Université de Metz

Licence de Mathématiques

1ère année, 1er semestre

Logique et théorie des ensembles

par Ralph Chill

Laboratoire de Mathématiques et Applications de Metz

Année 2008/09

Contenu

CHAPITRE 1

Logique

1. Logique des propositions

1.1. Proposition.

DÉFINITION 1.1 (Proposition). Une *proposition* est un énoncé déclaratif dont on peut dire s'il est vrai (valeur 1) ou s'il est faux (valeur 0), indépendamment de tout context de lieu, de temps, ou de personne qui le prononce. De plus, un énoncé qui est à la fois vrai et faux n'est pas une proposition.

REMARQUE 1.2. (a) En mathématiques, une proposition est dite vraie si elle est démontrable.
(b) On écrit tout court p, q, ... afin de désigner une proposition.

1.2. Connecteurs logiques. Les propositions sont les *atomes* en logique. A partir d'une, deux ou plusieurs propositions on peut créer de nouvelles propositions à l'aide de *connecteurs logiques*. Nous allons définir les règles pour les cinq connecteurs 'non', 'et', 'ou', 'si ... alors' et 'si et seulement si'.

DÉFINITION 1.3 (Négation, 'non'). La négation d'une proposition est une proposition qui est vraie si celle-ci est fausse et vice-versa.
Notation: $\neg$.

La *table de vérité* de la négation est la suivante:

p	$\neg p$
0	1
1	0

Quelques traductions usuelles: "non", "il est faux que", "ne ... pas".

EXEMPLES 1.4. (a) Vous n'êtes pas sans savoir que Beethoven a écrit l'Hymne à la Joie.
(b) Un androgyne n'est ni homme ni une femme.

DÉFINITION 1.5 (Conjonction, 'et'). La conjonction de deux propositions est une proposition qui est vraie si les deux propositions sont simultanément vraies. Elle est fausse dès que l'une au moins des deux propositions est fausse.
Notation: $\wedge$.

La *table de vérité* de la conjonction est la suivante:

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

Quelques traductions usuelles: ”et”, ”mais”, ”quoique”, ”bien que”.

Exemples 1.6. (a) Il ne m’a pas plu quoiqu’il ait du charme.
(b) Céline est un grand écrivain mais c’est un personnage contreversé.

Définition 1.7 (Disjonction, ’ou inclusif’). La disjonction de deux propositions est une proposition qui est vraie dès que l’une au moins des deux propositions est vraie. Elle est fausse si les deux propositions sont simultanément fausses.
Notation: $\vee$.

La *table de vérité* de la disjonction est la suivante:

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

Quelques traductions usuelles: ”ou”, ”à moins que”.

Exemples 1.8. (a) Ce médicament peut provoquer des troubles de l’équilibre ou de la vue.
(b) Simon viendra à moins qu’il soit malade.

Définition 1.9 (Implication, Conditionnelle, ’si ... alors’). Si p et q sont deux propositions, alors l’implication ”si p alors q” est une proposition qui est vraie si p est faux, ou bien si p et q sont simultanément vrais. Cette implication est fausse uniquement si l’*antécédant* p est vrai et le *conséquent* q faux.
Notation: $\rightarrow$.

La *table de vérité* de l’implication est la suivante:

p	q	$p \rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

Quelques traductions usuelles: ”si ... alors”, ”implique”, ”a pour conséquence”, ”donc”. L’implication $p \rightarrow q$ sera aussi traduit par ”p seulement si q”, car la proposition ”p seulement si q” n’est faux que dans le cas où p est vrai et q est faux, et elle a donc la même table de vérité que $p \rightarrow q$.

Exemple 1.10. (a) Si Jupin a de bons avocats alors il n’ira pas en prison.

DÉFINITION 1.11 (Equivalence, 'si et seulement si'). Si p et q sont des propositions, alors l'équivalence 'p si et seulement si q' est une proposition qui signifie *(p si q) et (p seulement si q)*. La valeur de vérité de l'équivalence 'p si et seulement si q' est la valeur de vérité de $(q \to p) \wedge (p \to q)$. L'équivalence '$p$ si et seulement si q' est donc vraie uniquement si p et q ont la même valeur de vérité.

Notation: $\leftrightarrow$.

La *table de vérité* de l'équivalence est la suivante:

p	q	$p \leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

Quelques traductions usuelles: "si et seulement si", "équivaut à", "équivaut à dire" ou "revient à dire".

REMARQUE 1.12. La négation est un connecteur *unaire* (elle n'a qu'un argument), alors que la conjonction, la disjonction, l'implication et l'équivalence sont des connecteurs *binaires* (elles ont deux arguments). La conjonction, la disjonction et l'équivalence sont *commutatives* dans le sens que les propositions $p \wedge q$ et $q \wedge p$ (respectivement $p \vee q$ et $q \vee p$, ou $p \leftrightarrow q$ et $q \leftrightarrow p$) ont la même table de vérité. L'implication n'est pas commutative; les propositions $p \to q$ et $q \to p$ n'ont pas la même table de vérité.

REMARQUE 1.13. Attention: "parce que", "à cause de cela", "que", "car" et "puisque" ne sont pas des connecteurs logiques. Ainsi, les schémas "p parce que q", "p à cause de cela q" etc. ne sont pas des schémas de propositions.

1.3. Formules et langage des propositions. Les symboles du langage abstrait (langage objet) que l'on va définir sont:

- des lettres de proposition: $p, q, r, \ldots$
- des symboles: $\neg, \wedge, \vee, \to, \leftrightarrow$
- des parenthèses: ()

DÉFINITION 1.14 (constructive).

(i) Une lettre de proposition est une formule dite atomique.
(ii) Si A est une formule, alors $\neg A$ l'est aussi.
(iii) Si A et B sont des formules, alors $(A \wedge B)$, $(A \vee B)$, $(A \to B)$ et $(A \leftrightarrow B)$ sont aussi des formules.
(iv) Rien d'autre n'est une formule.

EXEMPLE 1.15. $(\neg(p \vee q) \to (\neg p \wedge \neg q))$ est une formule.

Afin d'alléger l'écriture, on convient que l'on peut enlever les parenthèses extérieures dans l'assemblage final (et non dans les écritures intérmediaires).

Attention: les schémas $\neg(p)$ ou $(p \to q \to r)$ ne sont pas des formules!

1.4. Mise en formule et point de vue sémantique. Pour déterminer la valeur de vérité d'une proposition complexe, on peut envisager la méthode suivante:

- on fait apparaître la structure logique de la proposition en la décomposant en ses constituant atomiques. On obtient alors une formule (F) qui est un objet dénué de sens où apparaissent des lettres de propositions p, q, r, ... et des connecteurs logiques ($\wedge$, $\vee$, $\neg$, $\rightarrow$, $\leftrightarrow$);
- pour toute les attributions (assignations) possibles de valeurs de vérité à la suite de lettres p, q, r, ... intervenant dans la formule (F) on calcule la valeur de vérité du composé (F).

C'est la *méthode des fonctions (ou tables) de vérité*.

Pour simplifier l'écriture on conviendra de mettre le symbole 1 à la place de *vrai* et 0 à la place de *faux*.

La méthode consiste donc à interpréter la formule (F) (dénuée de sens) comme une fonction où les variables sont les lettres de propositions prenant leurs valeurs dans l'ensemble à deux éléments 0 et 1.

Cette intérprétation d'une formule comme fonction des valeurs de vérité des ses lettres de proposition considérées comme variables est le *point de vue sémantique*.

EXEMPLE 1.16. Considérons l'énoncé suivant:

> *L'accusé n'a pu se rendre coupable du crime* [C] *que s'il était à New-York à 18 heures le* 1^{er} *janvier* [N]. *Mais il a été établi qu'il était à ce moment-là à Washington* [W]. *Donc il n'est pas coupable du crime.*

En utilisant les abréviations entre les crochets, nous obtenons pour la mise en formule de cette proposition:

(C seulement si N mais W) donc non C,
ou: $((C \rightarrow N) \wedge W) \rightarrow \neg C$.

La table de vérité de cette formule/proposition est la suivante:

C	N	W	$((C \rightarrow N) \wedge W) \rightarrow \neg C$
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	0

1.5. Propositions logiquement vraies, fausses, équivalentes.

DÉFINITION 1.17. Une formule A est dite *valide* si sa table de vérité ne contient que des 1.

DÉFINITION 1.18. On appelera formule complète d'une proposition P une formule représentant la proposition donnée telle que les lettres utilisées dans cette représentation désignent des propositions (constituant P) ne contenant aucun connecteur logique.

DÉFINITION 1.19. Une proposition est *logiquement vraie* ou *tautologique* si sa formule complète est valide.

Une proposition est *logiquement fausse* ou *contradictoire* si sa négation est logiquement vraie.

EXEMPLE 1.20. La proposition *Paul est malade ou n'est pas malade* est logiquement vraie car sa formule $p \vee \neg p$ est valide.

REMARQUES 1.21. (a) Une proposition contradictoire a une formule complète dont la table de vérité ne comporte que des 0.

(b) Les formules sont réparties en trois classes, à savoir: les formules *valides*, les formules *contradictoires*, et les formules *neutres*, c.à.d. les formules qui ne sont ni valides ni contradictoires (formules dont la table de vérité contient à la fois des 0 et des 1).

DÉFINITION 1.22. On dit que deux propositions sont *logiquement équivalentes* si leurs formules complètes sont équivalentes, c.à.d. ont la même table de vérité.

On dit qu'une proposition P *implique logiquement* une proposition Q si la proposition '*si P alors Q*' est tautologique.

DÉFINITION 1.23. Un *enthymème* est une proposition qui semble logiquement vraie mais qui ne l'est pas car elle contient un implicite de l'esprit. Et lorsque l'on complète cette proposition avec l'argument implicite manquant, on obtient alors une tautologie.

EXEMPLE 1.24. La proposition

> *L'accusé n'a pu se rendre coupable du crime* [C] *que s'il était à New-York à 18 heures le* 1^{er} *janvier* [N]. *Mais il a été établi qu'il était à ce moment-là à Washington* [W]. *Donc il n'est pas coupable du crime.*

de l'exemple 1.16 est un enthymème. On a vu dans l'exemple 1.16 que cette proposition n'est pas logiquement vraie car sa table de vérité contient un 0. L'argument manquant est l'argument que l'accusé ne peut pas être à New-York à 18 heures le 1^{er} janvier et à ce moment là aussi à Washington. La formule complète avec l'argument manquant serait alors

$$((C \to N) \wedge W \wedge \neg(N \wedge W)) \to \neg C.$$

Cette formule est valide (vérifier par la table de vérité!), l'argument complété est tautologique.

2. Logique des prédicats

2.1. Variables et quanteurs. On constate que le langage abstrait des propositions introduit en Section 1.3 ne suffit pas pour mettre en formule toutes les propositions du langage usuel et les propositions mathématiques. Des exemples sont les énoncés

Tout être humain est mortel,
or Socrate est un être humain,
donc Socrate est mortel.

ou

tout éléphant est gros

ou

il existe $n \in \mathbb{N}$ tel que $n^2 = 4$.

