Mathématiques discretes

A. Lakmon, Y. Mensah

Chapitre 1

Divisibilité dans $\mathbb{Z}$

1.1 Divisibilité dans $\mathbb{Z}$

Définition 1.1.1 *Soit $a, b \in \mathbb{Z}$. On dit que a est* **multiple** *de b s'il existe $k \in \mathbb{Z}$ tel que $a = bk$. Si de plus $b \neq 0$, on dit que b est un* **diviseur** *de a (ou que a est divisible par b ou que b divise a)..*

On écrit $b|a$ pour signifier que b divise a.

Définition 1.1.2 *Deux entiers sont dits* **premiers entre eux** *si leurs seuls diviseurs communs sont -1 et 1.*

Proposition 1.1.3 *Soit $a, b, c \in \mathbb{Z}$ tels que $b \neq 0, c \neq 0$. Si $c|b$ et $b|a$ alors $c|a$.*

Proposition 1.1.4 *Soit $a, b, c \in \mathbb{Z}$ tels que $c \neq 0$.*
Si $c|a$ et $c|b$ alors c divise $ma + nb$ pour tous $m, n \in \mathbb{Z}$.
On dit alors que c divise toute **combinaison linéaire** *de a et b.*

Applications

1. Trouver les entiers n pour lesquels la fraction $\dfrac{n+17}{n+4}$ est entière.
2. Montrer que pour $n \neq -7$, la fraction $\dfrac{2n+15}{n+7}$ est irréductible.
3. Déterminer les entiers naturels a et b tels que $a^2 - 4b^2 = 20$.

1.2 La division euclidienne

Théorème 1.2.1 *Soit $a, b \in \mathbb{N}$ tels que $b \neq 0$.*
Il existe un unique couple $(q, r) \in \mathbb{N}^2$ tel que

$$a = bq + r \text{ avec } 0 \leq r < b.$$

On dit que a est le **dividende**, b le **diviseur** ; q le **quotient** et r le **reste** dans la division euclidienne de a par b.

Corollaire 1.2.2 *1. Dans la division de a par b il ne peut y avoir que b restes possibles à savoir 0, 1, 2, $\cdots$, $b-1$.*

2. b divise a équivaut à dire que $r=0$.

La définition s'étend aisément au cas où a, b sont des entiers relatifs, $b \neq 0$. On montre qu'il existe un unique couple $(q,r) \in \mathbb{Z} \times \mathbb{N}$ tel que

$$a = bq + r \text{ avec } 0 \leq r < |b|.$$

Application

Déterminer a, b, c entiers tels que $\dfrac{59}{3^2} = a + \dfrac{b}{3} + \dfrac{c}{3^2}$.

1.3 Arithmétique modulaire ou Congruence

Proposition et Définition 1.3.1 *Soit c un entier non nul. Deux entiers a, b ont le même reste dans la division par c ssi $a-b$ est un multiple de c. On dit alors que a et b sont* **congrus modulo**[1] *c et on note $a \equiv b[c]$ ou $b \equiv a[c]$.*

Proposition 1.3.2 *Soit $a, a', a'', c \in \mathbb{Z}$ avec $c \neq 0$.*
Si $a \equiv a'[c]$ et $a' \equiv a''[c]$ alors $a \equiv a''[c]$.

Proposition 1.3.3 *Soit $a, b, a', b' \in \mathbb{Z}$ avec $c \neq 0$.*

$$\text{Si } a \equiv b[c] \text{ et } a' \equiv b'[c] \text{ alors } \begin{cases} a + a' \equiv b + b'[c] \\ a - a' \equiv b - b'[c] \\ ka \equiv kb[c], \forall k \in \mathbb{Z} \\ aa' \equiv bb'[c] \\ a^n \equiv b^n[c], \forall n \in \mathbb{N}^*. \end{cases}$$

Remarque On ne peut pas simplifier une congruence. Par exemple on a $16 \equiv 20[4]$ mais 8 et 10 ne sont pas congru modulo 4.

Applications

1. Montrer que pour tout entier $n > 0$, $3^{2n} - 2^n$ est un multiple de 7.
2. Quel est le reste de la division de $352^{14\,546}$ par 5 ?

1. Cette notion a été introduite par C. F. Gauss en 1801.

Chapitre 2

Nombres premiers

2.1 Définitions et Exemples

Définition 2.1.1 *On dit que $p \in \mathbb{N}$ est* **premier** *s'il possède exactement deux diviseurs positifs : 1 et lui-même.*

Théorème 2.1.2 *Soit $n \in \mathbb{N}, n \geq 2$. Alors*

1. *n admet au moins un diviseur premier.*
2. *Si n n'est pas premier, il admet au moins un diviseur premier p tel que $p \leq \sqrt{n}$.*

Proposition 2.1.3 (Test de primalité) *Soit $n \in \mathbb{N}, n \geq 2$. Si n n'est divisible par aucun des nombres premiers inférieurs ou égaux à sa racine carrée alors n est premier.*

Applications Tester la primalité des entiers $2^7 - 1$ et $2^{11} - 1$.

2.2 Une infinité de nombres premiers

Proposition 2.2.1 *Il existe une infinité de nombres premiers.*

Il suffit de remarquer que tout produit de nombres premiers augmenté de 1 est un nombre premier.

2.3 Décomposition en produit de facteurs premiers

Théorème 2.3.1 *Soit n un entier ≥ 2. Alors n se décompose de façon unique (à l'ordre des facteurs près) en produit de facteurs premiers, en d'autres*

termes n se met sous la forme

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}$$

où chaque p_i est un nombre premier et chaque α_i est un entier naturel non nul.

