Université Claude Bernard–Lyon I
L1 de Mathématiques : Algèbre I
Année 2012–2013

Structures fondamentales

1° Logique

Calcul propositionnel

Une assertion (c'est-à-dire, une phrase syntaxiquement correcte) possède une « valeur de vérité » qui peut être *vrai* (V) ou *faux* (F). On adopte donc le *principe du tiers exclu*[1] : il n'y a pas d'autre valeur de vérité que V et F (cela pourrait être : « on ne sait pas »).

Si P et Q sont deux assertions, on en fabrique quatre nouvelles grâce aux « connecteurs » : ce sont non P, P et Q, P ou Q et $P \Rightarrow Q$, qui signifie : non(P) ou Q. Leur valeur de vérité, selon celle de P et de Q, est décrite par la « table de vérité » :

P	Q	non P	P et Q	P ou Q	$P \Rightarrow Q$
V	V	F	V	V	V
V	F	F	F	V	F
F	V	V	F	V	V
F	F	V	F	F	V

Un cinquième connecteur : on note $P \Leftrightarrow Q$ pour exprimer que P et Q ont les mêmes valeurs de vérité. On constate que $P \Leftrightarrow Q$ est vraie exactement lorsque $(P \Rightarrow Q)$ et $(Q \Rightarrow P)$.

On a, quelles que soient les assertions P, Q et R :

* P et (Q et R) $\Leftrightarrow$ (P et Q) et R ; P ou (Q ou R) $\Leftrightarrow$ (P ou Q) ou R ;
* P et (Q ou R) $\Leftrightarrow$ (P et Q) ou (P et R) ; P ou (Q et R) $\Leftrightarrow$ (P ou Q) et (P et R) ;
* non(P et Q) $\Leftrightarrow$ non(P) ou non(Q) ; non(P ou Q) $\Leftrightarrow$ non(P) et non(Q) ;
* non($P \Leftrightarrow Q$) $\Leftrightarrow$ P et non Q ;
* $P \Rightarrow Q \Leftrightarrow$ non$(Q) \Rightarrow$ non(P).

La *réciproque* de l'assertion $P \Rightarrow Q$ est l'assertion $Q \Rightarrow P$. Si on sait seulement si $P \Rightarrow Q$ est vraie ou pas (sans savoir si P et Q le sont), on ne peut pas savoir si $Q \Rightarrow P$ est vraie ou pas. La *contraposée* de $P \Rightarrow Q$ est : non$(Q) \Rightarrow$ non(P) : une implication et sa contraposées sont équivalentes.

Le connecteur $\Rightarrow$ *n'est pas* un raccourci typographique pour « donc » ; en effet, on peut vouloir démontrer ou utiliser le fait que $P \Rightarrow Q$ est vraie sans savoir si P est vraie ou pas. Au contraire, quand on écrit « P donc Q », cela signifie : « je sais que P est vraie ; j'en déduis que Q est vraie. » (Cette distinction est nécessaire pour comprendre pourquoi le raisonnement par récurrence démontre quelque chose.)

En revanche, pour *démontrer* que $P \Rightarrow Q$ est vraie, il est suffisant de montrer que si P est vraie, alors Q est vraie. (Il y a d'autres méthodes, voir plus loin.)

Quantificateurs

Étant donné une assertion $P(x)$ qui a un sens, dans un contexte donné, chaque fois que l'on remplace x par un élément d'un ensemble E donné, on fabrique deux assertions qui ne dépendent plus de rien, c'est-à-dire où x est une variable muette :

– l'assertion « $\forall x \in E,\ P(x)$ » signifie : pour toute valeur de $x \in E$, l'assertion $P(x)$ est vraie ;

1. Cela n'est pas neutre au plan épistémologique : les mathématiciens constructivistes rejettent l'axiome du tiers exclu (et donc le raisonnement par l'absurde, etc.).

– l'assertion « $\exists x \in E,\ P(x)$ » signifie : il existe au moins une valeur de $x \in E$ pour laquelle l'assertion $P(x)$ est vraie.

