MATH-F-307: Syllabus (étudiant) d'exercices

André Madeira Cortes
Nikita Marchant

Table des matières

1 Séance 1

Exercice 1. *Construisez un graphe simple et connexe sur* 8 *sommets tel que chaque sommet est contenu dans exactement trois arêtes. Pouvez-vous faire la même chose avec* 9 *sommets ?*

Exercice 2. *Dans un groupe de personnes, il y a toujours deux individus qui connaissent exactement le même nombre de membres du groupe.*

1. *Formalisez cette propriété dans le vocabulaire des graphes.*
2. *Démontrez cette propriété (par l'absurde).*

Exercice 3. *Soit $n \geq 2$ et soit G un graphe simple avec $2n$ sommets et $n^2 + 1$ arêtes. Montrez que G contient un triangle.*

Exercice 4. *Soit G un graphe simple avec $2p$ sommets. On suppose que le degré de chaque sommet est au moins égal à p. Démontrez que ce graphe est connexe.*

Exercice 5. *Soit G un graphe simple.*

1. *On suppose que G est connexe et que x est un sommet de G de degré* 1. *Prouvez que $G \setminus \{x\}$ est connexe.*
2. *Déduisez-en que, si G est connexe et $|V(G)| = n \geq 2$, alors G contient au moins $n - 1$ arêtes.*

Exercice 6. *Donnez un graphe simple et connexe sur au moins* 5 *sommets qui est :*

- *hamiltonien et eulérien ;*
- *hamiltonien et non eulérien ;*
- *non hamiltonien et eulérien ;*
- *non hamiltonien et non eulérien.*

Exercice 7. *Le graphe 1 est-il isomorphe à un (ou à plusieurs) des graphes ci-dessous ?*

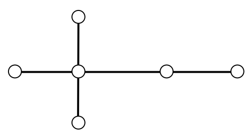

FIGURE 1

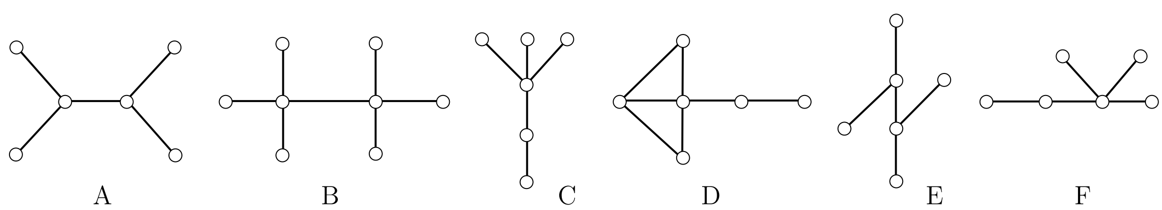

FIGURE 2

Exercice 8. *Les graphes suivants sont-ils isomorphes ? (Ne vous contentez pas d'une justification approximative : essayez de démontrer rigoureusement vos affirmations.)*

