MATH-F307 - Mathématiques Discrètes
Laurent La Fuente
Notes de cours

André Madeira Cortes

Nikita Marchant

Table des matières

1 Théorie des Graphes

1.1 Définitions

Définition 1
Un graphe Γ est un triplet (V, E, γ) où V est un ensemble fini dont les éléments sont appelés sommets, E est un ensemble fini dont les éléments sont appelés arêtes, γ est une fonction $\gamma : E \to Paires(V)$. On notera le plus souvent $\Gamma = (V, E)$ en omettant la fonction γ.

Soit $\gamma(e) = \{x, y\}$ pour $e \in E, x, y \in V$:

1. *On dit que x et y sont adjacents.*
2. *On dit que e est incidente à x et y.*

Définition 2
Soit $\Gamma = (V, E, \gamma)$ un graphe.

1. *$\gamma(e) = \{x, x\}$ pour $e \in E, x \in V$ est appelé un lacet.*
2. *Si au moins 2 arêtes sont incidentes à 2 mêmes sommets, on les appelle arêtes multiples.*
3. *Un graphe est simple s'il n'a ni lacet, ni arêtes multiples. Dans ce cas, on omet la fonction γ,on note $\Gamma = (V, E)$ et E est identifié un sous-ensemble de Paires(V).*

Définition 3
Soit $\Gamma = (V, E)$ un graphe. Le degré d'un sommet $v \in V$ est le nombre d'arêtes incidentes à v, les lacets comptant pour 2 arêtes. On note le degré de v par deg(V).

Exemple
Dans la figure suivante, nous avons 2 sommets de degré 4 et 6 sommets de degré 1.

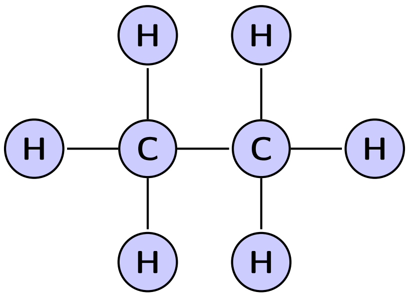


FIGURE 1 – Exemple degrés des sommets dans la molécule C_2H_6.

Théorème 1
Soit $\Gamma = (V, E)$, alors

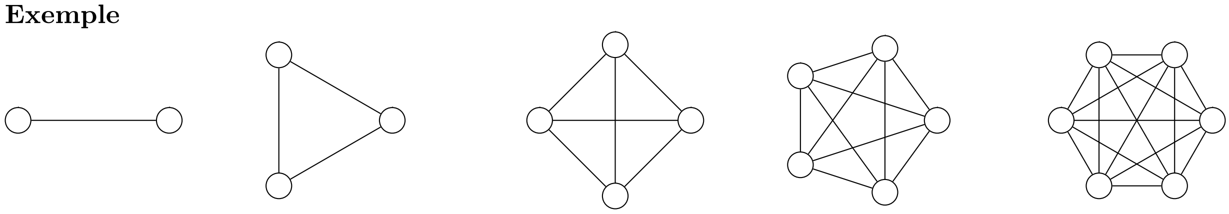
$$\sum_{i=1}^{\#V} deg(v_i) = 2\#E$$

Démonstration
Chaque arête contribue 2 fois dans la somme des degrés.

Corollaire
La somme des degrés des sommets d'un graphe est paire.

Définition 4
Le graphe complet K_n est le graphe simple à n sommets pour lequel chaque paire de sommets est une arête.

Exemple



Définition 5
Un graphe $\Gamma' = (U, F)$ est un sous-graphe de $\Gamma = (V, E)$ si $U \subseteq V$ et $F \subseteq E$. On notera $\Gamma' \leq \Gamma$.

Exemple
$K_m \leq K_n$ *si* $m \leq n$.

Exercice
Montrer que K_m possède $q = \frac{1}{2}n(n-1)$ arêtes.

1.2 Chemins dans les graphes

Définition 6
Soit $\Gamma = (V, E)$ et $v, w \in V$. Un chemin de v à w de longueur n est une séquence alternée de $(n+1)$ sommets $v_0, v_1, ..., v_n$ et de n arêtes $e_1, e_2, ..., e_n$ de la forme

$$(v_0, e_1, v_1, e_2, ..., e_n, v_n)$$

dans laquelle chaque e_i est incident à v_{i-1} et v_i pour $1 \leq i \leq n$ et $e_i \neq e_j, \forall i \neq j \in 1, ..., n$

Un chemin est simple si aucun sommet ne se répète sauf peut-être v_0 et v_n.

Dans un graphe simple on notera juste la suite des sommets lorsque l'on décrit un chemin.

Définition 7
Un graphe $\Gamma = (V, E)$ est connexe si $\forall x, y \in V : \exists$ un chemin de x à y.

La composante connexe de Γ contenant x est le sous-graphe Γ' de Γ dont les sommets et les arêtes sont contenus dans un chemin de Γ démarrant en x.

Définition 8
Soit $\Gamma = (V, E)$ et $v \in V$.

