**80.05M**

SESSION 2008

---

# Filière MP (groupe I)

Épreuve commune aux ENS de Paris, Lyon et Cachan

## Filière PC (groupe I)

Épreuve commune aux ENS de Paris et Lyon

---

# MATHÉMATIQUES - INFORMATIQUE

---

Durée : 4 heures

---

*Les calculatrices sont inutiles et de ce fait ne sont pas autorisées*

**Préambule** L'objet du sujet est d'étudier quelques propriétés mathématiques et algorithmiques des ensembles convexes : le lemme de Farkas et la programmation linéaire, les fonctions de jauge et le premier théorème de Minkowski, les minima successifs et les réseaux admissibles, une technique de réduction de base. Les applications de ces techniques sont nombreuses, notamment en optimisation combinatoire, mais ne sont pas abordées dans le sujet.

Les deux premières parties sont indépendantes. Les troisième et quatrième parties s'appuient essentiellement sur la deuxième. Le sujet n'est pas de difficulté progressive : chaque partie comporte des questions relativement difficiles et, globalement, le sujet comporte peu de questions élémentaires.

**Notations** On se place dans l'espace vectoriel euclidien $\mathbb{R}^n$, muni du produit scalaire usuel. Si $\vec{x}$ est un vecteur de $\mathbb{R}^n$, on note $x_i$ sa $i$-ème composante, pour $1 \leq i \leq n$. Si $\vec{x} \in \mathbb{R}^n$ et $\vec{y} \in \mathbb{R}^n$, on note $\vec{x}.\vec{y}$ leur produit scalaire. Les opérations portant sur des vecteurs sont à comprendre composante par composante : ainsi, $\vec{x} \geq \vec{0}$ signifie $x_i \geq 0$ pour tout $i$. Un vecteur peut être considéré comme vecteur ligne ou vecteur colonne selon le contexte, s'il n'y a pas ambiguïté. Ainsi, pour $\vec{x} \in \mathbb{R}^n$, $\vec{y} \in \mathbb{R}^m$ et une matrice $A$ de taille $n \times m$, on note $A\vec{y}$ le produit de $A$ par $\vec{y}$, $\vec{y}$ étant considéré comme vecteur colonne, et $\vec{x}A$ le produit de $\vec{x}$ par $A$, $\vec{x}$ étant considéré comme vecteur ligne. Enfin, on utilise les notations ensemblistes suivantes : si $S \subseteq \mathbb{R}^n$, $T \subseteq \mathbb{R}^n$, $\lambda \in \mathbb{R}$ et $\vec{x} \in \mathbb{R}^n$, on note $\vec{x} + S$ l'ensemble des vecteurs $\vec{x} + \vec{y}$ avec $\vec{y} \in S$, $\lambda S$ l'ensemble des vecteurs $\lambda\vec{y}$ avec $\vec{y} \in S$, et $S + T$ l'ensemble des vecteurs $\vec{y} + \vec{z}$ avec $\vec{y} \in S$ et $\vec{z} \in T$.

## Partie 1. Lemme de Farkas et théorème de dualité

Un ensemble $K \subseteq \mathbb{R}^n$ est **convexe** si $\forall \vec{x}, \vec{y} \in K$, $\forall \lambda \in \mathbb{R}$, $0 \leq \lambda \leq 1$, $\lambda\vec{x} + (1-\lambda)\vec{y} \in K$. C'est un **cône** si $\forall \vec{x}, \vec{y} \in K$, $\forall \lambda, \mu \in \mathbb{R}^+$, $\lambda\vec{x} + \mu\vec{y} \in K$. S'il existe une matrice $C$ à coefficients réels, de taille $m \times n$, telle que $K = \{\vec{x} \in \mathbb{R}^n \mid C\vec{x} \leq \vec{0}\}$, on dit que $K$ est un **cône polyédral**. S'il existe $\vec{a}_1, \ldots, \vec{a}_m \in \mathbb{R}^n$ tels que $K = \{\vec{x} \in \mathbb{R}^n \mid \vec{x} = \sum_{i=1}^m y_i\vec{a}_i \text{ avec } \forall i,\ y_i \geq 0\}$, on dit que $K$ est le **cône engendré** par $\vec{a}_1, \ldots, \vec{a}_m$. Dans ce cas, on peut aussi écrire $K$ matriciellement : $K = \{A\vec{y} \mid \vec{y} \geq 0\}$ où cette fois-ci $A$ est de taille $n \times m$ et les $\vec{a}_i$ sont les colonnes de $A$.

