ensemble du dual de V*

$$Hom_{\mathbb{Z}}(\Gamma, \mathbb{Z}) \simeq \{\tilde{\varphi} \in V^\star,\ \tilde{\varphi}(\varepsilon_i) \in \mathbb{Z},\ \textit{pour } 1 \leq i \leq n\} \subset V^\star.$$

Démonstration. — Soit $\varphi \in Hom_{\mathbb{Z}}(\Gamma, \mathbb{Z})$ un élément du dual de Γ. On peut l'étendre par linéarité en un élément $\tilde{\varphi} \in V^\star = Hom_{\mathbb{R}}(E, \mathbb{R})$ du dual de V par $\tilde{\varphi}(x_1\varepsilon_1 + \cdots + x_n\varepsilon_n) = x_1\varphi(\varepsilon_1) + \cdots + x_n\varphi(\varepsilon_n)$. L'application qui à φ associe $\tilde{\varphi}$ est injective. Décrivons maintenant son image.
Soit donc $\tilde{\psi}$ un élément de $V^\star$. Si c'est l'image d'un élément $\psi \in Hom_{\mathbb{Z}}(\Gamma, \mathbb{Z})$, alors ψ est la restriction à Γ de $\tilde{\psi}$. Or la restriction de $\tilde{\psi}$ à Γ est l'application $\mathbb{Z}\varepsilon_1 \oplus \cdots \oplus \mathbb{Z}\varepsilon_n \to \mathbb{R}$, $m_1\varepsilon_1 + \cdots + m_n\varepsilon_n \mapsto m_1\tilde{\psi}(\varepsilon_1) + \cdots + m_n\tilde{\psi}(\varepsilon_n)$. Elle est dans le dual $Hom_{\mathbb{Z}}(\Gamma, \mathbb{Z})$ de Γ si et seulement si $\tilde{\psi}(\varepsilon_i) \in \mathbb{Z}$ pour $1 \leq i \leq n$. □

L'isomorphisme du thm 2.12 permet d'associer au dual $Hom_{\mathbb{Z}}(\Gamma, \mathbb{Z}) \subset V^\star$ un sous-ensemble de V, que l'on va maintenant décrire.

Théorème 3.33. — *Soit $\psi \in V^\star$ et v_ψ le vecteur correspondant à ψ par l'isomorphisme du théorème 2.12. Les propositions suivantes sont équivalentes:*
(i) La restriction de ψ à Γ est dans le dual $Hom_{\mathbb{Z}}(\Gamma, \mathbb{Z})$ de Γ;
(ii) $v_\psi \cdot \varepsilon_i \in \mathbb{Z}$ pour tout $1 \leq i \leq n$;
(ii') $v_\psi \cdot x \in \mathbb{Z}$ pour tout $x \in \Gamma$;
(iii) $v_\psi \in \mathbb{Z}\check{\varepsilon}_1 \oplus \cdots \oplus \mathbb{Z}\check{\varepsilon}_n$.

Démonstration. — L'équivalence entre (i), (ii) et (ii') découle de la proposition précédente et de la définition de v_ψ. Comme $v_\psi = (v_\psi \cdot \varepsilon_1)\check{\varepsilon}_1 + \cdots + (v_\psi \cdot \varepsilon_n)\check{\varepsilon}_n$, ces trois propositions sont aussi équivalentes à (iii). □

Ce théorème nous conduit à la définition suivante:

Définition 3.34. — On appelle réseau dual du réseau Γ le réseau

$$\check{\Gamma} = \{v \in E,\ v \cdot x \in \mathbb{Z} \text{ pour tout } x \in \Gamma\} = \mathbb{Z}\check{\varepsilon}_1 \oplus \cdots \oplus \check{\mathbb{Z}}\varepsilon_n.$$

Exemple 3.35. — Déterminer le dual $\check{\Gamma}_3(r)$ du réseau hexagonal de rayon r. Montrer que ce n'est généralement pas un sous-réseau de $\Gamma_3(r)$.
On suppose maintenant que $r = \sqrt{2}$. Montrer que $\check{\Gamma}_3(\sqrt{2})$ est un sous-réseau de $\Gamma_3(\sqrt{2})$. Calculer son déterminant et en déduire la valeur de l'indice de $\check{\Gamma}_3(\sqrt{2})$ dans $\Gamma_3(\sqrt{2})$. Donner une description explicite du quotient $\Gamma_3(\sqrt{2})/\check{\Gamma}_3(\sqrt{2})$.

