# Réseaux et applications

Daniel PERRIN

**Avertissement** *Le texte ci-dessous est le troisième provenant de la récupération de mes vieux papiers du temps de Sèvres (l'école normale supérieure de jeunes filles). L'objectif de ces textes est de compléter le cours d'algèbre [DP].*

## 1 Introduction, notations, définition

### 1.1 Introduction

Du temps où je m'occupais de la préparation des sévriennes à l'agrégation, enseigner les réseaux était un passage obligé. En effet, la moitié des problèmes de l'épreuve de "Mathématiques générales" (en réalité algèbre et géométrie) mettaient en jeu ces objets. C'est la justification initiale de ce cours. Il faut y ajouter l'importance des réseaux notamment en théorie des nombres (théorèmes des deux et des quatre carrés, entiers de la forme $x^2 + dy^2$, etc.)

### 1.2 Notations

Dans tout ce qui suit, on désigne par $K$ un corps[1] commutatif de caractéristique zéro et par $E$ un $K$-espace vectoriel de dimension $n$. Si $A$ est une partie de $E$ on note $<A>$ le sous-espace vectoriel engendré par $A$ et on pose $\mathrm{rg}\, A = \mathrm{rg}\,(<A>)$. Pour des entiers $a, b$, la notation $a|b$ signifie que $a$ divise $b$.

### 1.3 Définition

**1.1 Définition.** *Soit $L$ un sous-groupe additif de $E$ et $r \in \mathbf{N}^*$. On dit que $L$ est un* **sous-réseau** *de rang $r$ de $E$ s'il existe une famille libre $e_1, \ldots, e_r$ d'éléments de $L$ tels que $L$ soit l'ensemble des combinaisons linéaires à coef-*

1. Le plus souvent, $K$ sera égal à $\mathbf{R}$.

*ficients entiers des $e_i$ :*

$$L = \{x = \sum_{i=1}^{r} x_i e_i \ \mid \ x_i \in \mathbf{Z}\}.$$

*La famille $e_1, \ldots, e_r$ est appelée une* **Z-base** *de $L$ et on a $r = \operatorname{rg} L$.*

*On appelle* **réseau** *un sous-réseau de rang maximum (c'est-à-dire $n$).*

**1.2** *Remarques.* 1) Un sous-réseau est un $\mathbf{Z}$-module libre de rang $r$, i.e. isomorphe à $\mathbf{Z}^r$ comme groupe abélien, au moyen de l'isomorphisme $\varphi : \mathbf{Z}^r \to L$ défini par $\varphi(x_1, \ldots, x_r) = \sum_{i=1}^{r} x_i e_i$.

2) Attention, il y a beaucoup de $\mathbf{Z}$-bases dans un réseau. Précisément, on a la proposition suivante :

**1.3 Proposition.** *Soient $e_1, \ldots, e_n$ et $\epsilon_1, \ldots, \epsilon_n$ deux bases de $E$. On suppose que $e_1, \ldots, e_n$ est une $\mathbf{Z}$-base d'un réseau $L$. Alors, $\epsilon_1, \ldots, \epsilon_n$ est une $\mathbf{Z}$-base de $L$ si et seulement si la matrice $P$ de passage des $e_i$ aux $\epsilon_j$ est dans $GL(n, \mathbf{Z})$ (c'est-à-dire à coefficients entiers et de déterminant $\pm 1$).*

*Démonstration.* Si $\epsilon_1, \ldots, \epsilon_n$ est une $\mathbf{Z}$-base de $L$, il est clair que $P$ est à coefficients entiers, ainsi que la matrice de passage, notée $Q$, des $\epsilon_j$ aux $e_i$. Mais on a $PQ = \mathrm{Id}_n$, donc $\det P \times \det Q = 1$, et comme les déterminants sont entiers, ils sont égaux à $\pm 1$.

Réciproquement, supposons que $P$ est dans $GL(n, \mathbf{Z})$, donc est à coefficients entiers ainsi que sa matrice inverse $Q$. Comme $P$ est à coefficients entiers, le réseau $M$ de $\mathbf{Z}$-base $\epsilon_1, \ldots, \epsilon_n$ est contenu dans $L$. Comme $Q$ est à coefficients entiers, $L$ est inclus dans $M$ et on a donc $L = M$.

**1.4** *Remarque.* Cette proposition permet de fabriquer des $\mathbf{Z}$-bases "longues" pour perturber un peu l'intuition des débutants. Par exemple, si $n = 2$, $E = \mathbf{R}^2$ et $L = \mathbf{Z}^2$, il existe une $\mathbf{Z}$-base dont le premier vecteur $e_1$ est égal à $(a, b)$ avec $a, b \in \mathbf{Z}$, pourvu que $a$ et $b$ soient premiers entre eux. En effet, en vertu du théorème de Bézout, il existe $c, d \in \mathbf{Z}$ tels que $ad - bc = 1$ et $e_2 = (c, d)$ complète alors la $\mathbf{Z}$-base. Par exemple, on peut prendre $e_1 = (13441, 1273)$ et $e_2 = (18583, 1760)$.

Plus généralement, on a le lemme suivant :

**1.5 Lemme.** *Soit $n$ un entier $\geq 2$. Soit $v = (a_1, \ldots, a_n)$ un vecteur à coefficients entiers premiers entre eux dans leur ensemble. Il existe une matrice $A \in GL(n, \mathbf{Z})$ dont $v$ est la première ligne (ou la première colonne).*

*Démonstration.* On raisonne par récurrence sur $n$. Pour $n = 2$, en vertu de Bézout, il existe $\lambda_1, \lambda_2 \in \mathbf{Z}$ tels que $\lambda_1 a_1 - \lambda_2 a_2 = 1$ et la matrice $\begin{pmatrix} a_1 & a_2 \\ \lambda_2 & \lambda_1 \end{pmatrix}$ convient. Supposons la propriété établie pour l'entier $n$ et passons à $n+1$. On appelle $d$ le *pgcd* de $a_1, \ldots, a_n$. Par hypothèse, il est premier avec $a_{n+1}$ et on a donc $\lambda, \mu \in \mathbf{Z}$ tels que $\lambda d - \mu a_{n+1} = 1$. Par ailleurs, on peut écrire, pour $i \leq n$, $a_i = da'_i$ et les $a'_i$ sont premiers entre eux. On pose $v' = (a'_1, \ldots, a'_n)$. Par l'hypothèse de récurrence, il existe une matrice $B_0$ à coefficients entiers, de taille $(n-1) \times n$ telle qu'en lui ajoutant $v'$ comme première ligne on obtienne $A_0 = (a_{ij}) \in GL(n, \mathbf{Z})$ et on peut même supposer $\det A_0 = 1$. La matrice $A$ obtenue remplaçant la première ligne de $A_0$ par $(a_1, \ldots, a_n)$ a alors pour déterminant $d$ et la matrice $A'$ obtenue en ajoutant $\mu v'$ comme dernière ligne à $A_0$ a pour déterminant $(-1)^{n-1}\mu$.

On considère alors la matrice $C$ obtenue en bordant $A$ par la $n+1$-ième ligne $(\mu v', \lambda)$ et par la $n+1$-ième colonne $(a_{n+1}, 0, \ldots, 0, \lambda)$ :

$$C = \begin{pmatrix} da'_1 & \ldots & da'_n & a_{n+1} \\ & & & 0 \\ & a_{ij} & & \vdots \\ & & & 0 \\ \mu a'_1 & \ldots & \mu a'_n & \lambda \end{pmatrix}.$$

Elle est à coefficients entiers, admet $(a_1, \ldots, a_{n+1})$ comme première ligne, et son déterminant, obtenu en développant par rapport à la dernière colonne vaut [2] $(-1)^n a_{n+1} \det A' + \lambda \det A = \lambda d - \mu a_{n+1} = 1$.

**1.6** *Remarques.* 1) On notera que la condition est nécessaire : si les $a_i$ ont un facteur commun $d$, le déterminant d'une matrice de première ligne $v$ est multiple de $d$.

2) On déduit de ce lemme que tout vecteur $v = (a_1, \ldots, a_n)$ à coefficients entiers premiers entre eux dans leur ensemble peut être pris comme premier vecteur de base du réseau $\mathbf{Z}^n$ de $\mathbf{R}^n$.

# 2 Le cas réel

Dans ce paragraphe, sauf mention expresse du contraire, on suppose $K = \mathbf{R}$.

2. Le lecteur vérifiera que je ne me suis pas trompé dans les signes ou les rectifiera si nécessaire.

## 2.1 Rappels de topologie

### 2.1.1 Normes et topologie produit

Soit $E$ un $\mathbf{R}$-espace vectoriel de dimension finie $n$. Il y a deux manières, chacune multiple en apparence, de munir $E$ d'une topologie.

1) On choisit une base $e_1, \ldots, e_n$ de $E$. Cette base définit une bijection de $\mathbf{R}^n$ sur $E$ en associant à $(x_1, \ldots, x_n)$ le vecteur $\sum_{i=1}^n x_i e_i$. On peut donc munir $E$ de la topologie déduite de la topologie produit de $\mathbf{R}^n$. On montre que cette topologie ne dépend pas du choix de la base. En effet, si l'on change de base, les coordonnées d'un vecteur dans la nouvelle base s'expriment linéairement en fonction des anciennes et cette application est continue ainsi que sa réciproque.

2) On munit $E$ d'une norme, par exemple en choisissant une base $e_1, \ldots, e_n$ et en posant $\| \sum_{i=1}^n x_i e_i \| = \sup |x_i|$ ou encore $\sum_{i=1}^n |x_i|$ ou $\sqrt{\sum_{i=1}^n x_i^2}$. Ici, le résultat crucial est que toutes les normes sur un $\mathbf{R}$-espace vectoriel de dimension finie sont équivalentes, donc définissent la même topologie. De plus, on montre aisément que cette topologie est aussi la topologie produit définie ci-dessus.

En définitive, il n'y a qu'une topologie raisonnable sur $E$, définie comme ci-dessus. On munira toujours $E$ de cette topologie.

### 2.1.2 Ensembles discrets

On rappelle qu'un sous-ensemble $A$ de $E$ est dit **discret** si la topologie induite sur $A$ par celle de $E$ est la topologie discrète. Cela signifie que pour tout $a \in A$ il existe un ouvert $\omega$ de $E$ tel que $\omega \cap A = \{a\}$. C'est encore équivalent au fait que, si une suite $(a_n)$ d'éléments de $A$ converge vers $a \in A$, elle est constante à partir d'un certain rang. Si $A$ est discret, il est clair que ses parties le sont aussi.

Le lemme suivant caractérise les ensembles fermés discrets de $\mathbf{R}^n$ :

**2.1 Lemme.** *Soit $A$ une partie de $E$. Les conditions suivantes sont équivalentes :*
*1) $A$ est fermé et discret,*
*2) pour toute partie bornée $\Omega$ de $E$, $A \cap \Omega$ est fini.*

*Démonstration.* Supposons qu'on a la condition 2). Alors, si $a$ est dans $A$ (resp. si $a$ n'est pas dans $A$), la boule $B(a, 1)$ ne contient qu'un nombre fini de points de $A$ et, quitte à diminuer son rayon, elle ne contient plus que $a$ (resp. elle ne contient plus aucun point de $A$). Cela montre que $A$ est discret (resp. fermé). Dans l'autre sens, supposons $A$ discret et soit $\Omega$ un ensemble borné. Si $\Omega$ contient une infinité d'éléments de $A$, il en est de même de son

adhérence $\overline{\Omega}$, qui est un compact. Il contient donc une suite $(a_n)$ avec $a_n \in A$, formée d'éléments distincts. En vertu de Bolzano-Weierstrass, on peut, quitte à extraire une sous-suite, supposer que $(a_n)$ converge vers $a$. Comme $A$ est fermé, le point $a$ est dans $A$. Mais alors, la suite est constante à partir d'un certain rang, ce qui est absurde.

**2.2** *Remarque.* Attention, la condition "fermé" est essentielle ici. Par exemple l'ensemble des $\frac{1}{n}$ pour $n \in \mathbf{N}^*$ est discret dans $\mathbf{R}$ (mais non fermé) et il ne vérifie évidemment pas la conclusion du lemme.

Cependant, en ce qui concerne les sous-groupes de $E$, on a le résultat suivant :

**2.3 Lemme.** *Soit $L$ un sous-groupe additif de $E$. Alors, si $L$ est discret, il est fermé.*

*Démonstration.* Soit $(a_n)$ une suite d'éléments de $L$ qui converge vers $x \in E$. Il s'agit de montrer que $x$ est dans $L$. Comme $(a_n)$ converge, la suite $a_n - a_{n+1}$ converge vers 0. Mais comme $L$ est un sous-groupe, $a_n - a_{n+1}$ et 0 sont dans $L$, et comme $L$ est discret, cela implique $a_n = a_{n+1}$ pour $n \geq N$. Mais alors on a $x = a_n$ pour $n \geq N$ et $x$ est dans $L$.

On a aussi une caractérisation des sous-groupes discrets :

**2.4 Proposition.** *Soit $L$ un sous-groupe additif de $E$. Alors, $L$ est discret si et seulement si l'ensemble des normes de ses éléments non nuls admet un minimum.*

*Démonstration.* Si $L$ est discret, le lemme 2.1 appliqué à une boule de centre 0 montre qu'il existe un élément de norme minimum dans $L$. Inversement, si $R$ est le minimum des normes des éléments non nuls de $L$ et si $a$ est dans $L$, on a $B(a, R/2) \cap L = \{a\}$ (si $b$ est dans l'intersection et distinct de $a$, $b - a$ est dans $B(0, R/2)$ et non nul et c'est absurde). Le singleton $\{a\}$ est donc ouvert dans $L$ ce qui montre que $L$ est discret.

## 2.2 Réseaux et sous-groupes discrets

L'objectif de ce paragraphe est de prouver le théorème suivant :

**2.5 Théorème.** *Soit $L$ un sous-groupe additif de $E$. Les conditions suivantes sont équivalentes :*
*1) $L$ est discret,*
*2) $L$ est un sous-réseau.*

### 2.2.1 Le sens facile : 2) $\Longrightarrow$ 1)

Soit $e_1, \ldots, e_r$ une $\mathbf{Z}$-base de $L$, que l'on complète en une base $e_1, \ldots, e_n$ de $E$. On a vu qu'on a un homéomorphisme $\varphi : E \to \mathbf{R}^n$ défini par $\varphi(\sum_{i=1}^n x_i e_i) = (x_1, \ldots, x_n)$. Comme $\varphi(L)$ est contenu dans $\mathbf{Z}^n$, il suffit de montrer que cet ensemble est discret. Soit $x = (x_1, \ldots, x_n) \in \mathbf{Z}^n$. Alors, l'ouvert $\omega$ défini par $\omega = \prod_{i=1}^n ]x_i - \frac{1}{3}, x_i + \frac{1}{3}[$ ne contient aucun point de $\mathbf{Z}^n$ à l'exception de $x$.