Négation : $\mathrm{non}(\forall x,\ P(x)) \Leftrightarrow \exists x,\ \mathrm{non}(P(x))$; $\mathrm{non}(\exists x,\ P(x)) \Leftrightarrow \forall x,\ \mathrm{non}(P(x))$.

La preuve d'une assertion de la forme $\forall x \in E,\ P(x)$ a (presque) toujours la structure suivante : « Soit $x \in E$. [...] Ainsi, $P(x)$ est vraie. » On sous-entend : « Comme x était quelconque au début, on a prouvé que pour toute valeur de x, $P(x)$ est vraie. »

Pour réfuter une assertion de la forme $\forall x \in E,\ P(x)$, on exhibe une valeur de $x_0 \in E$ pour laquelle $P(x_0)$ est fausse.

Pour prouver une assertion de la forme $\exists x \in E,\ P(x)$, on exhibe (ou on prouve par un théorème [2] l'existence d') une valeur $x_0 \in E$ pour laquelle $P(x_0)$ est vraie.

La réfutation d'une assertion de la forme $\exists x \in E,\ P(x)$ a (presque) toujours la structure suivante : « Soit $x \in E$. [...] Ainsi, $P(x)$ est fausse. » On prouve ainsi l'assertion : $\forall x \in E,\ \mathrm{non}(P(x))$.

Récurrence

Principe de récurrence : Soit $H(n)$ une assertion qui dépend d'une variable n et qui a un sens dans un contexte donné lorsqu'on remplace n par un entier naturel. On suppose que $H(0)$ est vraie et que, pour tout n, l'implication $H(n) \Rightarrow H(n+1)$ est vraie. Alors, $H(n)$ est vraie pour tout n.

En pratique, une preuve par récurrence se rédige commodément de la façon suivante :

– « Initialisation. Prouvons $H(0)$. [...] Ainsi, $H(0)$ est vraie.
– Hérédité. Soit $n \in \mathbb{N}$. Supposons que $H(n)$ est vraie. Alors [...] Donc $H(n+1)$ est vraie.
– Conclusion. Par récurrence, $H(n)$ est vraie pour tout n. »

À la fin du deuxième point, on a sous-entendu : « Comme n était quelconque, on a prouvé que $\forall n \in \mathbb{N},\ H(n) \Rightarrow H(n+1)$. » Pour la conclusion, on a sous-entendu : « On a prouvé que $H(0)$ était vraie et que $\forall n \in \mathbb{N},\ H(n) \Rightarrow H(n+1)$. Par le principe de récurrence, $H(n)$ est vraie pour tout entier n. »

Théorème de récurrence dite « forte ». Soit $H(n)$ une assertion qui dépend de n [et qui a un sens pour tout entier naturel n dans un contexte donné]. On suppose que $H(0)$ est vraie et que, pour tout n, l'implication $\big(H(0) \text{ et } H(1) \text{ et } \cdots \text{ et } H(n)\big) \Rightarrow H(n+1)$ est vraie. Alors, $H(n)$ est vraie pour tout n.

Rédaction typique :

– « Initialisation. Prouvons $H(0)$. [...] Ainsi, $H(0)$ est vraie.
– Hérédité. Soit $n \in \mathbb{N}$. Supposons que pour tout k compris entre 0 et n, $H(k)$ est vraie. Alors [...] Donc $H(n+1)$ est vraie.
– Conclusion. Par récurrence, $H(n)$ est vraie pour tout n. »

Modes de raisonnement

Soit à démontrer, sous des hypothèses H, une assertion C (conclusion). (Il s'agit donc, essentiellement, de prouver que $H \Rightarrow C$...) On peut citer, sans exhaustivité :

– Raisonnement direct : on part des hypothèses et, par déductions successives, on démontre la conclusion.
  Exemple : soit $q \in \mathbb{R}$, $q \neq 1$ et $n \in \mathbb{N}$, on note $s_n = \sum_{k=0}^{n} q^k$; pour prouver que $s_n = (q^{n+1}-1)/(q-1)$, on montre que $qs_n = q^{n+1} + s_n - 1$ et on en déduit la formule.

