# L'algèbre matricielle

Laurent Debize

B1 RPI

Mathématiques appliquées à l'informatique

# Exemple préliminaire

Trois élèves A, B et C ont obtenu sur 2 semestres et dans 4 matières les résultats ci-dessous :

| 1$^{\text{er}}$semestre | Français | Anglais | Maths | SVT |
|---|---|---|---|---|
| Élève A | 8 | 11 | 18 | 11 |
| Élève B | 15 | 11 | 10 | 10 |
| Élève C | 9 | 12 | 11 | 8 |

| 2$^{\text{e}}$semestre | Français | Anglais | Maths | SVT |
|---|---|---|---|---|
| Élève A | 8 | 13 | 16 | 15 |
| Élève B | 19 | 15 | 6 | 8 |
| Élève C | 9 | 10 | 11 | 10 |

On peut résumer ces valeurs dans deux tableaux $S_1$ et $S_2$ que l'on appellera **matrices** :

$$S_1 = \begin{pmatrix} 8 & 11 & 18 & 11 \\ 15 & 11 & 10 & 10 \\ 9 & 12 & 11 & 8 \end{pmatrix} \text{ et } S_2 = \begin{pmatrix} 8 & 13 & 16 & 15 \\ 19 & 15 & 6 & 8 \\ 9 & 10 & 11 & 10 \end{pmatrix}$$

# Total annuel

Pour obtenir le total annuel des points obtenus par chaque élève on ajoute les résultats de chaque semestre :

| Points sur l'année | Français | Anglais | Maths | SVT |
|---|---|---|---|---|
| Élève A | 16 | 24 | 34 | 26 |
| Élève B | 34 | 26 | 16 | 18 |
| Élève C | 18 | 22 | 22 | 18 |

On peut écrire le total annuel des points dans le tableau $S$ :

$$S = \begin{pmatrix} 16 & 24 & 34 & 26 \\ 34 & 26 & 16 & 18 \\ 18 & 22 & 22 & 18 \end{pmatrix}$$

On dit que $S$ est la **matrice somme** des matrices $S_1$ et $S_2$.
On note $S = S_1 + S_2$ et l'on a :

$$S = \begin{pmatrix} 16 & 24 & 34 & 26 \\ 34 & 26 & 16 & 18 \\ 18 & 22 & 22 & 18 \end{pmatrix} =$$

$$\begin{pmatrix} 8 & 11 & 18 & 11 \\ 15 & 11 & 10 & 10 \\ 9 & 12 & 11 & 8 \end{pmatrix} + \begin{pmatrix} 8 & 13 & 16 & 15 \\ 19 & 15 & 6 & 8 \\ 9 & 10 & 11 & 10 \end{pmatrix}$$

# Moyenne annuelle

Pour obtenir la moyenne annuelle obtenue par chaque élève on divise par 2 la somme annuelle :

| Moyenne annuelle | Français | Anglais | Maths | SVT |
|---|---|---|---|---|
| Élève A | 8 | 12 | 17 | 13 |
| Élève B | 17 | 13 | 8 | 9 |
| Élève C | 9 | 11 | 11 | 9 |

On peut écrire la moyenne annuelle dans le tableau $M$.

On note $M = \dfrac{1}{2} \cdot S$ et l'on a :

$$M = \begin{pmatrix} 8 & 12 & 17 & 13 \\ 17 & 13 & 8 & 9 \\ 9 & 11 & 11 & 9 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 16 & 24 & 34 & 26 \\ 34 & 26 & 16 & 18 \\ 18 & 22 & 22 & 18 \end{pmatrix}$$

# Coefficients

Les élèves peuvent s'orienter dans 2 filières d'étude distinctes. Pour définir leur meilleur profil on étudie leurs résultats suivant les coefficients retenus dans chacune des filières. Ces coefficients sont répartis par matières de la façon suivante :

| | Filière 1 | Filière 2 |
|---|---|---|
| Français | 2 | 4 |
| Anglais | 3 | 4 |
| Maths | 7 | 5 |
| SVT | 3 | 2 |

Les coefficients sont indiqués dans la matrice $C = \begin{pmatrix} 2 & 4 \\ 3 & 4 \\ 7 & 5 \\ 3 & 2 \end{pmatrix}$