Corollaire 2.3.2 *Si des nombres premiers $p_1, p_2, \ldots, p_k$ divisent un entier n alors leur produit $\prod_{i=1}^{k} p_i$ divisent n.*

2.4 Application à la recherche de diviseurs premiers

Théorème 2.4.1 *Si un entier naturel $n \geq 2$ se décompose en produit de facteurs premiers sous la forme $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ alors les diviseurs positifs de n sont les entiers de la forme $n = \prod_{i=1}^{k} p_i^{\beta_i}$ avec $0 \leq \beta_i \leq \alpha_i$ pour tout i.*

Exemple. Rechercher les diviseurs positifs de 60. (Utiliser un arbre de choix)

Corollaire 2.4.2 *Si un entier naturel $n \geq 2$ se décompose en produit de facteurs premiers sous la forme $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ alors le nombre de diviseurs positifs de n est $\prod_{i=1}^{k} (\alpha_i + 1)$.*

2.5 Exercices

1. Quel est le plus petit entier naturel admettant 12 diviseurs positifs ?
2. (a) Justifier que 503 est premier.
   (b) Déterminer deux entiers naturels x et y tels que $x^2 - y^2 = 503$.
3. Quel est le plus petit entier naturel qui, multiplié par 1998, donne un carré parfait ? Même question avec 2008.
4. (a) Vérifier que le nombre $(231)_{12}$ est composé.
   (b) Démontrer qu'il en est de même quelle que soit la base utilisée.
5. Un entier naturel n a exactement 36 diviseurs. Quel est ce nombre sachant que sa décomposition en facteurs premiers comporte 2, élevé à la puissance 3, ainsi que 5 et 7, élevés à une même puissance.

6. La décomposition en facteurs premiers d'un entier a ne contient que les entiers premiers 3 et 7. Déterminer a sachant qu'il possède 21 diviseurs positifs.

Chapitre 3

Pgcd-ppcm, Algorithme d'Euclide, Théorèmes de Bézout, de Gauss et de Fermat

3.1 pgcd

Soit a, b deux entiers non tous nuls. Les diviseurs communs à a et b sont les entiers qui divisent à la fois a et b. On va noter $\mathcal{D}(a, b)$ l'ensemble des diviseurs communs à a et b.

Propriétés 3.1.1 *On a* $\mathcal{D}(a, b) = \mathcal{D}(a - b, b) = \mathcal{D}(a - kb, b)$ *pour tout* $k \in \mathbb{Z}$.

Corollaire 3.1.2
1. *Si* $0 < b \leq a$. *On a* $\mathcal{D}(a, b) = \mathcal{D}(b, r)$ *où* r *:=reste dans la division de* a *par* b.
2. b *divise* a *ssi* $\mathcal{D}(a, b) = \mathcal{D}(b)$.

Définition 3.1.3 *Soit* a, b *deux entiers non tous nuls. On appelle Plus Grand Commun Diviseur de* a *et* b, *et on note* $pgcd(a, b)$, *le plus grand élément de* $\mathcal{D}(a, b)$.

Propriétés 3.1.4
1. $pgcd(a, b)$ *est un entier*≥ 1.

Théorème 3.1.5 *Soit* a, b *deux entiers non tous nuls. Alors*
1. $pgcd(a, b) = pgcd(a - kb, b)$ *pour tout* $k \in \mathbb{Z}$.
2. *En particulier* $pgcd(a, b) = pgcd(b, r)$ *où* r *est le reste dans la division euclidienne de* a *par* b.

3.2 Théorème de Bezout

3.3 Théorème/Lemme de Gauss

Théorème 3.3.1 *Soient a, b et c des entiers non nuls. Si a divise bc et a et b sont premiers entre eux alors a divise c.*

3.4 Petit théorème de Fermat

Théorème 3.4.1 *Si p est premier et a est un entier naturel non divisible par p, alors $a^{p-1} - 1$ est divisible par p ; en d'autres termes $a^{p-1} \equiv 1 \mod p$.*

une autre formulation de ce théorème est :

Théorème 3.4.2 *Si p est premier et a est un entier naturel alors $a^p - a$ est divisible par p ; en d'autres termes $a^p \equiv a \mod p$.*

3.5 Exercices

1. Trouver tous les entiers naturels $n < 100$ tels que $pgcd(n, 72) = 8$.
2. Soit n un entier naturel tel que, quand on divise 169 et 267 par n, on obtient le même reste 15. Démontrer que n est un diviseur commun à 154 et 252. Quelle est la plus grande valeur possible de n.
3. Quel est le plus grand entier n tel que quand on divise 569 par n, on obtient pour reste 15, et quand on divise 683 par n le reste est 1 ?
4. Déterminer deux entiers naturels a et b sachant que $pgcd(a, b) = 9$ et $a + b = 72$.
5. Déterminer deux entiers naturels a et b sachant que $pgcd(a, b) = 121$ et $ab = 439\,230$.
6. Trouver tous les couples d'entiers positifs (a, b) tels que $2a^2 + b^2 = 16\,072$ et $pgcd(a, b) = 14$.
7. Soient $a = 630$ et b est un entier naturel tel que $pgcd(a, b) = 105$ et $600 < b < 1100$. Trouver b.
8. A l'aide de l'algorithme d'Euclide, montrer que 5 002 et 2 005 sont premiers entre eux.
9. Montrer que si a est premier avec b et c alors a est premier avec bc.
10. Soit n un entier naturel. On pose $a = 2n + 1$ et $b = 3n + 2$. Déterminer $pgcd(a, b)$.
11. Deux entiers naturels a et b ont pour somme 286 et pour *ppcm* 660.

(a) Quelles sont les valeurs possibles de $pgcd(a, b)$?

(b) En étudiant les différents cas, déterminer tous les couples (a, b) possibles.

Chapitre 4

Logique et Raisonnement

4.1 Assertion et prédicat

Définition 4.1.1 *Une assertion (ou proposition) est un énoncé auquel on peut attribuer la valeur de vérité vrai (V) ou faux (F), mais jamais les deux à la fois. C'est le principe du tiers-exclu.*

Exemples 4.1.2
1. L'énoncé "Lomé est la capitale du Togo" est vrai (V).
2. L'énoncé "2,5 est un entier naturel" est faux (F).
3. L'énoncé "Koffi est mortel" est vrai (V).
4. L'énoncé " 19 est un multiple de 2" est faux (F).

