Théorie des ensembles : AC, cardinaux

Nicolas Fabiano

11 juin 2016

1 Préliminaires

1.1 Relations d'ordre

Une relation d'ordre sur E est une relation vérifiant pour tous $x, y, z \in E$:
(i) $x \leq x$
(ii) $(x \leq y \wedge y \leq x) \Rightarrow x = y$
(iii) $(x \leq y \wedge y \leq z) \Rightarrow x \leq z$

La relation d'ordre est dite totale si de plus pour tous $x, y \in E$:
(iv) $x \leq y \vee y \leq x$
On appelle chaîne de E toute partie de E totalement ordonnée.

La relation d'ordre est dite bonne si toute partie non vide de E admet un minimum.
Toute relation d'ordre bonne est totale.

$x \in E$ est dit maximal s'il n'admet aucun majorant strict, ie il n'existe pas de $y \in E$ tq $y > x$.

Exemples :
- $(\mathbf{R}, \leq)$ est totalement ordonné mais pas bien ordonné ($]0,1]$ n'a pas de minimum)
- $(\mathbf{N}, \leq)$ est totalement et bien ordonné.
- $(\mathbf{N}, |)$ n'est pas totalement ordonné (2 et 3 ne sont pas comparables). $\{2^n, n \in \mathbf{N}\}$ est une chaîne. 0 est maximal, c'est d'ailleurs le maximum.
- $(P(E), \subset)$ n'est pas totalement ordonné. E est maximal, c'est d'ailleurs le maximum.
- $(P(E) \backslash \{E\}, \subset)$ n'est pas totalement ordonné. $E\{x\}$ est maximal pour tout $x \in E$.

1.2 Relations d'équivalence

Une relation d'équivalence sur E est une relation vérifiant pour tous $x, y, z \in E$:
(i) $x \equiv x$
(ii) $x \equiv y \Rightarrow y \equiv x$

(iii) $(x \equiv y \wedge y \equiv z) \Rightarrow x \equiv z$

On appelle classe d'équivalence de x notée $\bar{x}$ l'ensemble des $y \in E$ tq $x \equiv y$.
Les classes d'équivalence forment une partition de E. On note $E/\equiv$ leur ensemble. Quand toutes les classes sont d'une même forme F, on note plutôt E/F.

Exemples :
- Pour une fonction de E dans A, on pose $x \equiv y \Leftrightarrow f(x) = f(y)$.
- Pour $n \in \mathbf{Z}$, on pose $a \equiv b \Leftrightarrow n|b - a$. On note l'ensemble des classes d'équivalence $\mathbf{Z}/n\mathbf{Z}$ (arithmétique modulo n).

2 AC, Zorn, Zermelo

2.1 Enoncés

Axiome 1 (AC) *Soit X ensemble d'ensembles non vides. Il existe une fonction définie sur X, appelée fonction de choix sur X, qui à chaque ensemble A appartenant à X associe un élément de A.*

Lemme 2 (Zorn) *Si toute chaîne de E est majorée, alors E possède un élément maximal.*

Théorème 3 (Zermelo) *Tout ensemble peut être muni d'un bon ordre.*

2.2 Equivalence

Théorème 4 *Dans ZF, AC $\Leftrightarrow$ Zorn $\Leftrightarrow$ Zermelo*

En effet :

- Zermelo $\Rightarrow$ AC

    On munit l'ensemble d'une bonne relation d'ordre et on utilise le min comme fonction de choix.

(- Zorn $\Rightarrow$ AC)

    On considère l'ensemble des fonctions de choix partielles, ie des fonctions qui font un choix parmi seulement certains ensembles.
    On le munit du prolongement de fonctions.
    Toute chaîne est majorée, donc il existe une fonction de choix partielle maximale, elle est alors totale.

- Zorn $\Rightarrow$ Zermelo ($\star$)

    On considère l'ensemble des bons ordres partiels, ie des couples $(F, \leq)$ avec $F \subset E$ et $\leq$ bon ordre sur F.
    On dit que $(F', \leq')$ prolonge $(F, \leq)$ si F est un début de $(F', \leq')$ et que $\forall (x, y) \in F^2, x \leq y \Rightarrow x \leq' y$.
    Toute chaîne est majorée, donc il existe un bon ordre partiel maximale, il est alors total.

