

Structures algébriques
(notes pour le cours d'automne de 2020, BA 1, EPFL)

Zsolt Patakfalvi

(avec l'aide de Quentin Posva)

September 21, 2020

Contents

1	Preuves et ensembles	5
1.1	Preuves	5
1.2	Ensembles	7
1.2.1	Axiomes de théorie des ensembles	7
1.2.2	Applications entres ensembles	9
1.2.3	Relations d'équivalence	11
1.2.4	Cardinal d'un ensemble	12
2	Théorie des nombres	15
2.1	Algorithme d'Euclide	15
2.2	Théorème fondamental de l'arithmétique	16
3	Théorie des groupes	19

Chapter 1

Preuves et ensembles

1.1 PREUVES

Une preuve est un argumentaire où chaque ligne est une conséquence logique des lignes précédentes. Grâce au langage de la logique mathématique, il existe une définition stricte d'une preuve mathématique. D'après cette définition, on ne peut utiliser que des signes mathématiques, comme :

- (1) il existe : \exists ,
- (2) il existe un unique : $\exists!$,
- (3) pour chaque : \forall ,
- (4) et : \wedge ,
- (5) ou : \vee ,
- (6) non : \neg ,
- (7) cela implique : \implies ,
- (8) et les autres signes que l'on aura définis.
- (9) etc.

Selon la logique mathématique, il faut démontrer toutes nos propositions en partant d'axiomes, et chaque ligne d'une preuve doit être l'une des suivantes :

- (1) un axiome,
- (2) une proposition déjà démontrée,
- (3) une tautologie, comme par exemple $\neg(A \vee B) \Leftrightarrow ((\neg A) \wedge (\neg B))$ (pour démontrer que c'est une tautologie, on peut vérifier que tous les deux côtés sont vrais si et seulement si A et B sont tous les deux faux).
- (4) moduls ponens: s'il y a une ligne précédente de la forme $A \implies B$, et une autre de la forme A , alors on peut écrire B .
- (5) etc

On appelle les preuve écrite de cette manière les *preuves formelles*. Écrire une preuve formelle est utile pour la vérifier avec un ordinateur. Mais il est quasiment impossible de la lire pour un lecteur humain. En pratique, on essaie d'approximer les preuves formelle par un mélange de

texte et de symboles mathématique. Quand on écrit une preuve, il faut trouver un compromis qui est lisible, et qui contient tous les pas importants de l'argumentaire. Il faut être strict : *tous les pas importants doivent figurer dans la preuve*. Quand on écrit une preuve, il faut se demander après chaque ligne : est-ce logiquement correct ? Il n'est pas possible de donner un algorithme pour l'écriture de preuves, seule la pratique permet de l'apprendre. On pourrait dire que c'est le but principal pour lequel vous êtes ici, et nous verrons beaucoup d'exemples pendant le semestre. Dans tous les cas, si vous n'êtes pas certain de la manière d'écrire une preuve, je suggère que vous vous exerciez beaucoup et que vous discutiez souvent avec les assistants.

Considérons ensemble un exemple de preuve. Elle suit un schéma logique fréquent : l'induction. L'idée de l'induction est que pour montrer une proposition pour chaque entier n , il suffit de le montrer pour $n = 0$, puis pour chaque $n > 0$ en supposant que la proposition est établie pour $n - 1$. Avant de donner cet exemple, nous avons besoin de définitions.

Définition 1.1.1. Un nombre entier a est *positif* si $a > 0$, et *non-négatif* si $a \geq 0$. En particulier 0 n'est ni positif ni négatif. (Nous suivons ici la terminologie usuelle aujourd'hui dans la pratique internationale de la mathématique.)

Définition 1.1.2. Soient a et q deux entiers. On dit que $q \neq 0$ *divise* a , ce que l'on dénote $q|a$, s'il existe un entier r tel que $a = rq$.

Proposition 1.1.3. (DIVISION AVEC RESTE) Soient q un entier positif, et a un entier non-négatif. Alors il existe deux uniques entiers non-négatifs b et r tels que $r < q$ et

$$a = bq + r. \quad (1.3.a)$$

Preuve. Supposons d'abord que b et r existent. On démontre qu'ils sont unique. Supposons que b, r, b' and r' soient des entiers non-négatifs tels que $r, r' < q$, $a = bq + r$ et $a = b'q + r'$. Alors,

$$bq + r = b'q + r' \implies \underbrace{r - r'}_{\substack{\uparrow \\ 0 \leq r, r' < q \implies -q < r - r' < q}} = \underbrace{q(b' - b)}_{\substack{\uparrow \\ \text{les possibilités sont} \\ \dots, -2q, -q, 0, q, 2q, \dots, \\ \text{parce que } b' - b \text{ est entier}}} \implies r - r' = 0 \implies r = r' \implies bq = b'q \xRightarrow{\substack{\uparrow \\ q > 0}} b = b'$$

Ceci démontre que b et r sont uniques, s'ils existent. Pour conclure la preuve, il faut encore démontrer que b et r existent. On le démontre par induction sur a .

