



IUT DE LAVAL
DÉPARTEMENT INFORMATIQUE

Mathématiques Discrètes

- *Exercices* -

Yann Walkowiak¹
<http://www.univ-lemans.fr/~ywalko>
yann.walkowiak@univ-lemans.fr

1. Merci à Patricia Everaere et Serge Iovleff dont les documents m'ont aidé à rédiger ces exercices de TD.

Table des matières

1	Théorie des ensembles	1
1.1	Opérations sur les ensembles	1
1.2	Modélisation	3
1.3	Sujets d'I.E. et d'examen	4
2	Logique	7
2.1	Logique Propositionnelle	7
2.2	Logique des Prédicats	10
2.3	Récurrence	11
2.4	Algèbre de Boole	12
2.5	Circuits logiques combinatoires	12
2.6	Sujets d'I.E. et d'examen	13
3	Relations sur un ensemble	15
3.1	Relations binaires	15
3.2	Opérations sur les relations	16
3.3	Relations d'équivalence	17
3.4	Relations d'ordres	18
3.5	Sujets d'I.E. et d'examen	20
4	Arithmétique	23
4.1	Divisibilité et nombres premiers	23
4.2	Équations diophantiennes	24
4.3	Congruences	24
4.4	Cryptographie	26
4.5	Sujets d'I.E. et d'examen	26

Partie 1

Théorie des ensembles

1.1 Opérations sur les ensembles

Exercice 1.1 Décrire explicitement (en extension) les ensembles suivants :

- $A = \{x \in \mathbb{Z}, \text{ tel que } -2,8 < x < 4,5\}$
- $B = \{x \in \mathbb{R}, \text{ tel que } -2,8 < x < 4,5\}$
- $C = \{x \in \mathbb{N}, \text{ tel que } x + 5 = 2\}$
- $D = \{x \in \mathbb{N}, \text{ tel que } x \text{ impair et } x < 17\}$
- $E = \{x \in \mathbb{N}, \text{ tel que } 3 \text{ divise } x \text{ et } x \leq 24\}$
- $F = \{x \in \mathbb{N}, \text{ tel que } x \text{ divise } 18\}$
- $G = \{x \in \mathbb{N}, \text{ tel que } \frac{x}{8} \leq 1\}$

Exercice 1.2 Enumérer les éléments de $\mathcal{P}(E)$ si $E = \{a, b, c\}$.

Exercice 1.3 On donne les ensembles : $A = \{1, 3, 4\}$, $B = \{1, 2, 3, 4, 5, 6\}$, $C = \emptyset$, $D = \{3, 4, 5, 7\}$ et $E = \{4, 6, 8\}$.

1. Quels sont les inclusions parmi les ensembles A, B, C, D et E ?
2. Donner les éléments des ensembles : $A \cup B$, $A \cap C$, $B \cup D$, $B \cap A$, $E \cap (B \cup D)$, $(E \cap B) \cup D$, $(E \cup B) \cap D$, $E \cup (B \cap D)$.

Exercice 1.4 Imaginer un diagramme d'Euler-Venn représentant trois ensembles A , B et C tels que $A \cap B = A \cap C$ et $B \neq C$. Faire de même pour trois ensembles vérifiant $A \cup B = A \cup C$ et $B \neq C$.

Exercice 1.5 Soient A , B et C trois parties d'un référentiel E .

1. Vérifier à l'aide de diagrammes d'Euler-Venn les formules de De Morgan qui suivent :

$$\overline{A \cup B} = \overline{A} \cap \overline{B} \quad \text{et} \quad \overline{A \cap B} = \overline{A} \cup \overline{B}$$

2. Prouvez en utilisant les définitions du cours les équivalences suivantes (la deuxième équivalence se déduit de la première) :

$$\begin{aligned} A \subset B &\Leftrightarrow \overline{B} \subset \overline{A} \\ A = B &\Leftrightarrow \overline{A} = \overline{B} \\ A \subset B &\Leftrightarrow A \cap B = A \Leftrightarrow A \cap \overline{B} = \emptyset \end{aligned}$$

3. En utilisant les formules de De Morgan, déduire de ce qui précède les équivalences :

$$A \subset B \Leftrightarrow A \cup B = B \Leftrightarrow \overline{A} \cup B = E$$

Exercice 1.6 Démontrer, en utilisant les propriétés des opérations sur les ensembles, les égalités suivantes :

$$\begin{aligned} [(A \cup B) \cap C] \cup B &= B \cup (A \cap C) \\ [(A \cap B) \cup (\overline{A} \cap B \cap C)] \cap \overline{B} &= \emptyset \\ [\overline{A} \cup (B \cap C)] \cap (A \cup C) &= (\overline{A} \cup B) \cap C \end{aligned}$$

Exercice 1.7 Soient A , B et C trois parties d'un référentiel E . Simplifier graphiquement les expressions suivantes en utilisant un diagramme d'Euler-Venn. Vérifier votre résultat par le calcul.

$$\begin{aligned} (A \cap B) \cup (A \cap \overline{B} \cap \overline{C}) \cup (A \cap \overline{B} \cap C) & \quad (A \cup B \cup \overline{C}) \cap C \cap \overline{B} \\ A \cup (B \cap \overline{A}) \cup B \cup (\overline{B} \cap C) & \quad \overline{A \cup B \cup \overline{C}} \cap A \end{aligned}$$

Exercice 1.8

1. Prouver les implications suivantes :

$$\begin{aligned} A = B &\Rightarrow A \cup C = B \cup C \\ A = B &\Rightarrow A \cap C = B \cap C \end{aligned}$$

2. Les implications réciproques sont-elles vraies ? Sinon donner un contre-exemple.
3. Prouver l'implication suivante :

$$\left\{ \begin{array}{l} (A \cup C) \subset (B \cup C) \\ (A \cap C) \subset (B \cap C) \end{array} \right\} \Rightarrow A \subset B$$

4. En déduire l'équivalence :

$$\left\{ \begin{array}{l} (A \cup C) = (B \cup C) \\ (A \cap C) = (B \cap C) \end{array} \right\} \Leftrightarrow A = B$$

Exercice 1.9 On appelle différence symétrique de deux parties A et B d'un référentiel E et on note $A \Delta B$, l'ensemble des éléments qui figurent soit dans A , soit dans B , mais pas dans A et B à la fois.

1. Représentez l'ensemble $A \Delta B$
2. Etablir les relations suivantes :

$$\begin{aligned} \text{(a)} \quad A \Delta B &= \mathcal{C}_{A \cup B}(A \cap B) \\ \text{(b)} \quad A \Delta B &= [\mathcal{C}_A(A \cap B)] \cup [\mathcal{C}_B(A \cap B)] \\ \text{(c)} \quad (A \Delta B) \cap A &= [\mathcal{C}_A(A \cap B)] \\ \text{(d)} \quad \mathcal{C}_E(A \Delta B) &= (A \cap B) \cup \overline{A \cup B} \end{aligned}$$

Exercice 1.10

1. On considère trois ensembles quelconques A, B, C . Montrer à l'aide des propriétés ensemblistes que l'ensemble $D = [A \cup (\overline{B} \cap \overline{C})] \cap [(A \cap C) \cup B]$ peut s'écrire plus simplement $D = A \cap (B \cup C)$.
2. On suppose à présent que les ensembles A, B, C vérifient $B \cap \overline{C} = \emptyset$.
(a) Faire un diagramme de Venn représentant trois ensembles A, B et C tels que $B \cap \overline{C} = \emptyset$.
(b) Représenter l'ensemble D sur ce dessin, et donner une forme simplifiée de D dans ces conditions.

1.2 Modélisation

Exercice 1.11

1. A l'aide de la formule sur les cardinaux : $|A \cup B| = |A| + |B| - |A \cap B|$, déduire une formule analogue pour $|A \cup B \cup C|$.
2. On étudie une population de 100 étudiants. Parmi eux : 32 étudient la Médecine, 20 la Physique, 45 la Biologie. 15 étudient la Médecine et la Biologie, 7 la Médecine et la Physique, 10 la Physique et la Biologie. 30 n'étudient aucune de ces trois matières. Combien étudient les trois matières en même temps ? Combien étudient Médecine et Biologie, mais pas physique ? Combien étudient une seule matière ? Représenter la situation par un diagramme de Venn et répondre à ces questions.