Définition 4.1.3 *Un prédicat est un énoncé contenant des lettres appelées variables et qui est tel que quand on remplace chacune de ces variables par un élément donné on obtient une assertion.*

Exemples 4.1.4
1. L'énoncé $P(n)$: "n est un multiple de 2" est un prédicat car il devient une assertion quand on donne une valeur à n.
   $P(10)$ est une assertion vraie mais $P(11)$ est une assertion fausse.
2. L'énoncé suivant $P(x, A)$: " $x \in A$" est un prédicat à deux variables.
   $P(1, \mathbb{N})$ est une assertion vraie par contre $P(\sqrt{2}, \mathbb{Q})$ est une assertion fausse.

4.2 Les connecteurs logiques

A partir de prédicats existants il est possible de construire de nouveaux prédicats appelés *prédicats composés*. Ceci se fait via les connecteurs logiques.

La négation

Définition 4.2.1 *La négation d'un prédicat P est le prédicat noté $\neg P$ ou $\neg P$ qui est vrai lorsque P est faux et faux lorsque P est vrai.*

On résume ceci dans le tableau suivant appelé *table de vérité* :

P	¬P
V	F
F	V

Exemples 4.2.2 *1. L'assertion P : " 24 est un multiple de 2 " a pour négation l'assertion $\neg P$: "24 n'est pas un multiple de 2".*

2. Le prédicat "$x \in A$" a pour négation le prédicat "$x \notin A$.".

La conjonction

Définition 4.2.3 *La conjonction des prédicats P et Q notée $P \wedge Q$ est le prédicat qui est vrai lorsque P et Q sont simultanément vrais et faux dans tous les autres cas.*

P	Q	P∧ Q
V	V	V
V	F	F
F	V	F
F	F	F

Exemples 4.2.4 *Considérons les deux propositions P et Q suivantes : P :"10 est divisible par 2" et Q :"10 est divisible par 3". La proposition $P \wedge Q$ est fausse.*

La disjonction

Définition 4.2.5 *La disjonction des prédicats P et Q notée $P \vee Q$) est le prédicat qui est vrai lorsque l'un au moins des deux prédicats P et Q est vrai et faux lorsque les deux sont faux.*

P	Q	P∨ Q
V	V	V
V	F	V
F	V	V
F	F	F

Exemples 4.2.6 Considérons les deux assertions P et Q suivantes :
P : "10 est divisible par 2" et Q : "10 est divisible par 3". L'assertion $P \vee Q$ est vraie.

L'implication

Définition 4.2.7 *Soient P et Q des prédicats. Le prédicat "$P \Rightarrow Q$", appelé implication de P vers Q, est un prédicat qui est faux lorsque P est vrai et Q faux et est vrai dans tous les autres cas.*

P	Q	P⇒ Q
V	V	V
V	F	F
F	V	V
F	F	V

Remarques 4.2.8
1. Dans $P \Rightarrow Q$, P est une condition suffisante pour Q et Q est une condition nécessaire pour P.
2. $Q \Rightarrow P$ s'appelle l'implication réciproque de $P \Rightarrow Q$.
3. $\neg Q \Rightarrow \neg P$ s'appelle la contraposée de $P \Rightarrow Q$.

Exemples 4.2.9 Soient les propositions : P :"il pleut." et Q : "Je me mets à l'abri." On a
$P \Rightarrow Q$: "S'il pleut alors je me mets à l'abri.".
$Q \Rightarrow P$:"Si je me mets à l'abri alors il pleut."
$\neg Q \Rightarrow \neg P$: "Si je ne me mets pas à l'abri alors il ne pleut pas."

L'équivalence

Définition 4.2.10 *Soient P et Q deux prédicats. Le prédicat "$P \Leftrightarrow Q$", appelé équivalence de P et de Q, est un prédicat qui*
– est vrai lorsque P et Q sont simultanément vrais ou faux,
– est faux dans tous les autres cas.

P	Q	P ⇔ Q
V	V	V
V	F	F
F	V	F
F	F	V

Définition 4.2.11 *Un prédicat composé qui est vrai quelles que soient les valeurs de vérité des prédicats qui le composent est appelé une* tautologie.

Exemples 4.2.12 1. $(P \vee \neg P)$
2. $(P \wedge (P \Rightarrow Q)) \Rightarrow Q$

Définition 4.2.13 *On dit que deux prédicats composés sont* incompatibles *si leur conjonction est fausse quelles que soient les valeurs de vérité des prédicats qui les composent.*

Exemples 4.2.14 1. Les prédicats P et $\neg P$ sont incompatibles.
2. Les prédicats "$x \leq 1$" et "$x \geq 2$" sont incompatibles.

4.3 Équivalence logique

Définition 4.3.1 *Soient R_1 et R_2 des prédicats composés. On dit que R_1 et R_2 sont* logiquement équivalents *si R_1 est vrai lorsque R_2 est vrai et R_1 est faux lorsque R_2 est faux. Cela revient au même de dire que R_1 et R_2 ont la même table de vérité et on note $R_1 \equiv R_2$. Dans le cas contraire on note $R_1 \not\equiv R_2$.*

Exemples 4.3.2 1. $\neg(\neg P) \equiv P$
2. $P \wedge Q \equiv Q \wedge P$
3. $P \vee Q \equiv Q \vee P$
4. $(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$
5. $(P \vee Q) \vee R \equiv P \vee (Q \vee R)$
6. $P \wedge (P \vee Q) \equiv P$
7. $P \Leftrightarrow Q \equiv Q \Leftrightarrow P$
8. $(\neg P \Rightarrow Q) \wedge (\neg P \Rightarrow \neg Q) \equiv P$
   Cette équivalence est à la base du raisonnement par l'absurde.
9. $\neg(P \vee Q) \equiv \neg P \wedge \neg Q$
10. $\neg(P \wedge Q) \equiv \neg P \vee \neg Q$
    (9. et 10. sont les *lois de Morgan* pour les prédicats)
11. $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$
12. $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$
13. $P \Rightarrow Q \equiv (\neg P \vee Q)$
14. $\neg(P \Rightarrow Q) \equiv (P \wedge \neg Q)$
15. $P \Rightarrow Q \equiv \neg Q \Rightarrow \neg P$
16. $P \Leftrightarrow Q \equiv (P \Rightarrow Q) \wedge (Q \Rightarrow P)$

4.4 Les quantificateurs mathématiques

À partir d'un prédicat $P(x)$ défini sur un ensemble E, on construit de nouvelles assertions dites assertions quantifiées en utilisant les quantificateurs " quel que soit" et "il existe".