Ces trois énoncés contiennent en fait des *variables*: c'est la variable n dans le troisième exemple, et une variable x non explicitement visible dans les premiers deux exemples (variable qui peut désigner un animal comme par exemple un éléphant ou un être humain). En plus, ces trois énoncés contiennent les *quanteurs* "tout" (ou "quelque soit") et "il existe". Ces éléments ne peuvent pas être traduits en formule dans le langage abstrait des propositions.

On va donc introduire de nouvelles formules qu'on appelle aussi *schémas de quantification* ou simplement *schémas*. Par exemple, on mettra

$$Gx \quad pour \quad x \text{ est gros}$$

et

$$Ex \quad pour \quad x \text{ est un éléphant,}$$

et on utilisera le symbol $\forall$ au lieu du quanteur "tout" ou "quelque soit". L'énoncé *Tout éléphant est gros* devient alors

$$\forall x(Ex \to Gx).$$

Attention: l'énoncé *x est gros* n'est pas une proposition. C'est un prédicat; plus précisément, un prédicat à une variable. Par contre, l'énoncé *Tout éléphant est gros* est une proposition (à condition que les termes *gros* et *éléphant* ont été definis clairement et sont donc indépendants de tout context, lieu ou personne qui prononce cet énoncé).

De la même manière on peut mettre

$$An \quad pour \quad n \text{ est un élément de } \mathbb{N}$$

et

$$Bn \quad pour \quad n^2 = 4,$$

et on utilisera le symbol $\exists$ au lieu du quanteur "il existe". L'enoncé *Il existe un* $n \in \mathbb{N}$ *tel que* $n^2 = 4$ devient alors

$$\exists n(An \wedge Bn).$$

2.2. Formules et langages de prédicats. Dans cette partie on va donc formellement élargir le langage des propositions qui était introduit dans la partie 1.3 de ce chapitre.

Les symboles du nouveau langage abstrait (langage objet) que l'on va définir sont:

- les lettres de prédicats à 0, 1, ou plusieurs arguments: $p, q, r, \ldots$
- les lettres de variables d'objets ou variables d'individus: $x, y, z, \ldots$
- les quantificateurs: $\forall$, $\exists$
- les symboles: $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$
- les parenthèses: ()

REMARQUE 1.25. Les prédicats à 0 arguments ne sont rien d'autre que les propositions définis dans la section précédente.

DÉFINITION 1.26 (constructive).

(i) Si p est un prédicat à n arguments et si $x_1, \ldots, x_n$ sont des variables, alors $p(x_1, \ldots, x_n)$ est une formule dite atomique.
(ii) Si A est une formule, alors $\neg A$ l'est aussi.
(iii) Si A et B sont des formules, alors $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$ et $(A \leftrightarrow B)$ sont aussi des formules.
(iv) Si A est une formule et x est une variable, alors $\forall x A$ et $\exists x A$ sont des formules.
(v) Rien d'autre n'est une formule.

Il faut comparer cette définition du langage des prédicats avec celle du langage des propositions (Définition 1.14). Les lettres de propositions sont remplacées par des lettres de prédicats (qui peuvent en plus dépendre d'une ou plusieurs variables), et on a ajouté les symboles $\forall$ et $\exists$. Contrairement au langage des propositions, dans le langage des prédicats pas toutes les formules représentent des propositions. La définition suivante peut servir pour reconnaître les propositions.

DÉFINITION 1.27. Une variable qui apparaît dans un quanteur est dite *liée*. Une variable qui n'apparaît dans aucun quanteur est dite *libre*.

Un énoncé (resp. une formule) qui ne comporte aucune variable libre est dit *clos* (resp. *close*). Un énoncé clos est une proposition.

DÉFINITION 1.28. La *clôture universelle* (resp. *clôture existentielle*) d'une formule est la formule obtenue en adjoignant au début de cette formule les quanteurs $\forall x$, $\forall y$, ... (resp. $\exists x$, $\exists y$, ...) correspondants aux variables libres (s'il en existe) $x, y, \ldots$ de cette formule.

2.3. Formules valides et inconsistentes.

DÉFINITION 1.29. Une formule est dite *valide* si sa clôture universelle est valide, c.à.d. si toutes les instances de sa clôture universelles sont vraies.

Une formule est dite *inconsistente* si sa négation est valide.

EXEMPLE 1.30. Considérons la formule

$$\neg(\forall x Fx \wedge \neg Fy). \tag{1.1}$$

La seule variable libre est la variable y. La clôture universelle est donc

$$\forall y \neg(\forall x Fx \wedge \neg Fy).$$

Par la loi de De Morgan (voir la Proposition 1.35 en bas), cette formule est équivalente à

$$\forall y(\neg \forall x Fx \vee \neg\neg Fy).$$

Comme $\neg\neg Fy$ et Fy sont équivalentes, on peut ré-écrire

$$\forall y(\neg \forall x Fx \vee Fy).$$

Comme $\neg p \vee q$ et $p \to q$ sont équivalentes, on simplifie pour obtenir

$$\forall y(\forall x Fx \to Fy).$$

Cette dernière formule est valide, car

- si $\forall x Fx$ est faux, alors l'implication $\forall x Fx \to Fy$ est vraie, et
- si $\forall x Fx$ est vrai, alors Fy pour toute valeur de y (intérprétation sémantique de $\forall$) et donc l'implication $\forall x Fx \to Fy$ est vraie.

Ainsi, la formule (1.1) est valide.

EXEMPLE 1.31. La formule

$$\exists x Fx \wedge \forall x \neg Fx$$

est inconsistante.

3. Modes de raisonnement

3.1. Raisonnement par table de vérité.

PRINCIPE 1.32. Afin de démontrer qu'une formule est valide, on vérifie que sa table de vérité ne contient que des 1 (Définitions 1.17 et 1.29). Afin de démontrer que deux formules sont équivalentes, on montre qu'elles ont la même table de vérité (Définition 1.22).

PROPOSITION 1.33 (Transitivité de l'implication). *La formule suivante est valide:*

$$((p \to q) \wedge (q \to r)) \to (p \to r).$$

DÉMONSTRATION. On écrit la table de vérité:

p	q	r	$((p \to q) \wedge (q \to r)) \to (p \to r)$
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	1

□

La proposition suivante est une conséquence immédiate de la proposition précécente.

PROPOSITION 1.34 (Transitivité de l'équivalence). *La formule suivante est valide:*

$$((p \leftrightarrow q) \wedge (q \leftrightarrow r)) \rightarrow (p \leftrightarrow r).$$

PROPOSITION 1.35 (Lois de De Morgan). *Les formules suivantes sont équivalentes:*

$$(a) \quad \neg(p \wedge q) \quad et \quad \neg p \vee \neg q,$$

$$(b) \quad \neg(p \vee q) \quad et \quad \neg p \wedge \neg q$$

DÉMONSTRATION. (a) On écrit la table de vérité

p	q	$\neg(p \wedge q)$	$\neg p \vee \neg q$
0	0	1	1
0	1	1	1
1	0	1	1
1	1	0	0

(b) On écrit la table vérité

p	q	$\neg(p \vee q)$	$\neg p \wedge \neg q$
0	0	1	1
0	1	0	0
1	0	0	0
1	1	0	0

□

3.2. Raisonnement par implications. Règle du modus ponens.

PRINCIPE 1.36 (Modus ponens). Si p est vraie et si $p \rightarrow q$ est vraie, alors q est vraie.

Ainsi, pour démontrer une propriété C (conséquence) partant d'une proposition vraie H (hypothèse), on démontrera

$$H \rightarrow P_0,\ P_0 \rightarrow P_1,\ \ldots,\ P_{n-1} \rightarrow P_n \text{ et } P_n \rightarrow C.$$

EXEMPLE 1.37.

EXERCICE 1.38. (1) Montrer sans calculer des dérivées que la fonction définie par $f(x) = \frac{x^2+1}{e^{-x}+1}$ est croissante sur $\mathbb{R}_+$.
(2) Montrer que l'ensemble des sommes de deux carrés d'entiers est stable par multiplication.
(3) Les formules

$$((p \rightarrow q) \rightarrow r) \rightarrow (p \rightarrow r)$$

ou

$$((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$$

sont-elles valides?
(4) Montrer que si une fonction $f : \mathbb{R} \to \mathbb{R}$ est dérivable en un point x_0, alors elle est continue en x_0.
(5) Sachant que pour tout $n \in \mathbb{N}$ l'on a $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$, montrer que pour tout $n \in \mathbb{N}^*$ l'on a $\sum_{k=1}^{n}(2k-1) = n^2$.

3.3. Raisonnement par équivalences.

PRINCIPE 1.39. On établit l'équivalence $p \leftrightarrow q$ à l'aide d'une chaine d'équivalences car l'équivalence est transitive (Proposition 1.34).

EXERCICE 1.40. (1) Résoudre dans $\mathbb{R}$ en raisonnant par équivalences l'équation $\sqrt{x^2+2} = 3x$.
(2) Résoudre dans $\mathbb{C}$ en raissonant par équivalences l'équation $z^5 = \overline{z}$.
(3) Trouver toutes les fonctions réelles dérivables vérifiant $y' = y$.

3.4. Raisonnement par disjonction des cas.

EXEMPLE 1.41. On montre que la formule suivante

$$(F) \qquad \underbrace{((p \to q) \wedge \neg q)}_{\text{antécédent}} \quad \to \quad \underbrace{\neg p}_{\text{conséquent}}$$

est valide.

- Si l'antécédent est faux, alors l'implication dans (F) est vraie.
- Si l'antécédent est vrai, alors $p \to q$ et $\neg q$ sont simultanément vraies, c.à.d. $p \to q$ est vrai et q est faux. On en déduit alors que $\neg p$ est vrai, c.à.d. le conséquent dans (F) est vrai. Donc, l'implication dans (F) est vraie.

Comme l'antécédent est soit vrai, soit faux, on conclut que (F) est valide.

EXERCICE 1.42. (1) Montrer que pour tout $n \in \mathbb{N}$ on a: $3|n(n^2+2)$.
(2) Montrer que

$$((p \vee q) \wedge (p \to r) \wedge (q \to r)) \to r$$

est valide.
(3) Calculer les parties réelles et imaginaires de $(1+i)^n$ pour $n \in \mathbb{Z}$.
(4) Montrer que la proposition suivante est vraie:

$$\exists x (x \in \mathbb{R} \setminus \mathbb{Q} \wedge x^{\sqrt{2}} \in \mathbb{Q}.$$

3.5. Raisonnement par l'absurde.

PRINCIPE 1.43. Pour démontrer la propriété p, on suppose $\neg p$ (hypothèse du raisonnement par l'absurde) et on en déduit une contradiction, c.à.d. une proposition q telle que q et $\neg q$ soient vraies. On conclut alors que p est vraie.

