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.

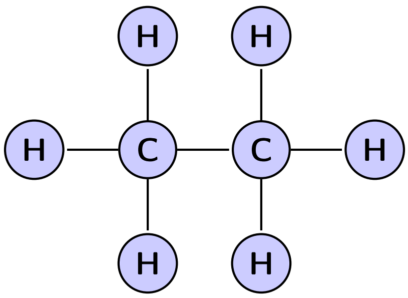


FIGURE 1 – Exemple degrés des sommets dans la molécule C_2H_6.

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

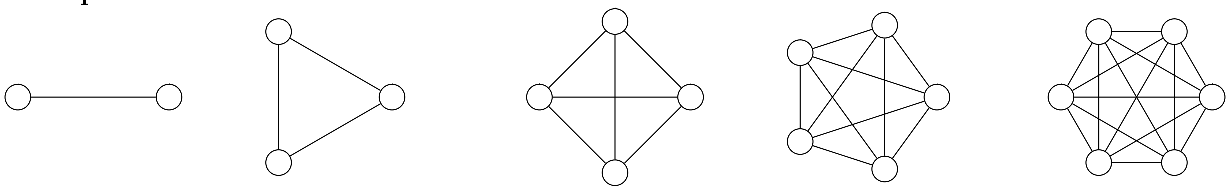
$$\sum_{i=1}^{\#V} deg(v_i) = 2\#E$$

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 $v_0, v_1, \ldots, v_n$ et de n arêtes $e_1, e_2, \ldots, e_n$ de la forme

$$(v_0, e_1, v_1, e_2, \ldots, e_n, v_n)$$

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

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).

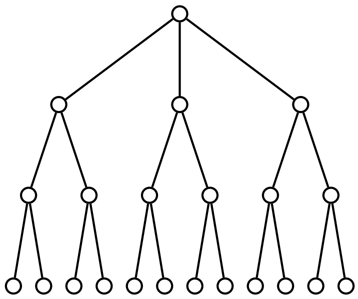
1.3 Arbres

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 $v_0, v_1, \ldots, v_r$ pour $v_i \in V$, $i = 0, \ldots, r$ de longueur maximale. Alors, v_0 et v_r sont de degré 1.

Théorème 2 (ATTENTION ! Ce théorème et sa démonstration font partie de ceux à connaitre par coeur à l'examen ! (pour l'année 2015-2016))
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 (par Proposition 1). 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 $T_1, T_2, \ldots, T_t$ 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.

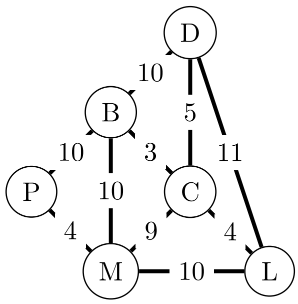
1.3.2 Arbres couvrants et arbres à poids

