Lemma 0.1: Identité de bezout

Soient a et b deux entiers relatifs non nuls. a et b sont premiers entre eux si et seulement si il existe deux entiers u et v tels que a·u + b·v = 1:

$a \wedge b = 1 \Leftrightarrow \exists (u, v) \in Z^2 \quad au + bv = 1$

Autrement dit deux entiers sont premiers entre eux signifie que leur PDCD=1
Soit PGCD(a,b)=1

Exemple de calcul à la main(Prenons deux entiers 23 et 8):
Calcul de leur PGCD puis des coefficients de bézout(Algorithme d'euclide étendu)
Calcul du PGCD:
23=8x2+7
8=7x1+1
1=1x1+0

Soit PGCD(23,8) le dernier reste non nul de la division euclidienne de 23 par 8 on en déduit donc que PGCD(23,8)=1

Appliquons donc désormais le théorème définie plus haut étant donné que PGCD(23,8)=1 $\Leftrightarrow \exists (u, v) \in Z^2 \quad au + bv = 1$

Calculons donc ces coefficients(u,v) par la méthode de l'algorithme d'euclide étendu tel que 23u+8v=1

8=7x1+1
23=8x2+7 (On remplace 8 par l'égalité au-dessus!)
23=(7x1+1)x2+7
23=(7+1)x2+7
1+23=8x2+7+1 (On ajoute 1 de chaque côté de l'égalité afin de factoriser les 8 à droite!)
1=-1x23+8x2+8
1=-1x23+8x3

(Définissons désormais l'algorithme avant la programmation en JAVA!)

r-2 := b; r-1 := a; u-2 := 0; u-1 := 1; v-2 := 1; v-1 := a div b
k := -1
Tant que rk > 0 faire
Début
k := k + 1
rk-2 = qk·rk-1 + rk (avec qk = rk-2 div rk-1 et rk = rk-2 mod rk-1)
uk := uk-2 - qk·uk-1

vk := vk-2 - qk·vk-1
On a la relation: rk = a·uk + b·vk
Fin
u = uk-1·qk
v = vk-1·qk

(Voici désormais le programme en JAVA permettant de calculer les coefficients de bézout!)

```
/**
* @param m le premier entier
* @param n le second entier
* @retourne un tableau d'entiers g[0] est le GCD de m et n.
* g[1] et g[2] sont deux entiers tel que g[0] = m g[1] + n g[2].
*/
public static int[] extgcd(int m, int n)

//Deux tableaux ma et na sont deux tableau de 3 entiers tel que:
// ma[0] = m ma[1] + n ma[2] and na[0] = m na[1] + n na[2]
int[] ma = new int[] m, 1, 0;
int[] na = new int[] n, 0, 1;
int[] ta; // Temporary variable
int i; // Loop index
int q; // Quotient
int r; // Rest

// Echange ma et na si m < n
if (m < n)
ta = na; na = ma; ma = ta;


Il peut être possible que m >= n
while (na[0] > 0)
q = ma[0] / na[0]; // Quotient
for (i = 0; i < 3; i++)
r = ma[i] - q * na[i];
ma[i] = na[i];
na[i] = r;


return ma;
```

Ceci est une référence au lemme de Bezout 0.1

1 Theorem and lemma examples with title

Theorem 1.1: Pythagoras' theorem

In a right triangle, the square of the hypotenuse is equal to the sum of the squares of the catheti.

$$a^2 + b^2 = c^2$$

In mathematics, the Pythagorean theorem, also known as Pythagoras' theorem (see theorem 1.1), is a relation in Euclidean geometry among the three sides of a right triangle.

2 Theorem and proof examples without title

Theorem 2.1

There exist two irrational numbers x, y such that x^y is rational.