EXERCICE 1.44. (1) Montrer que la formule

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

est valide.
(2) Montrer qu'il n'existe pas de surjection de l'ensemble E vers $P(E)$, ensemble

des parties de E.
(3) Montrer que la proposition suivante est vraie:

$$\exists x(x \in \mathbb{R} \setminus \mathbb{Q} \wedge x^{\sqrt{2}} \in \mathbb{Q}.$$

(4) Montrer que l'ensemble des entiers naturels premier est infini.
(5) Montrer qu'on a

$$\sqrt{2} \notin \mathbb{Q}.$$

3.6. Raisonnement par contraposition.

PROPOSITION 1.45. *Les implications $p \to q$ et $\neg q \to \neg p$ sont équivalentes.*

Cette proposition, qui se démontre facilement à l'aide d'une table de vérité, justifie le principe suivant.

PRINCIPE 1.46. Pour démontrer l'implication $p \to q$, on démontre $\neg q \to \neg p$.

EXERCICE 1.47. (1) Montrer que la relation $\leq$ est antisymétrique dans $\mathbb{R}$.
(2) Montrer que la formule

$$(p \to q) \leftrightarrow (\neg q \to \neg p)$$

est valide.
(3) Montrer que pour tout $(x, y) \in \mathbb{R}^2$ on a $(x \neq y) \to (x^3 \neq y^3)$.
(4) Montrer que si $\theta \in \mathbb{R} \setminus 2\pi\mathbb{Z}$, alors la suite $(e^{in\theta})_{n\in\mathbb{N}}$ diverge.

3.7. Raisonnement par récurrence.

PRINCIPE 1.48. Pour démontrer que la proposition

$$\forall n((n \in \mathbb{N}) \to P(n)),$$

est vraie on peut effectuer les deux étapes suivantes:
(i) On prouve $P(0)$.
(ii) On prouve que si $P(n)$ est vraie pour un certain $n \in \mathbb{N}$, alors $P(n+1)$ est vraie.

REMARQUE 1.49. Une variante du raisonnement par récurrence est la suivante:
(i) On prouve $P(0)$.
(ii) On prouve que si $P(0), \ldots, P(n)$ sont vraies pour un certain $n \in \mathbb{N}$, alors $P(n+1)$ est vraie.

EXERCICE 1.50. (1) Montrer que pour tout $n \in \mathbb{N}$ l'on a $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$.
(2) Montrer que pour tout $n \in \mathbb{N}$ l'on a $\sum_{k=0}^{n} k^3 = (\frac{n(n+1)}{2})^2$.
(3) Montrer que pour des entiers $k \leq n$, le nombre de sous-ensembles à k éléments d'un ensemble à n éléments est $C_n^k = \frac{n!}{k!(n-k)!}$.
(4) Montrer que si $a \in \mathbb{N}$, alors pour tout $n \in \mathbb{N}$ l'entier $(a+1)^{n+1} - a(n+1) - 1$ est multiple de a^2.

3.8. Raisonnement par contre-exemple.

PROPOSITION 1.51. *Les propositions* $\neg\forall x P(x)$ *et* $\exists x \neg P(x)$ *sont équivalentes.*

PRINCIPE 1.52. Pour démontrer que la proposition $\forall x P(x)$ est fausse, on trouve x_0 tel que $\neg P(x_0)$ soit vraie.

EXERCICE 1.53. (1) Montrer qu'un nombre entier divisible par 6 et par 4 n'est pas nécessairement divisible par 24.
(2) Montrer que l'intersection de deux disques dans le plan n'est pas nécessairement convexe.

CHAPITRE 2

Théorie des ensembles

1. L'approche naïve à la théorie des ensembles

En 1895, Georg Cantor donnait la définition suivante d'un ensemble:

> Nous appelons *ensemble* toute réunion M d'objets de notre conception, déterminés et bien distincts, que nous nommérons *éléments* de M.

ou

> Un *ensemble* est une collection dobjets (que l'on appelle éléments de l'ensemble), ou une multitude qui peut être comprise comme un tout.[1]

Cantor utilise les lettres majuscules pour les ensembles, et les lettres minuscules pour les éléments d'ensembles. Comme lui, nous utilisons la notation

$$M = \{x, y, c\}$$

pour écrire *en extension* l'ensemble M qui contient exactement les éléments x, y et c. Notons que l'élément x est bien distinct de l'ensemble $\{x\}$ qui contient x!

Nous allons en plus adopter le point de vue extensionnaliste d'identifier deux ensembles qui contiennent les mêmes éléments. Ainsi, par exemple, les ensembles

$$\{1, 1, 2\} \text{ et } \{1, 2\}$$

sont égaux.

Soit c le nombre de souffles que Jules César a fait le dernier jour avant sa mort. D'après la définition de Cantor,

$$E = \{20000, c\}$$

est un ensemble. C'est l'ensemble qui contient exactement le nombre 20000 et le nombre c. D'après le point de vue extensionnaliste, nous ne pouvons pas savoir si cet ensemble contient un élément ou deux, car il est tout à fait possible que $c = 20000$, auquel cas on aurait $E = \{20000\}$.

Quelques notations:
Nous écrivons $x \in E$ pour dire *x appartient à E* ou *x est élément de E*.

[1] L'original en allemand est: Unter einer 'Menge' verstehen wir jede Zusammenfassung M von bestimmten, wohlunterscheidbaren Objekten m unserer Anschauung oder unseres Denkens (welche die 'Elemente' von M genannt werden) zu einem Ganzen.

Nous dirons que E est une *partie* (ou: un *sous-ensemble*) de F si tout élément de E est aussi un élément de F, et nous écrivons tout court $E \subset F$. Plus formellement,

$$E \subset F \quad :\Leftrightarrow \quad \forall x\,(x \in E \to x \in F).$$

Si E et F sont deux ensembles *égaux*, nous écrivons $E = F$. Avec notre définition de la partie et avec le point de vue extensionnaliste, on a

$$E = F \quad \leftrightarrow \quad (E \subset F \wedge F \subset E).$$

Nous définissons la *réunion* $E \cup F$ comme l'ensemble qui contient tous les éléments de E et de F, et l'*intersection* $E \cap F$ comme l'ensemble qui contient tous les éléments qui appartiennent à la fois à E et à F. La *différence* $E \setminus F$ est l'ensemble de tous les éléments dans E qui n'appartiennent pas à F. Si $F \subset E$, alors nous notons aussi $\complement_E F = E \setminus F$ et nous appelons $\complement_E F$ le *complément* de F dans E. Enfin, la *différence symétrique* $E \triangle F$ est l'ensemble défini par $E \triangle F = (E \setminus F) \cup (F \setminus E)$.

Il est important à noter que l'approche naïve à la théorie des ensembles (basée sur la définition de Cantor) est malheureusement contradictoire, comme Bertrand Russell a démontré. Il a considéré l'ensemble E de tous les ensembles qui ne se contiennent pas eux-mêmes:

$$E = \{F : F \text{ est ensemble et } F \notin F\}. \tag{2.1}$$

Si $E \in E$, alors par la définition de E, $E \notin E$. Mais si $E \notin E$, alors par la définition de E, $E \in E$. On obtient donc $E \in E \wedge E \notin E$, ce qui est contradictoire.

Bertrand Russell a aussi formulé la variante suivante:

> Epiménides, le crétois, dit: tous les crétois sont des menteurs. Est-ce que Epiménides est un menteur?

2. Approche axiomatique à la théorie des ensembles

Dans la suite, *toutes* les lettres désignent des ensembles!!!

Dans cette partie, on va introduire la théorie des ensembles à partir de quelques axiomes. Par "définition", un axiome est une règle sans prémisses. Ou un axiome est par définition un théorème vrai qui ne nécessite pas de démonstration.

2.1. L'axiome de l'extensionalité. Le premier axiome nous dit quand est-ce que deux ensembles sont égaux; encore une fois, nous adoptons le point de vue extensionnaliste. Le premier axiome explique la signification du symbole = dans la théorie des ensembles (voir le paragraphe précédent).

Axiome 1 (Extensionalité). Deux ensembles qui contiennent les mêmes éléments sont égaux.

En langage des prédicats:

$$\forall E\, \forall F\, (\forall x(x \in E \leftrightarrow x \in F)) \to E = F.$$

Nous rappelons que d'après cet axiome, deux ensembles E et F sont égaux si et seulement si $E \subset F$ et $F \subset E$. C'est cette caractérisation de l'égalité qu'on utilise d'habitude pour montrer que deux ensembles sont égaux.

2.2. L'axiome de la compréhension. Le deuxième axiome permet de construire des ensembles à partir d'un ensemble donné et des propriétés données.

Axiome 2 (Compréhension). Si E est un ensemble et Px est une propriété, alors il existe l'ensemble

$$\{x \in E : Px\}.$$

Notons que cet axiome de compréhension marque une différence importante par rapport à l'approche naïf à la théorie des ensembles. Alors que la définition de Cantor implique que

$$\{x : x \text{ est un ensemble}\}$$

est un ensemble (l'ensemble *universel* de tous les ensembles!) et que

$$\{x : x \text{ est un ensemble et } x \notin x\}$$

est aussi un ensemble (l'ensemble du paradoxe de Russell), l'axiome de compréhension (Axiome 2) ne garantit pas que l'ensemble universel est *vraiement* un ensemble. Au contraire: avec l'axiome de compréhension on peut même démontrer que l'ensemble universel n'existe pas! En particulier, on *ne peut pas* construire l'ensemble de tous les ensembles qui ne se contiennent pas eux-mêmes. Le paradoxe de Russell qui montrait que l'approche naïf à la théorie des ensembles est contradictoire n'a donc plus de sens. Si on voulait démontrer que le système d'axiomes que nous allons présenter ici est contradictoire, il faudrait trouver une autre contradiction.

Proposition 2.1. *On suppose les Axiomes 1 et 2. Alors pour tout ensemble E il existe un ensemble F tel que $F \notin E$.*

Démonstration. Soit E un ensemble quelquonque. On définit

$$F := \{x \in E : x \notin x\}.$$

D'après l'Axiome 2, F est un ensemble. On montre que $F \notin E$. Pour cela, on fait un raisonnement par l'absurde.

Supposons alors que $F \in E$. Alors deux cas sont possibles. Soit $F \in F$, soit $F \notin F$. Si $F \notin F$, alors par définition de F, on obtient $F \in F$. De même, par la définition de F, si $F \in F$, alors $F \notin F$. On a donc trouvé $F \in F$ et $F \notin F$, ce qui est une contradiction. Ainsi, l'hypothèse $F \in E$ est faux, c.à.d. $F \notin E$. □

Remarque 2.2. Le raisonnement dans cette démonstration (disjonction des deux cas $F \in F$ et $F \notin F$) est celui qu'on utilise dans le paradoxe de Russell, mais ici c'est nécessaire que $F \in E$.

Les Axiomes 1 et 2 sont déjà suffisants pour définir l'intersection de deux ensembles et de dire que elle est de nouveau un ensemble.