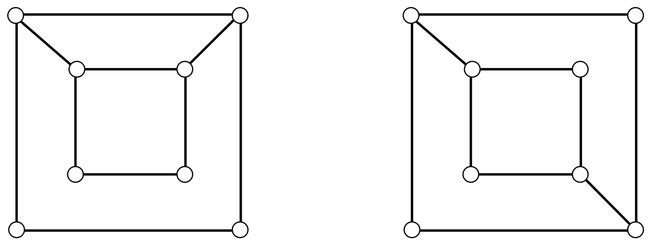

Figure 3

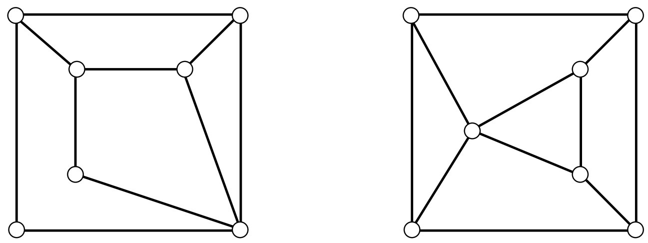

Figure 4

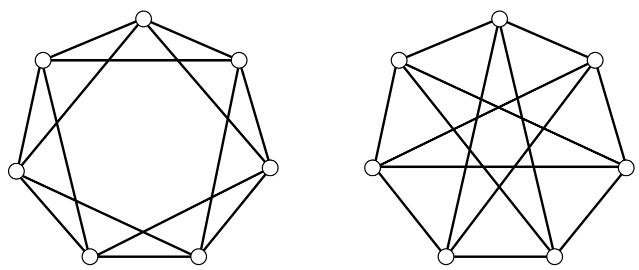

Figure 5

2 Séance 2

Exercice 9. *Considérez la grille $n \times n$, le graphe obtenu selon la Figure 6, avec n un naturel ≥ 3. Démontrez que n est pair si et seulement si le graphe est hamiltonien.*

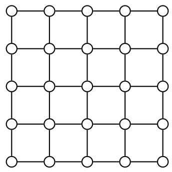

FIGURE 6 – Grille 5×5.

Exercice 10. *Prouvez que pour tout $n \geq 3$, le graphe complet K_n possède exactement $\frac{1}{2}(n-1)!$ cycles hamiltoniens.*

Exercice 11. *Combien d'arbres couvrants possèdent les deux graphes de la Figure 7 ?*

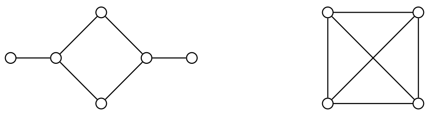

FIGURE 7

Exercice 12. *Montrez que tous les alcools $C_nH_{2n+1}OH$ sont des molécules dont le graphe est un arbre, en sachant que les valences de C, O et de H sont respectivement $4, 2, 1$.*

Exercice 13. *Démontrez que si un graphe hamiltonien $G = (V, E)$ est biparti selon la bipartition $V = A \cup B$, alors $|A| = |B|$. En déduire que $K_{n,m}$, le graphe biparti complet, est hamiltonien si et seulement si $m = n \geq 2$.*

Exercice 14. *Pour chaque graphe de la Figure 8, déterminez si*

1. *le graphe est hamiltonien,*
2. *le graphe est eulérien,*
3. *le graphe est biparti.*

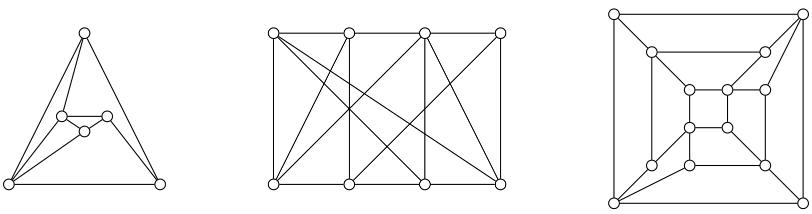

FIGURE 8

3 Séance 3

Exercice 15. *Construisez un code de Gray d'ordre 5 sur base du code de Gray d'ordre 4 ci-dessous.*
0000,0100,1100,1000,1010,1110,0110,0010,0011,0111,1111,1011,1001,1101,0101,0001

Exercice 16. *Dans le graphe ci-dessous, on donne un couplage de cardinal maximal. En utilisant la preuve du théorème de König vue au cours, trouvez un transversal de cardinal minimal.*

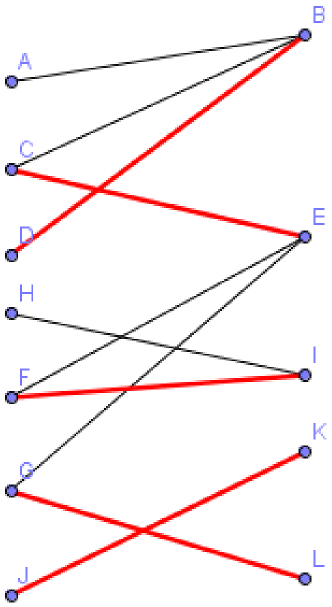

FIGURE 9

Exercice 17. *Sur* $\mathbb{R}^2$*, on définit les relations suivantes :*

$$(x, y)\mathcal{R}(x', y') \Leftrightarrow x \leq x' \text{ et } y \leq y',$$

$$(x, y)\mathcal{S}(x', y') \Leftrightarrow (x < x') \text{ ou } (x = x' \text{ et } y \leq y').$$