2. Le théorème des valeurs intermédiaires est un exemple de théorème dont la conclusion est l'existence d'une solution à une équation où l'on ne construit pas explicitement cette solution.

- Raisonnement par l'absurde : on suppose H et non(C), on travaille et on démontre une contradiction. (On prouve ainsi que H et non(C) est fausse, c'est-à-dire que sa négation non(H) ou C est vraie.)
- Raisonnement par contraposée : on suppose que non(C) est vraie, on travaille, et on prouve que non(H) est fausse.
- Raisonnement par récurrence (forte) : voir ci-dessus.
  Exemple : on peut montrer que $s_n = (q^{n+1} - 1)/(q - 1)$ pour tout n par récurrence.
- Disjonction des cas : on s'invente une hypothèse annexe H' dont on ne sait pas si elle est vraie ou fausse. On prouve d'abord que si H et H' sont vraies, alors C est vraie ; puis que H et non(H') est vraie, alors C est vraie. Cela prouve que si H est vraie, alors C est vraie.
  Exemple : on veut montrer que le carré de tout réel est positif ou nul. Soit x. L'hypothèse H est : $x \in \mathbb{R}$. On prend pour H' : $x \geq 0$. Si H' est vraie, le cours d'analyse (définition de $\mathbb{R}$) montre que $x^2 \geq 0$. Si H' est fausse, on écrit : $x^2 = (-x)^2 \geq 0$ car $-x > 0$.

2° Ensembles, applications

Ensembles

On ne définit pas ce qu'est un ensemble (bien incapable !). Lorsque x et E sont des objets mathématiques[3], on forme une assertion : $x \in E$, qu'on lit : « x *appartient à* E » ou « x est un élément de E ». La négation de cette assertion est notée : $x \notin E$.
Deux ensembles sont *égaux* s'ils ont les mêmes éléments : $E = F$ signifie : $\forall x,\ x \in E \iff x \in F$.
Il existe un ensemble vide noté $\emptyset$; il est caractérisé par la propriété : $\forall x,\ x \notin \emptyset$ (et il est unique).
On peut décrire un ensemble :
- en *extension*, en donnant la liste exhaustive de ses éléments : l'assertion $E = \{1, 3, 5\}$ signifie que pour tout x, on a : $x \in E \iff (x = 1$ ou $x = 3$ ou $x = 5)$; on a par ex. : $\{1, 3\} = \{3, 3, 1\}$;
- en *compréhension*, en donnant une propriété qui caractérise ses éléments : soit $P(x)$ une assertion dépendant d'une variable libre x, l'assertion $E = \{x,\ P(x)\}$ signifie que E a pour éléments les objets x tels que $P(x)$ soit vraie. Autrement dit : $\forall x,\ x \in E \iff P(x)$. Par exemple, si $P(x)$ est l'assertion : $(x \in \mathbb{Z}$ et $\exists k \in \mathbb{Z},\ x = 2k)$, l'ensemble correspondant est l'ensemble des entiers pairs.

Parties

Un ensemble F est appelé *partie* d'un ensemble E, ou que F est *inclus* ou *contenu* dans E, ou que E *contient* F si tout élément de F appartient à E, c'est-à-dire : $\forall x,\ x \in F \Rightarrow x \in E$. On note alors : $F \subset E$.
Critère d'égalité de deux ensembles : $E = F \iff (E \subset F)$ et $(F \subset E)$. Cela donne lieu à une méthode pour démontrer l'égalité de deux ensembles : on prouve que $E \subset F$ puis que $F \subset E$.

Pour tout ensemble E, il existe un ensemble noté $\mathcal{P}(E)$ dont les éléments sont les parties de E.