Exercice 1.12 Soit E un ensemble, A, B, C trois parties de E et $D = (\bar{A} \cup B) \cap C$.

1. Exprimer $|D|$ en fonction de $|C|$, $|A \cap C|$, et $|A \cap B \cap C|$. A quoi est égal $|A \cup B \cup C| - |D|$? (rappel : $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$ et $|A \cap \bar{B}| = |A| - |A \cap B|$).
2. On interroge 100 enfants sur leur goûts alimentaires : 50 aiment les frites, 30 aiment le riz, 10 aiment le riz et les pâtes, 17 aiment les frites et le riz, 13 aiment les pâtes et les frites, 3 n'aiment ni les pâtes ni le riz ni les frites, 7 aiment le riz et les frites et les pâtes.
 - (a) Représenter la situation par un diagramme de Venn.
 - (b) Parmi les enfants qui aiment les frites, combien sont-ils à aimer le riz ou à ne pas aimer les pâtes ? En déduire le nombre d'enfants qui aiment les pâtes (on pourra utiliser la première partie de l'exercice).

Exercice 1.13 Un ethnologue publie un article sur une tribu où l'on apprend que :

- Tout membre de la tribu porte un collier ou une boucle d'oreille.
 - Tous les guerriers portent un collier.
 - Ceux qui ne sont pas des guerriers n'ont pas de boucle d'oreille.
 - Ceux qui portent un collier sont des guerriers mâles.
 - Les hommes ne préparent jamais les repas.
 - Les repas sont préparés à tour de rôle par tous les guerriers.
1. En utilisant les ensembles suivants, traduire chacune des phrases de l'article :
 - T : ensemble des membres de la tribu
 - C : ensemble des membres de la tribu portant un collier
 - B : ensemble des membres de la tribu portant des boucles d'oreilles
 - G : ensemble des guerriers de la tribu
 - H : ensemble des hommes de la tribu
 - R : ensemble des membres de la tribu qui préparent les repas
 2. Démontrer qu'il n'y a pas de guerriers dans cette tribu. En déduire que cette tribu n'existe pas (on pourra utiliser le fait que pour tout ensemble A et B : $(A \subset B) \Leftrightarrow (\bar{B} \subset \bar{A})$).

Exercice 1.14 Au musée, un visiteur fait les remarques suivantes :

1. Parmi les tableaux exposés, les toiles qui ont plus de 50 ans représentent des bateaux.
2. Les deux-tiers des tableaux non encadrés sont peints par des femmes.
3. Les bateaux peints par des femmes ont plus de 50 ans.
4. Un tableau sur trois a un cadre.
5. Les tableaux de plus de 50 ans ne sont pas encadrés.
6. La moitié des tableaux peints par des femmes ont plus de 50 ans.

7. Parmi les tableaux de moins de 50 ans, ceux qui sont peints par des hommes ont un cadre, et ceux qui sont peints par les femmes n'en ont pas.

Questions :

1. Montrer que les tableaux peints par des femmes ne sont pas encadrés.
2. En déduire le nombre de tableaux peints par des femmes en fonction du nombre de tableaux total, et qu'il y a au moins $\frac{2}{9}$ de tableaux de plus de 50 ans.

Exercice 1.15 A la bibliothèque, Marie a le choix entre des livres d'aventure, des livres parlant des extra-terrestres, des livres scientifiques et des bandes dessinées. Elle cherche un livre qui parle d'aventure ou des extra-terrestres, et qui ne soit pas une bande dessinée. Pour l'aider à faire son choix, elle apprend que parmi les livres disponibles :

- Tous les livres parlant des extra-terrestres parlent d'aventure.
- Aucune bande dessinée ne parle des extra-terrestres.
- Tous les livres parlant d'aventure et de science sont des bandes dessinées.
- Tous les livres scientifiques parlent d'aventure, mais aucun d'entre eux ne parle des extra-terrestres.
- La moitié des livres parlent d'aventure, et le tiers des livres d'aventure sont des bandes dessinées.

Dans la suite de l'exercice, on notera :

L : ensemble des livres disponibles A : ensemble des livres d'aventure
 E : ensemble des livres parlant d'extra-terrestres S : ensemble des livres scientifiques
 B : ensemble des bandes dessinées

1. Ecrire L en fonction des ensembles A, E, S et B .
2. Traduire les phrases par des relations entre les ensembles A, E, S et B .
3. Réaliser un diagramme de Venn représentant les ensembles L, A, E, S et B en tenant compte des relations de la question précédente.
4. Ecrire l'ensemble des livres correspondant au choix de Marie (on notera cet ensemble M). Montrer qu'on peut simplifier cette écriture et écrire M en fonction des ensembles A et B .
5. Déduire des questions 2) et 4) la proportion de livres disponibles qui peuvent convenir à Marie.

1.3 Sujets d'I.E. et d'examen

Exercice 1.16 On considère l'ensemble de référence $E = \{1, 2, 3, 4, 5, 6, 7, 8\}$ ainsi que les parties de E suivantes :

- $A = \{x \in E \mid x \text{ est un multiple de } 2\}$
- $B = \{x \in E \mid -1 \leq x - 4 \leq 1\}$
- $C = \{x \in E \mid x^2 - 3x + 2 = 0\}$

1. Sous quelle forme sont donnés les ensembles A, B et C ?
2. Les donner en extension. Faire un diagramme d'Euler-Venn décrivant la situation.
3. Donner les éléments des ensembles $A \cup B, A \cap B, A \cap C, A \cap B \cap C$ et $\overline{A \cap B \cap C}$.
4. En utilisant le diagramme d'Euler-Venn, donner sans justifier $|\overline{A}|, |B \cap \overline{C}|$ et $|\overline{A} \cap B \cap \overline{C}|$.
5. En utilisant une formule du cours, exprimer $|\overline{A} \cup (B \cap \overline{C})|$ en fonction de $|\overline{A}|, |B \cap \overline{C}|$ et $|\overline{A} \cap B \cap \overline{C}|$.
 En déduire le nombre d'éléments de l'ensemble $\overline{A} \cup (B \cap \overline{C})$.

Exercice 1.17 Vérifier l'égalité suivante sur un diagramme d'Euler-Venn

$$(A \cap B) \cup (A \cap B \cap C) \cup (B \cap C \cap \overline{A}) \cup (A \cap C) = (A \cap B) \cup (A \cap C) \cup (B \cap C)$$

puis la démontrer par le calcul.

Exercice 1.18 Harry va chez un disquaire de son quartier afin d'acheter un disque pour l'anniversaire de sa mère. Il cherche un disque de musique classique, sans guitare et avec une chanteuse.

Parmi le stock de disques :

- il y a une chanteuse dans $1/4$ des disques,
- il n'y a jamais de chanteuse dans les disques de reggae,
- les disques de musique classique ne comportent jamais de guitare,
- parmi les disques avec chanteuse mais sans guitare, $1/6$ sont des disques de musique classique,
- parmi les disques avec chanteuse, les $2/3$ comportent de la guitare.

On utilise les notations suivantes :

- S : Ensemble des disques en stock,
- F : Ensemble des disques avec chanteuse,
- C : Ensemble des disques de musique classique,
- R : Ensemble des disques de reggae,
- G : Ensemble des disques avec guitare,
- D : Ensemble des disques correspondant à la demande de Harry.

1. Donner une écriture ensembliste des constatations ci-dessus.
2. Représenter tous ces ensembles sur un diagramme d'Euler.
3. Utiliser la notion de cardinal d'un ensemble pour déterminer dans quelle proportion de son stock le disquaire trouvera le disque recherché par Harry.