Est-ce que les relations $\mathcal{R}$ *et* $\mathcal{S}$ *sont des ordres ?*

Exercice 18. *Considérons le graphe biparti (bipartition donnée par une coloration des sommets) ci-dessous. Sur l'ensemble de ses sommets, on définit la relation $u \leq v$ pour u, v des sommets tels que u est un sommet rouge et $\{u, v\}$ est une arête. On pose aussi $u \leq u$ pour tout sommet u.*

(a) Vérifiez que $\leq$ est un ordre partiel.

(b) Construisez une partition des sommets par k chaînes et trouvez une antichaîne contenant k éléments.

(c) Déduisez-en un couplage de cardinalité maximale et un transversal de cardinalité minimale.

(d) (Bonus) Sur base de ce qui est fait ci-dessus, prouvez que le théorème de König implique le théorème de Dilworth.

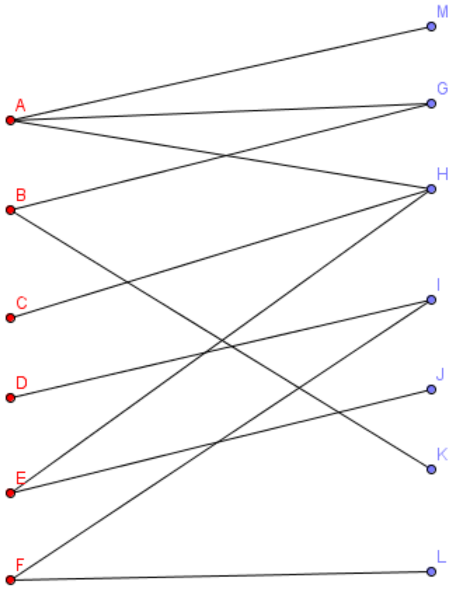

FIGURE 10

4 Séance 4

Exercice 19. *L'ensemble* $\{2^m | m \in \mathbb{Z}\}$ *forme-t-il un groupe lorsqu'il est muni de la multiplication usuelle ?*

Soit $X = 2^m, m \in \mathbb{Z}$ et $(X, .)$ le groupe à analyser.

$\forall x, y \in \mathbb{Z} : 2^x * 2^y = 2^{x+y} \in X$ car $(x+y) \in \mathbb{Z}$. L'ensemble X forme donc bien un groupe lorsqu'il est muni de la multiplication.

Exercice 20. *L'ensemble* $(\mathbb{Z}/2\mathbb{Z})^n = \{(x_1, x_2, \ldots, x_n) | x_1, x_2, \ldots, x_n \in \mathbb{Z}/2\mathbb{Z}\}$ *avec l'addition définie par*

$$(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$$

(où $x_i + y_i$ *est le résultat d'une addition modulo* 2*) forme-t-il un groupe ?*

Il faut tester si les 3 propriétés d'un groupe sont respectées.

1. Associativité : Chaque composante est calculée avec la forme $x_i + y_i, \forall i \in \{1, 2, ..., n\}$. $\mathbb{Z}_2$ est associatif, l'adition est faite composante par composante, donc Z_2^n est associatif. Il faut donc à présent montrer que $(x_i + y_i) + z_i = x_i + (y_i + z_i)$.

Exercice 21. *En appliquant l'algorithme d'Euclide à a et b ci-dessous, calculer :*
- *le PGCD*(a, b)*,*
- x *et* y *tels que* $ax + by = PGCD(a, b)$*,*

Les différentes valeurs de a et b sont :

(i) $a = 12, b = 34$,

(ii) $a = 13, b = 34$,

(iii) $a = 13, b = 31$,

Exercice 22. *(i) Trouver un entier* x *tel que le reste de la division de* $50x$ *par* 71 *donne* 1.

(ii) Trouver un entier x *tel que le reste de la division de* $50x$ *par* 71 *donne* 63.

(iii) Trouver un entier x *tel que le reste de la division de* $43x$ *par* 64 *donne* 1.