Proposition 3.36. — *Notons B la matrice de Gram du réseau Γ par rapport à une base $(\varepsilon_1, \ldots, \varepsilon_n)$. La matrice de Gram du réseau dual $\check{\Gamma}$ par rapport à la base duale euclidienne $(\check{\varepsilon}_1, \ldots, \check{\varepsilon}_n)$ est B^{-1}. En particulier,* $\det(\check{\Gamma}) = \frac{1}{\det(\Gamma)}$.

Démonstration. — Notons $b_{ij} = \varepsilon_i \cdot \varepsilon_j$ les coefficients de B et $B' = (b'_{ij})$ la matrice inverse de B de sorte que $\sum_{j=1}^n b'_{ij}b_{jk} = \delta_{ik}$.

Lemme 3.37. — *La base duale euclidienne de $(\varepsilon_1, \ldots, \varepsilon_n)$ est définie par $\check{\varepsilon}_i = \sum_{i=1}^n b'_{ij}\varepsilon_j$.*

En effet, si l'on définit les $\check{\varepsilon}_i$ comme dans le lemme, on a

$$\check{\varepsilon}_i \cdot \varepsilon_k = (\sum_{j=1}^{n} b'_{ij}\varepsilon_j) \cdot \varepsilon_k = \sum_{j=1}^{n} b'_{ij}\varepsilon_j \cdot \varepsilon_k = \sum_{j=1}^{n} b'_{ij}b_{jk} = \delta_{ik}.$$

C'est donc bien la base duale euclidienne. Pour montrer la proposition, il suffit maintenant de calculer $\check{\varepsilon}_i \cdot \check{\varepsilon}_j = \sum_{i=1}^{n} b'_{ik}\varepsilon_k \cdot \check{\varepsilon}_j = b'_{ij}$. □

3.5. Réseaux entiers. —

3.5.1. Définition. —

Définition 3.38. — Le réseau $\Gamma \subset V$ est dit entier si pour tous $x, y \in \Gamma$, $x \cdot y \in \mathbb{Z}$.

Ainsi, Γ est entier si et seulement si la matrice de Gram de Γ (par rapport à une base quelconque) est à coefficients dans $\mathbb{Z}$.
Ceci équivaut également à dire que Γ est inclus dans son dual $\check{\Gamma}$.

Exemple 3.39. — Le réseau $\mathbb{Z}^n$ est clairement entier. Il coïncide avec son dual.
Le réseau hexagonal de rayon 1 n'est pas entier.
Le réseau hexagonal de rayon $\sqrt{2}$ est entier. Il n'est pas égal à son dual.

Dans tout ce paragraphe, on suppose que L est un réseau entier.
La restriction à L du produit scalaire de $\mathbb{R}^n$, que l'on note b_L est alors à valeurs dans $\mathbb{Z}$. De sorte que (L, b_L) est un $\mathbb{Z}$-module quadratique. Notons que la forme b_L, puisqu'elle est une restriction du produit scalaire de $\mathbb{R}^n$, est définie positive.

Remarque 3.40. — Réciproquement, tout $\mathbb{Z}$-module quadratique défini positif peut-être vu comme un réseau.
En effet, soit E un $\mathbb{Z}$-module libre de rang n, muni d'une forme bilinéaire symétrique définie positive $b : E \times E \to \mathbb{Z}$, rapporté à une $\mathbb{Z}$-base $(\varepsilon_1, \ldots, \varepsilon_n)$. L'espace vectoriel $V = \mathbb{R}\varepsilon_1 \oplus \cdots \oplus \mathbb{R}\varepsilon_n$, muni de la forme bilinaire obtenue en prolongeant b par linéarité est un espace euclidien. Il admet donc une base orthonormale $(e_1, \ldots, e_n)$, ce qui permet de l'identifier à $\mathbb{R}^n$, muni de son produit scalaire canonique, et donc de voir E comme un réseau dans $\mathbb{R}^n$.

Remarque 3.41. — Certains auteurs appellent réseau toute forme quadratique entière, y-compris celles qui ne sont pas définie positive, et même, plus généralement, tout module quadratique entier sur l'anneau des entiers d'un corps de nombres. Dans le cadre de ce cours, on ne considèrera que des réseaux au sens plus restrictif de la définition ci-dessus.

3.5.2. Equivalence. —

Proposition 3.42. — *Deux réseaux entiers sont équivalents si et seulement si les modules quadratiques correspondants sont équivalents.*

Démonstration. — On a vu, en effet, qu'une équivalence de réseaux est un isomorphisme de $\mathbb{Z}$-modules qui préserve les formes bilinéaires. □

Remarque 3.43. — Notons qu'il s'agit ici d'une équivalence sur $\mathbb{Z}$. C'est une notion plus fine que la notion équivalente sur $\mathbb{R}$, où même sur $\mathbb{Q}$. Ainsi, les formes $2xy$ et $x^2 - y^2$ sont clairement équivalentes sur $\mathbb{Q}$, mais elles ne le sont pas en tant que $\mathbb{Z}$-formes quadratiques.

