Mathématiques pour l'informatique

Christophe GUYEUX et Jean-François COUCHOT
guyeux[arobase]iut-bm.univ-fcomte[point]fr
couchot[arobase]iut-bm.univ-fcomte[point]fr

12 février 2014

Table des matières

Première partie

Logique

Chapitre 1

Algèbre de Boole

I Propriétés générales

DÉFINITION 1.1 (ALGÈBRE DE BOOLE). On appelle *algèbre de Boole* la structure algébrique $(\mathcal{A}, +, ., \overline{\ })$ définie par un ensemble (non vide) $\mathcal{A}$ et trois opérations :

- la somme booléenne (binaire) : "+",
- le produit booléen (binaire) : "." et
- la négation booléenne (unaire) : "$\overline{\ }$" (par exemple $\overline{a}$).

et qui doivent posséder les propriétés données du tableau ci-dessous.

Propriété			
idempotence	$a+a=a$ $a\cdot a=a$	distributivités	$a\cdot(b+c)=a\cdot b+a\cdot c$ $a+b\cdot c=(a+b)\cdot(a+c)$
commutativité	$a+b=b+a$ $a\cdot b=b\cdot a$	involution	$\overline{\overline{a}}=a$
associativité	$a+(b+c)=(a+b)+c$ $a\cdot(b\cdot c)=(a\cdot b)\cdot c$	complémentation	$\overline{0}=1$ $\overline{1}=0$
éléments neutres	$a+0=a$ $a\cdot 1=a$	partition	$a+\overline{a}=1$ $a\cdot\overline{a}=0$
absorption	$a+1=1$ $a\cdot 0=0$	« Lois de De Morgan »	$\overline{a+b}=\overline{a}\cdot\overline{b}$ $\overline{a\cdot b}=\overline{a}+\overline{b}$

Propriétés d'une algèbre de Boole

REMARQUE 1.1. Les signes opératoires utilisés sont les mêmes que ceux de l'addition et de la multiplication des réels. Cependant, ces opérations n'ont évidemment pas les mêmes propriétés, et ne portent pas sur les mêmes éléments.

Exercice 1.1 (Somme disjonctive). *On considère une algèbre de Boole quelconque $(E, +, \cdot, \overline{\ })$.*
On définit l'opération « somme disjonctive », notée $\oplus$, par $a \oplus b = \overline{a}b + a\overline{b}$.

1. *Que vaut $a \oplus 0$? $a \oplus 1$?*
2. *Calculez $a \oplus a$ et $a \oplus \overline{a}$.*
3. *Calculez $\overline{a \oplus b}$.*
4. *Montrez que $\oplus$ est associative et commutative.*

Exercice 1.2 (Opérateurs de Sheffer et de Peirce). *Soit $(E, +, \cdot, \overline{\ })$ une algèbre de Boole.*

1. *On définit l'opération de Sheffer [1] par : $a|b = \overline{a} + \overline{b}$.*
   Comment obtenir $\overline{a}$, $a+b$, $a\cdot b$ en n'utilisant que l'opérateur $|$? Faire de même pour $a+\overline{b}$; étudier l'associativité de cette opération.
2. *On définit la flèche de Peirce [2] par : $a \downarrow b = \overline{a} \cdot \overline{b}$.Mêmes questions.*

1. D'après le logicien H.M. Sheffer
2. Lorsque les logiciens, dans les années 1930, cherchèrent un symbole pour exprimer le connecteur découvert par C.S. Peirce (1839-1914), "Pierce Arrow" était le nom d'une célèbre marque de voiture !

II Règles de calcul dans une algèbre de Boole

1. Les priorités habituelles sont respectées pour la somme et le produit booléen.
2. Les éléments neutres sont notés 0 et 1, par analogie avec les entiers de même symbole (ne pas oublier que ces calculs ne se déroulent pas dans $\mathbb{R}$...)
3. Il y a deux distributivités. Celle de la somme (booléenne) sur le produit (booléen) n'est pas habituelle. Par exemple, simplifier $(a+b)(a+c)(a+d)(a+e)(a+f)$
4. Signalons pour finir que, comme ci-dessus, le point pour le produit est souvent omis.

Dans une expression booléenne, une sous-expression est dite « redondante » lorsqu'on peut la supprimer sans changer la « valeur » de l'expression :

PROPRIÉTÉ 1.1 (SUPPRESSION DE REDONDANCE) : On a les trois règles suivantes :

1. Dans une somme booléenne, tout terme absorbe ses multiples : $a + a \cdot b = a$.
2. Dans un produit booléen, tout facteur absorbe tout autre facteur qui le contient en tant que terme : $a \cdot (a + b) = a$.
3. Ajouter à un terme un multiple b de son complément revient à ne lui ajouter que b : $a + \overline{a} \cdot b = a + b$

PREUVE On déomntre les trois règles comme suit :

1. En effet, $a+a\cdot b = a\cdot(\overline{b}+b)+a\cdot b = a\cdot\overline{b}+a\cdot b+a\cdot b = a\cdot\overline{b}+a\cdot b$ (par idempotence) $= a\cdot(\overline{b}+b) = a$.
2. En effet, $a \cdot (a + b) = a \cdot a + a \cdot b = a + a \cdot b = a$.
3. $a + \overline{a} \cdot b = (a + \overline{a}) \cdot (a + b) = 1 \cdot (a + b) = a + b$. ∎

EXEMPLE 1.3. $ab + \overline{a}c + \overline{b}c = ab + (\overline{a} + \overline{b}) \cdot c = ab + \overline{ab} \cdot c = ab + c$

Exercice 1.4. *Montrer que* $a \cdot b + \overline{a} \cdot c + b.c = a \cdot b + \overline{a} \cdot c$

Exercice 1.5 (Calcul booléen élémentaire). *Appliquer au maximum les règles précédentes pour supprimer les redondances dans les calculs suivants.*

1. $(a + b + c) \cdot (a + \overline{b} + c) \cdot (a + \overline{b} + \overline{c})$
2. $a + \overline{a} \cdot b \cdot c + \overline{a} + a \cdot b$
3. $a \cdot b + \overline{a} \cdot b \cdot c + a \cdot \overline{b} \cdot c$
4. $(a + b + c) \cdot (\overline{a} + \overline{b} + \overline{c} + d)$

Exercice 1.6 (Calcul booléen). *Même énoncé qu'à l'exercice précédent.*

1. $(\overline{a} + b)(\overline{c} + \overline{a} \cdot \overline{b} + a \cdot b)$.
2. $(a + \overline{b} + \overline{c}) \cdot (\overline{a} + b) \cdot (\overline{b} + c)$.
3. $(a + c) \cdot (\overline{a} + d) \cdot (\overline{b} + \overline{e}) \cdot (\overline{b} \cdot \overline{c} + b \cdot c) \cdot (\overline{d} + c \cdot e) \cdot (\overline{c} + d)$.
4. $(\overline{a} \cdot \overline{a \cdot (\overline{b} + \overline{c})} + a \cdot (\overline{b} + \overline{c})) \cdot (\overline{b} \cdot \overline{\overline{a} + c} + (\overline{a} + c) \cdot b) \cdot (a \cdot \overline{b} \cdot c + \overline{a \cdot \overline{b}} \cdot \overline{c})$.

III Fonctions booléennes

Soit $\mathcal{A}$ une algèbre de Boole.

DÉFINITION 1.2 (FONCTION BOOLÉENNE). On appelle *fonction booléenne de n variables* toute application de $\mathcal{A}^n$ dans $\mathcal{A}$ dont l'expression ne contient que :

— les symboles des opérations booléennes,
— des symboles de variables, de constantes,
— d'éventuelles parenthèses.

EXEMPLE 1.7. $f(a,b,c) = a \cdot \overline{b} + c$.

DÉFINITION 1.3 (ASPECT D'UNE VARIABLE). Si a est une variable booléenne, elle peut intervenir dans l'expression d'une fonction booléenne sous la forme a ou sous la forme $\overline{a}$, qui sont appelées les deux *aspects* de cette variable : affirmé et nié.

DÉFINITION 1.4 (FONCTION BOOLÉENNE NULLE). On appelle *fonction booléenne nulle* la fonction booléenne qui, à chaque valeur des variables, associe la valeur 0. Son expression est $f(x_1, x_2, \ldots, x_n) = 0$.

DÉFINITION 1.5 (FONCTION RÉFÉRENTIEL). On appelle *fonction référentiel* la fonction booléenne qui, à chaque valeur des variables, associe la valeur 1. Son expression est $f(x_1, x_2, \ldots, x_n) = 1$.

DÉFINITION 1.6 (MINTERME, MAXTERME). Un *minterme* à n variables est une fonction booléenne à n variables dont l'expression se présente sous la forme du produit d'un aspect et d'un seul de chacune des n variables.

Définition analogue pour un *maxterme* , en remplaçant dans la définition précédente « produit » par « somme ».

EXEMPLE 1.8 (MINTERME À TROIS VARIABLES). $a \cdot \overline{b} \cdot c$

EXEMPLE 1.9 (MAXTERME À TROIS VARIABLES). $\overline{a} + b + \overline{c}$.

Exercice 1.10. *Pour 3 variables a, b et c, repérez les mintermes et les maxtermes :* $b\overline{c}$, $a + \overline{b} + c$, $a\overline{b}b\overline{c}$, $\overline{a}bc$, $a + \overline{b}c$.

Exercice 1.11. *Dressez la liste des mintermes et des maxtermes pour deux variables* a *et* b.

PROPRIÉTÉ 1.2 (NOMBRE DE MINTERMES ET DE MAXTERMES) : Les mintermes et maxtermes, pour un nombre donné n de variables, sont au nombre de 2^n chacun.

III.1 Formes canoniques d'une fonction booléenne

DÉFINITION 1.7 (MONÔMES). Un *monôme* est une fonction booléenne produit de variables booléennes éventuellement niées.

Exercice 1.12. *Parmi les expressions suivantes dire lesquelles sont des monômes et lesquelles ne le sont pas en justifiant :* $a + b$, $a + bc$, $a(b + c)$, $a\overline{b}$, b.

PROPRIÉTÉ 1.3 : Quelle que soit l'expression de la fonction booléenne, il est possible de la mettre sous la forme d'une somme de monômes.

PREUVE En effet, comme elle ne fait intervenir que les trois opérations booléennes, il suffit de lui appliquer les règles du calcul booléen :

1. On développe les négations (en appliquant les règles $\overline{a + b} = \overline{a} \cdot \overline{b}$ et $\overline{a \cdot b} = \overline{a} + \overline{b}$), jusqu'à ce qu'il n'y ait plus de négations que sur les variables ;
2. Puis on développe les produits qui portent sur des sommes, en utilisant la distributivité du produit sur la somme ;
3. On obtient ainsi une expression qui s'écrit sans parenthèses, et qui ne contient que des sommes de produits de variables éventuellement niées. ■

PROPRIÉTÉ 1.4 : Chaque monôme peut ensuite être mis sous la forme d'une somme de mintermes.

PREUVE En effet, si, dans l'expression de ce monôme, toutes les variables interviennent, c'est déjà un minterme.

Dans le cas contraire, il manque (par exemple) la variable a dans son expression : on la fait intervenir sous la forme $(\overline{a} + a)$. On développe, les deux monômes obtenus font intervenir la variable a.

Ou bien, il s'agit de mintermes et le processus est terminé, ou bien il manque encore une variable, qu'on fait intervenir en utilisant le même procédé, et ainsi de suite jusqu'à aboutir aux mintermes. ■

On fait évidemment disparaître du résultat, par idempotence, les occurrences multiples de mintermes, pour pouvoir énoncer le résultat suivant :

PROPRIÉTÉ 1.5 (FORME CANONIQUE DISJONCTIVE) : Toute fonction booléenne à n variables (autre que la fonction nulle) peut se mettre sous la forme d'une somme de mintermes à n variables.

Cette forme, unique, s'appelle *Forme Canonique Disjonctive* (dans la suite, FCD).

REMARQUE 1.2. L'unicité de cette FCD permet la comparaison des fonctions booléennes entre elles.

Par négation booléenne de ce résultat, on obtient :

PROPRIÉTÉ 1.6 (FORME CANONIQUE CONJONCTIVE) : Toute fonction booléenne de n variables (autre que la fonction référentiel) peut se mettre sous la forme d'un produit de maxtermes à n variables.

Cette forme, unique, est la *Forme Canonique Conjonctive* (FCC dans la suite).

III.2 Obtention des formes canoniques

La méthode algébrique consiste à :
— tout développer pour mettre l'expression sous la forme d'une somme de monômes,
— dans chaque terme de cette somme, faire apparaître les valeurs qui n'y figurent pas.

EXEMPLE 1.13. On illustre cela :
$f(a,b,c) = a + bc = a(\overline{b} + b)(\overline{c} + c) + (\overline{a} + a)bc$
$= a\overline{b}\overline{c} + a\overline{b}c + ab\overline{c} + abc + \overline{a}bc + abc = m_3 + m_4 + m_5 + m_6 + m_7.$

Pour la FCC, on peut imaginer une méthode analogue.

EXEMPLE 1.14. $f(a,b,c) = a + bc = (a+b)(a+c) = (a+b+\overline{c}c)(a+\overline{b}b+c)$
$= (a+b+\overline{c}) \cdot (a+b+c) \cdot (a+\overline{b}+c) \cdot (a+b+c) = M_5 M_6 M_7$

REMARQUE 1.3. Si on prend la négation de la FCD, on obtient bien sûr une FCC... mais pas celle de la fonction, celle de sa négation !

Il suffit de prendre la négation de la fonction, de calculer sa FCD puis de prendre la négation du résultat.

Exercice 1.15. *Obtenir la FCC de $x + \overline{y}z$.*

Il existe une autre méthode pour obtenir ces formes canoniques : la méthode des diagrammes.