DÉFINITION 2.3 (Intersection). Soient E, F deux ensembles. On définit

$$E \cap F := \{x \in E : x \in F\},$$

et on appelle $E \cap F$ l'*intersection* de E et de F. D'après l'Axiome 2, l'intersection $E \cap F$ est un ensemble.

On a

$$E \cap F = F \cap E.$$

En effet, on a

$$\begin{aligned} x \in E \cap F &\leftrightarrow x \in E \wedge x \in F \\ &\leftrightarrow x \in F \wedge x \in E \\ &\leftrightarrow x \in F \cap E. \end{aligned}$$

L'égalité $E \cap F = F \cap E$ est donc une conséquence de l'Axiome 1 et de la définition de l'intersection.

DÉFINITION 2.4 (Différence). Soient E, F deux ensembles. On définit

$$E \setminus F := \{x \in E : x \notin F\},$$

et on appelle $E \setminus F$ la *différence* de E et de F. D'après l'Axiome 2, la différence $E \setminus F$ est un ensemble.

2.3. L'axiome de l'existence.

AXIOME 3 (Existence). Il existe un ensemble.

On suppose les Axiomes 1-3. Soit E un ensemble (qui existe d'après l'Axiome 3). Alors on peut définir

$$\emptyset := \{x \in E : x \neq x\}.$$

D'après l'Axiome 2, $\emptyset$ est un ensemble. On appelle $\emptyset$ l'*ensemble vide*. D'après l'Axiome 1, l'ensemble $\emptyset$ est unique (sa définition ne dépend par exemple pas de l'ensemble E de départ). L'ensemble vide est le premier (et jusqu'ici le seul!) ensemble concret.

L'axiome de l'existence sera plus tard remplacé par un axiome plus fort, notamment par l'axiome de l'existence d'un ensemble infini.

2.4. L'axiome de la réunion. L'existence de la réunion de deux ensembles n'est pas encore garanti après les premiers trois axiomes, et en fait, il faut un axiome supplémentaire pour garantir cette existence. Il y a deux version de l'axiome de l'existence de la réunion: l'existence de la réunion de deux ensembles (ou d'un nombre fini d'ensembles), et l'existence de la réunion d'une famille quelconque d'ensembles.

La première version est la suivante.

Axiome 4 (Réunion). Si E et F sont deux ensembles, alors il existe un ensemble qui contient tous les éléments de E et de F.

En langage des prédicats:

$$\forall E\, \forall F\, \exists G\, ((x \in E \vee x \in F) \to x \in G).$$

Définition 2.5. Soient E et F deux ensembles, et soit G un ensemble qui contient tous les éléments de E et de F (un tel ensemble existe d'après l'Axiome 4). Alors on définit

$$E \cup F := \{x \in G : x \in E \vee x \in F\},$$

et on appelle $E \cup F$ la réunion de E et de F. D'après l'Axiome 2, la réunion est un ensemble.

La définition de la réunion ne dépend pas de l'ensemble G d'après l'Axiome 1. En plus, on a

$$E \cup F = F \cup E.$$

La deuxième version de l'axiome de la réunion est la suivante.

Axiome 4' (Réunion). Pour tout ensemble E il existe un ensemble qui contient tous les éléments des éléments de E.

En langage des prédicats:

$$\forall E\, \exists F\, \forall x\, \forall X\, ((x \in X \wedge X \in E) \to x \in F).$$

Remarque 2.6. Attention: les deux axiomes de la réunion sont indépendants l'un de l'autre, c.à.d. le premier n'implique pas le deuxième et vice versa! Le deuxième axiome de la réunion impliquerait le premier si pour tout pair E et F d'ensembles on savait que $\{E, F\}$ est un ensemble. Mais l'existence de l'ensemble $\{E, F\}$ n'est pas garantie avec les Axiomes 1-3.

2.5. L'axiome de l'ensemble des parties.

Axiome 5 (Ensemble des parties). Si E est un ensemble, alors il existe un ensemble qui contient toutes les parties de E.

En langage des prédicats:

$$\forall E\, \exists P\, \forall F\, (F \subset E \to F \in P).$$

Définition 2.7. Soit E un ensemble, et soit P un ensemble qui contient toutes les parties de E (un tel ensemble existe d'après l'Axiome 5). Alors on définit

$$\mathcal{P}(E) := \{F \in P : F \subset P\},$$

et on appelle $\mathcal{P}(E)$ l'*ensemble des parties* de E.

L'axiome de l'ensemble des parties nous permet de construire de nouveaux ensembles. Rappelons que l'ensemble vide $\emptyset$ est toujours le seul ensemble concret dont nous savons l'existence. Certainement, $\emptyset$ est une partie de $\emptyset$, et c'est en fait la seule partie de $\emptyset$ (pourquoi?). D'après l'Axiome 5 et la Définition 2.7 nous savons alors

que $\{\emptyset\}$ est un ensemble. Attention: $\{\emptyset\}$ n'est l'ensemble vide, mais c'est l'ensemble qui contient $\emptyset$ comme seul élément.

Nous constatons ensuite que $\emptyset$ et $\{\emptyset\}$ sont deux parties de l'ensemble $\{\emptyset\}$, et que ce sont en fait les deux seules parties (pourquoi?). Ainsi, d'après l'Axiome 5 et la Définition 2.7, nous savons que $\{\emptyset, \{\emptyset\}\}$ est un ensemble.

Si nous continuous ce procédé de construire l'ensemble des parties, nous voyons que l'Axiome de l'ensemble des parties (avec l'Axiome de l'existence d'un ensemble) garantit l'existence d'une infinité d'ensembles. Ce sont

$$\begin{aligned}&\emptyset,\\ &\{\emptyset\},\\ &\{\emptyset, \{\emptyset\}\},\\ &\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\},\\ &\vdots\end{aligned}$$

Malheureusement, aucun des ces ensembles contient une infinité d'éléments, et en fait, l'existence d'un ensemble infini (pratiquement, l'existence de $\mathbb{N}$) est seulement la conséquence d'un autre axiome que nous allons discuter dans le troisième chapitre.

3. Le produit cartésien

Définition 2.8 (Couple ordonné). Soient E et F deux ensembles, et soient $x \in E$ et $y \in F$. Alors on définit le *couple ordonné* (x, y) par

$$(x, y) := \{\{x\}, \{x, y\}\}.$$

On doit vérifier si (x, y) est vraiement un ensemble dont l'existence est assuré par les Axiomes 1-5. Premièrement,

$$\{x\} = \{z \in E : z = x\}$$

et

$$\{x, y\} = \{z \in E \cup F : z = x \vee z = y\}$$

sont des ensembles; en fait, ce sont tous les deux parties de $E \cup F$. On utilisera l'Axiome 4 de la réunion et l'Axiome 2 de la compréhension pour voir ça. Par l'Axiome 5 de l'ensemble des parties, $\mathcal{P}(E \cup F)$ est un ensemble, et $\{x\}$, $\{x, y\} \in \mathcal{P}(E \cup F)$. Donc

$$\{\{x\}, \{x, y\}\} = \{z \in \mathcal{P}(E \cup F) : z = \{x\} \vee z = \{x, y\}\}$$

est un ensemble (on applique l'Axiome 2 de la compréhension encore une fois), qui est partie de $\mathcal{P}(E \cup F)$, ou élément de $\mathcal{P}(\mathcal{P}(E \cup F))$.

Le lemme suivant justifie d'appeler (x, y) couple ordonné. La propriété dans le lemme suivant sert des fois comme *définition* de couple ordonné, mais nous préférons de définir le couple ordonné comme un ensemble.

LEMME 2.9. *On a*

$$(x,y) = (x',y'),$$

si et seulement si

$$x = x' \quad et \quad y = y'.$$

DÉMONSTRATION. Premièrement, l'implication

$$(x = x' \wedge y = y') \to (x,y) = (x',y')$$

est une conséquence de la définition du couple ordonné.

Puis, on a les équivalences

$$\begin{aligned}
(x,y) = (x',y') &\leftrightarrow \{\{x\},\{x,y\}\} = \{\{x'\},\{x',y'\}\} \\
&\leftrightarrow \{x\} \in \{\{x'\},\{x',y'\}\} \wedge \{x,y\} \in \{\{x'\},\{x',y'\}\} \wedge \\
&\quad \wedge \{x'\} \in \{\{x\},\{x,y\}\} \wedge \{x',y'\} \in \{\{x\},\{x,y\}\} \\
&\leftrightarrow (\{x\} = \{x'\} \vee \{x\} = \{x',y'\}) \wedge \\
&\quad \wedge (\{x,y\} = \{x'\} \vee \{x,y\} = \{x',y'\}) \wedge \\
&\quad \wedge ((\{x'\} = \{x\} \vee \{x'\} = \{x,y\}) \wedge \\
&\quad \wedge (\{x',y'\} = \{x\} \vee \{x',y'\} = \{x,y\})
\end{aligned}$$

On va distinguer plusieurs cas. Premièrement,

$$\begin{aligned}
\{x\} = \{x'\} \wedge \{x,y\} = \{x',y'\} &\to x = x' \wedge \{x,y\} = \{x,y'\} \\
&\to x = x' \wedge (y = x \vee y = y') \wedge \{x,y\} = \{x',y'\} \\
&\to (x = x' = y \vee (x = x' \wedge y = y')) \wedge \{x,y\} = \{x',y'\} \\
&\to x = x' = y = y' \vee (x = x' \wedge y = y') \\
&\to (x = x' \wedge y = y').
\end{aligned}$$

Deuxèmement,

$$\begin{aligned}
\{x\} = \{x',y'\} \wedge \{x,y\} = \{x',y'\} &\to x = x' = y' \wedge \{x,y\} = \{x,y'\} \\
&\to x = x' = y' \wedge \{x,y\} = \{x'\} \\
&\to x = x' = y = y' \\
&\to (x = x' \wedge y = y').
\end{aligned}$$

Troisiémement,

$$\begin{aligned}
\{x\} = \{x',y'\} \wedge \{x,y\} = \{x'\} &\to x = x' = y' \wedge x = y = x' \\
&\to x = x' = y = y' \\
&\to (x = x' \wedge y = y')
\end{aligned}$$

Quatrièmement,

$$\begin{aligned}
\{x\} = \{x'\} \wedge \{x,y\} = \{x'\} &\to x = x' \wedge x = y = x' \\
&\to x = x' = y.
\end{aligned}$$

Dans le quatrième cas, la propriété $\{x', y'\} = \{x\} \vee \{x', y'\} = \{x, y\}$ devient simplement $\{x', y'\} = \{x\}$. Ceci implique $x = x' = y'$, et avec le quatrième cas, on obtient $x = x' = y = y'$.

Donc, dans tous les cas, $x = x'$ et $y = y'$. □

DÉFINITION 2.10. Soient E et F deux ensembles. On définit le *produit cartésien* $E \times F$ par

$$E \times F := \{z \in \mathcal{P}(\mathcal{P}(E \cup F)) : \exists x \in E \, \exists y \in F \ (z = (x, y))\}.$$

Le produit cartésien est un ensemble d'après les Axiome 4 et 5 (qui impliquent que $\mathcal{P}(\mathcal{P}(E \cup F))$ est un ensemble) et d'après l'Axiome 2 de compréhension.