- AC $\Rightarrow$ Zorn ($\star$)

  Une chaîne est dite continuable si elle admet un majorant strict.
  On fixe avec AC un majorant strict particulier pour toute chaîne continuable.
  Une chaîne est dite bonne si pour tout début strict de cette chaîne, le majorant fixé est dans la chaîne et est le plus petit élément de la fin de la chaîne.
  On montre que l'union de toutes les bonnes chaînes est une bonne chaîne.
  Montre par l'absurde qu'elle n'admet pas de majorant strict, son majorant est donc maximal.

Théorème 5 *Dans ZF, on ne peut ni prouver ni infirmer AC.*

2.3 Applications

Théorème 6 (Banach-Tarski) *Il existe une découpe d'une boule unité en un nombre fini de morceaux tels qu'à rotation et translation près ils forment deux boules unité.*

L'idée de la preuve est de définir une relation d'équivalence entre les points, d'utiliser AC pour choisir un représentant particulier de chaque classe, de l'utiliser pour paramétrer tous les autres points et de se ramener ainsi à un problème sur des alphabets infinis (voir référence en dernière page).

Soit $\mathbf{N}$ joueurs numérotés à partir de 0.

Un mathématicien machiavélique les place sur un escalier à $\mathbf{N}$ marches, et place sur la tête de chacun un chapeau blanc ou noir. Le joueur 0, tout en haut, voit tous les chapeaux sauf le sien ; le joueur 1, juste en dessous, vois tous les chapeaux à partir de 2 ; etc. à l'infini

Chaque joueur doit tenter de déterminer la couleur de son propre chapeau, sachant que tout échange est interdit une fois les chapeaux déposés (ils sont néanmoins autorisés avant pour se mettre d'accord sur une stratégie).

Existe-t-il une stratégie pour s'assurer qu'au moins un joueurs trouve la couleur de son chapeau ? ($\star$)

> Voici une stratégie pour s'assurer qu'au plus un nombre fini se trompe (et donc un nombre infini a juste, ce qui est encore mieux que demandé) :
> On définit une relation d'équivalence sur $\{N, B\}^{\mathbf{N}}$ par l'égalité des suites à partir d'un certain rang.
> On fixe avec AC un représentant particulier par classe d'équivalence.
> Chaque joueur peut déterminer à quelle classe la configuration réelle appartient, et il énonce que son chapeau est de la couleur du représentant particulier.
> Comme la configuration réelle et le représentant sont égaux à partir d'un certain rang, on a le résultat voulu.

3 Comparaison de cardinaux

3.1 Définitions

$f : A \longrightarrow B$ est dite injective si deux éléments distincts quelconques de A ont des images distinctes.

$f : A \longrightarrow B$ est dite surjective si tout élément de B admet un antécédent.

$f : A \longrightarrow B$ est dite bijective si elle est injective et surjective, ie si tout élément de B admet exactement 1 antécédent. On peut alors définir la fonction inverse, notée f^{-1}.

On note B^A ou $F(A, B)$ l'ensemble des fonctions de A dans B.

On note $A \hookrightarrow B$ pour signifier qu'il existe $f : A \longrightarrow B$ injective.

On note $A \sim B$ pour signifier qu'il existe $f : A \longrightarrow B$ bijective (A et B sont dits équipotents).

E est dit dénombrable si $E \hookrightarrow \mathbf{N}$.

3.2 Formules calculatoires

On a facilement pour tous A, B, C :

$A \sim A \quad ; \quad A \hookrightarrow A$

$(A \sim B \wedge B \sim C) \Rightarrow A \sim C \quad ; \quad (A \hookrightarrow B \wedge B \hookrightarrow C) \Rightarrow A \hookrightarrow C$

$A \sim B \Leftrightarrow B \sim A$

$\sim$ ressemble fortement à une relation d'équivalence, et $\hookrightarrow$ à une relation d'ordre, mais il y a quelques problèmes formels de définition, voir corollaire 8.

On a de plus pour tous A, B, E :

Si $A \hookrightarrow B$, alors $A^E \hookrightarrow B^E$ et $E^A \hookrightarrow E^B$

Si $A \sim B$, alors $A^E \sim B^E$ et $E^A \sim E^B$

$(E^A)^B \sim E^{A \times B}$

$(A \times B)^E \sim A^E \times B^E$

3.3 Equipotences classiques

S'il existe une surjection de E dans F, alors $F \hookrightarrow E$. Réciproque ?