Le plus petit entier non-négatif est 0. Commençons alors avec le cas $a = 0$. Dans ce cas, on peut choisir $b = r = 0$.

Il nous reste donc à démontrer le pas d'induction. Supposons démontrée l'existence si l'on remplace a par $a - 1$. On a ainsi $a - 1 = cq + s$, où c et s sont des entiers non-négatifs, et $s < q$. Il y a alors deux cas:

- (1) Si $s < q - 1$, on peut choisir $b = c$ et $r = s + 1 < q$, et dans ce cas on a

$$a = 1 + (a - 1) = 1 + cq + s = bq + r.$$

- (2) Si $s = q - 1$, on peut choisir $b = c + 1$ et $r = 0 < q$, et dans ce cas on a

$$a = 1 + (a - 1) = 1 + cq + s = 1 + cq + (q - 1) = q + cq = q(c + 1) = qb + 0 = qb + r.$$

Ceci conclut notre preuve. □

Exemple 1.1.4. Si $a = 13$, $q = 3$, alors $b = 4$ et $r = 1$, parce que $13 = 4 \cdot 3 + 1$.

1.2 ENSEMBLES

1.2.1 Axiomes de théorie des ensembles

La situation avec les ensembles est similaire à celle des preuves. Il y a une définition et une manière extrêmement précises de les manipuler, qui est lisible pour un ordinateur. Mais pour que nous soyons capables de travailler avec les ensembles, il faut l'assouplir un peu. La raison est que tout ce que vous allez rencontrer durant cette année, et qui semble être un ensemble, est presque sûrement un ensemble. Mais il est bien de se rappeler que notre intuition peut être trompeuse dans quelques cas délicats.

Intuitivement, un *ensemble* est une collection des "choses", et une sous-collection de "choses" est un *sous-ensemble*. Le problème avec cette définition est qu'elle nous mène au paradoxe de Russell.

Paradoxe de Russel. *La collection:*

$$B := \{ A \text{ est un ensemble} \mid A \text{ n'est pas un élément de } A \}$$

ne peut pas être pas un ensemble.

Preuve. La définition de B dit que B est contenu dans B si et seulement si B n'est pas contenu dans B . Avec les symboles :

$$B \in B \iff B \notin B.$$

C'est un paradoxe. □

Remarque 1.2.1.

On peut voir que l'origine de ce paradoxe est qu'on a considéré une collection de "choses" très spéciale. Donc il ne faut pas s'inquiéter, il n'y a pas de problèmes quand on travaille avec des ensembles raisonnables. Dans ce cours, on va travailler la plupart du temps avec des ensembles construits à partir de l'ensemble des entiers, et dans cette situation aucun problème ne peut survenir. Mentionnons quand même comment le paradoxe de Russel fut résolu vers la fin du XIX^e siècle.

Un système d'axiomes fut établi, appelé le système d'axiomes de Zermelo-Fraenkel. Ce système définit ce qui est un ensemble de manière précise ; en particulier la collection considérée dans le paradoxe de Russell n'est pas un ensemble. On donne en-dessous une approximation de ce système d'axiomes. (Il s'agit de culture générale, vous n'avez pas besoin de le retenir) :

- (0) A est égal à B si et seulement si ils ont les mêmes éléments.
- (1) Il existe un ensemble.
- (2) (Axiome du sous-ensemble) Si A est un ensemble, est $E(x)$ est une expression logique applicable aux éléments x de A , alors

$$\{ x \in A \mid E(x) \text{ est vrai} \}$$

est aussi un ensemble.

- (3) (Axiome de l'union) L'union d'ensembles, indicé par un ensemble, est aussi un ensemble. Avec des symboles : si A_i sont des ensembles pour chaque $i \in I$, où I est lui-même un ensemble, alors

$$\bigcup_{i \in I} A_i$$

est aussi un ensemble.

- (4) (Axiome de la paire) Si A et B sont des ensembles, $\{A, B\}$ est aussi un ensemble.
- (5) (Axiome de l'ensemble puissance) Si A est un ensemble, l'ensemble 2^A des tous les sous-ensembles de A est aussi un ensemble.
- (6) (Axiome du choix) Intuitivement: si A_i sont ensembles (pour $i \in I$), alors on peut choisir $a_i \in A_i$ pour chaque $i \in I$.
- (7) etc.

Il n'est pas nécessaire de mémoriser les axiomes au-dessus, mais il est utile de les comprendre, afin de

- connaître les opérations les plus basiques permettant de définir un ensemble (en commençant avec les autres ensembles), et pour
- savoir qu'il y a un système d'axiomes.

Par exemple, en utilisant le système des axiomes de Zermelo-Fraenkel, on peut déduire (mais on ne va pas le faire pas dans ce cours) que les collections suivantes sont des ensembles:

- (1) les ensembles finis:

- (i) l'ensemble vide: \emptyset
- (ii) l'ensemble à un élément: $\{1\}$
- (iii) l'ensemble à deux éléments: $\{1, 2\}$
- (iv) etc.