3.5.3. Invariants. — La matrice de Gram d'un réseau entier est à coefficients entiers. Le déterminant et le minimum d'un réseau entier sont des entiers.

Proposition 3.44. — *Soit L un réseau entier. Son déterminant est* $\det(L) = [L : \check{L}]$.

Démonstration. — On a vu en effet que $\det(L) = \det(\check{L})[L : \check{L}]^2$. Or $\det(\check{L}) = \frac{1}{\det(L)}$. On a donc $\det(L)^2 = [L : \check{L}]^2$. La forme étant définie positive, son déterminant est strictement positif, et on en déduit la proposition. □

Ceci nous conduit à la définition suivante:

Définition 3.45. — Un réseau entier L est unimodulaire s'il est de déterminant 1.

Le réseau L est unimodulaire si et seulement si il est égal à son réseau dual.

Définition 3.46. — Le réseau entier L est dit pair si $x \cdot x \in 2\mathbb{Z}$ pour tout $x \in L$.

Proposition 3.47. — *Le réseau entier L est pair si et seulement si les coefficients diagonaux de la matrice de Gram de L sont tous pairs.*

Démonstration. — La condition est clairement nécessaire. Elle est également suffisante car $b_L(x_1\varepsilon_1 + \cdots + x_n\varepsilon_n) = b_{11}x_1^2 + \cdots + b_{nn}x_n^2 + 2(\sum_{1\leq i<j\leq n} b_{ij}x_ix_j)$ est pair dès que les b_{ii} le sont tous. □

4. Codes

4.1. Généralités. —

4.1.1. Définition d'un code.— Quand on a une certaine information à transmettre, il y a généralement des perturbations qui font perdre une partie de l'information en question (e.g. un grain de poussière sur un CD). Comme on ne peut pas se débarrasser des ces perturbations, on envoie en réalité une information redondante, de façon à pouvoir corriger ces erreurs de transmission, c'est-à-dire retrouver l'information initiale à partir de ce que l'on lit, qui est légèrement différent.

Exemple 4.1. — Codes de répétition. On souhaite transmettre un mot à k-lettres $x \in \mathbb{F}_q^k$. On va en réalité transmettre le mot $(x, x) \in \mathbb{F}_q^{2k}$, ou encore $(x, x, x) \in \mathbb{F}_q^{3k}$, etc...
Ceci permet de détecter les erreurs (dans le cas de C_2), et éventuellement de les corriger. Par exemple, avec C_3, on peut corriger une erreur. Si l'on recoit le mot $(1, 2, 3; 1, 2, 3; 2, 2, 3)$ et si l'on sait qu'il y a eu au plus une erreur de transmission, le mot initial était $(1, 2, 3)$.

Définition 4.2. — Un code de longueur n est un sous-ensemble non vide $C \subset \mathbb{F}_q^n$.

Le code est en fait l'ensemble des mots que l'on souhaite transmettre, mais plongé dans un ensemble plus gros.

Exemple 4.3. — Dans l'exemple ci-dessus, le code est l'ensemble

$$C_\ell = \{(x, \ldots, x),\ x \in \mathbb{F}_q^k\} \subset \mathbb{F}_q^{\ell k}.$$

C'est donc un ensemble isomorphe à $\mathbb{F}_q^k$ (qui est le 'langage' de base), mais plongé dans un sous-ensemble plus gros (en l'occurence $\mathbb{F}_q^{\ell k}$).

Définition 4.4. — Si $q = 2$, on dit que C est un code binaire.

Les codes binaires sont très utilisés, notamment en informatique.

4.1.2. Distance de Hamming.— Pour pouvoir corriger plus facilement les erreurs, on va fabriquer des codes dont les mots sont éloignés les uns des autres.

Définition 4.5. — Soit $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$. On appelle poids de x la quantité

$$w(x) = \text{cardinal}\{i,\ x_i \neq 0\}.$$

Définition 4.6. — La distance de Hamming entre x et $y \in \mathbb{F}_q^n$ est

$$d(x, y) = w(x - y) \in \{0, \ldots, n\}.$$

Ainsi, la distance de Hamming est égale au nombre de coordonnés distinctes entre les deux mots x et y.

Exemple 4.7. — Pour le code de répétition C_ℓ, on observe que deux éléments distincts diffèrent d'au moins ℓ coordonnées. La distance de Hamming entre deux mots distincts de C_ℓ est donc au moins ℓ.