Afin d'allegér la notation, on va noter

$$(x, y, z) \text{ au lieu de } ((x, y), z) \text{ ou } (x, (y, z))$$

et

$$E \times F \times G \text{ au lieu de } (E \times F) \times G \text{ ou } E \times (F \times G).$$

De manière similaire pour les produits cartésiens de quatre ou plus d'ensembles.

DÉFINITION 2.11 (Relation). Soient E et F deux ensembles. Une *relation de E dans F* est une partie R de $E \times F$. Si $E = F$, alors on dit simplement que R est une *relation dans E*. Si $R \subset E \times F$ est une relation, alors on écrit xRy au lieu de $(x, y) \in R$.

4. Relations d'équivalence

DÉFINITION 2.12. Soit E un ensemble. Une relation $\sim$ dans E est appelée *relation d'équivalence* si les trois propriétés suivantes sont satisfaites:

(i) (Reflexivité) Quelque soit $x \in E$, on a $x \sim x$.
(ii) (Symétrie) Quelque soit $x, y \in E$, on a $x \sim y$ si et seulement si $y \sim x$.
(iii) (Transitivité) Quelque soit $x, y, z \in E$, si $x \sim y$ et $y \sim z$, alors $x \sim z$.

EXEMPLE 2.13. Supposons que l'ensemble $\mathbb{Z}$ est déjà construit. On dit qu'un nombre $n \in \mathbb{Z}$ est divisible par 3, s'il existe un entier $m \in \mathbb{Z}$ tel que $n = 3m$. On définit une relation $\sim$ dans $\mathbb{Z}$ par

$$x \sim y \quad :\Leftrightarrow \quad x - y \text{ est divisible par 3.}$$

Cette relation $\sim$ est une relation d'équivalence, parce que:
(i) Si $x \in \mathbb{Z}$, alors $x - x = 0$ est divisible par 3. Donc $x \sim x$ pour tout $x \in \mathbb{Z}$, c.à.d. $\sim$ est reflexive.
(ii) Si $x, y \in \mathbb{Z}$, et si $x \sim y$, alors $x - y$ est divisible par 3. Alors $y - x$ est aussi divisible par 3, et donc $y \sim x$. Ainsi, $\sim$ est symétrique.
(iii) Si $x, y, z \in \mathbb{Z}$ sont tels que $x \sim y$ et $y \sim z$, alors $\frac{x-y}{3}$ et $\frac{y-z}{3}$ sont des entiers. En prenant la somme, on voit que $\frac{x-z}{3}$ est entier, c.à.d. $x \sim z$. Ainsi, $\sim$ est transitive.

Bien sur, dans cet exemple, le nombre 3 peut être remplacé par n'importe quel autre nombre $n \in \mathbb{Z} \setminus \{0\}$.

Définition 2.14. Soit E un ensemble, et soit $\sim$ une relation d'équivalence dans E. Pour tout $x \in E$ on définit la *classe d'équivalence* $\overline{x}$ par

$$\overline{x} := \{y \in E : x \sim y\}.$$

En plus, on définit l'ensemble E/F de toutes les classes d'équivalences par

$$E/\sim := \{A \in \mathcal{P}(E) : \exists x \in E \ (A = \overline{x})\},$$

et on appelle $E/\sim$ le *quotient de E par la relation $\sim$*.

Définition 2.15. Soit E un ensemble. Une *partition* P de E est un sous-ensemble de $\mathcal{P}(E)$ vérifiant les trois propriétés suivantes:
(i) $\forall A \in P \ (A \neq \emptyset)$,
(ii) $\forall A, B \in P \ (A \neq B \to A \cap B = \emptyset)$, c.à.d. les ensembles dans P sont *mutuellement disjoints*, et
(iii) $\bigcup_{A \in P} A = E$.

Proposition 2.16. *Soit E un ensemble non-vide, et soit $\sim$ une relation d'équivalence dans E. Alors l'ensemble des classes d'équivalences $E/\sim$ est une partition de E.*

Démonstration. (i) Pour tout $x \in E$ on a $x \sim x$ par réflexivité de $\sim$. Donc, $x \in \overline{x}$, ce qui implique que toute classe d'équivalence est non-vide.

(ii) On démontre l'implication

$$\forall x, y \in E \ (\overline{x} \neq \overline{y} \to \overline{x} \cap \overline{y} = \emptyset)$$

par contraposition. Supposons que $\overline{x} \cap \overline{y} \neq \emptyset$. Alors il existe un élément z dans $\overline{x} \cap \overline{y}$, et pour cet élément z on a

$$x \sim z \text{ et } y \sim z.$$

Comme la relation $\sim$ est symétrique et transitive, ceci implique

$$x \sim y.$$

On démontre qu'alors $\overline{x} = \overline{y}$. En fait, si $u \in \overline{x}$, alors $x \sim u$. Comme on a aussi $x \sim y$, et comme $\sim$ est symétrique et transitive, on obtient $y \sim u$, et donc $u \in \overline{y}$. Inversement, si $u \in \overline{y}$, alors $y \sim u$. Comme on a aussi $x \sim y$, et comme $\sim$ est symétrique et transitive, on obtient $x \sim u$, et donc $u \in \overline{x}$. On a donc démontré que $\overline{x} = \overline{y}$ (Axiome 1) si $\overline{x} \cap \overline{y} \neq \emptyset$.

(iii) En utilisant la propriété $x \in \overline{x}$, on obtient

$$E = \bigcup_{x \in E} \{x\} \subset \bigcup_{x \in E} \overline{x} \subset E,$$

ou, d'après l'Axiome 1, $E = \bigcup_{x \in E} \overline{x}$. □

Exemple 2.17. Soit $\sim$ la relation sur $\mathbb{Z}$ qui a été définie dans l'Exemple 2.13. Alors la classe d'équivalence qui contient 0 est

$$\begin{aligned} \overline{0} &= \{x \in \mathbb{Z} : x \sim 0\} \\ &= \{x \in \mathbb{Z} : x \text{ est divisible par } 3\}, \end{aligned}$$

et de manière similaire,

$$\overline{1} = \{x \in \mathbb{Z} : x - 1 \text{ est divisible par } 3\}$$

et

$$\overline{2} = \{x \in \mathbb{Z} : x - 2 \text{ est divisible par } 3\}$$

On voit que $\overline{0} \cup \overline{1} \cup \overline{2} = \mathbb{Z}$, et donc, d'après la Proposition 2.16, il n'y a pas d'autres classes d'équivalences. Par exemple, on a $\overline{0} = \overline{3}$, car $0 \sim 3$.

On trouve alors que le quotient de $\mathbb{Z}$ par la relation d'équivalence $\sim$ (ou: l'ensemble des classes d'équivalences) est donné par

$$\mathbb{Z}/\sim = \{\overline{0}, \overline{1}, \overline{2}\}.$$

Ce quotient sera aussi noté $\mathbb{Z}/3\mathbb{Z}$.

La proposition suivante est une réciproque à la Proposition 2.16.

PROPOSITION 2.18. *Soit E un ensemble non-vide, et soit P une partition de E. Alors la relation $\sim$ définie par*

$$x \sim y \quad :\Leftrightarrow \quad \exists A \in P \ (x \in A \wedge y \in A)$$

est une relation d'équivalence dans E, et $E/\sim = P$.

5. Relations d'ordre

DÉFINITION 2.19. Soit E un ensemble. Une relation $\leq$ dans E est appelée *relation d'ordre dans E* si les trois propriétés suivantes sont satisfaites:

(i) (Reflexivité) Quelque soit $x \in E$, on a $x \leq x$.
(ii) (Anti-symétrie) Quelque soit $x, y \in E$, si $x \leq y$ et $y \leq x$, alors $x = y$.
(iii) (Transitivité) Quelque soit $x, y, z \in E$, si $x \leq y$ et $y \leq z$, alors $x \leq z$.

Un ensemble muni d'une relation d'ordre est dit *ordonné*.

EXEMPLE 2.20. Soit E un ensemble, et soit $\mathcal{P}(E)$ l'ensemble des parties de E. Alors l'inclusion $\subset$ est une relation d'ordre dans $\mathcal{P}(E)$. (Exercice).

EXEMPLE 2.21. On suppose que l'ensemble $\mathbb{N}$ des entiers relatifs est déjà construit. Soit $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$. Pour deux éléments $n, m \in \mathbb{N}^*$ on définit

$$n|m \quad :\Leftrightarrow \quad n \text{ divise } m.$$

Alors | est une relation d'ordre dans $\mathbb{N}^*$. En fait:
(i) Quelque soit $n \in \mathbb{N}^*$ on a que n divise n, ou $n|n$. La relation | est donc reflexive.
(ii) Quelque soit $n, m \in \mathbb{N}^*$, si n divise m, et si m divise n, alors $n = m$. La relation | est donc anti-symétrique.
(iii) Quelque soit $k, n, m \in \mathbb{N}^*$, si k divise n, et si n divise m, alors k divise m. La relation | est donc transitive.

DÉFINITION 2.22. Soit E un ensemble, et soit $\leq$ une relation d'ordre dans E. Soit $A \subset E$, $A \neq \emptyset$.

(i) On dit que l'ordre est *total* si

$$\forall x, y \in E \ (x \leq y \text{ ou } y \leq x).$$

(ii) On dit que l'ordre est *partiel*, s'il n'est pas total.
(iii) On dit que $m \in E$ est un *majorant* (resp. *minorant*) de A si

$$\forall x \in A \ (x \leq m) \quad (\text{resp. } (m \leq x)).$$

(iv) On dit que $M \in A$ est un *plus grand élément* (resp. *plus petit élément*) de A si M est un majorant de A (resp. un minorant de A).
(v) On dit que $m \in E$ est une *borne supérieure* (resp. *borne inférieure*) de A, et on note $m =: \sup A$ (resp. $m =: \inf A$), si m est le plus petit des majorants (resp. le plus grand des minorant).
(vi) On dit que $M \in E$ est *maximal* dans A si $M \in A$ et si

$$\forall x \in A \ (M \leq x \to M = x).$$

(vii) On dit que $M \in E$ est *minimal* dans A si $M \in A$ et si

$$\forall x \in A \ (x \leq M \to M = x).$$

Proposition 2.23. *Soit E un ensemble ordonné, et soit $A \subset E$ tel que $A \neq \emptyset$. Si A admet un plus grand élément (resp. un plus petit élément, resp. une borne supérieure, resp. une borne inférieure), alors cet élément est unique.*

Démonstration. Soient M et N deux plus grand éléments dans A. Alors $M \in A$, $N \in A$, et M et N sont des majorants de A. Comme M est majorant de A, alors $N \leq M$. Comme N est majorant de A, alors $M \leq N$. Comme la relation d'ordre $\leq$ est anti-symétrique, on obtient que $M = N$. Donc, il y a au plus un plus grand élément dans A.