### 2.2.2 Le lemme fondamental

Pour la réciproque, le point crucial est le suivant [3] :

**2.6 Lemme.** *(dit* **fondamental***) Soit $E$ un $K$-espace vectoriel de dimension $n$, $L$ un sous-groupe de $E$ et $a \in L$, $a \neq 0$. On pose $D = Ka$. Soit $H$ un supplémentaire de $D$ et $p : E \to H$ la projection parallèlement à $D$.*

*1) Si $K = \mathbf{R}$ et si $L$ est un sous-groupe discret de $E$, $p(L)$ est un sous-groupe discret de $H$.*

*2) Si $L \cap D = \mathbf{Z}a$, si $p(L)$ admet une $\mathbf{Z}$-base $\epsilon_1, \ldots, \epsilon_{r-1}$ et si l'on écrit $\epsilon_i = p(e_i)$ avec $e_i \in L$, alors $a, e_1, \ldots, e_{r-1}$ est une $\mathbf{Z}$-base de $L$.*

*Démonstration.* On commence par un lemme préliminaire :

**2.7 Lemme.** *On suppose $K \subset \mathbf{R}$. Avec les notations précédentes, si $y$ est dans $p(L)$, il existe $x \in L$ tel que $p(x) = y$ et $x = \lambda a + y$, avec $\lambda \in K$ et $0 \leq \lambda < 1$.*

*Démonstration.* Comme $y$ est dans $p(L)$ il s'écrit $y = p(x_0)$ avec $x_0 \in L$ et on a $x_0 = \mu a + y$ avec $\mu \in K$. Mais, si $[\mu]$ désigne la partie entière de $\mu$, on a $0 \leq \lambda := \mu - [\mu] < 1$ et si on pose $x = x_0 - [\mu]a = \lambda a + y$, on a $x \in L$ (car $a$ est dans $L$) et toujours $p(x) = y$, d'où le résultat.

Revenons au point 1) de 2.6. On utilise la caractérisation 2.1. Soit $\Omega$ une partie bornée de $E$ que l'on peut supposer contenue dans une boule $B(0, R)$ pour une norme quelconque. Si $y$ est dans $p(L) \cap \Omega$ on écrit $y = p(x)$ avec $x = \lambda a + y \in L$ et $0 \leq \lambda < 1$ grâce au lemme. On a alors $\|x\| \leq \|a\| + \|y\|$ et, comme $y$ est dans $B(0, R)$, $\|x\| \leq R + \|a\|$. Le point $x$ est donc dans $L \cap B(0, R + \|a\|)$ qui est fini puisque $L$ est discret. Mais alors, il n'y a qu'un nombre fini de $y = p(x)$ dans $p(L) \cap \Omega$.

Pour le point 2) on montre d'abord que $a, e_1, \ldots e_{r-1}$ est une famille libre. En effet, si l'on a une relation $\lambda a + \sum_{i=1}^{r-1} \lambda_i e_i = 0$, on en déduit, en appliquant

3. Ici, le corps $K$ est quelconque.

$p$, qu'on a $\sum_{i=1}^{r-1} \lambda_i \epsilon_i = 0$, ce qui montre que les $\lambda_i$ sont nuls, et, comme $a$ est non nul, il en résulte que $\lambda$ est nul lui aussi.

On montre ensuite que ces vecteurs forment une $\mathbf{Z}$-base de $L$. En effet, si $x$ est dans $L$, on a $p(x) = \sum_{i=1}^{r-1} \lambda_i \epsilon_i$ avec $\lambda_i \in \mathbf{Z}$ (car les $\epsilon_i$ forment une $\mathbf{Z}$-base de $p(L)$). Mais cela signifie qu'on a $p(x - \sum_{i=1}^{r-1} \lambda_i e_i) = 0$, donc que ce vecteur est dans $L \cap D = \mathbf{Z}a$ et on a le résultat.

### 2.2.3 La fin de la démonstration de 2.5

On raisonne par récurrence sur $n$. Le cas $n = 1$ est le lemme bien connu suivant :

**2.8 Lemme.** *Soit $L$ un sous-groupe additif de $\mathbf{R}$.*

*1) Si $L$ est discret, il existe $a \in \mathbf{R}$ tel que $L = \mathbf{Z}a$.*

*2) Sinon, $L$ est partout dense dans $\mathbf{R}$. C'est le cas, en particulier, si $L$ contient deux réels dont le rapport est irrationnel.*

*Démonstration.* 1) Si $L$ est nul l'assertion est évidente. Sinon, soit $b \in L$, $b \neq 0$. Comme $L$ est un sous-groupe, $-b$ est aussi dans $L$, de sorte qu'on peut supposer $b > 0$. En vertu de 2.1, il n'y a qu'un nombre fini d'éléments de $L$ dans $]0, b]$, soit $a$ le plus petit d'entre eux. Si $x$ est dans $L$, il existe $n \in \mathbf{Z}$ tel que $na \leq x < (n+1)a$ (c'est le fait que $\mathbf{R}$ est archimédien). Mais alors $x - na$ est dans $L$ et $< a$, donc nul et on a bien montré que $x$ est dans $\mathbf{Z}a$.

2) En vertu de 2.4, il y a dans $L$ des éléments de valeur absolue arbitrairement petite, donc, comme $\mathbf{R}$ est archimédien, des éléments de $L$ dans tout intervalle : $L$ est partout dense. Si l'on a $b, c \in L$ avec $b/c \notin \mathbf{Q}$, $L$ n'est pas discret, sinon il existerait $a \in \mathbf{R}^*$ tel que $L = \mathbf{Z}a$ et on aurait $b = ma$ et $c = na$ avec $m, n$ entiers, de sorte que $b/c$ serait rationnel.

Revenons à 2.5. Pour l'hérédité, on choisit $b \in L$, non nul et on pose $D = \mathbf{R}b$. Comme $D \cap L$ est discret, le lemme précédent montre qu'il est de la forme $\mathbf{Z}a$ et on a encore $D = \mathbf{R}a$. On choisit un supplémentaire $H$ de $D$, on projette $L$ dans $H$ parallèlement à $D$. En vertu de 2.6, $p(L)$ est un sous-groupe discret de $H$, donc un sous-réseau par hypothèse de récurrence. Il admet donc une $\mathbf{Z}$-base et $L$ aussi, toujours par 2.6

**2.9 Corollaire.** *Soit $L$ un réseau de $E$ et $M$ un sous-groupe de $L$. Alors $M$ est un sous-réseau de $E$.*

*Démonstration.* C'est clair car $L$ est discret, donc aussi $M$.

## 2.3 Applications pratiques

### 2.3.1 Reconnaître qu'un sous-groupe est un sous-réseau

Le problème est le suivant. On considère un **R**-espace vectoriel $E$ de dimension $n$, $r$ vecteurs $u_1, \ldots, u_r$ de $E$, donnés par la matrice $A$, de taille $n \times r$, de leurs coordonnées sur une base de $E$ et on appelle $L$ le sous-groupe additif de $E$ engendré par les $u_i$. Deux questions se posent :

- À quelle condition le sous-groupe $L$ est-il un sous-réseau ?
- Si c'est un sous-réseau, comment en déterminer une **Z**-base ?

Un premier travail consiste à sélectionner, parmi les $r$ vecteurs donnés, une famille libre maximale. Une procédure pour cela consiste à extraire de $A$ une sous-matrice inversible maximale. Les logiciels de calcul formel permettent de faire cela sans effort. Quitte à remplacer $E$ par le sous-espace vectoriel engendré par les $u_i$, on peut alors supposer que le rang de la famille $(u_i)$ est égal à $n$ et sélectionner une base parmi les $u_i$. À un petit changement de notations près, on est ramené à prouver le théorème suivant :

**2.10 Théorème.** *Soit $E$ un* **R***-espace vectoriel de dimension $n$, $e_1, \ldots, e_n$ une base de $E$ et $u_1, \ldots, u_r$ des vecteurs de $E$. Soit $L$ le sous-groupe additif de $E$ engendré par les $e_i$ et les $u_j$. Alors $L$ est un réseau si et seulement si les $u_j$ s'écrivent comme combinaisons linéaires à coefficients* **rationnels** *des $e_i$.*

*Démonstration.* Montrons que la condition est nécessaire [4]. Soit $M$ le réseau engendré par les $e_i$. Si $L$ est un réseau, $M$ en est un sous-réseau et en vertu de 3.13, il existe une **Z**-base $\epsilon_1, \ldots, \epsilon_n$ de $L$ adaptée au couple $L, M$, c'est-à-dire telle que $d_1\epsilon_1, \ldots, d_n\epsilon_n$ soit une **Z**-base de $M$. Comme la matrice de passage des $e_i$ aux $d_j\epsilon_j$ est dans $GL(n, \mathbf{Z})$ et que les $u_k$ sont combinaisons linéaires à coefficients entiers des $\epsilon_j$, on voit que les $u_k$ sont bien combinaisons linéaires des $e_i$ à coefficients rationnels.

Pour la réciproque, munissons $E$ de la structure euclidienne pour laquelle la base des $e_i$ est orthonormée. Il suffit de montrer que $L$ est discret et pour cela, en vertu de 2.4, de montrer que la norme de ses vecteurs non nuls admet un minimum. Soit $d$ un dénominateur commun des coefficients des $u_j$ sur les $e_i$ et soit $v$ un vecteur non nul de $L$. Il s'écrit sous la forme $\dfrac{a_1}{d}e_1 + \cdots + \dfrac{a_n}{d}e_n$ avec des $a_i \in \mathbf{Z}$. Si $v$ est non nul, l'un des $\dfrac{a_i}{d}$ l'est aussi, et on a $\|v\|^2 \geq \frac{1}{d^2}$.

4. La preuve qui suit utilise le paragraphe suivant mais on peut aussi raisonner en utilisant le lemme fondamental de projection et 2.8.

### 2.3.2 Détermination pratique d'une Z-base

On suppose qu'on est dans la situation de 2.10 et on donne un algorithme pour déterminer une **Z**-base de $L$. On procède par récurrence sur $r$ et on est ainsi ramené au cas où le réseau $L$ est engendré par la base canonique $e_i$ et par un vecteur supplémentaire $u = \frac{c_1}{d_1}e_1 + \cdots + \frac{c_n}{d_n}e_n$, avec les $c_i$ dans $\mathbf{Z}$ et non tous nuls, $d_i \in \mathbf{N}^*$ et $c_i$ et $d_i$ premiers entre eux.

**2.11 Lemme.** *Avec les notations précédentes, il existe un entier $\lambda$ tel que $c_1 + \lambda d_1, c_2, \ldots, c_n$ soient premiers entre eux dans leur ensemble.*

*Démonstration.* Il suffit de trouver $\lambda$ tel que $c_1 + \lambda d_1$ et $c_2$ soient premiers entre eux. Soit $p$ un facteur premier de $c_2$. Si $p$ divise $d_1$, il ne divise pas $c_1$, donc il ne divise aucun $c_1 + \lambda d_1$. On appelle $p_1, \ldots, p_r$ les facteurs premiers distincts de $c_2$ qui ne divisent pas $d_1$, de sorte que $d_1$ est inversible modulo $p_i$. On note $a_i$ la classe de $-c_1/d_1$ modulo $p_i$ et $b_i$ un entier dont la classe modulo $p_i$ est distincte de $a_i$. Comme les $p_i$ sont premiers entre eux, le lemme chinois assure qu'il existe $\lambda$ congru à $b_i$ modulo $p_i$ pour tout $i$. Mais alors, $\lambda d_1 + c_1$ n'est multiple d'aucun $p_i$, donc premier avec $c_2$.

**2.12** *Remarque.* Si $\lambda$ est l'entier donné par le lemme, il est clair que le réseau $L$ est égal au réseau engendré par $u + \lambda e_1$ et les $e_i$. Autrement dit, quitte à remplacer $u$ par $u + \lambda e_1$, on peut supposer les $c_i$ premiers entre eux.

On est ainsi ramené à prouver la proposition suivante.

**2.13 Proposition.** *Soit $L$ le sous-réseau engendré par les vecteurs $e_1, \ldots, e_n$ d'une base de $E$ et par le vecteur $u = \frac{c_1}{d_1}e_1 + \cdots + \frac{c_n}{d_n}e_n$, avec les $c_i$ dans $\mathbf{Z}$ et non tous nuls, $d_i \in \mathbf{N}^*$ et $c_i$ et $d_i$ premiers entre eux. On suppose que les $c_i$ sont premiers entre eux, on note $m = ppcm(d_1, \ldots, d_n)$ et on pose pour tout $i$, $m = d_i\delta_i$.*

*1) Les entiers $c_i\delta_i$ sont premiers entre eux.*

*2) Il existe une matrice $A_0 = (a_{ij})$, de taille $(n-1) \times n$, à coefficients entiers, telle que la matrice $A$ obtenue en bordant $A_0$ par la première ligne $(c_1\delta_1, \ldots, c_n\delta_n)$ soit dans $GL(n, \mathbf{Z})$.*

*3) Les vecteurs $u$ et $\epsilon_i = \sum_{j=1}^{n} a_{ij}e_j$, pour $i = 1, \ldots, n-1$ forment une **Z**-base de $L$.*

*Démonstration.* 1) Supposons qu'un nombre premier $p$ divise tous les $c_i\delta_i$. Par hypothèse, les $c_i$ sont premiers entre eux, donc $p$ divise au moins un des $\delta_i$. Mais, la définition des $\delta_i$ assure qu'ils sont premiers entre eux (sinon $m$ ne serait pas le *ppcm* des $d_i$), de sorte que $p$ ne les divise pas tous. Supposons par exemple que $p$ ne divise pas $\delta_1, \ldots, \delta_k$ mais qu'il divise $\delta_{k+1}, \ldots, \delta_n$ (avec

$1 \leq k < n$). Comme il divise tous les $c_i\delta_i$, il divise donc $c_1$. Mais, $p$ divise $\delta_n$, donc $m = \delta_n d_n = \delta_1 d_1$, donc, par Euclide, il divise $d_1$. Cela contredit le fait que la fraction $c_1/d_1$ est irréductible.

2) Cela résulte du lemme 1.5.