- (2) l'ensemble des entiers naturels:

$$\mathbb{N} := \{0, 1, 2, \dots\}$$

- (3) l'ensemble des entiers:

$$\mathbb{Z} := \{\dots, -2, -1, 0, 1, 2, \dots\}$$

- (4) etc.

Condition (2) du système de Zermelo-Fraenke dit que l'on peut couper des sous-ensembles avec des conditions logiques. Par exemple :

- (5) les entiers positifs forment un ensemble:

$$\mathbb{Z}^{>0} := \{x \in \mathbb{Z} \mid x > 0\}.$$

- (6) les entiers naturels pairs forment un ensemble:

$$\{x \in \mathbb{N} \mid x \text{ est pair} \}.$$

- (7) Plus généralement, on peut former des compléments: soit $A \subseteq B$ un sous-ensemble (ce qui signifie que chaque élément de A est aussi un élément de B , ou avec formules $a \in A \implies a \in B$). Dans ce cas on peut prendre la différence des deux ensembles, aussi appelée le complément de A dans B , définit par

$$B \setminus A = \{ b \in B \mid \underset{\uparrow}{b \neg \in A} \} = \{ b \in B \mid \underset{\uparrow}{b \notin A} \}$$

notation en logique mathématique

notation plus commune en mathématique

- (8) Une application similaire consiste à former des intersections. Plus précisément, si A et B sont des sous-ensembles de C , alors l'intersection $A \cap B$ est définie par l'équation suivante, qui nous montre qu'il s'agit aussi un sous-ensemble de C :

$$A \cap B = \{ c \in C \mid c \in A \wedge c \in B \} = \{ c \in C \mid c \in A, \text{ et } c \in B \}$$

notation en logique mathématique

notation plus commune en mathématique

Contrairement aux unions, on ne peut pas prendre l'intersection d'ensembles pris au hasard, mais seulement de sous-ensembles d'un ensemble ambiant fixé.

(9) etc.

1.2.2 Applications entres ensembles

On peut également déduire du système de Zermelo-Fraenkel (mais on ne va pas le faire pas dans ce cours) que pratiquement toutes les opérations mathématiques produisent des ensembles, entendu que l'on commence avec des ensembles. Un exemple est le produit d'ensembles:

Définition 1.2.2. Soient A et B des ensembles, l'ensemble produit $A \times B$ est l'ensemble des paires (a, b) avec $a \in A$ et $b \in B$:

$$A \times B = \{ (a, b) \mid a \in A, b \in B \}.$$

Etant donnée une paire (a, b) , on appelle a la première coordonnée et b la seconde.

Exemple 1.2.3. Soient $A = \{1, 2\}$ et $B = \{5, 6\}$. Dans ce cas on a

$$A \times B = \{(1, 5), (1, 6), (2, 5), (2, 6)\}.$$

Remarque 1.2.4. Soient A , B et C des ensembles. On a un isomorphisme naturel

$$(A \times B) \times C \cong A \times (B \times C)$$

$$((a, b), c) \leftrightarrow (a, (b, c))$$

On identifie les deux ensembles grâce à cet isomorphisme, et on les écrira simplement $A \times B \times C$.

Définition 1.2.5. Soient A et B des ensembles. Une application $\phi : A \rightarrow B$ est un sous-ensemble (appelé le graphe de ϕ)

$$\Gamma_\phi \subseteq A \times B$$

tel que:

$$\forall a \in A, \exists ! b \in B \text{ tel que } (a, b) \in \Gamma_\phi$$

i.e. l'ensemble des paires contenues dans Γ_ϕ dont la première coordonnée est a , est réduit à un seul élément. On note la deuxième coordonnée de cette paire $\phi(a)$, et on l'appelle l'image de a par ϕ .

On appelle A le domaine, et B le codomaine de ϕ .

Exemple 1.2.6. Soit A, B des ensembles. Voici quelques exemples d'applications entre A et B :

- (1) $\text{id}_A : A \rightarrow A$ est définie par

$$\forall a \in A : \text{id}_A(a) = a$$

$$\Updownarrow$$

$$\Gamma_{\text{id}_A} = \{ (a, a) \in A \times A \mid a \in A \}$$

(2) $\text{pr}_A : A \times B \rightarrow A$ est définie par

$$\forall (a, b) \in A \times B : \text{pr}_A((a, b)) = a$$

$$\Updownarrow$$

$$\Gamma_{\text{pr}_A} = \{ (a, b, a) \in A \times B \times A \mid a \in A, b \in B \}$$

Définition 1.2.7. Soit $\phi : A \rightarrow B$ une application entre ensembles. On dit que

(1) ϕ est *injective*, si

$$\phi(a) = \phi(a') \Rightarrow a = a'$$

(2) ϕ est *surjective*, si

$$\forall b \in B, \exists a \in A : \phi(a) = b$$

(3) ϕ est *bijjective*, si elle est injective et surjective.

