

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

André MADEIRA CORTES
Nikita MARCHANT

Table des matières

1	Séance 1	3
2	Séance 2	5
3	Séance 3	6
4	Séance 4	8
5	Séance 5	9
6	Séance 6 et 7	11

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 ?

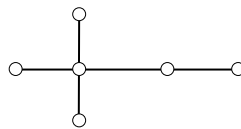


FIGURE 1

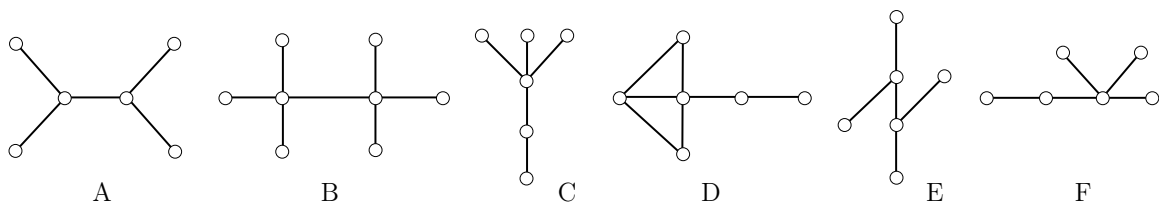


FIGURE 2

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

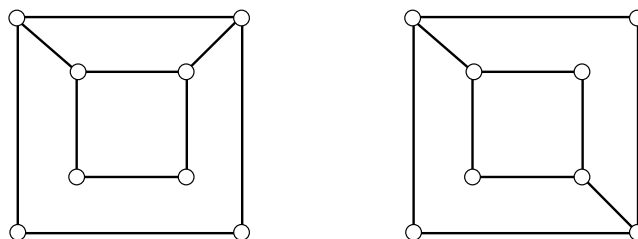


FIGURE 3

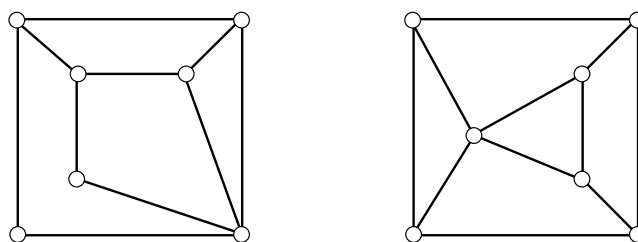


FIGURE 4

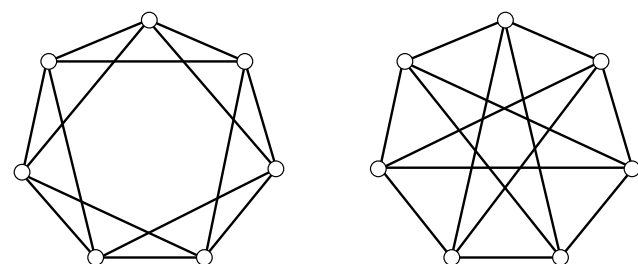


FIGURE 5

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.

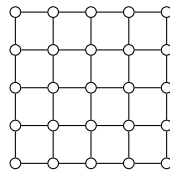


FIGURE 6 – Grille 5×5 .

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 ?

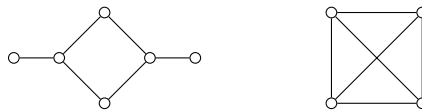


FIGURE 7

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.

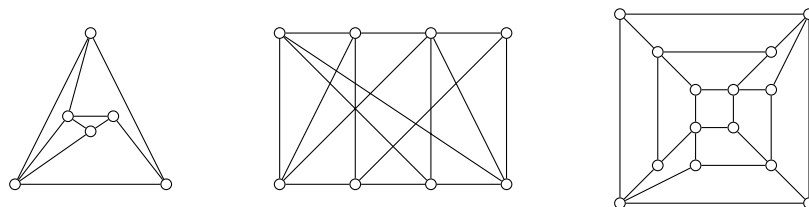


FIGURE 8

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.