3) Appelons $A_1, \ldots, A_n$ les $n-1$-mineurs de la matrice $A_0$. On a donc $\det A = \sum_{i=1}^n c_i\delta_i A_i = 1$. Soit $M$ la matrice $n \times n$ obtenue en bordant $A_0$ par la ligne des $c_i/d_i$. On a $\det M = \displaystyle\sum_{i=1}^{n} A_i c_i/d_i = \frac{1}{m}\sum_{i=1}^{n} A_i c_i \delta_i = \frac{1}{m}\cdot$ Comme ce nombre est non nul, on en déduit que les vecteurs lignes de $M$, c'est-à-dire $u$ et les $\epsilon_i$ sont indépendants. De plus, les $e_i$ sont donnés, en fonction de ces vecteurs, par la matrice inverse de $M$, dont les coefficients sont des produits de $m = (\det M)^{-1}$ par l'une au plus des fractions $\dfrac{c_i}{d_i}$ et par certains des $a_{ij}$. Comme $m$ est multiple des $d_i$, les coefficients de $M^{-1}$ sont entiers. Cela montre que les $e_i$ sont dans le réseau de $\mathbf{Z}$-base $u, \epsilon_i$, qui est donc égal à $L$.

### 2.3.3 Un exemple

On considère le réseau $L$ de $\mathbf{R}^3$ engendré par les vecteurs $e_1, e_2, e_3$ de la base canonique et par le vecteur $u_0 = \dfrac{2}{3}e_1 + \dfrac{4}{35}e_2 + \dfrac{6}{7}e_3$ et on détermine une $\mathbf{Z}$-base de $L$.

On commence par changer $u_0$ en $u = u_0 + e_1 = \dfrac{5}{3}e_1 + \dfrac{4}{35}e_2 + \dfrac{6}{7}e_3$, afin de rendre les numérateurs $c_i$ premiers entre eux. On a $m = ppcm(d_1, d_2, d_3) = 105$ et $\delta_1 = 35$, $\delta_2 = 3$, $\delta_3 = 15$, puis $c_1\delta_1 = 175$, $c_2\delta_2 = 12$ et $c_3\delta_3 = 90$. Comme 175 et 12 sont premiers entre eux, on a une relation de Bézout : $5 \times 175 - 73 \times 12 = -1$, de sorte qu'on peut prendre $A_0 := \begin{pmatrix} 73 & 5 & 0 \\ 0 & 0 & -1 \end{pmatrix}$, matrice dont les mineurs sont $A_1 = -5$, $A_2 = 73$ et $A_3 = 0$. On a donc trouvé la $\mathbf{Z}$-base de $L$ : $u = \dfrac{5}{3}e_1 + \dfrac{4}{35}e_2 + \dfrac{6}{7}e_3$, $v = 73e_1 + 5e_2$ et $w = -e_3$.

On peut d'ailleurs vérifier que les $e_i$ sont bien dans le réseau de $\mathbf{Z}$-base $u, v, w$ : la matrice de passage est $M^{-1} = \begin{pmatrix} -525 & 12 & -450 \\ 7665 & -175 & 6570 \\ 0 & 0 & -1 \end{pmatrix}$ et elle est bien à coefficients entiers.

**2.14** *Exercice.* Trouver une $\mathbf{Z}$-base du réseau de $\mathbf{R}^3$ engendré par la base canonique et par les vecteurs $u = \frac{13}{7}e_1 + \frac{25}{43}e_2 + \frac{53}{17}e_3$ et $v = -\frac{31}{12}e_1 + \frac{4}{19}e_2 + \frac{1729}{18}e_3$.

# 3 Structure des sous-réseaux

## 3.1 Quelques rappels sur les groupes

On renvoie à [DP] pour les généralités sur les groupes.

### 3.1.1 Ordres

**3.1 Proposition.** *Soit $G$ un groupe cyclique d'ordre $n$. Pour tout $d$ diviseur de $n$ il existe un unique sous-groupe de $G$ d'ordre $d$.*

*Démonstration.* C'est bien connu. On peut supposer $G = \mathbf{Z}/n\mathbf{Z}$ et, si l'on écrit $n = de$, le sous-groupe cherché est engendré par $\overline{e}$.

**3.2 Proposition.** *Soit $G$ un groupe abélien (noté additivement).*

*1) Si $a$ et $b$ sont des éléments de $G$ d'ordres $p, q$ premiers entre eux, la somme $a + b$ est d'ordre $pq$.*

*2) Si $a_1, \ldots, a_n$ sont des éléments d'ordre $p_1, \ldots, p_n$ deux à deux premiers entre eux, la somme des $a_i$ est d'ordre $p_1 \cdots p_n$.*

*Démonstration.* Le point 2) s'obtient par récurrence sur $n$. Pour 1) on note d'abord qu'on a $pq(a+b) = 0$, de sorte que l'ordre de $a+b$ divise $pq$. Supposons qu'on ait $r(a + b) = 0$ avec $r > 0$. En multipliant par $p$ on a $(rp)b = 0$, de sorte que $q$ divise $rp$, donc $r$ par le théorème de Gauss. On montre de même que $p$ divise $r$ et on conclut en utilisant encore le fait que $p$ et $q$ sont premiers entre eux.

### 3.1.2 Exposant

**3.3 Définition.** *Soit $G$ un groupe abélien fini (noté additivement).* **L'exposant** *de $G$ est le plus petit entier positif $d$ qui vérifie $dx = 0$ pour tout $x \in G$.*

L'exposant existe car le cardinal du groupe annule tous ses éléments.

**3.4 Lemme.** *Soit $G$ un groupe abélien fini d'exposant $d$. On a les propriétés suivantes.*

*1) Il existe un élément de $G$ d'ordre $d$.*

*2) Si $n$ annule $G$, $n$ est multiple de $d$.*

*3) Pour tout $x \in G$, l'ordre de $x$ est un diviseur de $d$.*

*Démonstration.* Le point 1) est évident car $G$ est fini. Pour 2) on divise $n$ par $d$ : $n = qd + r$ avec $0 \leq r < d$. Comme $n$ et $d$ annulent $G$ il en est de même de $r$ et, par définition de $d$, on a $r = 0$.

3) Soit $n$ l'ordre de $x$ (c'est-à-dire le plus petit entier positif qui vérifie $nx = 0$). Cette fois on effectue la division euclidienne de $d$ par $n$ : $d = nq + r$ avec $0 \leq r < n$. On a alors $dx = nx = 0$, donc $rx = 0$, donc $r = 0$ par définition de l'ordre.

Nous aurons aussi besoin du résultat suivant :

**3.5 Proposition.** *Soit $G$ un groupe abélien engendré par des éléments $x_1$, ..., $x_r$ d'ordres $n_1, \ldots, n_r$. Il existe un élément de $G$ dont l'ordre est le ppcm des $n_j$. L'exposant de $G$ est égal à ce ppcm.*

*Démonstration.* Soit $m$ le *ppcm* des $n_j$. On peut écrire tous les $n_j$ comme produits de puissances de nombres premiers $p_1, \ldots, p_s$, distincts (avec éventuellement certains exposants nuls) et $m$ s'écrit alors $m = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ où $\alpha_i$ est le maximum des exposants de $p_i$ dans les différents $n_j$. Il en résulte que $p_i^{\alpha_i}$ divise l'un des $n_j$. Comme le sous-groupe engendré par $x_j$ est cyclique d'ordre $n_j$, il contient un élément $y_i$ d'ordre $p_i^{\alpha_i}$ (voir 3.1) et comme les $p_i^{\alpha_i}$ sont deux à deux premiers entre eux, le produit $y_1 \cdots y_r$ est d'ordre $m$ en vertu de 3.2. L'assertion sur l'exposant est alors immédiate.

### 3.1.3 Torsion

**3.6 Proposition-Définition.** *Soit $G$ un groupe abélien. L'ensemble $T$ des $x \in G$ qui sont annulés par un entier non nul est un sous-groupe de $G$ appelé* **sous-groupe de torsion** *de $G$. On dit que $G$ est* **de torsion** *s'il est égal à son sous-groupe de torsion.*

*Démonstration.* C'est facile : si $x, y$ sont dans $T$ il existe $m, n \in \mathbf{N}^*$ tels que $mx = ny = 0$ et on a alors $mn(x - y) = 0$.

## 3.2 Deux résultats d'unicité

### 3.2.1 Groupes abéliens libres

**3.7 Théorème.** *Soient $r, s$ deux entiers positifs. Si les groupes $\mathbf{Z}^r$ et $\mathbf{Z}^s$ sont isomorphes on a $r = s$.*

*Démonstration.* On raisonne par l'absurde en supposant $r < s$ et on plonge $\mathbf{Z}^r$ dans $\mathbf{Q}^r$. Il existe donc un homomorphisme de groupes injectif $\varphi : \mathbf{Z}^s \to \mathbf{Q}^r$. Soit $e_1, \ldots, e_s$ la $\mathbf{Z}$-base canonique de $\mathbf{Z}^s$. Montrons que les $s$ vecteurs $\varphi(e_i)$ sont indépendants sur $\mathbf{Q}$, ce qui sera une contradiction puisque $\mathbf{Q}^r$ est un $\mathbf{Q}$-espace vectoriel de dimension $r$. Si l'on a $\sum_{i=1}^{s} \frac{p_i}{q_i} \varphi(e_i) = 0$, on peut supposer tous les $q_i$ égaux à $q$ en prenant un dénominateur commun et on

en déduit $\sum_{i=1}^{s} p_i\varphi(e_i) = 0 = \varphi(\sum_{i=1}^{s} p_i e_i)$. Mais, comme $\varphi$ est injectif, on a $\sum_{i=1}^{s} p_i e_i = 0$, de sorte que les $p_i$ sont nuls.

### 3.2.2 Produits de groupes cycliques

Rappelons que, pour des entiers $a, b$, la notation $a|b$ signifie que $a$ divise $b$. Le but de ce paragraphe est de prouver le théorème suivant :

**3.8 Théorème.** *Soit $G$ un groupe abélien fini. On suppose que $G$ s'écrit de deux manières comme produit de groupes cycliques :*

$$G \simeq \mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_r\mathbf{Z} \quad \text{et} \quad G \simeq \mathbf{Z}/\delta_1\mathbf{Z} \times \cdots \times \mathbf{Z}/\delta_s\mathbf{Z}$$

*avec $r, s \geq 1$ et où les $d_i$ et les $\delta_j$ sont des entiers $\geq 2$ qui vérifient $d_1|d_2|\cdots d_r$ et $\delta_1|\delta_2|\cdots|\delta_s$. Alors, on a $r = s$ et, pour tout $i = 1, \ldots, r$, $d_i = \delta_i$.*

*Démonstration.* Pour un groupe abélien $G$ et un entier $n$, on note $\mu_n : G \to G$ la multiplication par $n$, $x \mapsto nx$.

**3.9 Lemme.** *Si $G$ est cyclique d'ordre $d$ le cardinal de* $\operatorname{Ker}\mu_n$ *est égal à $pgcd(n, d)$.*

*Démonstration.* On peut supposer $G = \mathbf{Z}/d\mathbf{Z}$. Soit $\delta = pgcd(n, d)$. On a donc $n = \delta n'$ et $d = \delta d'$ avec $n'$ et $d'$ premiers entre eux. Un élément $\overline{x}$ de $G$, avec $0 \leq x < d$ est dans $\operatorname{Ker}\mu_n$ si et seulement si on a $nx = kd$, donc $n'x = kd'$. En vertu du théorème de Gauss, cela signifie exactement que $x$ est multiple de $d' : x = 0, d', \ldots, (\delta - 1)d'$, d'où le résultat.

**3.10 Lemme.** *Si $G$ est isomorphe à un produit $G \simeq \mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_r\mathbf{Z}$, le cardinal de* $\operatorname{Ker}\mu_n$ *est égal à $\prod_{i=1}^{r} pgcd(n, d_i)$.*

*Démonstration.* Cela résulte du lemme précédent appliqué à chaque facteur.

Le théorème est alors conséquence du lemme purement arithmétique suivant :

**3.11 Lemme.** *Soient $r, s$ des entiers $\geq 1$ et $d_i$ et $\delta_j$ des entiers $\geq 2$ qui vérifient $d_1|d_2|\cdots d_r$ et $\delta_1|\delta_2|\cdots|\delta_s$. On suppose qu'on a, pour tout $n \in \mathbf{N}^*$ l'égalité :*

$$(*_n). \qquad D_n := \prod_{i=1}^{r} pgcd(n, d_i) = \Delta_n := \prod_{j=1}^{s} pgcd(n, \delta_j)$$

*Alors, on a $r = s$ et pour tout $i = 1, \ldots, r$, $d_i = \delta_i$.*

*Démonstration.* Si $n$ est un multiple de $d_r$ (resp. $\delta_s$) on a $D_n = d_1 \cdots d_r$ (resp. $\Delta_n = \delta_1 \cdots \delta_s$). Appliquant $(*_n)$ avec $n$ multiple à la fois de $d_r$ et $\delta_s$, on obtient $d_1 \cdots d_r = \delta_1 \cdots \delta_s$. On note ensuite que $d_r$ (resp. $\delta_s$) est le plus petit entier $n$ tel que $D_n = d_1 \cdots d_r$ (resp. $\Delta_n = \delta_1 \cdots \delta_s$). En effet, si $n < d_r$ par exemple, on a $pgcd(n, d_i) \leq d_i$ pour $i < r$ et $pgcd(n, d_r) \leq n < d_r$. Cela montre qu'on a $d_r = \delta_s$.

Supposons que la propriété soit fausse et choisissons un contre-exemple avec $r$ minimum. Comme on a $d_r = \delta_s$, donc $pgcd(n, d_r) = pgcd(n, \delta_s)$, les entiers $d_1, \ldots, d_{r-1}$ et $\delta_1, \ldots, \delta_{s-1}$ vérifient encore les égalités analogues à $(*_n)$. On en déduit, par minimalité, qu'on a $r - 1 = s - 1$ et que les $d_i$ sont égaux aux $\delta_i$ et c'est une contradiction.

**3.12** *Remarque.* Nous verrons plus loin (voir 3.20) que tout groupe abélien fini s'écrit effectivement comme produit de groupes cycliques.

## 3.3 Le théorème fondamental

Le corps de base est toujours égal à $\mathbf{R}$.

**3.13 Théorème.** *Soit $L$ un réseau de $E$ et $M$ un sous-groupe de $L$. Il existe une $\mathbf{Z}$-base $e_1, \ldots, e_n$ de $L$, un entier $r$ avec $0 \leq r \leq n$ et des entiers $d_1, \ldots, d_r \in \mathbf{N}^*$ tels que $d_1 | d_2 | \cdots | d_r$ et que $d_1 e_1, \ldots, d_r e_r$ soit une $\mathbf{Z}$-base de $M$. On dit que $e_1, \ldots, e_n$ est une $\mathbf{Z}$-base de $L$* **adaptée** *au sous-groupe $M$ (ou au couple $L, M$). Les entiers $r$ et $d_1, \ldots, d_r$ sont déterminés de manière unique.*

Pour la preuve de l'unicité, voir 3.16.