# Coefficients

On a donc les deux tableaux suivants :

| | Filière 1 | Filière 2 |
|---|---|---|
| Français | 2 | 4 |
| Anglais | 3 | 4 |
| Maths | 7 | 5 |
| SVT | 3 | 2 |

| Moyenne annuelle | Français | Anglais | Maths | SVT |
|---|---|---|---|---|
| Élève A | 8 | 12 | 17 | 13 |
| Élève B | 17 | 13 | 8 | 9 |
| Élève C | 9 | 11 | 11 | 9 |

Quelle est la moyenne générale de chaque élève en fonction de chaque filière ?

| Moyenne générale | Filière 1 | Filière 2 |
|---|---|---|
| Élève A | $8\times2+12\times3+17\times7+13\times3=210$ | $8\times4+12\times4+17\times5+13\times2=191$ |
| Élève B | $17\times2+13\times3+8\times7+9\times3=156$ | $17\times4+13\times4+8\times5+9\times2=178$ |
| Élève C | $9\times2+11\times3+11\times7+9\times3=155$ | $9\times4+11\times4+11\times5+9\times2=153$ |

# Coefficients

Le total des points suivant les filières est indiqué dans le tableau $P$ ci-dessous :

$$P = \begin{pmatrix} 210 & 191 \\ 156 & 178 \\ 155 & 153 \end{pmatrix}$$

On dit que la matrice $P$ est le **produit** de la matrice $M$ par la matrice $C$.
On note $P = M \times C$ et l'on a :

$$\begin{pmatrix} 8 & 12 & 17 & 13 \\ 17 & 13 & 8 & 9 \\ 9 & 11 & 11 & 9 \end{pmatrix} \times \begin{pmatrix} 2 & 4 \\ 3 & 4 \\ 7 & 5 \\ 3 & 2 \end{pmatrix} = \begin{pmatrix} 210 & 191 \\ 156 & 178 \\ 155 & 153 \end{pmatrix}$$

# Définitions

## Définition

On appelle **matrice réelle de dimension** $n \times p$ tout tableau rectangulaire de nombres réels comportant $n$ lignes et $p$ colonnes.
Les matrices à $n$ lignes et $n$ colonnes sont appelées **matrices carrées d'ordre** $n$.

## Exemples

- $A = \begin{pmatrix} 1 & 3 & 5 \\ -2 & 0 & -1 \end{pmatrix}$ est une matrice $2 \times 3$ (lire « matrice 2, 3 »).
- $B = \begin{pmatrix} -1 & 0 \\ 5 & 3 \end{pmatrix}$ est une matrice carrée d'ordre 2.
- $C = \begin{pmatrix} 2 \\ -3 \\ 7 \end{pmatrix}$ est une matrice $3 \times 1$ appelée **matrice colonne**.
- $D = \begin{pmatrix} 5 & 8 & 0 & -1 \end{pmatrix}$ est une matrice $1 \times 4$ appelée **matrice ligne**.

# Généralités – Définitions

## Remarque

Une matrice $A$ de dimension $n \times p$ est encore notée $(a_{ij})$ pour $1 \leqslant i \leqslant n$ et $1 \leqslant j \leqslant p$
où $a_{ij}$ désigne le terme de la ligne $i$ et de la colonne $j$.
On peut ainsi noter la matrice $A$ de dimension $3 \times 3$ :

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

# Exercice 1

Écrire sous forme de tableau la matrice $A = (a_{ij})$, matrice carrée d'ordre 3 définie par : $\begin{cases} a_{ij} = 0 & \text{si} \quad i = j \\ a_{ij} = 2i & \text{si} \quad i < j \\ a_{ij} = i + j & \text{si} \quad i > j \end{cases}$

# Généralités – Définitions

## Définitions

- La matrice $(a_{ij})$ telle que $a_{ij} = 0$ pour tout couple $(i, j)$ est appelée **matrice nulle**. On note la note 0.
- Dans l'ensemble des matrices carrées d'ordre $n$, la matrice $(a_{ij})$ telle que $\begin{cases} a_{ij} = 1 & \text{si} \quad i = j \\ a_{ij} = 0 & \text{si} \quad i \neq j \end{cases}$ est appelée **matrice identité** et est notée $I_n$.