D'une manière similaire, on montre qu'il y a au plus un plus petit élément.

Le fait qu'il y a au plus une borne supérieure et au plus une borne inférieure de A est une conséquence de la définition de la borne supérieure comme plus petit des majorants (resp. de la borne inférieure comme plus grands des minorants) et de ce qu'on vient de démontrer sur l'unicité du plus petit (resp. plus grand) élément. □

Proposition 2.24. *Soit E un ensemble ordonné, et soit $A \subset E$ tel que $A \neq \emptyset$. Alors l'élément $M \in E$ est le plus grand élément (resp. plus petit élément) de A si et seulement si $M \in A$ et $M = \sup A$ (resp. $M = \inf A$).*

Proposition 2.25. *On considère l'ensemble ordonné $(\mathbb{R}, \leq)$. Soit $A \subset \mathbb{R}$ non-vide, et soient $m, M \in \mathbb{R}$. Alors*
(i) $M = \sup A$ si et seulement si

$$\forall x \in A \, (x \leq M) \text{ et } \forall \varepsilon > 0 \, \exists x_\varepsilon \in A \, (M - \varepsilon \leq x_\varepsilon), \text{ et}$$

(ii) $m = \inf A$ si et seulement si

$$\forall x \in A \, (m \leq x) \text{ et } \forall \varepsilon > 0 \, \exists x_\varepsilon \in A \, (x_\varepsilon \leq m + \varepsilon).$$

EXEMPLES 2.26. (i) Dans $(\mathbb{R}, \leq)$ l'intervalle $A = [0, 1[$ admet un plus petit élément (qui est 0), mais pas de plus grand élément. De plus, $\sup A = 1$ et $\inf A = 0$.
(ii) Dans $(\mathbb{Q}, \leq)$, l'ensemble $A = \{x \in \mathbb{Q} : x^2 \leq 2\}$ n'a pas de borne supérieure, et donc a fortiori pas de plus grand élément.
(iii) Dans $(\mathbb{N}^*, |)$, tout nombre premier est minimal.
(iv) Dans $(P(\Omega), \subset)$ on a $\sup\{A, B\} = A \cup B$ et $\inf\{A, B\} = A \cap B$.

6. Fonctions et applications

DÉFINITION 2.27 (Fonction, application). Soient E et F deux ensembles. Une *fonction* de E dans F est une relation de E dans F ayant la propriété que si $x, x' \in E$ et $y \in F$ sont tels que $(x, y) \in f$ et $(x', y) \in f$, alors $x = x'$. Si $(x, y) \in f$, alors on appelle x l'antécédant de y, et y l'image de x. On note

$$\begin{aligned} f : E &\to F, \\ x &\mapsto y = f(x) \end{aligned}$$

pour dire que f est une fonction de E dans F, et que $f(x)$ est l'image de x.

Si f est une fonction de E dans F, alors nous appelons

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

le domaine de définition de f. C'est donc l'ensemble de tous les x qui possèdent une image.

Une *application* de E dans F est une fonction de E dans F donc le domaine de définition est E.

La fonction $f = \emptyset$ est appelée la *fonction vide*.

DÉFINITION 2.28 (Injection, surjection, bijection). Soient E et F deux ensembles. On dit qu'une fonction f de E dans F est
- *injective* si

$$\forall x, \, y \in E \, (f(x) = f(y) \to x = y),$$

- *surjective* si

$$\forall y \in F \, \exists x \in E \, (f(x) = y).$$

Une *injection* est une application injective. Une *surjection* est une application surjective. Une *bijection* est une application qui est injection et surjection.

EXEMPLE 2.29. Soit E un ensemble. L'*application identique* $1_E : E \to E$ définie par $1_E(x) = x$ est une bijection.

DÉFINITION 2.30 (Composition de fonctions). Soient E, F et G trois ensembles. Si $f : E \to F$ et $f : F \to G$ sont deux fonctions de domaine de définition respectifs $D(f)$ et $D(g)$, alors la *composée* $g \circ f$ est la fonction de E dans G définie par $g \circ f(x) = g(f(x))$, son domaine de définition étant l'ensemble $D(g \circ f) = \{x \in E : x \in D(f)$ et $f(x) \in D(g)\}$.

PROPOSITION 2.31. *La composée de deux applications (resp. injections, resp. surjections, resp. bijections) est une application (resp. injection, resp. surjection, resp. bijection).*

PROPOSITION 2.32. *Si f est une bijection de E dans F, alors il existe une unique bijection g de F dans E vérifiant $g \circ f = 1_E$ et $f \circ g = 1_F$.*

DÉFINITION 2.33 (Bijection réciproque). Soit f une bijection de E dans F. Alors l'unique bijection g de F dans E vérifiant $g \circ f = 1_E$ et $f \circ g = 1_F$ (Proposition 2.32) est appelée *bijection réciproque* et on note $g =: f^{-1}$.

DÉFINITION 2.34 (Images directes et réciproques). Soit $f : E \to F$ une fonction, et soient $A \subset E$, $B \subset F$. On pose

$$\begin{aligned} f(A) &= \{y \in F : \exists x \in A\,(f(x) = y)\} \text{ et} \\ f^{-1}(B) &= \{x \in E : \exists y \in B\,(y = f(x))\}, \end{aligned}$$

et on appelle $f(A)$ l'*image directe* de A, et $f^{-1}(B)$ l'*image réciproque* de B.

PROPOSITION 2.35. *Soient $f : E \to F$ une fonction et $A_i \subset E$, $B_i \subset F$ pour $i \in I$. Alors*
(i) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$,
(ii) $f(\bigcup_{i\in I} A_i) = \bigcup_{i\in I} f(A_i)$,
(iii) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$,
(iv) $f^{-1}(\bigcup_{i\in I} B_i) = \bigcup_{i\in I} f^{-1}(B_i)$,
(v) $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$,
(vi) $f^{-1}(\bigcap_{i\in I} B_i) = \bigcap_{i\in I} f^{-1}(B_i)$,
(vii) $f^{-1}(\complement_F B) = \complement_E f^{-1}(B)$.

EXERCICE 2.36. Donner un exemple qui montre qu'en général $f(A_1 \cap A_2) \neq f(A_1) \cap f(A_2)$. Est-ce qu'au moins une des inclusions $f(A_1 \cap A_2) \supset f(A_1) \cap f(A_2)$ ou $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$ est vraie?

EXERCICE 2.37. Si E et F sont deux ensembles, alors on note F^E pour l'ensemble des applications de E dans F.
(a) Montrer que si E contient n éléments, et si F contient m éléments, alors F^E contient m^n éléments.
(b) Trouver une bijection entre $\mathbb{R} \times \mathbb{R}$ -le produit cartésien - et $\mathbb{R}^2$ - l'ensemble de toutes les applications de 2 (vu comme un ensemble; voir le prochain chapitre) et $\mathbb{R}$.

7. Lois de composition

DÉFINITION 2.38. Une *loi interne* T sur E est une application $T : E \times E \to E$. On note xTy au lieu de $T(x, y)$ l'image de $(x, y) \in E \times E$.

Une *loi externe* sur E à domaine d'opérateurs dans K est une application $T : K \times E \to E$. On note $\lambda T x$ au lieu de $T(\lambda, x)$ l'image de $(\lambda, x) \in K \times E$.

EXEMPLES 2.39. (i) L'addition + et la multiplication $\cdot$ sont des lois internes dans $\mathbb{R}$ (resp. $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$).
(ii) Si E est un ensemble, alors la composition $\circ$ est une loi interne dans l'ensemble des applications de E dans E.
(iii) Si E est un ensemble, alors l'intersection $\cap$ et la différence symétrique $\triangle$ sont des lois internes dans $P(E)$ (l'ensemble des parties de E).

DÉFINITION 2.40. Soit E un ensemble. Une loi interne T sur E est dite
- *commutative* si $\forall x, y \in E$ on a $xTy = yTx$,
- *associative* si $\forall x, y, z \in E$ on a $(xTy)Tz = xT(yTz)$,
- *distributive* par rapport à une deuxième loi interne S si $\forall x, y, z \in E$ on a $xT(ySz) = (xTy)S(xTz)$ et $(xSy)Tz = (xTz)S(yTz)$.

La loi interne T admet un *élément neutre* $e \in E$ si $\forall x \in E$ on a $xTe = eTx = x$. Si T admet un élément neutre, alors un élément inverse de $x \in E$ est un élément $x' \in E$ tel que $xTx' = x'Tx = e$.

LEMME 2.41. *Soit E un ensemble, et soit T une loi interne sur E. Alors:*
(i) il existe au plus un élément neutre, et
(ii) si T admet un élément neutre et si T est associative, alors pour tout $x \in E$ il existe au plus un élément inverse.

DÉMONSTRATION. (i) Soient e et e' deux éléments neutres. Alors

$$e = eTe',$$

parce que e' est élément neutre, et

$$eTe' = e',$$

parce que e est élément neutre. Donc, $e = e'$, ce qui veut dire qu'il existe au plus un élément neutre.

(ii) Soit $e \in E$ l'élément neutre. Soit $x \in E$, et soient $x', x'' \in E$ deux éléments inverse. Alors, comme e est élément neutre, et comme x'' est élément inverse de x,

$$x' = x'Te = x'T(xTx'').$$

De la même manière,

$$x'' = eTx'' = (x'Tx)Tx''.$$

Comme T est associative, on obtient donc $x' = x''$, ce qui veut dire qu'il existe au plus un élément inverse. □

EXEMPLES 2.42. (i) L'addition + et la multiplication $\cdot$ dans $\mathbb{R}$ sont commutatives et associatives, et la multiplication est distributive par rapport à l'addition. L'élément 0 est un élément neutre pour l'addition, et 1 est un élément neutre pour la multiplication.
(ii) Si E est un ensemble, et si

$$\mathrm{Sym}(E) := \{f \in P(E \times E) : f \text{ est une bijection}\}$$

est l'ensemble de bijections de E dans E, alors la composition $\circ$ est une loi interne sur $\mathrm{Sym}(E)$ qui est associative, mais non commutative (exemple!). L'application identique 1_E est l'élément neutre, et si $f \in \mathrm{Sym}(E)$, alors la fonction réciproque f^{-1} est l'élément inverse.
(iii) L'intersection $\cap$ et la différence symétrique $\triangle$ dans $P(E)$ sont commutatives et associatives, et l'intersection est distributive par rapport à la différence symétrique. L'élement neutre pour l'intersection est l'ensemble E, l'élément neutre pour la

différence symétrique est l'ensemble vide $\emptyset$. Si A est une partie de E, alors son inverse par rapport à la différence symétrique est A. En général, il n'y a pas d'élément inverse pour l'intersection.