Exercice 1.19 Une enquête est effectuée dans une classe d'IUT informatique afin de savoir quels systèmes d'exploitation sont utilisés sur les ordinateurs personnels des étudiants. Dans cette classe, il y a 28 étudiants et tous sauf 1 ont un ordinateur personnel. Les différents systèmes installés sont Linux (L), Mac OS (M) et Windows (W). On a recueilli les informations suivantes :

- 4 étudiants utilisent Mac OS, 18 utilisent Linux et 13 utilisent Windows ;
- 1 peut démarrer sous Mac OS ou Windows, 3 peuvent démarrer sous Mac OS ou Linux et 5 peuvent démarrer sous Windows ou Linux ;

1. Démontrer les résultats suivants :

(a) $\forall A, B, C$ sous-ensembles de E

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

(b) $\forall A, B$ sous-ensembles de E

$$|A \cap \overline{B}| = |A| - |A \cap B|$$

2. Combien d'étudiants ont un triple-boot Mac Os + Linux + Windows (on pourra utiliser un des résultats ci-dessus) ?
3. Dessiner un diagramme d'Euler-Venn représentant la situation. Vous indiquerez le cardinal de chaque portion dessinée sans justifier.
4. On souhaite savoir combien d'étudiants n'utilisent pas Windows, mais utilisent soit Linux, soit Mac OS, soit les deux. On note D l'ensemble de ces étudiants.
 - (a) Représenter D par des hachures sur le diagramme.
 - (b) Exprimer D en fonction de M , L et $\overline{W}$.
 - (c) En déduire $|D|$.

Partie 2

Logique

2.1 Logique Propositionnelle

2.1.1 Introduction

Exercice 2.1 Le professeur Leblond parlait avec son assistant Lebrun et l'étudiant Leroux :

- Vous remarquerez que l'un d'entre nous est blond, que l'autre est brun et le troisième roux, dit celui qui a les cheveux bruns. Et pourtant aucun d'entre nous n'a un nom qui correspond à la couleur de ses cheveux ! Amusant, non ? - Tu as raison, dit le professeur.

De quelle couleur sont les cheveux de l'assistant ?

Exercice 2.2 On se trouve devant trois coffres dont l'un contient un trésor. Sur chaque coffre, il y a un message. Sur les deux premiers coffres, le message est : "le deuxième coffre est vide" ; sur le troisième coffre : "le premier coffre est vide". On sait que le message du coffre au trésor est vrai, et qu'il y a au moins un message faux. Où est le trésor ?

Exercice 2.3 Vous connaissez peut-être l'île de Puro Pira. Je vous rappelle brièvement comment elle était peuplée. Certains habitants appelés Purs disent toujours la vérité. D'autres appelés Pires mentent toujours. Ces deux catégories d'habitants sont les seules qui composent la population de l'île. Une étrange épidémie a balayé l'île de Puro Pira. Elle ne dura en tout et pour tout qu'une semaine, et a touché à peu près la moitié des habitants. Les effets de cette maladie étaient purement psychologiques. Tous ceux qui furent atteints virent leur rôle d'éternel menteur ou de sincère perpétuel s'inverser. Le fait que les Purs disent toujours la vérité et que les Pires mentent tout le temps n'était plus vrai. Au lieu de cela, les Purs malades se mirent à mentir systématiquement et les Pires malades se mirent à dire toujours la vérité. Durant cette étrange semaine, il y eut quatre types d'habitants à Puro Pira : les Purs malades, les Purs sains, les Pires malades et les Pires sains. Les Purs sains et les Pires malades disaient toujours la vérité, alors que les Purs malades et les Pires sains mentaient toujours. Ainsi donc, quand vous rencontriez un indigène qui vous faisait une affirmation que vous saviez fausse, en général vous ne pouviez pas savoir s'il s'agissait d'un Pur malade ou d'un Pire sain.

1. Pendant l'épidémie, un indigène dit "je suis un pur malade". Cet indigène est-il un Pur malade, un Pur sain, un Pire malade ou un Pire sain ?
2. Rappelons nous que le sorcier est un Pur et l'astrologue un Pire. Pendant l'épidémie, le sorcier a été épargné par la maladie, mais pas l'astrologue, de telle sorte qu'ils disent tous les deux la vérité. Le sorcier et l'astrologue se promenaient lorsqu'ils ont vu un indigène avancer vers eux. "Oh ! je le connais, dit l'astrologue au sorcier. Je peux vous dire si c'est un Pur ou un Pire mais pas s'il est malade." Lorsque l'indigène les croisa, il leur dit "Je suis un Pur sain". Alors l'astrologue confia au

sorcier : "Bien, maintenant je sais s'il est malade ou pas."
Cet indigène était-il un Pur ou un Pire, et était-il malade ?

Exercice 2.4

1. En admettant les propositions suivantes, que peut-on conclure ?
"Les informaticiens sont des gens heureux"
"Les armateurs ont de l'argent"
"Les gens qui ont de l'argent ne sont pas heureux"
2. De même (d'après Lewis CARROLL) :
"Les bébés sont illogiques"
"Personne n'est méprisé, qui soit capable de maîtriser un crocodile"
"Les gens illogiques sont méprisés"

2.1.2 Calcul propositionnel

Exercice 2.5 On considère les propositions suivantes : p : "Alain aime Marie" et q : "Marie aime Alain".

Traduire par une phrase les propositions :

1. $\neg p$
2. $(\neg q) \rightarrow p$
3. $(\neg p) \wedge (\neg q)$
4. $q \vee (\neg p)$

Exercice 2.6 On note respectivement p et q les propositions : "L'eau est chaude" et "L'eau est bleu turquoise". Ecrire avec les notations logiques les phrases suivantes :

- "L'eau est chaude et bleu turquoise"
- "L'eau n'est ni chaude, ni bleu turquoise"
- "Il est faux que l'eau soit chaude ou bleu turquoise"
- "L'eau est chaude ou froide et bleu turquoise"

Que peut-on dire de la dernière phrase ?

Exercice 2.7 Les propositions suivantes sont-elles vraies ou fausses ?

- "3 est pair et la somme des angles d'un triangle vaut 180° "
- "2 est pair implique que $\pi \simeq 3,14$ "
- "3 est pair implique que $\pi \simeq 3,14$ "
- "Il n'est pas vrai qu'un nombre entier impair ne puisse pas être divisible par 6"

Exercice 2.8 Ecrire dans un français intelligible la négation des propositions suivantes :

- "Le nombre 342 n'est pas divisible par 3 mais il est multiple de 17"
- "Si tu es plus lourd que l'air alors tu ne voleras pas"
- "Si I est un intervalle et si f est continue sur I , alors f a une primitive sur I "

Exercice 2.9 Donner la table de vérité des propositions suivantes :

1. $(\neg p) \vee (p \wedge q)$
2. $(\neg p \rightarrow \neg q)$
3. $\neg p \leftrightarrow (p \wedge q)$
4. $(p \wedge q) \rightarrow (\neg q)$

5. $[p \vee (\neg q)] \rightarrow [(p \vee r) \leftrightarrow (q \vee r)]$
6. $[(p \vee r) \leftrightarrow (q \vee r)] \rightarrow (p \leftrightarrow q)$

Exercice 2.10

1. Les propositions suivantes sont-elles des antilogies, des tautologies, ou ni l'un, ni l'autre ?
 - $(p \wedge q) \rightarrow q$
 - $p \rightarrow (p \rightarrow q)$
 - $p \wedge (p \rightarrow q) \wedge \neg q$
2. Que peut-on dire de p si :
 - $p \Rightarrow F$
 - $p \Rightarrow V$
 - $F \Rightarrow p$
 - $V \Rightarrow p$
3. Dans chacun des cas suivants, déterminer si les deux formules propositionnelles sur la même ligne sont égales :

– $p \rightarrow (q \rightarrow r)$	$(p \rightarrow q) \rightarrow r$
– $\neg p$	$[\neg(p \vee q)] \vee [(\neg p) \wedge q]$

Exercice 2.11 Démontrer que $P \Rightarrow Q$ avec

$P = \text{“à partir de 4 tout nombre pair est la somme de deux nombres premiers”}$

$Q = \text{“à partir de 7 tout nombre impair est la somme de trois nombres premiers”}$

Que peut-on en conclure ?

Exercice 2.12 Le but de cet exosol est de mettre en évidence que l'ensemble des connecteurs logiques peut s'exprimer à l'aide du connecteur unaire $\neg$ et d'un seul connecteur binaire, qu'on dira de référence.

1. $\wedge$ de référence : écrire sous forme logiquement équivalente, en vous servant uniquement des connecteurs $\neg$ et $\wedge$ chacune des expressions logiques suivantes :
 - $p \vee q$
 - $p \rightarrow q$
 - $p \leftrightarrow q$
2. Même énoncé en se servant des connecteurs $\neg$ et NAND ($\text{NAND}(p, q) = \neg(p \wedge q)$).