On a vu précédemment que le code C_3 permet de corriger une erreur. Nous allons maintenant montrer un résultat général qui explique ce phénomène.

Définition 4.8. — On appelle distance minimale du code $C \subset \mathbb{F}_q^n$ la distance minimale entre deux mots du code:

$$d(C) = Min\{d(x, y),\ x, y \in C,\ x \neq y\}.$$

Exemple 4.9. — La distance minimale du code C_ℓ est ℓ.

Proposition 4.10. — *Un code de distance minimale d avec $d = 2t + 1$ ou $d = 2t + 2$ est capable de corriger t erreurs.*

Démonstration. — Soit $x' \in \mathbb{F}_q^n$ le mot reçu, et x le mot initial. On suppose que la transmission génère au maximum t erreurs, i.e. $d(x, x') \leq t$. Le point x se trouve donc dans la boule B de centre x' et de rayon t. Or, par l'inégalité triangulaire, deux points de B sont à une distance maximale de $2t < d$. Par ailleurs, deux points du code sont séparés par une distance d'au moins d. Aucun autre point du code ne peut donc appartenir à B. Ceci permet de retrouver le point x qui est l'unique point d'intersection de B et de C. □

4.1.3. Taux d'information. — On va donc être amenés à construire des codes ayant une distance minimale assez grande. Mais il faut également faire cela sans augmenter trop la taille des données à transmettre, i.e. la longueur du code!
Revenons à l'exemple du code de répétition C_2, dont la distance est 2. Il est très facile de construire un code de distance 2 de longueur beaucoup plus petite. Il suffit de considérer le code $C_{somme} = \{(x_1, \ldots, x_k, x_1 + \cdots + x_k)\} \subset \mathbb{F}_q^{k+1}$. Ce code est de distance minimale 2 et de longueur $k + 1$. Il est donc beaucoup moins couteux en transmission!
On va maintenant mesurer ceci de la manière suivante:

Définition 4.11. — Le taux d'information de C est la quantité

$$R_C = \frac{\log_q(|C|)}{\log_q(|\mathbb{F}_q^n|)} = \frac{\log_q(|C|)}{n}.$$

Ainsi, si le taux d'information est proche de 1, la transmission sera plus rapide ou moins couteuse en moyens!

Exemple 4.12. — Le code C_ℓ a un taux d'information égal à $\frac{1}{\ell}$.
Le code C_{somme} ci-dessus a un taux d'information qui vaut $\frac{k}{k+1}$. A distance minimale égale, C_{somme} est donc bien meilleur que C_2.

Un 'bon' code est donc un code qui a à la fois une distance minimale assez grande et un taux d'information asez proche de 1. Notons que ces deux objectifs sont assez contradictoires...

4.2. Codes linéaires. —

4.2.1. Définition et invariants. — Dans la suite, on va s'intéresser aux codes linéaires, définis comme suit:

Définition 4.13. — Un code linéaire est un $\mathbb{F}_q$-sous-espace vectoriel de $\mathbb{F}_q^n$.

Définition 4.14. — Un $[n,k]$-code (resp. $[n,k,d]$-code) est un code linéaire de longueur n, de dimension k (resp. et de distance minimale d).

Exemple 4.15. — En réalité, tous les exemples étudiés ci-dessus sont des exemples de codes linéaires. Le code C_ℓ est un $[\ell k, k, \ell]$-code. Le code C_{somme} est un $[k+1, k, 2]$-code

Les invariants définis ci-dessus sont plus faciles à calculer pour les codes linéaires.

Proposition 4.16. — *Si C est linéaire, la distance minimale de C est égale au poids minimal d'un point non nul du code.*

Exemple 4.17. — Dans le cas du code de répétition C_ℓ, on voit bien que le poids minimal d'un point non nul est ℓ.

Proposition 4.18. — *Le taux d'information d'un code de longueur n et de dimension k est $\frac{k}{n}$.*

4.2.2. Description matricielle. — Comme toujours en algèbre linéaire, on peut utiliser les matrices pour décrire les choses. Attention cependant, il s'agit ici de matrices à coefficients dans un corps fini. Nous allons dans ce paragraphe revenir aux conventions habituelles de l'algèbre linéaire, et noter en colonne un vecteur de $\mathbb{F}_q^n$.
Soit $f : \mathbb{F}_q^k \to \mathbb{F}_q^n$ une application linéaire injective. Son image est un $[n,k]$-code. Si A est la matrice de f, c'est une matrice à n lignes et k colonnes, dont les colonnes forment une base de $C \subset \mathbb{F}_q^n$. Autrement dit, si on identifie un vecteur $x \in \mathbb{F}_q^n$ (ou $\mathbb{F}_q^k$) avec le vecteur colonne $X \in M_{n,1}(\mathbb{F}_q)$ (ou $M_{k,1}(\mathbb{F}_q)$) correspondant, on obtient $C = \{AX,\ X \in M_{k,1}(\mathbb{F}_q)\}$.