Exercice 23. *Dans le système RSA, prenons* $p = 11$, $q = 13$ *et* $e = 7$. *Que vaut alors s ? Si* 99 *est le message à coder, quel est le message crypté ? Vérifier en décriptant le message.*

5 Séance 5

Exercice 24. *Montrer le résultat suivant : si* $a \equiv b \ (mod\ n)$ *et* $c \equiv d \ (mod\ n)$*, alors*

$$a + c \equiv b + d \ (mod\ n) \text{ et } a.c \equiv b.d \ (mod\ n).$$

$a \equiv b \ (mod\ n) \Rightarrow b - a = kn \qquad c \equiv d \ (mod\ n) \Rightarrow d - c = ln$

Exercice 25. *Montrer que, si* $a \equiv b \ (mod\ n)$*, alors*

$$a + c \equiv b + c \ (mod\ n) \ \forall c \in \mathbb{Z}$$

et

$$a.c \equiv b.c \ (mod\ n) \ \forall c \in \mathbb{Z}.$$

Exercice 26. *Prouver que, si* $a \equiv b \ (mod\ n)$*, alors* $a^k \equiv b^k \ (mod\ n)$ *pour tout entier* $k > 0$.

$a^k \equiv b^k \ (mod\ n) \Rightarrow b^k - a^k = xn \Leftrightarrow ln(b^k - a^k) = ln(xn) \Leftrightarrow \frac{ln(b^k)}{ln(a^k)} = ln(xn) \Leftrightarrow \frac{\cancel{k}ln(b)}{\cancel{k}ln(a)} = ln(xn) \Leftrightarrow ln(b) - ln(a) = ln(xn) \Leftrightarrow b - a = xn \Rightarrow a \equiv b \ (mod\ n)$

Exercice 27. *Trouver toutes les solutions aux congruences suivantes :*

- $2x \equiv 3 \ (mod\ 4)$ *avec* $x \in \mathbb{Z}/4\mathbb{Z}$ *;*
- $2x \equiv 2 \ (mod\ 4)$ *avec* $x \in \mathbb{Z}/4\mathbb{Z}$ *;*
- $2x \equiv 3 \ (mod\ 5)$ *avec* $x \in \mathbb{Z}/5\mathbb{Z}$.

Que pouvez-vous en déduire ?

Exercice 28. *Soient* a, b *deux entiers. Montrer que*

$$a\mathbb{Z} \cap b\mathbb{Z} = ppcm(a, b)\mathbb{Z}$$

et

$$a\mathbb{Z} + b\mathbb{Z} = pgcd(a, b)\mathbb{Z}.$$

Sous-question 1 :

Soit $m = ppcm(a, b)$. Nous pouvons en déduire 3 propriétés :

1. $\frac{a}{m}$
2. $\frac{b}{m}$
3. si $\frac{a}{z}$ et $\frac{b}{z}$, alors $\frac{m}{z}$

Nous voulons donc prouver que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. Pour ce faire, nous devons montrer que l'un est inclus dans l'autre, et vice-versa.

($\subseteq$) Soit $z \in a\mathbb{Z} \cap b\mathbb{Z}$, i.e. $\exists k, k' \in \mathbb{Z}$ $\quad z = ak = bk' \Leftrightarrow \frac{a}{z}$ et $\frac{b}{z}$

Montrer que $z \in m\mathbb{Z}$.
Par la propriété 3, $\frac{m}{z} \Leftrightarrow z \in m\mathbb{Z}$

($\supseteq$) Soit $z \in m\mathbb{Z}$, i.e. $\frac{m}{z}$

Montrer que $z \in a\mathbb{Z} \cap b\mathbb{Z}$, i.e. $\frac{a}{z}$ et $\frac{b}{z}$.

Par la propriété 1, $\frac{a}{m}$

$\frac{m}{z} \Rightarrow \frac{a}{z}$ et $\frac{b}{z}$

Par la propriété 2, $\frac{b}{m}$

Sous-question 2 :

Exercice 29. *Montrer que*

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \ncong \mathbb{Z}/9\mathbb{Z}$$

mais que

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}.$$