DÉFINITION 2.43 (Anneau). Un triplet $(A, +, \cdot)$ qui consiste d'un ensemble A et de deux lois internes $+$ et $\cdot$ sur A est appelé *anneau (unitaire)* si
(i) l'addition $+$ est commutative, associative, admet un élément neutre (noté 0), et tout élément $x \in A$ admet un élément inverse pour l'addition, et
(ii) la multiplication $\cdot$ est associative, distributive par rapport à l'addition, et admet un élément neutre (noté 1).
Si de plus, la multiplication $\cdot$ est commutative, alors on dit que $(A, +, \cdot)$ est un *anneau commutative*.

EXEMPLES 2.44. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ et $(P(E), \triangle, \cap)$ sont des anneaux commutatives.

CHAPITRE 3

Arithmétique

1. L'axiome de l'ensemble infini et définition de $\mathbb{N}$

Jusqu'ici, dans les exemples, on a déjà utilisé les ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, munis des lois internes qui sont l'addition et la multiplication, et munis de l'ordre $\leq$. On a supposé que ces ensembles sont connus.

Dans ce chapitre on va définir $\mathbb{N}$ (à partir d'un nouvel axiome) et ensuite construire $\mathbb{Z}$ à partir de $\mathbb{N}$. Ce sera un exercice de construire $\mathbb{Q}$ à partir de $\mathbb{Z}$. On ne va pas décrire une construction de $\mathbb{R}$ ici.

Afin de pouvoir définir $\mathbb{N}$ on a besoin de l'axiome suivant qui garantit l'existence d'un ensemble infini, et bien un peu plus. L'axiome suivant est donc une extension de l'axiome de l'existence d'un ensemble (Axiome 3).

Axiome 6 (Existence d'un ensemble récursif). Il existe un ensemble *récursif E* avec les propriétés suivantes:
(i) $\emptyset \in E$ et
(ii) si $x \in E$, alors $x \cup \{x\} \in E$.

Définition 3.1 (de $\mathbb{N}$). Soit E un ensemble récursif (Axiome 6). On définit

$$\mathbb{N} := \bigcap \{F \in P(E) : F \text{ est récursif}\}$$

comme l'intersection de tous les sous-ensembles récursifs de E.

Par définition, l'ensemble $\mathbb{N}$ est le plus petit ensemble récursif. L'ensemble $\mathbb{N}$ contient exactement les éléments

$$\begin{aligned} \emptyset, & \\ \{\emptyset\} &= \emptyset \cup \{\emptyset\}, \\ \{\emptyset, \{\emptyset\}\} &= \{\emptyset\} \cup \{\{\emptyset\}\}, \\ \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} &= \{\emptyset, \{\emptyset\}\} \cup \{\{\emptyset, \{\emptyset\}\}\}, \\ \vdots & \end{aligned}$$

Afin d'alléger la notation, on définit

$$\begin{aligned} 0 &:= \emptyset, \\ 1 &:= \{\emptyset\} = \{0\}, \\ 2 &:= \{\emptyset, \{\emptyset\}\} = 1 \cup \{1\} = \{0, 1\}, \\ 3 &:= 2 \cup \{2\} = \{0, 1, 2\}, \\ 4 &:= 3 \cup \{3\} = \{0, 1, 2, 3\}, \\ 5 &:= 4 \cup \{4\} = \{0, 1, 2, 3, 4\}, \\ &\vdots \end{aligned}$$

et alors $\mathbb{N}$ est l'ensemble qui contient exactement les éléments 0, 1, 2, 3, 4, 5, ... L'existence de l'ensemble $\mathbb{N}$ est maintenant garantit par l'Axiome 6.

On remarque qu'avec la définition ci-dessus les *nombres* 0, 1, 2, 3, 4, 5, ... sont des ensembles! Par exemple, le nombre 4 est l'ensemble qui contient les quatre éléments 0, 1, 2 et 3. Avec ce point de vue, il est naturel de définir l'ordre suivant sur $\mathbb{N}$.

PROPOSITION 3.2 (Ordre sur $\mathbb{N}$). *Pour tout $n, m \in \mathbb{N}$ on définit*

$$n \leq m \quad :\Leftrightarrow \quad n \subset m.$$

Alors $\leq$ est une relation d'ordre dans $\mathbb{N}$.

PROPOSITION 3.3 (Addition sur $\mathbb{N}$). *On définit l'addition $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ comme suivant: on définit premièrement*

$$\begin{aligned} n + 0 &:= n \quad et \\ n + 1 &:= n \cup \{n\}, \end{aligned}$$

et si $n + m$ est déja définit, alors

$$n + (m + 1) := (n + m) + 1.$$

Alors l'addition $+$ est une loi interne sur $\mathbb{N}$ qui est commutative, associative, et qui admet 0 comme élément neutre.

PROPOSITION 3.4 (Multiplication sur $\mathbb{N}$). *On définit la multiplication $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ comme suivant: on définit premièrement*

$$\begin{aligned} n \cdot 0 &:= 0 \quad et \\ n \cdot 1 &:= n, \end{aligned}$$

et si $n \cdot m$ est déja définit, alors

$$n \cdot (m + 1) := (n \cdot m) + n.$$

Alors la multiplication $\cdot$ est une loi interne sur $\mathbb{N}$ qui est commutative, associative, distributive par rapport à l'addition, et qui admet 1 comme élément neutre.

2. Construction de $\mathbb{Z}$

En supposant que $(\mathbb{N}, +, \cdot, \leq)$ est construit, on va maintenant construire $\mathbb{Z}$ à l'aide d'une relation d'équivalence.

PROPOSITION 3.5. *Pour tout* $(a, b), (c, d) \in \mathbb{N}^2$ *on pose*

$$\begin{aligned}(a, b) + (c, d) &:= (a + c, b + d) \text{ et}\\ (a, b) \cdot (c, d) &:= (ac + bd, ad + bc),\end{aligned}$$

et on définit une relation $\sim$ *par*

$$(a, b) \sim (c, d) \quad :\Leftrightarrow \quad a + d = b + c.$$

Alors $+$ *et* $\cdot$ *sont des lois internes sur* $\mathbb{N}^2$*, et* $\sim$ *est une relation d'équivalence dans* $\mathbb{N}^2$*. En plus, pour tout* $(a, b), (c, d), (a', b'), (c', d') \in \mathbb{N}^2$ *on a*

$$\begin{aligned}&(a, b) \sim (a', b') \text{ et } (c, d) \sim (c', d') \quad \Rightarrow\\ &\quad \Rightarrow \quad \overline{(a, b) + (c, d)} = \overline{(a', b') + (c', d')} \text{ et } \overline{(a, b) \cdot (c, d)} = \overline{(a', b') \cdot (c', d')}.\end{aligned}$$

DÉFINITION 3.6 (de $\mathbb{Z}$). On pose

$$\mathbb{Z} := \mathbb{N}/\sim,$$

et on appelle $\mathbb{Z}$ l'*ensemble des entiers relatifs*. Sur $\mathbb{Z}$, on définit l'addition $+$ et la multiplication $\cdot$ par

$$\begin{aligned}\overline{(a, b)} + \overline{(c, d)} &:= \overline{(a, b) + (c, d)} \text{ et}\\ \overline{(a, b)} \cdot \overline{(c, d)} &:= \overline{(a, b) \cdot (c, d)}.\end{aligned}$$

REMARQUES 3.7. (a) On remarque premièrement que pour tout élément $\overline{(a, b)}$ dans $\mathbb{Z}$ il existe un $n \in \mathbb{N}$ tel que

$$\overline{(a, b)} = \overline{(n, 0)} \quad \text{ou} \quad \overline{(a, b)} = \overline{(0, n)}.$$

Afin de voir cela, il suffit de démontrer que pour tout $(a, b) \in \mathbb{N}^2$ il existe un $n \in \mathbb{N}$ tel que

$$a = b + n \quad \text{ou} \quad a + n = b.$$

En conséquent, tous les éléments de $\mathbb{Z}$ s'ecrivent de la forme $\overline{(n, 0)}$ ou $\overline{(0, n)}$ pour un $n \in \mathbb{N}$.
(b) On remarque deuxièmement que pour tout $(a, b) \in \mathbb{N}^2$ on a

$$\overline{(a, b)} + \overline{(b, a)} = \overline{(b, a)} + \overline{(a, b)} = \overline{(a + b, a + b)},$$

et que $\overline{(a + b, a + b)} = \overline{(0, 0)}$ est l'élément neutre pour l'addition. En particulier, tout élément de $\mathbb{Z}$ admet un élément inverse pour l'addition.

PROPOSITION 3.8. *Soient* $\mathbb{Z}$*, l'addition* $+$ *et la multiplication* $\cdot$ *sur* $\mathbb{Z}$ *comme ci-dessus. Alors* $(\mathbb{Z}, +, \cdot)$ *est un anneau.*

PROPOSITION 3.9. *L'application*

$$\begin{aligned} i : \mathbb{N} &\to \mathbb{Z}, \\ n &\mapsto \overline{(n, 0)}, \end{aligned}$$

est injective. En plus, pour tout $n, m \in \mathbb{N}$ on a

$$\begin{aligned} i(n+m) &= i(n) + i(m) \quad \textit{et} \\ i(n \cdot m) &= i(n) \cdot i(m). \end{aligned}$$

Si on identifie $\mathbb{N}$ avec son image direct $i(\mathbb{N})$, alors on peut dire que $\mathbb{N}$ est un sous-ensemble de $\mathbb{Z}$, et l'addition et la multiplication dans $\mathbb{N}$ coincide (sous cette indentification) avec l'addition et la multiplication dans $\mathbb{Z}$.

Dans la suite, on va identifier $\mathbb{N}$ avec son image direct $i(\mathbb{N})$. En plus, on note les éléments de $\mathbb{Z}$ simplement $n, m, k, \ldots$. Si $n \in \mathbb{Z}$, alors on note $-n$ l'élément inverse pour l'addition. On écrit $n - m$ au lieu de $n + (-m)$.

D'après la Remarque 3.7 (a), pour tout $n \in \mathbb{Z}$ on a

$$n \in \mathbb{N} \quad \text{ou} \quad -n \in \mathbb{N}.$$

PROPOSITION 3.10. *On définit, pour tout $n, m \in \mathbb{Z}$,*

$$n \leq m \quad :\Leftrightarrow \quad m - n \in \mathbb{N}.$$

Alors $\leq$ est une relation d'ordre sur $\mathbb{Z}$ qui, quand on la restreint sur $\mathbb{N}$, coincide avec la relation d'ordre sur $\mathbb{N}$.

3. L'algorithme d'Euclide

DÉFINITION 3.11. Pour tout $n \in \mathbb{Z}$ on définit la *valeur absolue* $|n|$ par $|n| := \sup\{n, -n\}$.