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

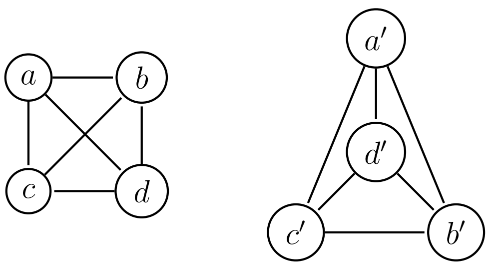


FIGURE 2 – Deux graphes isomorphes

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

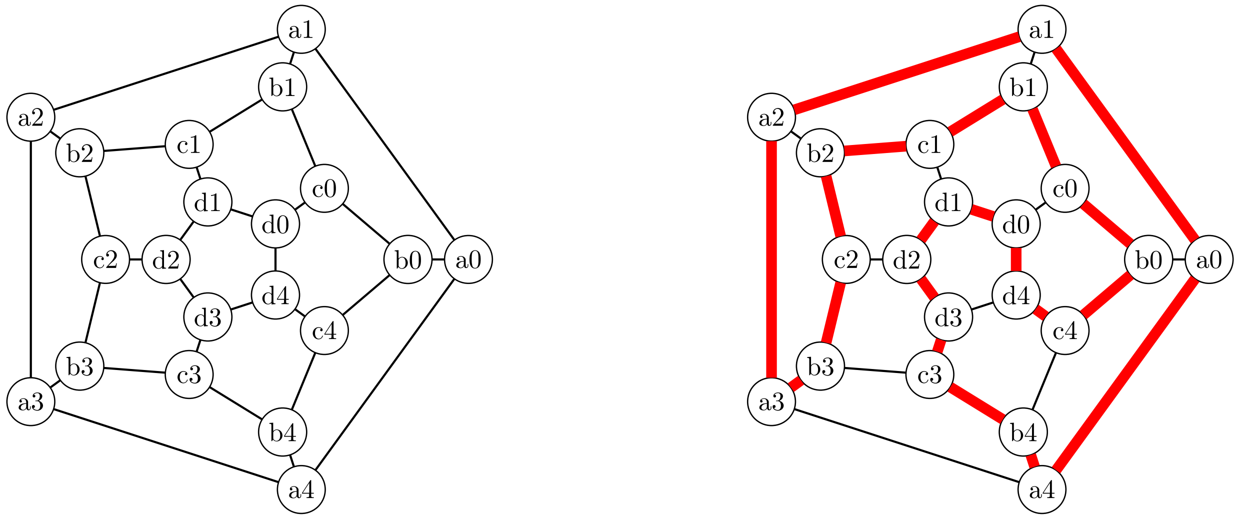


FIGURE 3 – Graphe hamiltonien et cycle hamiltonien

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

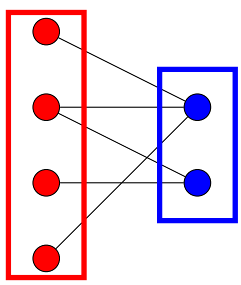


FIGURE 4 – B en rouge, W en bleu

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

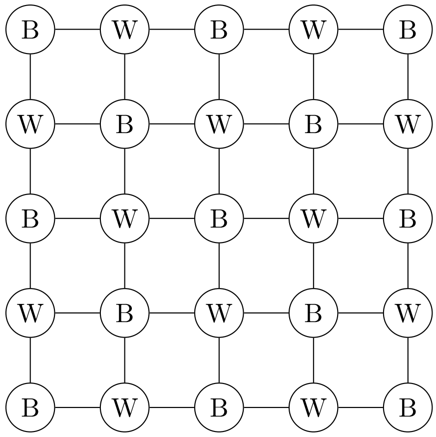


Figure 5 – Graphe biparti mais non hamiltonien.

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 $C = (v_0, v_1, \ldots, v_k)$ 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 $\{v_1, \ldots, v_k\}$

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

Comme $k < q$, il doit exister $i \in \{0, \ldots, k-1\}$ tel que $\{v_i, v_k\} \in E$ et $\{v_0, v_{i+1}\} \in E$.

On obtient un cycle $\widetilde{C} = (v_0, v_1, \ldots, v_i, v_k, v_{k-1}, \ldots, v_{i+1}, v_0)$

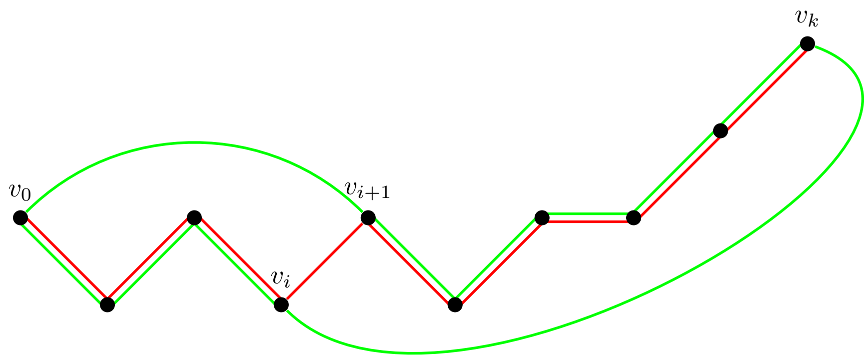


FIGURE 6 – Les 2 chemins, C en rouge, $\widetilde{C}$ en vert.

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 $j = \{0, \ldots, k\}$.

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

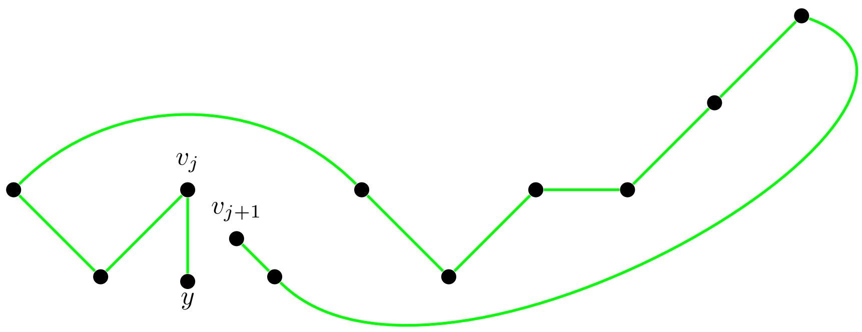
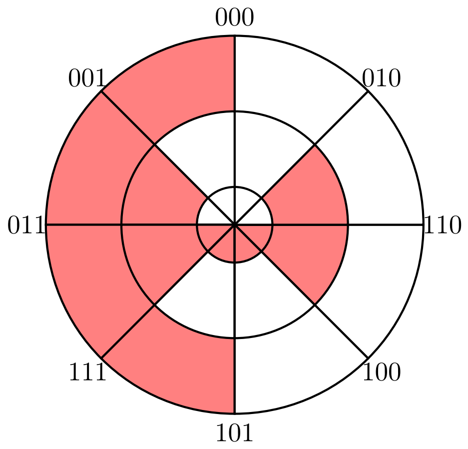


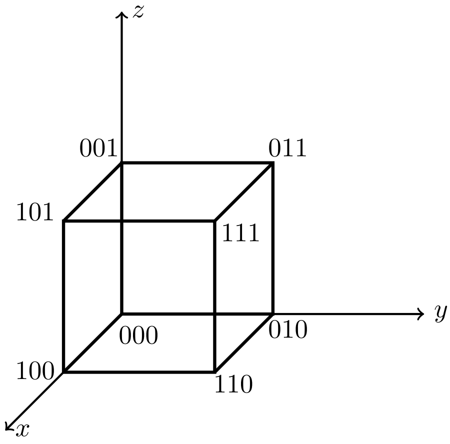
FIGURE 7 – Chemin $\overline{C}$

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.

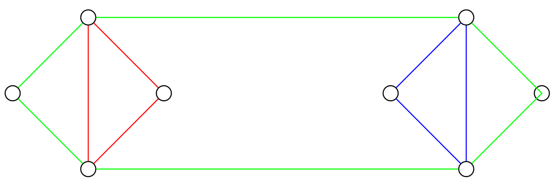
1.6 Graphes Eulériens

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.

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



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* $C_1 \cup C_2 \cup \ldots \cup C_n$.
5. *Donc,* $C_1 \cup C_2 \cup \ldots \cup C_n$ *est une partition arête-disjointe des arêtes de* Γ.