### 3.3.1 Preuve de 3.13 : le cas $\operatorname{rg} L = \operatorname{rg} M$

Dans ce paragraphe, on montre 3.13 dans le cas où $M$ est lui même un réseau de $E$ :

**3.14 Théorème.** *Soient $L$ et $M$ deux réseaux de $E$ avec $M \subset L$. Alors :*

*1) Le groupe quotient $L/M$ est fini.*

*2) Il existe une $\mathbf{Z}$-base $e_1, \ldots, e_n$ de $L$ et des entiers $d_1, \ldots, d_n \in \mathbf{N}^*$ tels que $d_1 | d_2 | \cdots | d_n$ et que $d_1 e_1, \ldots, d_n e_n$ soit une $\mathbf{Z}$-base de $M$.*

*3) Le groupe quotient $L/M$ est isomorphe au produit direct $\mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_n\mathbf{Z}$. Il est d'ordre $d_1 \cdots d_n$ et d'exposant $d_n$.*

*Démonstration.* Notons déjà que le point 3) est conséquence de 2). En effet, on considère l'homomorphisme $\varphi : L \to \mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_n\mathbf{Z}$ qui à $\sum_{i=1}^n x_i e_i$

associe $(\overline{x_1}, \ldots, \overline{x_n})$. Il est clairement surjectif et son noyau est $M$, d'où le résultat.

Prouvons le point 1). On considère des $\mathbf{Z}$-bases quelconques $e_1, \ldots, e_n$ de $L$ et $\epsilon_1, \ldots, \epsilon_n$ de $M$. Comme $M$ est inclus dans $L$, on peut écrire $\epsilon_j = \sum_{i=1}^n a_{ij} e_i$ avec $a_{ij} \in \mathbf{Z}$. Comme $(\epsilon_j)$ est une base de $E$ sur $\mathbf{R}$, la matrice $A = (a_{ij})$ est inversible et son inverse $B$ est de la forme $B = \frac{1}{d}C$ où $d = \det A$ est dans $\mathbf{Z}$ et où $C = (c_{ij})$, est la comatrice [5] de $A$, donc à coefficients entiers. On a donc $e_j = \frac{1}{d}\sum_{i=1}^n c_{ij}\epsilon_i$, de sorte que $de_j$ est combinaison linéaire des $\epsilon_i$ à coefficients entiers, donc est dans $M$. Comme $L/M$ est un groupe abélien engendré par un nombre fini d'éléments $\overline{e_1}, \ldots, \overline{e_n}$ tous d'ordre fini $\leq d$, ses éléments ont tous une écriture de la forme $\sum_{i=1}^n x_i \overline{e_i}$ avec $0 \leq x_i < d$, ce qui prouve que $L/M$ est fini.

Il reste le point 2) que l'on prouve par récurrence sur $n$. Le cas $n = 1$ est clair car on a vu que les sous-groupes de $\mathbf{R}$ sont de la forme $a\mathbf{Z}$. Soit $d$ l'exposant du groupe fini $G := L/M$. On peut supposer $d > 0$, sinon $M = L$ et le résultat est évident. Il existe un élément $b \in L$ tel que $\overline{b}$ soit d'ordre exactement $d$ dans $G$. On considère la droite $D = \mathbf{R}b$. Le groupe $L \cap D$ est discret, donc un réseau de $D$, donc de la forme $\mathbf{Z}a$ avec $a \in L$. Je dis que $\overline{a}$ est encore d'ordre $d$ dans $G$. Déjà, il est d'ordre $\leq d$ par 3.4. Ensuite, comme on a $b = \lambda a$ avec $\lambda \in \mathbf{Z}$, si $n$ annule $\overline{a}$, il annule aussi $\overline{b}$, donc est $\geq d$.

En définitive, on a donc $D \cap M = \mathbf{Z}da$. On choisit un supplémentaire $H$ de $D$ dans $E$ et on applique le lemme fondamental 2.6 aux deux réseaux $L$ et $M$ et à la projection $p : E \to H$ parallèlement à $D$. On a $p(M) \subset p(L)$ et ces sous-groupes sont des réseaux [6] de $H$. En vertu de l'hypothèse de récurrence, il existe une $\mathbf{Z}$-base $\epsilon_1, \ldots, \epsilon_{n-1}$ de $p(L)$ et des entiers $d_i > 0$ avec $d_1 | \cdots | d_{n-1}$ tels que $d_1\epsilon_1, \ldots, d_{n-1}\epsilon_{n-1}$ soit une $\mathbf{Z}$-base de $p(M)$. De plus, $d_{n-1}$ divise $d$. En effet, le point 3) du théorème appliqué à $p(L)$ et $p(M)$ montre que $H := p(L)/p(M)$ est un groupe d'exposant $d_{n-1}$. Comme $d$ annule $G$, donc $H$, on a le résultat par 3.4.

On relève alors $d_i\epsilon_i$ en $e'_i \in M$. On obtient ainsi une $\mathbf{Z}$-base $e'_1, \ldots, e'_{n-1}, da$ de $M$. Posons alors $e_i = \frac{e'_i}{d_i}$. On aura terminé si l'on montre que $e_i$ est dans $L$ car alors $e_1, \ldots, e_{n-1}, a$ sera la $\mathbf{Z}$-base de $L$ cherchée.

Comme $\epsilon_i = \frac{p(e'_i)}{d_i} = p(e_i)$ est dans $p(L)$, on a $e_i = f_i + \lambda_i a$ avec $f_i \in L$ et $\lambda_i \in \mathbf{R}$ et il reste à montrer que $\lambda_i$ est entier. Mais, on a $de_i = df_i + d\lambda_i a$, et, comme $f_i$ est dans $L$ et que $d$ annule $L/M$, $df_i$ est dans $M$. Par ailleurs, on sait que $d_i e_i = e'_i$ est dans $M$, donc aussi $de_i$ puisque $d$ est multiple de $d_i$. Mais alors $d\lambda_i a$ est dans $M \cap \mathbf{R}a = \mathbf{Z}da$, de sorte que $\lambda_i$ est entier.

5. C'est-à-dire la transposée de la matrice des cofacteurs.

6. *A priori* ce sont des sous-réseaux, mais le relèvement des $\mathbf{Z}$-bases montre qu'ils sont de rang maximal.

### 3.3.2 Preuve de 3.13 : le cas $L/M$ sans torsion

On a vu que le cas $\operatorname{rg} L = \operatorname{rg} M$ conduit à un groupe quotient $L/M$ fini, donc de torsion. Le cas envisagé maintenant est donc l'opposé du cas précédent.

**3.15 Proposition.** *Soit $L$ un réseau et $M$ un sous-groupe de $L$. On suppose que $L/M$ est sans torsion. Alors, si $e_1, \ldots, e_r$ est une $\mathbf{Z}$-base de $M$, on peut la compléter en une $\mathbf{Z}$-base $e_1, \ldots, e_r, e_{r+1}, \ldots, e_n$ de $L$.*

*Démonstration.* On peut supposer $M \neq 0$ et on raisonne par récurrence sur $n$, le cas $n = 1$ étant trivial. On pose $a = e_1$ et $D = \mathbf{R}a$ et on va appliquer le lemme fondamental 2.6. On note d'abord qu'on a $D \cap M = \mathbf{Z}a$. C'est évident avec l'indépendance des $e_i$. On note ensuite qu'on a aussi $D \cap L = \mathbf{Z}a$. En effet, en vertu de 2.8, on a $D \cap L = \mathbf{Z}b$ et comme $a$ est dans $L$ on a $a = db$. Mais si $d$ est différent de $\pm 1$ cela signifie qu'on a $d\overline{b} = \overline{0}$ dans $L/M$ et cela contredit le fait que $L/M$ est sans torsion.

On choisit alors comme supplémentaire de $D$ un hyperplan $H$ contenant $e_2, \ldots, e_r$ et on appelle $p$ la projection de $E$ sur $H$ parallèlement à $D$. Le quotient $p(L)/p(M)$ est encore sans torsion. En effet, si l'on a $dp(x) \in p(M)$ avec $x \in L$ et $d \in \mathbf{N}^*$, on a $dx = y + \lambda a$ avec $y \in M$ et $\lambda \in \mathbf{R}$. Mais, comme $dx$ et $y$ sont dans $L$, $\lambda a$ aussi, donc $\lambda$ est entier et $\lambda a$ est aussi dans $M$. Il en résulte que $dx$ est dans $M$, ce qui, comme $L/M$ est sans torsion, impose $x \in M$, donc $p(x) \in p(M)$. On peut alors appliquer la récurrence. Comme les vecteurs $e_2, \ldots, e_r$ forment une $\mathbf{Z}$-base de $p(M)$ on peut la compléter en une $\mathbf{Z}$-base $e_2, \ldots, e_r, \epsilon_{r+1}, \ldots, \epsilon_n$ de $p(L)$ et le lemme 2.6 permet de la relever [7] en une $\mathbf{Z}$-base $a, e_2, \ldots, e_r, e_{r+1}, \ldots, e_n$ de $L$.

### 3.3.3 Preuve de 3.13 : le cas général

On peut maintenant finir de prouver 3.13. Soit $\varphi : L \to L/M$ la projection canonique et soit $T$ le sous-groupe de torsion de $L/M$. On pose $N = \varphi^{-1}(T)$, de sorte qu'on a $T = N/M$. C'est un sous-groupe de $L$, donc un sous-réseau. On vérifie d'abord que $N$ et $M$ ont même rang. En effet, sinon, il existe $e \in N$ tel que $e \notin <M>$, ce qui implique que $de \notin M$ pour tout $d \in \mathbf{N}^*$. Mais alors, $\overline{e}$ est d'ordre infini dans $N/M$, ce qui contredit le fait que ce groupe est de torsion. On vérifie ensuite que $L/N$ est sans torsion. En effet, si $dx \in N$ avec $x \in L$ et $d \in \mathbf{N}^*$, comme $N/M$ est de torsion, il existe $\delta \in \mathbf{N}^*$ tel que $\delta(dx) \in M$. Mais alors $(\delta d)x \in M$ donc l'image $\overline{x}$ est de torsion dans $L/M$, donc $\overline{x}$ est dans $T$ et $x$ est dans $N$. On peut alors appliquer 3.14 à $N$ et $M$. Si l'on a $\operatorname{rg} N = \operatorname{rg} M = r$ il existe une $\mathbf{Z}$-base $e_1, \ldots, e_r$ de $N$ et

7. Le lecteur vérifiera qu'on peut relever les premiers vecteurs en eux-mêmes.

des $d_i$ convenables tels que $d_1e_1, \ldots, d_re_r$ soit une $\mathbf{Z}$-base de $M$. On applique ensuite 3.15 à $L$ et $N$ pour compléter cette base en une $\mathbf{Z}$-base de $L$.

### 3.3.4 Description du quotient

Le corollaire suivant donne la structure du quotient $L/M$ et l'unicité des invariants :

**3.16 Corollaire.** *On reprend les notations de 3.13. Le groupe quotient $L/M$ est isomorphe à $\mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_r\mathbf{Z} \times \mathbf{Z}^{n-r}$. Son sous-groupe de torsion est $T = \mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_r$. Il est d'ordre $d_1 \cdots d_r$ et d'exposant $d_r$.*

*Les entiers $r$ et $d_1, \ldots, d_r$ sont uniquement déterminés par le couple $(L, M)$. On les nomme* **invariants** *du couple $(L, M)$.*

*Démonstration.* Soient $e_1, \ldots, e_n$ une $\mathbf{Z}$-base de $L$ adaptée au sous-groupe $M$. On considère l'homomorphisme $\varphi : L \to \mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_r\mathbf{Z} \times \mathbf{Z}^{n-r}$ qui à $\sum_{i=1}^n x_ie_i$ associe $(\overline{x_1}, \ldots, \overline{x_r}, x_{r+1}, \ldots, x_n)$. Cet homomorphisme est surjectif et son noyau est $M$, d'où l'isomorphisme. Le sous-groupe de torsion $T$ de $L/M$ est alors le produit des groupes cycliques et le quotient de $L/M$ par $T$ est le groupe libre $\mathbf{Z}^{n-r}$. En vertu de 3.7, cela montre que $n - r$ est unique, donc aussi $r$. Pour les autres invariants, il faut prendre garde que certains des $d_i$ peuvent être égaux à 1, disons $d_1 = \ldots = d_k = 1$. Mais alors, le groupe de torsion est isomorphe à $\mathbf{Z}/d_{k+1}\mathbf{Z} \times \cdots \times \mathbf{Z}/d_r\mathbf{Z}$ avec des $d_i \geq 2$. En vertu de 3.8, cela montre l'unicité de $r - k$, donc de $k$, et des $d_i$ pour $i \geq k + 1$ et on a le résultat.

## 3.4 Application aux groupes abéliens de type fini

**3.17 Définition.** *On dit qu'un groupe abélien est* **de type fini** *s'il est engendré par un nombre fini de générateurs. Un groupe abélien isomorphe à $\mathbf{Z}^n$ est dit* **abélien libre de rang** *$n$.*

**3.18** *Remarque.* Un groupe abélien $G$ est de type fini si et seulement si il existe un homomorphisme surjectif $\varphi : \mathbf{Z}^n \to G$. Si l'on pose $L = \mathbf{Z}^n$ et $M = \operatorname{Ker}\varphi$ on a alors $G \simeq L/M$.

La remarque ci-dessus fournit une voie d'approche des groupes abéliens de type fini qui consiste à représenter les groupes libres comme des réseaux. Ainsi, le théorème fondamental sur les sous-réseaux 3.13 donne déjà comme sous-produit le résultat analogue sur les groupes libres :

**3.19 Corollaire.** *Soit $L$ un groupe abélien libre de rang $n$ et $M$ un sous-groupe de $L$. Alors $M$ est libre. Plus précisément, il existe une $\mathbf{Z}$-base $e_1, \ldots, e_n$*

*de $L$, un entier $r$ avec $0 \leq r \leq n$ et des entiers $d_1, \ldots, d_r \in \mathbf{N}^*$ tels que $d_1|d_2|\cdots|d_r$ et que $d_1e_1, \ldots, d_re_r$ soit une $\mathbf{Z}$-base de $M$.*

*Démonstration.* Il suffit de plonger $\mathbf{Z}^n$ dans $\mathbf{R}^n$ pour se ramener au théorème 3.13.