Définition 4.19. — La matrice A est appelée matrice génératrice du code C.

Notons que tout code (linéaire!) peut être décrit comme l'image d'une application linéaire. Tout code admet donc une (et même plusieurs) matrices génératrices.
Soit maintenant $g : \mathbb{F}_q^n \to \mathbb{F}_q^{n-k}$ une application linéaire surjective. Son noyau $C = \ker g$ est un $[n,k]$-code.
Soit B la matrice de g. C'est une matrice à $n-k$ lignes et n colonnes. Elle donne les relations qui définissent le code. On a en effet, avec les mêmes identifications que ci-dessus, $C = \{X \in M_{n,1}(\mathbb{F}_q),\ BX = 0\}$.

Définition 4.20. — La matrice B est appelée matrice de parité du code C.

A nouveau, tout code peut-être décrit comme noyau d'une application linéaire et admet donc (plusieurs) matrices de parité.

Exemple 4.21. — Exemple du code C_{somme}.
C'est l'image de l'application $\mathbb{F}_q^k \to \mathbb{F}_q^{k+1}$, $(x_1, \dots, x_k) \mapsto (x_1, \dots, x_k, x_1 + \cdots + x_k)$.
C'est aussi le noyau de l'application $\mathbb{F}_q^{k+1} \to \mathbb{F}_q$, $(y_1, \dots, y_{k+1}) \mapsto y_{k+1} - (y_1 + \cdots + y_k)$.
Il a donc pour matrice génératrice et matrice de parité les matrices suivantes

$$A = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \\ 1 & \dots & 1 \end{pmatrix}; \; B = \begin{pmatrix} -1 & \dots & -1 & 1 \end{pmatrix}.$$

Remarque 4.22. — Se donner un code revient donc finalement à se donner une suite exacte

$$1 \to \mathbb{F}_q^k \to \mathbb{F}_q^n \to \mathbb{F}_q^{n-k} \to 1.$$

Ceci revient à dire que la première application est injective, la seconde surjective, et de noyau égal à l'image de la précédente.

4.2.3. Le code de Hamming. — Historiquement, c'est probablement l'un des premiers codes efficaces, introduit par Hamming dans les années 1950. C'est un code binaire de longueur 7, noté H, et défini comme étant l'image de l'application:

$$\mathbb{F}_2^4 \to \mathbb{F}_2^7, \; (x_1, x_2, x_3, x_4) \mapsto (x_1, x_2, x_3, x_4, x_1 + x_2 + x_3, x_1 + x_2 + x_4, x_1 + x_3 + x_4)$$

Exemple 4.23. — Trouver une matrice de parité et une matrice génératrice de H.

On peut écrire explicitement la liste des éléments de H:

$$\begin{aligned} H = \; & \{0000000; 1000111; 0100110; 0010101; 0001011; 1100001; 1010010; 1001100; \\ & 0110011; 0101101; 0011110; 1110100; 1101010; 1011001; 0111000; 1111111\}. \end{aligned}$$

Ainsi, outre le mot nul, H contient 7 mots de poids 3, 7 mots de poids 4, et le mot 1111111 de poids 7. En particulier, le poids minimal d'un mot non nul est 3, et on a $d(H) = 3$; ainsi, H est un $[7, 4, 3]$-code.
Son taux d'information est égal à $4/7$. A distance minimale égale, il est donc bien plus efficace que le code de répétition C_3 (de taux $1/3$).

4.2.4. Dualité. — Munissons l'espace vectoriel $\mathbb{F}_q^n$ de la forme bilinéaire symétrique non dégénérée définie par $x \cdot_{\mathbb{F}_q} y = \sum_{i=1}^n x_i y_i$.

Définition 4.24. — Le code dual du code linéaire $C \subset \mathbb{F}_q^n$ est

$$C^\perp = \{y \in \mathbb{F}_q^n, \; x \cdot_{\mathbb{F}_q} y = 0 \; \forall x \in C\}.$$

C'est un code linéaire de dimension $n - \dim C$.