Proof 2.1

If $x = y = \sqrt{2}$ is an example, then we are done; otherwise $\sqrt{2}^{\sqrt{2}}$ is irrational, in which case taking $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$ gives us:

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\sqrt{2}} = \sqrt{2}^2 = 2.$$

$\square$

3 Matrices

Voici un exemple de matrice!

$$\begin{Vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{Vmatrix}$$

Prenons les matrices suivantes A, B, C:

A)

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$$

B)

$$\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$$

C)

$$\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

DÉFINITIONS

-A est une matrice de taille (3,3)
-Le terme de position (1,3) est égal à 3
-Le terme de position (3,3) est égal à 9
-A est une matrice carrée dont le nombre de lignes est égal au nombre de colonnes.
-B est une matrice ligne dont le nombre de lignes est égal à 1
-C est une matrice colonne dont le nombre de colonnes est égal à 1

REMARQUE

Pour une matrice carrée, on appelle diagonale principale, la diagonale qui relie le coin situé en haut à gauche au coin situé en bas à droite. Sur l'exemple ci-dessous, les coefficients de la diagonale principale sont marqués en rouge :

A=$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 7 \end{pmatrix}$

DÉFINITIONS

-La matrice nulle de dimension np est la matrice de dimension np dont tous les coefficients sont nuls
-Une matrice diagonale est une matrice carrée dont tout les coefficients situés en dehors de la diagonale principale sont nuls.
-La matrice unité de dimension n est la matrice carrée de dimension n qui contient des 1 sur la diagonale principale et des 0 ailleurs:

A=$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$

EXEMPLES

La matrice A=$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

est une matrice diagonale d'ordre 4. La matrice unité d'ordre 2 est I_2 =

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} I$

2. OPÉRATIONS SUR LES MATRICES

DÉFINITION (SOMME DE MATRICES)

-Soient A et B deux matrices de même dimension.
-La somme A+B des matrices A et B s'obtient en ajoutant les coefficients de A aux coefficients de B situés à la même position.

EXEMPLE

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

et B=$\begin{pmatrix} -1 & 1 & 1 \\ -2 & 2 & 0 \end{pmatrix}$

Alors : A+B=$\begin{pmatrix} 2-1 & -2+1 & 1+1 \\ -1-2 & 1+2 & 0+0 \end{pmatrix}$=$\begin{pmatrix} 1 & -1 & 2 \\ -3 & 3 & 0 \end{pmatrix}$

REMARQUES

On ne peut additionner deux matrices que si elles ont les même dimensions, c'est à dire le même nombre de lignes et le même nombre de colonnes. On définit de manière analogue la différence de deux matrices.

DÉFINITION (PRODUIT D'UNE MATRICE PAR UN NOMBRE RÉEL)

-Soient A une matrice et k un nombre réel..
-Le produit kA est la matrice obtenue en multipliant chacun des coefficients de A par k.

EXEMPLE

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

alors :

2A=$\begin{pmatrix} 2\times 1 & 2\times 1 & 2\times 0 \\ 2\times 2 & 2\times 0 & 2\times 0 \end{pmatrix}$=$\begin{pmatrix} 2 & 2 & 0 \\ 4 & 0 & 0 \end{pmatrix}$

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

PROPRIÉTÉS

-Soient A, B et C trois matrices de mêmes dimensions k et k' deux réels.

A+B = B+A (commutativité de l'addition)
(A+B)+C = A+(B+C)(associativité de l'addition)

k(A+B) = kA+kB
(k+k')A = kA+k'A

k(k'A) = (kk')A

DÉFINITION (PRODUIT D'UNE MATRICE LIGNE PAR UNE MATRICE COLONNE)

Soient A$=(a_1 a_2 \cdots a_n)$**une matrice ligne (1,n) et B**$=\begin{pmatrix} b_1 \\ b_2 \\ \cdots \\ b_n \end{pmatrix}$ **=une matrice colonne (n,1).**

Le produit de A par B est le nombre réel:$A\times B = (a_1 a_2 \cdots a_n)\times \begin{pmatrix} b_1 \\ b_2 \\ \cdots \\ b_n \end{pmatrix} =$

$a_1 b_1 + a_2 b_2 + \cdots + a_n b_n$

REMARQUE

Les deux matrices A et B doivent avoir le même nombre n de coefficients. Pour cette formule, la matrice ligne doit être impérativement en premier!