En mettant ensemble 3.18, 3.13 et 3.16 on obtient le théorème de structure des groupes abéliens de type fini :

**3.20 Corollaire.** *Soit $G$ un groupe abélien de type fini. Il existe des entiers $n, r \in \mathbf{N}$, avec $r \leq n$ et des entiers $d_1, \ldots, d_r \in \mathbf{N}^*$ tels que $d_1|d_2|\cdots|d_r$ tels que l'on ait $G \simeq \mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_r\mathbf{Z} \times \mathbf{Z}^{n-r}$.*

*Le sous-groupe de torsion de $G$ est le groupe fini $\mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_r\mathbf{Z}$, d'ordre $d_1 \ldots d_r$ et d'exposant $d_r$. En particulier, si $G$ est fini, on a $r = n$ et $G$ est produit de groupes cycliques $G \simeq \mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_r\mathbf{Z}$.*

*Les entiers $r$ et $d_1, \ldots, d_r$ sont déterminés de manière unique.*

## 3.5 Calcul des invariants

Pour appliquer le théorème fondamental 3.13, encore faut-il savoir calculer les invariants $d_i$. C'est l'objet du théorème suivant :

**3.21 Théorème.** *Soit $E$ un $\mathbf{R}$-espace vectoriel de dimension $n$, $L$ et $M$ deux réseaux de $E$ avec $M \subset L$ et $d_1, \ldots, d_n$ les invariants du couple $(L, M)$. Rappelons qu'on a $d_1|d_2|\cdots|d_n$. Soit $e_1, \ldots, e_n$ (resp. $u_1, \ldots, u_n$) une $\mathbf{Z}$-base de $L$ (resp. $M$) et soit $A \in \mathbf{M}(n, \mathbf{Z})$ la matrice des $u_j$ sur les $e_i$ : $u_j = \sum_{i=1}^n a_{ij}e_i$. Alors, pour $k = 1, \ldots, n$, le produit $d_1 \cdots d_k$ est le pgcd positif des mineurs d'ordre $k$ de $A$. En particulier $d_1$ est le pgcd des coefficients de $A$ et $d_1 \cdots d_n$ la valeur absolue du déterminant de $A$.*

*Démonstration.* 1) Supposons d'abord les bases $(e_i)$ et $(u_j)$ adaptées. Dans ce cas, la matrice $A$ est la matrice diagonale formée par les $d_i$ et le résultat est clair car les mineurs d'ordre $k$ non nuls sont les $d_{i_1} \cdots d_{i_k}$ et comme les $d_i$ se divisent, leur *pgcd* est bien $d_1 \cdots d_k$.

2) La conclusion du théorème vient alors du lemme suivant :

**3.22 Lemme.** *Sous les hypothèses de 3.21, le pgcd positif $\delta_k$ des mineurs d'ordre $k$ de $A$ ne dépend pas du choix des $\mathbf{Z}$-bases $(e_i)$, $(u_j)$.*

*Démonstration.* a) On traite d'abord le cas $k = 1$. Soient $(e'_i)$ et $(u'_j)$ d'autres $\mathbf{Z}$-bases de $L$ et $M$, $A'$ la matrice des $u'_j$ sur les $e'_i$ et $\delta'_1$ le *pgcd* des coefficients de $A'$. On désigne par $P$ (resp. $Q$) la matrice de passage des $e'_i$ aux $e_i$ (resp. des $u_j$ aux $u'_j$). On sait que $P$ et $Q$ sont dans $GL(n, \mathbf{Z})$ et on a $A' = PAQ$, autrement dit : $a'_{ij} = \sum_{k,l} p_{ik}a_{kl}q_{lj}$. Comme $\delta_1$ divise tous les $a_{ij}$, il divise

aussi tous les $a'_{ij}$ donc leur *pgcd* $\delta'_1$. Mais, les matrices $P^{-1}$ et $Q^{-1}$ sont aussi à coefficients entiers et le même raisonnement appliqué dans l'autre sens montre que $\delta'_1$ divise $\delta_1$, de sorte qu'on a bien $\delta_1 = \delta'_1$.

b) On se reportera à l'annexe 6.1 pour les résultats sur l'algèbre extérieure et les espaces $\Lambda^k E$.

On considère l'espace vectoriel $\Lambda^k E$. Si $e_1, \ldots, e_n$ est une base de $E$, on en déduit la base associée de $\Lambda^k E$, formée des

$$e_{i_1} \wedge \cdots \wedge e_{i_k}, \text{ avec } 1 \leq i_1 < i_2 < \cdots < i_k \leq n.$$

Si $e'_1, \ldots, e'_n$ est une autre base de $E$ et si $P = (p_{ij})$ est la matrice de passage des $e_i$ aux $e'_i$, la matrice de passage des $e_{i_1} \wedge \cdots \wedge e_{i_k}$ aux $e'_{i_1} \wedge \cdots \wedge e'_{i_k}$ est la matrice des mineurs d'ordre $k$ de $P$ :

$$e'_{j_1} \wedge \cdots \wedge e'_{j_k} = \sum_{\underline{i},\underline{j}} p_{i_1,\ldots,i_k;j_1,\ldots,j_k} e_{i_1} \wedge \cdots \wedge e_{i_k}.$$

Reprenons les notations de 3.22 et du point a), avec les matrices $A, A', P, Q$. On considère, dans l'espace vectoriel $\Lambda^k E$, les réseaux $\Lambda^k L$ et $\Lambda^k M$ de $\mathbf{Z}$-bases $e_{i_1} \wedge \cdots \wedge e_{i_k}$ et $u_{i_1} \wedge \cdots \wedge u_{i_k}$. Ces réseaux admettent aussi respectivement les $\mathbf{Z}$-bases $e'_{i_1} \wedge \cdots \wedge e'_{i_k}$ et $u'_{i_1} \wedge \cdots \wedge u'_{i_k}$. On a $\Lambda^k M \subset \Lambda^k L$ et, plus précisément, la matrice des $u_{i_1} \wedge \cdots \wedge u_{i_k}$ sur les $e_{i_1} \wedge \cdots \wedge e_{i_k}$ (resp. des $u'_{i_1} \wedge \cdots \wedge u'_{i_k}$ sur les $e'_{i_1} \wedge \cdots \wedge e'_{i_k}$) est la matrice des $k$-mineurs de $A$ (resp. $A'$). Mais alors, le point a) appliqué à ces réseaux montre que le *pgcd* des mineurs $\delta_k$ est indépendant du choix des bases.

## 3.6 Détermination des bases adaptées

Soit $L$ un réseau de $E$ et $M$ un sous-réseau de $L$. Nous donnons dans ce paragraphe un algorithme permettant de trouver une base adaptée au couple $L, M$. La mise en œuvre de cet algorithme est beaucoup plus efficace si l'on utilise un logiciel de calcul formel, par exemple *xcas*.

On peut supposer que $E$ est l'espace $\mathbf{R}^n$ et $L$ le réseau défini par la base canonique $e_i = (0, \ldots, 0, 1, \ldots, 0)$. Le sous-réseau $M$ est alors donné par une $\mathbf{Z}$-base $u_1, \ldots, u_r$ avec $r \leq n$ et on écrit les $u_j$ sur les $e_i$ au moyen d'une matrice $A$ à coefficients entiers : $u_j = \sum_{i=1}^n a_{ij} e_i$. Nous illustrerons l'algorithme proposé sur l'exemple suivant : $n = 3$ et $A = \begin{pmatrix} -30 & 22 & 54 \\ 45 & -31 & -78 \\ -28 & 12 & 28 \end{pmatrix}$. On a donc $u_1 = -30e_1 + 45e_2 - 28e_3$, $u_2 = 22e_1 - 31e_2 + 12e_3$ et $u_3 = 54e_1 - 78e_2 + 28e_3$.

**3.23** *Remarque.* Le rang de $M$ est égal au rang de la matrice $A$.

### 3.6.1 Le cas du rang $n$

Dans les quatre paragraphes qui suivent, on suppose que le sous-réseau $M$ est de rang $n$. La matrice $A$ est alors une matrice carrée $n \times n$, inversible sur $\mathbf{R}$ et même sur $\mathbf{Q}$, et il s'agit, à partir des $a_{ij}$, de déterminer des vecteurs $\epsilon_1, \ldots, \epsilon_n$ qui constituent une $\mathbf{Z}$-base de $L$ et des entiers $d_1, \ldots, d_n$, se divisant, tels que $d_1\epsilon_1, \ldots, d_n\epsilon_n$ soit une $\mathbf{Z}$-base de $M$. On appelle $B$ la matrice inverse de $A$, on écrit chacun de ses termes $b_{ij}$ sous forme irréductible $b_{ij} = \dfrac{c_{ij}}{q_{ij}}$ et on note $q_j$ le *ppcm* des dénominateurs des coefficients de la colonne $j$.

Dans le cas de l'exemple, le rang de $A$ est bien 3 et on a $B = \begin{pmatrix} \frac{17}{144} & \frac{1}{18} & -\frac{7}{96} \\ \frac{77}{48} & \frac{7}{6} & \frac{5}{32} \\ -\frac{41}{72} & -\frac{4}{9} & -\frac{5}{48} \end{pmatrix}$.

On a donc $q_1 = 144$, $q_2 = 18$ et $q_3 = 96$.

### 3.6.2 Détermination des invariants

Ce travail a été fait en 3.21. On a vu que les invariants se calculent à partir des *pgcd* des mineurs de $A$ des différentes tailles. Dans le cas de l'exemple on a $d_1 = 1$, $d_2 = 2$ (on voit aussitôt que les 2-mineurs sont tous pairs et deux mineurs bien choisis suffisent à montrer que le *pgcd* vaut 2) et, comme $\det A = 576$, on a $d_3 = 288$.

### 3.6.3 Détermination de $\epsilon_n$

On sait que $d_n$ est l'exposant du groupe quotient $L/M$ et le vecteur $\epsilon_n$ cherché est un élément d'ordre $d_n$ dans ce quotient. Pour le déterminer on utilise le lemme suivant :

**3.24 Lemme.** *Dans le quotient $L/M$, le vecteur $e_j$ est d'ordre $q_j$.*

*Démonstration.* On a $e_j = \displaystyle\sum_{i=1}^{n} \frac{c_{ij}}{q_{ij}} u_i$. Comme $q_j$ est multiple des $q_{ij}$, il est clair que $qe_j$ est dans $M$. Inversement, si $ke_j$ est dans $M$, on voit que $q_{ij}$ divise $kc_{ij}$ pour tout $i$ et, comme il est premier avec $c_{ij}$, il divise $k$, qui est donc multiple des $q_{ij}$, donc de leur *ppcm* $q_j$.

On peut maintenant trouver un vecteur $\epsilon_n$. Comme les $\overline{e_j}$ engendrent $L/M$, on a vu en 3.5 que $d_n$ est le *ppcm* des $q_j$. On écrit $d_n$ comme produit de puissances de nombres premiers $p_i^{\alpha_i}$, ce nombre divise l'un des $q_j$ et il y a donc un élément $\lambda_j \overline{e}_j$ qui est de cet ordre. Alors, la somme de ces éléments convient.

Dans l'exemple, on voit que $\overline{e}_1$ est d'ordre 144, $\overline{e}_2$ d'ordre 18 et $\overline{e}_3$ d'ordre 96. On a $288 = 2^5 3^2 = 32 \times 9$. L'élément $3e_3$ est d'ordre 32 dans le quotient, l'élément $2e_2$ d'ordre 9, l'élément $\epsilon_3 = 2e_2 + 3e_3$ est d'ordre 288 dans $L/M$. De plus, on vérifie que l'on a $L \cap \mathbf{R}\epsilon_3 = \mathbf{Z}\epsilon_3$.

### 3.6.4 Projection sur un supplémentaire

Pour aller plus loin, on utilise la méthode du théorème 3.13. On considère un supplémentaire $H$ de $\mathbf{R}\epsilon_n$. Quitte à renuméroter les $e_i$, on peut supposer qu'il s'agit de $H =< e_1, \dots e_{n-1} >$. On appelle $p : E \to H$ la projection parallèlement à $\mathbf{R}\epsilon_n$. On sait que $p(L)$ et $p(M)$ sont alors des réseaux de $H$ et que si on a une $\mathbf{Z}$-base adaptée à ce couple, et si on relève ses vecteurs dans $L$ et $M$, on obtient une $\mathbf{Z}$-base adaptée à $L, M$ en lui adjoignant $\epsilon_n$.

Dans l'exemple, on prend $H$ engendré par $e_1, e_2$. La projection s'écrit :

$$p(x_1e_1 + x_2e_2 + x_3e_3) = x_1e_1 + (x_2 - \frac{2x_3}{3})e_2.$$

Le réseau $p(L)$ de $H$ est engendré par $p(e_1) = e_1$, $p(e_2) = e_2$ et $p(e_3) = -\frac{2}{3}e_2$. Une $\mathbf{Z}$-base de $p(L)$ est donc $e_1, e_2' = \frac{1}{3}e_2$. Le réseau $p(M)$ est engendré par $v_1 := p(u_1) = -30e_1 + \frac{191}{3}e_2 = -30e_1 + 191e_2'$, $v_2 := p(u_2) = 22e_1 - 117e_2'$ et $v_3 := p(u_3) = 54e_1 - 290e_2'$.

Pour trouver une $\mathbf{Z}$-base adaptée au couple $p(L), p(M)$, on commence par trouver une $\mathbf{Z}$-base de $p(M)$ en utilisant 2.13. On écrit $v_3$ comme combinaison de $v_1$ et $v_2$ :

$$v_3 = \frac{-31}{346}v_1 + \frac{807}{346}v_2.$$

Avec les notations de 2.13 on a donc $m = 346$, $d_1 = d_2 = 1$, $c_1 = -31$ et $c_2 = 807$. On écrit une relation de Bézout avec $c_1$ et $c_2$ : $807 \times 1 + (-26) \times (-31) = 1$. On peut alors prendre comme $\mathbf{Z}$-base de $p(M)$, $w_1 = v_1 - 26v_2 = -602e_1 + 3233e_2'$ et $w_2 = v_3 = 54e_1 - 290e_2'$. On vérifie que le déterminant de cette base sur $e_1, e_2'$ est $-2$ et le calcul de l'inverse donne : $e_1 = 145w_1 + \frac{3233}{2}w_2$ et $e_2' = 27w_1 + 301w_2$. Cela montre que $e_2'$ est dans $p(M)$ et que $e_1$ est d'ordre 2 dans $p(L)/p(M)$ et le couple $e_2', e_1$ est donc une base adaptée à $p(L), p(M)$.

L'étape suivante est de relever $e_2'$ et $2e_1$ dans $M$. Pour cela, on les écrit en fonction des $v_i$ : $e_2' = 27v_1 - 702v_2 + 301v_3 = p(27u_1 - 702u_2 + 301u_3) = p(-501e_2 - 752e_3)$ et $2e_1 = p(290u_1 - 7540u_2 + 3233u_3) = p(2e_1 - 5384e_2 - 8076e_3)$.

En définitive, une $\mathbf{Z}$-base adaptée à $L, M$ est la suivante :

$$\epsilon_1 = -501e_2 - 752e_3,\ \epsilon_2 = e_1 - 2692e_2 - 4038e_3,\ \epsilon_3 = 2e_2 + 3e_3.$$

On vérifie que le déterminant des $\epsilon_j$ sur les $e_i$ est égal à $-1$ (donc que la matrice de passage est dans $GL(3, \mathbf{Z})$).