> Noter l'utilisation d'AC dans le sens direct.
> La réciproque est vraie, mais seulement si F est non vide.

$\mathbf{N} \sim \mathbf{N}^2 \sim \mathbf{Z} \sim \mathbf{Q}$

> Faire des dessins.

$\mathbf{R} \sim \mathbf{R}^2 \sim [0, 1] \sim \{0, 1\}^{\mathbf{N}}$

> Utiliser la décomposition en base 2 pour $\mathbf{R} \sim \mathbf{R}^2$ et $[0, 1] \sim \{0, 1\}^{\mathbf{N}}$ (on ne se préoccupe pas des problèmes d'écritures impropres, ils seront gérés avec Cantor-Bernstein) et la fonction tangente pour ramener $\mathbf{R}$ dans $[0, 1]$.

$P(E) \sim \{0, 1\}^E$ pour tout E

Choisir un sous-ensemble revient pour chaque élément à choisir s'il est dedans (1) ou non (0).

Théorème 7 (Cantor) *Pour tout E, $E \not\sim P(E)$*

Pour une fonction $f : E \longrightarrow P(E)$, on utilise $\{x \in E, x \notin f(x)\}$. On vérifie par l'absurde qu'il ne peut pas avoir d'antécédent.

Corollaire 8 *Il n'existe pas d'ensemble de tous les ensembles.*

Il contiendrait en particulier toutes ses parties, ce qui est impossible. (On peut aussi montrer le résultat plus fort qu'il n'existe pas d'ensemble de tous les ordinaux)

Corollaire 9 $\mathbf{N} \not\sim \mathbf{R}$

$\mathbf{R} \sim \{0,1\}^{\mathbf{N}}$ ou bien preuve directe par la diagonale de Cantor.

3.4 Cantor-Bernstein

Théorème 10 (Cantor-Bernstein) *Pour tous A, B :*
$(A \hookrightarrow B \wedge B \hookrightarrow A) \Rightarrow A \sim B$

Lemme 11 *Pour tous $E \subset A$:*
$A \hookrightarrow E \Rightarrow A \sim E$

Faire un dessin.
On note $f : A \longrightarrow E$ injective.
On note $C_0 = A \backslash E$, puis $C_{n+1} = f(C_n)$ pour tout n et $C = \bigcup C_n$
On pose $g : A \longrightarrow E$ qui à x associe $f(x)$ si $x \in C$ et x sinon.
On vérifie que g est bijective.

On considère l'image de A dans B par l'injection : A lui est clairement équipotent, et B l'est par le lemme (la composée deux deux injections est injective).

3.5 Totalité

Théorème 12 *Pour tous A, B :*
$A \hookrightarrow B \vee B \hookrightarrow A$

On considère l'ensemble des bijections partielles, ie des ensembles de couples (x_i, y_i) avec $x_i \in A$, $y_i \in B$ et chaque élément qui apparaît dans au plus un couple.
On le munit de l'inclusion.
Toute chaîne est majorée, donc il existe une bijection partielle maximale.
Alors $\{x_i\} = A$, auquel cas on obtient une injection de A dans B, ou $\{y_i\} = B$ et on obtient une injection de B dans A.

3.6 Exercices

A quoi est équipotent l'ensemble ... : (réponse à donner parmi $\mathbf{N}, \mathbf{R}, P(\mathbf{R}), P(P(\mathbf{R})), ...$)

(i) ... des intervalles ouverts de $\mathbf{R}$?
(ii) ... des parties finies de $\mathbf{N}$?
(iii) $\mathbf{N}^{\mathbf{N}}$?
(iv) ... des suites à valeurs dans $\mathbf{N}$ bornées ?
(v) ... des suites à valeurs dans $\mathbf{N}$ croissantes ?
(vi) $\mathbf{N}^{(\mathbf{N})}$ l'ensemble des suite à valeurs dans $\mathbf{N}$ à support fini (ie nombre fini de termes non nuls) ?
(vii) ... des bijections de $\mathbf{N}$ dans lui-même ? ($\star$)
(viii) $\mathbf{R}^{\mathbf{N}}$?
(ix) $\mathbf{R}^{\mathbf{R}}$?
(x) ... des parties dénombrables de $\mathbf{R}$?
(xi) ... des fonctions de $\mathbf{R}$ dans $\mathbf{R}$ qui ont une limite en $\pm\infty$?
(xii) ... des fonctions de $\mathbf{R}$ dans $\mathbf{R}$ continues ? ($\star$)
(xiii) ... des fonctions de $\mathbf{R}$ dans $\mathbf{R}$ croissantes ? ($\star$)