EXEMPLE

Si A=(1234) $A = (1234) et B = \begin{pmatrix} 5 \\ 6 \\ 7 \\ 8 \end{pmatrix}$

A$\times B = 1 \times 5 + 2 \times 6 + 3 \times 7 + 4 \times 8 = 5 + 12 + 21 + 32 = 70$

DÉFINITION (PRODUIT DE DEUX MATRICES)

Soient A$=(a_{ij})$ **une matrice (n,p) et B**$=(b_{ij})$ **une matrice (p,q).**
Le produit de A par B est la matrice C$=(c_{ij})$ **à n lignes et q colonnes dont le coefficient situé à la i-ième ligne et la j-ième colonne est obtenu en multipliant la i-ième ligne de A par la j-ième colonne de B. C'est à dire que pour tout:**
$1 \leq i \leq n$ **et tout** $1 \leq j \leq q$:

$c_{ij} = a_{i1} b_{1j} + a_{i2} b_{2j} + \cdots + a_{ip} b_{pj}$

REMARQUE

Faites bien attention aux dimensions des matrices: Le nombre de colonnes de la première matrice doit être égal au nombre de lignes de la seconde pour que le calcul soit possible.
Par exemple, le produit d'une matrice 2×3 **par une matrice** 3×4 **est possible et donnera une matrice** 2×4.
Par contre, le produit d'une matrice 2$\times3$ **par une matrice** $2\times$**3 n'est pas possible.**

EXEMPLE

Calculons le produit **C=A**$\times B avec : A = \begin{pmatrix} 2 & 4 \\ 1 & 0 \end{pmatrix} et B = \begin{pmatrix} -1 & 0 & 2 \\ -2 & 1 & 0 \end{pmatrix}$

Ce calcul est possible car le nombre de colonnes de A est égal au nombre de lignes de B. Le résultat C sera une matrice 2$\times 3 (2\times 2 par 2\times 3 \to 2\times 32323)$

$Notons C = \begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \end{pmatrix}$

Pour calculer c$_{11}$ **on multiplie la première ligne de A et la première colonne de B:**

C$=\begin{pmatrix} 2 & 4 \\ 1 & 0 \end{pmatrix} \times \begin{pmatrix} -1 & 0 & 2 \\ -2 & 1 & 0 \end{pmatrix}$

on a donc c$_{11} = 2\times(-1) + 4\times(-2) = -2-8 = -10$

C$=\begin{pmatrix} 2 & 4 \\ 1 & 0 \end{pmatrix} \times \begin{pmatrix} -1 & 0 & 2 \\ -2 & 1 & 0 \end{pmatrix} = \begin{pmatrix} -10 & \cdots & \cdots \\ \cdots & \cdots & \cdots \end{pmatrix}$

Pour calculer c$_{12}$ **on multiplie la première ligne de A et la seconde colonne de B:**$C = \begin{pmatrix} 2 & 4 \\ 1 & 0 \end{pmatrix} \times \begin{pmatrix} -1 & 0 & 2 \\ -2 & 1 & 0 \end{pmatrix}$

on a donc c$_{12} = 2\times 0 + 4\times 1 = 0+4 = 4$

C$=\begin{pmatrix} 2 & 4 \\ 1 & 0 \end{pmatrix} \times \begin{pmatrix} -1 & 0 & 2 \\ -2 & 1 & 0 \end{pmatrix} = \begin{pmatrix} -10 & 4 & \cdots \\ \cdots & \cdots & \cdots \end{pmatrix}$

Et ainsi de suite... Au final on trouve: C$=\begin{pmatrix} 2 & 4 \\ 1 & 0 \end{pmatrix} \times \begin{pmatrix} -1 & 0 & 2 \\ -2 & 1 & 0 \end{pmatrix} = \begin{pmatrix} -10 & 4 & 4 \\ -1 & 0 & 2 \end{pmatrix}$

Dans ce qui suit, on s'intéressera principalement à des matrices carrées.

PROPRIÉTÉ

Soit A, B, et C, trois matrices carrées de même dimension.