Définition 4.4.1 *Le quantificateur "quel que soit", noté $\forall$, permet de définir l'assertion quantifiée " $\forall x \in E, P(x)$ " qui est vraie si pour tous les éléments x de E, l'assertion $P(x)$ est vraie.*

Exemples 4.4.2 1. "$\forall x \in [-3, 1], x^2 + 2x - 3 \leq 0$" est vraie.
2. "$\forall n \in \mathbb{N}, n(n-3) > 0$" est fausse.

Définition 4.4.3 *Le quantificateur "il existe", noté $\exists$, permet de définir l'assertion quantifiée " $\exists\, x \in E, P(x)$ " qui est vraie si on peut trouver (au moins) un élément x de E pour lequel l'assertion $P(x)$ est vraie.*

Remarques 4.4.4 1. S'il en existe un et un seul, on pourra écrire

$$\exists\, !x \in E, P(x).$$

2. Si "$\forall x \in E, P(x)$" est vraie alors "$\exists\, x \in E, P(x)$" est vraie.

Exemples 4.4.5 1. "$\exists\, x \in \mathbb{R}, x^2 = 4$" est vraie.
2. "$\exists\, !x \in \mathbb{R}, \ln(x^2) = 1$" est fausse.

Proposition 4.4.6 *Soit $P(x)$ un prédicat. On a :*
1. $\neg(\forall x \in E, P(x)) \equiv \exists\, x \in E, \neg(P(x))$.
2. $\neg(\exists x \in E, P(x)) \equiv \forall\, x \in E, \neg(P(x))$.

Exemples 4.4.7 $\neg(\forall x \in E, P(x) \Rightarrow Q(x)) \equiv \exists\, x \in E, P(x) \wedge \neg(Q(x))$.

Définition 4.4.8 *Soit $P(x, y)$ un prédicat à deux variables avec $x \in E$ et $y \in F$.*

1. L'assertion quantifiée

$$\forall x \in E, \forall y \in F, P(x, y)$$

est vraie lorsque pour chaque élément x de E et chaque élément y de F, $P(x, y)$ est vraie.

2. L'assertion quantifiée

$$\exists x \in E, \exists y \in F, P(x, y)$$

est vraie lorsqu'il existe un élément x de E et un élément y de F tels que $P(x, y)$ est vraie.

Exemples 4.4.9 1. L'assertion "$\forall n \in \mathbb{N}, \forall x \in [0, +\infty[, 1 + nx \leq (1 + x)^n$" est vraie.

2. L'assertion "$\exists x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y = 5$" est vraie.

Remarques 4.4.10 On peut combiner des quantificateurs de natures différentes. Par exemple, l'énoncé " tout nombre complexe possède une racine carrée" s'écrit sous la forme :

$$\forall z \in \mathbb{C}, \exists u \in \mathbb{C}, u^2 = z.$$

Mais on prendra soin de respecter les règles suivantes :

1. On peut permuter deux quantificateurs identiques.

$$(\forall x \in E, \forall y \in F, P(x, y)) \equiv (\forall y \in F, \forall x \in E, P(x, y)) .$$

$$(\exists x \in E, \exists y \in F, P(x, y)) \equiv (\exists y \in F, \exists x \in E, P(x, y)) .$$

2. Ne jamais permuter deux quantificateurs différents.

$$(\exists x \in E, \forall y \in F, P(x, y)) \not\equiv (\forall y \in F, \exists x \in E, P(x, y)) .$$

Exemples 4.4.11 L'assertion quantifiée " $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y = 0$" est vraie. Par contre, l'assertion " $\exists y \in \mathbb{R}, \forall x \in \mathbb{R}, x + y = 0$" est fausse.

4.5 Différents modes de démonstration

Raisonnement par hypothèse auxiliaire

1. But : montrer qu'un énoncé Q est vrai.
2. Principe : il s'appuie sur la tautologie :

$$(P \wedge (P \Rightarrow Q)) \Rightarrow Q.$$

   Ainsi si P est vrai et si l'implication $P \Rightarrow Q$ est vraie alors Q est vrai.
3. Méthodologie : On montre que l'énoncé P est vrai et on en déduit que Q est vrai.

Raisonnement par l'absurde

1. But : montrer qu'un énoncé P est vrai.
2. Principe : il s'appuie sur la tautologie :

$$(\neg P \Rightarrow Q) \wedge (\neg P \Rightarrow \neg Q) \equiv P.$$

   Un raisonnement par l'absurde consiste à montrer que $\neg P$ entraîne un énoncé Q et sa négation $\neg Q$.

3. Méthodologie : On suppose que l'énoncé $\neg P$ est vrai et on recherche une contradiction.

   Exercice. Soit $a, b \geq 0$. Montrer que si $\dfrac{a}{1+b} = \dfrac{b}{1+a}$ alors $a = b$.

Raisonnement par contraposition

1. But : montrer l'implication $P \Rightarrow Q$.
2. Principe : il s'appuie sur l'équivalence logique :

$$P \Rightarrow Q \equiv \neg Q \Rightarrow \neg P.$$

   Ainsi, au lieu de montrer $P \Rightarrow Q$, on montre sa contraposée $\neg Q \Rightarrow \neg P$.
3. Méthodologie : On fait l'hypothèse que $\neg Q$ est vrai et on montre que cela entraîne $\neg P$.

   Exercice. Montrer que si n^2 est pair alors n est pair.

Raisonnement par contre-exemple

1. But : il sert à montrer qu'un énoncé de la forme

$$\forall x \in E, P(x)$$

   est faux.
2. Principe : il s'appuie sur l'équivalence logique :

$$\neg(\forall x \in E, P(x)) \equiv \exists x \in E, \neg(P(x)).$$

3. Méthodologie : On cherche à exhiber un élément x de E qui ne vérifie pas $P(x)$.

Exercice. Est-ce que tout entier positif est la somme de trois carrés ?