**Question 1.1.** *Vérifier qu'un cône polyédral (respectivement engendré) est bien un cône. Montrer que $K$ est un cône si et seulement s'il est convexe et $\forall \vec{x} \in K$, $\forall \lambda \geq 0$, $\lambda\vec{x} \in K$. Montrer qu'un cône polyédral est intersection de demi-espaces, c'est-à-dire d'ensembles de la forme $\{\vec{x} \in \mathbb{R}^n \mid \vec{c}.\vec{x} \leq 0\}$.*

Pour $K \subseteq \mathbb{R}^n$, on définit le **polaire** de $K$ comme l'ensemble $K^* = \{\vec{z} \in \mathbb{R}^n \mid \forall \vec{x} \in K,\ \vec{z}.\vec{x} \leq 1\}$.

**Question 1.2.** *Montrer les propriétés suivantes : a) $K^*$ est convexe, b) $K \subseteq (K^*)^*$ ; c) si $K$ est un cône, $K^*$ est un cône et $K^* = \{\vec{z} \in \mathbb{R}^n \mid \forall \vec{x} \in K,\ \vec{z}.\vec{x} \leq 0\}$ ; d) si $K$ est un cône engendré, $K^*$ est un cône polyédral ; e) si $K$ est un cône polyédral, $K = (K^*)^*$.*

Soit $A$ une matrice réelle de taille $n \times m$, $n \leq m$, de rang $n$ et $\vec{b}$ de dimension $n$. On note $\vec{a}_1, \ldots, \vec{a}_m$ les colonnes de $A$ et $\mathcal{D} = \{\vec{a}_{i_1}, \ldots, \vec{a}_{i_n}\}$ un ensemble constitué de $n$ vecteurs linéairement indépendants parmi ces $m$ vecteurs. On effectue les opérations suivantes :

**Étape 1 :** Écrire $\vec{b}$ (de façon unique) comme $\vec{b} = \sum_{j=1}^n \mu_{i_j}\vec{a}_{i_j}$.

**Étape 2 :** Choisir, s'il existe, l'indice minimal $h \in \{i_1, \ldots, i_n\}$ tel que $\mu_h < 0$, sinon STOP.

**Étape 3 :** Soit $\vec{c}$ tel que $\vec{c}.\vec{a}_{i_j} = 0$ pour tout $i_j \neq h$ et $\vec{c}.\vec{a}_h = 1$. Choisir, s'il existe, l'indice minimal $k \in \{1, \ldots, m\}$ tel que $\vec{c}.\vec{a}_k < 0$, sinon STOP.

**Étape 4 :** Remplacer $\mathcal{D}$ par $\mathcal{D} \setminus \{\vec{a}_h\} \cup \{\vec{a}_k\}$ et reprendre à l'étape 1.

**Question 1.3.** *On note $K$ le cône engendré par les vecteurs $(\vec{a}_i)_{1 \leq i \leq m}$.*

1. *Montrer que l'algorithme précédent est bien défini, que s'il stoppe à l'étape 2 alors $\vec{b} \in K$ et que s'il stoppe à l'étape 3 alors il existe $\vec{c}$ tel que $\vec{c}.\vec{b} < 0$ et $-\vec{c} \in K^*$.*
2. *Montrer que l'algorithme ne boucle pas. Indication : s'il existe deux itérations $i < j$ pour lesquelles l'ensemble $\mathcal{D}$ est le même, on pourra considérer le plus grand indice $r$ tel que $\vec{a}_r$ quitte $\mathcal{D}$ (à l'itération $p$) et y retourne (à l'itération $q$) avec $i \leq p < q < j$ et calculer $\vec{c}_q.\vec{b}$ avec $\vec{b}$ exprimé dans la base utilisée à l'étape $p$.*
3. *En déduire le* **lemme de Farkas** *: de deux choses l'une, soit il existe $\vec{y} \geq \vec{0}$ tel que $\vec{b} = A\vec{y}$, soit il existe $\vec{c}$ tel que $\vec{c}.\vec{b} < 0$, $\vec{c}A \geq \vec{0}$ et $\vec{c}.\vec{a}_i = 0$ pour $(n-1)$ vecteurs $\vec{a}_i$ linéairement indépendants.*

On admettra que le lemme de Farkas se généralise au cas où $A$ est une matrice quelconque : dans ce cas, la condition portant sur $\vec{c}$ est que $\vec{c}$ est orthogonal à $t-1$ vecteurs $\vec{a}_i$ linéairement indépendants où $t$ est le rang de $(\vec{a}_1, \ldots, \vec{a}_m, \vec{b})$. On sera également amené à utiliser l'énoncé (légèrement affaibli) suivant : il existe $\vec{y} \geq \vec{0}$ tel que $\vec{b} = A\vec{y}$ si et seulement si $\vec{c}A \leq \vec{0}$ implique $\vec{c}.\vec{b} \leq 0$.