IV Diagrammes de Karnaugh

La représentation des fonctions booléennes par diagrammes de Karnaugh-Veitch : est fondée sur les propriétés des mintermes (ils réalisent une partition de l'unité),

Ces derniers diagrammes deviennent rapidement inextricables quand le nombre de variables augmente, c'est pourquoi, dans les diagrammes de Karnaugh, on divise systématiquement l'« univers » (le référentiel E) en deux parties égales en superficie pour représenter la partie concernée et son complémentaire.

À chaque introduction de variable supplémentaire, chaque case du précédent diagramme est divisée en 2.

On obtient, par exemple :

	$\overline{a}$	a
$\overline{b}$	$\overline{a}\overline{b}$	$a\overline{b}$
b	$\overline{a}b$	ab

Cas de trois variables :
— les deux premières colonnes correspondent à $\overline{a}$, les deux dernières à a,
— la première et la dernière colonne correspondent à $\overline{b}$, les deux centrales à b,
— enfin, la première ligne est associée à $\overline{c}$, la deuxième à c.
...ce qui donne

	00	01	11	10
0	$\overline{a}\overline{b}\overline{c}$	$\overline{a}b\overline{c}$	$ab\overline{c}$	$a\overline{b}\overline{c}$
1	$\overline{a}\overline{b}c$	$\overline{a}bc$	abc	$a\overline{b}c$

Dans un tel diagramme, chaque case représente un minterme. Les autres monômes regroupent un nombre de cases qui est une puissance de 2, selon le nombre de variables présentes.

Exercice (corrigé) 1.16. *Faire un diagramme à cinq variables.*

	000	001	011	010	110	111	101	100
00	$\overline{a}\overline{b}\overline{c}\overline{d}\overline{e}$	$\overline{a}\overline{b}\overline{c}\overline{d}e$	$\overline{a}\overline{b}cd\overline{e}$	$\overline{a}\overline{b}c\overline{d}\overline{e}$	$ab\overline{c}\overline{d}\overline{e}$	$abcd\overline{e}$	$a\overline{b}cd\overline{e}$	$a\overline{b}\overline{c}\overline{d}\overline{e}$
01	$\overline{a}\overline{b}\overline{c}\overline{d}e$	$\overline{a}\overline{b}\overline{c}de$	$\overline{a}\overline{b}cde$	$\overline{a}\overline{b}c\overline{d}e$	$ab\overline{c}\overline{d}e$	$abcde$	$a\overline{b}cde$	$a\overline{b}\overline{c}\overline{d}e$
11	$\overline{a}\overline{b}\overline{c}de$	$\overline{a}\overline{b}cde$	$\overline{a}bcde$	$\overline{a}b\overline{c}de$	$ab\overline{c}de$	$abcde$	$a\overline{b}cde$	$a\overline{b}\overline{c}de$
10	$\overline{a}\overline{b}\overline{c}d\overline{e}$	$\overline{a}\overline{b}cd\overline{e}$	$\overline{a}bcd\overline{e}$	$\overline{a}b\overline{c}d\overline{e}$	$ab\overline{c}d\overline{e}$	$abcd\overline{e}$	$a\overline{b}cd\overline{e}$	$a\overline{b}\overline{c}d\overline{e}$

Les diagrammes peuvent être utilisés en réunion, en intersection ou en complémentation.
Ils permettent :
— d'obtenir la FCD d'une fonction booléenne plus aisément que par le calcul algébrique (utilisé pour découvrir la forme en question),
— une première approche du problème de la simplification des fonctions booléennes (dans des cas simples et pour un petit nombre de variables)...

Utilisation des diagrammes de Karnaugh pour représenter les fonctions booléennes...

En réunion. Soit par exemple $f(a,b,c) = a + \overline{b}c$. Son diagramme est :

c \ ab	00	01	11	10
0	0	2	6	4
1	1	3	7	5

On lit aisément la FCD de f sur le diagramme : $f(a,b,c) = m_1 + m_4 + m_5 + m_6 + m_7$.

En intersection. Soit $f(a,b,c) = (a + \overline{b})(a + c)$.

On peint en rouge les cases correspondant à $a + \overline{b}$, et on note en italique les nombres correspondant à $a + c$:

c \ ab	00	01	11	10
0	*0*	2	*6*	*4*
1	*1*	*3*	*7*	*5*

La représentation de f est contenue dans les cases rouges possédant les nombres en italique. Comme $(a + \overline{b})(a + c) = a + \overline{b}c$, on retrouve la même FCD.

En complémentation. Soit $f(a,b,c) = a + \overline{b}c$, de diagramme :

c \ ab	00	01	11	10
0	0	2	6	4
1	1	3	7	5

Alors la négation de $a + \overline{b}c$ est dans les cases pas rouge : la FCD de $\overline{f}$ est $m_0 + m_2 + m_3$.

Exercice 1.17 (Fonctions booléennes). *Donner la forme canonique disjonctive de la fonction booléeene dont l'expression est*

$$f(a, b, c, d, e) = \overline{a} \cdot [\overline{b} \cdot \overline{e} \cdot (c + d) + b \cdot (\overline{c} \cdot \overline{d} \cdot \overline{e} + c \cdot \overline{d \cdot e})].$$

Exercice 1.18. *Pour chacune des expressions suivantes...*

$$\begin{aligned} E_1 &= xyz + xy\overline{z} + \overline{x}y\overline{z} + \overline{x}.\overline{y}z \\ E_2 &= xyz + xy\overline{z} + x\overline{y}z + \overline{x}.\overline{y}z \\ E_3 &= xyz + xy\overline{z} + \overline{x}y\overline{z} + \overline{x}.\overline{y}.\overline{z} + \overline{x}.\overline{y}z \end{aligned}$$

donner la forme minimale en exploitant les diagrammes de Karnaugh

Exercice 1.19 (Application de la méthode de Karnaugh). *Trouver une forme minimale de* $E = x\overline{y} + xyz + \overline{x}.\overline{y}.\overline{z} + \overline{x}yz\overline{t}$.

Exercice 1.20 (Composition de la méthode de Karnaugh). *On considère deux fonctions booléennes* u *et* v *des quatres variables* a, b, c, d *définies par* $u = (a + d)(b + c)$ *et* $v = (a + c)(\overline{b} + d)$.

1. *Dessiner les diagrammes de Karnaugh de* u *et de* v.
2. *En déduire le diagramme de Karnaugh de* $w = uv + \overline{u}.\overline{v}$.
3. *Donner une forme minimale pour* w

Exercice 1.21 (BTS-2009). *La société K-Gaz décide de recruter en interne des collaborateurs pour sa filiale en Extrême-Orient. Pour chaque employé, on définit les variables booléennes suivantes :*

- *a = 1 s'il a plus de cinq ans d'ancienneté dans l'entreprise ;*
- *b = 1 s'il possède un B.T.S. informatique de gestion (BTS-IG) ;*
- *c = 1 s'il parle couramment l'anglais.*

La direction des ressources humaines décide que pourront postuler les employés :

- *qui satisfont aux trois conditions,*
- *ou qui ont moins de 5 ans d'ancienneté mais qui maîtrisent l'anglais,*
- *ou qui ne maîtrisent pas l'anglais mais qui possèdent un BTS-IG.*

1. *Écrire une expression booléenne* E *traduisant les critères de la direction.*
2. *Représenter l'expression* E *par un tableau de Karnaugh.*
3. *À l'aide du tableau de Karnaugh, donner une expression simplifiée de* E.
4. *Retrouver ce résultat par le calcul.*
5. *En déduire une version simplifiée des critères de la direction.*

Exercice 1.22 (BTS-2002). *On considère l'expression* $E = a.c + b.c + a.b + a.b.c$ *dépendant des variables booléennes* a, b *et* c *:*

1. *Simplifier l'expression* E *à l'aide de la lecture d'un tableau de Karnaugh (ou d'une table de vérité).*
2. *Dans un organisme qui aide des personnes au chômage à trouver un emploi, on considère pour ces personnes, trois variables booléennes définies ainsi :*
   - *a = 1 si la personne est âgée de 45 ans ou plus (sinon a = 0) ;*
   - *b = 1 si la personne est au chômage depuis un an ou plus (sinon b = 0) ;*
   - *c = 1 si la personne a déjà suivi une formation l'année précédente (sinonc = 0).*

   Une formation qualifiante sera mise en place pour les personnes vérifiant au moins un des critères suivants :
   - *avoir 45 ans ou plus et être au chômage depuis moins de un an ;*
   - *avoir moins de 45 ans et ne pas avoir suivi de formation l'année précé- dente ;*
   - *être au chômage depuis un an ou plus et ne pas avoir suivi de formation l'année précédente ;*

— *avoir moins de 45 ans, être au chômage depuis moins de un an et avoir suivi une formation l'année précédente.*

Les personnes qui ne répondent à aucun de ces quatre critères, pourront par- ticiper à un stage d'insertion en entreprise.

(a) Écrire l'expression booléenne F en fonction des variables a, b et c qui traduit le fait que la personne pourra suivre cette formation qualifiante.

(b) En déduire une caractérisation simple des personnes qui participeront à un stage d'insertion en entreprise.

Fin du Chapitre

Chapitre 2

Logique des prédicats

Qu'est-ce donc qu'un raisonnement ? Si l'on sait que tous les écureuils sont des rongeurs, que tous les rongeurs sont des mammifères, que tous les mammifères sont des vertébrés et que tous les vertébrés sont des animaux, on peut en déduire que tous les écureuils sont des animaux.[...].

Ce raisonnement est simple à l'extrême, mais sa structure ne diffère pas fondamentalement de celle d'un raisonnement mathématique. Dans les deux cas, le raisonnement est formé d'une suite de propositions dans laquelle chacune découle logiquement des précédentes, [...]. Dans ce cas, on applique la même règle trois fois. Cette règle permet, si l'on sait déjà que tous les Y sont des X et que tous les Z sont des Y, de déduire que tous les Z sont des X [Dow07].

I Les propositions

L'homme exprime son raisonnement par un discours, et ce discours utilise une langue (une langue naturelle, français, anglais,...). Ce discours est articulé en phrases et c'est l'étude de ces « énoncés » que se propose de faire la logique.

DÉFINITION 2.1 (PROPOSITION). Parmi tous les énoncés possibles qui peuvent être formulés dans une langue, on distingue ceux auxquels il est possible d'attribuer une « valeur de vérité » : vrai ou faux. Ces énoncés porteront le nom de *propositions* .

EXEMPLE 2.1. Ainsi, « Henri IV est mort assassiné en 1610 », « Napoléon Bonaparte a été guillotiné en 1852 » sont des propositions, puisqu'on peut leur attribuer une valeur de vérité (« vrai » pour la première, « faux » pour la seconde).

Le calcul que l'on étudie considère toujours comme acquises les vérités suivantes, élevées au rang d'axiomes.

Principe de non-contradiction : Une proposition ne peut être simultanément vraie et fausse.

Principe du tiers-exclu : Une proposition est vraie ou fausse (il n'y a pas d'autre possibilité).

II Les connecteurs logiques

L'analyse logique d'une phrase (reconnue comme proposition) fait apparaître des sous-phrases qui constituent elles-mêmes des propositions. Ces « membres de phrases » sont reliés entre eux par des « connecteurs logiques ».

Considérons l'énoncé : « J'ai obtenu une mauvaise note à cet examen parce que je n'ai pas assez travaillé ou parce que le cours est trop difficile ». On suppose qu'il est possible d'attribuer une valeur de vérité à cet énoncé « global », ce qui le classe parmi les propositions.

Globalement, cet énoncé exprime que « ma mauvaise note » est conséquence de l'une (au moins) des deux causes suivantes :

— « mon manque de travail »,

— « un cours trop difficile », soit :

(« mon manque de travail » ou « cours trop difficile ») entraîne « ma mauvaise note »

Attention, le calcul propositionnel ne se préoccupe que des valeurs de vérité, et pas du tout des liens sémantiques qui peuvent exister entre des propositions. Ces dernières sont reliées entre elles syntaxiquement par des connecteurs comme « ou » ou « entraîne ». Les connecteurs logiques sont donc des symboles qui permettent de produire des propositions (« plus complexes ») à partir d'autres propositions (« plus simples »).

II.1 Tables de vérité des connecteurs logiques

P	Q	$P \vee Q$
F	F	F
F	V	V
V	F	V
V	V	V

P	Q	$P \wedge Q$
F	F	F
F	V	F
V	F	F
V	V	V

P	$\neg P$
F	V
V	F

P	Q	$P \Rightarrow Q$
F	F	V
F	V	V
V	F	F
V	V	V

P	Q	$P \Longleftrightarrow Q$
F	F	V
F	V	F
V	F	F
V	V	V

REMARQUE 2.1. — Dans le langage courant, le mot « ou » est souvent employé de deux façons distinctes :
— il est parfois utilisé avec le sens « les deux cas peuvent se produire » (comme ici) et,
— parfois avec le sens « p ou q , mais pas les deux » (e.g. « il ira à Paris ou à Marseille »).
Sauf indication contraire, le « ou » sera toujours employé avec cette première signification.
— Lorsque la proposition P est fausse, la proposition « Si P, alors Q » est vraie, quelle que soit la valeur de vérité de la proposition Q,

Exercice 2.2. *Déterminer la valeur de vérité des propositions suivantes* dans le monde actuel *(c.-à-d. celui dans lequel nous vivons) :*

1. *« si la terre est plate, alors la lune est carrée ; »*
2. *« si le soleil tourne autour de la terre alors la terre est ronde »*
3. *« si la terre est ronde alors le soleil tourne autour de la terre »*
4. *« si vous étudiez la logique alors $E = m.c^2$ »*

Exercice 2.3. *En notant M et C les affirmations suivantes :*
— *M = « Jean est fort en Maths »,*
— *C = « Jean est fort en Chimie »,*
représenter les affirmations qui suivent sous forme symbolique, à l'aide des lettres M et C et des connecteurs usuels.

1. *« Jean est fort en Maths mais faible en Chimie »*
2. *« Jean n'est fort ni en Maths ni en Chimie »*
3. *« Jean est fort en Maths ou il est à la fois fort en Chimie et faible en Maths »*

Exercice 2.4.