A$\times (B+C) = A\times B + A\times C$ **(distributivité à gauche)**
$(A+B)\times C = A\times C + B\times C$ **(distributivité à droite)**
$A\times(B\times C) = (A\times B)\times C$ **(associativité de la multiplication)**
Par contre en général : $A\times B \neq B\times A$ **: la multiplication n'est pas commutative.**

EXEMPLE

Soit A$=\begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}$

et

B$=\begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$

A $\times B = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$

tandis que :

B $\times A = \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}$

Par conséquent A$\times B \neq B\times A$

DÉFINITION (PUISSANCE D'UNE MATRICE)

Soit A une matrice carrée et n un entier naturel.
On note $\mathbf{A}^n$**la matrice:**

$\mathbf{A}^n = A \times A \times \cdots . \times A(nfacteurs)$

REMARQUE

Par convention, on considèrera que $\mathbf{A}^0$**est la matrice unité de même taille que A**

DÉFINITION (MATRICE INVERSIBLE)

Une matrice carrée A de dimension n est inversible si et seulement si il existe une matrice B telle que

$\mathbf{A}\times B = B \times A = I_n$

où $\mathbf{I}_n$**est la matrice unité de dimension n**

La matrice B est appelée matrice inverse de A et notée $\mathbf{A}^{-1}$

3. RÉSOLUTION DE SYSTÈMES D'ÉQUATIONS

Soit le système: $(S) \begin{cases} ax + by = s \\ cx + dy = t \end{cases} (S)$

d'inconnues x et y.

Si l'on pose A=$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$**, X=**$\begin{pmatrix} x \\ y \end{pmatrix}$ **et B=**$\begin{pmatrix} s \\ t \end{pmatrix}$ **, le système** (S) **peut s'écrire:** $A \times X = B.$

Le théorème ci-dessous permet alors de résoudre ce système.

THÉORÈME

Soit A une matrice carrée.
Si A est inversible, le système $\mathbf{A}\times X = B$ **admet une solution unique donnée par:**

$\mathbf{X}=\mathbf{A}^{-1} \times B$

EXEMPLE

On cherche à résoudre le système : $(S) \begin{cases} 3x + 4y = 1 \\ 5x + 7y = 2 \end{cases} (S)$

Pour cela on pose : A=$\begin{pmatrix} 3 & 4 \\ 5 & 7 \end{pmatrix}$ **, X=**$\begin{pmatrix} x \\ y \end{pmatrix}$ **et B=**$\begin{pmatrix} 1 \\ 2 \end{pmatrix}$

. L'écriture matricielle est alors $\mathbf{A}\times X = B$

A la calculatrice, on trouve que A est inversible d'inverse $\mathbf{A}^{-1} = \begin{pmatrix} 7 & -4 \\ -5 & 3 \end{pmatrix}.$

La solution du système est donné par:$X = A^{-1}\times B = \begin{pmatrix} 7 & -4 \\ -5 & 3 \end{pmatrix}\times\begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} -1 \\ 1 \end{pmatrix}$

C'est à dire x=1 et y=1

4 Graph

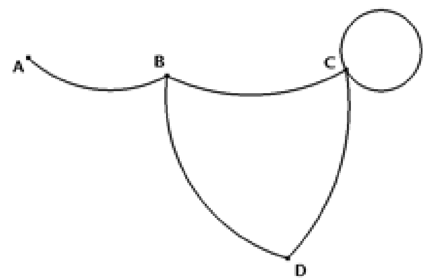
1. VOCABULAIRE

DÉFINITION

Un graphe est composé de sommets et d'arêtes (ou arcs) reliant certains de ces sommets.

EXEMPLE

Le diagramme ci-dessous représente un graphe comportant 4 sommets et 5 arêtes.