**Question 1.4.**

1. *En utilisant le lemme de Farkas, montrer que si $K$ un est cône engendré alors $(K^*)^* = K$ et $K$ est polyédral. Pour ce deuxième point, utiliser la condition supplémentaire du lemme de Farkas portant sur $\vec{c}$ : "$\vec{c}.\vec{a}_i = 0$ pour $t-1$ vecteurs $\vec{a}_i$ linéairement indépendants".*
2. *Montrer que si $K$ est un cône polyédral, il est engendré. On pourra considérer un cône engendré $J$ tel que $J^* = K$.*

**Question 1.5.** *On note $I_n$ la matrice identité de taille $n$. Soit $A$ une matrice réelle de taille $n \times m$, $\vec{b} \in \mathbb{R}^n$ et $\vec{c} \in \mathbb{R}^m$. Montrer, en considérant la matrice $\begin{pmatrix} A & -A & I_n \end{pmatrix}$, de taille $n \times (2m+n)$, et le lemme de Farkas, qu'il existe $\vec{x}$ tel que $A\vec{x} \leq \vec{b}$ si et seulement si $\vec{y}.\vec{b} \geq 0$ pour tout $\vec{y} \geq \vec{0}$ tel que $\vec{y}A = \vec{0}$. Montrer ensuite le* **théorème de dualité** *suivant. Si $\{\vec{x} \mid A\vec{x} \leq \vec{b}\}$ et $\{\vec{y} \mid \vec{y} \geq \vec{0},\ \vec{y}A = \vec{c}\}$ sont non vides alors :*

$$\max\{\vec{c}.\vec{x} \mid A\vec{x} \leq \vec{b}\} = \min\{\vec{y}.\vec{b} \mid \vec{y} \geq \vec{0},\ \vec{y}A = \vec{c}\}$$

*Pour cela, on montrera, en utilisant la première partie de la question, qu'il existe $\vec{x}$ et $\vec{y}$ tels que :*

$$\begin{pmatrix} A & 0 \\ 0 & {}^tA \\ 0 & -{}^tA \\ -{}^t\vec{c} & {}^t\vec{b} \\ 0 & -I_n \end{pmatrix} \begin{pmatrix} \vec{x} \\ \vec{y} \end{pmatrix} \leq \begin{pmatrix} \vec{b} \\ \vec{c} \\ -\vec{c} \\ 0 \end{pmatrix}$$

*(Tous les vecteurs sont ici des vecteurs colonnes. On utilise la notation ${}^t$ pour les transposer.) On sera amené à distinguer deux cas selon qu'une certaine variable réelle, introduite par l'application du lemme de Farkas, est nulle ou pas.*

## Partie 2. Corps convexes, normes et premier théorème de Minkowski

Pour $\vec{x} \in \mathbb{R}^n$, on définit $\|\vec{x}\|_r = (\sum_{i=1}^n |x_i|^r)^{\frac{1}{r}}$. On rappelle que pour $r \geq 1$, $\|.\|_r$ est une **norme**.

**Question 2.1.** *Soit la fonction $\Gamma$ définie par $\Gamma(x) = \int_0^{+\infty} e^{-t}t^{x-1}dt$.*

1. *Rappeler pourquoi la fonction $\Gamma$ est bien définie sur $\mathbb{R}^{+*}$ et $\Gamma(x+1) = x\Gamma(x)$.*
2. *Montrer que $\Gamma(p)\Gamma(q) = \Gamma(p+q)\int_0^1 (1-t)^{p-1}t^{q-1}dt$, par un calcul d'intégrale double et en remarquant que $0 \leq t < +\infty$, $t \leq u < +\infty$ si et seulement si $0 \leq u < +\infty$, $0 \leq t \leq u$.*