(4) l'image de ϕ est

$$\phi(A) = \{ \phi(a) \in B \mid a \in A \}$$

Quelquefois une application injective est appelée une *injection*, une application surjective est appelée une *surjection*, et une application bijective est appelée une *bijection*.

Définition 1.2.8. Soient $\phi : A \rightarrow B$ et $\xi : B \rightarrow C$ les applications entre ensembles. La composition $\xi \circ \phi$ est l'application

$$(\xi \circ \phi)(a) = \xi(\phi(a))$$

$$\Updownarrow$$

$$\Gamma_{\xi \circ \phi} = \{ (a, c) \mid \exists b \in B : (a, b) \in \Gamma_\phi \text{ et } (b, c) \in \Gamma_\xi \}$$

Proposition 1.2.9. Soient $\phi : A \rightarrow B$ et $\xi : B \rightarrow C$ les applications entre ensembles, et supposons que $\xi \circ \phi$ est surjective. Alors,

(1) ξ est aussi surjective, mais

(2) ϕ n'est pas nécessairement surjective.

Preuve. (1) Fixons $c \in C$. Il faut montrer qu'il existe au moins un $b \in B$ tel que $\xi(b) = c$. On a supposé que $\xi \circ \phi$ est surjective : il existe donc un $a \in A$ tel que $\xi(\phi(a)) = c$, et donc on peut choisir $b = \phi(a)$.

(2) Voici un contre-exemple :

$$A = \{1\}, \quad B = \{1, 2\} \quad C = \{1\},$$

$$\phi(1) = 1, \quad \xi(1) = 1, \quad \xi(2) = 1.$$

□

Définition 1.2.10. Soit $\phi : A \rightarrow B$ une bijection entre ensembles. L'inverse ϕ^{-1} de ϕ est l'application $\phi^{-1} : B \rightarrow A$ définie par

$$\phi^{-1}(b) = a \iff \phi(a) = b.$$

$$\Updownarrow$$

$$(b, a) \in \Gamma_{\phi^{-1}} \iff (a, b) \in \Gamma_\phi.$$

Exemple 1.2.11. Soit $\phi : \{1, 2\} \rightarrow \{5, 6\}$ la bijection définie par $\phi(1) = 6$ et $\phi(2) = 5$. Dans ce cas $\phi^{-1} : \{5, 6\} \rightarrow \{1, 2\}$ est l'application pour laquelle on a $\phi^{-1}(5) = 2$ et $\phi^{-1}(6) = 1$.

1.2.3 Relations d'équivalence

Définition 1.2.12. Soit A un ensemble. Une relation d'équivalence est un sous-ensemble $R \subseteq A \times A$ tel que

- (1) (identité) $\forall a \in A : (a, a) \in R$,
- (2) (réflexivité) $(a, b) \in R \Rightarrow (b, a) \in R$,
- (3) (transitivité) $(a, b) \in R, (b, c) \in R \Rightarrow (a, c) \in R$.

Proposition 1.2.13. Si a, b et m sont des entiers tel que $m > 0$, $m|a$ et $m|b$, alors $m|a + b$.

Preuve. Par définition, $m|a$ et $m|b$ signifie qu'il existe des entiers c et d tels que $a = cm$ et $b = dm$. Si on somme les deux dernières égalités, on obtient $a + b = cm + dm = (c + d)m$. Ainsi $m|a + b$. \square

Exemple 1.2.14. Fixons un entier $m > 0$. On définit une relation d'équivalence sur \mathbb{Z} par le sous-ensemble $R \subseteq \mathbb{Z} \times \mathbb{Z}$ défini par la condition suivante :

$$(a, b) \in R \iff m|a - b$$

On vérifie que ce R définit une relation d'équivalence:

- (1) (identité) $\forall a \in \mathbb{Z} : m|a - a \implies (a, a) \in R$,
- (2) (réflexivité) $(a, b) \in R \implies m|a - b \implies m|b - a \implies (b, a) \in R$,
- (3) (transitivité) $(a, b) \in R, (b, c) \in R \implies m|a - b$ et $m|b - c$
 $\implies m|(a - b) + (b - c) = a - c \implies (a, c) \in R$.

Définition 1.2.15. Soit $R \subseteq A \times A$ une relation d'équivalence. Pour chaque $a \in A$ on définit la classe d'équivalence de a par

$$R_a := \{ b \in A \mid (a, b) \in R \}.$$

Remarque 1.2.16. On démontre en exercice que $(a, b) \in R \iff R_a = R_b$.

Définition 1.2.17. Soit $R \subseteq A \times A$ une relation d'équivalence. L'ensemble quotient A/R est l'ensemble des classes d'équivalences, vu comme un sous-ensemble de l'ensemble puissance de A . En d'autres termes :

$$A/R = \{ R_a \subseteq A \mid a \in A \} \subseteq 2^A$$

Le prochain exemple est notre premier exemple de groupe. Nous donnerons la définition de groupe dans quelques semaines.

Exemple 1.2.18. Soit $m \in \mathbb{Z}$. On définit $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/R$, où R est la relation d'équivalence défini dans [Exemple 1.2.14](#).

