Université d'Aix-Marseille

Préparation à l'agrégation : Option C

`http://iml.univ-mrs.fr/~kohel/tch/Agreg/`

Algèbre linéaire

Un reseau $\mathcal{L}$ dans $V = \mathbb{R}^n$ est un sous-groupe de type fini de V qui contient une base pour V. Soit $\{v_1, v_2, \ldots, v_n\}$ une base pour $\mathcal{L}$ (comme groupe abélien), et A la matrice avec les lignes v_i. On définit $\det(\mathcal{L}) = |\det(A)|$.

Exercices

1. Soit A la matrice $\begin{pmatrix} 1 & 0 & 2 \\ 2 & 1 & 1 \\ 3 & 4 & 7 \end{pmatrix}$.

- **a.** Trouver la décomposition LU de A.
- **b.** Calculer le déterminant de A $(= \det(LU))$.
- **c.** Déterminer les solutions à $Ax = [1, 1, -1]^t$ (en résolvant $Ly = [1, 1, -1]^t$ et puis $Ux = y$).

2. Démontrer l'identité $|\det(A)| = \sqrt{\det(AA^t)}$ et interpréter $\det(\mathcal{L})$ comme le volume de :

$$\mathcal{F}(\mathcal{L}) = \left\{ \sum_{i=0}^{n} \lambda_i v_i \mid 0 \leq \lambda_i < 1 \right\}.$$

Indication : considérer le cas où les vecteurs v_i sont orthogonaux, et utiliser Gramm-Schmidt pour réduire à une base rectangulaire (avec le même volume). **Attention** : $\mathcal{F}(\mathcal{L})$ dépend du choix de base $\{v_1, \ldots, v_n\}$.

3. Si $\mathcal{L} \subseteq \mathbb{Z}^n$, montrer que le cardinal du groupe $\mathbb{Z}^n/\mathcal{L}$ est $\det(\mathcal{L})$, et qu'il existe $\det(\mathcal{L})$ éléments dans $\mathbb{Z}^n \cap \mathcal{F}(\mathcal{L})$. Préciser les points pour $\{v_1 = (3, 7), v_2 = (2, 1)\}$, et après un changement de base, pour $\{v_1 = (2, 1), v_2 = (-1, 5)\}$.

4. Déterminer les décompositions $A = LDL^t$ de Cholesky, des matrices

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 8 \end{pmatrix} \text{ et } A = \begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 2 \end{pmatrix}.$$

5. Soit A la matrice

$$\begin{pmatrix} -2 & 4 & 1 & -2 \\ 1 & -1 & 2 & 0 \\ 0 & 11 & 0 & 0 \end{pmatrix}.$$

Déterminer les formes normales de Hermite et Smith de A.

```
def LU(A):
    """
    sage: A = matrix(QQ,[[1,0,2],[2,1,1],[3,4,7]])
    sage: L, U = LU(A)
    sage: L*U == A
    True
    """
    assert A.is_square()
    n = A.nrows()
    X = A.parent()
    L = X(1)
    U = X(0)
    for i in range(n):
        for j in range(n):
            if j < i:
                L[i,j] = U[j,j]^-1*(A[i,j] - sum([ L[i,k]*U[k,j] for k in range(j) ]))
            else:
                U[i,j] = A[i,j] - sum([ L[i,k]*U[k,j] for k in range(i) ])
    return L, U;

def choleskyLDL(A):
    """
    sage: A = matrix(QQ,[[2,1,0],[1,2,1],[0,1,2]])
    sage: L, D = choleskyLDL(A)
    sage: L*D*L.transpose() == A
    True
    """
    assert A.is_symmetric()
    n = A.nrows()
    X = A.parent()
    L = X(1)
    D = X(0)
    for j in range(n):
        D[j,j] = A[j,j] - sum([ L[j,k]^2*D[k,k] for k in range(j) ])
        u = D[j,j]^-1
        for i in range(j+1,n):
            L[i,j] = u*(A[i,j] - sum([ L[i,k]*L[j,k]*D[k,k] for k in range(j) ]))
    return L, D
```

Réseaux euclidiens

Pour les prochaines exercices, on suppose que $K = \mathbb{Q}(\sqrt{-d})$ est un corps de nombres quadratique imaginaire, et $\mathcal{O}_K$ l'anneau des entiers :