1. *Dans un même tableau, construire les tables de vérité de $P \wedge Q$, $\neg(P \wedge Q)$, $\neg P \wedge \neg Q$, $P \wedge \neg Q$ $P \vee Q$, $\neg(P \vee Q)$, $\neg P \vee \neg Q$, $P \Rightarrow Q$ et $\neg(P \Rightarrow Q)$*
2. *Définir les négations de $P \wedge Q$, $P \vee Q$ et $P \Rightarrow Q$.*

PROPRIÉTÉ 2.1 : On a les règles syntaxiques suivantes de simplification de négations :
— $\neg(A \vee B) = (\neg A) \wedge (\neg B)$;
— $\neg(A \wedge B) = (\neg A) \vee (\neg B)$;
— $\neg\neg A = A$;
— $\neg(A \Rightarrow B) = A \wedge (\neg B)$.
On remarque que la troisième règle se déduit des trois autres : $\neg(A \Rightarrow B) = \neg(\neg A \vee B) = (\neg\neg A) \wedge (\neg B)$.

Exercice 2.5. *Énoncer la négation des affirmations suivantes en évitant d'employer l'expression : « il est faux que »*

1. *« S'il pleut ou s'il fait froid je ne sors pas »*
2. *« Le nombre 522 n'est pas divisible par 3 mais il est divisible par 7 »*
3. *« Ce quadrilatère n'est ni un rectangle ni un losange »*
4. *« Si Paul ne va pas travailler ce matin il va perdre son emploi »*

II.2 Variables et formules propositionnelles

Comme le calcul propositionnel ne s'occupe que des valeurs de vérité, il est possible, dans une expression logique, de remplacer chaque proposition donnée par un symbole (en général, une lettre de l'alphabet majuscule), ou *variable propositionnelle* et d'étudier ensuite les valeurs de vérité de l'expression en fonction des valeurs de vérité de ces symboles.

PROPRIÉTÉ 2.2 : Les règles (de syntaxe) qui permettent de former des *formules propositionnelles* sont les suivantes :

- toute variable propositionnelle est une formule propositionnelle ;
- si F et G sont des formules propositionnelles, alors $\neg(F)$, $(F) \vee (G)$, $(F) \wedge (G)$, $(F) \Rightarrow (G)$ et $(F) \iff (G)$ sont des formules propositionnelles.

REMARQUE 2.2. Ce ne sont plus des propositions, en ce sens qu'elles n'ont en général pas de valeur de vérité déterminée. Cette dernière est une fonction des valeurs de vérité des variables propositionnelles qui interviennent dans l'expression de la formule propositionnelle considérée.

Exercice 2.6. *A et B sont des variables propositionnelles, susceptibles de représenter n'importe quelle proposition. Formaliser, à l'aide de connecteurs logiques appropriés, les énoncés suivants :*

1. *« A si B »*
2. *« A est condition nécessaire pour B »*
3. *« A seulement si B »*
4. *« A est condition suffisante pour B »*
5. *« A bien que B »*
6. *« Non seulement A, mais aussi B »*
7. *« A et pourtant B »*
8. *« Ni A, ni B »*

Exercice 2.7. *Les variables propositionnelles N et T serviront, dans cet exercice, à représenter (respectivement) les propositions « Un étudiant a de bonnes notes » et « Un étudiant travaille ». À l'aide des variables propositionnelles N et T, formaliser les propositions suivantes (si, pour l'une ou l'autre d'entre elles, la traduction vous paraît impossible, dites-le et expliquez pourquoi) :*

1. *C'est seulement si un étudiant travaille qu'il a de bonnes notes.*
2. *Un étudiant n'a de bonnes notes que s'il travaille.*
3. *Pour un étudiant, le travail est une condition nécessaire à l'obtention de bonnes notes.*
4. *Malgré son travail, un étudiant a de mauvaises notes.*
5. *Un étudiant travaille seulement s'il a de bonnes notes.*

Exercice 2.8. *Combien de lignes contient la table de vérité d'une formule propositionnelle qui dépend de n variables ?*

Lorsqu'on remplace, dans une formule propositionnelle, les variables propositionnelles par des propositions, l'assemblage obtenu est une proposition. Cependant, une formule propositionnelle n'est pas une proposition : $A \Rightarrow B$ n'est ni vrai ni faux.

PROPRIÉTÉ 2.3 (RÈGLES DE PRIORITÉ DES CONNECTEURS LOGIQUES) : Les conventions de priorité des connecteurs logiques sont les suivantes (par ordre de priorité décroissante) :

- la négation,
- la conjonction et la disjonction (au même niveau),
- l'implication et l'équivalence (au même niveau).

EXEMPLE 2.9. $\neg A \wedge B \Rightarrow C$ doit être interprété par $((\neg A) \wedge B) \Rightarrow C$ et $A \vee B \wedge C$ n'a pas de sens, car les deux connecteurs ont même niveau de priorité.

PROPRIÉTÉ 2.4 (ASSOCIATIVITÉ DES OPÉRATEURS $\vee$ ET $\wedge$) : Les opérateurs $\vee$ et $\wedge$ sont associatifs :
— $(A \vee B) \vee C = A \vee (B \vee C) = A \vee B \vee C$,
— $(A \wedge B) \wedge C = A \wedge (B \wedge C) = A \wedge B \wedge C$.
Mais le parenthésage est obligatoire quand $\vee$ et $\wedge$ se trouvent dans la même proposition, puisqu'il n'y a pas de priorité entre $\vee$ et $\wedge$: $(A \vee B) \wedge C \neq A \vee (B \wedge C)$.

Exercice 2.10. *Construire les tables de vérité des formules propositionnelles suivantes :*

1. $(P \vee Q) \vee (\neg R)$
2. $P \vee (\neg(Q \wedge R))$
3. $(\neg P) \Rightarrow ((\neg Q) \vee R)$
4. $(P \vee R) \Rightarrow (R \vee (\neg P))$
5. $(P \Rightarrow (\neg Q)) \vee (Q \Rightarrow R)$
6. $(P \vee (\neg Q)) \Rightarrow ((\neg P) \vee R)$
7. $(P \Rightarrow (\neg R)) \vee (Q \wedge (\neg R))$
8. $(P \Rightarrow Q) \Rightarrow ((Q \Rightarrow R) \Rightarrow (P \Rightarrow R))$

III Sémantique du calcul propositionnel

Dans ce qui suit, on donne un sens aux symboles représentant les connecteurs logiques en fonction de la valeur de vérité des propositions de base (ainsi $\neg$ signifie non).

III.1 Fonctions de vérité

Soit F une formule propositionnelle, dans l'expression de laquelle interviennent les variables propositionnelles $P_1, P_2, P_3, \ldots, P_n$. À chacune de ces variables propositionnelles, on associe une variable booléenne (généralement la même lettre de l'alphabet, mais en minuscules), qui représente la valeur de vérité qu'elle peut prendre (faux ou vrai, F ou V, 0 ou 1).

DÉFINITION 2.2 (FONCTION DE VÉRITÉ DE F). La fonction de vérité de F est la fonction booléenne Φ_F des n variables booléennes concernées, obtenue de la manière suivante :

1. Si c'est une variable P, propositionnelle, alors $\Phi_P(p) = p$.
2. Si c'est une négation d'une formule propositionnelle G, alors $\Phi_{\neg G} = \overline{\Phi_G}$.
3. Si c'est une disjonction entre deux formules propositionnelle G ou H, alors $\Phi_{G \vee H} = \Phi_G + \Phi_H$.
4. Si c'est une conjonction entre deux formules propositionnelle G et H, alors $\Phi_{G \wedge H} = \Phi_G \cdot \Phi_H$.
5. Si elle est de la forme $G \Rightarrow H$, où G et H sont des formules propositionnelles, alors $\Phi_{G \Rightarrow H} = \overline{\Phi_G} + \Phi_H$.
6. Si c'est une équivalence entre les formules propostionnelles G et H, alors $\Phi_{G \Leftrightarrow H} = \overline{\Phi_G} \cdot \overline{\Phi_H} + \Phi_G \cdot \Phi_H$.

EXEMPLE 2.11. Soit $F = (A \vee \neg B) \wedge (B \Rightarrow C)$. Cette formule dépend des trois variables A, B et C.On a alors :

$$\Phi_F(a,b,c) = \Phi_{(A \vee \neg B) \wedge (B \Rightarrow C)}(a,b,c) =$$
$$\Phi_{A \vee \neg B}(a,b) \cdot \Phi_{B \Rightarrow C}(b,c) = (\Phi_A(a) + \Phi_{\neg B}(b)) \cdot (\overline{\Phi_B(b)} + \Phi_C(c)) =$$
$$(a + \overline{\Phi_B(b)}) \cdot (\overline{b} + c) = (a + \overline{b}) \cdot (\overline{b} + c) = \overline{b} + ac$$

La détermination de la valeur de vérité d'une proposition composée se ramène à un simple calcul en algèbre de Boole sur la fonction de vérité de la formule propositionnelle associée.

III.2 Formules propositionnelles particulières

On verra dans cette section deux formules particulières : les tautologies et les antilogies.

III.2.1 Tautologies

DÉFINITION 2.3 (TAUTOLOGIE). Toute formule propositionnelle dont la fonction de vérité est la fonction référentielle est appelée *tautologie* .

Ainsi, une tautologie est une formule propositionnelle dont la fonction de vérité est indépendante des valeurs de vérité associées à ses variables. Autrement dit, quelle que soit la valeur de vérité des propositions par lesquelles on remplacerait les variables propositionnelles, la proposition obtenue serait vraie.

NOTATION : La notation utilisée pour marquer une tautologie F est $\models F$ (se lit : « F est une tautologie »).

EXEMPLE 2.12. Soit $F = A \Rightarrow A$. Comme $\Phi_F(a) = \overline{a} + a = 1$, on a $\models F$.

EXEMPLE 2.13. $F = (A \Rightarrow C) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \vee B \Rightarrow C))$.

$$\begin{array}{ll} \Phi_F(a,b,c) & = \\ \overline{\Phi_{A\Rightarrow C}}(a,c) + \overline{\Phi_{B\Rightarrow C}}(b,c) + \Phi_{A\vee B\Rightarrow C}(a,b,c) & = \\ \overline{\overline{a}+c} + \overline{\overline{b}+c} + \overline{a+b}+c & = \\ a\overline{c} + b\overline{c} + \overline{a}\overline{b} + c & = \\ a + b + \overline{a}\overline{b} + c & = 1 + c = 1 \end{array}$$

Il ne faudrait pas croire, au vu de ces exemples simples, que les tautologies se ramènent toutes à des trivialités totalement inintéressantes et indignes d'être énoncées. Ainsi, dans une théorie mathématique, tous les théorèmes sont des tautologies ; la reconnaissance de cette propriété n'est cependant pas toujours complètement évidente...

Exercice 2.14. *Les formules propositionnelles suivantes sont-elles des tautologies ?*

1. $P \Rightarrow ((\neg P) \Rightarrow P)$
2. $\models \neg\neg A \Rightarrow A$
3. $P \Rightarrow (P \Rightarrow P)$
4. $(P \Rightarrow Q) \Rightarrow ((Q \Rightarrow R) \Rightarrow (P \Rightarrow R))$
5. $\models (A \Rightarrow C) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \vee B \Rightarrow C))$
6. $P \Rightarrow (P \Rightarrow Q)$
7. $\models (A \Rightarrow B) \Rightarrow ((A \Rightarrow \neg B) \Rightarrow A)$

III.2.2 Antilogies

DÉFINITION 2.4 (ANTILOGIE). Toute formule propositionnelle dont la fonction de vérité est la fonction nulle est appelée *antilogie* .

La proposition obtenue en remplaçant les variables par des propositions ne peut alors jamais être vraie.

EXEMPLE 2.15. Soit $F = A \wedge \neg A$. $\Phi_F(a) = a \cdot \overline{a} = 0$. Donc F est bien une antilogie.

Exercice 2.16. *Calculer les fonctions de vérité des formules propositionnelles suivantes, et dire s'il s'agit éventuellement de tautologies ou d'antilogies :*

1. $A \wedge (A \vee B) \Longleftrightarrow A$
2. $(\neg A \vee B \Rightarrow (A \Rightarrow \neg A \vee B)) \Longleftrightarrow (\neg A \vee B \Rightarrow (A \Rightarrow (A \Rightarrow B)))$
3. $(A \Rightarrow B) \wedge (A \vee C) \Rightarrow B \vee C$
4. $(A \Rightarrow B) \wedge (A \vee C) \Rightarrow (A \Rightarrow C)$

III.3 Conséquences logiques

Soit $\mathcal{F} = \{F_1, \ldots, F_n\}$ un ensemble de formules propositionnelles .

DÉFINITION 2.5 (CONSÉQUENCE LOGIQUE). On dit que la formule propositionnelle A est une *conséquence logique* des formules propositionnelles $F_1, \ldots, F_n$ lorsque, chaque fois que les fonctions de vérité Φ_{F_1}, ..., Φ_{F_n} prennent simultanément la valeur « vrai » (ou 1), il en est de même pour la fonction de vérité de la forme A.

NOTATION : On note ce résultat : $\{F_1, \ldots, F_n\} \models A$ (se lit : A est conséquence logique de $\{F_1, \ldots, F_n\}$).

EXEMPLE 2.17. On reconsidère l'ensemble des deux formules propositionnelles

$$\{P, P \Rightarrow Q\}$$

et on va montrer autrement que Q est conséquence logique de ces deux formules. Autrement dit, on va remontrer que : $\{P, P \Rightarrow Q\} \models Q$.

— $\Phi_P(p) = p$: prend la valeur 1 lorsque p prend la valeur 1.
— $\Phi_{P\Rightarrow Q}(p, q) = \overline{p} + q$: prend la valeur 1 lorsque $p = 0$ (quelle que soit la valeur de q) et lorsque $p = 1$ et $q = 1$.
— $\Phi_P(p)$ et $\Phi_{P\Rightarrow Q}(p, q)$ prennent simultanément la valeur 1 uniquement lorsque $p = 1$ et $q = 1$; dans ce cas, $\Phi_Q(q) = q = 1$ aussi. Donc Q est conséquence logique de $\{P, P \Rightarrow Q\}$.