Théorème 5 (ATTENTION ! Ce théorème et sa démonstration ainsi que le lemme et la proposition utilisés dans la démonstration font partie de ceux à connaitre par coeur à l'examen ! (pour l'année 2015-2016))
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* $C_1 \cup C_2 \cup \ldots \cup C_n$.

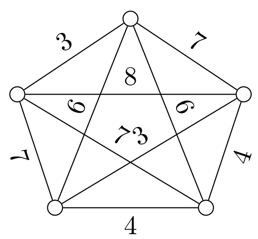
1. *Si n=1, c'est bon.*
2. *Si* $n > 1$, *comme* Γ *est connexe,* $\exists$ *une arête incidente à un* $v \in C_1$ *et un* $w \notin C_1$. *Cette arête est dans* C_j *pour un* $j = 2, \ldots, n$ *(car on a une partition de E). On attache ce cycle en v. S'il reste des cycles dans la partition, on itère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



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.

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

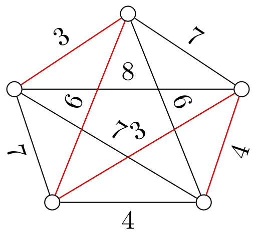
Algorithme de Kurskal :

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



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
$(\mathbb{N}, \leq)$

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

Lien avec la théorie des graphes :

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.

Ex : ({1,2,3,4,5,6,10,12,15,20,30,60}, |)

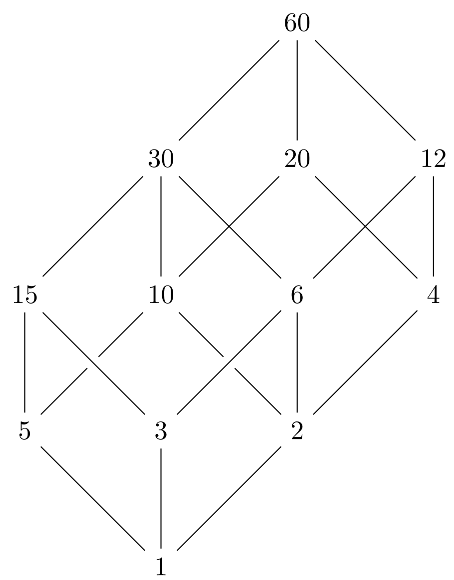


FIGURE 8 – Diagramme de Hasse

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* $\#Q = \#A$*.*

Lien avec les graphes bipartis :

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*.*

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*.*

Exemple

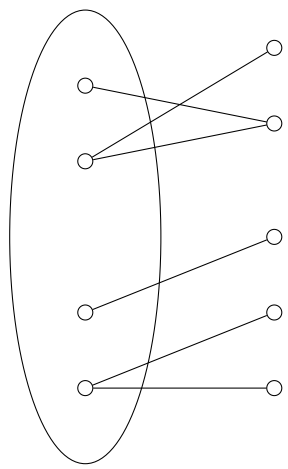


FIGURE 9 – Couplage : 4 arêtes. Transversal : 4 sommets.

Définition 21
Soit $\Gamma = (B \amalg W, E)$ un graphe biparti et M un couplage. Un chemin alterné est un chemin qui démarre en un sommet non-couplé de B et alterne une arrête de E/M puis une arrête dans M et ainsi de suite.

Exemple

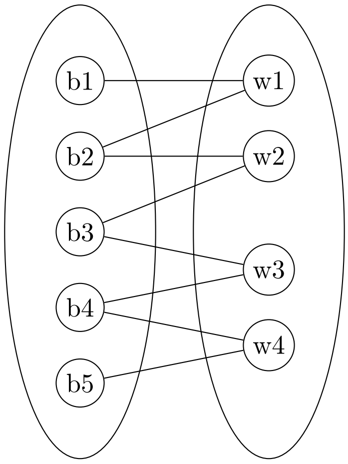


FIGURE 10 – Couplage max : (b1, w1, b2, w2, b3, w3, b4, w4, b5)

Démonstration
Soit M un couplage de cardinalité maximale. $\forall$ arête de M, choisissons un de ses sommets incidents comme suit :

1. *Le sommet dans W s'il existe un chemin alternant arrivant à ce sommet.*
2. *Le sommet dans B sinon.*

Notons U cet ensemble de sommets. Il faut montrer que cet ensemble U de $\#M$ sommets est un transversal de Γ.

Soit $e = \{b, w\} \in E$, il faut montrer que soit $b \in U$, soit $w \in U$. On peut supposer que $e \notin M$.

M est maximal $\Rightarrow \exists e' \in M$ tel que $b' = b$ ou $w' = w$

On peut supposer $b' = b$ (car si b n'est pas couplé et $w' = w \Rightarrow \{b, w\} = \{b, w'\}$ est donc un chemin alterné et $w' \in U$ par construction).

Donc, il existe un chemin alterné P terminant en w'.

Donc, il existe un chemin alterné P' terminant en w :

1. *Soit $P' = P \setminus \{\{w, b\}, \{b, w'\}\} \Rightarrow w \in U$ car P' est un chemin alterné arrivant en W.*
2. *Soit on définit un nouveau chemin en rajoutant 2 arêtes $P' = P \cup \{w', b\} \cup \{b, w\}$.*
   (a) *Si w est couplé $\Rightarrow w \in U$*
   (b) *Si w pas couplé, on construit un matching + grand en gardant les arêtes de M qui ne sont pas dans P' et en ajoutant les arêtes de P' qui ne sont pas dans M (impossible ?).*

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 : $Q = \{C_1, \ldots, C_n\}$ où

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

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 22
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 (quotient) et r (reste) tels que $a = bq + r$ et $0 \leq r < |b|$

Définition 23
Un nombre $p \in \mathbb{Z}$ est premier si $p \neq 1, -1, 0$ et p n'est divisible que par 1, -1, p et -p.