**Question 2.2.** *On note $V_{r,n}(R)$ le volume de $\{\vec{x} \in \mathbb{R}^n \mid \|\vec{x}\|_r \leq R\}$, la boule de rayon $R$ en dimension $n$ pour la norme $\|.\|_r$. Établir une relation entre $V_{r,n}(R)$ et $V_{r,n}(1)$ puis entre $V_{r,n}(1)$ et $V_{r,n-1}(1)$ et montrer finalement que :*

$$V_{r,n}(1) = \frac{\{2\Gamma(\frac{1}{r}+1)\}^n}{\Gamma(\frac{n}{r}+1)}$$

*À quoi est égal ce volume lorsque $r = 1$, $r = 2$ ?*

Soit $K \subseteq \mathbb{R}^n$. On rappelle que $\vec{x}$ appartient à l'**adhérence** de $K$, notée $\overline{K}$, si $\vec{x}$ est limite d'une suite d'éléments de $K$ et que $\vec{x}$ appartient à l'**intérieur** de $K$, noté $\overset{\circ}{K}$, s'il existe $r > 0$ tel que la boule de centre $\vec{x}$ et de rayon $r$ appartient à $K$.

**Question 2.3.** *Montrer que si $K$ est convexe, son adhérence $\overline{K}$ et son intérieur $\overset{\circ}{K}$ sont convexes. Montrer que si, de plus, $\vec{0} \in \overset{\circ}{K}$ alors $\lambda K \subseteq \overset{\circ}{K}$ si $0 \leq \lambda < 1$ et $\overline{K} \subseteq \lambda K$ si $\lambda > 1$. (Ne pas hésiter à s'aider de dessins pour toutes ces propriétés.)*

Un **corps convexe** est un convexe borné $K$ tel que $\vec{0} \in \overset{\circ}{K}$. On lui associe la **fonction de jauge** $f$ définie par $f(\vec{x}) = \inf\{\lambda \mid \lambda \geq 0,\ \vec{x} \in \lambda K\}$ pour tout $\vec{x} \neq \vec{0}$ et $f(\vec{0}) = 0$.

**Question 2.4.** *Montrer que la fonction de jauge $f$ d'un corps convexe $K$ est bien définie et que :*
**(i)** *$f(\vec{x}) > 0$ si $\vec{x} \neq \vec{0}$ ;*
**(ii)** *$f(\alpha\vec{x}) = \alpha f(\vec{x})$ si $\alpha > 0$.*
**(iii)** *$f(\vec{x}+\vec{y}) \leq f(\vec{x}) + f(\vec{y})$ si $\vec{x} \in \mathbb{R}^n$ et $\vec{y} \in \mathbb{R}^n$.*
*Pour démontrer (iii), on commencera par montrer que $\vec{x}/f(\vec{x}) \in \overline{K}$ puis, en utilisant les résultats de la question 2.3, que $\vec{x} \in \overset{\circ}{K}$ si et seulement si $f(\vec{x}) < 1$ et $\vec{x} \in \overline{K}$ si et seulement si $f(\vec{x}) \leq 1$.*

On remarque que lorsque $K$ est symétrique par rapport à $\vec{0}$, c'est-à-dire $\vec{x} \in K$ si et seulement si $-\vec{x} \in K$, alors sa fonction de jauge $f$ vérifie de plus $f(\alpha\vec{x}) = |\alpha| f(\vec{x})$, c'est donc une **norme**.

**Question 2.5.** *Réciproquement, soit $f$ une fonction de $\mathbb{R}^n$ dans $\mathbb{R}$ satisfaisant les propriétés (i), (ii) et (iii) précédentes. Montrer qu'il existe $M > 0$ tel que pour tout $\vec{x} \in \mathbb{R}^n$, $f(\vec{x}) \leq M \sum_i |x_i|$. En déduire que $f$ est continue en $\vec{0}$, puis sur $\mathbb{R}^n$. Montrer enfin que l'ensemble $K = \{\vec{x} \in \mathbb{R}^n \mid f(\vec{x}) \leq 1\}$ est un corps convexe dont $f$ est la fonction de jauge.*

Lorsque $f$ est une norme, donc lorsque $f$ possède en plus la propriété $f(\alpha\vec{x}) = |\alpha| f(\vec{x})$, il est facile de voir que le corps convexe $K = \{\vec{x} \mid f(\vec{x}) \leq 1\}$ est symétrique par rapport à $\vec{0}$. On suppose que c'est le cas dans tout le reste de cette partie.