Exercice 2.18. *Dans chacun des cas suivants, déterminer si le premier ensemble de formules a pour conséquence logique la deuxième formule :*

1	$\{P \Rightarrow (Q \vee R)\}$	$(P \Rightarrow Q) \vee (P \Rightarrow R)$
2	$\{A \Rightarrow (P \vee Q), \neg S \vee A\}$	$(\neg P \vee S) \Rightarrow Q$
3	$\{A \Rightarrow (B \wedge C), \neg C \vee D \vee R, R \Rightarrow \neg B\}$	$(A \wedge D) \Rightarrow \neg R$

Exercice 2.19. *Dans chacun des cas suivants, que peut-on dire d'une formule propositionnelle :*

1. *qui a pour conséquence logique une antilogie,*
2. *qui a pour conséquence logique une tautologie,*
3. *qui est conséquence logique d'une antilogie,*
4. *qui est conséquence logique d'une tautologie.*

Exercice 2.20. *La formule propositionnelle F étant fixée, que peut-on dire d'une formule propositionnelle G qui possède chacune des deux propriétés :*

— *$F \vee G$ est une tautologie,*
— *$F \wedge G$ est une antilogie.*

III.4 Formules équivalentes

DÉFINITION 2.6 (FORMULES ÉQUIVALENTES). Si la formule propositionnelle G est conséquence logique de la formule propositionnelle F et si F est aussi conséquence logique de G, alors ces deux formules sont dites *équivalentes* (que l'on note $\approx$), soit :

$$\{F\} \models G \text{ et } \{G\} \models F \text{ si et seulement si } F \approx G.$$

C'est cette notion de formules équivalentes qui autorise le remplacement d'une expression par une autre (équivalente, bien sûr) dans une formule propositionnelle.

REMARQUE 2.3. On est autorisé à remplacer $\neg\neg A$ par A, puisque ces formules sont équivalentes.

Exercice 2.21. *Dans chacun des cas suivants, dire si les deux formules propositionnelles inscrites sur la même ligne sont équivalentes :*

1	$\neg(\neg P)$	P
2	$P \wedge (P \Rightarrow Q)$	$P \wedge Q$
3	$P \Rightarrow Q$	$(\neg P) \vee (P \wedge Q)$
4	$P \Rightarrow Q$	$(\neg P) \Rightarrow (\neg Q)$
5	$P \vee Q$	$\neg((\neg P) \wedge (\neg Q))$
6	$P \wedge Q$	$\neg((\neg P) \vee (\neg Q))$
7	$\neg P$	$(\neg(P \vee Q)) \vee ((\neg P) \wedge Q)$
8	$P \Rightarrow (Q \Rightarrow R)$	$(P \Rightarrow Q) \Rightarrow R$
9	$P \Rightarrow (Q \wedge R)$	$(P \Rightarrow Q) \wedge (P \Rightarrow R)$
10	$P \Rightarrow (Q \vee R)$	$(P \Rightarrow Q) \vee (P \Rightarrow R)$
11	$(P \Rightarrow Q) \wedge (Q \Rightarrow P)$	$(P \wedge Q) \Rightarrow (P \wedge Q)$
12	$(P \wedge Q) \vee (Q \wedge R) \vee (R \wedge P)$	$(P \vee Q) \wedge (Q \vee R) \wedge (P \vee R)$

Exercice 2.22. *Soit F une formule propositionnelle dépendant de trois variables P, Q, R qui possède deux propriétés :*

— *$F(P, Q, R)$ est vraie si P, Q, R sont toutes les trois vraies,*

— *la valeur de vérité de $F(P, Q, R)$ change quand celle d'une seule des trois variables change.*

Construire la table de vérité de F, et déterminer une formule possible pour F.

Réponse : table de vérité

P	Q	R	F
V	V	V	V
V	V	F	F
V	F	V	F
F	V	V	F
V	F	F	V
F	F	V	V
F	V	F	V
F	F	F	F

Formule : $(P \wedge Q \wedge R) \vee (P \wedge \neg Q \wedge \neg R) \vee (\neg P \wedge \neg Q \wedge R) \vee (\neg P \wedge Q \wedge \neg R)$

III.5 Simplification du calcul des fonctions de vérité

PROPRIÉTÉ 2.5 (THÉORÈME DE LA VALIDITÉ) : Soit $\{G_1, G_2, \ldots, G_n\}$ un ensemble de formules propositionnelles et H une formule propositionnelle ; alors :

$$\{G_1, G_2, \ldots, G_{n-1}\} \models G_n \Rightarrow H \text{ si et seulement si } \{G_1, G_2, \ldots, G_n\} \models H$$

PREUVE **Si.** Supposons $\{G_1, G_2, \ldots, G_n\} \models H$, c'est à dire, chaque fois que les formules de $\{G_1, G_2, \ldots, G_n\}$ sont vraies, H l'est aussi). Supposons que les formules de $\{G_1, G_2, \ldots, G_{n-1}\}$ soient vraies :

— Alors, si G_n est vraie, toutes les formules de $\{G_1, G_2, \ldots, G_n\}$ sont vraies, et donc, d'après l'hypothèse, H est vraie. Dans ce cas (voir table de vérité de l'implication logique), $G_n \Rightarrow H$ est vraie.

— Et si G_n n'est pas vraie, alors $G_n \Rightarrow H$ est vraie.

Seulement si. Supposons $\{G_1, G_2, \ldots, G_{n-1}\} \models G_n \Rightarrow H$. En d'autres termes, chaque fois que les formules de $\{G_1, G_2, \ldots, G_{n-1}\}$ sont vraies, $G_n \Rightarrow H$ est vraie. Regardons si H est une conséquence logique de $\{G_1, G_2, \ldots, G_n\}$ en distinguant selon que G_n est vraie ou pas.

— soit lorsque G_n n'est pas vraie, indépendamment de la valeur de vérité de H sur laquelle on ne peut alors rien dire, mais peu importe, puisque, dans ce cas, les formules de $\{G_1, G_2, \ldots, G_n\}$ ne sont pas toutes vraies, puisque G_n n'est pas vraie.

— soit lorsque G_n est vraie, et, dans ce cas, on sait que H est obligatoirement vraie aussi. Ceci se produit chaque fois que toutes les formules de $\{G_1, G_2, \ldots, G_n\}$ sont vraies, et, dans ce cas, H l'est aussi. Donc $\{G_1, G_2, \ldots, G_n\} \models H$. ∎

EXEMPLE 2.23 (EXEMPLE D'APPLICATION). Soit à montrer que :

$$\models (A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C)).$$

On pourrait bien entendu déterminer la fonction de vérité de cette formule. Mais, d'après le théorème précédent, la démonstration du résultat demandé est équivalente à celle de :

$$\{A \Rightarrow (B \Rightarrow C)\} \models (A \Rightarrow B) \Rightarrow (A \Rightarrow C).$$

Une nouvelle application de ce même théorème nous montre que la démonstration demandée est encore équivalente à celle de :

$$\{A \Rightarrow (B \Rightarrow C), (A \Rightarrow B)\} \models (A \Rightarrow C).$$

Et enfin à celle de :

$$\{A \Rightarrow (B \Rightarrow C), (A \Rightarrow B), A\} \models C.$$

Or les fonctions de vérité de $\{A \Rightarrow (B \Rightarrow C), (A \Rightarrow B), A\}$ sont

$$\begin{cases} \overline{a} + \overline{b} + c \\ \overline{a} + b \\ a \end{cases} \quad \text{qui valent sim. 1 quand} \quad \begin{cases} a = 1 \\ b = 1 \\ c = 1 \end{cases}$$

Ainsi C est vraie et on a terminé la démonstration.

Exercice 2.24. *Trois dirigeants d'une Société (Pierre P., Marc M. et Alain A.) sont prévenus de malversations financières ; au cours de l'enquête, l'agent du fisc enregistre leurs déclarations :*

- *Pierre P. : "Marc est coupable et Alain est innocent".*
- *Marc M. : "Si Pierre est coupable, Alain l'est aussi".*
- *Alain A. : "Je suis innocent, mais l'un au moins des deux autres est coupable".*

1. *Ces trois témoignages sont-ils compatibles ?*
2. *En supposant qu'ils sont tous les trois innocents, lequel a menti ?*
3. *En supposant que chacun dit la vérité, qui est innocent et qui est coupable ?*
4. *En supposant que les innocents disent la vérité et que les coupables mentent, qui est innocent et qui est coupable ?*

Exercice 2.25. *Simplifier le règlement suivant :*

- *Les membres de la Direction Financière doivent être choisis parmi ceux de la Direction Générale.*
- *Nul ne peut être à la fois membre de la Direction Générale et de la Direction Technique s'il n'est membre de la Direction Financière.*
- *Aucun membre de la Direction Technique ne peut être membre de la Direction Financière.*

Exercice 2.26. *Un inspecteur des services de santé visite un hôpital psychiatrique où des phénomènes étranges lui ont été signalés.*

Dans cet hôpital, il n'y a que des malades et des médecins, mais les uns comme les autres peuvent être sains d'esprit ou totalement fous. L'inspecteur doit faire sortir de l'hôpital les personnes qui n'ont rien à y faire, c'est à dire les malades sains d'esprit et les médecins totalement fous (quitte à les réintégrer ultérieurement en tant que malades...). Il part du principe que les personnes saines d'esprit ne disent que des choses vraies, alors que les personnes folles ne disent que des choses fausses.

Dans une salle, il rencontre deux personnes (appelons-les A et B pour préserver leur anonymat). A affirme que B est fou et B affirme que A est médecin.

1. *Après une intense réflexion, l'inspecteur fait sortir l'un des deux de l'hôpital. Lequel (et pourquoi ?)*
2. *Peut-il dire quelque chose au sujet de l'autre ?*

Exercice 2.27. *Le prince de Beaudiscours est dans un cruel embarras. Le voici au pied du manoir où la méchante fée Antinomie maintient prisonnière la douce princesse Vérité. Deux portes y donnent accès. L'une d'elles conduit aux appartements de la princesse, mais l'autre s'ouvre sur l'antre d'un dragon furieux. Le prince sait seulement que l'une de ces deux portes s'ouvre lorsqu'on énonce une proposition vraie, et l'autre si on énonce une proposition fausse.*

Comment peut-il délivrer la princesse ?

Exercice 2.28. *Que dire des raisonnements suivants ?*

1. *Si Jean n'a pas rencontré Pierre l'autre nuit, c'est que Pierre est le meurtrier ou que Jean est un menteur. Si Pierre n'est pas le meurtrier, alors Jean n'a pas rencontré Pierre l'autre nuit et le crime a eu lieu après minuit. Si le crime a eu lieu après minuit, alors Pierre est le meurtrier ou Jean n'est pas un menteur. Donc Pierre est le meurtrier*
2. *Manger de la vache folle est dangereux pour la santé ; manger du poulet aux hormones aussi, d'ailleurs. Quand on ne mange pas de la vache folle, on mange du poulet aux hormones. Notre santé est donc en danger.*
3. *Si je n'étudie pas, j'ai des remords. Mais si je ne vis pas à fond ma jeunesse, j'ai aussi des remords. Or je n'ai pas de remords. C'est donc que j'étudie tout en vivant à fond ma jeunesse.*
4. *Quand Marie est là, c'est qu'elle accompagne Paul ou Jean. Paul ne vient jamais en même temps que son cousin Serge. Si Jean et Serge viennent tous les deux, leur sœur Louise les accompagne. Si Louise se pointe, Raoul ne reste pas. Hier, Raoul et Serge étaient présents jusqu'au bout. Peut-on en conclure que Marie n'était pas présente ?*

Fin du Chapitre

Deuxième partie

Théorie des ensembles

Chapitre 3

Introduction à la théorie des ensembles

I Rappels de théorie des ensembles

I.1 Notion première d'ensemble

Ensemble Un ensemble est une collection d'objets distincts réunis en vertu d'une propriété commune.

On peut définir un ensemble de deux manières :

— *en extension* : on donne la liste exhaustive des éléments qui y figurent,

— *en compréhension* : en donnant la propriété que doivent posséder les éléments de l'ensemble.

NOTATION : On note $\mathbb{N}_n$ l'ensemble des entiers inférieurs ou égaux à n.

Exercice 3.1.

1. *Définir les ensembles suivants en compréhension :*
   (a) *A = {1,2,4,8,16,32,64} ;*
   (b) *B = {1,2,7,14}.*
2. *Définir les ensembles suivants en extension :*
   (a) $A = \{x \in \mathbb{R} | x(x+5) = 14\}$;
   (b) $C = \{x \in \mathbb{N}_{10}^* | x^4 - 1$ *est divisible par 5* $\}$.

I.2 Règles de fonctionnement

Relation d'appartenance. On admet être capable de décider si un objet est ou non élément d'un ensemble. Le fait que l'élément x appartienne à l'ensemble X se note : $x \in X$.

Objets distincts. On admet aussi être capable de distinguer entre eux les éléments d'un ensemble. En particulier, un ensemble ne peut pas contenir deux fois le même objet.

Ensemble vide. Il existe un ensemble ne contenant aucun élément, appelé ensemble vide : $\varnothing$. L'ensemble vide ne correspond pas à rien ; c'est en fait un ensemble qui ne contient rien, mais en tant qu'ensemble il n'est pas rien : un sac vide est vide, mais le sac en lui même existe.

Dernière règle de fonctionnement des ensembles. Un ensemble ne peut pas s'appartenir à lui-même.

I.3 Sous-ensembles, ensemble des parties

Les sous-ensembles sont définis par la relation d'inclusion...

DÉFINITION 3.1. A est un sous-ensemble de B ($A \subset B$) » si et seulement si tout élément de A appartient à B. On dit aussi que A est une partie de B.

PROPRIÉTÉ 3.1 : L'ensemble vide est inclus dans n'importe quel ensemble.