Raisonnement par récurrence

1. But : montrer qu'un énoncé de la forme

$$\text{pour tout entier naturel } n \geq n_0, P(n).$$

2. Principe : Si $P(n_0) \wedge (P(n) \Rightarrow P(n+1))$ alors $\forall n \geq n_0, P(n)$.
3. Méthodologie : On vérifie que $P(n_0)$ est vrai, on suppose ensuite $P(n)$ et on montre que cela entraîne $P(n+1)$. Et enfin on conclut $\forall n \geq n_0, P(n)$.

   Exercice. Montrer que $\forall n \in \mathbb{N}$, $2^n > n$.

Chapitre 5

Ensembles, Applications et Relations

5.1 Ensembles

Intuitivement, un ensemble est une collection d'objets appelés *éléments* de l'ensemble. Nous admettons qu'il existe un ensemble noté $\emptyset$, appelé *ensemble vide* , qui ne contient aucun élément. Si E est un ensemble et $P(x)$ une propriété vérifiée par certains éléments x de E, l'ensemble de ces éléments est noté $\{x \in E, P(x)\}$.

Définition 5.1.1 *On dit que l'ensemble E est* inclus *ou est* contenu *dans l'ensemble F si tout élément de E est élément de F. On dit aussi que E est une partie ou un sous-ensemble de F. On écrit $E \subset F$ ou $F \supset E$.*

$$(E \subset F) \Leftrightarrow (\forall x, x \in E \Rightarrow x \in F).$$

On vérifie que quel que soit l'ensemble E, on a $E \subset E$. Si ($E \subset F$ et $F \subset G$) alors $E \subset G$.

Définition 5.1.2 *On dit que l'ensemble E est égal à l'ensemble F, et on écrit $E = F$, si $E \subset F$ et $F \subset E$.*

Etant donné un ensemble E, on désigne par $\mathscr{P}(E)$ l'ensemble des parties de E, y compris l'ensemble vide et l'ensemble E lui-même.

$$A \in \mathscr{P}(E) \Leftrightarrow A \subset E.$$

Définition 5.1.3 *Soient A et B des ensembles. L'ensemble $\{x : x \in A$ et $x \notin B\}$ s'appelle* différence *de A et B et se note $A \setminus B$.*

Définition 5.1.4 *Soient E un ensemble et A une partie de E. On appelle* complémentaire *de A dans E, et on note $E\setminus A$ ou $\mathscr{C}_E^A$, l'ensemble des éléments de E qui n'appartiennent pas à A.*

$$\mathscr{C}_E^A = \{x \in E : x \notin A\}.$$

Proposition 5.1.5 *1.* $\mathscr{C}_E^{(\mathscr{C}_E^A)} = A;\ \mathscr{C}_E^E = \emptyset;\ \mathscr{C}_E^\emptyset = E.$

2. Soit $A, B \in \mathscr{P}(E)$

$$A \subset B \Rightarrow \mathscr{C}_E^B \subset \mathscr{C}_E^A.$$

Définition 5.1.6 *On appelle* intersection *de deux ensembles E et F, et on note $E \cap F$, l'ensemble des éléments qui appartiennent à la fois à E et à F.*

$$E \cap F = \{x : x \in E \text{ et } x \in F\}.$$

Si $E \cap F = \emptyset$, on dit que E et F sont disjoints.

Définition 5.1.7 *On appelle* réunion *de deux ensembles E et F, et on note $E \cup F$, l'ensemble des éléments qui appartiennent à E ou à F.*

$$E \cup F = \{x : x \in E \text{ ou } x \in F\}.$$

Proposition 5.1.8 *1.* $E \cap \emptyset = \emptyset,\ E \cup \emptyset = E.$

2. $E \cup F = \emptyset \Rightarrow E = \emptyset$ *et* $F = \emptyset.$

3. associativité

$$(A \cup B) \cup C = A \cup (B \cup C),\ (A \cap B) \cap C = A \cap (B \cap C).$$

4. commutativité

$$A \cup B = B \cup A,\ A \cap B = B \cap A.$$

5. distributivité

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

6. idempotence

$$A \cup A = A,\ A \cap A = A.$$

Théorème 5.1.9 *(Lois de de Morgan)*

$$\mathscr{C}_E^{(A\cap B)} = \mathscr{C}_E^A \cup \mathscr{C}_E^B,\ \mathscr{C}_E^{(A\cup B)} = \mathscr{C}_E^A \cap \mathscr{C}_E^B.$$

Définition 5.1.10 *Soient E et F deux ensembles. On appelle* produit cartésien *de E et F, et on note $E \times F$, l'ensemble des couples (x, y) tels que $x \in E$ et $y \in F$.*

$$E \times F = \{(x, y) : x \in E \text{ et } y \in F\}.$$

Proposition 5.1.11 *Soient A,B,C,D des ensembles.*

1.
$$A \subset C \text{ et } B \subset D \Rightarrow A \times B \subset C \times D.$$

2.
$$A \times (B \cup C) = (A \times B) \cup (A \times C).$$
$$A \times (B \cap C) = (A \times B) \cap (A \times C).$$

3.
$$A \times B = \emptyset \Leftrightarrow A = \emptyset \text{ ou } B = \emptyset.$$

Le produit cartésien $E \times E$ se note E^2. On appelle *diagonale* de E^2 l'ensemble

$$\Delta = \{(x, x) : x \in E\}.$$

Plus généralement, le produit cartésien de n ensembles $E_1, \ldots, E_n$, noté

$$E_1 \times \cdots \times E_n \text{ ou } \prod_{i=1}^{n} E_i,$$

est l'ensemble des n-uples $(x_1, \ldots, x_n)$ tels que $x_i \in E_i,\ i = 1, \ldots, n$.
Si $E_i = E\ \forall i$, on note E^n au lieu de $E \times \cdots \times E$. Par exemple $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$ se note $\mathbb{R}^3$.

Définition 5.1.12 *On appelle* partition *d'un ensemble non vide E une famille $(A_i)_{i\in I}$ de parties de E (indexée par I) telles que*

1. $\forall i \in I,\ A_i \neq \emptyset$,
2. $\forall i, j \in I,\ (i \neq j \Rightarrow A_i \cap A_j = \emptyset)$,
3. $\bigcup_{i\in I} A_i = E$.