Autrement dit, si $m\mathbb{Z}$ dénote le sous-ensemble

$$m\mathbb{Z} = \{ a \in \mathbb{Z} \mid m|a \} = \{ bm \in \mathbb{Z} \mid b \in \mathbb{Z} \}$$

de \mathbb{Z} , et si $m\mathbb{Z} + x$ dénote le sous-ensemble

$$m\mathbb{Z} + x = \{ c + x \in \mathbb{Z} \mid c \in m\mathbb{Z} \}$$

de \mathbb{Z} , alors on a

$$\mathbb{Z}/m\mathbb{Z} = \{ m\mathbb{Z}, m\mathbb{Z} + 1, \dots, m\mathbb{Z} + (m - 1) \}.$$

Par exemple,

$$\mathbb{Z}/2\mathbb{Z} = \left\{ \{ \dots, -4, -2, 0, 2, 4, \dots \}, \{ \dots, -5, -3, -1, 1, 3, 5, \dots \} \right\}.$$

1.2.4 Cardinal d'un ensemble

Le dernier sujet important à propos des 'ensembles que l'on aborde dans ce cours est la définition de la taille d'un ensemble. On donne dans la définition suivante la notion d'"avoir le même cardinal", ce qui veut dire que les deux ensemble concernés ont la même grandeur.

Définition 1.2.19. Soient A et B des ensembles. On dit que

- (1) A et B ont le même cardinal, ce que l'on écrit $|A| = |B|$, s'il existe une bijection $\phi : A \rightarrow B$,
- (2) le cardinal de A est plus petit que celui de B , ce que l'on écrit $|A| \leq |B|$, s'il existe une injection $\phi : A \rightarrow B$,
- (3) A est infinie dénombrable, si A a le même cardinal que \mathbb{N} .
- (4) A a le cardinal du continu, si A a le même cardinal que \mathbb{R} .

La relation "avoir le même cardinal" semble être une relation d'équivalence, parce qu'elle satisfait les trois conditions de la Définition 1.2.12: identité (par d'existence des applications d'identité), réflexivité (par d'existence des inverses des bijections), transitivité (par composition des application). Mais il faut faire attention : le paradoxe de Russell nous dit que ce n'est pas vraiment une relation d'équivalence, parce que l'ensemble des tous les ensembles n'existe pas, donc il n'existe pas d'ensemble auquel cette relation s'applique. On peut dire que "avoir le même cardinal" est juste une propriété de deux ensembles, qui satisfait les trois propriétés de Définition 1.2.12, mais qui n'est pas une relation d'équivalence. Une conséquence importante est que l'on ne peut pas prendre les classes d'équivalences de cette relation.

Théorème 1.2.20 (Théorème de Cantor-Schröder-Bernstein). Soient A et B des ensembles. Si $|A| \leq |B|$ et $|B| \leq |A|$, alors $|A| = |B|$.

On doit démontrer un lemme avant de procéder à la preuve du Théorème 1.2.20. Dans ce lemme, on utilisera la notation suivante:

Définition 1.2.21. Soient X et Y des sous-ensembles d'un ensemble A . Ils sont *disjoints*, si $X \cap Y = \emptyset$, et ils forment une *partition* de A , s'ils sont disjoints et satisfont $X \cup Y = A$. Ces deux notions sont définies d'une manière similaire pour une collection de sous-ensembles $\{X_i\}$ de A .

Exemple 1.2.22. Les classes d'équivalences d'une relation d'équivalence $R \subseteq A \times A$ forment une partition de A .

Dans la preuve du lemme suivant, on s'autorise un abus de langage courant en mathématique : on ne change pas la notation d'une application après avoir restreint son codomaine. Par exemple, dans la preuve ci-dessous, $g|_Y$ est a priori une application $Y \rightarrow A$, mais on la considère vraiment comme une application $Y \rightarrow g(Y)$. Avec cette convention, $g|_Y$ devient bijective, et on peut prendre son inverse.

Lemme 1.2.23. Soit $f : A \rightarrow B$ et $g : B \rightarrow A$ des injections. S'il existe un sous-ensemble $X \subseteq A$ tel que

$$X = A \setminus g(B \setminus f(X)), \quad (2.23.a)$$

alors il existe une bijection $A \rightarrow B$.

