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

Zsolt Patakfalvi

(avec l'aide de Quentin Posva)

September 15, 2020

Contents

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 : $\Longrightarrow$,

(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 est seulement si A est B sont tous les deux faux).

(4) moduls ponens: s'il y a une ligne précédente de la forme $A \Longrightarrow B$, 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 un 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 un 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. (DIVISON 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*

$$a = bq + r. \tag{1.3.a}$$

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,

$$bq + r = b'q + r' \implies \underbrace{r - r'}_{\uparrow} = \underbrace{q(b' - b)}_{\uparrow} \implies r - r' = 0 \implies r = r' \implies bq = b'q \underset{\uparrow}{\implies} b = b'$$

$0 \leq r, r' < q \implies -q < r - r' < q$

les possibilités sont $\ldots, -2q, -q, 0, q, 2q, \ldots$, parce que $b' - b$ est entier

$q > 0$

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 r par $r - 1$. On a ainsi $r - 1 = cq + s$, 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

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

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

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

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 celles 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 rencontrez 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 un collection des "choses", et une sous-collections 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:*

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

ne peut pas être pas un ensemble.

Preuve. La définition de B dit que B est contenu dans B si est 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 cette 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 de temps avec des ensembles construits à partir de l'ensemble des entiers, et dans cette situation aucun problème ne peut arriver. Mentionnons quand même comment le paradoxe de Russel fût résolu vers la fin de la XIXe siècle.

Un système d'axiomes fût 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 est 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:
$$\mathbb{Z}^{>0} := \{x \in \mathbb{Z} | x > 0\}.$$

(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 appellée le complément de A dans B, définit par
$$B \setminus A = \{\ b \in B \mid \underbrace{b \neg \in A}_{\text{notation en logique mathématique}}\ \} = \{\ b \in B \mid \underbrace{b \notin A}_{\text{notation plus commune en mathématique}}\ \}$$

(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 :

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

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 $b \in B$:

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

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

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

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

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

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

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

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 $\phi : A \to B$ 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 coordonne 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) $\mathrm{id}_A : A \to A$ est définie par

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

$$\Updownarrow$$

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

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

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

$$\Updownarrow$$

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

Définition 1.2.7. Soit $\phi : A \to B$ 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 *bijective*, si elle est injective et surjective.

(4) l'image de ϕ est

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

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 $\phi : A \to B$ et $\xi : B \to C$ des applications entre ensembles. La composition $\xi \circ \phi$ est l'application

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

$$\Updownarrow$$

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

Proposition 1.2.9. *Soient $\phi : A \to B$ et $\xi : B \to C$ es 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 :

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

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

□

Définition 1.2.10. Soit $\phi : A \to B$ une bijection entre ensembles. *L'inverse* ϕ^{-1} de ϕ est l'application $\phi^{-1} : B \to A$ 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 $\phi : \{1,2\} \to \{5,6\}$ la bijection définie par $\phi(1) = 6$ et $\phi(2) = 5$. Dans ce cas $\phi^{-1} : \{5,6\} \to \{1,2\}$ 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 $m|a+b$. □

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

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

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 :

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

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 $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/R$, ou R est la relation d'équivalence défini dans Exemple 1.2.14.

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

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

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

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

de $\mathbb{Z}$, alors on a

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

Par exemple,

$$\mathbb{Z}/2\mathbb{Z} = \Big\{ \ \{ \ \ldots, -4, -2, 0, 2, 4, \ldots \ \} \ , \ \{ \ \ldots, -5, -3, -1, 1, 3, 5, \ldots \ \} \ \Big\}.$$

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 $\phi : A \to B$,

(2) *le cardinal* de A et *plus petit* que celui de B, ce que l'on écrit $|A| \leq |B|$, s'il existe une injection $\phi : A \to B$,

(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 le trois conditions de la Définition 1.2.12: identité (par d'existence des applications d'identité), reflexivité (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 dois 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 forme 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 $Y \to A$, mais on la consièdre vraiment comme une application $Y \to g(Y)$. Avec cette convention, $g|_Y$ devient bijective, et on peut prendre son inverse.

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

$$X = A \setminus g\big(B \setminus f(X)\big), \tag{2.23.a}$$

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

Preuve. Définissons

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

(2.23.a)

g est injective, alors elle induit une bijection $Y \to Y_A = g(Y) \Longrightarrow$ 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, $f : X \to X_B = f(X)$ et $g^{-1} : Y_A = g(Y) \to Y$ sont des bijections. Le diagramme suivant résume la situation :

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

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

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

□

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

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

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 :

$$X \subseteq Z \underset{\uparrow}{\Longrightarrow} f(X) \subseteq f(Z) \underset{\uparrow}{\Longrightarrow} B \setminus f(X) \supseteq B \setminus f(Z) \underset{\uparrow}{\Longrightarrow} g\big(B \setminus f(X)\big) \supseteq g\big(B \setminus f(Z)\big)$$

par définition de l'image dans la Définition 1.2.7 — prendre le complément renverse l'inclusion (ce sera un exercice) — par définition de l'image dans la Définition 1.2.7

$$\underset{\uparrow}{\Longrightarrow} H(X) = A \setminus g\big(B \setminus f(X)\big) \subseteq A \setminus g\big(B \setminus f(Z)\big) = H(Z) \quad (2.23.b)$$

prendre le complément renverse l'inclusion

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 $H(W) \subseteq W$:

$$W \underset{\uparrow}{\subseteq} \bigcap_{\substack{X \subseteq A \\ H(X) \subseteq X}} X \underset{\uparrow}{\Longrightarrow} H(W) \subseteq \bigcap_{\substack{X \subseteq A \\ H(X) \subseteq X}} H(X) \underset{\uparrow}{\subseteq} \bigcap_{\substack{X \subseteq A \\ H(X) \subseteq X}} X \underset{\uparrow}{=} W$$

(2.23.c) — (2.23.b) — $H(X) \subseteq X$ — (2.23.c)

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 que on peut démontrer que ce n'est pas possible de démontrer si $\left|2^{\mathbb{N}}\right| = |\mathbb{R}|$ ou $\left|2^{\mathbb{N}}\right| \neq |\mathbb{R}|$. Anciennement on savait pas si ces le cas. Ainsi les mathématiciens quelque fois ont supposé que l'égalité est vrai, ce que on appelle l'hypothèse du continu. Cohen a démontré finalement que c'est indépendant de système d'axioms de Zermelo-Fraenkel, construisant un modèle ou c'est vrai, et un autre ou c'est faux. Cohen a reçu le plus grand prix de la mathématique, le Médaille Fields, pour ce résultat.

Chapter 2

Théorie des nombres

Chapter 3

Théorie des groupes