Définition 24
Un entier d est un plus grand commun diviseur (pgcd) de 2 entiers a et b ssi :

1. *d/a, d/b*
2. *Si $c \in \mathbb{Z} : c|a$ et $c|b \Rightarrow c|d$*

On note pgcd(a,b) le pgcd positif de a et b $\in \mathbb{Z}_0$ et on pose pgcd(a,0) = |a|, $\forall a \in \mathbb{Z}_0$

2.1.1 L'algorithme d'Euclide

Proposition 4
Si $a, b \in \mathbb{Z}, b \neq 0$ et $q, r \in \mathbb{Z}$ tel que $a = bq + r$, alors pgcd(a,b) = pgcd(b,r).

Démonstration
Comme a = bq + r, si c/b et r $\Rightarrow$ c/a. Comme a - bq = r, si c/a et b $\Rightarrow$ c/r. Donc, l'ensemble des diviseurs communs de b et r est égal à l'ensemble des diviseurs communs de a et b.

Algorithme d'Euclide : Pour trouver explicitement pgcd(a,b) $\forall a, b \in \mathbb{Z}, b \neq 0$, on procède comme suit :

On suppose que a et b ≥ 0 car pgcd(a,b) = pgcd(-a,b) = pgcd(a,-b) = pgcd(-a,-b).

Par le théorème de division euclidienne : $a = bq_1 + r_1$ pour $q_1 \in \mathbb{Z}$ et $0 \leq r_1 < b$ alors $pgcd(a, b) = pgcd(b, r_1)$.

Si $r_1 = 0$ alors pgcd(a,b) = pgcd(b,0) = b. Sinon, $r_1 > 0$ et par division euclidienne : $b = r_1 q_2 + r_2 \quad 0 \leq r_2 < r_1$.

Si $r_2 = 0 \Rightarrow pgcd(a, b) = r_1$. Sinon, on itère $r_1 = r_2 q_3 + r_3 \quad 0 \leq r_3 < r_2$.

On obtient des restes $r_1, r_2, \ldots$ qui sont des entiers non négatifs décroissants. Il doit donc exister $n \in \mathbb{N}_0$ tel que $r_{n+1} = 0$ et $r_n \neq 0$.

$pgcd(a, b) = pgcd(b, r_1) = pgcd(r_1, r_2) = \ldots = pgcd(r_{n-1}, r_n) = pgcd(r_n, 0) = r_n$

Proposition 5 (Identité de Bézout)
Soit $a, b \in \mathbb{Z}$, alors $\exists s, t \in \mathbb{Z}$ tels que pgcd(a,b) = sa + tb.

Démonstration
Supposons que a et b > 0. Soient $r_1, \ldots, r_n$ les restes de la division euclidienne donnés par l'algorithme d'Euclide tels que :

$$\begin{array}{ll} a = bq_1 + r_1 & \\ b = r_1q_2 + r_2 & 0 < r_1 < b \\ r_i = r_{i+1}q_{i+2} + r_{i+2} & 0 < r_2 < r_1 \\ r_{n-3} = r_{n-2}q_{n-1} + r_{n-1} & 0 < r_{i+2} < r_{i+1} \\ r_{n-2} = r_{n-1}q_n + r_n & 0 < r_n < r_{n-1} \\ r_{n-1} = r_nq_{n+1} + 0 & \end{array}$$

$pgcd(a, b) = pgcd(b, r_1) = pgcd(r_2, r_3) = \ldots = pgcd(r_{n-1}, r_n)$

On pose $r_0 = b$ et $r_{-1} = a$ pour l'algo.

On construit s et t comme suit :

$$pgcd(a, b) = r_n = r_{n_2} - q_nr_{n-1} = s_1r_{n-2} + t_1r_{n-1} \quad avec\ \ s_1 = 1, t_1 = -q_n$$

Ensuite, on utilise $r_{n-3} = r_{n-2}q_{n-1} + r_{n-1} \Leftrightarrow r_{n-1} = r_{n-3} - q_{n-1}r_{n-2}$

$$\begin{aligned} Donc,\ \ pgcd(a, b) &= s_1r_{n-2} + t_1(r_{n-3} - q_{n-1}r_{n-2}) = t_1r_{n-3} + (s_1 - q_{n-1}t_1)r_{n-2} \\ &= s_2r_{n-3} + t_2r_{n-2} \quad avec\ \ s_2 = t_1, t_2 = s_1 - q_{n-2}t_1 \end{aligned}$$

Inductivement, on construit $s_k = t_{k-1}$ et $t_k = s_{k-1} - t_{k-1}q_{n-(k-1)}$ tel que pgcd(a,b) = $s_kr_{n-(k+1)} + t_kr_{n-k}$
$\Rightarrow pgcd(a, b) = pgcd(r_{-1}, r_0) = s_nr_{-1} + t_nr_0 = s_na + t_nb$ *avec* $s_n = t_{n-1}$ *et* $t_n = s_{n-1} - t_{n-1}q_1$

2.2 Groupes, anneaux et entiers modulo n

2.2.1 Définitions

Les groupes apparaissent naturellement dès qu'on parle des symétries d'un objet.