Opérations sur les ensembles

Soit E et F deux ensembles. La *réunion* de E et F est l'ensemble noté $E \cup F$ défini par : $\forall x,\ x \in E \cup F \iff (x \in E)$ ou $(x \in F)$. L'*intersection* de E et F est l'ensemble noté $E \cap F$ défini par : $\forall x,\ x \in E \cap F \iff (x \in E)$ et $(x \in F)$.
La *différence* de E et F est l'ensemble noté $E \backslash F$ défini par : $\forall x,\ x \in E \backslash F \iff (x \in E)$ et $(x \notin F)$.
Le *complémentaire d'une partie* A d'un ensemble E est la partie ${}^cA = E \setminus A$.
Relations : si E, F, G sont des ensembles, on a :

* $E \cap F = F \cap E$; $E \cup F = F \cup E$;

3. Ici, par « objet mathématique », on n'entend pas grand-chose de plus que des symboles.

* $E \cap (F \cap G) = (E \cap G) \cap G$; $E \cup (F \cup G) = (E \cup G) \cup G$;
* $E \cap (F \cup G) = (E \cap F) \cup (E \cap G)$; $E \cup (F \cap G) = (E \cup F) \cap (E \cup G)$;
* si E et F sont des parties d'un même ensemble : ${}^c(E \cup F) = {}^cE \cap {}^cF$; ${}^c(E \cap F) = {}^cE \cup {}^cF$;

Soit x et y. Le couple (x, y) est une ≪ liste ordonnée ≫[4] formée de deux éléments. Notation : (x, y), à distinguer de (y, x) si $x \neq y$. Le produit cartésien de deux ensembles E et F est l'ensemble des couples (x, y) où x est un élément de E et y un élément de F.
On définit par récurrence E^n pour E un ensemble et n un entier naturel non nul : $E^1 = E$; $E^2 = E \times E$; soit $n \in \mathbb{N}$, on suppose avoir défini E^n, alors $E^{n+1} = E \times E^n$. On peut vérifier que E^3 s'identifie (sens ?) aux triplets ordonnés d'éléments de E.

Relations
Une *relation* sur un ensemble E est une partie de $E \times E$. Si $\mathcal{R}$ est une relation et $x, y \in E$, on note $x\mathcal{R}y$ pour exprimer que $(x, y) \in \mathcal{R}$. On dit qu'une relation $\mathcal{R}$ est :
– *réflexive* si $\forall x \in E,\ x\mathcal{R}x$;
– *symétrique* si $\forall x, y \in E,\ x\mathcal{R}y \ \Rightarrow\ y\mathcal{R}x$;
– *anti-symétrique* si $\forall x, y \in E,\ (x\mathcal{R}y \text{ et } y\mathcal{R}x) \Rightarrow x = y$;
– *transitive* si $\forall x, y, z \in E,\ (x\mathcal{R}y \text{ et } y\mathcal{R}z) \Rightarrow x\mathcal{R}z$).
Une relation est appelée une *relation d'ordre* si elle est réflexive, anti-symétrique et transitive (≪ RAT ≫) et une *relation d'équivalence* si elle est réflexive, symétrique et transitive (≪ RST ≫).

Applications (fonctions)
Soit E, F deux ensembles. Une partie Γ de $E \times F$ est appelée *graphe d'application*[5] dans $E \times F$ si pour tout $x \in E$, il existe exactement un élément $y \in F$ tel que $(x, y) \in \Gamma$. Une application est la donnée de trois ensembles (E, F, Γ) où Γ est un graphe d'application dans $E \times F$.
Pour $x \in E$, on appelle *image* de x par f et on note $f(x)$ l'unique élément $y \in F$ tel que $(x, y) \in \Gamma$. Le *graphe* de f est : $\Gamma = \{(x, y) \in E \times F,\ y = f(x)\}$.
Autrement dit, l'application f est la donnée d'un ensemble de départ E, d'un ensemble d'arrivée F et d'un ensemble de couples $(x, f(x))$ où x parcourt E et $f(x)$ est un élément de F qui dépend de x. Notation :

$$f : \begin{array}{ccc} E & \longrightarrow & F \\ x & \longmapsto & f(x) \end{array} \qquad \text{ou} \qquad f : E \to F,\ x \mapsto f(x).$$

Pour la suite, on fixe une application $f : E \to F$.
On appelle *image directe* d'une partie A de E l'ensemble :

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

On appelle *image réciproque* d'une partie B de F l'ensemble :

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

On appelle *antécédent* d'un élément $y \in F$ par f tout élément $x \in E$ tel que $f(x) = y$.
Notation : $f^{-1}(y) = f^{-1}(\{y\})$ pour $y \in F$: c'est la partie de F dont les éléments sont les antécédents de y par f.