**3.25** *Remarque.* On peut parfois éviter une partie des calculs précédents. En effet, il arrive que la matrice donnant les $e_i$ par rapport aux $u_j$ fasse aussitôt apparaître des vecteurs indépendants vérifiant $d_i\epsilon_i \in M$. Voir notamment l'exercice 3.27.

### 3.6.5 Exercices

**3.26** *Exercice.* 1) Soit $L = \mathbf{Z}^2$ le réseau naturel de $\mathbf{R}^2$ de $\mathbf{Z}$-base $e_1 = (1, 0)$ et $e_2 = (0, 1)$ et soit $M$ le sous réseau de $\mathbf{Z}$-base $u_1 = e_1 + 2e_2$ et $u_2 = 2e_1 + e_2$. Déterminer les invariants du couple $(L, M)$ et en trouver une base adaptée. (Réponse : $d_1 = 1$, $d_2 = 3$ et, par exemple, $\epsilon_1 = u_2$ et $\epsilon_2 = e_1$.)

2) Mêmes questions avec $M$ défini par la $\mathbf{Z}$-base $v_1 = 3e_1 - 4e_2$, $v_2 = 9e_1 + 8e_2$. (Réponse : $d_1 = 1$ et $d_2 = 60$ et, par exemple, $\epsilon_1 = -3e_1 - 16e_2$, $\epsilon_2 = e_1 + 5e_2$.)

**3.27** *Exercice.* On considère le réseau standard $L = \mathbf{Z}^3 \subset \mathbf{R}^3$ et le réseau $M \subset L$ dont les vecteurs de base sont $u_1 = (54, -78, 28)$, $u_2 = (22, -31, 12)$ et $u_3 = (-30, 45, -14)$. Déterminer les invariants du couple $(L, M)$ et calculer une $\mathbf{Z}$-base adaptée. (Réponses : $d_1 = 1$, $d_2 = 2$, $d_3 = 6$. Pour la base adaptée, le lecteur moins maladroit que moi contemplera la matrice inverse et la base lui sautera au visage ou presque : $\epsilon_1 = (2, 1, 0)$, $\epsilon_2 = (0, 0, 1)$ et $\epsilon_3 = (1, 0, 0)$.)

# 4 Volumes et théorème de Minkowski

On travaille toujours sur un espace vectoriel réel de dimension finie $n$. On fixe une fois pour toutes une base $\epsilon_1, \ldots, \epsilon_n$ de $E$. Si $E$ est muni d'une structure euclidienne on peut prendre, par exemple, une base orthonormée.

## 4.1 Rappels sur les volumes

Le choix de la base des $\epsilon_i$ fournit un isomorphisme de $E$ sur $\mathbf{R}^n$ et une mesure de Lebesgue $\mu$ associée à ce choix. Rappelons qu'il existe alors une partie $\mathcal{M}(E) \subset \mathcal{P}(E)$ dont les éléments sont les parties **mesurables** de $E$ et une application $\mu : \mathcal{M}(E) \to \mathbf{R}^+ \cup \{+\infty\}$, appelée aussi **volume**, avec les propriétés suivantes.

1) L'ensemble $\mathcal{M}(E)$ est une $\sigma$-algèbre, c'est-à-dire stable par union dénombrable et passage au complémentaire. En fait, $\mathcal{M}(E)$ contient "presque" toutes[8] les parties de $E$, et en tous cas, toutes les parties usuelles,

8. Si l'on refuse l'axiome du choix, on peut supposer que toutes les parties de $E$ sont mesurables.

ouverts, fermés, unions dénombrables de fermés, intersections dénombrables d'ouverts, etc.

2) La mesure $\mu$ est unique si l'on impose que la mesure du pavé unité $P = \{\sum_{i=1}^{n} x_i \epsilon_i \ \mid \ 0 \leq x_i \leq 1\}$ est égale à 1.

3) La mesure $\mu$ est $\sigma$-additive : si les $A_n$, $n \in \mathbf{N}$, sont dans $\mathcal{M}(E)$ et sont disjointes, on a $\mu(\bigcup_{n\in\mathbf{N}} A_n) = \sum_{n\in\mathbf{N}} \mu(A_n)$ où la somme est soit une série convergente, soit $+\infty$.

4) Elle est invariante par translation : si $A$ est dans $\mathcal{M}(E)$ et $x \in E$ on a $\mu(x + A) = \mu(A)$.

5) Elle est homogène : si $A$ est dans $\mathcal{M}(E)$ et $\lambda \in \mathbf{R}$ on a $\mu(\lambda A) = |\lambda|^n \mu(A)$.

6) On a la formule de changement de variables : si $\epsilon'_1, \ldots, \epsilon'_n$ est une base de $E$ et si $P'$ est le pavé unité bâti sur les $\epsilon'_i$ on a $\mu(P') = |\det_{(\epsilon_i)}(\epsilon'_i)|$.

7) Enfin, on sait que si une partie est contenue dans un hyperplan elle est de mesure nulle. En particulier, le volume d'un pavé est le même qu'il soit ouvert, fermé ou semi-ouvert.

## 4.2 Volume d'un réseau

### 4.2.1 Définition

**4.1 Proposition-Définition.** *Soit $L$ un réseau de $E$ muni d'une* $\mathbf{Z}$*-base $e_1, \ldots, e_n$. On désigne par $D$ le pavé unité semi-ouvert bâti sur $(e_i)$ : $D = \{x = \sum_{i=1}^{n} x_i e_i \ \mid \ x_i \in \mathbf{R}$ et $0 \leq x_i < 1 \ \}$. Alors la mesure $\mu(D)$ est égale à la valeur absolue du déterminant de $e_1, \ldots, e_n$ sur la base canonique, elle est indépendante du choix de la* $\mathbf{Z}$*-base de $L$, on l'appelle* **volume** *de $L$ et on le note* $\mathrm{vol}\,(L)$.

*Démonstration.* La formule de changement de variables donne aussitôt $\mu(D) = |\det_{(\epsilon_i)}(e_i)|$. Si l'on change la $\mathbf{Z}$-base $(e_i)$ en $(e'_i)$, cette quantité est multipliée par la valeur absolue du déterminant de la matrice de passage des $(e_i)$ aux $(e'_i)$. Comme cette matrice est dans $GL(n, \mathbf{Z})$ en vertu de 1.3, son déterminant est $\pm 1$ et on a le résultat.

**4.2** *Remarque.* On notera que $D$ est un **domaine fondamental** pour l'action de $L$ sur $E$ par translation. Cela signifie que $D$ est un système de représentants du quotient $E/L$ ou encore que, pour tout $x \in E$, il existe un unique $a \in L$ tel que $x = a + y$ avec $y \in D$. On a donc $E = \bigcup_{a\in L} a + D$ et cette réunion est disjointe.

### 4.2.2 La formule des réseaux emboîtés

**4.3 Proposition.** *Soient $L$ et $M$ deux réseaux de $E$ avec $M \subset L$. Alors, le groupe quotient $L/M$ est fini et on a $|L/M| = \mathrm{vol}\,(M)/\mathrm{vol}\,(L)$.*

*Démonstration.* Nous donnons deux démonstrations de ce résultat.

1) En vertu du théorème 3.13, il existe une $\mathbf{Z}$-base de $L$ adaptée à $M$, avec des invariants $d_1, \ldots, d_n$. Comme la matrice de passage de l'une à l'autre est la matrice diagonale des $d_i$, on a bien $\mathrm{vol}\,(M)/\mathrm{vol}\,(L) = d_1 \cdots d_n$. Mais on a vu en 3.16 que cette quantité est également le cardinal du groupe $L/M$.

2) La deuxième preuve [9] n'utilise pas 3.13.

Soient $D$ et $\Delta$ des domaines fondamentaux de $L$ et $M$ (voir 4.2). On a donc $E = \bigcup_{a\in L} a + D = \bigcup_{x\in M} x + \Delta$ (unions disjointes). On en déduit $\Delta = \bigcup_{a\in L}(\Delta \cap (a+D))$ et, comme cette union est disjointe et $L$ dénombrable, $\mu(\Delta) = \sum_{a\in L} \mu(\Delta \cap (a + D))$. Notons $\overline{a} \in L/M$ la classe de $a$. La somme précédente peut se décomposer selon les classes de $L/M$ :

$$\mu(\Delta) = \sum_{\overline{a}\in L/M} \sum_{x\in\overline{a}} \mu(\Delta \cap (x + D)).$$

Mais, on a le lemme :

**4.4 Lemme.** *On a* $\displaystyle\sum_{x\in\overline{a}} \mu(\Delta \cap (x + D)) = \mu(D)$.

Si ce lemme est vrai, on a $\mu(\Delta) = \sum_{\overline{a}\in L/M} \mu(D) = |L/M|\,\mu(D)$ ce qui prouve que $L/M$ est fini et donne la formule annoncée.

*Démonstration.* (du lemme) Dire que $x$ est dans $\overline{a}$ signifie qu'il existe $m \in M$ tel que $x = a + m$. Cela permet d'écrire :

$$\sum_{x\in\overline{a}} \mu(\Delta \cap (x + D)) = \sum_{m\in M} \mu(\Delta \cap (m + a + D))$$

et, en vertu de l'invariance de $\mu$ par translation, cette quantité est encore égale à $\sum_{m\in M} \mu((-m + \Delta) \cap (a + D))$. Mais, comme $\Delta$ est un domaine fondamental pour $M$, le même raisonnement que ci-dessus appliqué à $a + D$ montre que l'on a $\sum_{m\in M} \mu((-m + \Delta) \cap (a + D)) = \mu(a + D) = \mu(D)$.

9. Cette preuve – parmi bien d'autres – m'a été soufflée par Claire Voisin lorsqu'elle était agrégative.

## 4.3 Le lemme de chevauchement

Il s'agit du résultat suivant :

**4.5 Lemme.** *Soit $L$ un réseau de $E$ et $A$ une partie de $E$. On suppose qu'on a $\mu(A) > \mathrm{vol}\,(L)$. Alors, il existe $x, y \in A$, avec $x \neq y$, tels que $x - y \in L$.*

**4.6** *Remarque.* Si on note $p : E \to E/L$ la projection canonique, le résultat signifie que $p(x)$ et $p(y)$ sont égaux dans le quotient.

*Démonstration.* Soit $D$ un domaine fondamental de $L$, de sorte qu'on a $\mu(D) = \mathrm{vol}\,(L)$. On a alors $E = \bigcup_{a\in L} a + D$ et, en prenant l'intersection avec $A$, $A = \bigcup_{a\in L}(a + D) \cap A$. Comme les ensembles $a + D$ sont disjoints, on en déduit $\mu(A) = \sum_{a\in L} \mu((a+D)\cap A)$. Comme $\mu$ est invariante par translation, on a $\mu((a + D) \cap A) = \mu(D \cap (-a + A))$. Mais, on a $\bigcup_{a\in L} D \cap (-a + A) \subset D$. Si les ensembles $D \cap (-a + A)$, pour $a \in L$, étaient disjoints, on aurait donc $\mu(A) = \sum_{a\in L} \mu(D \cap (-a + A)) \leq \mu(D)$, ce qui contredit l'hypothèse $\mu(A) > \mathrm{vol}\,(L) = \mu(D)$.

Il existe donc $a, b \in L$, distincts, tels que $D \cap (-a + A)$ et $D \cap (-b + A)$ se rencontrent, donc $x, y \in A$ avec $-a + x = -b + y$, ou encore $x - y = a - b \in L$ et $x \neq y$ comme annoncé.

## 4.4 Le théorème de Minkowski

**4.7 Théorème.** *Soit $L$ un réseau de $E$ (toujours supposé de dimension $n$) et soit $A \subset E$ une partie convexe*[10] *et symétrique par rapport à l'origine* 0*. On suppose qu'on a $\mu(A) > 2^n \mathrm{vol}\,(L)$. Alors, il existe $a \in A \cap L$, $a \neq 0$.*

*Démonstration.* L'ensemble $2L = \{2a \mid a \in L\}$ est un réseau, de $\mathbf{Z}$-base $2e_i$ si $e_i$ est une $\mathbf{Z}$-base de $L$. Comme le domaine fondamental de $2L$ s'obtient à partir de celui de $L$ par une homothétie de centre 0 et de rapport 2, on a $\mathrm{vol}\,(2L) = 2^n \mathrm{vol}\,(L)$. Le lemme de chevauchement 4.5 assure alors qu'il existe $x, y \in A$, distincts, tels que $x - y \in 2L$, donc $x - y = 2a$, $a \in L$. Il en résulte que $\dfrac{x - y}{2}$ est dans $L$. Mais, comme $A$ est symétrique, $-y$ est dans $A$ et comme $A$ est convexe, $\dfrac{x + (-y)}{2}$ y est aussi et on a le résultat.

**4.8 Corollaire.** *On reprend les notations de 4.7. Soit $R$ un réel positif et $A = \overline{B}(0, R)$ la boule fermée de rayon $R$. On suppose $\mu(A) \geq 2^n \mathrm{vol}\,(L)$. Alors, il existe $a \in A \cap L$, $a \neq 0$.*

10. Sauf erreur de ma part, une partie convexe est automatiquement mesurable.

*Démonstration.* Bien entendu, seul le cas où l'inégalité est une égalité pose problème. On considère les boules $A_k = \overline{B}(0, R + \frac{1}{k})$. En vertu de 4.7, il y a un point $a_k \in L \cap A_k$, $a_k \neq 0$. Comme la suite $(a_k)$ est bornée on peut en extraire une sous-suite convergeant vers $a$. Comme $L$ est fermé et discret, la suite est nécessairement stationnaire, de sorte qu'on a $a \in L$ et $a \neq 0$. Comme on a $\|a_k\| \leq R + \frac{1}{k}$ et que $\|a_k\|$ tend vers $\|a\|$, on voit que $a$ est dans $A$ et on a la conclusion.

# 5 Les théorèmes des deux et des quatre carrés

## 5.1 Les deux carrés

### 5.1.1 Présentation

Il s'agit de savoir à quelles conditions un entier $n \in \mathbf{N}$ s'écrit sous la forme $n = a^2 + b^2$ avec $a, b \in \mathbf{N}$. On notera $\Sigma_2$ l'ensemble des entiers $\geq 0$ qui sont de cette forme. Le premier résultat est le suivant :

**5.1 Proposition.** *L'ensemble $\Sigma_2$ est stable par multiplication.*

*Démonstration.* Cela résulte de l'identité $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$ que l'on comprend mieux en interprétant $a^2 + b^2$ et $c^2 + d^2$ comme les "normes" des nombres complexes $z = a + ib$ et $w = c + id$.