2.1.3 Modélisation

Exercice 2.13 Un homme qui semble divaguer déclare à toute la clientèle d'un café :

1. Le jour où je ne bois pas et où je dors, je ne suis pas content.
2. Le jour où je bois, je ne suis pas content et je dors.
3. Le jour où je ne mange pas, ou bien je ne suis pas content, ou bien je dors ou les deux.
4. Le jour où je mange, ou bien je suis content, ou bien je bois ou les deux.
5. Le jour où il ne pleut pas et où je suis content, je ne mange pas.
6. Aujourd'hui, je suis content.

A-t-il bu ? mangé ? dormi ? Quel temps fait-il ?

Exercice 2.14 Dans une boîte, il y a des objets qui sont :

- des cubes ou des sphères,
- verts ou noirs,
- petits ou grands,
- en bois ou en fer.

On sait d'autre part que :

- ceux en fer sont grands,
- les verts sont des cubes,
- il n'y a pas de petits cubes verts,
- tous les objets sont cubiques, ou verts, ou petits et noirs.

1. Y a-t-il des petits objets verts dans cette boîte ?
2. Décrire succinctement le contenu de la boîte.

Exercice 2.15 Trois collègues, Albert, Bernard et Charles déjeunent ensemble chaque jour ouvrable. Les affirmations suivantes sont vraies :

1. Si Albert commande un apéritif, Bernard en commande un aussi.
2. Chaque jour, soit Bernard, soit Charles, mais pas les deux, commandent un apéritif.
3. Albert ou Charles, ou les deux, commandent chaque jour un apéritif.
4. Si Charles commande un apéritif, Albert fait de même

Que peut on en déduire ? Pouvait on arriver à la même conclusion en supprimant l'une des quatre affirmations ?

Exercice 2.16 La petite histoire ci-dessous est extraite d'un livre de logique. Expliquez d'abord pourquoi on peut voir cet exercice comme une recherche d'antilogie.

Pour constituer un club, on a énoncé le règlement suivant :

- Article premier : tout membre non écossais porte des chaussettes oranges.
- Article second : tout membre porte une jupe ou ne porte pas de chaussettes oranges.
- Article troisième : les membres mariés ne sortent pas le dimanche.
- Article quatrième : un membre sort le dimanche si et seulement s'il est écossais.
- Article cinquième : tout membre qui porte une jupe est écossais et marié.
- Article sixième : tout membre écossais porte une jupe.

Expliquer pourquoi ce club n'a jamais recruté de membre.

2.2 Logique des Prédicats

Exercice 2.17 Soient A et B deux parties de $\mathbb{N}$. Ecrire à l'aide de quantificateurs les propositions suivantes :

1. A est non vide
2. A est différent de $\mathbb{N}$
3. 5 est le plus petit élément de A
4. Tous les éléments de A sont impairs
5. Tous les éléments de A ne sont pas pairs
6. A est inclus dans B
7. A et B sont disjoints
8. Tous les éléments de B sont divisibles par 4

Exercice 2.18

- Exprimer les propositions suivantes à l'aide des deux quantificateurs, le référentiel étant l'ensemble des étudiants E.
 - Aucun étudiant n'a une taille supérieure ou égale à 2 m.
 - Certains étudiants ont une taille supérieure ou égale à 2 m.
 - Tous les étudiants ont une taille strictement inférieure à 2 m et supérieure ou égale à 1,50 m.
- Donner les négations de ces propositions.

Exercice 2.19 Soient f_1, f_2 , et f_3 trois fonctions de $\mathbb{R}$ dans $\mathbb{R}$. Traduire graphiquement les propriétés :

- $\forall i \in \{1, 2, 3\}, \exists a \in \mathbb{R}, f_i(a) = 1$
- $\exists i \in \{1, 2, 3\}, \forall a \in \mathbb{R}, f_i(a) = 1$
- $\exists a \in \mathbb{R}, \forall i \in \{1, 2, 3\}, f_i(a) = 1$
- $\forall a \in \mathbb{R}, \exists i \in \{1, 2, 3\}, f_i(a) = 1$

Exercice 2.20 On note $A = \{1, 2, 3, 4\}, B = \{-3, 0, 3\}$ et $C = \{-15, 0, 3\}$.

- Les propositions suivantes sont-elles vraies ou fausses ? La réponse est à justifier.
 - $\exists a \in A, \exists b \in B, a + b < 2$
 - $\forall a \in A, \forall b \in B, \exists c \in C, ab > c$
 - $\exists a \in A, \forall b \in B, \forall c \in C, a \geq b + c$
- Ecrire la négation de ces propriétés.

Exercice 2.21 Les propositions suivantes sont-elles vraies ou fausses ?

- $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x^2 - y < 0$
- $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, x^2 - y < 0$
- $\forall x \in \mathbb{R}, \exists y \in \mathbb{N}, \frac{x}{y} \in \mathbb{N}$
- $\forall x \in \mathbb{N}, \exists y \in \mathbb{R}, \frac{x}{y} \in \mathbb{N}$

2.3 Récurrence

Exercice 2.22 Démontrer les formules suivantes, où n est un entier naturel :

- $\forall n \geq 1, 1 + 3 + 5 + \dots + (2n - 1) = n^2$
- $\forall n \geq 1, 1^3 + 2^3 + 3^3 + \dots + n^3 = \frac{n^2(n+1)^2}{4}$
- $\forall n \geq 1, 1.(1!) + 2.(2!) + 3.(3!) + \dots + n.(n!) = (n + 1)! - 1$

Exercice 2.23 Que pensez-vous des raisonnements suivants ?

- Si j'ai 1 euro, je suis pauvre. Si je suis pauvre avec n euros, alors je suis pauvre avec $n + 1$ euros.
Conclusion : Quelle que soit la somme que je possède, je suis pauvre.
- Une personne quelconque a le même âge qu'elle-même. Si on admet que pour tout groupe de n personnes, ces personnes ont le même âge, cela est vrai pour tout groupe de $n + 1$ personnes (puisque si on compare l'âge de deux personnes de ce groupe, elles sont incluses dans un sous groupe de n personnes, et ont donc le même âge) Conclusion : Nous avons tous le même âge ?

2.4 Algèbre de Boole

Exercice 2.24 Soient a, b, c, d des éléments de l'algèbre de Boole B . Prouver les égalités suivantes et écrire leurs duales :

$$a + \overline{b.a} = 1 \quad (2.1)$$

$$\overline{a.b + \overline{a} + \overline{b}} = 0 \quad (2.2)$$

$$abc + ab\overline{c} + a\overline{b}c + a\overline{b}\overline{c} = a \quad (2.3)$$

$$a + c = a + \overline{a}bc(ad + c) + bc \quad (2.4)$$

$$\overline{(a + b)(b + c) + (c + d)(d + a)} = \overline{ac + bd} \quad (2.5)$$

$$(a + b)(b + c)(c + d)(d + a) = ac + bd \quad (2.6)$$

Exercice 2.25 Soient a, b, c des éléments de l'algèbre de Boole B et $e = abc + \overline{b}c + \overline{a}b$.

1. Ecrire $a.b$ en n'utilisant que les opérations addition et complémentation.
2. Ecrire $a + b$ en n'utilisant que les opérations produit et complémentation.
3. Ecrire e en n'utilisant que l'opération addition et la complémentation.
4. Ecrire e en n'utilisant que l'opération produit et la complémentation.