PREUVE Raisonnons par l'absurde : si l'ensemble vide n'est pas inclus dans A, alors il existe au moins un élément de l'ensemble vide qui n'appartient pas à A. Ceci est absurde puisque l'ensemble vide est vide. ∎

PROPRIÉTÉ 3.2 : Tout ensemble est inclus dans lui-même.

DÉFINITION 3.2. Soit A un ensemble. L'ensemble des parties de A, noté $\mathcal{P}(A)$, est l'ensemble de tous les sous-ensembles de A.

PROPRIÉTÉ 3.3 : Pour tout ensemble A, on a $\varnothing, A \in \mathcal{P}(A)$.

EXEMPLE 3.2. Si $A = \{1, 2, 3\}$, alors $\mathcal{P}(A) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

Exercice 3.3. *Justifier le fait que le nombre d'éléments de $\mathcal{P}(A)$ est égal à 2^n, où n représente le nombre d'éléments de A.*

Exercice 3.4. *On considère A = {1,2}. Dire quelles assertions sont exactes :*

1. $1 \in A$,
2. $1 \subset A$,
3. $\{1\} \in A$,
4. $\{1\} \subset A$,
5. $\varnothing \in A$,
6. $\varnothing \subset A$.

Exercice 3.5. *Reprendre l'exercice précédent, avec $A = \{\{1\}, \{2\}\}$.*

Exercice 3.6. *Est-ce que $\{a\} \in \{a, b, c\}$? Former la liste des parties de $\{a, b, c\}$.*

Exercice 3.7. *Montrer que $\mathcal{P}(A) \subset \mathcal{P}(B)$ quand $A \subset B$.*

II Opérations sur les ensembles

II.1 Égalite de deux ensembles

DÉFINITION 3.3. Deux ensembles sont *égaux* si et seulement si ils ont les mêmes éléments.

$A \subset B$ et $B \subset A \iff A = B$.

Exercice 3.8. *Dans chacun des cas suivants, déterminer si les ensembles sont égaux :*

1. $A = \{x \in \mathbb{R} | x > 0\}$ *et* $B = \{x \in \mathbb{R} | x \geqslant |x|\}$ *;*
2. $A = \{x \in \mathbb{R} | x > 0\}$ *et* $B = \{x \in \mathbb{R} | x \leqslant |x|\}$ *;*
3. $A = \mathbb{Z}$ *et* $B = \{x \in \mathbb{Z} | x(x-1)$ *pair* $\}$ *; on pourra réfléchir sur la parité de* $x(x-1)$.

II.2 Réunion, intersection

DÉFINITION 3.4 (REUNION). La *réunion* des deux ensembles A et B, notée $A \cup B$ est l'ensemble des éléments qui sont éléments de A ou de B.

EXEMPLE 3.9. $A = \{1, 2, 3\}, B = \{1, 4, 5\},$ alors $A \cup B = \{1, 2, 3, 4, 5\}$

DÉFINITION 3.5 (INTERSECTION). L'*intersection* des deux ensembles A et B, notée $A \cap B$, est l'ensemble des éléments communs à A et à B.

PROPRIÉTÉ 3.4 (PROPRIÉTÉS DE LA RÉUNION ET DE L'INTERSECTION) : La réunion de deux ensembles possède certaines propriétés :

— idempotence : $A \cup A = A$ et $A \cap A = A$;
— commutativité : $A \cup B = B \cup A$ et $A \cap B = B \cap A$;
— associativité : $A \cup (B \cup C) = (A \cup B) \cup C$ et $A \cap (B \cap C) = (A \cap B) \cap C$;
— éléments neutres : $A \cup \varnothing = A$ et $A \cap \Omega = A$.

Exercice 3.10.

Construire la réunion puis l'intersection des ensembles $A = \{x \in \mathbb{R} | 0 \leqslant x \leqslant 3\}$, $B = \{x \in \mathbb{R} | -2 < x \leqslant 1\}$.

Exercice 3.11. *Faire la réunion des ensembles A et B, quand* $A = \{x \in \mathbb{N} | x$ *impair* $\}$, *et* $B = \{x \in \mathbb{N} | x$ *pas divisible par 3* $\}$.

PROPRIÉTÉ 3.5 (DISTRIBUTIVITÉS DE $\cup$ ET $\cap$) : On a les distributivités :

— de $\cup$ sur $\cap$: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
— de $\cap$ sur $\cup$: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Exercice 3.12. *On se donne trois ensembles* A, B, C *tels que* $A \cap B \cap C = \varnothing$. *Sont-ils nécessairement disjoints deux à deux ? Donner des exemples.*

II.3 Complémentation

DÉFINITION 3.6 (COMPLÉMENTATION). Pour $A \subset E$, on définit le *complémentaire* de A par rapport à E comme l'ensemble des éléments de E qui ne sont pas éléments de A. On note le complémentaire de A dans E : $E \setminus A$ (« E moins A ») ou $\bar{A}$ quand ce n'est pas ambiguë.

PROPRIÉTÉ 3.6 : La complémentation a plusieurs propriétés remarquables :

— involution : $\bar{\bar{A}} = A$,
— loi de De Morgan : $\overline{A \cup B} = \overline{A} \cap \overline{B}$, et $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

Exercice 3.13. *Pour deux ensembles* A *et* B, *on appelle différence symétrique, note* $A \Delta B$, *l'ensemble défini par* $A \Delta B = (A \cup B) \setminus (A \cap B)$ *c'est-à-dire que* $A \Delta B$ *est constitué des éléments qui appartiennent soit à* A, *soit à* B, *mais pas aux deux.*

1. *Montrez que* $A \Delta B = [A \cap (E \setminus B)] \cup [(E \setminus A) \cap B]$.
2. *Simplifier les expressions* $A \Delta A$, $A \Delta (E \setminus A)$, $A \Delta E$ *et* $E \setminus (A \triangle B)$.
3. *Montrer que, si* $A \triangle B = C$, *alors* $A \triangle C = B$ *et* $B \triangle C = A$.
4. *Montrer que si* $A \Delta B = A \Delta C$ *alors* $B = C$.

II.4 Produit cartésien

Le produit cartésien des ensembles A et B (dans cet ordre) est l'ensemble, que l'on note $A \times B$ (« A croix B ») des couples ordonnés (a, b) où $a \in A$ et $b \in B$. Dans le couple (a, b) :

— (a, b) n'est pas un ensemble et
— (a, b) est distinct de (b, a).

Exercice 3.14. *Énumérez les éléments de* $\{a, b, c\} \times \{1, 2\}$. *Combien y en a-t-il ?*

III Exercices supplémentaires

Exercice 3.15. *Soit E un ensemble non vide et A, B, C, X, Y des parties de E.*

1. *Montrer que si on a $(X \cap A = X \cap B)$ et $Y \subset X$ sont alors on a $Y \cap A = Y \cap B$.*
2. *Montrer que si on a $(A \cup C) \subset (A \cup B)$ et $(A \cap C) \subset (A \cap B)$ alors on a $C \subset B$.*
3. *Montrer que si on a $A \subset (B \cap C)$ et $(B \cup C) \subset A$ alors on a $A = B = C$.*

Exercice 3.16. *Soit E un ensemble non vide et $\mathcal{P}(E)$ l'ensemble de ses parties.*

Soit f une application croissante, pour l'inclusion, de $\mathcal{P}(E)$ dans lui-même (c'est-à-dire : si X et Y sont deux parties de E et si $X \subset Y$, alors $f(X) \subset f(Y)$).

1. *Montrer que, pour tout couple (X, Y) de parties de E, on a : $f(X) \cup f(Y) \subset f(X \cup Y)$.*
2. *On dit qu'une partie X de E est régulière si et seulement si $f(X) \subset X$. Montrer qu'il existe au moins une partie régulière dans E et que, si X est régulière, il en est de même de $f(X)$.*
3. *Soit A l'intersection de toutes les parties régulières de E. Montrer que A est régulière et que $f(A) = A$.*

Exercice 3.17 (Fonction caractéristique des parties d'un ensemble). *On appelle fonction caractéristique de la partie A de l'ensemble E $(E \neq \emptyset,\ A \neq \emptyset,\ A \subset E)$ l'application $f_A : E \Rightarrow \{0, 1\}$, définie par :*

— $\forall x \in A,\ f_A(x) = 1$;

— $\forall x \in E \setminus A,\ f_A(x) = 0$.

On pose de plus $\forall x \in E, f_\emptyset(x) = 0$ et $f_E(x) = 1$.

Étudier les fonctions caractéristiques d'une réunion, d'une intersection de deux parties, ainsi que celle du complémentaire d'une partie.

Fin du Chapitre

Chapitre 4

Relations binaires entre ensembles

Dans tout ce chapitre, on se donne deux ensembles E et F.

I Relations

DÉFINITION 4.1 (RELATION BINAIRE). On définit une *relation binaire* entre les deux ensembles E et F lorsqu'on construit une partie G de l'ensemble produit $E \times F$ ($G \subset E \times F$). Si x dans E et y dans F sont tels que $(x, y) \in G$, on dit que x est *en Relation avec* y. On note cela $x\mathcal{R}y$.

Exercice 4.1.
1. *Définir la relation « a pour mention au Bac » comme une relation entre deux ensembles.*
2. *Définir l'index d'un livre comme une relation entre deux ensembles.*
3. *Définir le fait d'avoir un compte dans une banque comme une relation entre deux ensembles.*

REMARQUE 4.1. Lorsque $E = F$, on parle de relation binaire définie dans l'ensemble E. Son graphe est une partie de E^2. Dans ce cas, il est possible que $x\mathcal{R}y$ sans que $y\mathcal{R}x$. (Penser à la relation « est plus âgé que »).

II Relations d'ordre

On se place dans le cas où $E = F$. Soit $\mathcal{R}$ une relation binaire définie dans un ensemble E.

II.1 Réflexivité, antisymétrie, transitivité

DÉFINITION 4.2 (RÉFLEXIVITÉ). $\mathcal{R}$ est dite *réflexive* quand tout élément de E est en relation avec lui-même : $\forall x \in E,\ x\mathcal{R}x$.

DÉFINITION 4.3 (ANTISYMÉTRIE). $\mathcal{R}$ est dite *antisymétrique* si, lorsque x est en relation avec y, alors y ne peut pas être en relation avec x (sauf si $x = y$) : $\forall (x, y) \in E^2,\ x\mathcal{R}y$ et $y\mathcal{R}x \Rightarrow\ x = y$.

DÉFINITION 4.4 (TRANSITIVITÉ). $\mathcal{R}$ est dite *transitive* lorsque, si x est en relation avec y, et si y l'est avec z, alors x est en relation avec z : $\forall x \in E,\ \forall y \in E, \forall z \in E,\ x\mathcal{R}y$ et $y\mathcal{R}z \Rightarrow x\mathcal{R}z$.

Exercice 4.2. *Les relations suivantes sont-elles réflexives, antisymétriques ou transitives ?*
1. $A = \mathbb{R}$ *et* $x\mathcal{R}y$ *si* $|x| = |y|$.
2. $A = \mathbb{R}$ *et* $x\mathcal{R}y$ *si* $\sin^2 x + \cos^2 y = 1$.
3. $A = \mathbb{N}$ *et* $x\mathcal{R}y$ *s'il existe* p *et* q *entiers tels que* $y = px^q$.

Exercice 4.3. *Sur* $\mathbb{N}^*$ *on définit la relation* $a\mathcal{R}b$ *si et seulement si* $a^b \leq b^a$.
1. *Vérifier que cette relation est réflexive et transitive.*
2. *Comparer 2 et 4. La relation est-elle antisymétrique ?*

II.2 Relation d'ordre

DÉFINITION 4.5 (RELATION D'ORDRE). $\mathcal{R}$ est une *relation d'ordre* si elle est réflexive, antisymétrique et transitive.

EXEMPLE 4.4. Quelques relations d'ordre : $(\mathbb{R}, \leqslant)$, $(\mathcal{P}(E), \subset)$

EXEMPLE 4.5 (RELATION DE DIVISIBILITÉ). On note $a|b$ si et seulement si b est un multiple de a ($\exists k \in \mathbb{N}^*, b = ka$). C'est une relation d'ordre définie dans $\mathbb{N}^*$. En effet, elle est

réflexive : $a = 1a$, donc $a|a$ est vrai,

antisymétrique : si $a|b$ et $b|a$, alors $\exists k, k' \in \mathbb{N}^*, a = kb$ et $b = k'a$. Donc $a = kk'a$. Comme $a \neq 0$, $kk' = 1$. Mais $k, k' \in \mathbb{N}^*$, donc $k = k' = 1$, et $a = b$.

transitive : si $a|b$ et $b|c$, alors alors $\exists k, k' \in \mathbb{N}^*, a = kb$ et $b = k'c$. Donc $a = kk'c$: il existe $k'' \in \mathbb{N}^*$ ($k'' = kk'$) tel que $a = k''c$: $a|c$.

Exercice 4.6. *On définit une relation binaire $\mathcal{R}$ sur $\mathbb{R} \times \mathbb{R}^+$ par $(x, y)\mathcal{R}(x', y')$ ssi $x^2 + y^2 < x'^2 + y'^2$ ou ($x^2 + y^2 = x'^2 + y'^2$ et $x \leq x'$). Montrer qu'il s'agit d'une relation d'ordre.*

Exercice 4.7 (Diagrammes de transitivité). *On considère...*

1. $E = \{1\,,\,2\,,\,3\,,\,4\,,\,5\,,\,6\,,\,7\,,\,8\,,\,9\}$ *et on définit la relation binaire $\mathcal{R}$ dans E par son graphe $G = \{$(1,1), (1,2), (1,3), (1,4), (1,5), (1,6), (1,7), (1,8), (1,9), (2,2), (2,3), (2,4), (2,6), (2,8), (2,9), (3,3), (4,3), (4,4), (4,6), (4,8), (4,9), (5,3), (5,4), (5,5), (5,6), (5,7), (5,8), (5,9), (6,6), (6,8), (6,9), (7,7), (7,8), (7,9), (8,8), (9,9)$\}$ (c'est-à-dire : $1\mathcal{R}1$, etc...). Justifier que cette relation est une relation d'ordre.*
2. *Mêmes questions pour $E' = \{1\,,\,2\,,\,3\,,\,4\,,\,5\,,\,6\}$ et $G' = \{$(1,1), (1,2), (1,3), (1,4), (1,5), (1,6), (2,2), (2,4), (2,5), (2,6), (3,3), (3,4), (3,6), (4,4), (4,6), (5,5), (5,6), (6,6)$\}$.*

III Relations d'équivalence

On se place encore dans ce paragraphe dans le cas où $E = F$. Soit $\mathcal{R}$ une relation binaire définie dans un ensemble (non vide) E, de graphe G.