## Exemple

Pour les matrices carrées d'ordre 3, la matrice nulle est :

$$0 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Et la matrice identité est : $I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

# Généralités – Définitions

## Définition - identité des matrices

Soient $A = (a_{ij})$ et $B = (b_{ij})$ deux matrices de dimension $n \times p$.
$A = B$ si et seulement si pour tout couple $(i, j)$ : $a_{ij} = b_{ij}$

## Exemple

Soient $A = \begin{pmatrix} a & -1 \\ 0 & 3 \end{pmatrix}$ et $B = \begin{pmatrix} 3 & -1 \\ b & 3 \end{pmatrix}$
$A = B$ si et seulement si $a = 3$ et $b = 0$.

# Exercice 2

On considère les matrices A et B définies par : $A = \begin{pmatrix} 1 & a-b \\ b-5 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 3 \\ 4b & 1 \end{pmatrix}$.

A quelles conditions avons-nous $A = B$ ?

# Addition des matrices – Produit par un réel

## Définition

Soient $A = (a_{ij})$ et $B = (b_{ij})$ deux matrices de dimension $n \times p$.
**L'addition des matrices** est définie par :

$$A + B = (a_{ij} + b_{ij})$$

**Le produit externe des matrices** est défini, pour $k \in \mathbb{R}$, par :

$$k \cdot A = (k \cdot a_{ij})$$

# Addition des matrices – Produit par un réel

## Méthode : Comment additionner deux matrices ?

- vérifier que les deux matrices ont même taille
- additionner coefficient par coefficient, aux place identiques dans les deux matrices

## Méthode : Comment multiplier une matrice par un réel $k$ ?

- multiplier chaque coefficient de la matrice par $k$

# Addition des matrices – Produit par un réel

## Exemples

Si $A = \begin{pmatrix} 2 & 1 & -7 \\ 3 & -5 & 4 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 & 6 \\ 1 & 1 & -2 \end{pmatrix}$ alors :

$$A + B = \begin{pmatrix} 2 & 2 & -1 \\ 4 & -4 & 2 \end{pmatrix}$$

$$2 \cdot A = \begin{pmatrix} 4 & 2 & -14 \\ 6 & -10 & 8 \end{pmatrix}$$

$$-2 \cdot A + 3 \cdot B = \begin{pmatrix} -4 & 1 & 32 \\ -3 & 13 & -14 \end{pmatrix}$$

# Addition des matrices – Produit par un réel

## Propriétés de la somme

Soient $A$, $B$ et $C$ trois matrices de dimension $n \times p$.

- Commutativité : $A + B = B + A$
- Associativité : $(A + B) + C = A + (B + C)$
- Élément neutre est la matrice nulle 0 : $A + 0 = 0 + A = A$
- Si $A = (a_{ij})$, alors la matrice $(-a_{ij})$ est appelée **matrice opposée** de $A$, et est notée $-A$
  Elle vérifie : $A + (-A) = (-A) + A = 0$
- $(-1) \cdot A = -A$
- $A - B = A + (-B)$

**Notation**

La somme finie de $n$ termes $A + A + \cdots + A$ est notée $n \cdot A$.

# Addition des matrices – Produit par un réel

## Propriétés du produit externe

Soient $a$ et $b$ deux réels, $A$ et $B$ deux matrices de dimension $n \times p$. Alors :

- $a \cdot (b \cdot A) = (ab) \cdot A$
- $(a + b) \cdot A = a \cdot A + b \cdot A$
- $a \cdot (A + B) = a \cdot A + a \cdot B$
- $1 \cdot A = A$

# Exercice 3

Soient A et B les matrices : $A = \begin{pmatrix} 1 & 4 & -2 \\ -5 & 7 & 3 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 3 & 0 \\ -8 & 4 & 1 \end{pmatrix}$

Calculer 2A+3B.

# Préliminaire – « Le produit 1 ligne par 1 colonne »

## Définition

On considère les matrices $A = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \end{pmatrix}$ et $B = \begin{pmatrix} b_1 \\ b_2 \\ \cdots \\ b_n \end{pmatrix}$

Le produit de la matrice $A$ par la matrice $B$, noté $A \times B$ ou $AB$, est une matrice carrée d'ordre 1 définie par :

$$AB = \begin{pmatrix} a_1 b_1 + a_2 b_2 + \cdots + a_n b_n \end{pmatrix}$$

## Exemple

Si $A = \begin{pmatrix} 1 & -3 & 5 & 4 \end{pmatrix}$ et $B = \begin{pmatrix} 2 \\ 1 \\ 0 \\ -1 \end{pmatrix}$ alors