Exercice 2.26 a, b, c étant des éléments de l'algèbre de Boole B , prouver les implications suivantes et examiner leurs réciproques :

$$ab + \overline{c} = 0 \Rightarrow \overline{a}c + \overline{b}c = 1 \quad (2.7)$$

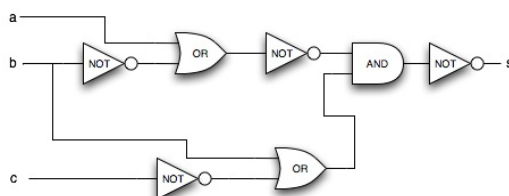
$$a = b + c \Rightarrow \overline{a} = \overline{a}b\overline{c} \quad (2.8)$$

Exercice 2.27 Soient a, b, c, d, e des éléments de B . Donner les décompositions canoniques disjonctives et conjonctives des expressions suivantes :

1. $f(a, b) = (a + b)\overline{a}b$
2. $f(a, b, c) = \overline{a}b\overline{c} + \overline{a}b$
3. $f(a, b, c) = \overline{(a + b + c)(\overline{a} + \overline{b} + \overline{c})}$
4. $f(a, b, c, d) = abcd + a\overline{d} + a\overline{b}\overline{c} + ab\overline{d}$
5. $f(a, b, c, d, e) = b\overline{c}d + \overline{a}d + \overline{c}e + ab\overline{c}d + \overline{a}$

2.5 Circuits logiques combinatoires

Exercice 2.28 Soit le circuit logique à 3 entrées a, b, c et une sortie s :



1. Déterminer s .
2. Construire un circuit logique équivalent comportant un minimum de portes :
 - (1) OU, ET, NON (2) Uniquement des portes NAND (3) Uniquement des portes NOR

Exercice 2.29 On donne $s = \overline{a}b + \overline{a}c + d$

1. Construire un circuit logique à 4 entrées, a, b, c, d et une sortie s , ne comportant que 4 portes de type OU, ET, NON.
2. Les 4 entrées sont maintenant liées par la relation $\overline{b} + \overline{c} = 1$. Simplifier s et donner un circuit logique qui réalise s et qui ne comporte que deux portes.

Exercice 2.30 Soit le montage électrique :

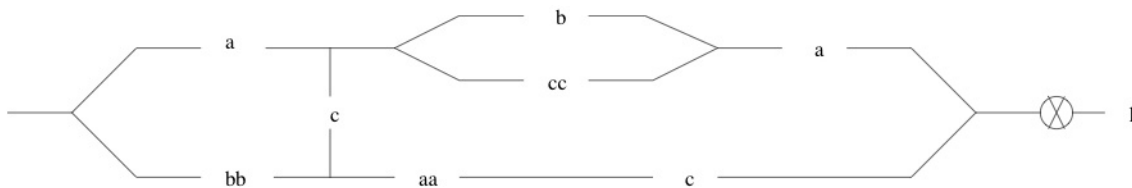


FIGURE 2.1 – a, b et c sont des interrupteurs

1. Exprimer la fonction l en fonction de a, b, c (sur le schéma, aa signifie $\overline{a}$).
2. Construire un circuit électrique réalisant la fonction de commande l et comportant un minimum d'interrupteurs.

Exercice 2.31 Réaliser un circuit ne contenant que des portes NOR, puis que des portes NAND pour représenter les fonctions suivantes :

$$f(a, b) = ab + \overline{a}\overline{b} \quad (2.9)$$

$$f(a, b, c) = ac(b + \overline{c}) \quad (2.10)$$

2.6 Sujets d'I.E. et d'examen

Exercice 2.32 Nier la proposition : “Si j’ai une moyenne au S1 supérieure ou égale à 10 et au-dessus de 8 dans les deux unités, alors je valide le semestre 1.”

Exercice 2.33 Donner la table de vérité de la proposition logique

$$\neg(p \vee q) \vee ((\neg p) \wedge q)$$

Donner une proposition logique équivalente ne faisant pas intervenir la variable q .

Exercice 2.34 Soient les 4 propositions logiques suivantes :

$$(a) \exists x \in \mathbb{R}, \forall y \in \mathbb{R}, \quad x + y > 0 \quad (b) \forall x \in \mathbb{R}, \exists y \in \mathbb{R}, \quad x + y > 0$$

$$(c) \forall x \in \mathbb{R}, \forall y \in \mathbb{R}, \quad x + y > 0 \quad (d) \exists x \in \mathbb{R}, \forall y \in \mathbb{R}, \quad y^2 > x$$

1. Les propositions logiques (a) , (b) , (c) et (d) sont-elles vraies ou fausses? (Justifier)
2. Donner leur négation.

Exercice 2.35 Soit $(\mathcal{B}, +, \cdot, -)$ une algèbre de Boole. On considère la fonction booléenne

$$f(a, b, c) = \bar{a}\bar{b}\bar{c} + ab + ab\bar{c} + ac + a\bar{b}$$

1. À l'aide d'un diagramme de Karnaugh, donner la décomposition canonique disjonctive de la fonction f .
2. Donner une simplification de la fonction f en regroupant les termes dans le diagramme de Karnaugh.
3. Dessiner un circuit logique implémentant la fonction f et ne comportant que 3 portes logiques.

Exercice 2.36 Soit E un ensemble. Montrer que, $\forall A, B \in \mathcal{P}(E)$

$$(A \cap B = A \cup B) \Leftrightarrow (A = B)$$

Partie 3

Relations sur un ensemble

3.1 Relations binaires

Exercice 3.1 Sur l'ensemble $S = \{1, 2, 3, 5\}$, on considère les relations suivantes :

- xRy ssi $x + y$ est impair
- xSy ssi $x \leq y$

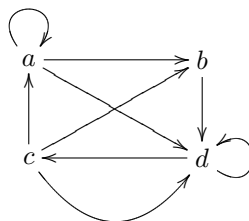
1. Représenter ces deux relations par une matrice et un graphe.
2. Quelles propriétés ont ces deux relations (parmi réflexive, symétrique, antisymétrique, transitive) ?
3. Donner la matrice et le graphe de $R \cap S$, $R \cup S$, $\bar{R}$, et S^t . Donner, si possible, une caractérisation de ces relations.

Exercice 3.2 Les relations suivantes sont-elles réflexives, symétriques, antisymétriques ou transitives ? (Réponses à justifier).

1. R_1 est définie sur l'ensemble $E = \{a, b, c, d\}$ par la matrice :

	a	b	c	d
a	1	1		1
b	1	1		
c	1	1	1	
d				1

2. R_2 est définie sur l'ensemble $E = \{a, b, c, d\}$ par le graphe :



3. Sur l'ensemble $E = \{1, 2, 3, 4, 5, 6\}$,

$$xR_3y \Leftrightarrow x \text{ divise } y$$

$$xR_4y \Leftrightarrow x \text{ est multiple de } y$$

Existe-il un lien entre R_3 et R_4 ?

4. Sur $\mathbb{N}$,

$$xR_5y \Leftrightarrow x - y \text{ est pair}$$

Peut-on exprimer autrement R_5 ?

5. Sur $\mathbb{R}$,

$$xR_6y \Leftrightarrow |x| = |y|$$

6. Sur $\mathcal{P}(E)$ (ensemble des parties d'un ensemble E) :

$$AR_7B \Leftrightarrow A \cap B = \emptyset$$

$$AR_8B \Leftrightarrow A \subset B$$

7. Sur $\mathbb{N}$:

$$xR_9y \Leftrightarrow \text{il existe } p \text{ et } q \text{ entiers, } q \neq 0, \text{ tels que } y = px^q$$

Exercice 3.3

1. Que peut-on dire d'une relation à la fois symétrique et antisymétrique ?
2. On dit qu'une relation R sur un ensemble E possède la propriété (P) si l'on n'a jamais à la fois xRy et yRx :
 - (a) Une telle relation est-elle antisymétrique ?
 - (b) Une relation antisymétrique a-t-elle la propriété (P) ?

3.2 Opérations sur les relations

Exercice 3.4

Sur $E = \{a, b, c\}$, définissons les relations

$$\begin{aligned}\mathcal{R} &= \{(a, a), (a, b), (b, c), (c, b)\} \\ \mathcal{S} &= \{(a, b), (b, c), (c, a)\}\end{aligned}$$

1. Donner les matrices et les graphes des relations $\mathcal{R}$ et $\mathcal{S}$.
2. Donner les matrices et les graphes des relations $\overline{\mathcal{R}}$, $\mathcal{R}^t$, $\mathcal{R} \cap \mathcal{S}$, $\mathcal{R} \cup \mathcal{S}$.
3. Pour chacune des relations ci dessus examinez les propriétés suivantes : **réflexivité** (R), **symétrie** (S), **antisymétrie** (A) et **transitivité** (T).