DÉFINITION 4.6 (RELATION SYMÉTRIQUE). $\mathcal{R}$ est dite *symétrique* si, dès que x est en relation avec y, alors y est en relation avec x : $\forall x \in E, \forall y \in E,\ x\mathcal{R}y \Rightarrow y\mathcal{R}x$.

DÉFINITION 4.7 (RELATION D'ÉQUIVALENCE). $\mathcal{R}$ est une relation d'équivalence lorsqu'elle est réflexive, symétrique et transitive.

EXEMPLE 4.8. L'égalité est une relation d'équivalence.

EXEMPLE 4.9 (RELATION DE CONGRUENCE MODULO n DANS $\mathbb{Z}$). Par définition :

$$x \equiv y\ [n] \text{(lire : « } x \text{ est congru à } y \text{ modulo } n \text{ »)} \Leftrightarrow \exists k \in \mathbb{Z},\ x - y = k \cdot n.$$

réflexive : $x \equiv x[n]$: en effet, $x - x = 0 \cdot n$, et $0 \in \mathbb{Z}$.

symétrique : si $x \equiv y\ [n]$, $\exists k \in \mathbb{Z}$, $x - y = k \cdot n$; alors $y - x = (-k) \cdot n$; or, si $k \in \mathbb{Z}$, $(-k) \in \mathbb{Z}$, donc $y \equiv x\ [n]$.

transitive : si $x \equiv y\ [n]$ et $y \equiv z\ [n]$, $\exists k \in \mathbb{Z}$, $x - y = k \cdot n$ et $\exists l \in \mathbb{Z}$, $y - z = l \cdot n$. En additionnant membre à membre ces deux égalités, on obtient $x - z = (k + l) \cdot n$, or $(k, l) \in \mathbb{Z}^2$, donc $k + l \in \mathbb{Z}$, donc $x \equiv z\ [n]$.

Exercice 4.10. *Montrer que les relations suivantes sont des relations d'équivalence :*

— *Sur $\mathbb{Z}$, on écrit $x\mathcal{R}y$ quand $x + y$ est pair.*

— *Sur $\mathbb{R}$, on écrit $x\mathcal{R}y$ quand* $\cos(2x) = \cos(2y)$.

III.1 Classes d'équivalence

DÉFINITION 4.8 (CLASSE D'ÉQUIVALENCE). Soit x un élément de E, et $\mathcal{R}$ une relation d'équivalence sur E. On appelle *classe d'équivalence* de cet élément l'ensemble des éléments de E qui sont en relation avec x (on dit encore : « qui sont équivalents à x »).

NOTATION : On note $\dot{x}$ la classe de l'élément x : $\dot{x} = \{y \in E \mid y\mathcal{R}x\}$.

Exercice 4.11. *Dans $\mathbb{R}$, on considère la relation binaire $\mathcal{R}$ définie par : $x\mathcal{R}y$ ssi $x^2 - y^2 = x - y$.*

1. *Vérifier que $\mathcal{R}$ est une relation d'équivalence.*
2. *Pour tout réel x, déterminer $\dot{x}$.*

Exercice 4.12. *Dans $\mathbb{R}$, on considère la relation binaire $\mathcal{R}$ définie par : $x\mathcal{R}y$ ssi $x.e^y = y.e^x$.*

1. *Vérifier que $\mathcal{R}$ est une relation d'équivalence.*
2. *Pour tout réel x, déterminer le nombre d'éléments de $\dot{x}$.*

PROPRIÉTÉ 4.1 : L'intersection de deux classes d'équivalence distinctes est vide. On dit aussi que les classes sont deux à deux disjointes.

PREUVE 1 : *On considère deux classes, $\dot{x}$ et $\dot{y}$, soit $z \in \dot{x} \cap \dot{y}$; $\forall t \in \dot{x}$, on a $(t, x) \in G$; mais $z \in \dot{x}$, donc $(z, x) \in G$, donc (symétrie) $(x, z) \in G$, donc (transitivité) $(t, z) \in G$; mais $z \in \dot{y}$, donc $(z, y) \in G$, donc (transitivité) $(t, y) \in G$, donc (finalement) $t \in \dot{y}$, et donc $\dot{x} \subset \dot{y}$; raisonnement analogue pour tout $t \in \dot{y}$, qui aboutit à $\dot{y} \subset \dot{x}$, et enfin (par double inclusion) $\dot{x} = \dot{y}$; si deux classes ont un élément commun, elles sont confondues ; donc deux classes distinctes sont disjointes).* †

DÉFINITION 4.9 (PARTITION D'UN ENSEMBLE). Une *partition* d'un ensemble E est une famille de sous-ensembles de E, 2 à 2 disjoints, et dont la réunion est égale à E.

PROPRIÉTÉ 4.2 : Les classes d'équivalence réalisent une partition de E.

PREUVE 2 : *Comme les classes sont des parties de E, leur réunion est une partie de E. Réciproquement, tout élément de E appartient à une classe (« tout élément est classé »). Donc E est une partie de la réunion des classes ; et E est égal à la réunion des classes.* †

EXEMPLE 4.13. On reprend la congruence modulo n, par exemple pour $n = 4$.On a :
$\dot{0} = \{\ldots, -12, -8, -4, 0, 4, 8, 12, \ldots\}$
$\dot{1} = \{\ldots, -11, -7, -3, 1, 5, 9, 13, \ldots\}$
$\dot{2} = \{\ldots, -10, -6, -2, 2, 6, 10, 14, \ldots\}$
$\dot{3} = \{\ldots, -9, -5, -1, 3, 7, 11, 15, \ldots\}$

Exercice 4.14. *Soit $\mathcal{R}$ la relation d'équivalence suivante dans l'ensemble $A = \{1, 2, 3, 4, 5, 6\}$: $\mathcal{R} = \{(1,1), (1,5), (2,2), (2,$ Trouver la partition de A induite par $\mathcal{R}$, c'est-à-dire trouver les classes d'équivalence de $\mathcal{R}$.*

Exercice 4.15. *On considère l'ensemble des points du plan rapporté à deux axes de coordonnées rectangulaires et deux points P_1 et P_2 de coordonnées respectives (x_1, y_1) et (x_2, y_2) ; on définit dans cet ensemble la relation binaire $\mathcal{R}$ par :*

1. *$P_1\mathcal{R}P_2 \Leftrightarrow x_1y_1 = x_2y_2$. Est-ce une relation d'équivalence ? Si oui, étudier ses classes.*
2. *Mêmes questions pour $\mathcal{R}$, définie par $P_1\mathcal{R}P_2 \Leftrightarrow x_1y_1 = x_2y_2$ et $x_1x_2 \geqslant 0$*

Fin du Chapitre

Troisième partie

Arithmétique

Chapitre 5

Ensembles de nombres entiers

I Principe de récurrence

Pour démontrer par *récurrence* qu'une propriété $P(n)$ est vraie quel que soit l'entier $n \geq n_0$, on procède en deux étapes :

1. on vérifie que $P(n_0)$ est vraie ;
2. on suppose que $P(n)$ est vraie pour un certain entier $n \geq n_0$, c'est l'hypothèse de récurrence, et on démontre que $P(n+1)$ est vraie.

Le *principe de récurrence* dit alors que $P(n)$ est vraie quel que soit l'entier $n \geq n_0$.

Exercice 5.1. *1. Calculez 1, 1+3, 1+3+5, et 1+3+5+7.*

2. A quoi $1+3+5+7+...+(2n-1)+(2n+1)$ *semble-t-il être égal (en fonction de* n*) ?*

3. Démontrer par récurrence que l'on a effectivement l'égalité.

Exercice 5.2. *Soit la suite* $(U_n)_{n\in\mathbb{N}}$ *définie par* $U_n = 3^{2n+1} + 2^{n+2}$.

1. Calculer U_0*,* U_1 *et* U_2*. Remarquer que ce sont tous des multiples de* 7*.*

2. Montrer que $U_{n+1} = 7 \times 3^{2n+1} + 2U_n$*.*

3. Montrer que 7 *est un multiple de* U_n *pour tout entier naturel* n*.*

Exercice 5.3. *Montrer que pour tout entier naturel* n*, 3 divise* $4^n - 1$.

II Nombres premiers

DÉFINITION 5.1 (MULTIPLE, DIVISEUR). Si un entier n peut s'écrire sous la forme $n = pq$, où p et q sont des entiers, on dit que n est un *multiple* de p et que p est un *diviseur* de n. On écrit aussi $p \mid n$ pour p divise n.

DÉFINITION 5.2 (NOMBRE PREMIER). Un *nombre premier* est un nombre entier strictement supérieur à 1 qui n'est divisible que par 1 et par lui-même.

Ainsi, le plus petit nombre premier (et le seul qui soit pair) est 2.

REMARQUE 5.1. Le problème de la primalité d'un nombre (très grand, évidemment) est difficile.

DÉFINITION 5.3 (DÉCOMPOSITION EN FACTEURS PREMIERS). L'écriture d'un entier n sous la forme $n = a^\alpha b^\beta c^\gamma \ldots$, où

— a, b, c, ... sont des nombres premiers distincts deux à deux tels que $a < b < c < \ldots$ et
— les exposants α, β, γ sont des entiers naturels non nuls

s'appelle la *décomposition en facteurs premiers* de n.

On dit que les exposants α, β, γ, ... sont les ordres de multiplicité des diviseurs a, b, c, ...

PROPRIÉTÉ 5.1 : La décomposition d'un entier en ses facteurs premiers est unique.

Exercice 5.4. *Écrivez les nombres 3850 et 1911 sous forme de produits de nombres premiers.*

Exercice 5.5. *Montrer qu'un entier naturel qui est à la fois le carré d'un nombre et le cube d'un nombre est aussi un nombre à la puissance 6.*

PROPRIÉTÉ 5.2 : Il existe une infinité de nombres premiers.

Exercice 5.6 (Nombres premiers en quantité infinie). *Supposons comme hypothèse que l'ensemble des nombres premiers $\{p_1, p_2, p_3 \dots p_{n-1}, p_n\}$ est de cardinalité finie n. On construit le nombre $N = p_1.p_2.p_3.\dots.p_{n-1}.p_n + 1$.*

1. *Montrer que d'après l'hypothèse, il existe un nombre premier q tel que N est un multiple de q.*
2. *Montrer cependant que N n'est pas un multiple de p_1. Idem pour p_2, $\dots$ p_n.*
3. *En déduire que q est un nombre premier différent de p_1, de p_2, $\dots$ de p_n.*
4. *En déduire une contradiction dans l'hypothèse.*

DÉFINITION 5.4 (PGCD, PPCM). Soient a et b deux entiers naturels strictement positifs.

— L'ensemble des diviseurs communs à a et b admet un plus grand élément d, le *plus grand commun diviseur (PGCD)* de ces entiers. On le note *PGCD*(a, b).

— L'ensemble des multiples strictement positifs communs à a et b admet un plus petit élément m, le *plus petit commun multiple (PPCM)* de ces deux entiers. On le note *PPCM*(a, b).

Pour a et b dans $\mathbb{N}$, *PGCD*(a, b) et *PPCM*(a, b) et sont respectivement notés $a \wedge b$ et $a \vee b$.

DÉFINITION 5.5 (NOMBRES PREMIERS ENTRE EUX). Deux nombres entiers strictement positifs a et b sont dits *premiers entre eux* lorsque $a \wedge b = 1$.

Exercice 5.7 (Nombres de Fermat). *Pour $p \in \mathbb{N}$, les nombres de Fermat sont ceux de la forme $F_p = 2^{2^p} + 1$.*

1. *Question préliminaire : montrer que les deux égalités suivantes sont établies :*
   (a) $x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \dots + x + 1)$ pour tout entier naturel n strictement positif.
   (b) $x^n + 1 = (x + 1)(x^{n-1} - x^{n-2} + \dots - x + 1)$ pour tout entier naturel n impair
2. *Montrer que, pour que $2^n + 1$ soit premier, il est nécessaire que n soit une puissance de 2.*
3. *Pour montrer que ce n'est pas suffisant, vérifier que F_5 est divisible par 641.*
4. *Montrer que, pour $k \geqslant 1$, F_p divise $F_{p+k} - 2$.*
5. *En déduire que F_p et F_{p+k} sont premiers entre eux.*

III Division euclidienne dans $\mathbb{Z}$ et applications

On se donne deux entiers relatifs a et b, b non nul.

PROPRIÉTÉ 5.3 : Il existe un et un seul couple d'entiers relatifs q et r qui vérifient la relation suivante : $a = bq + r$, avec $0 \leqslant r < |b|$.

DÉFINITION 5.6 (DIVISION EUCLIDIENNE). Obtenir les valeurs de q et de r, c'est effectuer la *division euclidienne* de a par b. Le nombre q est appelé *quotient*, et le nombre r est appelé *reste* (dans la division euclidienne). Lorsque r est nul, a est dit *divisible* par b, ou b est un *diviseur* de a.

EXEMPLE 5.8. Tout nombre non nul est au moins divisible par 1 et par lui-même ($a = a \times 1 + 0$).

EXEMPLE 5.9. 0 est divisible par tout nombre entier non nul ($0 = 0 \times b + 0$).

Exercice 5.10. *Quels sont le quotient et le reste de la division euclidienne de m par n dans le cas où :*

1. $m = -38$ *et* $n = 6$,
2. $m = 165$ *et* $n = -14$.