$AB = \begin{pmatrix} 1 \times 2 + (-3) \times 1 + 5 \times 0 + 4 \times (-1) \end{pmatrix} = \begin{pmatrix} -5 \end{pmatrix}$

# Produit des matrices

## Définition

Soient $A = (a_{ij})$ une matrice $n \times p$ et $B = (b_{ij})$ une matrice $p \times q$. On appelle **produit de la matrice A par la matrice B**, et l'on note $A \times B$ ou $AB$, la matrice $C = (c_{ij})$ de dimension $n \times q$ définie par :

$$c_{ij} = \sum_{k=1}^{p} a_{ik} b_{kj} = a_{i1} b_{1j} + a_{i2} b_{2j} + \cdots + a_{ip} b_{pj}$$

# Produit des matrices

## Méthode : Comment multiplier deux matrices entre elles ?

Soient $A$ et $B$ deux matrices. Pour effectuer le produit $A \times B$ :

- **vérifier que le nombre de colonnes de $A$ est égal au nombre de lignes de $B$**
- placer la matrice $A$ en bas à gauche et la matrice $B$ en haut à droite
- pour calculer le coefficient ligne $i$ colonne $j$ dans la matrice $A \times B$ :
  - isoler la ligne $i$ dans $A$
  - isoler la colonne $j$ dans $B$
  - faire les produits des termes deux à deux, l'un dans la ligne de $A$, l'autre dans la colonne de $B$
  - faire la somme des résultats obtenus
  - placer ce résultat à l'intersection de la ligne de $A$ et de la colonne de $B$
- recommencer pour tous les coefficients

# Produit des matrices

## Méthode : Comment multiplier deux matrices entre elles ?

Prenons une matrice $A$ de dimension $3 \times 4$ et une matrice $B$ de dimension $4 \times 5$.
Premièrement nous remarquons que $A$ a 4 colonnes et $B$ a 4 lignes, donc le produit est possible.
Ensuite nous plaçons les matrices et calculons par exemple le coefficient ligne 2 colonne 3 :

$$\begin{array}{cc} & \begin{pmatrix} \cdot & \cdot & b_{13} & \cdot & \cdot \\ \cdot & \cdot & b_{23} & \cdot & \cdot \\ \cdot & \cdot & b_{33} & \cdot & \cdot \\ \cdot & \cdot & b_{43} & \cdot & \cdot \end{pmatrix} \\ \begin{pmatrix} \cdot & \cdot & \cdot & \cdot \\ a_{21} & a_{22} & a_{23} & a_{24} \\ \cdot & \cdot & \cdot & \cdot \end{pmatrix} & \begin{pmatrix} \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & c_{23} & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix} \end{array}$$

# Produit des matrices

## Exemple

Soient $A = \begin{pmatrix} 2 & 1 \\ 3 & -5 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \\ -2 & 1 \end{pmatrix}$.

Calculons $C = AB$ et $D = BA$ :

$$C = \begin{pmatrix} 2 & 1 \\ 3 & -5 \end{pmatrix} \times \begin{pmatrix} 0 & 1 \\ -2 & 1 \end{pmatrix} = \begin{pmatrix} -2 & 3 \\ 10 & -2 \end{pmatrix}$$

$$D = \begin{pmatrix} 0 & 1 \\ -2 & 1 \end{pmatrix} \times \begin{pmatrix} 2 & 1 \\ 3 & -5 \end{pmatrix} = \begin{pmatrix} 3 & -5 \\ -1 & -7 \end{pmatrix}$$

# Exercice 4

Soient A et B les matrices : $A = \begin{pmatrix} 1 & 4 & -2 \\ 2 & 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 3 & 0 \\ 4 & 1 \\ 0 & -1 \end{pmatrix}$

Calculer les matrices AB et BA.

# Produit des matrices

## Autre exemple

Soient $A = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 2 & 1 & -7 \\ 3 & -5 & 4 \end{pmatrix}$ et $C = \begin{pmatrix} 0 & 1 \\ -1 & 1 \\ 2 & 3 \end{pmatrix}$.

$A$ est une matrice $2 \times 2$, $B$ est une matrice $2 \times 3$ et $C$ est une matrice $3 \times 2$.