Définition 25
Un groupe $(G, *)$ est un ensemble non vide G muni d'une loin de composition $* : G \times G \to G$ tel que :

*(i) * soit associative*

(ii) $\exists e \in G : g * e = g = e * g$ (e est appelé le neutre)

(iii) $\forall g \in G : \exists g^{-1} \in G$ tq $g * g^{-1} = e = g^{-1} * g$

Exemple

1. $(\mathbb{Z}, +)$ *est un groupe*
2. $(\mathbb{Z}_0, \cdot)$ *n'est pas un groupe*
3. $(\mathbb{R}, \cdot)$ *n'est pas un groupe*
4. $(\mathbb{R}_0, \cdot)$ *est un groupe*

Définition 26
Soit (G,) un groupe. Un sous-ensemble $H \subseteq G$ est un sous-groupe de G si (H,*) est un groupe. On note $H \leq G$ ou $(H, *) \leq (G, *)$*

Proposition 6
Soit (G,) un groupe.* $H \subseteq G$ *est un sous-groupe de* G *ssi :*

1. $e \in H$
2. $\forall g, h \in H : g * h^{-1} \in H$

Exemple
$2\mathbb{Z} = \{\ldots, -2, 0, 2, \ldots\} = \{2z | z \in \mathbb{Z}\}$ *est un sous-groupe de* $(\mathbb{Z}, +)$

$3\mathbb{Z} = \{\ldots, -3, 0, 3, \ldots\} = \{3z | z \in \mathbb{Z}\}$ *est un sous-groupe de* $(\mathbb{Z}, +)$

Proposition 7
Soit $S \subseteq \mathbb{Z}$ *un sous-ensemble non-vide tel que* $(S, +) \leq (\mathbb{Z}, +) \Rightarrow\ \exists\, k \in \mathbb{Z}$ *tel que* $S = k\mathbb{Z}$

Démonstration
Posons k *le plus petit entier positif dans* $S \Rightarrow k\mathbb{Z} \subseteq S$

Supposons que $\exists s \in S : s \notin k\mathbb{Z}$ *(on peut supposer* $s > 0$*)*

$\overset{DivEucl}{\Rightarrow} s = kq + r$ *avec* $0 < r < k$

$\Rightarrow r = s - kq \in S \Rightarrow$ *Incompatible avec le fait que k est le plus petit entier.*

Exemple
Interprétation du pgcd : Soit $k, l \in \mathbb{Z}$*. On définit* $k\mathbb{Z} + l\mathbb{Z} = \{kz_1 + lz_2 | z_1, z_2 \in \mathbb{Z}\}$*. On a* $k\mathbb{Z} + l\mathbb{Z} = pgcd(k, l)\mathbb{Z}$*.*

Démonstration

1) *Montrer que* $pgcd(k, l)\mathbb{Z} \subseteq k\mathbb{Z} + l\mathbb{Z}$ *: On sait que* $\exists s, t$ *tel que* $pgcd(k, l) = ks + lt \in k\mathbb{Z} + l\mathbb{Z}$*.*
2) *Montrer que* $k\mathbb{Z} + l\mathbb{Z} \subseteq pgcd(k, l)$ *: Soit* $z_1, z_2 \in \mathbb{Z}$ *et* $kz_1 + lz_2 \in k\mathbb{Z} + l\mathbb{Z}$*. Par définition du pgcd :* $\exists y_1, y_2$ *tel que* $k = pgcd(k, l)y_1,\ \ l = pgcd(k, l)y_2 \Rightarrow lz_1 + lz_2 = pgcd(k, l)(y_1 z_1 + y_2 z_2) \in pgcd(k, l)\mathbb{Z}$

2.2.2 Groupes quotients

Soit (G,+) un groupe commutatif. Dans ce cas, on note l'inverse de g, $\overline{g}$.

Définition 27
Soit $(N, +) \leq (G, +)$*. Une classe latérale de* N *est un ensemble* $g + N : \{g + n | n \in N\}$ *pour un élément fixé* $g \in G$*.*

Proposition 8
Deux éléments $g, g' \in G$ *dét. la même classe latérale de* N *ssi* $g + N = g' + N \Leftrightarrow \forall n \in N, \exists! n' \in N$ *tel que* $g + n = g' + n'$

Démonstration
$\Leftarrow$ *OK*

$\Rightarrow$

· $\forall n \in N : g + n \in g + N = g' + N \Rightarrow \exists n' \in N$ *tq* $g + n = g' + n'$
· *Unicité :* n' *et* n'' *tels que* $g' + n' = g' + n'' \Rightarrow g' + (-g') = n'' + (-n') \Rightarrow e = n'' + (-n') \Leftrightarrow n' = n''$

Définition 28
On note G/N l'ensemble de classe latérale de N. $G/N = \{g + N | g \in G\}$

Exemple
$(\mathbb{Z}, +)$ *et* $7 \in \mathbb{Z} : \mathbb{Z}/7\mathbb{Z} = \{0 + 7\mathbb{Z}, 1 + 7\mathbb{Z}, \ldots, 6 + 7\mathbb{Z}\}$ *que l'on note* $\{\overline{0}, \overline{1}, \ldots, \overline{6}\}$*. Remarque :* $\overline{7} = \overline{0}$

Proposition 9
Soit le groupe $(\mathbb{Z}, +)$ *et* $k \in \mathbb{Z}$*. Alors* $\mathbb{Z}/k\mathbb{Z}$ *est une partition de* $\mathbb{Z}$*.*