Exercice 5.11 (Numéro Sécurité Sociale (www.bibmath.net)). *Le numéro de Sécurité Sociale d'un individu est composé de 13 chiffres et d'une clé de contrôle de deux chiffres avec dans l'ordre :*

- *le chiffre 1 pour les hommes et 2 pour les femmes ;*
- *les deux derniers chiffres de l'année de naissance ;*
- *le numéro du mois de naissance (2 chiffres) ;*
- *le numéro du département de naissance (2 chiffres) ;*
- *le numéro du la commune de naissance (2 chiffres) ;*
- *numéro d'ordre de l'acte de naissance dans le mois et la commune (3 chiffres)*

Les deux derniers chiffres sont une clé de contrôle C. *En notant A le nombre formé des 13 premiers chiffres, on a $C = 97 - r$ où r est le reste de la division euclidienne de A par 97.*

1. *Vérifier la clé de votre numéro INSEE.*

On note $A_t = 100A + C$ le numéro INSEE en entier (c'est donc un nombre de 15 chiffres). Soit également $\tilde{A}_t$ un nombre obtenu à partir de A_t en changeant un chiffre et un seul. On note $\tilde{A}$ les 13 premiers chiffres de $\tilde{A}_t$ et $\tilde{C}$ les deux derniers.

3. *On suppose que le changement de chiffre s'est effectué sur la clé C. Montrer que $\tilde{C}$ n'est pas la clé de contrôle valide de $\tilde{A}$. En déduire que $\tilde{A}_t$ n'est pas un numéro SS valide.*
4. *On suppose ici que le changement de chiffre s'est effectué sur A et que $\tilde{C}$ est la clé de contrôle de $\tilde{A}$.*
   (a) *Montrer que 97 divise $\tilde{A} - A$.*
   (b) *Montrer que $|A - \tilde{A}| = a \times 10^n$, où a et n sont des entiers naturels avec $1 \leq a \leq 9$.*
   (c) *Conclure que $\tilde{A}_t$ n'est pas un numéro INSEE valide.*

Exercice 5.12. *On se place dans l'ensemble $\mathbb{N}$.*

1. *Trouver les restes dans la division par 5 du carré d'un entier.*
2. *Trouver les restes dans la division par 8 du carré d'un entier impair.*
3. *Trouver les restes dans la division par 11 de 37^n (pour $n \in \mathbb{N}^*$).*
4. *Montrer que $10^n(9n - 1) + 1$ est divisible par 9.*

IV Algorithmes d'Euclide

Par définition, le PGCD de a non nul avec 0 est a (défintion raisonnable, car 0 est divisible par tout entier non nul, donc par a, qui l'est aussi par a) et enfin le PGCD de 0 et de 0 n'est pas défini.

L'algorithme consistant à comparer les décompositions en facteurs premiers n'est pas efficace. La découverte de diviseurs de nombres très grands est un problème difficile dont nous reparlerons plus loin.

IV.1 L'algorithme initial

On se limite ici au cas de deux entiers a et b strictement positifs. Supposons par exemple $a > b$

1. La division euclidienne de a par b peut s'écrire $a = bq + r$ avec $0 \leqslant r < b$.
2. Montrons que « d est un diviseur commun à a et b » est équivalent à « d est un diviseur commun à b et r ».
   — Soit d un diviseur commun à a et b, qui peuvent alors s'écrire $a = da'$ et $b = db'$. L'égalité $a = bq + r$ devient $da' = db'q + r$ ou encore $r = d(a' - b'q)$, donc d est aussi un diviseur commun à b et r.
   — Réciproquement, soit d un diviseur commun à b et r, qui peuvent alors s'écrire $b = db'$ et $r = dr'$ et l'égalité $a = bq + r$ devient $a = d(b'q + r')$. Donc d est un diviseur commun à a et b.
   Ainsi, les ensembles des diviseurs communs à a et b d'une part et à b et r d'autre part sont identiques. En particulier $a \wedge b = b \wedge r$.
3. Si $r = 0$ on a $a \wedge b = b \wedge 0$ qui est égal à b.
4. Sinon, r est différent de 0 et on peut donc effectuer la division euclidienne de b par r, qui donne un reste r_1, tel que $0 \leq r_1 < r$ et $b \wedge r = r \wedge r_1$.
5. Cet algorithme est itéré jusqu'à l'obtention d'un reste nul, ce qui se produit obligatoirement puisqu'il s'agit d'entiers et que la suite des restes ainsi construite est strictement décroissante. Le PGCD est alors l'avant-dernier reste (le dernier non nul).

REMARQUE 5.2. Cet algorithme permet donc d'obtenir le PGCD de deux nombres sans connaître leurs décompositions en facteurs premiers.

Exercice 5.13. *Déterminer* $154 \wedge 35$ *par l'algorithme d'Euclide.*

Exercice 5.14. *Donner le code d'un programme qui prend en entrée deux entiers naturels* a *et* b *tels que* $a > b \geq 0$ *et qui retourne leur PGCD*

Exercice 5.15. *Soit* $(U_n)_{n\in\mathbb{N}}$ *la suite d'entiers définie par* $U_0 = 14$ *et* $U_{n+1} = 5U_n - 6$.

1. *Calculer* U_1, U_2 *et* U_3.
2. *Calculer* $U_0 \wedge U_1$, $U_1 \wedge U_2$ *et* $U_2 \wedge U_3$.
3. *Soit* d *le PGCD entre deux termes successifs, Montrer que ce PGCD est un diviseur de 6 en exploitant l'égalité* $U_{n+1} = 5U_n - 6$.
4. *Montrer que si 2 divise* U_n, *alors 2 divise* U_{n+1}.
5. *Montrer que si 3 divise* U_{n+1}, *alors 3 divise* U_n.
6. *Conclure que le PGCD est 2.*

Voici sa programmation itérative en Python :

```
def pgcd_euclide(a,b) :
    assert a>b and b >=0
    while b != 0 :
        r = a%b
        a = b
        b = r
    return a
```

PROPRIÉTÉ 5.4 (THÉORÈME DE BÉZOUT) : On considère deux nombres entiers strictement positifs a et b. Il existe un couple d'entiers u et v tels que $au - bv = d$, où d est le PGCD de a et de b.

PREUVE On peut se ramener au cas où $a \wedge b = 1$.

En effet, si $d > 1$, on peut écrire $a = a'd$ et $b = b'd$ avec $a' \wedge b' = 1$; si le théorème est établi dans le cas du PGCD égal à 1, on peut affirmer l'existence de u et de v tels que $a'u - b'v = 1$; en multipliant les deux membres de cette égalité par d, on obtient $a'du - b'dv = d$, soit $au - bv = d$.

Il suffit donc d'établir le théorème dans le cas où $d = 1$ (a et b premiers entre eux). Plaçons nous dans $(\mathbb{Z}/b\mathbb{Z})^*$ et considérons l'application de cet ensemble dans lui-même définie par $x \longmapsto ax$. Essayons de résoudre $ax = ax'$, soit $a(x - x') = 0$, soit encore $a(x - x') \equiv 0[b]$, ou finalement $a(x - x') = kb$, avec $k \in \mathbb{Z}$.

Comme $a \wedge b = 1$, a ne divise pas b, donc divise k ; on peut écrire $k = k'a$, il reste $x - x' = k'b$, donc $x \equiv x'[b]$, donc $x = x'$; finalement $ax = ax' \Rightarrow x = x'$, donc l'application envisagée est injective ; comme il s'agit d'un ensemble fini, elle est évidemment aussi surjective, donc il existe u tel que $au = 1$, ce qui s'écrit encore $au \equiv 1[b]$, ou encore $au = bv + 1$, finalement $au - bv = 1$. ∎

REMARQUE 5.3. Ce couple n'est pas unique.

PREUVE En effet, si (u, v) est un couple de Bézout pour (a, b), donc tel que $au - bv = d$, où $d = a \wedge b$, alors, pout tout k dans $\mathbb{Z}$, $a(u + kb) - b(v + ka) = au - bv + kab - kab = au - bv = d$ aussi. ∎

Exercice 5.16 (Application de l'algorithme d'Euclide et de Bézout). *Si* p *est un nombre premier, et* n *un entier avec* $n \geq 2$, *on note* $a = p^n + 1$ *et* $b = p^n - 1$.

1. *On suppose que* p *est égal à 2.*
   (a) *Montrer que* $2^n - 1 = 2 \times (2^{n-1} - 1) + 1$ *pour* $n \geq 2$.
   (b) *Calculer* $d = a \wedge b$ *au moyen de l'algorithme d'Euclide.*
   (c) *Déterminer un couple d'entiers relatifs* (u, v) *tels que* $ua + vb = d$.
2. *On suppose maintenant que* p *est différent de 2.*
   (a) *Montrer que* a *et* b *sont pairs et poser* $a = 2A$ *et* $b = 2B$.
   (b) *Calculer* $A - B$. *En déduire la valeur* d *de* $a \wedge b$.
   (c) *Déterminer un couple d'entiers relatifs* (u, v) *tels que* $ua + vb = d$.

IV.2 Algorithme d'Euclide généralisé

Pour deux entiers positifs a et b, on a vu que l'algorithme d'Euclide s'écrit : $a \wedge b = b \wedge r$, où r est le reste dans la division euclidienne de a par b.

En supposant $a > b$, si on pose $a = r_0$ et $b = r_1$, on définit une famille finie $(r_0, r_1, \ldots, r_k, r_{k+1})$ par $r_i = q_{i+1}r_{i+1} + r_{i+2}$ (c'est-à-dire que r_{i+2} est le reste dans la division euclidienne de r_i par r_{i+1}).
Cette famille...

— est strictement décroissante,

— est telle que $r_{k+1} = 0$,

— vérifie $r_0 \wedge r_1 = r_1 \wedge r_2 = \ldots = r_{k-1} \wedge r_k = r_k \wedge r_{k+1} = r_k \wedge 0 = r_k$.

On remarque que r_{k-1} est un multiple de r_k, puisque la division euclidienne de r_{k-1} par r_k s'écrit $r_{k-1} = q_k r_k$.

Soit d le PGCD de a et de b (évidemment, $d = r_k$), on peut écrire $1 \times r_k - 0 \times r_{k-1} = d$ puis $1 \times r_{k-2} - q_{k-1} \times r_{k-1} = d$.

D'une manière générale, si (u, v) est un couple de Bézout pour r_{i+1} et r_{i+2}, soit $u \cdot r_{i+1} + v \cdot r_{i+2} = d$, comme $r_i = q_{i+1} \cdot r_{i+1} + r_{i+2}$, on a $u \cdot r_{i+1} + v \cdot (r_i - q_{i+1} \cdot r_{i+1}) = d$, soit $(u - q_{i+1} \cdot v) \cdot r_{i+1} + v \cdot r_i = d$.

IV.3 L'algorithme.

Ceci donne l'idée de construire deux familles par les relations :

— $u_0 = 1$, $u_1 = 0$,$u_{i+2} = u_i - q_{i+1} \cdot u_{i+1}$

— $v_0 = 0$, $v_1 = 1$, $v_{i+2} = v_i - q_{i+1} \cdot v_{i+1}$.

C'est ce que l'on appelle algorithme d'Euclide généralisé. On a alors $(u_k, v_k, r_k) = (u, v, d)$, u et v tels que $a \cdot u + b \cdot v = d$.

PREUVE 3 : *Pour cela, il suffit de montrer par récurrence que* $\forall i \in \{0, \ldots, k\}, r_0 \cdot u_i + r_1 \cdot v_i = r_i$.

— *Initialisation de la récurrence : la relation est vraie pour* $i = 0$, *en effet* $r_0 \cdot u_0 + r_1 \cdot v_0 = r_0$, *puisque* $u_0 = 1$ *et* $v_0 = 0$.

— *Caractère héréditaire de la propriété : en supposant que* i *est un entier pour lequel* $r_0 \cdot u_i + r_1 \cdot v_i = r_i$ *et* $r_0 \cdot u_{i+1} + r_1 \cdot v_{i+1} = r_{i+1}$, *calculons* $r_0 \cdot u_{i+2} + r_1 \cdot v_{i+2} = r_0 \cdot (u_i - q_{i+1} \cdot u_{i+1}) + r_1 \cdot (v_i - q_{i+1} \cdot v_{i+1}) = r_0 \cdot u_i + r_1 \cdot v_i - q_{i+1} \cdot (r_0 \cdot u_{i+1} + r_1 \cdot v_{i+1}) = r_i - q_{i+1} \cdot r_{i+1} = r_{i+2}$. †

IV.4 Exemple.

Illustrons la mise en œuvre de cet algorithme...

EXEMPLE 5.17. Soit à obtenir un couple de Bézout pour (23,17) :

(23,1,0)	(17,0,1)	$\longrightarrow$	$q = 1$
(17,0,1)	(6,1,-1)	$\longrightarrow$	$q = 2$
(6,1,-1)	(5,-2,3)	$\longrightarrow$	$q = 1$
(5,-2,3)	(1,3,-4)	$\longrightarrow$	$q = 5$
(1,3,-4)	(0,-17,23)	$\longrightarrow$	FIN

On a bien $3 \times 23 - 4 \times 17 = 1$.

REMARQUE 5.4. Il est possible d'obtenir -1 (ou $-d$ en général) comme résultat, donc $au - bv = -1$, cela dépend de la parité du nombre d'itérations effectuées dans l'algorithme précédent.

Ce n'est pas un résultat faux, puisqu'alors $bv - au = 1$ et qu'on a quand même un couple de Bézout pour (b, a).

S'il est nécessaire d'obtenir un couple (u, v) tel que $au - bv = 1$ et où a et b figurent dans cet ordre, et que l'algorithme a fourni un couple (u', v') tel que $bv' - au' = 1$, il suffit de prendre $u = b - u'$ et $v = a - v'$ et, dans ces conditions $au - bv = a(b - u') - b(a - v') = ab - au' - ab + bv' = bv' - au' = 1$.