Exercice 3.5

Soient $\mathcal{R}$ et $\mathcal{S}$, deux relations sur un ensemble E . Définissons la **composition des relations** $\mathcal{R}$ et $\mathcal{S}$ de la manière suivante : $\forall x, y \in E$,

$$x(\mathcal{R} \circ \mathcal{S})y \text{ ssi } \exists z \in E, x\mathcal{R}z \text{ et } z\mathcal{S}y$$

1. Si E est un ensemble de personnes, $\mathcal{R}$ est la relation "être le fils de", et $\mathcal{S}$ est la relation "être le frère de", que sont les relations $\mathcal{R} \circ \mathcal{S}$ et $\mathcal{S} \circ \mathcal{R}$?

2. Sur $E = \{a, b, c\}$, définissons les relations

$$\begin{aligned}\mathcal{R} &= \{(a, a), (a, b), (b, c), (c, b)\} \\ \mathcal{S} &= \{(a, b), (b, c), (a, c)\}\end{aligned}$$

Dessinez les matrices et les graphes des relations $\mathcal{R} \circ \mathcal{S}$ et $\mathcal{S} \circ \mathcal{R}$.

3. L'ensemble E est de cardinal fini. Donnez une méthode pour effectuer les calculs de composition de relations qui utilise le calcul **booléen**.
4. Pour les relations de la question 2, calculez $(\mathcal{R} \circ \mathcal{S})^t$ et $\mathcal{S}^t \circ \mathcal{R}^t$.
5. Pour les relations $\mathcal{R}$ et $\mathcal{S}$ de la question 2, calculez $\mathcal{R}^2 = \mathcal{R} \circ \mathcal{R}$, et $\mathcal{R}^3 = \mathcal{R}^2 \circ \mathcal{R}$, puis $\mathcal{S}^2, \mathcal{S}^3$. Interprétez ces relations en terme de chemins dans le graphe de $\mathcal{R}$ et $\mathcal{S}$.

3.3 Relations d'équivalence

Exercice 3.6

Soit $\mathcal{R}$ la relation sur $E = \{s, t, u, v, w, x, y, z\}$ de matrice

	s	t	u	v	w	x	y	z
s	1		1					
t		1		1	1		1	
u	1		1					
v		1		1	1		1	
w		1		1	1		1	
x						1		
y		1		1	1		1	
z								1

- Vérifier que cette relation est une **relation d'équivalence**.
- Donnez les **classes d'équivalence** de $\mathcal{R}$.
- Réordonnez les éléments de E suivant les classes d'équivalence. Quelles est alors la matrice de $\mathcal{R}$?
- Dessinez le graphe de E .

Exercice 3.7 (construction des rationnels ($\mathbb{Q}$))

Notons $A = \mathbb{Z} \times (\mathbb{Z} - \{0\})$ et définissons sur A la relation $\mathcal{R}$ par

$$\forall (a, b) \in A, \forall (c, d) \in A, (a, b) \mathcal{R} (c, d) \text{ ssi } ad = bc$$

- Montrez que $\mathcal{R}$ est une **relation d'équivalence**. Notons $[(a, b)]$ la **classe d'équivalence** de (a, b) .
- Quels sont les éléments de A contenus dans les classes d'équivalence suivantes : $[(1, 2)], [(0, 1)], [(1, 1)]$?
- Parmi les paires suivantes, lesquelles appartiennent à la même classe d'équivalence : $(1, 3), (0, 1), (10, 30), (0, 2)$? Munissons l'ensemble des classes d'équivalence de $\mathcal{R}$ des opérations ci-dessous :

$$[(a, b)] + [(c, d)] = [(ad + bc, bd)]$$

$$[(a, b)] * [(c, d)] = [(ac, bd)]$$

4. Quels sont les éléments de A contenus dans les classes d'équivalence suivantes $[(1, 2)] + [(4, 6)]$, $[(1, 1)] + [(2, 2)]$, $[(5, 4)] * [(0, 4)]$, $[(1, 2)] * [(2, 1)]$?
5. Pouvez-vous trouver une meilleure notation pour les classes ci-dessus ?
6. La relation $\mathcal{R}$ sur $\mathbb{Z} \times \mathbb{Z}$ est-elle transitive ?

3.4 Relations d'ordres

Exercice 3.8 (La relation “est multiple de”)

Soit $E = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$, l'ensemble des diviseurs de 60. Soit $\mathcal{R}$ la relation sur E définie par

$$\forall x, y \in E, x\mathcal{R}y \text{ ssi } x \text{ est multiple de } y$$

$\mathcal{R}$ est une relation d'ordre.

1. $\mathcal{R}$ est-elle une relation d'ordre total ? Justifiez votre réponse.
2. Dessinez le diagramme de Hasse de $\mathcal{R}$ de telle sorte que toutes les flèches soient orientées de la gauche vers la droite.
3. Quel est l'élément nul de $(E, \mathcal{R})$? Quel est l'élément universel de $(E, \mathcal{R})$?
4. Posons $A_1 = \{1, 2, 3, 4, 6, 12\}$, $A_2 = \{12, 15\}$, et $A_3 = \{2, 3, 4, 6, 12\}$. Remplissez le tableau ci-dessous :

$(E, \mathcal{R})$	A_1	A_2	A_3
minorants			
majorants			
plus petit élément			
plus grand élément			
borne inférieure			
borne supérieure			
éléments minimaux			
éléments maximaux			

Exercice 3.9 (La relation “ $\leq$ ”)

Nous considérons dans cet exonsol l'ensemble ordonné $(\mathbb{R}, \leq)$. Soit $A_1 = [0, 1]$, $A_2 =]2, 3[$, $A_3 = A_1 \cup A_2$. Remplissez le tableau ci-dessous :

$(\mathbb{R}, \leq)$	A_1	A_2	A_3
minorants			
majorants			
plus petit élément			
plus grand élément			
borne inférieure			
borne supérieure			
éléments minimaux			
éléments maximaux			

Exercice 3.10 (Diagrammes de Hasse) Sur $E = \{a, b, c, d, e, f\}$, soient les relations $\mathcal{R}_1, \mathcal{R}_2, \mathcal{R}_3$ dont les matrices sont données ci-dessous.

Pour chacune, vérifiez qu'il s'agit d'une relation d'ordre et donnez son diagramme de Hasse.

$\mathcal{R}_1$	a	b	c	d	e	f
a	1	0	0	0	0	0
b	1	1	0	1	1	1
c	1	0	1	1	1	1
d	0	0	0	1	0	0
e	1	0	0	1	1	1
f	0	0	0	0	0	1

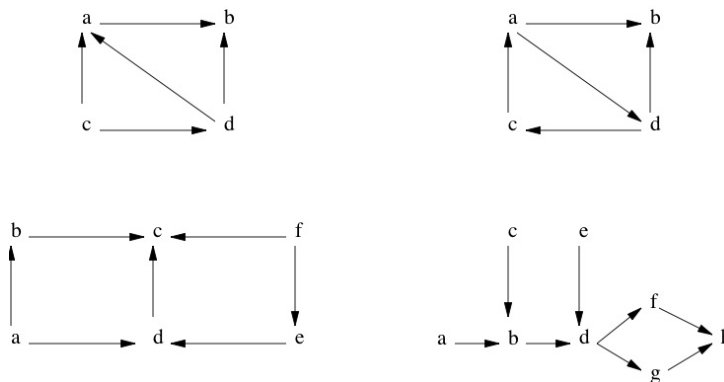
$\mathcal{R}_2$	a	b	c	d	e	f
a	1	1	1	1	1	1
b	0	1	1	1	1	1
c	0	0	1	1	1	1
d	0	0	0	1	0	1
e	0	0	0	0	1	1
f	0	0	0	0	0	1

$\mathcal{R}_3$	a	b	c	d	e	f
a	1	0	1	0	0	0
b	0	1	1	0	1	1
c	0	0	1	0	0	0
d	1	1	1	1	1	1
e	0	0	1	0	1	0
f	0	0	1	0	0	1

Pour chacune de ces relations d'ordre, donner s'ils existent l'élément nul et l'élément universel ainsi que les éléments particuliers des ensembles $X = \{a, b, c\}$ et $Y = \{e, f\}$.

Exercice 3.11 (Diagrammes de Hasse???)

Parmi les 4 graphes ci-dessous lesquels sont des diagrammes de Hasse? Quand c'est le cas, donnez la matrice de la relation d'ordre associée.