Exemples 5.1.13 Soit A une partie propre non vide de E. Alors A et C_E^A forment une partition de E.

5.2 Applications

Définitions et exemples

Définition 5.2.1 *Soient E et F deux ensembles. On appelle* fonction *f de E vers F toute relation qui associe à chaque élément de E au plus un élément de F.*

On note $f : E \to F$ ou $E \xrightarrow{f} F$. Si l'élément x de E est associé à l'élément y de F, on dit que x est un *antécédent* de y et y est *l'image* de x. On écrit $y = f(x)$. L'ensemble des éléments de E ayant une image par f est appelé *ensemble de définition* de f et noté D_f.

$$D_f = \{x \in E : \exists y \in F, y = f(x)\}.$$

L'ensemble $\Gamma = \{(x, f(x)) \in E \times F : x \in D_f\}$ est appelé le *graphe* de f.

Définition 5.2.2 *Une fonction $f : E \to F$ est appelée* application *si son ensemble de définition est E.*

L'ensemble des applications de E vers F est souvent noté F^E.

Exemples 5.2.3 1. La fonction

$$\begin{array}{rcl} f : \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \frac{1}{x-2} \end{array}$$

n'est pas une application car $D_f \neq \mathbb{R}$.

2. La fonction

$$\begin{array}{rcl} g : \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \sin x \end{array}$$

est une application car $D_g = \mathbb{R}$.

3. L'application

$$\begin{array}{rcl} E & \longrightarrow & E \\ x & \longmapsto & x \end{array}$$

est appelée *application identique* ou *identité* de E. Elle est souvent notée Id_E ou 1_E.

4. Soit A une partie d'un ensemble E. On appelle *fonction caractéristique* de A l'application χ_A définie de E vers $\{0, 1\}$ par

$$\chi_A(x) = \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{si } x \notin A. \end{cases}$$

5. Les applications
$$\begin{array}{rcl} pr_1 : E \times F & \longrightarrow & E \\ (x, y) & \longmapsto & x \end{array}$$
et
$$\begin{array}{rcl} pr_2 : E \times F & \longrightarrow & F \\ (x, y) & \longmapsto & y \end{array}$$
sont respectivement appelées *première projection* et *deuxième projection.*

Définition 5.2.4 *Soient $f : E \to F$ et $g : E' \to F'$ deux applications. On dit que f égale g et on note $f = g$ si*

$$E = E',\ F = F' \text{ et } \forall x \in E,\ f(x) = g(x).$$

Composition des applications

Soient E, F et G des ensembles, $f : E \to F$, $g : F \to G$ des applications. L'application

$$\begin{array}{rcl} E & \to & G \\ x & \mapsto & g(f(x)) \end{array}$$

s'appelle l'application composée de f par g et se note $g \circ f$.

En général on a $g \circ f \neq f \circ g$. Cependant :

Proposition 5.2.5 *Soient les applications $f : E \to F$, $g : F \to G$ et $h : G \to H$. On a*
$$h \circ (g \circ f) = (h \circ g) \circ f.$$

On dit que la loi $\circ$ est *associative*. L'application $h \circ (g \circ f)$ est simplement notée $h \circ g \circ f$.

Applications particulières

Définition 5.2.6 *Soient E et F deux ensembles et $f : E \to F$ une application.*

1. *On dit que f est* injective *(ou est une injection) si pour tous $x, y \in E$,*
$$f(x) = f(y) \Rightarrow x = y.$$
2. *On dit que f est* surjective *(ou est une surjection) si pour tout $y \in F$, il existe $x \in E$ tel que $y = f(x)$.*
3. *On dit que f est* bijective *(ou est une bijection) si elle est à la fois injective et surjective i.e pour tout $y \in F$, il existe un unique $x \in E$ tel que $y = f(x)$.*

Soit $f : E \to F$ une bijection. L'application $f^{-1} : F \to E$ qui à chaque élément y de F associe l'unique élément x de E tel que $y = f(x)$ est une bijection. Elle est appelée *application réciproque* de f. On a

$$(f^{-1})^{-1} = f,\ f^{-1} \circ f = Id_E,\ f \circ f^{-1} = Id_F.$$

Proposition 5.2.7 *Si $f : E \to F$ et $g : F \to G$ sont injectives (resp. surjectives, resp. bijectives) alors il en est de même de $g \circ f$. De plus dans le dernier cas, on a*

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Images directes, images réciproques

Définition 5.2.8 *Soit $f : E \to F$ une application, A une partie de E et B une partie de F.*

1. *L'*image directe *ou simplement l'*image *de A par f, notée $f(A)$ est l'ensemble des images des éléments de A par f.*

$$f(A) = \{f(x) : x \in A\}.$$

2. *L'*image réciproque *de B par f, notée $f^{-1}(B)$, est l'ensemble des éléments de E qui ont leurs images dans B.*

$$f^{-1}(B) = \{x \in E : f(x) \in B\}.$$

Proposition 5.2.9 *Soit $f : E \to F$ une application, A, A' deux parties de E, B, B' deux parties de F.*

1. *Si $A \subset A'$ alors $f(A) \subset f(A')$.*
2. $$f(A \cup A') = f(A) \cup f(A').$$
   $$f(A \cap A') \subset f(A) \cap f(A').$$
3. *Si $B \subset B'$ alors $f^{-1}(B) \subset f^{-1}(B')$.*
4. $$f^{-1}(B \cup B') = f^{-1}(B) \cup f^{-1}(B').$$
   $$f^{-1}(B \cap B') = f^{-1}(B) \cap f^{-1}(B').$$
   $$f^{-1}(\mathscr{C}_F^B) = \mathscr{C}_E^{f^{-1}(B)}.$$

5.3 Relations binaires dans un ensemble

Définitions et Exemples

Définition 5.3.1 *Soit E un ensemble. On appelle* relation binaire *sur E tout couple $\mathcal{R} = (E, \Gamma)$ où Γ est une partie de $E \times E$ appelée* graphe *de $\mathcal{R}$.*

Si $(x, y) \in \Gamma$, on dit que x est en relation avec y et on note $x\mathcal{R}y$.