Démonstration

- $z \in \mathbb{Z} \Rightarrow \exists q, r \ tq \ z = kq + r \in r + k\mathbb{Z}$
- $r_1, r_2 \in \mathbb{Z}$ *: montrer que* $r_1 + k\mathbb{Z} \cap r_2 + k\mathbb{Z} \neq 0 \Leftrightarrow r_1 + k\mathbb{Z} = r_2 + k\mathbb{Z} \Leftrightarrow r_1 + kq_1 = r_2 + kq_2 \Leftrightarrow r_1 - r_2 = k(q_1 - q_2) \in k\mathbb{Z} \Leftrightarrow r_1 + k\mathbb{Z} = r_2 + k\mathbb{Z}$

Théorème 10
Soit $(G,+)$ *un groupe commutatif et* $N \leq G$*. Alors* G/N *est muni d'une loi* $\overline{+}$ *tel que* $(G/N, \overline{+})$ *soit un groupe commutatif. Précisément, on définit*

$$\forall g, g' \in G : \overline{g}\overline{+}\overline{g'} = \overline{g + g'} = (g + N)\overline{+}(g' + N) = g + g' + N$$

Démonstration

- *On montre que* $\overline{+}$ *est bien défini. C'est à dire :* g, g' *et* $h, h' \in G$ *tels que* $\overline{g} = \overline{h}$ *et* $\overline{g'} = \overline{h'}$*. Montrons que* $\overline{g + g'} = \overline{h + h'}$*.*
  $\overline{g} = \overline{h} \Rightarrow g - h = n, \quad n \in N$
  $\overline{g'} = \overline{h'} \Rightarrow g' - h' = n', \quad n' \in N$
  Donc, $g + g' - (h + h') = g + g' + (-h) + (-h') = (g - h) + (g' + h') = n + n' \in N$
  $\Rightarrow \overline{g + g'} = \overline{h + h'}$
- $\overline{+}$ *est associative car + l'est :* $\forall g, g', g''$
  $(\overline{g} \mathbin{\overline{+}} \overline{g'}) \mathbin{\overline{+}} \overline{g''} = \overline{g + g'} \mathbin{\overline{+}} \overline{g''} = \overline{(g + g') + g''}$
  $\overline{g} \mathbin{\overline{+}} (\overline{g'} \mathbin{\overline{+}} \overline{g''}) = \overline{g} \mathbin{\overline{+}} \overline{g' + g''} = \overline{g + (g' + g'')}$
- $\overline{+}$ *est commutative*
- *le neutre est* $\overline{e}$ *où* e *est le neutre de* $(G,+)$
- *L'inverse/opposé de* $\overline{g}$ *est* $\overline{-g}$

Définition 29 (et exemple principal)
Pour $n \in \mathbb{N}$*, on définit le groupe des entiers modulo* n *comme le groupe quotient* $(\mathbb{Z}/n\mathbb{Z}, +)$ *où* $\overline{a} + \overline{b} = \overline{a + b} \quad \forall a, b \in \mathbb{Z}$

Exemple
$\mathbb{Z}/8\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{7}\}$.

$\overline{0}$ *est neutre.*

$\overline{2} + \overline{3} = \overline{5}$

$\overline{6} + \overline{10} = \overline{16} = \overline{0}$

2.2.3 Isomorphismes de groupe

Définition 30
Soit $(G, *)$ *et* $(G', *)$ *deux groupes. Un morphisme de groupe est une application* $f : G \to G'$ *tel que* $\forall g, h \in G : f(g * h) = f(g) * f(h)$

Exemple

1) $(\mathbb{R}, +)$ *et* $(\mathbb{R}_0^+, \cdot)$ $\quad exp : \begin{matrix} \mathbb{R} \to \mathbb{R}_0^+ \\ x \to e^x \end{matrix}$

morphisme $e^{x+y} = e^x \cdot e^y$

2) $(\mathbb{R}_0^+, \cdot)$ *et* $(\mathbb{R}, +)$ $\quad exp : \begin{matrix} \mathbb{R}_0^+ \to \mathbb{R} \\ x \to log(x) \end{matrix}$

morphisme $log(x \cdot y) = log(x) + log(y)$

Définition 31
Un morphisme de groupe $f : G \to G'$ *est dit :*

Injectif : *Si* $\forall g_1, g_2 \in G : f(g_1) = f(g_2) \Rightarrow g_1 = g_2$

Surjectif : *Si* $\forall g' \in G : \exists g \in G$ *tq* $f(g) = g'$

Définition 32
Soit (G,) et* $(G', *')$ *deux groupes et* $f : G \to G'$ *un morphisme de groupe.*

- *L'image de f est l'ensemble Im(f) =* $\{g' \in G' | \exists g \in G : f(g) = g'\} \subseteq G'$
- *Le noyau de f est l'ensemble Ker(f)=* $\{g \in G | f(g) = e\} \subseteq G$

Proposition 10
Soient (G,) et* $(G', *')$ *deux groupes et* $f : G \to G'$ *un morphisme de groupe. Alors :*

1. *f est injectif* $\Leftrightarrow$ *Ker(f) =* $\{e\}$
2. *f est surjectif* $\Leftrightarrow$ *Im(f) =* G'

Définition 33
Soient (G,) et* $(G', *')$ *deux groupes. Un isomorphisme de groupe est un morphisme bijectif* $f : G \to G'$. *Ils sont dits isomorphes et on note* $(G, *) \cong (G', *')$

Théorème 11 (Théorème d'isomorphisme)
Soient (G,) et* $(G', *')$ *deux groupes commutatifs et f un morphisme de groupe surjectif :* $f : G \to G'$, *Im(f)* $= G' \Rightarrow G/Ker(f) \cong G'$

L'ordre d'un groupe et de ses éléments

Définition 34
Soit (G,) un groupe fini. L'ordre de G est le cardinal de G. On le note #G.*