**Question 2.6.** *Montrer que la fonction de jauge $f^*$ du polaire $K^* = \{\vec{z} \mid \forall \vec{x} \in K,\ \vec{z}.\vec{x} \leq 1\}$ d'un ensemble $K$ est égal à $f^*(\vec{z}) = \sup\{\vec{z}.\vec{x} \mid \vec{x} \in K\}$.*

Dans la suite, on parlera de volumes sans se préoccuper de questions théoriques d'existence et on notera $\mathrm{Vol}(K)$ le **volume** de $K$. On utilisera en particulier la relation $\mathrm{Vol}(\lambda K) = \lambda^n \mathrm{Vol}(K)$ en dimension $n$ pour tout $\lambda > 0$.

**Question 2.7.** *On suppose que $Vol(K) > 1$. Pour $\vec{x} \in \mathbb{Z}^n$, soit $V_{\vec{x}}$ le volume de $K \cap (\vec{x}+C)$ où $C$ est le cube $\{\vec{y} \in \mathbb{R}^n \mid 0 \leq y_i < 1, \forall i\}$. En remarquant que $Vol(K) = \sum_{\vec{x} \in \mathbb{Z}^n} V_{\vec{x}}$ et en considérant les intersections $C \cap (K - \vec{x})$, montrer qu'il existe $\vec{z}_1 \in K$ et $\vec{z}_2 \in K$ tels que $\vec{z}_1 - \vec{z}_2 \in \mathbb{Z}^n$.*

**Question 2.8.** *En considérant $\frac{1}{2}K$ et en utilisant le fait que $K$ est symétrique, montrer que si $Vol(K) > 2^n$, il existe $\vec{x} \neq \vec{0}$ tel que $\vec{x} \in \mathbb{Z}^n \cap K$ (**premier théorème de Minkowski**). Montrer que ceci reste vrai si $Vol(K) \geq 2^n$ et $K$ est fermé.*

**Question 2.9.** *Montrer que $\inf\{\lambda > 0 \mid (\lambda K \cap \mathbb{Z}^n) \neq \{\vec{0}\}\} = \min\{f(\vec{x}) \mid \vec{x} \in \mathbb{Z}^n \setminus \{\vec{0}\}\}$ où $f$ est la fonction de jauge de $K$. En déduire qu'il existe $\vec{x} \in \mathbb{Z}^n$, $\vec{x} \neq \vec{0}$, tel que $f(\vec{x}) \leq 2\, Vol(K)^{-1/n}$. Soit $A$ une matrice carrée de taille $n$ inversible. Montrer, par un changement de variable, qu'il existe $\vec{y} \in \mathbb{Z}^n$, $\vec{y} \neq \vec{0}$, tel que $f(\vec{x}) \leq 2\, Vol(K)^{-1/n} |\det(A)|^{1/n}$ où $\vec{x} = A\vec{y}$.*

**Question 2.10.** *Soit $A$ une matrice carrée de taille $n$ inversible. Soit $K = \{\vec{x} \in \mathbb{R}^n \mid |x_i| \leq 1, \forall i\}$. Montrer qu'il existe $\vec{y} \in \mathbb{Z}^n$, $\vec{y} \neq \vec{0}$ tel que $\vec{x} = A\vec{y}$ vérifie $|x_i| \leq |\det A|^{1/n}$ pour tout $i$ et donc $|x_1 \cdots x_n| \leq |\det(A)|$. En utilisant cette fois la fonction de jauge $f(\vec{x}) = \sum_i |x_i|/n$ et une inégalité de convexité, montrer qu'on peut choisir $\vec{y} \in \mathbb{Z}^n \setminus \{\vec{0}\}$ pour que $|x_1 \cdots x_n| \leq |\det(A)| n!/n^n$.*

**Question 2.11.** *Soit $A$ une matrice de taille $n$ telle que $|\det(A)| = 1$ et $c_1, \ldots, c_n$ des réels de produit égal à 1. Montrer qu'il existe $\vec{y} \in \mathbb{Z}^n$, $\vec{y} \neq \vec{0}$, tel que pour tout $i$, $|x_i| \leq c_i$ où $\vec{x} = A\vec{y}$. En déduire le résultat d'approximation simultanée suivant : pour tous réels $\alpha_1, \ldots, \alpha_n$ et $N > 1$, il existe un entier positif non nul $q \leq N$ et des entiers $p_1, \ldots, p_n$ tels que, pour tout $i$, $|\alpha_i - \frac{p_i}{q}| \leq N^{-1-1/n}$.*