Un cycle est un chemin de v à v.

Un cycle simple est un cycle de v à v dans lequel aucun sommet n'est répété (mis à part le départ et l'arrivée).

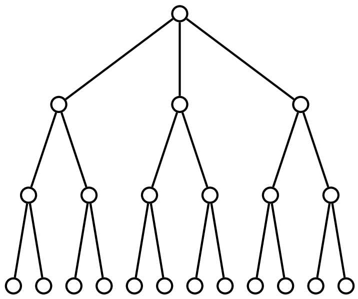
1.3 Arbres

1.3.1 Définitions

Définition 9
Un arbre est un graphe simple connexe qui ne contient aucun cycle.

Définition 10
Dans un arbre, les sommets de degré 1 sont appellés les feuilles.

Exemple



Proposition 1
Si T est un arbre avec $p \geq 2$ sommets, alors T contient au moins 2 feuilles.

Démonstration
T a p sommets. Tous les chemins sont de longueur inférieure ou égale à p. Considérons un chemin $v_0, v_1, ..., v_r$ pour $v_i \in V$, $i = 0, ..., r$ de longueur maximale. Alors, v_0 et v_r sont de degré 1.

Théorème 2
Soit T un graphe simple à p sommets. Alors les 3 assertions suivantes sont équivalentes :

i *T est un arbre.*

ii *T a $(p-1)$ arêtes et aucun cycle.*

iii *T a $(p-1)$ arêtes et est connexe.*

Démonstration
(i) ⇒ (ii) ***: Montrer qu'un arbre à p sommets a (p-1) arêtes.***

Par récurrence :

1. *$p = 1$ OK*
2. *Supposons que ce soit vrai pour tout arbre à $k \geq 1$ sommets et montrons le pour un arbre à (k+1) sommets. Soit T un tel arbre, il a au moins 2 feuilles. Enlevons une de ces feuilles ainsi que l'arête incidente. On obtient un arbre T' à k sommets. Par l'hypothèse de récurrence : T' a (k-1) arêtes, donc T a k arêtes.*

(ii) ⇒ (iii) ***: Supposons (ii) et T ne soit pas connexe.***

Notons $T_1, T_2, ..., T_t$ les composantes connexes de T avec $t \geq 2$. Chaque T_i est un arbre, pour $1 \leq i \leq t$ (car pas de cycle). Soit p_i le nombre de sommets de T_i, alors chaque T_i a $(p_i - 1)$ arêtes.

$$\sum_{i=1}^{t} p_i = p$$

et *donc* $\Rightarrow t = 1$

$$p - 1 = \sum_{i=1}^{t} (p_i - 1) = p - t$$

(iii) ⇒ (i) ***: Supposons que T ne soit pas un arbre.***

Alors, T contient un cycle C. Enlevons une arête de C. On obtient le sous-graphe T' de T qui est toujours connexe. Si T' contient un cycle, alors on itère le processus. Sinon, T' est un arbre à p sommets qui a strictement moins que (p-1) arêtes.

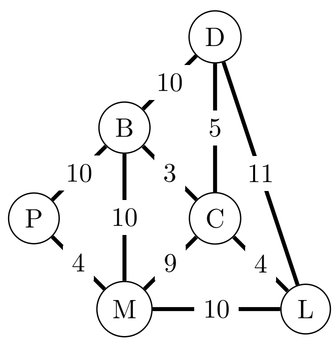
1.3.2 Arbres couvrants et arbres à poids

Définition 11
Un arbre couvrant dans un graphe Γ est un arbre qui est un sous-graphe de Γ et qui contient tous les sommets de Γ.

Dans certains problèmes, certaines arêtes sont plus importantes que d'autres. En théorie des graphes, on modélise cela en assignant une valeur à chaque arête.

Définition 12
Un arbre à poids est un couple (Γ, w) où Γ est un arbre w est une fonction $w : E \to \mathbb{R}^+$. Le nombre w(e) est appelé le poids de l'arête e.

Exemple



1.4 Isomorphisme

Définition 13
Deux graphes $\Gamma_1 = (V_1, E_1, \gamma_1)$ et $\Gamma_2 = (V_2, E_2, \gamma_2)$ sont isomorphes s'il existe une bijection $f : V_1 \to V_2$ et une bijection $g : E_1 \to E_2$ telles que $\forall e \in E_1$: e est incident à v,w $\in V_1$ ssi g(e) est incident à f(v),f(w) $\in V_2$. Le couple (f,g) est appelé un isomorphisme de graphe et on note $\Gamma_1 \cong \Gamma_2$.

Deux graphes isomorphes ont les mêmes propriétés.