Preuve. Définissons

$$Y_A := A \setminus X \underset{\uparrow}{=} g(B \setminus f(X)), \quad Y := B \setminus f(X) \underset{\uparrow}{=} (g|_Y)^{-1}(Y_A), \quad X_B := f(X)$$

(2.23.a)

g est injective, alors elle induit une bijection $Y \rightarrow Y_A = g(Y) \implies$ on dénote l'inverse de cette bijection par g^{-1}

On obtient directement que X et Y_A forment une partition de A , et que X_B et Y forment une partition de B . De plus, $f : X \rightarrow X_B = f(X)$ et $g^{-1} : Y_A = g(Y) \rightarrow Y$ sont des bijections. Le diagramme suivant résume la situation :

$$\begin{array}{ccc} A & & B \\ \parallel & & \parallel \\ X & \xrightarrow[\text{bijection}]{f} & X_B \\ \cup & & \cup \\ Y_A & \xrightarrow[\text{bijection}]{g^{-1}} & Y \end{array}$$

Cela implique que l'on peut définir une bijection $\phi : A \rightarrow B$ par la formule

$$\phi(a) = \left\{ \begin{array}{ll} f(a) & \text{si } a \in X \\ g^{-1}(a) & \text{si } a \in Y_A \end{array} \right\}$$

□

Preuve du Théorème 1.2.20. Pour chaque sous-ensemble $X \subseteq A$ définissons

$$H(X) := A \setminus g(B \setminus f(X))$$

Par le **Lemme 1.2.23**, il suffit de montrer qu'il existe un X pour lequel $X = H(X)$. Premièrement on démontre que H respecte la relation d'inclusion :

$$\begin{array}{c} X \subseteq Z \implies f(X) \subseteq f(Z) \implies B \setminus f(X) \supseteq B \setminus f(Z) \implies g(B \setminus f(X)) \supseteq g(B \setminus f(Z)) \\ \uparrow \quad \quad \quad \uparrow \quad \quad \quad \uparrow \\ \boxed{\begin{array}{l} \text{par définition de} \\ \text{l'image dans la} \\ \text{Définition 1.2.7} \end{array}} \quad \boxed{\begin{array}{l} \text{prendre le complément renverse} \\ \text{l'inclusion (ce sera un exercice)} \end{array}} \quad \boxed{\begin{array}{l} \text{par définition de} \\ \text{l'image dans la} \\ \text{Définition 1.2.7} \end{array}} \\ \implies H(X) = A \setminus g(B \setminus f(X)) \subseteq A \setminus g(B \setminus f(Z)) = H(Z) \quad (2.23.b) \\ \uparrow \\ \boxed{\begin{array}{l} \text{prendre le complément renverse l'inclusion} \end{array}} \end{array}$$

Deuxièmement on définit

$$W := \bigcap_{\substack{X \subseteq A \\ H(X) \subseteq X}} X, \quad (2.23.c)$$

et on observe que la définition fait sens, puisque A lui-même satisfait $H(A) \subseteq A$. On finit notre preuve en démontrant que $H(W) = W$. On commence par démontrer que $H(W) \subseteq W$:

$$\begin{array}{c} W \subseteq \bigcap_{\substack{X \subseteq A \\ H(X) \subseteq X}} X \implies H(W) \subseteq \bigcap_{\substack{X \subseteq A \\ H(X) \subseteq X}} H(X) \subseteq \bigcap_{\substack{X \subseteq A \\ H(X) \subseteq X}} X = W \\ \uparrow \quad \quad \quad \uparrow \quad \quad \quad \uparrow \\ \boxed{(2.23.c)} \quad \boxed{(2.23.b)} \quad \boxed{H(X) \subseteq X} \quad \boxed{(2.23.c)} \end{array}$$

Pour conclure, il suffit maintenant de montrer que $H(W) \supseteq W$. Notons que $H(W) \subseteq W$ et (2.23.b) implique que $H(H(W)) \subseteq H(W)$. Cela veut dire que $H(W)$ fait partie de la collection que X parcourt dans (2.23.c). Ceci implique que $H(W) \supseteq W$, ce qui conclut notre argument. □

Un aspect fascinant de la théorie des ensembles, est la suivante: on peut démontrer en utilisant les axiomes de Zermelo-Fraenkel qu'il existe un cardinal ω_1 minimal entre les cardinaux plus grand que $|\mathbb{N}| = \omega_0$. Il y aura une exercise aussi sur la fiche d'exercice qui nous montre que

$|\mathbb{R}| = |2^{\mathbb{N}}| > \omega_0$. Ainsi, c'est naturel de demander si $|\mathbb{R}| = \omega_1$. Ce qui est surprenant ce que l'on peut démontrer qu'il n'est pas possible de prouver que $|\omega_1| = |\mathbb{R}|$ ni que $|\omega_1| \neq |\mathbb{R}|$ dans le système d'axiomes de Zermelo-Fraenkel. Cette question est longtemps restée ouverte ; les mathématiciens ont quelquefois supposé que l'égalité était vraie, ce que on appelle l'hypothèse du continu. Cohen a finalement démontré que l'hypothèse du continu est indépendante du système d'axiomes de Zermelo-Fraenkel, en construisant un modèle où elle est vraie, et un autre où elle est fausse. Cohen a d'ailleurs reçu le prix mathématique le plus prestigieux, la Médaille Fields en 1966, pour ce résultat.

Chapter 2

Théorie des nombres

2.1 ALGORITHME D'EUCLIDE

Définition 2.1.1. Soit $a, b \in \mathbb{Z}^{>0}$. Le *plus grand commun diviseur* de a et b et

$$\max \{ m \in \mathbb{Z}^{>0} \mid m|a \text{ et } m|b \}$$

(On note que l'ensemble ci-dessus est non-vidé, parce qu'il contient $m = 1$, et qu'il est majoré par $\min\{a, b\}$. Ainsi le maximum existe.)