Forts du résultat précédent, il est naturel de se demander quels nombres premiers peuvent être sommes de deux carrés :

**5.2 Proposition.** *Soit $p$ un nombre premier congru à 3 modulo 4.*

*1) Le nombre $p$ n'est pas somme de deux carrés.*

*2) Plus précisément, si $p$ divise une somme de deux carrés $a^2 + b^2$ il divise $a$ et $b$ (et donc $p^2$ divise $a^2 + b^2$).*

*Démonstration.* Il suffit de prouver le point 2). Rappelons le lemme suivant (voir [DP] III, 2.13) :

**5.3 Lemme.** *Soit $p$ un nombre premier impair. Alors, $-1$ est un carré modulo $p$ si et seulement si $p$ est congru à 1 modulo 4.*

Le point 2) est alors clair car si $p$ ne divise pas $b$, on a, dans le corps $\mathbf{F}_p$, $(\frac{a}{b})^2 = -1$ et c'est absurde.

### 5.1.2 Le résultat principal

Le point essentiel concerne les nombres premiers congrus à 1 modulo 4 :

**5.4 Théorème.** *Soit $p$ un nombre premier congru à 1 modulo 4. Alors, il existe $a, b \in \mathbf{N}$ tels que $p = a^2 + b^2$.*

*Démonstration.* On considère le réseau $\mathbf{Z}^2$ de $\mathbf{R}^2$. Ses éléments $(a, b)$ ont pour carré de la norme la somme $a^2 + b^2$. L'idée est de construire un sous-réseau $L$ de $\mathbf{Z}^2$ dont tous les éléments soient tels que $p$ divise $a^2 + b^2$, en espérant qu'un élément de norme minimale fasse l'affaire.

**5.5** *Remarque.* Attention, le candidat naturel $R = \{(a, b) \in \mathbf{Z}^2 \mid p \,|\, a^2 + b^2 \}$ n'est pas un réseau (par exemple, pour $p = 5$, on $(1, 2) \in R$, $(2, 1) \in R$ mais $(1, 2) + (2, 1) = (3, 3) \notin R$). La condition signifie que $a/b$ est une racine de $-1$ dans $\mathbf{F}_p$ mais, pour avoir la stabilité par somme, il faut toujours choisir la même racine. Cela explique la définition suivante.

Soit $u \in \mathbf{Z}$ un entier qui vérifie $u^2 \equiv -1 \pmod{p}$ (voir 5.3). On définit la partie $L$ de $\mathbf{Z}^2$ comme suit :

$$L = \{(a, b) \in \mathbf{Z}^2 \mid b \equiv ua \pmod{p} \}.$$

Alors, $L$ est un réseau. En effet la condition signifie qu'il existe $n \in \mathbf{Z}$ tel que $b = ua + np$, de sorte qu'un élément $(a, b)$ de $L$ s'écrit $a(1, u) + n(0, p)$ avec $a, n \in \mathbf{Z}$. C'est donc un réseau de $\mathbf{Z}$-base $(1, u)$, $(0, p)$. De plus, si $(a, b)$ est dans $L$, on a $a^2 + b^2 = a^2(1 + u^2) + 2uanp + n^2p^2$ et, par définition de $u$, on voit que $a^2 + b^2$ est multiple de $p$. Pour trouver un élément dont le carré de la norme soit exactement $p$, on applique le théorème de Minkowski. Le volume de $L$ est donné par le déterminant de sa $\mathbf{Z}$-base, c'est donc $p$. On considère alors un disque $D(0, R)$ avec $\pi R^2 > 4p$, par exemple $R^2 = \frac{3p}{2}$. En vertu du théorème de Minkowski, ce disque contient un point $(a, b)$ non nul de $L$ qui vérifie donc $a^2 + b^2 \leq R^2 = \frac{3p}{2}$. Comme $a^2 + b^2$ est multiple de $p$, la seule solution est $a^2 + b^2 = p$.

### 5.1.3 Bilan

On peut maintenant finir de déterminer les éléments de $\Sigma_2$ :

**5.6 Corollaire.** *Un entier naturel est somme de deux carrés si et seulement si, dans sa décomposition en produit de facteurs premiers, les facteurs congrus à 3 modulo 4 sont à une puissance paire.*

*Démonstration.* Par multiplicativité il est clair que la condition est suffisante. Pour voir qu'elle est nécessaire on raisonne par l'absurde et on choisit un contre-exemple minimal $n$, somme de deux carrés $a^2 + b^2$ et admettant un facteur premier $p \equiv 3 \pmod 4$ à une puissance impaire. En vertu de 5.2, $p$ divise $a$ et $b$, mais alors $n/p^2$ est encore somme de deux carrés, il contient le facteur $p$ à une puissance impaire et il est $< n$ ce qui est absurde.

### 5.1.4 L'algorithme de Cornacchia

Il s'agit d'un algorithme très efficace proposé par Cornacchia en 1908 qui permet d'écrire un nombre sous forme de somme de carrés. Nous en donnons ici une version élémentaire. Pour une interprétation en termes de fractions continues, voir [N].

Soit $p$ un nombre premier congru à 1 modulo 4 et $u$ un entier tel que $u^2 \equiv -1 \pmod p$ et $u < p$. L'idée est d'effectuer l'algorithme d'Euclide avec $p$ et $u$. On pose $r_0 = p$ et $r_1 = u$ puis $r_0 = r_1 q_1 + r_2$ avec $0 \leq r_2 < r_1$, $r_1 = r_2 q_2 + r_3$ avec $0 \leq r_3 < r_2$, etc. $r_{n-1} = r_n q_n + r_{n+1}$ avec $0 \leq r_{n+1} < r_n$.

On sait que l'algorithme d'Euclide peut être utilisé pour trouver les coefficients de Bézout relatifs à $p$ et $u$. Précisément, on va écrire, pour tout $n \geq 0$ : $r_n = a_n p + b_n u$ (relation $(*)$). Pour cela, on pose $a_0 = 1$, $b_0 = 0$, $a_1 = 0$, $b_1 = 1$ et on calcule les suivants grâce aux deux relations de récurrence :

$$(**) \qquad a_{n+1} = a_{n-1} - q_n a_n \quad \text{et} \quad b_{n+1} = b_{n-1} - q_n b_n.$$

On sait que les $r_n$ décroissent et que le dernier reste non nul est le *pgcd* de $p$ et $u$, c'est-à-dire 1. On peut donc énoncer le résultat de Cornacchia :

**5.7 Théorème.** *Si $n$ est le plus petit entier tel que $r_n < \sqrt{p}$, on a $p = r_n^2 + b_n^2$.*

*Démonstration.* Ce qui est clair c'est qu'on obtient ainsi un multiple de $p$ :

**5.8 Lemme.** *Pour tout $n \geq 0$, $r_n^2 + b_n^2$ est multiple de $p$.*

*Démonstration.* C'est évident avec la relation $r_n = a_n p + b_n u$ et le fait que $u^2 \equiv -1 \pmod p$.

Pour conclure il reste à contrôler la taille de $b_n$. C'est l'objet du lemme suivant :

**5.9 Lemme.** *Pour tout $n > 0$ on a $r_{n-1}|b_n| \leq p$.*

Si on a établi ce lemme, on a le théorème. En effet, si $n$ est le plus petit entier tel que $r_n < \sqrt{p}$, on a $r_{n-1} \geq \sqrt{p}$, donc, par le lemme, $|b_n| \leq \sqrt{p}$. On a donc $r_n^2 + b_n^2 < 2p$ et ce nombre, qui est multiple de $p$, est bien égal à $p$.

*Démonstration.* (du lemme 5.9) Elle résulte d'un autre lemme :

**5.10 Lemme.** *Avec les notations précédentes, on a les résultats suivants :*
*1) Pour tout $k \geq 0$, $b_{2k}$ est $\leq 0$ et $b_{2k+1} \geq 0$.*
*2) Pour tout $n \geq 0$, on a $a_n b_{n+1} - a_{n+1} b_n = (-1)^n$.*
*3) Pour tout $n \geq 0$ on a $b_{n+1} r_n - b_n r_{n+1} = (-1)^n p$.*
*4) Pour tout $n \geq 0$ on a $|b_{n+1}| r_n = p - |b_n| r_{n+1}$.*

Il est clair que le lemme 5.9 résulte du point 4) ci-dessus appliqué en $n-1$.

*Démonstration.* (du lemme 5.10) Le point 1) est immédiat par récurrence sur $n$ grâce à la deuxième relation de $(**)$. Le point 2) s'établit aussi par récurrence. En effet, il est clair pour $n = 0$ et pour passer de $n$ à $n+1$ il suffit d'écrire $b_{n+1}$ et $a_{n+1}$ avec les relations $(**)$. Le point 3) est alors évident en écrivant $r_n$ et $r_{n+1}$ grâce à $(*)$. Enfin, le point 4) n'est que la traduction de 3) en distinguant les signes selon la parité de $n$.

**5.11** *Remarque.* Pour mettre en œuvre l'algorithme il suffit de déterminer $u$ et de faire l'algorithme d'Euclide jusqu'à rencontrer un reste $r_n < \sqrt{p}$ (il est inutile de calculer les $b_k$). En effet, on trouvera alors $b_n$ comme racine carrée de $p - r_n^2$.

**5.12** *Exemple.* Avec $p = 123456821$, on trouve $u = 2222450$ et les restes successifs 12344571, 9877879, 2466692 et 11111 qui est $< \sqrt{p}$. On vérifie qu'on a $123456821 = 11111^2 + 50^2$.

## 5.2 Les quatre carrés

Il s'agit du célèbre théorème conjecturé par Bachet et prouvé par Lagrange :

**5.13 Théorème.** *Tout entier naturel est somme de quatre carrés d'entiers.*

*Démonstration.* Notons $\Sigma_4$ l'ensemble des entiers de la forme $a^2+b^2+c^2+d^2$. On commence par un résultat de multiplicativité :

**5.14 Proposition.** *L'ensemble $\Sigma_4$ est stable par multiplication.*

*Démonstration.* Le plus simple est d'utiliser le corps des quaternions $\mathbf{H}$. Si $q = a + bi + cj + dk$ est un quaternion, sa "norme" $N(q) = q\,\overline{q}$ est égale à $a^2 + b^2 + c^2 + d^2$ et elle est multiplicative : $N(qq') = N(q)N(q')$. On a alors la conclusion en prenant deux quaternions à coefficients entiers.

**5.15** *Remarque.* En termes d'identités, on a :

$$(a^2+b^2+c^2+d^2)(a'^2+b'^2+c'^2+d'^2) = (aa'+bb'+cc'+dd')^2$$
$$+(ab'-ba'+dc'-cd')^2+(ac'-ca'+bd'-db')^2+(ad'-da'+cb'-bc')^2.$$

La proposition précédente montre qu'il suffit d'établir le théorème pour un nombre premier $p$, ce que nous allons faire en utilisant encore le théorème de Minkowski. On considère le réseau $\mathbf{Z}^4$ de $\mathbf{R}^4$. Pour un point $q = (a, b, c, d)$ on a $N(q) = \|q\|^2 = a^2 + b^2 + c^2 + d^2$. Comme dans le cas des deux carrés, la stratégie est de construire un sous-réseau $L$ dont tous les éléments aient des "normes" multiples de $p$. Cela nécessite d'abord de travailler dans $\mathbf{F}_p$.

**5.16 Lemme.** *Soit $p$ un nombre premier impair.*

*1) Il existe des éléments $u, v \in \mathbf{F}_p$ tels que $u^2 + v^2 + 1 = 0$.*

*2) La forme quadratique $x^2 + y^2 + z^2 + t^2$ sur $\mathbf{F}_p$ est d'indice 2. Un sous-espace totalement isotrope maximal (setim), de dimension 2, est le sous-espace $V$ engendré par $(u, v, 1, 0)$ et $(v, -u, 0, 1)$.*

*Démonstration.* On utilise librement ici les résultats de [DP]. On sait (voir [DP] Ch. III) que $\mathbf{F}_p$ contient $(p + 1)/2$ carrés. C'est aussi le cardinal des nombres de la forme $-1 - v^2$. Il y a donc un élement de $\mathbf{F}_p$ qui est à la fois de la forme $u^2$ et de la forme $-1 - v^2$ et on a le résultat.

2) Il est clair que les deux vecteurs sont isotropes et orthogonaux, de sorte qu'ils engendrent un *setim*.

On peut maintenant définir le sous-réseau $L$ de $\mathbf{Z}^4$. On dispose d'une projection $\pi : \mathbf{Z}^4 \to \mathbf{F}_p^4$, dont le noyau est le sous-réseau $(p\mathbf{Z})^4$. Le réseau $L$ est intermédiaire entre $\mathbf{Z}^4$ et $(p\mathbf{Z})^4$, précisément, on pose $L = \pi^{-1}(V)$ où $V$ est le *setim* défini ci-dessus. Il est clair que $L$ est un sous-groupe de $\mathbf{Z}^4$, donc un sous-groupe discret de $\mathbf{R}^4$, donc un sous-réseau et, comme il contient $(p\mathbf{Z})^4$, c'est un réseau. On peut aussi le montrer en exhibant une $\mathbf{Z}$-base de $L$ formée des quatre vecteurs $(u, v, 1, 0)$, $(v, -u, 0, 1)$, $(p, 0, 0, 0)$ et $(0, p, 0, 0)$. Cela permet d'ailleurs de calculer le volume de $L$ qui est le déterminant de cette $\mathbf{Z}$-base et qui vaut donc $p^2$.

On peut alors appliquer Minkowski en se souvenant que le volume de la boule de rayon $R$ de $\mathbf{R}^4$ est $\dfrac{\pi^2 R^4}{2}$. Si on choisit $R^2$ vérifiant $R^2 > \dfrac{4\sqrt{2}}{\pi} p \simeq 1,8\, p$ et $R^2 < 2p$, le théorème de Minkowski assure qu'il y a dans la boule $B(0, R)$ un point $(a, b, c, d)$ non nul de $L$. Pour ce point, la "norme" $a^2 + b^2 + c^2 + d^2$ est multiple de $p$ (car les points de $L$ s'envoient par $\pi$ sans le *setim* $V$) et comme on a $a^2 + b^2 + c^2 + d^2 \leq R^2 < 2p$, c'est nécessairement qu'on a $p = a^2 + b^2 + c^2 + d^2$ avec $a, b, c, d$ entiers, comme annoncé.

**5.17** *Remarque.* Le choix du réseau $L$ s'explique de plusieurs manières.

1) D'abord, comme dans le cas des deux carrés, l'ensemble des $q \in \mathbf{Z}^4$ tels que $N(q)$ soit multiple de $p$ n'est pas un carré. En prenant l'image réciproque d'un sous-espace vectoriel de $\mathbf{F}_p^4$ en revanche on obtient un sous-groupe, donc un sous-réseau.

2) Bien entendu, $(p\mathbf{Z})^4$ ne convient pas car les normes de ses éléments sont multiples de $p^2$.