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{-d}] \text{ si } d \equiv 1, 2 \bmod 4, \text{ou} \\ \mathbb{Z}[(1+\sqrt{-d})/2] \text{ si } d \equiv 3 \bmod 4, \end{cases}$$

pour un entier positif d sans facteur carré. On note que K admit une norme $\mathrm{N}_K : K \to \mathbb{Q}$

$$\mathrm{N}_K(a + b\sqrt{-d}) = (a + b\sqrt{-d})(a - b\sqrt{-d}) = a^2 + b^2 d,$$

telle que l'image $\mathrm{N}_K(\mathcal{O}_K)$ de sa restriction à $\mathcal{O}_K$ est dans $\mathbb{Z}$. De plus, sous un plongement $K \subseteq \mathbb{C}$, on a $\mathrm{N}_K(\xi) = |\xi|^2$ pour tout $\xi \in K$.

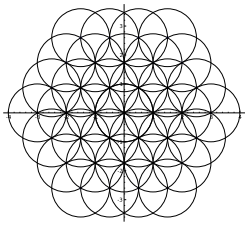
On dit que $\mathcal{O}_K$ est euclidien pour la norme si pour tout $\alpha, \beta \in \mathcal{O}_K$, avec $\beta \neq 0$, il existe $\kappa, \rho \in \mathcal{O}_K$ tel que $\alpha = \kappa\beta + \rho$ avec $\mathrm{N}_K(\rho) < \mathrm{N}_K(\beta)$.

5. Montrer que $\mathcal{O}_K$ étant euclidien pour la norme est équivalent de chaqu'une des conditions suivantes :

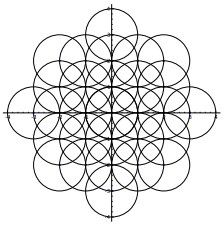
- **a.** Pour tout $\xi \in K$, il existe $\kappa \in \mathcal{O}_K$ tel que $\mathrm{N}_K(\xi - \kappa) < 1$.
- **b.** Pour tout $\xi \in \mathbb{C}$, il existe $\kappa \in \mathcal{O}_K$ tel que $|\xi - \kappa| < 1$.
- **c.** $\mathcal{O}_K + \mathcal{F} = \mathbb{C}$, où $\mathcal{F} = \{y \in \mathbb{C} \mid |y| < 1\}$.

6. Il est bien connu que $\mathcal{O}_K$ est un anneau principal si et seulement si d est dans $\{1, 2, 3, 7, 11, 19, 43, 67, 163\}$. Montrer (graphiquement) que $\mathcal{O}_K$ est euclidien pour la norme si et seulement si $d \in \{1, 2, 3, 7, 11\}$.

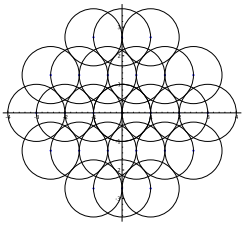
$d = 3$:



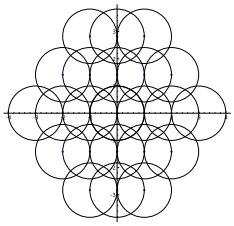
$d = 1$:



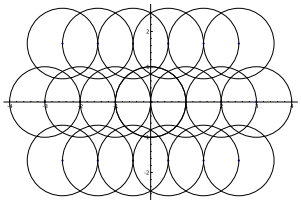
$d = 7$:



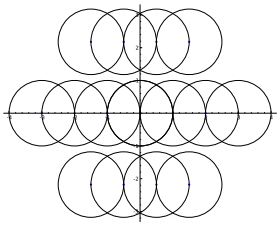
$d = 2$:



$d = 11$:



$d = 19$:



LLL

7. Soit $\alpha \equiv -219 \bmod 2^{12}$. Déterminer un polynôme f cubique avec des petits coefficients tel que $f(\alpha) \equiv 0 \bmod 2^{12}$.

8. Soit $g = x^5 - 5x^4 + 5x^3 - 21x^2 + 9x - 1$ avec racine $\alpha \equiv -107 \bmod 2^8$. Trouver un facteur cubique de g tel que $g(\alpha) \equiv 0 \bmod 2^8$.