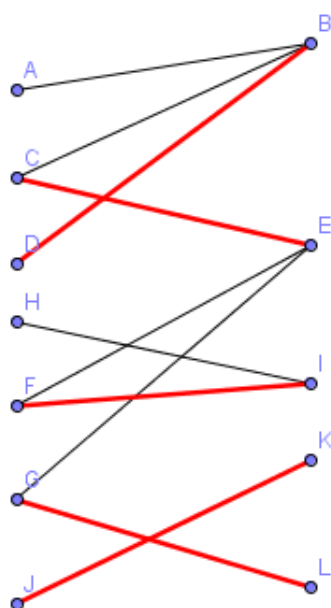


FIGURE 9

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 antichaine 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.

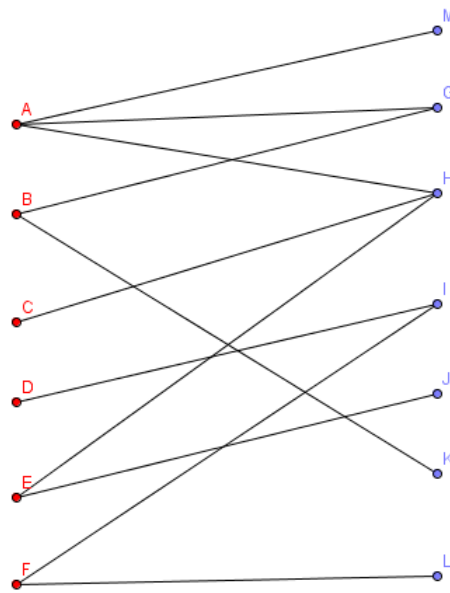


FIGURE 10

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 $(\mathbb{Z}/2\mathbb{Z})^n = \{(x_1, x_2, \dots, x_n) | x_1, x_2, \dots, x_n \in \mathbb{Z}/2\mathbb{Z}\}$ avec l'addition définie par

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

(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 $x_i + y_i, \forall i \in \{1, 2, \dots, n\}$. \mathbb{Z}_2 est associatif, l'addition est faite composante par composante, donc \mathbb{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 $ax + by = \text{PGCD}(a, b)$,

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 décryptant le message.

5 Séance 5

Exercice 24. Montrer le résultat suivant : si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors

$$a + c \equiv b + d \pmod{n} \text{ et } a.c \equiv b.d \pmod{n}.$$

$$a \equiv b \pmod{n} \Rightarrow b - a = kn \qquad c \equiv d \pmod{n} \Rightarrow d - c = ln$$

Exercice 25. Montrer que, si $a \equiv b \pmod{n}$, alors

$$a + c \equiv b + c \pmod{n} \quad \forall c \in \mathbb{Z}$$

et

$$a.c \equiv b.c \pmod{n} \quad \forall c \in \mathbb{Z}.$$

Exercice 26. Prouver que, si $a \equiv b \pmod{n}$, alors $a^k \equiv b^k \pmod{n}$ pour tout entier $k > 0$.

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

Exercice 27. Trouver toutes les solutions aux congruences suivantes :

- $2x \equiv 3 \pmod{4}$ avec $x \in \mathbb{Z}/4\mathbb{Z}$;
- $2x \equiv 2 \pmod{4}$ avec $x \in \mathbb{Z}/4\mathbb{Z}$;
- $2x \equiv 3 \pmod{5}$ avec $x \in \mathbb{Z}/5\mathbb{Z}$.

Que pouvez-vous en déduire ?

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

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

et

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

Sous-question 1 :

Soit $m = \text{ppcm}(a, b)$. 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. $\exists k, k' \in \mathbb{Z} \quad z = ak = bk' \Leftrightarrow \frac{a}{z} \text{ et } \frac{b}{z}$

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, $\frac{a}{m}$

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

Par la propriété 2, $\frac{b}{m}$

Sous-question 2 :

Exercice 29. Montrer que

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \not\cong \mathbb{Z}/9\mathbb{Z}$$

mais que

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

6 Séance 6 et 7

Exercice 30. Soient A et B deux ensembles finis avec $|A| = a$ et $|B| = b$ ($a, b \in \mathbb{N}$). Que valent :

- (i) $|A \times B|$,
- (ii) $|B^A|$ où $B^A := \{f : A \rightarrow B\}$,
- (iii) $|\{f : A \rightarrow B : f \text{ est une injection de } A \text{ dans } B\}|$,
- (iv) $|\text{Sym } A|$ où $\text{Sym } A$ est l'ensemble des permutations de A .