Exemple

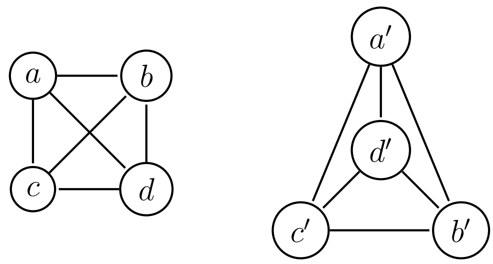


FIGURE 2 – Deux graphes isomorphes

1.5 Graphes hamiltoniens

Hamilton propose le problème suivant : Considérons le graphe du dodécaèdre. Est-il possible, en partant d'un des vingts sommets et en suivant les arêtes du graphe, de visiter tous les sommets une et une seule fois et de revenir au sommet de départ ?

L'exemple suivant montre un chemin qui réponds à ce problème.

Exemple

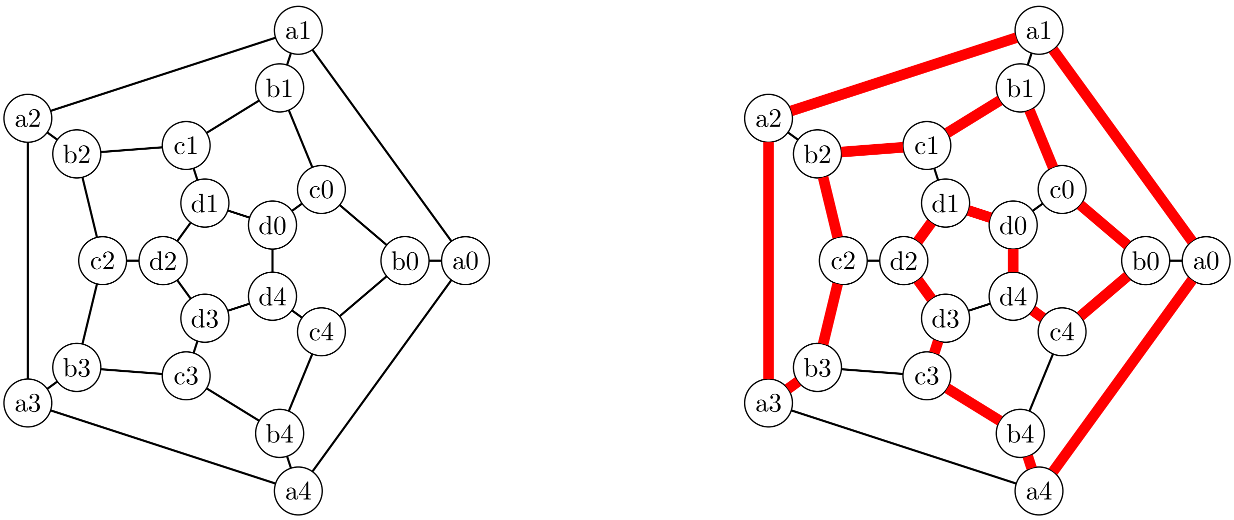


FIGURE 3 – Graphe hamiltonien et cycle hamiltonien

Définition 14
Un cycle hamiltonien dans un graphe Γ est un cycle simple contenant tous les sommets de Γ.

Pour donner un exemple de graphe non-hamiltonien on introduit la notion de graphe biparti.

Définition 15
Un graphe $\Gamma = (V, E)$ est biparti si on peu écrire $V = B \cup W$ avec $B \cap W = \varnothing$ et toute arête de Γ joint un sommet dans B à un sommet dans W.

Exemple

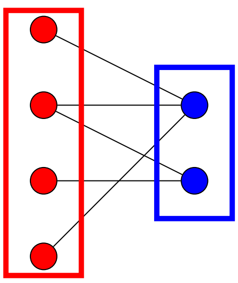


FIGURE 4 – B en rouge, W en bleu

Lemme
Si Γ est biparti, alors Γ ne contient pas de cycle simple de longueur impaire.

Théorème 3
Un graphe biparti avec un nombre impaire de sommets n'est pas hamiltonien.

Démonstration
Pour être hamiltonien, il doit admettre un cycle simple passant par tous ses sommets, donc de longueur impaire. Ce n'est pas possible à cause du Lemme précédent.

Exemple

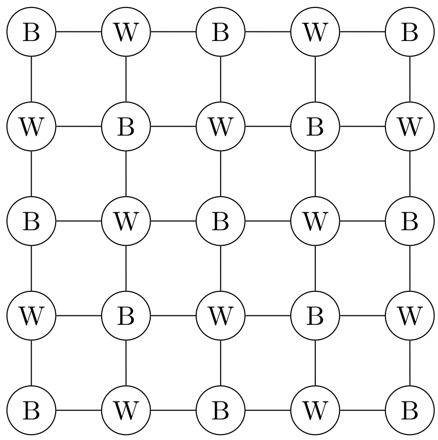


FIGURE 5 – Graphe biparti mais non hamiltonien.

Théorème 4 (Dirac 1950)
Soit $\Gamma = (V, E)$ un graphe simple avec $p \geq 3$ sommets. Si $\forall v \in V : deg(v) \geq \frac{1}{2}p$, alors Γ est Hamiltonien.

Démonstration
Γ est connexe. Soit $C = (v_0, v_1, ..., v_k)$ un plus long chemin simple dans Γ avec $v_0 \neq v_k, k < p$.