Exercice 5.18. *Exprimer PGCD*$(1330, 602)$ *comme combinaison à coefficients entiers des nombres 1330 et 602.*

PROPRIÉTÉ 5.5 (THÉORÈME DE GAUSS) : Soient a, b et c trois entiers naturel non nuls. Si a divise le produit bc et si a est premier avec b, alors a divise c.

Exercice 5.19. *L'objectif est de résoudre l'équation (E) d'inconnues x et y $405x - 120y = 15$.*

1. *Trouver le pgcd de 405 et 120 à l'aide de l'algorithme d'Euclide.*
2. *En déduire une solution particulière de cette équation.*
3. *En utilisant la solution particulière, montrer que (E) est équivalente à $27(x-3) = 8(y-10)$.*
4. *Utiliser le théorème de Gauss pour montrer que l'ensemble solution de (E) est $\{(8k+3; 27k+10) | k \in \mathbb{Z}\}$.*

Exercice 5.20. *On considère l'équation $\frac{x}{9} - \frac{y}{4} = 3$ où x et y sont des entiers naturels.*

1. *Montrer que cela implique qu'il existe $k \in \mathbb{N}$ tel que $x = 9(k+3)$ et $y = 4k$.*
2. *Démontrer que le PGCD de x et y ne peut être qu'un diviseur de 108.*
3. *Soit m le ppcm de x et de y. On envisage la décomposition de m en facteurs premiers. Trouver l'ensemble des entiers naturel k pour que*
   (a) *m ne contienne pas le facteur 2.*
   (b) *m contienne le facteur 2 ou le facteur 2^2.*
   (c) *m ne contienne pas le facteur 3.*
   (d) *m contienne le facteur 3, ou le facteur 3^2, ou le facteur 3^3.*
4. *Comment faut-il choisir x et y de telle façon que l'on ait PGCD$(x, y) = 18$?*

Exercice 5.21.

1. *Décomposer 319 en facteurs premiers.*
2. *Démontrer que si x et y sont deux entiers naturels premiers entre eux, il en est de même pour les nombres $3x + 5y$ et $x + 2y$.*
3. *Résoudre dans $\mathbb{Z}^2$ le système d'inconnues a et b :*

$$\begin{cases} (3a+5b)(a+2b) &= 1276 \\ ab &= 2m \text{ tel que } m \text{ est le PPCM de } a \text{ et } b. \end{cases}$$

Exercice 5.22. *Au 8° siècle, un groupe composé d'hommes et de femmes a dépensé 100 pièces de monnaie dans une auberge. Les hommes ont dépensé 8 pièces chacun et les femmes 5 pièces chacune. Combien pouvait-il y avoir d'hommes et de femmes dans le groupe ?*

V Arithmétique modulo n

On rappelle ici la définition de la relation dite de « congruence modulo n » définie dans $\mathbb{Z}$ étudiée dans le chapitre consacré aux relations entre ensembles.

DÉFINITION 5.7 (CONGRUENCE MODULO n). Soit n un entier strictement supérieur à 1 et x et y deux éléments de $\mathbb{Z}$. On dit que « x est *congru* à y *modulo* n » lorsque x et y possèdent le même reste dans la division (euclidienne) par n :

$$x \equiv y[n] \Leftrightarrow \exists k \in \mathbb{Z}, x - y = k \cdot n$$

Exercice 5.23. *Calculez :*

1. $3 * 10^9 \bmod 97$,
2. $3^{1024} \bmod 1037$.

PROPRIÉTÉ 5.6 : La relation de congruence modulo n est une relation d'équivalence dans $\mathbb{Z}$.

PREUVE En effet :

— $\forall x \in \mathbb{Z}, x - x = 0 = 0 \cdot n$; or $0 \in \mathbb{Z}$, donc $x \equiv x[n]$ (réflexivité).

— Si $x \equiv y[n]$, $\exists k \in \mathbb{Z}, x - y = k \cdot n$; alors $y - x = (-k) \cdot n$, et, puisque $k \in \mathbb{Z}$, $(-k) \in \mathbb{Z}$, donc $y \equiv x[n]$ (symétrie).

— Si $x \equiv y[n]$, $\exists k \in \mathbb{Z}$, $x - y = k \cdot n$; si, de plus, $y \equiv z[n]$, $\exists l \in \mathbb{Z}$, $y - z = l \cdot n$; alors (par addition), $x - z = (k + l) \times n$; comme $k \in \mathbb{Z}$ et $l \in \mathbb{Z}$, $(k + l) \in \mathbb{Z}$, donc $x \equiv z[n]$ (transitivité). ∎

La classe d'équivalence d'un entier donné comprend donc cet entier et tous ceux qui ont le même reste que lui dans la division euclidienne par n.

EXEMPLE 5.24. Si $n = 3$, il y a trois classes distinctes :
- $\dot{0} = \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\}$,
- $\dot{1} = \{\ldots, -5, -2, 1, 4, 7, 10, \ldots\}$,
- $\dot{2} = \{\ldots, -4, -1, 2, 5, 8, 11, \ldots\}$.

On retrouve ensuite les mêmes éléments : $\dot{3} = \dot{0}$, etc...

D'une manière générale, pour n quelconque, il y a exactement n classes d'équivalence, notées de $\dot{0}$ à $(n \dot{-} 1)$, c'est-à-dire, il faut le remarquer, un nombre fini.

PROPRIÉTÉ 5.7 : L'ensemble-quotient (ensemble des classes d'équivalence) de la relation de congruence modulo n est un ensemble fini.

NOTATION : Il est noté $\mathbb{Z}/n\mathbb{Z}$.

EXEMPLE 5.25. $\mathbb{Z}/3\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}\}$.

DÉFINITION 5.8. On dit qu'une relation d'équivalence, notée $\equiv$, définie dans une structure algébrique S, est compatible avec les lois de S lorsque les résultats des opérations effectuées sur des éléments équivalents demeurent équivalents :
- pour l'addition : si $x \equiv x'$ et $y \equiv y'$, alors on doit avoir $x + y \equiv x' + y'$;
- pour la multiplication $\times$: si $x \equiv x'$ et $y \equiv y'$, alors on doit avoir $x \times y \equiv x' \times y'$.

PROPRIÉTÉ 5.8 : La relation de « congruence modulo n » est compatible avec l'addition et la multiplication des nombres entiers.

PREUVE En effet, on suppose que :
- $x \equiv x'[n] \Leftrightarrow \exists k \in \mathbb{Z},\ x - x' = k \cdot n$;
- $y \equiv y'[n] \Leftrightarrow \exists l \in \mathbb{Z}, y - y' = l \cdot n$.

Alors :
- par addition, $(x+y) - (x'+y') = (k+l) \cdot n$; $(k+l) \in \mathbb{Z}$, donc $(x+y) \equiv (x'+y')[n]$: la congruence modulo n est compatible avec l'addition dans $\mathbb{Z}$
- en multipliant l'égalité $x - x' = k \cdot n$ par y, on a $xy - x'y = (ky) \cdot n$ et l'égalité $y - y' = l \cdot n$ par x' on a $x'y - x'y' = (x'l) \cdot n$.
  Par addition, $xy - x'y' = (ky + lx') \cdot n$. $(ky + lx') \in \mathbb{Z}$, donc $x \cdot y \equiv x' \cdot y'[n]$: la congruence modulo n est aussi compatible avec la multiplication dans $\mathbb{Z}$. ∎

DÉFINITION 5.9. Par définition, on pose $\dot{x} + \dot{y} = (x \dot{+} y)$ et $\dot{x} \cdot \dot{y} = (\dot{xy})$.

EXEMPLE 5.26. C'est ainsi qu'on obtient les tables d'opérations suivantes dans $\mathbb{Z}/4\mathbb{Z}$:

$+$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{0}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{1}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{0}$
$\dot{2}$	$\dot{2}$	$\dot{3}$	$\dot{0}$	$\dot{1}$
$\dot{3}$	$\dot{3}$	$\dot{0}$	$\dot{1}$	$\dot{2}$

$\times$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{0}$	$\dot{2}$
$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{2}$	$\dot{1}$

REMARQUE 5.5. On aperçoit la présence de « diviseurs de zéro » ($\dot{2} \times \dot{2} = \dot{0}$), mais aussi l'apparition d'un inverse pour certains éléments ($\dot{3} \times \dot{3} = \dot{1}$).

Exercice 5.27. *Résolvez modulo 18 les équations suivantes :*

1. $2x + 17 = 15$,
2. $3x + 4 = 12$,
3. $5x + 13 = 16$.

Exercice 5.28 (Systèmes de congruences). *Il s'agit de trouver des entiers x qui satisfont des systèmes de la forme*

$$\begin{cases} x & \equiv & a\,[p] \\ x & \equiv & b\,[q] \end{cases}$$

Un tel système peut ne pas avoir de solution (par exemple, $a = 1,\ p = 2,\ b = 0,\ q = 4$: un nombre impair ne peut être un multiple de 4).

Une condition suffisante d'existence de solutions est que p et q soient premiers entre eux.

C'est le cas que nous traiterons ici ; dans ce cas, il existe deux entiers u et v tels que $pu + qv = 1$ (théorème de Bézout).

Donc $pu \equiv 1\,[q]$ et $qv \equiv 1\,[p]$, et $x = bpu + aqv$ est une solution du système (pourquoi ? ?) ; les autres sont de la forme $x + kpq$, où k est un entier quelconque.

1. *Résoudre le système de congruences*
$$\begin{cases} x & \equiv & 2\,[88] \\ x & \equiv & 1\,[27] \end{cases}.$$
2. *Application au problème du cuisinier : une bande de 17 pirates s'est emparée d'un butin composé de pièces d'or, toutes d'égale valeur.*

   Ils décident de se les partager également et de donner le reste éventuel au cuisinier. Celui-ci recevrait alors 3 pièces d'or.

   Malheureusement, une querelle éclate, au cours de laquelle 6 pirates sont tués. Le cuisinier recevrait alors 4 pièces d'or.

   Dans un naufrage ultérieur, seuls le butin, 6 pirates et le cuisinier sont sauvés. Le partage laisserait alors 5 pièces à ce dernier.

   Quel est le plus petit nombre de pièces d'or qu'il espère lorsqu'il décide d'empoisonner les derniers pirates ?

Exercice 5.29. *Si m est un entier naturel plus grand que 2, quel est l'inverse de $m - 1$ modulo m ?*

Exercice 5.30. *Un nombre « pseudo-premier de base b » est un entier naturel non premier p tel que $(b^p - b) \bmod p = 0$. Vérifier que 561 est pseudo-premier de base 3 et que 341 est pseudo-premier de base 2.*

Quatrième partie

Annexes

Chapitre 6

Programme Pédagogique National 2005 (PPN)

Voici le contenu de l'Unité de Formation Mathématiques Discrètes (TC-CCG-MATH1) du PPN actuel :

Volume horaire : 70 h

Pré-requis : aucun.

Objectifs :
- Connaître le calcul booléen.
- Calculer dans Z/nZ.
- Connaître les notions de base en théorie des graphes, des langages et des automates.

Compétences minimales :
- Mettre en œuvre des schémas de raisonnement (contraposée, absurde, récurrence, etc.).
- Mettre en œuvre des algorithmes d'arithmétique (Euclide, Bézout, etc.).
- Faire le lien entre langage usuel et langage formalisé (propositions et prédicats).

Contenu :
- Vocabulaire de la théorie des ensembles, relations, ensembles ordonnés.
- Logique : calcul propositionnel et calcul des prédicats.
- Arithmétique : nombres premiers, division euclidienne, congruences.
- Éléments de théorie des graphes : graphes orientés et non orientés.
- Éléments de langages et d'automates.

Indications de mise en œuvre : Exemples d'algorithmes de plus courts chemins, de parcours et d'arbre couvrant de poids minimum.

Prolongements possibles :
- Exemples de raisonnement par récurrence (en liaison avec les enseignements d'algorithmique).
- Développement des liens avec les enseignements d'informatique, en particulier « Architectures, Systèmes et Réseaux » et « Outils et Modèles du Génie logiciel » (algèbre relationnelle, etc.).
- Chaînage avant et chaînage arrière.
- Résolution d'équations en nombres entiers.
- Cryptographie (RSA, méthode du « sac à dos », etc.).
- Codes correcteurs et codes détecteurs d'erreurs.

Bibliographie

[Dow07] Gilles Dowek. *Les Métamorphoses du calcul, une étonnante histoire des mathématiques*. Éditions le Pommier, 2007.

Bibliographie (suite)

Outils mathématiques pour l'informaticien, *Michel Marchand* [De Boeck] : les thèmes abordés sont proches de ce cours de mathématiques discrètes (notre première année y est plus détaillée que la partie concernant automates, graphes et langages).

On y trouve des exercices, corrigés, parfois repris dans ce support. Cependant, le formalisme choisi s'éloigne par moment de celui adopté dans notre document, ce qui pourrait en destabiliser certains.

Méthodes mathématiques pour l'informatique, *Jacques Vélu* [Dunod] : Reprend une grande partie du cours de mathématiques discrètes, et y ajoute un peu de probabilités et d'algèbres linéaires. Contient des exercices corrigés. Un peu dense par moment, mais une bonne référence quand même.

Le magazine Tangente : que l'on trouve chaque mois chez les bons marchants de journaux. Niveau lycée et plus. On y trouve fréquemment des articles sur les graphes, la logique, le cryptage, etc. Ludique et plaisant, pour ceux qui aiment les mathématiques, veulent les découvrir. Les hors-séries sur la logique, sur les codes secrets, etc. me servent à trouver des idées de TP, ou à enrichir le cours.

Introduction à la logique, *François Rivenc* [Petite Bibliothèque Payot] : Pour un public avertis, souhaitant étudier plus systématiquement la logique, sous ses aspects mathématiques et philosophiques.

http ://www.apprendre-en-ligne.net/ Site de Didier Müller, sur lequel j'ai repris la partie graphes. A noter une autre partie (très riche, bien fournie) consacrée à la cryptographie, et un blog très intéressant sur les mathématiques.