- (i) $a \cdot b$
- (ii) b^a
- (iii) voir cahier
- (iv) $a!$

Exercice 31. Quels sont les ensembles F non vides ayant la propriété suivante :

- (i) pour tout ensemble X , $|F^X| = 1$?
- (ii) pour tout ensemble Y , $|Y^F| = 1$?

- (i) $|F| = 1$
- (ii) Ensemble vide (mais pas possible par énoncé)

Exercice 32. Soient $f : A \rightarrow B$ et $g : B \rightarrow C$ deux fonctions. Démontrer :

- (i) $g \circ f$ injective $\Rightarrow f$ injective ;
- (ii) $g \circ f$ surjective $\Rightarrow g$ surjective ;
- (iii) $g \circ f$ bijective $\Rightarrow (f$ injective et g surjective).

- (i) Si f non injective, deux éléments a_1 et a_2 différents de A vont être envoyés par f sur un élément b de B . De plus, ces deux éléments vont être envoyés par $g \circ f$ sur un même élément c de C , car $g(f(a_1)) = g(b) = c = g(b) = g(f(a_2))$
- (ii) On sait que $\forall c \in C, \exists a \in A$ tel que $g \circ f(a) = c$. On veut montrer que g est surjective. C'est à dire que $\forall c \in C, \exists b \in B$ tel que $g(b) = c$. Ceci est vérifié en prenant $b = f(a)$.
- (iii) Implication de (i) et (ii)

Exercice 33. Donner une preuve bijective de l'identité de somme parallèle $\binom{k}{k} + \binom{k+1}{k} + \dots + \binom{m}{k} = \binom{m+1}{k+1}$.

Exercice 34. Donner deux démonstrations de

$$\sum_{k=0}^n \binom{n}{k} = 2^n.$$

Exercice 35. Qu'obtient-on comme identité sur les coefficients binomiaux en écrivant

$$(x+y)^{2n} = (x+y)^n (x+y)^n ?$$

Exercice 36. Qu'obtient-on en dérivant la formule du binôme ?

Exercice 37. Trouver le nombre de solutions de l'équation $x+y+z+w=15$, dans les naturels.

Exercice 38. Combien l'équation

$$x+y+z+t+u=60$$

possède-t-elle de solutions entières (x, y, z, t, u) telles que

$$x > 0, \quad y \geq 9, \quad z > -2, \quad t \geq 0 \quad \text{et} \quad u > 10 ?$$

Exercice 39. Trouver le nombre de solutions de l'inéquation

$$x + y + z + t \leq 6$$

(i) dans les naturels ;

(ii) dans les entiers > 0 ;

(iii) dans les entiers, avec comme contraintes supplémentaires $x > 2$, $y > -2$, $z > 0$ et $t > -3$.

Exercice 40. Avec les lettres du mot *MISSISSIPPI*, combien peut-on écrire de mots différents de 11 lettres ?

$$1 \text{ M } 4 \text{ I } 4 \text{ S } 2 \text{ P} \text{ Mots de 11 lettres } (11!) / ((4!)(4!)(2!)(1!))$$

Exercice 41. Avec les lettres du mot

HUMUHUMUNUKUNUKUAPUAA

(“poisson” en hawaïen), combien peut-on écrire de mots différents de 21 lettres ne comprenant pas deux lettres *U* côte à côte ?

Faire mots de 12 lettres sans *U*. Rajouter proba de foutre les *U* dans les 13 places qui restent pour faire des mots de 21 lettres. Donc, $(13 \ 9)$ (13 chouk 9).

Exercice 42. Si $0 \leq m \leq n$, que vaut

$$\sum_{k=m}^n \binom{k}{m} \binom{n}{k} \quad ?$$

(Hint : essayer une preuve bijective.)

Exercice 43. Si on jette simultanément n dés identiques, combien de résultats différents peut-on obtenir ? (Deux résultats sont considérés comme équivalents s'ils ont le même nombre de 1, le même nombre de 2, ..., le même nombre de 6.)