$deg(v_0) \geq \frac{p}{2}$, tous les sommets adjacents à v_0 sont dans $\{v_1, ..., v_k\}$

$deg(v_k) \geq \frac{p}{2}$, tous les sommets adjacents à v_k sont dans $\{v_0, ..., v_{k-1}\}$

Comme $k < q$, il doit exister $i \in \{0, ..., k-1\}$ tel que $\{v_i, v_k\} \in E$ et $\{v_0, v_{i+1}\} \in E$. On obtient un cycle $\widetilde{C} = (v_0, v_1, ..., v_i, v_k, v_{k-1}, ..., v_{i+1}, v_0)$

On note que $\widetilde{C}$ est un cycle Hamiltonien.

Supposons :

$\exists y \in \widetilde{C} \Rightarrow$ On peut supposer que $\{v_j, y\} \in E$ pour $j = \{0, ..., k\}$.

$\Rightarrow$ On construit un chemin $\overline{C} = (y, v_j, v_{j-1}, ...v_0, v_{i+1}, ..., v_k, v_i, v_{i-1}, ..., v_{j-1})$. $\overline{C}$ est un chemin plus long que C.

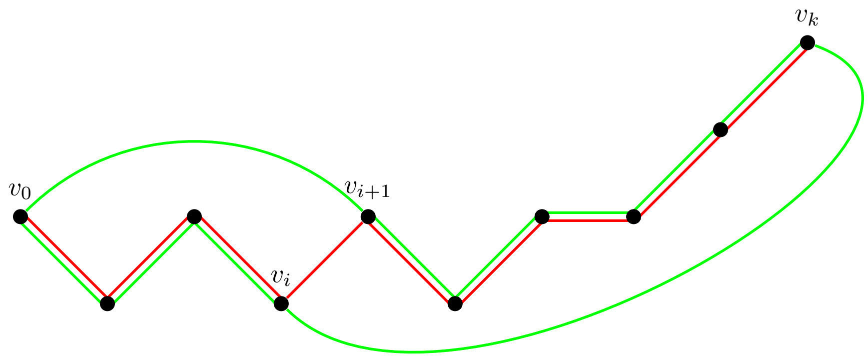


FIGURE 6 – Les 2 chemins, C en rouge, $\widetilde{C}$ en vert.

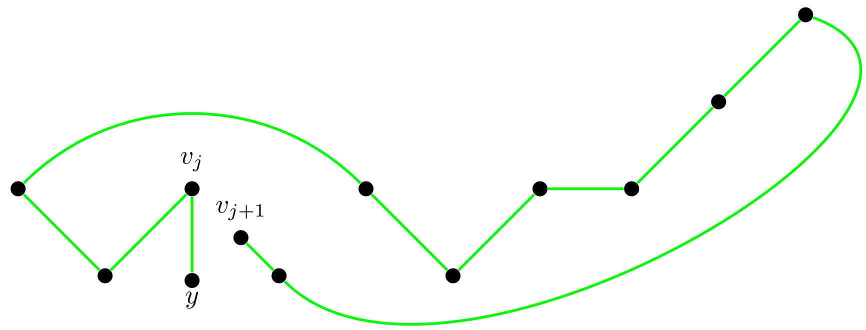


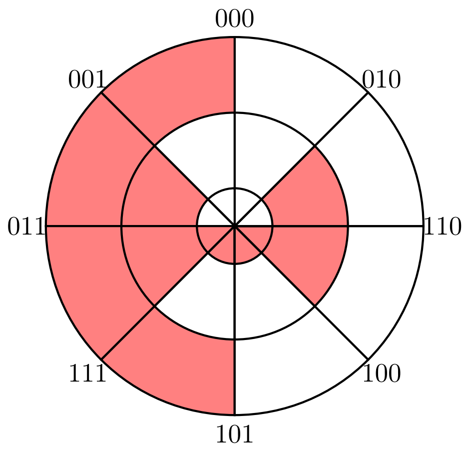
FIGURE 7 – Chemin $\overline{C}$

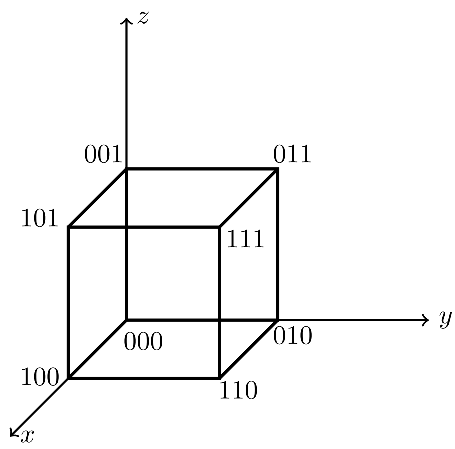
Illustration : Code de Gray

Un code de Gray d'ordre n est un arrangement cyclique de 2^n mots binaires de longueur n tels que 2 mots adjacents ne diffèrent qu'en une seule position.