Montrer que pour tout E infini :
(i) $E \cup \mathbf{N} \sim E$
(ii) $E \times \mathbf{N} \sim E$ ($\star$)
(iii) $E^2 \sim E$ ($\star\star\star$)
(iv) $E^{(\mathbf{N})} \sim E$

3.7 Solutions

(i) $\mathbf{R}$ (utiliser $(\mathbf{R} \cup \{\pm\infty\})^2 \sim \mathbf{R}^2$)
(ii) $\mathbf{N}$ (utiliser la décomposition comme somme de puissances de 2)
(iii) $\mathbf{R}$ (probablement aucune "belle" construction, utiliser par exemple les décompositions en base)
(iv) $\mathbf{R}$ (utiliser (iii) et Cantor-Bernstein avec $\mathbf{R} \sim \{0,1\}^{\mathbf{N}}$)
(v) $\mathbf{R}$ (idem)
(vi) $\mathbf{N}$ (utiliser la décomposition en facteurs premiers)
(vii) $\mathbf{R}$ (injecter $\{0,1\}^{\mathbf{N}}$ en transposant ou pas $2n$ et $2n+1$)
(viii) $\mathbf{R}$ (calcul purement formel)
(ix) $P(\mathbf{R})$ (calcul purement formel, utiliser $[0,1] \times \mathbf{N} \sim \mathbf{R}$)
(x) $\mathbf{R}$ (injecter dans $\mathbf{R}^{\mathbf{N}}$)
(xi) $P(\mathbf{R})$ ($P(\mathbf{R}) \sim \mathbf{R}^{[0,1]} \hookrightarrow$ l'ensemble, en prolongeant toute fonction par 0 hors de $[0,1]$)
(xii) $\mathbf{R}$ (utiliser la restriction à $\mathbf{Q}$ ou utiliser que toute fonction continue sur $[0,1]$ est limite uniforme d'une suite de polynômes)
(xiii) $\mathbf{R}$ (utiliser la restriction à $\mathbf{Q}$; coder les points de discontinuité, dénombrables, dans $(\mathbf{R} \times \mathbf{R})^{\mathbf{N}}$)

(i) Ecrire $E = F \cup \mathbf{N}$ en utilisant une injection de $\mathbf{N}$ dans E (sans AC), puis $E \sim F \cup \mathbf{N} \sim F \cup (\mathbf{N} \cup \mathbf{N}') \sim E \cup \mathbf{N}$.

(ii) Ecrire $E = F \times \mathbf{N}$ en utilisant au choix :

- la structure conférées par Zermelo en quotientant E par une relation d'équivalence

- le lemme de Zorn sur l'ensemble des bijections entre une partie de E et $\mathbf{N}\times$(une partie de $P(E)$), ordonnées par l'inclusion sur l'ensemble de définition (Noter l'importance de prendre $P(E)$ et pas E pour s'assurer de ne jamais tout remplir, ce qui compromettrait à la fois la preuve que toute partie est majorée et la conclusion en utilisant l'ensemble maximal)

... puis $E \sim F \times \mathbf{N} \sim F \times (\mathbf{N} \times \mathbf{N}') \sim E \times \mathbf{N}$.

(iii) Il suffirait pour appliquer la même méthode de parvenir à écrire $E = \{0,1\}^F$, mais cela ne semble pas se faire de manière aussi élémentaire (et est d'ailleurs faux dans le cas général si on suppose l'hypothèse du continu fausse). Une référence (voir dernière page) propose de le prouver par récurrence transfinie sur les ordinaux puis de l'étendre à tout ensemble par Zermelo.