Matriciellement, on a le résultat suivant:

Proposition 4.25. — *Si A est une matrice génératrice du code C, sa transposée ${}^tA$ est une matrice de parité du code dual $C^\perp$. Si B est une matrice de parité du code C, sa transposée ${}^tB$ est une matrice génératrice du code dual $C^\perp$.*

Démonstration. — Ceci découle de la définition du code dual par un calcul matriciel assez direct. Remarquons en effet que si les vecteurs x et y de $\mathbb{F}_q^n$ correspondent respectivement aux vecteurs colonnes X et Y, alors on a $x \cdot_{\mathbb{F}_q} y = {}^tXY$. Ainsi,

$$\begin{aligned} C^\perp = & \{y \in \mathbb{F}_q^n,\ x \cdot_{\mathbb{F}_q} y = 0\ \forall x \in C\} = \{Y \in M_{n,1}(\mathbb{F}_q),\ {}^t(AX)Y = 0,\ \forall X \in M_{k,1}(\mathbb{F}_q)\} \\ & = \{Y \in M_{n,1}(\mathbb{F}_q),\ {}^tX({}^tAY) = 0,\ \forall X \in M_{k,1}(\mathbb{F}_q)\} = \{Y \in M_{n,1}(\mathbb{F}_q),\ {}^tAY = 0\}, \end{aligned}$$

et ceci prouve bien que ${}^tA$ est une matrice de parité de C.
Pour la matrice de parité, un calcul analogue à celui qui précède montre que

$$\{{}^tBY,\ Y \in M_{n-k,1}(\mathbb{F}_q)\} \subset C^\perp.$$

Or $C^\perp$ est de dimension $n-k$ et le rang de ${}^tB$ est égal au rang de B qui vaut $n-k$. On a donc bien égalité entre ces deux ensembles, et ${}^tB$ est une matrice génératrice de $C^\perp$. □

Par définition du code dual, on a l'équivalence suivante

$$C \subset C^\perp \ \Leftrightarrow\ \forall x, y \in C,\ x \cdot_{\mathbb{F}_q} y = 0.$$

Définition 4.26. — Le code C est dit auto-dual si $C^\perp = C$.

Notons que comme $\dim C^\perp = n - \dim C$, si le code C est autodual, alors la longueur n du code est paire, $n = 2k$, et $\dim C = \dim C^\perp = k$.
Réciproquement, si n est pair, $C \subset C^\perp$ et $\dim C = n/2$, alors C est auto-dual.

Remarque 4.27. — Puisqu'il est de longueur impaire, le code de Hamming ne peut pas être autodual. Le devoir proposé porte sur la construction d'un code binaire de longueur 8, appelé le code de Hamming étendu, dont on montrera qu'il est auto-dual.

4.3. Codes pairs et doublement pairs. —

Définition 4.28. — Le code binaire C est dit pair (resp. doublement pair) si tous les mots de C sont de poids pair (resp. multiple de 4).

Proposition 4.29. — *Si C est un code binaire doublement pair, alors $C \subset C^\perp$.*

Démonstration. — Soit c et c' deux mots de C. Par hypothèse, leurs longueurs $w(c)$ et $w(c')$ sont multiples de 4. Notons $\tilde{c}$ et $\tilde{c}'$ les vecteurs de $\{0,1\}^n \subset \mathbb{R}^n$ associés à c et c'. On a $c \cdot_{\mathbb{F}_2} c' = \overline{\tilde{c} \cdot \tilde{c}'} \in \mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2$, où $\tilde{c} \cdot \tilde{c}'$ désigne le produit scalaire euclidien dans $\mathbb{R}^n$ de $\tilde{c}$ et $\tilde{c}'$. Or ce dernier vaut $\tilde{c} \cdot \tilde{c}' = \frac{1}{2}((\tilde{c}+\tilde{c}') \cdot (\tilde{c}+\tilde{c}') - \tilde{c} \cdot \tilde{c} - \tilde{c}' \cdot \tilde{c}')$. Les deux derniers termes de la somme sont $\tilde{c} \cdot \tilde{c} = w(c)$ et $\tilde{c}' \cdot \tilde{c}' = w(c')$, et sont donc multiples de 4. Par ailleurs, les coordonnées du vecteur $\tilde{c} + \tilde{c}'$ sont 0, 1 ou 2. Le nombre de 1 est exactement la longueur du mot $c + c' \in C$. Si l'on note s le nombre de 2, on obtient $(\tilde{c}+\tilde{c}') \cdot (\tilde{c}+\tilde{c}') = w(c+c') + 4s$ qui est également un multiple de 4. Ainsi, $\tilde{c} \cdot \tilde{c}'$ est pair, $c \cdot_{\mathbb{F}_2} c' = 0 \in \mathbb{F}_2$ et C est inclus dans son dual. □

Corollaire 4.30. — *Un $[2k, k]$-code binaire doublement pair est nécessairement auto-dual.*

5. Des codes aux réseaux

Dans ce paragraphe, nous allons définir le réseau associé à un code linéaire binaire $C \subset \mathbb{F}_2^n$, et étudier les propriétés de ce réseau en fonction des propriétés du code initial.