## Partie 3. Minima successifs et réseaux admissibles

Soit $K \subset \mathbb{R}^n$ un corps convexe symétrique par rapport à $\vec{0}$ et $f$ sa fonction de jauge associée. On définit les **minima successifs** $\lambda_i(K)$, pour $1 \leq i \leq n$, de la façon suivante :

$$\lambda_i(K) = \inf\{\lambda \mid \dim(\lambda K \cap \mathbb{Z}^n) \geq i\}$$

où $\dim(E)$ est la dimension de l'espace vectoriel engendré par les vecteurs de $E$. En d'autres termes, $\lambda_i(K)$ est le plus petit $\lambda$ tel que $\lambda K$ contienne $i$ vecteurs entiers linéairement indépendants. On a bien sûr $\lambda_1(K) \leq \ldots \leq \lambda_n(K)$. S'il n'y a pas ambiguïté, on notera simplement $\lambda_i$ au lieu de $\lambda_i(K)$.

**Question 3.1.** *Montrer qu'on peut définir $n$ vecteurs entiers $\vec{x_1}, \ldots, \vec{x_n}$, linéairement indépendants, tels que $f(\vec{x_i}) = \lambda_i$ et $f(\vec{x_i})$ est la plus petite valeur de $f(\vec{x})$ pour $\vec{x}$ dans $\mathbb{Z}^n$ qui n'est pas combinaison linéaire de $\vec{x_1}, \ldots, \vec{x_{i-1}}$.*

Soit $\vec{a}_1, \ldots, \vec{a}_n$ une base de $\mathbb{R}^n$. L'ensemble $\Lambda$ des combinaisons linéaires *entières* de ces vecteurs est appelé **réseau** engendré par (ou de base) $\vec{a}_1, \ldots, \vec{a}_n$. Matriciellement $\Lambda = \{\vec{x} \mid \vec{x} = A\vec{y}, \vec{y} \in \mathbb{Z}^n\}$ où $A$ est la matrice dont les colonnes sont les $\vec{a}_i$. On dira aussi que $A$ est une base de $\Lambda$.

**Question 3.2.** *Montrer que si $A$ et $B$ sont deux bases d'un même réseau $\Lambda$ alors il existe une matrice carrée $Q$ entière, d'inverse entière, tel que $B = AQ$. En déduire que $|\det(A)|$ ne dépend pas de la base $A$ d'un réseau. On l'appelle le* **déterminant** *du réseau, noté* $\det(\Lambda)$.

Soit $K$ un corps convexe symétrique par rapport à $\vec{0}$. On dit qu'un réseau $\Lambda$ est admissible pour $K$ si $K \cap \Lambda = \{\vec{0}\}$. On définit $\Delta(K) = \inf\{\det(\Lambda) \mid \Lambda \text{ admissible pour } K\}$.

**Question 3.3.** *Montrer que l'inégalité $2^n \Delta(K) \geq Vol(K)$ est une reformulation du premier théorème de Minkowski.*

Soit $K$ tel que $\mathrm{Vol}(K) < 1$. Pour un nombre premier $p$ et $\vec{u} \in \mathbb{Z}^n$ tel que $u_1 = 1$ et $0 \leq u_i < p$ pour $2 \leq i \leq n$, on définit le réseau $\Lambda(p, \vec{u})$ de base $\vec{u}$, $(0, p, 0, \ldots, 0)$, $(0, 0, p, 0, \ldots, 0)$, $\ldots$, $(0, \ldots, 0, p)$.

**Question 3.4.** *Montrer que, pour $p$ fixé, pour tout $\vec{v} \in \mathbb{Z}^n$ tel que $v_1$ n'est pas un multiple de $p$, il existe un unique réseau $\Lambda(p, \vec{u})$ contenant $\vec{v}$. En déduire que $Y = \{\vec{v} \in \mathbb{Z}^n \mid v_1$ n'est pas multiple de $p\}$ est union disjointe de $p^{n-1}$ ensembles $\Lambda(p, \vec{u}) \cap Y$.*

On considère, pour chaque $\vec{x} \in p^{-(n-1)/n}\mathbb{Z}^n$ (c'est-à-dire tel que $p^{(n-1)/n}\vec{x}$ est entier), le cube $C_{\vec{x}} = \vec{x} + p^{-(n-1)/n}C$ où $C$ est le cube $\{\vec{y} \in \mathbb{R}^n \mid 0 \leq y_i < 1, \forall i\}$. Ces cubes, tous de volume $p^{-(n-1)}$, forment une partition de $\mathbb{R}^n$ et, si $\#S$ représente le nombre d'éléments d'un ensemble fini $S$, on a :

$$\lim_{p \to +\infty} p^{-(n-1)} \#\{\vec{x} \in p^{-(n-1)/n}\mathbb{Z}^n \mid K \cap C_{\vec{x}} \neq \emptyset\} = \mathrm{Vol}(K) < 1$$

résultat intuitif que l'on admettra.