Lemme 2.1.2. Si, $a, b \in \mathbb{Z}^{>0}$ et $r \in \mathbb{Z}$, alors $(a, b) = (a, b + ra)$.

Preuve. Par **Définition 2.1.1**, il suffit de montrer que pour chaque entier $m \in \mathbb{Z}^{>0}$,

$$m|a \text{ et } m|b \iff m|a \text{ et } m|b + ra$$

On montre chaque direction de cette équivalence ci-dessous:

- $\boxed{\implies} m|a \implies m|ra \xRightarrow{\uparrow} m|b + ra.$

$m|b \text{ et Proposition 1.2.13}$
- $\boxed{\impliedby} m|a \implies m|-ra \xRightarrow{\uparrow} m|(b + ra) - ra = b.$

$m|b + ra \text{ et Proposition 1.2.13}$

□

Notation 2.1.3. ALGORITHME D'EUCLIDE Soient $a, b \in \mathbb{Z}^{>0}$. On définit l'algorithme récursif suivant, en prenant pour valeurs initiales $i := 2$, $q_1 := \max\{a, b\}$ et $q_2 := \min\{a, b\}$. Le pas de récursion est:

- si $q_i | q_{i-1}$, alors on s'arrête, q_i est le résultat de l'algorithme, et on pose $t := i$ (t encode le temps d'arrêt de l'algorithme) ;
- sinon, on définit q_{i+1} prenant division avec reste: $q_{i-1} := s_i q_i + q_{i+1}$ (notez que par le point précédent $q_i \nmid q_{i-1}$, ainsi en utilisant la définition de la division avec reste on a $0 < q_{i+1} < q_i$)
- on augmente i de 1.

On note aussi que cet algorithme s'arrête toujours. En effet, dans le cas $a = b$ il s'arrête au début ; et quand $a \neq b$ on a la suite $q_1 > q_2 > \dots > q_t > 0$ de nombres entiers, qui ne peut avoir de plus q_1 pas, autrement dit $t \leq q_1$.

Lemme 2.1.4. Dans la situation de la *Notation 2.1.3*, il existe $m, n \in \mathbb{Z}$ tel que $ma + nb = q_t$.

Preuve. On démontre par induction descendante sur i qu'il existe $m_i, n_i \in \mathbb{Z}$ tel que $m_i q_i + n_i q_{i+1} = q_t$ pour chaque entier $1 \leq i \leq t-1$.

Pour $i = t-1$ on peut choisir $m_i = 0$ et $n_i = 1$. Il faut encore montrer le pas d'induction. Fixons $i \leq t-1$, et supposons connue la proposition pour les indices supérieurs ou égaux à i . Le calcul suivant démontre la proposition pour $i-1$:

$$q_t = m_i q_i + n_i q_{i+1} = m_i q_i + n_i (q_{i-1} - s_i q_i) = \underbrace{n_i}_{\substack{\uparrow \\ \boxed{:= m_{i-1}}}} q_{i-1} + \underbrace{(m_i - n_i s_i)}_{\substack{\uparrow \\ \boxed{:= n_{i-1}}}} q_i$$

□

Lemme 2.1.5. Dans la situation de la *Notation 2.1.3*, $q_t | q_i$ pour chaque entier $1 \leq i \leq t$.

Preuve. On démontre la proposition par induction descendant par rapport à i . Pour $i = t$, on a $q_i = q_t$, auquel cas la proposition est trivialement vraie. Pour $i = t-1$ on a $q_{t-1} | q_t$ par la définition de l'algorithme.

Supposons maintenant que $i < t$, que l'on sait la proposition pour les indices supérieurs ou égaux à i , et on démontre la proposition pour $i-1$. C'est une conséquence immédiate de la définition de l'algorithme :

$$q_{i-1} = q_{i+1} + s_i q_i \quad \xRightarrow{\substack{\uparrow \\ \boxed{q_t | q_{i+1} \text{ et } q_t | q_i \text{ par hypothèse d'induction}}}} q_t | q_{i-1}$$

□

Théorème 2.1.6. Si $a, b \in \mathbb{Z}^{>0}$, l'algorithme d'Euclide nous donne $q_t = (a, b)$.

En particulier, on a une relation de Bézout : il existe $m, n \in \mathbb{Z}$ tels que $ma + nb = (a, b)$.

Preuve. $\boxed{q_t = (a, b)}$: C'est impliqué par les deux lemmes précédent :

- **Lemme 2.1.4** dit que $(a, b) | q_t$, et
- **Lemme 2.1.5** dit que $q_t | a$ et $q_t | b$, alors $q_t | (a, b)$.

$\boxed{\text{Existence de } m \text{ et } n}$: c'est impliqué par $q_t = (a, b)$ et par le **Lemme 2.1.4**.