Exercice 3.12 Un marchand d'ordinateur caractérise ses machines à l'aide de deux nombres : la puissance de calcul, notée p et la capacité du disque dur, notée c . A chaque machine est donc associé un couple (p, c) . Deux machines (p, c) et (p', c') seront considérées identiques $((p, c) = (p', c'))$ si et seulement si $p = p'$ et $c = c'$. Avant de choisir ses prix, il souhaite pouvoir ordonner ses machines. Ne sachant pas vraiment comment s'y prendre, il propose à son stagiaire les quatre relations ci-dessous et lui demande s'il s'agit de relations d'ordre :

1. $\forall (p, c) \in \mathbb{N} \times \mathbb{N}, \forall (p', c') \in \mathbb{N} \times \mathbb{N}, (p, c) \mathcal{R}_1 (p', c') \Leftrightarrow p \leq p' \text{ ou } c \leq c'$
2. $\forall (p, c) \in \mathbb{N} \times \mathbb{N}, \forall (p', c') \in \mathbb{N} \times \mathbb{N}, (p, c) \mathcal{R}_2 (p', c') \Leftrightarrow p < p' \text{ ou } (p = p' \text{ et } c \leq c')$
3. $\forall (p, c) \in \mathbb{N} \times \mathbb{N}, \forall (p', c') \in \mathbb{N} \times \mathbb{N}, (p, c) \mathcal{R}_3 (p', c') \Leftrightarrow p \leq p' \text{ et } c \geq c'$
4. $\forall (p, c) \in \mathbb{N} \times \mathbb{N}, \forall (p', c') \in \mathbb{N} \times \mathbb{N}, (p, c) \mathcal{R}_4 (p', c') \Leftrightarrow p + c \leq p' + c'$

Pour chacune de ces quatre relations, examinez s'il s'agit ou non d'une relation d'ordre en justifiant vos affirmations.

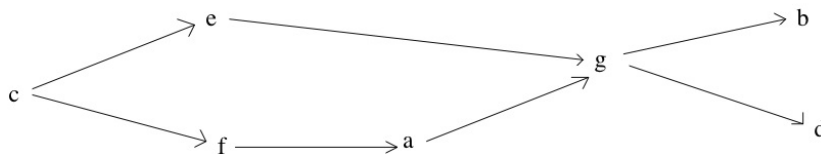
3.5 Sujets d'I.E. et d'examen

Exercice 3.13 On considère la relation $\mathcal{R}$ sur $E = \{a, b, c, d, e\}$ définie par la matrice suivante :

$\mathcal{R}$	a	b	c	d	e
a	1		1	1	
b	1	1			
c		1		1	
d	1			1	
e	1	1			1

1. Donner la représentation sagittale de la relation $\mathcal{R}$.
2. La relation $\mathcal{R}$ est-elle réflexive ? symétrique ? antisymétrique ? transitive ? (Justifier)
3. Est-ce une relation d'équivalence ? une relation d'ordre ?

Exercice 3.14 On considère la relation d'ordre R sur l'ensemble $E = \{a, b, c, d, e, f, g\}$ définie par son diagramme de Hasse :



1. Donner, s'ils existent, l'élément nul et l'élément universel de E .
2. Pour les sous-ensembles $X = \{c, e, f\}$ et $Y = \{e, f, a, g\}$, remplir le tableau suivant afin de donner les éléments particuliers de ces deux sous-ensembles.

$(E, \mathcal{R})$	X	Y
minorants		
majorants		
plus petit élément		
plus grand élément		
borne inférieure		
borne supérieure		
éléments minimaux		
éléments maximaux		

Exercice 3.15 On considère la relation $\mathcal{R}$ définie sur l'ensemble $E = \{a, b, c, d, e, f, g, h\}$ par la matrice ci-dessous.

1. Montrer, à l'aide de la matrice, que la relation $\mathcal{R}$ est une relation d'ordre.
2. Est-ce une relation d'ordre partiel ou total ?
3. Dessiner le diagramme de Hasse de la relation $\mathcal{R}$.
4. Donner *sans justifier* les éléments particuliers des sous-ensembles $A = \{c, d, e, f\}$ et $B = \{e, g\}$ de E .

$\mathcal{R}$	a	b	c	d	e	f	g	h
a	1	0	0	1	1	1	1	1
b	0	1	1	1	1	1	1	1
c	0	0	1	1	1	1	1	1
d	0	0	0	1	1	1	1	1
e	0	0	0	0	1	0	1	1
f	0	0	0	0	0	1	1	1
g	0	0	0	0	0	0	1	1
h	0	0	0	0	0	0	0	1

$(E, \mathcal{R})$	$A = \{c, d, e, f\}$	$B = \{e, g\}$
minorants		
majorants		
plus petit élément		
plus grand élément		
borne inférieure		
borne supérieure		
éléments minimaux		
éléments maximaux		

Exercice 3.16 On considère la relation $\mathcal{R}$ définie sur $\mathbb{R}$ par

$$x \mathcal{R} y \Leftrightarrow \exists \lambda \in \mathbb{R}^*; x = \lambda y$$

(on rappelle que $\mathbb{R}^*$ signifie $\mathbb{R}$ privé de 0)

1. La relation $\mathcal{R}$ est-elle réflexive ? symétrique ? antisymétrique ? transitive ? (Justifier toutes les réponses)
2. La relation $\mathcal{R}$ est-elle une relation d'équivalence ? une relation d'ordre ? (Justifier)
3. Donner les classes d'équivalences des éléments 1 et 0.
4. Que se passe-t-il si on autorise la valeur 0 pour λ dans la définition de la relation $\mathcal{R}$?

Partie 4

Arithmétique

4.1 Divisibilité et nombres premiers

Exercice 4.1

1. Ecrire la division euclidienne de 12 par 5 et de -12 par 5.
2. Quels sont les restes possibles dans une division par 5 ? Trouver tous les entiers naturels de quotient 26 quand on les divise par 5.
3. Trouver un nombre de deux chiffres égal au double de leur produit.
4. Démontrer les critères de divisibilité par 2 et 5, 4 et 25, 3 et 9.

Exercice 4.2 Calculer $a \wedge b$ et $a \vee b$, en utilisant

1. La décomposition en nombres premiers
2. L'identité de Bezout

pour les nombres suivants :

- $a = 325$ et $b = 120$
- $a = 429$ et $b = 700$

En déduire dans chaque cas u et v tels que $au + bv = d$ ($= a \wedge b$).

Exercice 4.3 Soit $p \geq 5$ premier.

1. Montrer que $3|(p^2 - 1)$ et $8|(p^2 - 1)$
2. En déduire que $24|(p^2 - 1)$.

Exercice 4.4 Soit $n \in \mathbb{Z}$. Montrer que $n^5 - n$ est divisible par 30.

Exercice 4.5 Soient $n \geq 3$, $a_n = 2^n - 1$ et $b_n = 2^n + 1$. Montrer que si l'un des nombres a ou b est premier alors l'autre ne l'est pas (On montre que $3|ab$).

Exercice 4.6 Soit p un nombre premier et $p|ab$. Montrer que $p|a$ ou $p|b$.

4.2 Équations diophantiennes

Exercice 4.7 Résoudre les équations suivantes dans $\mathbb{Z}$

1. $17x + 9y = 2$
2. $6x + 10y = 4$
3. $3x + 6y = 7$
4. $2x - 3y = 2$

Exercice 4.8 Soient $a > 1$ et $n > 1$. Montrer que si $a^n - 1$ est premier alors $a = 2$ et n est premier.

Exercice 4.9 Ecrire 100 comme somme de deux entiers positifs, l'un divisible par 11 et l'autre par 7.

Exercice 4.10 Un objet vaut x euros et y centimes. Par erreur vous payez y euros et x centimes soit deux fois le prix plus 5 centimes. Quel est le prix de l'objet ?

Exercice 4.11 Deux enfants ont 100 billes à eux deux. Si le premier met ses billes par paquets de 8, il lui en reste 7, et si le second met ses billes par paquets de 10, il lui en reste 7 aussi. Combien chacun ont-ils de billes ?

4.3 Congruences

Exercice 4.12 (Divisibilité par 11) Soit n un entier qui s'écrit en base 10 comme $x_p x_{p-1} \dots x_0$.