**Question 3.5.** *Montrer que si $p$ est choisi suffisamment grand, il existe un réseau $\Lambda(p, \vec{u})$ tel que $\#(K \cap p^{-(n-1)/n}(\Lambda(p, \vec{u}) \cap Y)) < 1$, c'est-à-dire $(p^{(n-1)/n}K) \cap (\Lambda(p, \vec{u}) \cap Y) = \emptyset$. De plus, si $p$ est suffisamment grand pour que $|x_i| < p^{1/n}$ pour tout $\vec{x} \in K$, alors $(p^{(n-1)/n}K) \cap \Lambda(p, \vec{u}) \subseteq \{\vec{0}\}$. En déduire qu'il existe un réseau admissible pour $K$ de déterminant 1.*

**Question 3.6.** *Soit $K$ de volume quelconque. Montrer que $\Delta(K) \leq Vol(K)$.*

## Partie 4. Réduction de base de Lovász et Scarf

Dans cette partie, $K \subset \mathbb{R}^n$ est un corps convexe et on note $f$ sa fonction de jauge associée. Étant donnée une base $(\vec{b_1}, \ldots, \vec{b_n})$ du réseau $\mathbb{Z}^n$, on définit $n$ fonctions $f_i$, pour $1 \leq i \leq n$, par $f_i(\vec{x}) = \inf\{f(\vec{x} + \alpha_1\vec{b_1} + \ldots \alpha_{i-1}\vec{b_{i-1}}) \mid \alpha_1 \in \mathbb{R}, \ldots, \alpha_{i-1} \in \mathbb{R}\}$. Par définition, $f_1 = f$.

**Question 4.1.** *Montrer que $f_i(\vec{x}) = g_i(\pi_i(\vec{x}))$ où $\pi_i$ est la projection sur l'espace vectoriel engendré par $\vec{b_i}, \ldots, \vec{b_n}$, parallèlement à $\vec{b_1}, \ldots, \vec{b_{i-1}}$, et $g_i$ est la fonction de jauge associée à $\pi_i(K)$.*

**Question 4.2.** *Montrer que si $f_1(\vec{b_1}) \leq f_2(\vec{b_2}) \leq \ldots \leq f_n(\vec{b_n})$ alors $\vec{b_1}$ atteint le premier minimum successif, c'est-à-dire $f(\vec{b_1}) = \lambda_1(K)$.*

Il est difficile de trouver une base vérifiant les conditions précédentes. On s'intéresse alors à des conditions plus faibles. Soit $\epsilon \in \mathbb{R}$, $0 < \epsilon < \frac{1}{2}$. On dit que la base $(\vec{b_1}, \ldots, \vec{b_n})$ est **réduite** si pour tout $i$, $1 \leq i < n$ :

**(i)** $f_i(\vec{b_{i+1}} + \mu\vec{b_i}) \geq f_i(\vec{b_{i+1}})$ quel que soit $\mu \in \mathbb{Z}$.

**(ii)** $f_i(\vec{b_{i+1}}) \geq (1 - \epsilon)f_i(\vec{b_i})$.

Pour construire une base réduite pour $n \geq 2$, on applique l'algorithme suivant.

**Étape 1 :** Soit $(\vec{b_1}, \ldots, \vec{b_n})$ une base de $\mathbb{Z}^n$, par exemple la base canonique, et poser $i = 1$.

**Étape 2 :** Remplacer $\vec{b_{i+1}}$ par $\vec{b_{i+1}} + \mu\vec{b_i}$ tel que $f_i(\vec{b_{i+1}} + \mu\vec{b_i})$ soit minimal.

**Étape 3 :** Si $f_i(\vec{b_{i+1}}) < (1 - \epsilon)f_i(\vec{b_i})$, échanger $\vec{b_i}$ et $\vec{b_{i+1}}$, et remplacer $i$ par $\max(1, i - 1)$ ; sinon remplacer $i$ par $i + 1$.