Proposition 11
Soit (G,) un groupe et* $g \in G, g \neq e \Rightarrow < g >= \{g^k | k \in \mathbb{Z}\}$ *est un sous-groupe commutatif de G où :*

1. $g^0 = e$
2. $g^k = g * \ldots * g \qquad$ *si* $k \in \mathbb{N}_0$
3. $g^{-k} = (g^{-1})^k \qquad$ *si* $k \in \mathbb{N}_0$

Proposition 12
Soit (G,) un groupe fini et* $e \neq g \in G \Rightarrow \exists k \in \mathbb{N}_0 : g^k = e$

Définition 35
Soig (G,) un groupe et* $g \in G$*. On définit l'ordre de g et on note O(g) le plus petit nombre naturel non nul tel que* $g^{O(g)} = e$*. Si* $g^k \neq e, \forall k$ *: on pose* $O(g) = \infty$

2.2.4 Les anneaux

Définition 36
Un anneau $(A, +, \cdot)$ *est un ensemble non vide A muni de 2 lois de composition :* $+ : A \times A \to A \ \ (a, b) \to a + b$ *et* $\cdot : A \times A \to \ \ (a, b) \to a \cdot b$

1. *(A,+) est un groupe commutatif*
2. *La multiplication est associative : (ab)c = a(bc),* $\forall a, b, c \in A$.
3. *La multiplication est distributive : (a+b)c = ac + bc et a(b+c)= ab + ac,* $\forall a, b, c \in A$.

Définition 37
Lorsque $\cdot$ *est commutative :* $(A, +, \cdot)$ *est un anneau commutatif.*
Si $\exists 1 \in A$ *tq* $a \cdot 1 = a = 1 \cdot a \quad \forall a \neq 0 \in A \Rightarrow (A, +, \cdot)$ *est un anneau unital.*

Exemple

1. $(\mathbb{Z}, +, \cdot)$ *anneau commutatif unital.*
2. $(M_2(\mathbb{R}) = \left(\begin{smallmatrix} ab \\ cd \end{smallmatrix} \right) | a, b, c, d \in \mathbb{R}, +, \cdot)$ *anneau unital (non commutatif)*

Proposition 13
Soit $k \neq 1 \in \mathbb{Z}_0$ *et soit le groupe* $(\mathbb{Z}/k\mathbb{Z}, \overline{+})$*. On définit* $\bar{\cdot} : \mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z} \to \mathbb{Z}/k\mathbb{Z}$ *tel que* $\forall l, l' \in \mathbb{Z} : \bar{l} \,\bar{\cdot}\, \bar{l'} = \overline{l\,l'}$*. Alors,* $(\mathbb{Z}/k\mathbb{Z}, \overline{+}, \bar{\cdot})$ *est un anneau commutatif unital.*

Démonstration
Il faut montrer que $\bar{\cdot}$ *est bien défini.*

$$l_1 \text{ et } l_2 \text{ tq } \overline{l_1} = \overline{l_2} \Rightarrow l_1 = l_2 + kz$$

$$l_1{}' \text{ et } l_2{}' \text{ tq } \overline{l_1{}'} = \overline{l_2{}'} \Rightarrow l_1{}' = l_2{}' + kz'$$

$$\Rightarrow l_2 \cdot l_2{}' = (l_1 - kz)(l_1{}' - kz') = l_1 l_1{}' - k l_1{}' z - k l_1 z' - kkz\overline{z}$$

$$\Rightarrow \overline{l_2 l_2{}'} = \overline{l_1 l_1{}'}$$

Les autres propriétés découlent des propriétés de + et $\cdot$ *dans* $\mathbb{Z}$.

Remarque : $\overline{1}$ *est neutre pour* $\bar{\cdot}$

Exemple
Dans $(\mathbb{Z}/10\mathbb{Z}, \overline{+}, \bar{\cdot})$ *:*

$\overline{1} \,\bar{\cdot}\, \overline{2} = \overline{2}$

$\overline{2} \,\bar{\cdot}\, \overline{5} = \overline{10} = \overline{0}$

Interprétation des pgcd, nombres premiers :

Définition 38
Soit $(A, +, \cdot)$ *un anneau :*

1. $a \in A$ *est inversible si* $\exists b \in A : ab = 1$
2. $a \in A$ *est un diviseur de 0 si* $\exists b \in A, b \neq 0 : ab = 0$

Exemple
Soient $0 < a \leq b < k \in \mathbb{N}_0$ *tels que* $ab = k$

$\Rightarrow \bar{a}$ *et* $\bar{b}$ *sont des div. de zéro dans* $\mathbb{Z}/k\mathbb{Z}$

Proposition 14 (ATTENTION ! Cette proposition fait partie de ceux à connaitre par coeur à l'examen ! (pour l'année 2015-2016))
Soit $k \in \mathbb{N}_0, k > 1$ *et soit* $l \in \mathbb{Z}$ *alors :* $\bar{l}$ *est inversible dans* $\mathbb{Z}/k\mathbb{Z} \Leftrightarrow l$ *et* k *sont premiers entre eux.*

Démonstration
$\Leftarrow$ *: pgcd(l,k) = 1* $\Rightarrow \exists s, t \in \mathbb{Z} : sl + tk = 1$. *Donc,* $\overline{sl + tk} = \bar{1} \Rightarrow \overline{sl} = \bar{1} \Rightarrow \bar{s} \cdot \bar{l} = \bar{1}$