3) Enfin, l'image réciproque d'une droite isotrope $V$ de $\mathbf{F}_p^4$ est trop petite. En effet, on sait que le volume de $L$ est le cardinal du groupe quotient $\mathbf{Z}^4/L$, donc de $\mathbf{F}_p^4/V$. Si $V$ est une droite c'est donc $p^3$ et on voit qu'alors Minkowski ne donnerait pas le bon résultat.

## 5.3 Deux autres exemples d'applications de Minkowski

### 5.3.1 Les entiers de la forme $x^2 + 2y^2$

On montre facilement, en utilisant les complexes, que si deux entiers sont de la forme $x^2 + 2y^2$, leur produit aussi. Cela amène à s'intéresser en priorité aux nombres premiers $p$ qui sont de cette forme. Si $p$ est un nombre premier impair qui vérifie $p = x^2 + 2y^2$, $p$ ne divise pas $y$ (sinon il divise aussi $x$ et $p^2$ divise $p$), de sorte que, dans le corps $\mathbf{F}_p$, $-2 = \left(\frac{x}{y}\right)^2$ est un carré. On sait (voir [DP] Ch. 3) que $-1$ est un carré modulo $p$ si et seulement si $p$ est congru à 1 modulo 4. Pour 2, on a le lemme suivant (on se reportera à [DP] ou à [S] pour des détails sur les corps finis) :

**5.18 Lemme.** *Soit $p$ un nombre premier impair. L'entier 2 est un carré modulo $p$ si et seulement si on a $p \equiv \pm 1 \pmod 8$.*

*Démonstration.* Comme $p$ est impair, 8 divise $p^2 - 1 = (p-1)(p+1)$ car l'un des facteurs est multiple de 4. Il en résulte que le groupe multiplicatif du corps $\mathbf{F}_{p^2}$ est de cardinal multiple de 8. Comme il est cyclique, il contient un élément $\zeta$ d'ordre 8 (une racine primitive 8-ième de l'unité). Si $\Phi_8$ est le polynôme cyclotomique d'ordre 8, on a $\Phi_8(X) = X^4 + 1$ et donc $\zeta^4 + 1 = 0$, ou encore $\zeta^2 + \zeta^{-2} = 0$. On considère $\alpha = \zeta + \zeta^{-1}$. On a $\alpha^2 = \zeta^2 + \zeta^{-2} + 2 = 2$. L'élément $\alpha$ est dans $\mathbf{F}_{p^2}$ et 2 est un carré de $\mathbf{F}_p$ si et seulement si il est dans $\mathbf{F}_p$. En appliquant l'homomorphisme de Frobenius, cela revient à dire qu'on a $\alpha^p = \zeta^p + \zeta^{-p} = \alpha = \zeta + \zeta^{-1}$. Il est clair qu'on a cette relation si $p \equiv \pm 1 \pmod 8$. Inversement, si $p \equiv \pm 3 \pmod 8$ on a $\zeta^p + \zeta^{-p} = \zeta^3 + \zeta^{-3}$. Si l'on avait $\zeta^3 + \zeta^{-3} = \zeta + \zeta^{-1}$, on aurait $\zeta^4 + \zeta^{-2} = \zeta^2 + 1$ et comme on a $\zeta^4 = -1$ et $\zeta^{-2} = -\zeta^2$, on aurait $\zeta^2 + 1 = 0$ et $\zeta$ serait racine quatrième de l'unité.

En mettant ensemble les résultats concernant $-1$ et 2 on obtient :

**5.19 Corollaire.** *Soit $p$ un nombre premier impair. L'entier $-2$ est un carré modulo $p$ si et seulement si on a $p \equiv 1 \pmod 8$ ou $p \equiv 3 \pmod 8$.*

On voit qu'une condition nécessaire pour qu'un nombre premier soit de la forme $x^2 + 2y^2$ est qu'il soit congru à 1 ou 3 modulo 8. L'examen des premières

valeurs ($17 = 9 + 2 \times 4$, $41 = 9 + 2 \times 16$, ..., $3 = 1 + 2 \times 1$, $11 = 9 + 2 \times 1$, $19 = 1 + 2 \times 9$ ...) montre que cette condition semble suffisante. De fait :

**5.20 Théorème.** *Soit $p$ un nombre premier congru à 1 ou 3 modulo 8. Alors, $p$ est de la forme $x^2 + 2y^2$ avec $x, y \in \mathbf{N}$.*

*Démonstration.* Soit $u \in \mathbf{Z}$ tel que $u^2 \equiv -2 \pmod{p}$. On considère le réseau $L$ de $\mathbf{R}^2$ de $\mathbf{Z}$-base $(1, 0)$ et $(0, \sqrt{2})$ et son sous-réseau $M$ formé des couples $(uy + zp, y\sqrt{2})$ avec $y, z \in \mathbf{Z}$. Les carrés des normes des points de ce réseau, qui sont de la forme $x^2 + 2y^2$ avec $x, y \in \mathbf{Z}$, sont tous multiples de $p$. Le volume de ce réseau est $p\sqrt{2}$, et comme on a $2\sqrt{2} < \pi$, on peut trouver un réel $R$ qui vérifie $\frac{4\sqrt{2}}{\pi} p < R^2 < 2p$, donc $\pi R^2 > 4p\sqrt{2} = 4\mathrm{vol}\,(M)$. En vertu de Minkowski, $M$ contient un point non nul dans le disque $D(0, R)$, dont le carré de la norme est multiple de $p$, plus petit que $R^2$, donc que $2p$, donc égal à $p$, et on a le résultat.

### 5.3.2 Les entiers de la forme $x^2 + 3y^2$

La méthode est analogue et nous laissons au lecteur la plus grande partie du travail. Le lemme initial est le suivant :

**5.21 Lemme.** *Soit $p$ un nombre premier $> 3$. L'entier $-3$ est un carré modulo $p$ si et seulement si on a $p \equiv 1 \pmod{3}$.*

*Démonstration.* On prend une racine primitive cubique de l'unité $j$ dans $\mathbf{F}_{p^2}$. La formule usuelle $j = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ est encore valable et donne $i\sqrt{3} = 2j + 1$. On voit que $-3$ est un carré de $\mathbf{F}_p$ si et seulement si $2j + 1 \in \mathbf{F}_p$ donc si $j$ est dans $\mathbf{F}_p$. Mais cela signifie exactement qu'il y a un élément d'ordre 3 dans $\mathbf{F}_p^*$, donc que 3 divise $p - 1$.

On obtient alors le théorème :

**5.22 Théorème.** *Un nombre premier $p > 3$ est de la forme $x^2 + 3y^2$ avec $x, y \in \mathbf{N}$ si et seulement si on a $p \equiv 1 \pmod{3}$.*

*Démonstration.* On considère un réseau analogue à celui du paragraphe précédent. Attention, comme $\pi > 2\sqrt{3}$, on n'a pas la conclusion de manière immédiate, mais on montre que $p$ ou $2p$ est de la forme $x^2 + 3y^2$. Mais la deuxième solution est impossible car on aurait $2p \equiv 2 \equiv x^2 \pmod{3}$ et c'est absurde.

**5.23** *Exercice.* En appliquant les méthodes précédentes, montrer qu'un nombre premier $p$ est de la forme $x^2 + 7y^2$ si et seulement si $p = 7$ ou $p \equiv 1, -3, 2 \pmod{7}$. (Minkowski permet d'affirmer que $p$, $2p$ ou $3p$ est de la forme voulue et des arguments de congruence modulo 4 ou 7 permettent de conclure.)

**5.24** *Exercice.* Soit $n$ un entier $> 0$. On munit $\mathbf{R}^n$ de la forme euclidienne pour laquelle la base canonique est orthonormée. Soit $q$ une forme quadratique définie positive sur $\mathbf{R}^n$, définie sur la base canonique par une matrice symétrique à coefficients **entiers**. On appelle $D$ le discriminant de $q$, c'est-à-dire le déterminant de $M$.

Montrer qu'il existe $x \in \mathbf{Z}^n$ non nul tel que l'on ait $q(x) \leq \dfrac{4\sqrt[n]{D}}{\sqrt[n]{\omega_n^2}}$ où $\omega_n$ est le volume de la boule unité de $\mathbf{R}^n$ pour la forme euclidienne canonique.

**5.25** *Remarque.* Il y a bien d'autres applications du théorème de Minkowski, par exemple à la recherche des entiers de la forme $x^2 + 5y^2$ (voir [TER]) ou à la résolution d'équations diophantiennes (par exemple $3x^2 - 35y^2 = c$), voir `http://www.math.u-psud.fr/~perrin/CAPES/arithmetique/Equation-diophantienne4.pdf`.

# 6 Annexes

## 6.1 Les espaces $\Lambda^k E$

### 6.1.1 Définitions

On considère un espace vectoriel $E$ de dimension $n$ sur un corps $K$ et un entier $k$ vérifiant $1 \leq k \leq n$. Rappelons la définition suivante :

**6.1 Définition.** *Une application $f : E^k \to K$, qui à $(x_1, \ldots, x_k)$ associe $f(x_1, \ldots, x_k)$, est appelée une* **forme $k$-linéaire alternée** *si $f$ est linéaire par rapport à chaque variable $x_i$ et si $f(x_1, \ldots, x_k)$ est nulle dès que deux des variables sont égales.*

**6.2 Proposition.** *Soit $e_1, \ldots, e_n$ une base de $E$ et soit $f : E^k \to K$ une forme $k$-linéaire.*

*1) La forme $f$ est déterminée par les valeurs $f(e_{i_1}, \ldots, e_{i_k})$ pour $i_1, \ldots, i_k \in \{1, \ldots, n\}$.*

*2) Si de plus $f$ est alternée, $f$ est déterminée par les $f(e_{i_1}, \ldots, e_{i_k})$ avec $1 \leq i_1 < i_2 < \cdots < i_k \leq n$.*

*Démonstration.* 1) Si $x_j = \sum_{i=1}^n x_{ij} e_i$, le résultat vient de la formule :

$$f(x_1, \ldots, x_k) = \sum x_{i_1,1} \cdots x_{i_k k} f(e_{i_1}, \ldots, e_{i_k})$$

2) Si $f$ est alternée, elle est nulle lorsque deux indices coïncident, de sorte qu'on peut supposer les $e_{il}$ distincts. De plus, on peut les supposer ordonnés car si $\sigma$ est une permutation de l'ensemble $\{1, \ldots, k\}$, on a $f(x_{\sigma(1)}, \ldots, x_{\sigma(k)}) = \epsilon(\sigma) f(x_1, \ldots, x_k)$.

**6.3 Définition.** *1) On appelle $A_k(E)$ l'espace vectoriel des formes $k$-linéaires alternées sur $E$.*

*2) On appelle $\Lambda^k E$ le dual de $A_k(E)$.*

### 6.1.2 Bases

Soit $e_1, \ldots, e_n$ une base de $E$. Pour une suite d'entiers $1 \leq i_1 < i_2 < \cdots < i_k \leq n$ on définit $f_{i_1,\ldots,i_k} \in A_k(E)$ comme suit :

a) $f_{i_1,\ldots,i_k}(e_{j_1}, \ldots, e_{j_k}) = 0$ si $\{i_1, \ldots, i_k\} \neq \{j_1, \ldots, j_k\}$.

b) Si $\{i_1, \ldots, i_k\} = \{j_1, \ldots, j_k\}$ et si $\sigma \in \mathfrak{S}_k$ est la permutation définie par $\sigma(i_p) = j_p$, $f_{i_1,\ldots,i_k}(e_{j_1}, \ldots, e_{j_k}) = \epsilon(\sigma)$.

**6.4 Proposition.** *Les formes $f_{i_1,\ldots,i_k}$ constituent une base de $A_k(E)$ qui est donc de dimension $\binom{n}{k}$.*

*Démonstration.* Cela résulte de 6.2.

On a une application naturelle $\varphi : E^k \to \Lambda^k E$ qui à $(x_1, \ldots, x_k)$ associe $x_1 \wedge \cdots \wedge x_k$ définie par $(x_1 \wedge \cdots \wedge x_k)(f) = f(x_1, \ldots, x_k)$ pour toute $f \in A_k(E)$. Il est clair que $\varphi$ est une application $k$-linéaire alternée.

**6.5 Proposition.** *La famille des*

$$e_{i_1} \wedge \cdots \wedge e_{i_k}, \text{ avec } 1 \leq i_1 < i_2 < \cdots < i_k \leq n$$

*est une base de $\Lambda^k E$.*

*Démonstration.* La définition des $e_{i_1} \wedge \cdots \wedge e_{i_k}$ montre qu'ils constituent la base duale de celle des $f_{i_1,\ldots,i_k}$.

**6.6 Proposition.** *Avec les notations de 6.5, si $e'_1, \ldots, e'_n$ est une autre base de $E$ et si $A = (a_{ij})$ est la matrice de passage des $e_i$ aux $e'_i$, la matrice de passage des $e_{i_1} \wedge \cdots \wedge e_{i_k}$ aux $e'_{i_1} \wedge \cdots \wedge e'_{i_k}$ est la matrice des mineurs d'ordre $k$ de $A$.*

*Démonstration.* On écrit $e'_j = \sum_{i=1}^n a_{ij} e_i$ et on calcule :

$$e'_{j_1} \wedge \cdots \wedge e'_{j_k} = \sum_i a_{i,j_1} e_i \wedge \cdots \wedge \sum_i a_{i,j_k} e_i.$$

Vu l'alternance, le coefficient sur $e_{i_1} \wedge \cdots \wedge e_{i_k}$ est $\sum_{\sigma \in \mathfrak{S}_k} \epsilon(\sigma) a_{\sigma(i_1)j_1} \cdots a_{\sigma(i_k)j_k}$, c'est-à-dire le déterminant $k \times k$ extrait de $A$ qui correspond aux lignes d'indices $i_1, \ldots, i_k$ et aux colonnes d'indices $j_1, \ldots, j_k$.

# 7 Références

[N] NITAJ Abderrahmane, *L'algorithme de Cornacchia*, Expositiones Math. 13 (1995), pp. 358-365.

[DP] PERRIN Daniel, *Cours d'algèbre*, Ellipses, 1996.

[IGADP] PERRIN Daniel, *Géométrie algébrique, une introduction*, Interéditions, Paris, 1995.

[GeoDP] PERRIN Daniel, *Géométrie projective et applications aux géométries euclidienne et non euclidiennes*
`http://www.math.u-psud.fr/~perrin/Livre_de_geometrie_projective.html`

[S] SERRE Jean-Pierre, *Cours d'arithmétique*, PUF, Paris, 1970.

[ST] STEWART Ian & TALL David, *Algebraic Number Theory*, Chapmann-Hall, 1987.

[TER] PERRIN Daniel, *Anneaux d'entiers des corps quadratiques imaginaires*, rédaction de TER (disponible pour les collègues sur simple demande).