Exemple

Le code de Grey ci-dessous provient d'un cycle hamiltonien sur le graphe du cube :





Un code de Gray d'ordre (n+1) se construit à partir d'un code de Gray d'ordre n comme suit :

1. On écrit le code de Gray donné d'ordre n en ajoutant à la fin de chaque mot un zéro.
2. On le fait suivre par le même code de Gray parcouru dans l'autre sens et en ajoutant à la fin de chaque mot un 1.

1.6 Graphes Eulériens

Définition 16
Un cycle Eulérien dans un graphe Γ est un cycle qui contient toutes les arêtes de Γ. Un graphe est Eulérien s'il contient un cycle Eulérien.

Exemple
<EXEMPLE PAGE 15>

Proposition 2
Si un graphe est Eulérien, alors tous ses sommets sont de degré pair.

Lemme
Soit Γ un graphe dans lequel chaque sommet est de degré pair, alors l'ensemble E se partitionne en une union de cycles (arête-)disjointe.

Exemple
<DRAWING 3 CYCLES PAGE 15>

Démonstration
Par récurrence, sur le nombre d'arêtes

1. *Le lemme est vrai pour $q = 2$.*
2. *Supposons qu'il soit vrai pour tout graphe à $q \leq k$ arêtes et montrons-le pour un graphe à (k+1) arêtes.*
3. *Soit v_0 un sommet de Γ. On démarre un chemin en v_0 et on le suit jusqu'à ce qu'un sommet soit répété 2 fois. On le note v_j et C le cycle de v_j à v_j.*
4. *Soit Γ' le sous-graphe de Γ, obtenu par $V = V'$ et $E' = E \setminus C$. Γ' a $\#E' \leq k$ arêtes. Par hypothèse de récurrence, les arêtes de Γ' se partitionnent en une union arête-disjointe de cycles $C_1 \cup C_2 \cup ... \cup C_n$.*
5. *Donc, $C_1 \cup C_2 \cup ... \cup C_n$ est une partition arête-disjointe des arêtes de Γ.*

Théorème 5
Soit Γ un graphe connexe. Alors, Γ est eulérien si et seulement si chaque sommet a un degré pair.

Démonstration
$\Rightarrow$ *OK par proposition précédente.*
$\Leftarrow$ *Par le Lemme : E se partitionne en une union (arête-)disjointe de cycles $C_1 \cup C_2 \cup ... \cup C_n$.*

1. *Si n=1, c'est bon.*
2. *Si $n > 1$, comme Γ est connexe, $\exists$ une arête incidente à un $v \in C_1$ et un $w \notin C_1$. Cette arête est dans C_j pour un $j = 2, ..., n$ (car on a une partition de E). On attache ce cycle en v. S'il reste des cycles dans la partition, on itère ce procédé jusqu'à avoir utilisé tous les cycles.*

1.7 Application : le problème du voyageur de commerce (TSP)

1.7.1 Énoncé du problème

Énoncé : Un vendeur de livres démarre de chez lui et doit visiter un certain nombre de librairies avant de rentrer chez lui. Comment doit-il choisir sa route pour minimiser la distance parcourue ?

Objet mathématique : Un graphe valué (à chaque arête est associé un nombre appelé poids) où les sommets représentent les librairies et les arêtes représentent les routes.

<VALUED K5 GRAPH HERE PAGE 17>

Objectif : Trouver un cycle hamiltonien de poids minimal.

Remarque : Un graphe complet K_n à n sommets possède $\frac{1}{2}(n-1)!$ cycles hamiltoniens différents. Par exemple, pour $n = 10 \Rightarrow 181440$ cycles. On ne connait pas encore d'algorithme efficace qui donne une solution au problème.

1.7.2 Arbres couvrant minimum

Définition 17
Un arbre couvrant dans un graphe Γ est un arbre qui est un sous-graphe de Γ et qui contient tous les sommets de Γ.

Exemple
<GRAPH TO MIN SPANNING TREE EXAMPLES HERE>

Il existe un algorithme qui donne des arbres couvrants de poids minimum dans un graphe valué.

Algorithme de Kurskal :

i Choisir une arêtes de plus petit poids.
ii Choisir parmi les arêtes restantes une arête de plus petit poids dont l'inclusion ne crée pas un cycle.
iii Continuer jusqu'à obtenir un arbre couvrant.

Exemple
<GRAPH K5 WITH PATH HERE>

Remarque : Si C est un cycles hamiltonien dans un graphe Γ, alors $\forall e \in E$ arête de C : $C \setminus \{e\}$ est un arbre couvrant.

$\Rightarrow$ (Solution de TSP) $\geq$ (longueur minimum d'un arbre couvrant)

Mieux : Soit v un sommet de Γ. Tout cycle hamiltonien contient 2 arêtes incidentes à v. Le reste du chemin est un arbre couvrant de $\Gamma \setminus \{v\}$.

$\Rightarrow$ (Solution de TSP) $\geq$ ($\sum$ des longueurs des 2 plus courtes arêtes incidentes à v) + (longueur minimum d'un arbre couvrant de $\Gamma \setminus \{v\}$)

Remarque : Il existe une borne supérieure à TSP en utilisant des cycles eulériens.