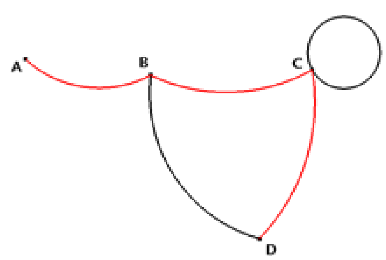
DÉFINITIONS

L'ordre d'un graphe est le nombre de sommets de ce graphe. Le degré d'un sommet est le nombre d'arêtes dont ce sommet est une extrémité. Deux sommets reliés par une arête sont adjacents. EXEMPLE

Le graphe représenté ci-dessus est d'ordre 4. Le degré du sommet B est 3. Celui de C est 4 (la boucle compte 2 fois). A et B sont adjacents. A et D ne le sont pas. DÉFINITIONS

Une chaîne (ou un chemin) est une suite de sommets telle que chaque sommet est relié au suivant par une arête. La longueur d'une chaîne est le nombre d'arêtes composant cette chaîne.

EXEMPLE



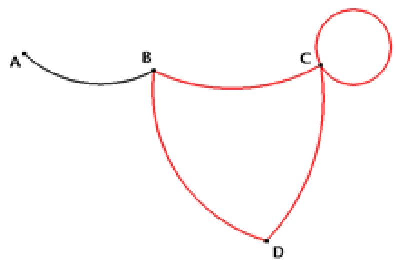
(A; B; C; D) est une chaîne de longueur 3.

DÉFINITION

Un cycle est une chaîne fermée (c'est à dire dont l'origine et

l'extrémité sont identiques) dont toutes les arêtes sont distinctes.

EXEMPLE



(B; C; C; D; B) est un cycle.

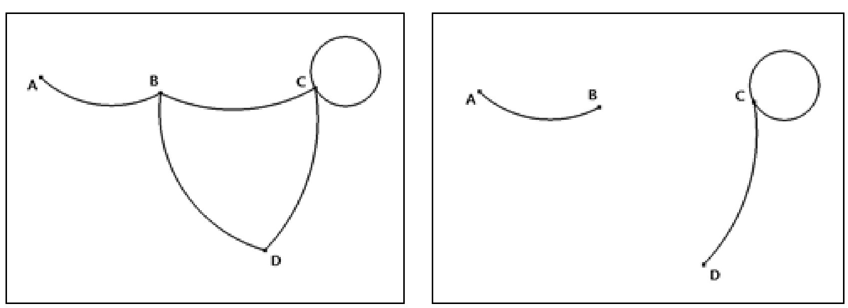
DÉFINITION

On dit qu'un graphe est connexe si deux sommets quelconques peuvent être reliés par une chaîne.

REMARQUE

Intuitivement, cela signifie que le graphe comporte un seul "morceau"

EXEMPLE

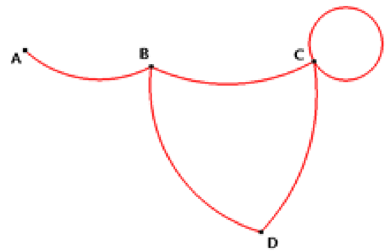


Graphe connexe *Graphe non connexe*

2. CHAÎNES ET CYCLES EULÉRIENS

DÉFINITION

Une chaîne eulérienne est une chaîne qui contient une fois et une seule chacune des arêtes du graphe. Si cette chaîne est un cycle, on parle de cycle eulérien.



EXEMPLE

(A; B; C; C; D; B) est une chaîne eulérienne. Ce graphe ne contient aucun cycle eulérien.

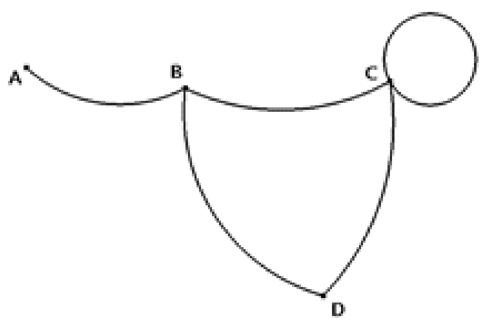
REMARQUE

Un graphe connexe contient une chaîne eulérienne si et seulement si on peut le tracer "sans lever le crayon". Le théorème d'Euler (ci-dessous) permet de déterminer facilement ce type de graphe. On ne peut jamais tracer un graphe non connexe sans lever le crayon !