5.1. Définition du réseau associé à un code. —

5.1.1. Lemme préliminaire. — On commence par montrer le résultat suivant:

Lemme 5.1. — *Soient* Γ *un réseau et* $\Gamma' \subset \Gamma$ *un sous-groupe non trivial de* Γ. *C'est un sous-réseau de* Γ *si et seulement si le quotient* Γ/Γ' *est fini.*

Démonstration. — Par le théorème 3.9, il existe une base $(\varepsilon_1, \ldots, \varepsilon_n)$ de Γ, un entier k, $0 < k \leq n$ et des entiers non nuls $d_1, \ldots, d_k$ tels que $(d_1\varepsilon_1, \ldots, d_k\varepsilon_k)$ est une base de Γ'. Le quotient Γ/Γ' est alors isomorphe à $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z} \times \mathbb{Z}^{n-k}$. Il est donc fini si et seulement si $k = n$.
Or si $k < n$, alors Γ' est inclus dans le sous-espace vectoriel $\mathbb{R}\varepsilon_1 \oplus \cdots \oplus \mathbb{R}\varepsilon_k$ qui est strictement inclus dans l'espace euclidien sous-jacent $V = \mathbb{R}^n$. Aucune base de Γ' n'est donc une base de V, et ceci prouve que Γ' n'est pas un réseau.
Si en revanche $k = n$, alors $(d_1\varepsilon_1, \ldots, d_n\varepsilon_n)$ est une base de V et Γ' est bien un réseau. □

5.1.2. Réseau associé à un code. — On considère le réseau standard $\mathbb{Z}^n \subset \mathbb{R}^n$, et l'application $\rho : \mathbb{Z}^n \to (\mathbb{Z}/2\mathbb{Z})^n = \mathbb{F}_2^n$ définie par $\rho(x_1, \ldots, x_n) = (\bar{x}_1, \ldots, \bar{x}_n)$.

Lemme 5.2. — *Soit* $C \subset \mathbb{F}_2^n$ *un code linéaire binaire. Le sous-groupe* $\rho^{-1}(C) \subset \mathbb{Z}^n$ *est un sous-réseau de* $\mathbb{Z}^n$.

Démonstration. — Par un calcul direct, $\rho^{-1}(C) = \{y \in \mathbb{Z}^n,\ \rho(y) \in C\}$ est le noyau du morphisme surjectif de groupe $f : \mathbb{Z}^n \to \mathbb{F}_2^n/C$, qui à $y \in \mathbb{Z}^n$ associe la classe dans le quotient $\mathbb{F}_2^n/C$ de $\rho(y)$. C'est donc un sous-groupe de $\mathbb{Z}^n$, et le quotient $\mathbb{Z}^n/\rho^{-1}(C) \simeq \mathbb{F}_2^n/C$ est fini. La conclusion découle alors du lemme préliminaire. □

Définition 5.3. — Le réseau associé au code linéaire binaire $C \subset \mathbb{F}_2^n$ est

$$\Gamma_C := \frac{1}{\sqrt{2}}\rho^{-1}(C) \subset \mathbb{R}^n.$$

Pour tout point $c \in \mathbb{F}_2^n$, on note encore c le vecteur correspondant $c \in \{0,1\}^n \subset \mathbb{R}^n$. On a alors, en particulier $c \cdot_{\mathbb{F}_2} c' = \overline{c \cdot c'} \in \mathbb{F}_2$, et $c \cdot c$ est la longueur $w(c)$ du mot $c \in C$. Avec ces notations, on observe que $\Gamma_c = \{\frac{1}{\sqrt{2}}(c + 2z),\ c \in C \text{ et } z \in \mathbb{Z}^n\} \subset \mathbb{R}^n$. De cette description, on déduit immédiatement:

Proposition 5.4. — *Soient* C_1 *et* C_2 *deux codes linéaires binaires. Si* $C_1 \subset C_2$, *alors* $\Gamma_{C_1} \subset \Gamma_{C_2}$.

5.2. Déterminant de Γ_C. —

Proposition 5.5. — *Si* C *est un* $[n,k]$*-code, alors le réseau associé a pour déterminant* $\det(\Gamma_c) = 2^{n-2k}$.