Quelle est la taille de la matrice $AB$ ? $2 \times 3$
Quelle est la taille de la matrice $BA$ ? produit non défini
Quelle est la taille de la matrice $BC$ ? $2 \times 2$
Quelle est la taille de la matrice $CB$ ? $3 \times 3$
Quelle est la taille de la matrice $AC$ ? produit non défini
Quelle est la taille de la matrice $CA$ ? $3 \times 2$

# Produit des matrices

## Remarques

- On a $AB \neq BA$ : la multiplication des matrices n'est pas commutative.
- Les matrices $AB$ et $BA$ peuvent avoir des tailles différentes.
- Le produit $AB$ peut exister sans que le produit $BA$ n'existe.
- Le produit d'une matrice $n \times p$ par une matrice $p \times q$ donne une matrice $n \times q$ :
  **le nombre de colonnes de la matrice $A$ doit être égal au nombre de lignes de la matrice $B$.**
- Le produit de 2 matrices carrées d'ordre $n$ est une matrice carrée d'ordre $n$.
- Si $A$ est une matrice carrée d'ordre $n$ alors : $AI_n = I_nA = A$ et en particulier $I_n \times I_n = I_n$.

# Exercice 5

Soient A et B les matrices : $A = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 3 & 0 \\ 4 & 1 \\ 0 & -1 \end{pmatrix}$

Est-ce que les produits AB et BA existent ?
Si oui, effectuer le calcul.

# Produit des matrices

## Propriété : associativité

Soient $A$ une matrice $n \times p$, $B$ une matrice $p \times q$ et $C$ une matrice $q \times r$. Alors :

$$(AB)C = A(BC)$$

On dit que la multiplication des matrices est associative et le produit $A(BC)$ est noté $ABC$.

# Exercice 6

Soient A, B et C les matrices : $A = \begin{pmatrix} -1 & 1 & 4 \\ 0 & 3 & 2 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 1 \\ 0 & -2 \\ 4 & 3 \end{pmatrix}$ et $C = \begin{pmatrix} 2 & -3 \\ 4 & 1 \end{pmatrix}$

1. Quelle est la nature des matrices AB et BC ?
2. Déterminer de deux façons différentes le produit ABC.

# Produit des matrices

## Propriétés

Soient $A$, $B$ et $C$ trois matrices et $k$ un réel. Lorsque les produits sont définis :

- $A(B+C) = AB + AC$
- $(A+B)C = AC + BC$
- $(k.A)B = A(k.B) = k.(AB)$

## Exemple

Pour $A$, $B$ et $I_n$ matrices carrées d'ordre $n$ :

$$\begin{aligned}(2A - 3I_n)(3B + 2I_n) &= 2A(3B + 2I_n) - 3I_n(3B + 2I_n)\\ &= 6AB + 4AI_n - 9I_nB - 6I_nI_n\\ &= 6AB + 4A - 9B - 6I_n\end{aligned}$$

# Produit des matrices

## Remarque

L'égalité $AB = 0$ n'entraîne pas nécessairement $A = 0$ ou $B = 0$.
Par exemple si $A = \begin{pmatrix} 3 & 1 \\ 3 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} -1 & 1 \\ 3 & -3 \end{pmatrix}$, on a bien $AB = 0$, alors que $A \neq 0$ et $B \neq 0$.

# Puissance d'une matrice

Le produit de 2 matrices carrées d'ordre $n$ étant une matrice carrée d'ordre $n$, l'associativité du produit permet de définir la puissance d'une matrice.

## Définition

Soit $A$ une matrice carrée d'ordre $n$. On appelle puissance de la matrice $A$ et l'on note $A^n$ la matrice définie par :

$$\begin{cases} A^1 = A \\ A^{n+1} = A \times A^n = A^n \times A \qquad \text{si } n \geqslant 1 \end{cases}$$

# Puissance d'une matrice

## Exemple

Soit $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Alors :

$A^1 = A$

$A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$

$A^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

$A^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

# Puissance d'une matrice

## Conséquence : identités remarquables pour les matrices carrées

- $(A+B)(A-B) = A^2 - AB + BA - B^2$
- $(A+B)^2 = A^2 + AB + BA + B^2$
- $(A-B)^2 = A^2 - AB - BA + B^2$

## Exemples : développement d'expressions matricielles

- $(A+I_n)^2 = A^2 + AI_n + I_nA + I_n^2 = A^2 + 2A + I_n$
- $(A-I_n)^2 = A^2 - AI_n - I_nA + I_n^2 = A^2 - 2A + I_n$
- $(2A+3B)^2 = 4A^2 + 6AB + 6BA + 9B^2$
- $(A+2I_n)(A-3I_n) = A^2 - 3AI_n + 2I_nA - 6I_n^2 = A^2 - A - 6I_n$

# Puissance d'une matrice

## Remarque

Pour les factorisations on notera, par exemple, que $A^2 - 2A = A \cdot (A - 2 \cdot I_n)$ et non $A^2 - 2 \cdot A = A \cdot (A - 2)$ car l'expression ≪ A - 2 ≫n'a pas de sens.