1. Exprimer $\bar{n}[11]$ (reste de la division de n par 11) en fonction de $x_0, x_1, x_2, \dots, x_p$.
2. En déduire un critère de divisibilité par 11 des nombres entiers écrits en base 10.
3. Donner des exemples.

Exercice 4.13

1. $\bar{a}$ est-il inversible dans les cas suivants ? Si oui, calculer son inverse.
 - (a) $\bar{a} = \bar{9}$ dans $\mathbb{Z}/17\mathbb{Z}$
 - (b) $\bar{a} = \bar{72}$ dans $\mathbb{Z}/6125\mathbb{Z}$
 - (c) $\bar{a} = \bar{24}$ dans $\mathbb{Z}/30\mathbb{Z}$
2. En déduire dans chacun des cas précédents la solution de l'équation $\bar{a} \bar{x} = \bar{5}$.

Exercice 4.14 Résoudre les équations suivantes :

1. $2x + 1 \equiv 14 [15]$
2. $206x + 6 \equiv 3 [5]$
3. $28x + 167 \equiv -1 [15]$

Exercice 4.15 Résoudre les équations suivantes :

1. $x^2 = 1$ dans $\mathbb{Z}/17\mathbb{Z}$
2. $x^2 - x - 1 = 0$ dans $\mathbb{Z}/5\mathbb{Z}$
3. $-6x^2 - 3x + 2 = 0$ dans $\mathbb{Z}/7\mathbb{Z}$
4. $x^2 = 1$ dans $\mathbb{Z}/8\mathbb{Z}$

Exercice 4.16 Résoudre les équations de congruence suivantes :

1. $6x \equiv 2 [8]$
2. $2x \equiv 3 [5]$
3. $4x \equiv 5 [9]$

Exercice 4.17 Résoudre les systèmes de congruence suivants

$$\begin{cases} x \equiv 5 [6] \\ x \equiv 1 [2] \end{cases} \quad \begin{cases} x \equiv 3 [4] \\ x \equiv 6 [8] \end{cases}$$

Exercice 4.18 Déterminer tous les entiers x tels que :

$$\begin{cases} x \equiv 2 [3] \\ x \equiv 3 [4] \\ x \equiv 4 [5] \end{cases}$$

Exercice 4.19 Déterminer tous les entiers n avec $1 \leq n \leq 105$ tels que les restes des divisions euclidiennes de n par 3, 5 et 8 sont respectivement 1, 3 et 6.

Exercice 4.20 Soit p un nombre premier

1. Dans $\mathbb{Z}/p\mathbb{Z}$, montrer que 1 et $p-1$ sont leurs propres inverses et que ce sont les seuls.
2. Montrer que si x est l'inverse de y , alors $p-x$ est l'inverse de $p-y$.
3. Imaginer une méthode rapide pour calculer les inverses de tous les éléments de $(\mathbb{Z}/p\mathbb{Z})^*$ (Combien faut-il en calculer au plus?)
4. Application : Déterminer l'inverse de chaque élément dans les cas suivants :
 - (a) $\mathbb{Z}/5\mathbb{Z}$
 - (b) $\mathbb{Z}/11\mathbb{Z}$
 - (c) $\mathbb{Z}/23\mathbb{Z}$

Exercice 4.21 (Euler)

Soit ϕ la fonction d'Euler.

1. Calculer $\phi(n)$ lorsque $n = 200$, $n = 345$ et $n = 1250$
2. En déduire les restes des divisions suivantes : 17^{162} par 200, 8^{180} par 345 et 21^{502} par 1250

Exercice 4.22 Déterminer les restes des divisions suivantes :

1. 13^{1996} par 17
2. $13^{3^{1998}}$ par 11

Exercice 4.23 On considère le polynôme suivant :

$$P(x) = a_0 + a_1x + a_2x^2$$

avec $a_0 = 15^{1995}$, $a_1 = 13^{2022}$ et $a_2 = 8^{3303}$

1. Trouver une écriture plus simple de p dans $\mathbb{Z}/11\mathbb{Z}$.
2. Quel est le reste de la division de $P(3^{1002})$ par 11?

Exercice 4.24 Soit $A = 1000^{2000^{3000^{4000}}}$. On cherche le reste de la division de A par 19. On note $a = 2000^{3000^{4000}}$.

1. Déterminer le reste r de la division de 2000 par 18.
2. Montrer que 3000^{4000} est un multiple de 6
3. En déduire que $a \equiv 10 [18]$ (on montrera par récurrence que $2^{6n} \equiv 10 [18]$).
4. Diviser 1000 par 19.
5. Utiliser ce qui précède et le théorème de Fermat pour déterminer $\overline{A} [19]$.

4.4 Cryptographie

Exercice 4.25 On se propose de coder les mots de la façon suivante :

- Correspondance lettre-nombre : $A = 01, B = 02, \dots, Z = 26$ et espace = 27.
- Codage RSA par groupe de 2 chiffres avec $n = 33$ et $e = 7$

Décoder le message $GAZB$

Exercice 4.26 Même exercice avec $n = 91$ et $e = 17$

1. Encoder le mot OK .
2. Décoder le message 61754123

Exercice 4.27 Mettez vous par binôme, encodez chacun un message de 4 lettres et envoyez le à l'autre qui le décodera.

4.5 Sujets d'I.E. et d'examen

Exercice 4.28 Donner la décomposition en facteurs premiers de 90 et 189. En déduire le pgcd et le ppcm de 90 et 189.

Exercice 4.29 Un voyant, à qui on demande de prouver son pouvoir, fait l'expérience suivante avec un passant : “ Bonjour, je suis voyant, je vais deviner votre date de naissance. Prenez votre jour de naissance. Multipliez le par 31. Prenez votre mois de naissance. Multipliez le par 12. Ajoutez ces deux nombres. Combien trouvez-vous ? ” Le passant répond “ 811 ”. Après quelques instants de concentration, le voyant reprend : “ Vous êtes né un 25 mars ! ”, et le passant approuve, impressionné par autant de talent. Et vous, serez-vous dupe ?

Nous allons voir trois méthodes qui permettent de répondre comme le voyant. Chaque méthode est indépendante des autres mais repose sur la même équation de départ.

On note j le jour de naissance et m le mois de naissance. Donner l'équation (E) dont les réponses au problème sont solutions. Quelles sont les contraintes sur j et m ?

1. Méthode 1 : on se place dans $\mathbb{Z}/31\mathbb{Z}$
 - (a) Montrer que l'équation (E) s'écrit dans $\mathbb{Z}/31\mathbb{Z}$

$$(E_1) \quad \overline{12} \times \overline{m} = \overline{5}$$

- (b) $\overline{12}$ est-il inversible dans $\mathbb{Z}/31\mathbb{Z}$? Si oui, donner son inverse.
- (c) Résoudre l'équation (E_1) dans $\mathbb{Z}/31\mathbb{Z}$.

- (d) En tenant compte des contraintes de l'énoncé, en déduire la seule valeur possible pour m , puis la valeur de j correspondante et donner la solution du problème.
2. Méthode 2 : on se place dans $\mathbb{Z}/12\mathbb{Z}$
- (a) Montrer que l'équation (E) s'écrit dans $\mathbb{Z}/12\mathbb{Z}$
- $$(E_2) \quad \bar{7} \times \bar{j} = \bar{7}$$
- (b) $\bar{7}$ est-il inversible dans $\mathbb{Z}/12\mathbb{Z}$? Si oui, donner son inverse.
- (c) Résoudre l'équation (E_2) dans $\mathbb{Z}/12\mathbb{Z}$.
- (d) En tenant compte des contraintes de l'énoncé, en déduire les valeurs possibles pour j , puis les valeurs de m correspondantes et donner la solution du problème.
3. Méthode 3 : équation diophantienne du type $ax + by = c$
- (a) Trouver une solution particulière de (E) à l'aide d'une identité de Bachet-Bézout obtenue via l'algorithme d'Euclide étendu.
- (b) Trouver la forme générale de l'ensemble des solutions de (E) .
- (c) En tenant compte des contraintes, donner la solution du problème.

Exercice 4.30 Montrer que l'équation $x^4 + x^3 + x^2 + x + 1 = 0$ n'a pas de solution dans $\mathbb{Q}$.