(iv) En utilisant (iii), construire une injection de $E^{(\mathbf{N})}$ dans $\mathbf{N} \times E$, en codant d'abord l'indice du dernier terme non nul puis en utilisant $E^2 \sim E$ pour ramener tous les éléments de E à un seul de manière récursive (regrouper les deux derniers, puis le nouveau dernier au nouvel avant-dernier, etc.).

4 Exercices bonus

4.1 Enoncés

Soit A ensemble. Montrer que A dénombrable $\Leftrightarrow$ il existe (A_n) suite croissante pour l'inclusion de parties finies de A dont l'union vaut A.

Montrer qu'une union dénombrable d'ensembles dénombrables est dénombrable.

Retrouver $\mathbf{N}^2$ dénombrable.

Existe-t-il une fonction continue de $\mathbf{R}$ dans $\mathbf{R}$ envoyant les rationnels dans les irrationnels et les irrationnels dans les rationnels ? ($\star$)

Montrer sans AC que les trois propositions suivantes sont équivalentes pour A quelconque :

(i) A contient un sous-ensemble infini dénombrable.

(ii) $\forall B$ dénombrable, $A \cup B$ équipotent à A.

(iii) A est en bijection avec une de ses parties propres.

Montrer que pour tout A, $\mathbf{N} \hookrightarrow A \Leftrightarrow \forall n \in \mathbf{N}, [\![1,n]\!] \hookrightarrow A$.

Soit E fini à n éléments. Soit A_1, ..., A_k parties de E tq $A_i \cap A_j \neq \emptyset$ pour tous $i \neq j$. Montrer que $k \leq 2^{n-1}$.

Soit $(A, +, \cdot)$ un anneau, ie un ensemble où $+$ et $\cdot$ ont les propriétés habituelles mais où l'on a pas le droit de diviser (exemples : $\mathbf{Z}$, $\mathbf{Z}/n\mathbf{Z}$, $\mathbf{Z}[X]$).

On appelle idéal de A tout $I \subset A$ tq :

(0) $0 \in I$

(i) Pour tous $x, y \in I$, on a $x + y \in I$

(ii) Pour tous $x \in I, \lambda \in A$, on a $\lambda \cdot x \in I$

I est dit propre si $I \neq A$.

Théorème 13 (Krull) *Pour tout idéal propre I de A, il existe un idéal propre maximal (pour l'inclusion) de A contenant I.*

4.2 Solutions

- Solution premier exercice, deuxième question :

Soit (A_n) suite d'ensembles dénombrables.

On écrit (avec AC) chaque A_n comme $\bigcup_{k \in \mathbf{N}} A_{n,k}$ avec $A_{n,k}$ fini pour tout n et tout k.

On pose $B_i = \bigcup_{0 \leq n \leq i} \bigcup_{0 \leq k \leq i} A_{n,k}$ pour tout $i \in \mathbf{N}$. La suite (B_i) est une suite croissante pour l'inclusion de parties finies.

Alors $\bigcup_{n \in \mathbf{N}} A_n = \bigcup_{i \in \mathbf{N}} B_i$ dénombrable.

- ... troisième question :

On écrit $\mathbf{N} \times \mathbf{N} = \bigcup_{n \in \mathbf{N}} \{n\} \times \mathbf{N}$.

- Solution du deuxième exercice :

Une telle fonction ne prendrait qu'un nombre dénombrable de valeurs donc par continuité serait constante, absurde.

- Solution du cinquième exercice :

On ne peut avoir à la fois un ensemble et son complémentaire.

- Solution du sixième exercice :

Utiliser Zorn. Pour prouver que l'union d'une chaîne d'idéaux propres est propre, utiliser qu'un idéal est propre si et seulement s'il ne contient pas 1 (vérification élémentaire).

Références :

www.normalesup.org/rpeyre/pro/popul/zorn.pdf (Rémi Peyre) : Lemme de Zorn et applications (en particulier preuves plus détaillées)

www.madore.org/david/math/bantar.pdf (?) : Preuve de Banach-Tarski

Pour la science n^{o}384, rubrique "Logique et Calcul" (Jean-Paul Delahaye) : Problème des chapeaux

www.alain.troesch.free.fr, rubrique "Devoirs", premier DS de l'année (Alain Troesch) : Preuve de $E^2 \sim E$