Démonstration. — Par la proposition 3.27, appliquée au sous-réseau $\rho^{-1}(C) \subset \mathbb{Z}^n$, on a $\det(\rho^{-1}(C)) = \det(\mathbb{Z}^n) \times |\mathbb{Z}^n/\rho^{-1}(C)|^2 = 2^{2n-2k}$.
La matrice de Gram de Γ_C est obtenue à partir de celle de $\rho^{-1}(C)$ en multipliant chaque coefficient par $\frac{1}{\sqrt{2}} \times \frac{1}{\sqrt{2}} = \frac{1}{2}$. On a donc $\det(\Gamma_C) = (\frac{1}{2})^n \det(\rho^{-1}(C)) = 2^{n-2k}$. □

5.3. Dualité. — Le théorème qui suit explique la présence du facteur $\frac{1}{\sqrt{2}}$ dans la définition de Γ_C:

Théorème 5.6. — *Le réseau associé au code dual $C^\perp$ est le dual du réseau associé au code C,*

$$\Gamma_{C^\perp} = \check{\Gamma}_C.$$

Démonstration. — Commençons par montrer que $\Gamma_{C^\perp} \subset \check{\Gamma}_C$. Par définition de $\check{\Gamma}_C$, il suffit de vérifier que quels que soient $x \in \Gamma_C$ et $y \in \Gamma_{C^\perp}$, $x \cdot y \in \mathbb{Z}$. Ecrivons $x = \frac{1}{\sqrt{2}}(c+2z)$ et $y = \frac{1}{\sqrt{2}}(c' + 2z')$ avec $c \in C$, $c' \in C^\perp$ et $z, z' \in \mathbb{Z}^n$. On a alors

$$x \cdot y = \frac{1}{2}(c \cdot c' + 2c \cdot z' + 2c' \cdot z + 4z \cdot z').$$

Or $\overline{c \cdot c'} = c \cdot_{\mathbb{F}_2} c' = 0$ puisque $c \in C$ et $c' \in C^\perp$. Ainsi, $c \cdot c' \in 2\mathbb{Z}$ et $x \cdot y \in \mathbb{Z}$.
Le réseau $\Gamma_{C^\perp}$ est donc un sous-réseau $\check{\Gamma}_C$. De plus, $|\check{\Gamma}_C/\Gamma_{C^\perp}|^2 = \frac{\det(\Gamma_{C^\perp})}{\det(\check{\Gamma}_C)} = \det(\Gamma_{C^\perp}) \times \det(\Gamma_C)$. Or, si C est un $[n,k]$-code, alors $C^\perp$ est un $[n, n-k]$-code, et on obtient $|\check{\Gamma}_C/\Gamma_{C^\perp}|^2 = 2^{n-2k} \times 2^{n-2(n-k)} = 1$. Ceci prouve le théorème □

Corollaire 5.7. — *Le réseau Γ_C est entier si et seulement si $C \subset C^\perp$.*

Démonstration. — Si $C \subset C^\perp$, alors par la proposition 5.4, on a bien $\Gamma_C \subset \Gamma_{C^\perp} = \check{\Gamma}_C$. Supposons réciproquement que $\Gamma_C \subset \check{\Gamma}_C = \Gamma_{C^\perp}$. On a alors $\sqrt{2}\Gamma_C \subset \sqrt{2}\Gamma_{C^\perp}$, et donc $\rho(\sqrt{2}\Gamma_C) \subset \rho(\sqrt{2}\Gamma_{C^\perp})$. Le code C est donc bien inclus dans son dual $C^\perp$. □

Corollaire 5.8. — *Le réseau Γ_C est entier unimodulaire si et seulement si le code C est autodual.*

Démonstration. — Le réseau Γ_C est unimodulaire si et seulement si il est entier et de déterminant 1. Par le corollaire précédent et la proposition 5.5, ceci revient à dire que $C \subset C^\perp$ et $n = 2k$. Ceci équivaut bien à $C = C^\perp$. □

Proposition 5.9. — *Le réseau Γ_C est pair si et seulement si le code C est doublement pair.*

Démonstration. — Par définition, Γ_C est pair s'il est entier et si $x \cdot x \in 2\mathbb{Z}$ pour tout $x \in \Gamma_C$. Or si $x = \frac{1}{\sqrt{2}}(c+2z)$, alors $x \cdot x = \frac{1}{2}(w(c) + 4c \cdot z + 4z \cdot z)$. Ainsi, $x \cdot x \in 2\mathbb{Z}$ si et seulement si $w(c) \equiv 0 \mod 4$. □

Mars 2007

Anne Quéguiner-Mathieu