1.8 Ordres partiels

Définition 18
Soit P un ensemble. Un ordre partiel sur P est une relation sur P, c'est à dire un ensemble de couples $(p_1, p_2) \in P \times P$, noté $p1 \leq p2$ tel que :

1. $p \leq p$ *(réflexive)*
2. $(p \leq q$ *et* $q \leq p) \Rightarrow p = q$ *(anti-symétrique)*
3. $(p \leq q$ *et* $q \leq r) \Rightarrow p \leq r$ *(transitive)*

On note $(P, \leq)$ un ensemble partiellement ordonné.

Remarque : Soit $(P, \leq)$ un ensemble partiellement ordonné, alors on définit un ordre partiel $\geq$ par :

$$x \geq y \Leftrightarrow y \leq x$$

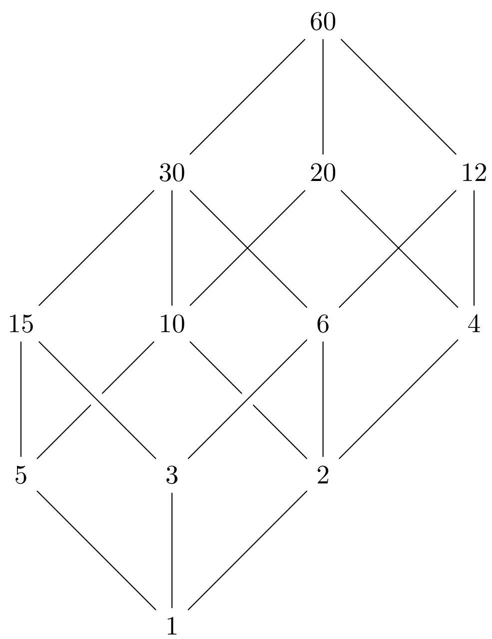
Définition 19
Soit P un ensemble.

1. *$(P, \leq)$ est dit totalement ordonné si $\forall p_1, p_2 \in P$, $p_1 \leq p_2$ ou $p_2 \leq p_1$*
2. *Soit $(P, \leq)$ un ordre partiel : une chaîne C est un sous-ensemble de P qui est totalement ordonné.*

Exemple
1. $(\mathbb{N}, \leq)$
2. $(\mathbb{N}, |)$ *où* $a \mid b$ *si* $\exists c \in \mathbb{Z}$ *tel que* $a \cdot c = b$ $(a, b \in \mathbb{Z})$

Une relation d'ordre partiel peut se représenter à l'aide d'un graphe dirigé, mais il est très compliqué. On le simplifie en laissant tomber toutes les relations qui s'obtiennent par transitivité et les lacets.

Par transitivité et anti-symétrie : on sait qu'il n'y a pas de cycles, on peut se passer des flèches et on note de bas en haut.



Définition 20
Soit $(P, \leq)$ un ensemble partiellement ordonné. Une anti-chaîne est un sous-ensemble A de P tel que $\forall a_1, a_2 \in A : a_1 \nleq a_2$ et $a_2 \nleq a_1$

Exemple
({1,2,3,6,8},|), A = {2,3} est une anti-chaîne.

Théorème 6 (Dilworth)
Soit $(P, \leq)$ un ensemble fini partiellement ordonné. Alors il existe une anti-chaîne A et une partition Q de P par des chaînes telle que $\#Q = \#A$.

Théorème 7
Soit $\Gamma = (V, E)$ *un graphe simple.*

1. *Un couplage* M *de* Γ *est un sous-ensemble d'arêtes de* Γ*, 2 à 2 non adjacentes. Les sommets incidents aux arêtes de* M *sont dits couplés.*
2. *Un transversal de* Γ *est un sous-ensemble* T *de* V *tel que toute arêtes* Γ *est incidente à au moins un sommet de* T*.*

<IMAGE COUPLAGE TRANSVERSAL ANTICHAINE>

Théorème 8 (König)
Soit $\Gamma = (B \amalg W, E)$ *un graphe biparti. La cardinalité maximale d'un couplage de* Γ *est égale à la cardinalité minimum d'un transversal de* Γ*.*

Démonstration
<DEMO PAS CLAIRE, DEMANDER AU PROF>

Démonstration
On va montrer König $\Rightarrow$ Dilworth.

Soit $(P, \leq)$ un ordre partiel. On construit un graphe biparti $\Gamma = (B \amalg W, E)$ où $B = \{(p,1) | p \in P\}$ et $W = \{(p,2) | p \in P\}$ et $\{(p,1),(q,2)\} \in E \Leftrightarrow p \leq q$ et $p \neq q$.

Soit M un couplage de cardinalité maximale de Γ et T un transversal de cardinalité minimale de Γ. Par König, $\#M = \#T$.

On définit $A \subseteq P$ par $A = \{p \in P | (p,1) \in T$ et $(p,2) \notin T\}$ et $\#A \geq \#P - \#T$.