$\Rightarrow$ *:* $\exists s \in \mathbb{Z}$ *tel que* $\bar{l} \cdot \bar{s} = \bar{1} \Leftrightarrow \exists t \in \mathbb{Z} : ls = 1 + kt \Rightarrow sl + (-t)k = 1 \overset{Bezout}{\Rightarrow} k$ *et* l *sont premiers entre eux.*

Exemple
Dans $\mathbb{Z}/5\mathbb{Z} : \bar{2}$ *est inversible* $(\bar{2} \cdot \bar{3} = \bar{1})$

Dans $\mathbb{Z}/6\mathbb{Z} : \bar{2}$ *n'est inversible et* $(\bar{2} \cdot \bar{3} = \bar{0})$

Définition 39
$(K, +, \cdot)$ *est un champ si* $(K, +, \cdot)$ *est un anneau commutatif unital et si tout élément non nul de* K *admet un inverse pour la multiplication.*

Proposition 15
Soit $k \in \mathbb{N}_0, k > 1$, *alors :* $\mathbb{Z}/k\mathbb{Z}$ *est un champ ssi* k *est un nombre premier.*

Démonstration
(SUPER LONG)

2.2.5 Relation de congruence

Définition 40
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* $\bar{a} = \bar{b}$ *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
$\forall n \in \mathbb{N} : (n+1)^p \equiv n^p + 1 (mod\ p)$ si p est un nombre premier.

Théorème 12 (Le petit théorème de Fermat (ATTENTION ! Ce théorème, le lemme le précédent, et leurs démonstrations mutuelles font partie de ceux à connaitre par coeur à l'examen ! (pour l'année 2015-2016)))
Soit $p \in \mathbb{N}$ un nombre premier.
Soit $a \in \mathbb{N}$ un nombre tel que $p \not| a$ (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

$$(n+1)^p = \sum_{i=0}^{p} \binom{p}{i} n^i = n^p + \sum_{i=0}^{p-1} \binom{p}{i} n^i + 1 = n^p + 1 + \sum_{i=1}^{p-1} \binom{p}{i} n^i (mod\ p)$$

Par récurrence sur i : on va montrer que $p | \binom{p}{i}$ pour $i = 1, \ldots, (p-1)$. i=1 : $\binom{p}{1} = p$ et $p|p$

Supposons que $p | \binom{p}{i}$ pour $1 \leq i < p-1$ et montrons que $p | \binom{p}{i+1}$

$$\binom{p}{i+1} = \frac{p!}{(i+1)!(p-i-1)} = \binom{p}{i} \frac{(p-i)}{(i+1)}$$

$$p | \binom{p}{i} \Rightarrow \binom{p}{i} = pb \text{ pour } b \in \mathbb{Z} \Rightarrow \binom{p}{i+1} = \frac{pb(p-i)}{(i+1)} \in \mathbb{N}$$

p premier et $1 < i+1 \leq p+1$

$$\Rightarrow (i+1) | b(p-i) \qquad (\text{ car } \ (i+1) \not| p)$$

$$\Rightarrow \binom{p}{i+1} = p \cdot \frac{b(p-i)}{i+1} \Rightarrow p | \binom{p}{i+1}$$

$$\Rightarrow \binom{p}{i} = 0 (mod\ p) \qquad \text{pour } \ i = 1, \ldots, p-1$$

$$\Rightarrow (n+1)^p = n^p + 1 (mod\ p)$$

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 $\in \mathbb{N}$, $p \neq q$, 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)

Théorème 13
$\forall 0 < M < N = pq \in \mathbb{Z}$, p et q premiers. Soit $u = 1(O(N))$. Alors $M^u = M(mod\ N)$.

Démonstration
$O < M < N \Rightarrow p \not| M$ *ou* $q \not| M$

Cas 1 $p \not| M$ *et* $q \not| M$ $\quad u = 1 + tO(N) = 1 + t(p-1)(q-1) \Rightarrow M^u = M + M^{t(p-1)(q-1)}$ *Or, par le petit théorème de Fermat :*

$$(M^{t(p-1)})^{q-1} = 1(mod\ q)$$
$$(M^{t(q-1)})^{p-1} = 1(mod\ p)$$
$$\Rightarrow \begin{cases} M^u = M(mod\ q) \\ M^u = M(mod\ p) \end{cases} \Rightarrow \begin{cases} M^u - M = 0(mod\ q) \\ M^u - M = 0(mod\ p) \end{cases}$$
$$ie\ p|M^u - M\,et\,q|M^u - M \Rightarrow pq|M^u - M$$
$$\Rightarrow M^u - M = 0(mod\ N)$$
$$\Rightarrow M^u = M(mod\ N)$$

Cas 2 $p|M$ *et* $q \not| M$ $\quad u = 1 + t(p-1)(q-1)$

$$q \not| M \xrightarrow[de\ Fermat]{Petit\ Thrm} (M^{t(p-1)})^{q-1} = 1(mod\ q)$$
$$\Rightarrow M^{t(p-1)(q-1)} = 1 + lq\ pour\ un\ l \in \mathbb{Z}$$
$$Donc,\ M^u = MM^{t(p-1)(q-1)} = M(1 + lq)$$
$$p|M \Rightarrow \exists c \in \mathbb{Z} : pc = M$$
$$\Rightarrow M^u = M(1 + lq) = pc(1 + lq) = pc + lpcq = M + lcpq$$
$$\Rightarrow M^u = M(mod\ N)$$

Cas 3 $p \not| M$ *et* $q|M$ *(exo à faire chez soi)*

3 Suite

Pour la suite, voir le syllabus de l'année passée. Il faut étudier les 3 premiers chapitres ("Comptage élémentaire","Relations de récurrence" et "Fonctions génératrices")