# Exercice 7

Soit A la matrice : $A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$

1. Déterminer les matrices $A^2$ et $A^3$.
2. En déduire la matrice $A^{2003}$.

# Le chiffre de Hill

On donne la matrice $A = \begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix}$.

Le but de cet exercice est de décrire un procédé de codage d'un *mot* de deux lettres (partie A) à l'aide de la matrice $A$ puis de détailler une méthode de décodage de ce *mot* (partie C) en s'appuyant sur des résultats mathématiques établis dans la partie B.

Un *mot* de deux lettres est assimilé à une matrice colonne $X = \begin{pmatrix} x \\ y \end{pmatrix}$, où $x$ est le nombre correspondant à la première lettre du *mot*, et $y$ le nombre correspondant à la deuxième lettre du *mot*, selon le tableau de correspondance ci-après :

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |

| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Ainsi par exemple, le *mot* « SI » est assimilé à la matrice $X = \begin{pmatrix} 18 \\ 8 \end{pmatrix}$

# Le chiffre de Hill

## Partie A : chiffrement

Pour coder le *mot* assimilé à la matrice $X = \begin{pmatrix} x \\ y \end{pmatrix}$ on calcule la matrice $U = \begin{pmatrix} u \\ v \end{pmatrix}$ telle que $AX = U$, puis la matrice $C = \begin{pmatrix} c \\ d \end{pmatrix}$, où les nombres $c$ et $d$ sont les restes respectifs de la division euclidienne par 26 des nombres $u$ et $v$.

Le *mot* codé est alors le *mot* de deux lettres assimilé à la matrice $C = \begin{pmatrix} c \\ d \end{pmatrix}$, selon le tableau de correspondance précédent, c'est-à -dire que $c$ et $d$ sont les deux lettres du *mot* codé.

Déterminer le *mot* codé correspondant au *mot* « SI ».

# Le chiffre de Hill

## Partie B : deux résultats mathématiques

On considère les matrices $B = \begin{pmatrix} 2 & -1 \\ -3 & 4 \end{pmatrix}$ et $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

1. Justifier la congruence : $5 \times 21 \equiv 1$ modulo 26.
2. a. Calculer le produit matriciel $B \times A$, puis exprimer ce produit en fonction de la matrice $I$.

   b. Soit $U = \begin{pmatrix} u \\ v \end{pmatrix}$ et $X = \begin{pmatrix} x \\ y \end{pmatrix}$ deux matrices quelconques à deux lignes et une colonne.
   Justifier que si $AX = U$, alors $5X = BU$.

# Le chiffre de Hill

## Partie C : déchiffrement

On souhaite décoder le *mot* ≪ BE ≫ associé à la matrice $C = \begin{pmatrix} 1 \\ 4 \end{pmatrix}$.

Si $X = \begin{pmatrix} x \\ y \end{pmatrix}$ est la matrice associée au *mot* de départ ; la matrice $U = \begin{pmatrix} u \\ v \end{pmatrix}$ définie par l'égalité $AX = U$ a ses coefficients qui vérifient : $\left\{ \begin{array}{lcl} u & \equiv & 1 \text{ modulo } 26 \\ v & \equiv & 4 \text{ modulo } 26 \end{array} \right.$ d'après la **partie A**.

1. En utilisant la question **B. 2.** démontrer que $\left\{ \begin{array}{lcl} 5x & = & 2u - v \\ 5y & = & -3u + 4v \end{array} \right.$.
   En déduire que $\left\{ \begin{array}{lcl} 5x & \equiv & -2 \text{ modulo } 26 \\ 5y & \equiv & 13 \text{ modulo } 26 \end{array} \right.$.
2. En utilisant la question **B. 1** démontrer que $\left\{ \begin{array}{lcl} x & \equiv & 10 \text{ modulo } 26 \\ y & \equiv & 13 \text{ modulo } 26 \end{array} \right.$. puis décoder le *mot* ≪ BE ≫.