**Étape 4 :** Si $i < n$, aller à l'étape 2 sinon STOP.

**Question 4.3.** *Montrer que cet algorithme finit par s'arrêter et construit bien une base réduite.*

On admettra que lorsque $K$ est de la forme $\{\vec{x} \in \mathbb{R}^n \mid A\vec{x} \leq \vec{b}\}$ où $A$ est une matrice entière de taille $n \times m$ et $\vec{b} \in \mathbb{Z}^m$, alors on sait implanter cet algorithme par des techniques reliées aux résultats de la partie 1.

**Question 4.4.** *En remarquant que* $f_{i+1}(\vec{b}_{i+1}) = \min\{f_i(\vec{b}_{i+1} + \alpha\vec{b}_i) \mid \alpha \in \mathbb{R}\}$, *montrer que si* $(\vec{b}_1, \ldots, \vec{b}_n)$ *est une base réduite, alors pour tout* $i$, $1 \leq i < n$, $f_{i+1}(\vec{b}_{i+1}) \geq (\frac{1}{2} - \epsilon) f_i(\vec{b}_i)$, *puis que* $\lambda_1(K) \leq f(\vec{b}_1) \leq \lambda_1(K)(\frac{1}{2} - \epsilon)^{1-n}$.

On dit qu'une base $(\vec{c}_1, \ldots, \vec{c}_n)$ de $\mathbb{Z}^n$ est **propre** si, pour tous $i$ et $j$ tels que $j < i$, les fonctions $f_i$ définies à partir de cette base vérifient $f_j(\vec{c}_i + \mu\vec{c}_j) \geq f_j(\vec{c}_i)$ quel que soit $\mu \in \mathbb{Z}$.

**Question 4.5.** *Soit* $(\vec{b}_1, \ldots, \vec{b}_n)$ *est une base de* $\mathbb{Z}^n$. *Montrer que, quels que soient* $\mu_{i,j} \in \mathbb{Z}^n$, $j < i$, *la famille* $(\vec{c}_1, \ldots, \vec{c}_n)$ *définie par* $\vec{c}_i = \vec{b}_i + \sum_{j=1}^{i-1} \mu_{i,j}\vec{b}_j$ *est une base de* $\mathbb{Z}^n$ *telle que les fonctions* $f_i$ *définies à partir de la première base sont les mêmes que celles définies à partir de la seconde. Montrer qu'il existe* $\mu_{i,j}$, $j < i$, *tels que la base* $(\vec{c}_1, \ldots, \vec{c}_n)$ *soit propre et qu'elle est réduite si la base* $(\vec{b}_1, \ldots, \vec{b}_n)$ *l'est.*

Dans la suite, on suppose que $(\vec{b}_1, \ldots, \vec{b}_n)$ est une base réduite de $\mathbb{Z}^n$.

**Question 4.6.** *On suppose d'abord que* $(\vec{b}_1, \ldots, \vec{b}_n)$ *est réduite propre. En s'inspirant de la démonstration de la question 4.4, montrer par une récurrence descendante sur* $j$ *que, pour tout* $j < i$, $f_j(\vec{b}_i) \leq f_i(\vec{b}_i) + \frac{1}{2}\left(f_{i-1}(\vec{b}_{i-1}) + \ldots + f_j(\vec{b}_j)\right)$, *puis* $f_1(\vec{b}_i) \leq f_i(\vec{b}_i)(\frac{1}{2} - \epsilon)^{1-i}$ *et enfin* $\lambda_i(K) \leq f_i(\vec{b}_i)(\frac{1}{2} - \epsilon)^{1-i}$. *Pourquoi cette dernière relation est-elle vraie même si la base n'est pas propre ?*

**Question 4.7.** *Soient* $\vec{x}_i = \sum_{j=1}^{n} x_{i,j}\vec{b}_j$, $1 \leq i \leq n$, $n$ *vecteurs linéairement indépendants tels que* $f(\vec{x}_i) = \lambda_i(K)$. *Montrer que pour tout* $i$, *il existe* $j \leq i \leq k$ *tels que* $x_{j,k} \neq 0$. *En considérant, pour* $i$ *fixé, le plus grand* $k$ *tel que* $x_{j,k} \neq 0$ *et* $j \leq i \leq k$, *montrer que* $\lambda_i(K) \geq \lambda_j(K) \geq f_i(\vec{b}_i)(\frac{1}{2} - \epsilon)^{n-i}$.

On obtient donc un algorithme, basé sur la fonction de jauge d'un corps convexe polyédral $K$, pour l'approximation de ses minima successifs.