□

Corollaire 2.1.7. Supposons que $q, a, b \in \mathbb{Z}^{>0}$, $q | ab$ et que $(q, a) = 1$. Alors $q | b$.

Preuve. Par le **Théorème 2.1.6**, il existe $m, n \in \mathbb{Z}^{>0}$ tel que $1 = ma + nq$. En multipliant cette équation par b on obtient $b = mab + nqb$. Puisqu'on a supposé que $q | ab$, on obtient que $q | b$. □

2.2 THÉORÈME FONDAMENTAL DE L'ARITHMÉTIQUE

Définition 2.2.1. Soit $p \geq 2$ un entier. On dit que :

- (1) p est *irréductible*, si pour chaque $a \in \mathbb{Z}^{>0}$: $a | p \implies a = 1$ ou $a = p$.
- (2) p est *premier*, si pour chaque $a, b \in \mathbb{Z}^{>0}$: $p | ab \implies p | a$ ou $p | b$.

Remarque 2.2.2. Notez bien que $p \geq 2$ dans cette définition. En particulier, le nombre 1 n'est, par convention, ni premier ni irréductible.

Proposition 2.2.3. *Si $p \geq 2$ est un entier, alors p est irréductible si et seulement si p est premier.*

Preuve. $\boxed{\Leftarrow}$ Soit $a \in \mathbb{Z}^{>0}$ un diviseur de p . On peut écrire $ab = p$ pour un entier $b \in \mathbb{Z}^{>0}$. En particulier $a, b \leq p$. En utilisant que p est premier on obtient $p|a$ ou $p|b$. Cela implique, en utilisant $a, b \leq p$, que $p = a$ ou $p = b$. Si $p = b$, on obtient que $a = 1$. En somme, on a obtenu que $a = p$ ou $a = 1$, ce qui est exactement la définition d'être irréductible.

$\boxed{\Rightarrow}$ Prenons $a, b \in \mathbb{Z}^{>0}$ tels que $p|ab$. Il faut montrer que $p|a$ ou $p|b$. Si $p|a$ on a terminé, donc on peut supposer que $p \nmid a$, autrement dit que $(p, a) \neq p$. Mais p est irréductible, alors il a seulement deux diviseurs (positifs) 1 et p . Cela force $(p, a) = 1$. Finalement dans ce cas **Corollaire 2.1.7** nous donne que $p|b$. \square

Théorème 2.2.4. *Pour chaque $n \in \mathbb{Z}^{>1}$ on peut écrire $n = \prod_{i=1}^r p_i$ pour un nombre fini de premiers p_1, \dots, p_r . De plus la liste de ces premiers sont uniques modulo leur ordre.*

Preuve. $\boxed{\text{Existence:}}$ On démontre qu'on peut écrire $n = \prod_{i=1}^r p_i$ par induction sur n . Pour $n = 2$ c'est clair, parce que 2 est premier.

Supposons que $n > 2$ et qu'on a déjà démontré la proposition pour chaque entier plus grand que 1 et plus petit que n . Si n est premier on a terminé. Sinon, en utilisant **Proposition 2.2.3**, n n'est pas irréductible, et ainsi il existe $n > a, b \in \mathbb{Z}^{>0}$ tels que $n = ab$. Par l'hypothèse d'induction on peut écrire $a = \prod_{i=1}^s p_i$ et $b = \prod_{i=s+1}^r p_i$ pour certains nombres premiers p_i . Ainsi on obtient

$$n = ab = \left(\prod_{i=1}^s p_i \right) \cdot \left(\prod_{i=s+1}^r p_i \right) = \prod_{i=1}^r p_i$$

$\boxed{\text{Unicité:}}$ Supposons qu'il y ait deux expressions:

$$n = \prod_{i=1}^r p_i = \prod_{j=1}^s q_j \tag{2.4.a}$$

où les p_i et q_j sont des nombres premiers. En échangeant si besoin les p_i et les q_j , on peut supposer que $r \leq s$.

On démontre par induction sur s que les listes des p_i et des q_j est la même modulo leur ordre. Si $s = 1$, alors $r = 1$, et il n'y a rien à démontrer.

Supposons que $s > 1$. Dans ce cas on a

$$q_1 | n = \prod_{i=1}^r p_i.$$

Utilisant $r - 1$ fois la contraposée de la définition d'être premier on obtient qu'il existe un indice j tel que $q_1 | p_j$. Par la **Proposition 2.2.3**, p_j est irréductible. En utilisant que $q_1 > 1$, on obtient $q_1 = p_j$. Alors par (2.4.a) on obtient

$$\mathbb{Z} \ni \frac{n}{q_1} = \prod_{1 \leq i \leq r, i \neq j} p_i = \prod_{j=2}^s q_j$$

En particulier $r > 2$, parce qu'autrement le premier produit dans (2.2) serait vide. Ça veut dire que on peut appliquer l'hypothèse d'induction pour les deux produits dans (2.2). Ceci conclut notre démonstration. \square

Chapter 3

Théorie des groupes