Exemples 5.3.2 Dans $\mathscr{P}(E)$ la relation $\mathcal{R}$ définie par $A\mathcal{R}B \Leftrightarrow A \subset B$ est une relation binaire.

Définition 5.3.3 *Soit E un ensemble et $\mathcal{R}$ une relation binaire sur E. On dit que $\mathcal{R}$ est :*
– réflexive *si*

$$\forall x \in E,\ x\mathcal{R}x.$$

– symétrique *si*

$$\forall x, y \in E,\ x\mathcal{R}y \Rightarrow y\mathcal{R}x.$$

– antisymétrique *si*

$$\forall x, y \in E,\ x\mathcal{R}y \text{ et } y\mathcal{R}x \Rightarrow x = y.$$

– transitive *si*

$$\forall x, y, z \in E,\ x\mathcal{R}y \text{ et } y\mathcal{R}z \Rightarrow x\mathcal{R}z.$$

Exemples 5.3.4

1. La relation d'égalité est une relation réflexive, symétrique, antisymétrique et transitive.
2. Dans $\mathscr{P}(E)$, la relation d'inclusion est réflexive, antisymétrique et transitive.
3. Dans $\mathbb{Z}^*$, la relation de divisibilité définie par

$$x\mathcal{R}y \Leftrightarrow x \text{ divise } y$$

est réflexive et transitive. Elle n'est ni symétrique ni antisymétrique.

Relations d'équivalence

Définition 5.3.5 *On appelle* relation d'équivalence *sur E toute relation binaire sur E qui est à la fois réflexive, symétrique et transitive.*

Une telle relation $\mathcal{R}$ peut se noter $x\mathcal{R}y$ ou $x \equiv y\,(mod\,\mathcal{R})$ et on lit "x est équivalent à y modulo $\mathcal{R}$".
La classe d'équivalence d'un élément x de E constituée des éléments y de E qui sont équivalents à x est notée $cl(x)$ ou $\overline{x}$ ou $\dot{x}$. L'ensemble de toutes les classes d'équivalence s'appelle *l'ensemble quotient* de E par $\mathcal{R}$ et se note $E/\mathcal{R}$. Tout élément d'une classe d'équivalence est appelé *représentant* de cette classe.
L'application

$$\begin{array}{ccc} E & \to & E/\mathcal{R} \\ x & \mapsto & \overline{x} \end{array}$$

est surjective ; elle est appelée *surjection canonique.*

Exemples 5.3.6 Soit p un entier ≥ 1. Dans $\mathbb{Z}$ la relation

$$x\mathcal{R}y \Leftrightarrow p \text{ divise } x - y$$

est une relation d'équivalence. La classe de l'entier n est l'ensemble

$$\{\ldots, n-2p, n-p, n, n+p, n+2p, \ldots\}.$$

On l'appelle *classe de congruence de n modulo p.* L'ensemble quotient $E/\mathcal{R}$ se note ici $\mathbb{Z}/p\mathbb{Z}$.

Proposition 5.3.7 *Soit $\mathcal{R}$ une relation d'équivalence sur E. L'ensemble des classes d'équivalence modulo $\mathcal{R}$ forme une partition de E. Réciproquement, toute partition de E définit une relation d'équivalence dont les classes sont les éléments de la partition donnée.*

Relations d'ordre

Définition 5.3.8 *On appelle* relation d'ordre *sur E toute relation binaire sur E qui est réflexive, antisymétrique et transitive.*

Une relation d'ordre est souvent notée $\leq$ et le couple $(E, \leq)$ est appelé *ensemble ordonné.*
Dans un ensemble ordonné, deux éléments x et y sont dits *comparables* si $x \leq y$ ou $y \leq x$. Si deux éléments quelconques de E sont comparables, on dit que *l'ordre est total* ou que le couple $(E, \leq)$ est totalement ordonné. Dans le cas contraire on dit que *l'ordre est partiel* ou que le couple $(E, \leq)$ est partiellement ordonné.

Exemples 5.3.9 1. Dans $\mathbb{N}$,$\mathbb{Z}$,$\mathbb{Q}$ et $\mathbb{R}$, l'ordre usuel est un ordre total.

2. Soit E un ensemble. La relation d'inclusion est une relation d'ordre partiel sur $\mathscr{P}(E)$.
3. Dans $\mathbb{N}$, la relation de divisibilité est une relation d'ordre partiel.

Définition 5.3.10 *Soit $(E, \leq)$ un ensemble ordonné. S'il existe $a \in E$ tel que*

$$\forall x \in E, a \leq x \Rightarrow x = a (resp. \forall x \in E, x \leq a \Rightarrow x = a)$$

*on dit que a est un élément maximal (*resp. *minimal) de E.*

Exemples 5.3.11
1. Dans $(\mathbb{N} \setminus \{1\}, |)$, les éléments minimaux sont les nombres premiers. Dans $(\mathbb{N}, |)$, 0 est le seul élément maximal.
2. Dans $(\mathscr{P}(E) \setminus \{\emptyset\}, \subset)$, les éléments minimaux sont les parties réduites à un élément.
3. Dans $(\mathbb{R}, \leq)$, il n'y a ni élément maximal ni élément minimal.

Définition 5.3.12 *Soit $(E, \leq)$ un ensemble ordonné. S'il existe un élément $a \in E$ tel que $\forall x \in E, x \leq a$ (resp. $a \leq x$) cet élément est unique ; on l'appelle le plus grand (resp. le plus petit) élément de E, on le note max(E) (resp. min(E)).*

Remarques 5.3.13 Si $(E, \leq)$ admet un plus grand élément a alors a est l'unique élément maximal de $(E, \leq)$.

Exemples 5.3.14
1. Dans $(\mathscr{P}(E), \subset)$, $\emptyset$ est le plus petit élément, E est le plus grand élément.
2. $(\mathbb{N}, |)$, 0 est le plus grand élément ; 1 est le plus petit élément. Par contre dans $(\mathbb{N}, \leq)$, 0 est le plus petit élément, il n'y a pas de plus grand élément.