PROPOSITION 3.12. *Pour tout $n, m \in \mathbb{Z}$ on a*

$$\begin{aligned} |n| = 0 &\Leftrightarrow n = 0, \\ |n+m| &\leq |n| + |m| \quad \textit{et} \\ |n \cdot m| &= |n| \cdot |m|. \end{aligned}$$

PROPOSITION 3.13 (Division avec reste). *Pour tout $n, m \in \mathbb{Z}$, $m \neq 0$, il existe des éléments unique $q, r \in \mathbb{Z}$ tel que*

$$n = q \cdot m + r \quad \textit{et} \quad 0 \leq r < |m|.$$

DÉMONSTRATION. Unicité: Supposons qu'il y a deux solutions pour la division avec reste, c.à.d. supposons que $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ sont tels que

$$\begin{aligned} n &= q_1 \cdot m + r_1 \quad \text{et} \quad 0 \leq r_1 < |m| \quad \text{et} \\ n &= q_2 \cdot m + r_2 \quad \text{et} \quad 0 \leq r_2 < |m|. \end{aligned}$$

Alors

$$m \cdot (q_2 - q_1) = r_1 - r_2$$

ce qui implique

$$|m| \cdot |q_2 - q_1| = |r_1 - r_2|.$$

Ainsi, on trouve que $|r_1 - r_2| \geq 0$ est un multiple de $|m|$. Avec la condition $0 \leq r_1$, $r_2 < |m|$, ce n'est possible que si $|r_1 - r_2| = 0$ ce qui implique d'un côté $r_1 = r_2$ et d'autre côté $|m| \cdot |q_2 - q_1| = 0$. Comme $m \neq 0$, on trouve alors nécessairement $q_1 = q_2$. On a donc démontré unicité.

Existence: On suppose que $m > 0$; le cas $m < 0$ se démontre d'uns façon similaire. Si $m > 0$, alors il existe un $q \in \mathbb{Z}$ tel que

$$q \cdot m \leq n < (q+1) \cdot m. \tag{3.1}$$

En fait, l'ensemble $A = \{q' \in \mathbb{Z} : q \cdot m \leq n\}$ est borné supérieurement. En plus, dans $\mathbb{Z}$, toute partie non-vide majorée admet une borne supérieure. Si on pose $q = \sup A$, alors on trouve (3.1). Après avoir établit (3.1), il suffit de poser $r = n - q \cdot m$. □

Exemples 3.14.

$$\begin{aligned} &n = 20, \quad m = 7, \quad && 20 = 7 \cdot 2 + 6; \\ &n = 20, \quad m = -7, \quad && 20 = (-7) \cdot (-2) + 6; \\ &n = -20, \quad m = 7, \quad && -20 = 7 \cdot (-3) + 1; \\ &n = -20, \quad m = -7, \quad && -20 = (-7) \cdot 3 + 1. \end{aligned}$$

Définition 3.15. Soient $a, b \in \mathbb{Z}$, $a \neq 0$.
(i) On dit que *a divise b* s'il existe $q \in \mathbb{Z}$ tel que $aq = b$.
(ii) On dit que a est *premier* si les seuls diviseurs de a sont a, $-a$, 1 et -1.
(iii) Le *plus grand commun diviseur* de a et b (noté $a \wedge b$ ou $\operatorname{pgcd}(a, b)$) est le plus grand des diviseurs communs à a et à b. (iv) On dit que *a est premier avec b* si $a \wedge b = 1$.

Théorème 3.16 (Algorithme d'Euclide). *Soient $a, b \in \mathbb{Z}$, $a \neq 0$. On pose*

$$\begin{aligned} r_{-1} &:= a \quad \textit{et} \\ r_0 &:= b. \end{aligned}$$

Si r_{j-1} et r_j sont donnés, et si $r_j \neq 0$, alors il existe des uniques éléments q_j, $r_{j+1} \in \mathbb{Z}$ tels que

$$r_{j-1} = r_j q_j + r_{j+1} \quad \textit{et} \quad 0 \leq r_{j+1} < |r_j|; \tag{3.2}$$

(division avec reste). Alors il existe un $n \in \mathbb{N} \cup \{-1\}$ tel que $r_{n+1} = 0$ et $r_n \neq 0$. Pour ce dernier reste non nul on a $r_n = a \wedge b$.

Démonstration. Si $n = -1$, c.á.d. si a est le dernier reste non nul et $b = 0$, alors $a = a \wedge b$, et il n'y a plus rien a démontrer. Si $n = 0$, c.à.d. si b est le dernier reste non nul (b est un diviseur de a), alors $b = a \wedge b$, et il n'y a plus rien à démontrer non plus. Donc, on suppose que $n \geq 1$.

On montre premièrement que

$$\forall\, 0 \leq j \leq n-1 : \; r_{j-1} \wedge r_j = r_j \wedge r_{j+1}. \tag{3.3}$$

Plus particulièrement, on montre la proposition plus forte:

$$\forall\, 0 \le j \le n-1\ \forall d \ge 1: \qquad \begin{array}{l} d \text{ est diviseur commun de } r_{j-1} \text{ et } r_j \text{ si et} \\ \text{seulement si } d \text{ est diviseur commun de } r_{j-1} \text{ et } r_j. \end{array}$$

Il est clair que cette proposition implique (3.3).

Soit d un diviseur commun de r_{j-1} et r_j. Alors il existe des nombres $k, l \in \mathbb{Z}$ tel que $r_{j-1} = d\,k$ et $r_j = d\,l$. Par l'algorithme (3.2),

$$\begin{aligned} r_{j+1} &= r_{j-1} - q_j r_j \\ &= d\,(k - q_j\,l), \end{aligned}$$

et donc d est diviseur de r_{j+1}. Comme d est toujours diviseur de r_j, alors d est diviseur commun de r_j et r_{j+1}.

Si d est diviseur commun de r_j et r_{j+1} alors on démontre de la même façon que d est diviseur commun de r_{j-1} et r_j.

On obtient donc la propriété (3.3).

De cette propriété on obtient

$$a \wedge b = r_0 \wedge r_1 = \cdots = r_{n-1} \wedge r_n.$$

Mais d'après l'algorithme (3.2),

$$r_{n-1} = r_n q_n + r_{n+1} = r_n q_n,$$

parce que $r_{n+1} = 0$, et donc r_n est diviseur de r_{n-1}. Ceci implique $r_{n-1} \wedge r_n = r_n$, et le théorème est démontré. □

Dans la suite, si $a \in \mathbb{Z}$, alors

$$a\mathbb{Z} = \{an : n \in \mathbb{Z}\}.$$

Proposition 3.17 (Relation de Bezout). *Soient $a, b \in \mathbb{Z}$, $a \neq 0$. Alors*

$$a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}. \tag{3.4}$$

Démonstration. L'inclusion

$$a\mathbb{Z} + b\mathbb{Z} \subset (a \wedge b)\mathbb{Z}$$

est facile.

Afin de démontrer l'autre inclusion

$$a\mathbb{Z} + b\mathbb{Z} \supset (a \wedge b)\mathbb{Z},$$

il suffit de démontrer que $a \wedge b \in (a\mathbb{Z} + b\mathbb{Z})$ ce qui veut dire que

$$\exists x, y \in \mathbb{Z}: \quad ax + by = a \wedge b. \tag{3.5}$$

On reprend l'agorithme d'Euclide (3.2) et on montre que

$$\forall\, j = -1, \ldots, n\ \exists x_j, y_j \in \mathbb{Z}: \quad ax_j + by_j = r_j. \tag{3.6}$$

Cette relation est certainment vérifiée pour $n = 0$. En fait $r_{-1} = a = a \cdot 1 + b \cdot 0$ et $r_0 = b = a \cdot 0 + b \cdot 1$. Si $n = 0$, alors (3.6) est déjà démontré. Sinon, supposons qu'il existe k tel que $0 \leq k \leq n - 1$ et tel que

$$\forall j = -1, \ldots, k \, \exists x_j, y_j \in \mathbb{Z} : \quad ax + by = r_j.$$

D'après l'algorithme (3.2),

$$r_{k-1} = r_k q_k + r_{k+1}$$

ou

$$\begin{aligned} r_{k+1} &= (ax_k + by_k)q_k - (ax_{k-1} + by_{k-1}) \\ &= a\,(x_k q_k - x_{k-1}) + b\,(y_k q_k - y_{k-1}). \end{aligned}$$

Ceci implique, par récurrence que (3.6) est vrai. En particulier,

$$a \wedge b = r_n = ax_n + by_n,$$

ce qui termine la démonstration. □

REMARQUE 3.18. Si $a, b \in \mathbb{Z}$ sont premiers entre eux, alors il existe $n, m \in \mathbb{Z}$ tel que

$$an + bm = 1;$$

voir (3.5) ci-dessus. Ceci est une autre formulation de la relation de Bezout.

PROPOSITION 3.19. *Soit $n \in \mathbb{N}$, $n \neq 0$. Pour tout $a, b \in \mathbb{Z}$ on définit*

$$a \sim b \quad :\Leftrightarrow \quad \exists q \in \mathbb{Z} \, : \, a - b = q \cdot n.$$

Alors $\sim$ est une relation d'équivalence sur $\mathbb{Z}$.

Si $n \in \mathbb{N}$, $n \neq 0$, et si $\sim$ est la relation d'équivalence de la proposition précédente, alors on note $\mathbb{Z}/n\mathbb{Z}$ pour l'ensemble $\mathbb{Z}/\sim$ des classes d'équivalences. Notons que deux éléments $a, b \in \mathbb{Z}$ sont dans la même classe d'équivalence si la division de $a - b$ par n donne le reste 0. D'une manière équivalente, deux éléments $a, b \in \mathbb{Z}$ sont dans la même classe d'équivalence si la division de a resp. b par n donne le même reste. On a

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\},$$

et on vérifie que l'addition et la multiplication données par

$$\begin{aligned} \overline{a} + \overline{b} &:= \overline{a + b} \quad \text{et} \\ \overline{a} \cdot \overline{b} &:= \overline{a \cdot b} \end{aligned}$$

sont bien définis dans $\mathbb{Z}/n\mathbb{Z}$.

PROPOSITION 3.20. $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ *est un anneau commutatif.*

4. L'anneau des polynômes

CHAPITRE 4

L’axiome du choix

Bibliographie

1. H. Brézis, *Analyse fonctionnelle*, Masson, Paris, 1992.
2. L. C. Evans, *Partial Differential Equations*, Graduate Studies in Mathematics, vol. 19, American Mathematical Society, Providence, RI, 1998.
3. D. Gilbarg and N. S. Trudinger, *Elliptic Partial Differential Equations of Second Order*, Springer Verlag, Berlin, Heidelberg, New York, 2001.
4. F. John, *Partial Differential Equations. Fourth Edition*, Applied Mathematical Sciences, vol. 1, Springer Verlag, New York, Heidelberg, Berlin, 1982.
5. J.-L. Lions, *Quelques méthodes de résolution des problèmes aux limites non linéaires*, Dunod, Gauthier-Villars, Paris, 1969.
6. J.-E. Rakotoson and J.-M. Rakotoson, *Analyse fonctionnelle appliquée aux équations aux dérivées partielles*, Presse universitaire de France, Paris, 1999.
7. H. Reinhard, *Equations aux dérivées partielles. Introduction*, Dunod, Paris, 2001.