On construit des chaînes comme suit : $Q = \{C_1, ..., C_n\}$ où

$$\begin{cases} \text{Soit } C_i = \{p_0, ..., p_e\},\ l \geq 1 \text{ si } \{(p_k,1),(p_{k+1},2)\} \in M \text{ et } (p_e,1) \text{ n'est pas incident à } M,\ (p_0,2) \text{ n'est pas incident à } M. \\ \text{Soit } C_i = \{p\} \text{ si } (p,1) \text{ et } (p,2) \text{ ne sont pas incidents à } M. \end{cases}$$

Alors, Q est une partition de P (car, par construction, $P = \bigcup_{i=1}^{n} C_i$ et $C_i \cap C_j = \varnothing, \forall i \neq j$)

Et $\#P = \sum_{i=1}^{n} \#C_i = \#M + \#Q$

$\Rightarrow \#Q = \#P - \#M$

$\xRightarrow{(Konig)} \#Q = \#P - \#T \leq \#A$

$\Rightarrow \#Q = \#A$

2 Arithmétique Modulaire

2.1 Les entiers et la division euclidienne

L'ensemble des entiers est noté $\mathbb{Z}$, il contient les entiers naturels ($\mathbb{N}$) et leur opposé. Il est naturellement muni de 2 opérations qui satisfont les propriétés suivantes :

1. **L'addition** $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} : (a, b) \to a + b$
   Propriétés :
   (a) **Associativité** $(a + b) + c = a + (b + c)$, $\forall a, b, c \in \mathbb{Z}$
   (b) **Élément neutre** $0 \in \mathbb{Z} : a + 0 = a = 0 + a$, $\forall a \in \mathbb{Z}$
   (c) **Opposé** $\forall a \in \mathbb{Z} : \exists - a \in \mathbb{Z}$ tel que $a + (-a) = 0 = (-a) + a$
   (d) **Commutativité** $\forall a, b \in \mathbb{Z} : a + b = b + a$

   On dit que $(\mathbb{Z}, +)$ est un groupe (a,b,c) commutatif (d).

2. **La multiplication** $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} : (a, b) \to a \cdot b$
   Propriétés :
   (a) **Associativité** $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
   (b) **Distributivité par rapport à l'addition**
   $$\left.\begin{array}{l} a \cdot (b+c) = ab+ac \\ (a+b) \cdot c = ac+bc \end{array}\right. \quad \forall a, b, c \in \mathbb{Z}$$
   (c) **Commutativité** $a \cdot b = b \cdot a, \forall a, b \in \mathbb{Z}$
   (d) **Élément neutre** $1 \in \mathbb{Z} : 1 \cdot a = a = a \cdot 1$, $\forall a \in \mathbb{Z}$
   (e) $\forall a, b, c \in \mathbb{Z} : a \cdot c = a \cdot b \Rightarrow c = b$

   On dit que $(\mathbb{Z}, +, \cdot)$ est un anneau ($(\mathbb{Z}, +)$ est un groupe commutatif et $\cdot$ satisfait a et b) unital (d), commutatif (c) et intègre (e).

On a aussi sur $\mathbb{Z}$ une relation d'ordre $\leq$ telle que :

1. $\leq$ est un ordre total
2. $\forall a, b, c \in \mathbb{Z}$, $a \leq b \Rightarrow a + c \leq b + c$
3. $\forall a, b, c \in \mathbb{Z}$, $a \leq b$, $c \geq 0 \Rightarrow ac \leq bc$

La valeur absolue est une application

$$| \, | : \mathbb{Z} \to \mathbb{N} : a \to \begin{cases} a & \text{si } a \geq 0 \\ -a & \text{si } a \leq 0 \end{cases}$$

telle que :

1. $\forall a \in \mathbb{Z} : |a| = 0$ ssi $a = 0$
2. $\forall a, b \in \mathbb{Z} : |a \cdot b| = |a| \cdot |b|$

Remarque : L'équation $ax = b, a, b \in \mathbb{Z}$ n'a pas toujours de solution dans $\mathbb{Z}$.

Définition 21
Soit $a, b \in \mathbb{Z}$, on dit que a divise b, et on note $a|b$, si $\exists c \in \mathbb{Z}$ tel que $ac = b$. On dit aussi que b est un multiple de a.