Définition 5.3.15 *Soit $(E, \leq)$ un ensemble ordonné et A une partie de E. S'il existe un élément $m \in E$ tel que*

$$\forall x \in A, x \leq m \ (resp.\ m \leq x)$$

on dit que A est majoré (resp. minoré) et que m est un majorant (resp. minorant) de A dans E.
Une partie bornée est une partie à la fois majorée et minorée.

Définition 5.3.16 *Soit $(E, \leq)$ un ensemble ordonné et A une partie de E. Si l'ensemble des majorants (resp. minorants) de A admet un plus petit (resp. plus grand) élément, cet élément est appelé borne supérieure (resp. borne inférieure) de A et se note* $\sup(A)$ *(resp.* $\inf(A)$*).*

Exemples 5.3.17 Dans $(\mathbb{R}, \leq)$, la partie $A = \{x \in \mathbb{R} : 0 \leq x < 1\}$ admet 0 pour borne inférieure et 1 pour borne supérieure.

5.4 Dénombrement

Ensembles finis, cardinaux

Définition 5.4.1 *Deux ensembles sont dits* **équipotents** *s'il existe une bijection de l'un sur l'autre.*

On vérifie, grâce aux propriétés des bijections que l' équipotence est une relation réflexive, symétrique et transitive entre ensembles. Cependant ce n'est pas une relation binaire sur un ensemble ; on ne parlera donc pas de relation d'équivalence.

Définition 5.4.2 *Un ensemble E est dit* **fini** *s'il est vide ou s'il est équipotent à $\mathbb{N}_n := \{1, ..., n\}$ pour un certain entier $n \geq 1$ donné.*

L'entier n est appelé **cardinal** de E et on note $Card(E) = n$. On pose par définition $Card(\emptyset) = 0$.

Définition 5.4.3 *Un ensemble est dit* **infini** *s'il n'est pas fini.*

Proposition 5.4.4
1. *Toute partie F d'un ensemble fini E est fini et $Card(F) \leq Card(E)$.*
2. *l'intersection d'une famille (finie ou infinie) d'ensembles finis est finie.*
3. *Soient E un ensemble fini et $f : E \to F$ une application. Alors $f(E)$ est un ensemble fini et $Card(f(E)) \leq Card(E)$, avec égalité ssi f est une injection.*
4. *Soient un ensemble fini et $f : E \to F$ une surjection. Alors F est fini et $Card(F) \leq Card(E)$, avec égalité ssi f est une bijection.*
5. *Soit $f : E \to F$ une injection. Si $f(E)$ est fini alors E est fini et $Card(E) = Card(f(E))$.*

On en déduit le théorème suivant.

Théorème 5.4.5 *Soient E et F deux ensembles finis, de même cardinal, et $f : E \to F$ une application. Alors les affirmations suivantes sont équivalentes :*
1. *f est injective*
2. *f est surjective*
3. *f est bijective.*

Ensembles dénombrables

Définition 5.4.6 *Un ensemble E est dit dénombrable s'il est équipotent à $\mathbb{N}$.*

On montre que les ensembles suivants sont dénombrables : $\mathbb{Z}$, $\mathbb{Q}$. Par contre $\mathbb{R}$ n'est pas dénombrable.

Proposition 5.4.7 *Toute partie d'un ensemble dénombrable est finie ou dénombrable. (On dit qu'elle est au plus dénombrable.)*

5.4.1 Analyse combinatoire

Principe de l'addition : Si les ensembles $(A_i)_{i\in I}$, I fini, sont deux à deux disjoints alors

$$Card(\underset{i\in I}{\cup} A_i) = \sum_{i\in I} Card(A_i).$$

Proposition 5.4.8 *Soient A, B deux parties d'un ensemble fini E. Alors*

1. $Card(A \setminus B) = Card(A) - Card(A \cap B)$.
2. $Card(C_E^A) = Card(E) - Card(A)$.
3. $Card(A \cup B) = Card(A) + Card(B) - Card(A \cap B)$.

Principe de la multiplication : Si une situation comporte p étapes avec respectivement $n_1, \ldots, n_p$ possibilités alors le nombre total d'issues est $\prod_{i=1}^{p} n_i$.

Proposition 5.4.9 *(Produit cartésien)*
Soient E et F deux ensembles finis.

1. $Card(E \times F) = Card(E) \times Card(F)$.
2. $Card(E^k) = (Card(E))^k,\ k \in \mathbb{N}^*$.

Proposition 5.4.10 *(Nombres d'applications)*
Soient E et F des ensembles finis.

$$Card(F^E) = Card(F)^{Card(E)}.$$

Le nombre de p-uplets d'un ensemble à n éléments est n^p.

Proposition 5.4.11 *(Nombres d'injections)*
Soient E un ensemble à p éléments et F un ensemble à n éléments. Le nombre d'injections de E vers F est

$$A_n^p = n(n-1)\ldots(n-p+1) = \frac{n!}{(n-p)!}.$$

C'est aussi le nombre de p-arrangements d'un ensemble à n éléments.

Proposition 5.4.12 *(Nombres de parties de cardinal donné)*
Soit E un ensemble à n éléments. Le nombre de parties de E à p éléments i.e le nombre de p-combinaisons ($0 \leq p \leq n$) est

$$C_n^p = \frac{A_n^p}{p!} = \frac{n!}{p!(n-p)!}.$$

Propriétés des C_n^p, Formule du binôme , Triangle de Pascal

Convention : On pose $C_n^p = 0$ si $p > n$.

Proposition 5.4.13 $C_n^0 = 1$, $C_n^1 = n$, $C_n^n = 1$, $C_n^p = C_n^{n-p}$, $C_n^p = C_{n-1}^p + C_{n-1}^{p-1}$.

Proposition 5.4.14 *(Formule du binôme)*
$(a+b)^n = \sum_{p=0}^{n} C_n^p a^p b^{n-p}$.

Proposition 5.4.15 *(Ensembles des parties)*
Soit E un ensemble fini.

$$Card(\mathscr{P}(E)) = 2^{Card(E)}.$$