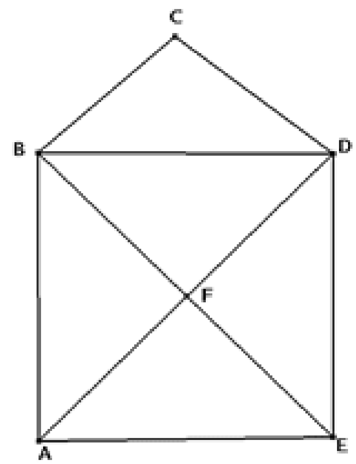
THÉORÈME

Théorème d'Euler. Un graphe connexe contient une chaîne eulérienne si et seulement si il possède 0 ou 2 sommets de degré impair. Un graphe connexe contient un cycle eulérien si et seulement si il ne possède aucun sommet de degré impair (autrement dit tous ses sommets sont de degré pair)

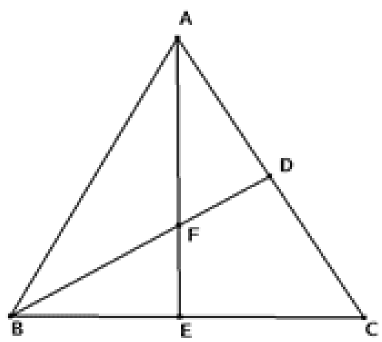
EXEMPLE



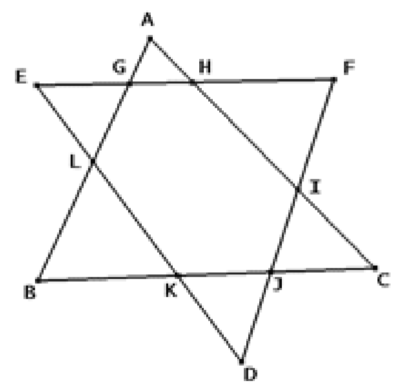
Exemple 1



Exemple 2



Exemple 3



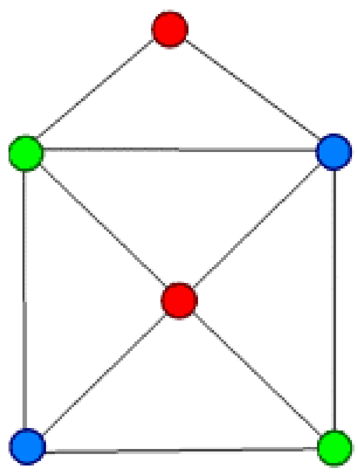
Exemple 4

Dans l'exemple 1, il y a deux sommets de degré impair (A:1 et B:3). Le graphe contient une chaîne eulérienne, par exemple (A; B; C; C; D; B) mais pas de cycle eulérien. Dans l'exemple 2, il y a deux sommets de degré impair (A:3 et E:3). Le graphe contient une chaîne eulérienne, par exemple (A; F; D; B; F; E; D; C; B; A; E) mais pas de cycle eulérien. Dans l'exemple 3, il y a 4 sommets de degré impair (A:3, B:3, D:3 et E:3). Le graphe ne contient pas de chaîne eulérienne. Dans l'exemple 4, tous les sommets sont de degré pair . Le graphe contient un cycle eulérien, par exemple: (G; A; H; F; I; C; J; D; K; B; L; E; G; H; I; J; K; L; G). 3. COLORATION D'UN GRAPHE

DÉFINITION

Colorier un graphe c'est associer à tout sommet une couleur telle que deux sommets adjacents n'aient pas la même couleur. Le plus petit nombre de couleurs nécessaire pour colorier un graphe s'appelle le nombre chromatique du graphe.

EXEMPLE



Le graphe ci-dessus a été colorié a l'aide de 3 couleurs différentes. Il n'est pas possible de le colorier avec seulement 2 couleurs. Le nombre chromatique du graphe est donc 3.

THÉORÈME

Le nombre chromatique d'un graphe est inférieur ou égal à $d_{max}+1d$

où $d_{max}d$

est le plus grand degré des sommets.

EXEMPLE

Dans l'exemple précédent le plus grand degré est 4. Le nombre chromatique du graphe est donc inférieur ou égal à 5 (On a vu que c'était 3).