Proposition 3
$|$ est une relation :

1. ***Réflexive*** $\forall a \in \mathbb{Z} : a|a$
2. ***Transitive*** $\forall a, b, c \in \mathbb{Z} : a|b$ *et* $b|c \Rightarrow a|c$
3. ***Anti-symétrique*** $\forall a, b \in \mathbb{Z} : a|b$ *et* $b|a \Rightarrow a = \pm b$

Théorème 9 (Division Euclidienne)
$\forall a, b \in \mathbb{Z}$, $b \neq 0$, $\exists$ *des entiers uniques* q *et* r *tels que* $a = bq + r$ *et* $0 \leq r < |b|$

<PAGES 3 À 6>

2.2 Groupes, anneaux et entiers modulo n

<PAGES 7 À 18>

2.2.1 Relation de congruence

Définition 22
Soient $a, b, k \in \mathbb{Z}, k \neq 0, 1, -1$. *On dit que* a *est congru à* b *modulo* k *et on note* $a \equiv b(mod\ k)$ *si* $a - b \in k\mathbb{Z}$ *(ou encore si* $\overline{a} = \overline{b}$ *dans* $\mathbb{Z}/k\mathbb{Z}$*).*

Propriétés :

1. La congruence modulo k est une relation d'équivalence.
   - **Réflexivité** $\forall a \in \mathbb{Z} : a \equiv a(mod\ k)$
   - **Symétrie** $\forall a, b \in \mathbb{Z} : a \equiv b(mod\ k) \Leftrightarrow b \equiv a(mod\ k)$
   - **Transitivité** $\forall a, b, c \in \mathbb{Z} : \begin{cases} a \equiv b(mod\ k) \\ b \equiv c(mod\ k) \end{cases} \Rightarrow a \equiv c(mod\ k)$
2. $\forall a_1, b_1, a_2, b_2, k \in \mathbb{Z}, k \neq 0, 1, -1$.

   Si $a_1 \equiv a_2(mod\ k)$ et $b_1 \equiv b_2(mod\ k)$, alors $\begin{cases} a_1 + b_1 \equiv a_2 + b_2(mod\ k) \\ a_1 b_1 \equiv a_2 b_2(mod\ k) \end{cases}$

   En conséquence : $\forall c \in \mathbb{Z} : a_1 c \equiv a_2 c(mod\ k)$

Exemple
$6 \equiv 2(mod\ 4)$
$7 \equiv 0(mod\ 7)$

2.3 Cryptologie : Le système RSA

Pour comprendre le système de cryptage RSA, on aura besoin d'un résultat technique.

Lemme
$\forall z \in \mathbb{N} : (z+1)^p \equiv n^p + 1(mod\ p)$ *si* p *est un nombre premier.*

Théorème 10 (Le petit théorème de Fermat)
Soit $p \in \mathbb{N}$ *un nombre premier.*
Soit $a \in \mathbb{N}$ *un nombre tel que* $p \nmid a$ *(p ne divise pas a).*
Alors, $a^{p-1} \equiv 1(mod\ p)$

Démonstration
Nous allons procéder par plusieurs étapes.

1. *Montrons par récurrence que* $\forall a \in \mathbb{N} : a^p \equiv a (mod\ p)$.
   $a = 1 : 1^p = 1 (mod\ p)$
   Supposons vrai pour $a \in \mathbb{N}$ *et montrons pour* $a + 1$.
   Par le lemme, on sait que $(a+1)^p \equiv a^p + 1 (mod\ p)$. *Alors, par hypothèse de récurrence :* $(a+1)^p \equiv a + 1 (mod\ p)$.

2. *On va maintenant utiliser* $p \not| a$.
   On a : $\forall a \in \mathbb{N} : a^p \equiv a (mod\ p)$.
   $\Rightarrow$ *Dans* $\mathbb{Z}/p\mathbb{Z} : \overline{ap} = \overline{a}$ *et comme* $p \not| a : \exists \overline{b} \in \mathbb{Z}/p\mathbb{Z}$ *un inverse de* $\overline{a}$.
   $\Rightarrow \overline{b}\overline{a^p} = \overline{b}\overline{a}$
   $\Rightarrow \overline{b}\overline{a}^p = \overline{1}$
   $\Rightarrow \overline{a}^{p-1} = \overline{1} \Leftrightarrow a^{p-1} \equiv 1 (mod\ p)$

Démonstration (du Lemme)
<WHOLE DEMO>

2.3.1 Fonctionnement des clés de chiffrement RSA

2 personnes (A et B) veulent communiquer de manière sûre entre elles.

A choisit 2 nombres premiers p et q $\in \mathbb{N}$ appelés clé privée. A calcule :

1. $N = pq$
2. $O(N) = (p-1)(q-1)$
3. $e \in \mathbb{Z}$ tel que pgcd(e, O(N)) = 1

appelé l'exposant de chiffrement.

O(N) et e sont premiers entre eux $\Rightarrow \exists 0 < s < O(N) : es \equiv 1 (mod\ O(N))$, c'est à dire que $\overline{s}$ est l'inverse de $\overline{e}$ dans $\mathbb{Z}/O(N)\mathbb{Z}$. **s est gardé secret**.

A publie les nombres (N,e) appelés la clé publique.

B souhaite envoyer un message à A. Dans le système RSA, la taille du message est $0 < M < N$.

B utilise la clé publique et envoie le message chiffré : $\tilde{M} = M^e (mod\ N)$

Pour déchiffrer le message, A utilise s et obtient : $\tilde{M}^s = M^{es} (mod\ N) = M (mod\ N)$ (par le théorème suivant)

3 Combinatoire énumérative

4 Théorie des Codes

5 Transformées de Fourier discrètes