4. Codage en théorie des ensembles : $(x, y) = \{\{x\}, \{x, y\}\}$. Si $x = y$, on trouve : $(x, x) = \{\{x\}\}$; sinon, (x, y) est un ensemble à deux éléments, qui sont eux-mêmes des ensembles et permettent de retrouver x et y dans l'ordre.

5. On définit un *graphe de fonction* en remplaçant ≪ exactement un y ≫ par ≪ au moins un y ≫. C'est du pinaillage et on peut considérer les mots ≪ fonctions ≫ et ≪ applications ≫ comme synonymes.

Injections, surjections, bijections
On dit que l'application f est *injective* si tout élément de l'ensemble d'arrivée possède au plus un antécédent. En symboles (faire le lien entre les deux) :

$$\forall (x,x') \in E^2,\ f(x) = f(x') \ \Rightarrow\ x = x'.$$

On dit que l'application f est *surjective* si tout élément de l'ensemble d'arrivée possède au moins un antécédent. En symboles :

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

Reformulations de la surjectivité : $\forall y \in F,\ f^{-1}(y) \neq \emptyset$, ou encore : $f(E) = F$.
L'application f est *bijective* si elle est injective et bijective.

Supposons que f est bijective. Tout élément $y \in F$ possède un unique antécédent par f : on le note $f^{-1}(y)$. On définit ainsi une application $f^{-1} : F \to E$ appelée *application réciproque*. On a alors : $\forall (x,y) \in E \times F,\ y = f(x) \ \Leftrightarrow\ x = f^{-1}(y)$. Cela signifie que le graphe de f^{-1} est l'image de celui de f par la symétrique $\sigma : E \times F \to F \times E,\ (x,y) \mapsto (y,x)$ (si $E = F = \mathbb{R}$, σ est la symétrie par rapport à la première bissectrice des axes).
De plus, on a : $f^{-1} \circ f = \mathrm{Id}_E$ et $f \circ f^{-1} = \mathrm{Id}_F$, où Id_E est l'application « identité de E » : $\mathrm{Id}_E : E \to E,\ x \mapsto x$ et Id_F est définie de façon analogue. Enfin, f^{-1} est une bijection et $(f^{-1})^{-1} = f$.
Attention au conflit de notations $f^{-1}(y)$ qui a deux sens selon si f est ou n'est pas une bijection.

La composée de deux bijections $f : E \to F$ et $g : F \to G$ est une bijection $g \circ f : E \to G$ et on a : $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Cardinaux
On dit que deux ensembles E et E' sont *équipotents* ou qu'ils *ont le même cardinal* s'il existe une bijection de E sur E' ; on note alors : $E \simeq E'$. Soit E, E' et E'' trois ensembles, alors :
- on a : $E \simeq E$;
- si $E \simeq E'$, alors $E' \simeq E$ (la réciproque de $f : E \to E'$ est une bijection de E sur E') ;
- si $E \simeq E'$ et $E' \simeq E''$, alors $E \simeq E''$ (la composée de deux bijections en est une).

Lemme [6] : il existe une injection de E dans E' SSI il existe une surjection de E' sur E.
Un critère d'équipotence, le théorème de Cantor-Bernstein (admis) : s'il existe une injection de E dans E' et une injection de E' dans E, alors il existe une bijection de E sur E'.

Ensembles finis
Trichant un peu, on dit qu'un ensemble E est *fini* s'il existe un entier n tel que $E \simeq \{1, \ldots, n\}$. (On convient que pour $n = 0$, $\{1, \ldots, n\} = \emptyset$.)
Principe des tiroirs : pour aucun entier n, il n'existe d'injection de $\{1, \ldots, n+1\}$ dans $\{1, \ldots, n\}$ (c'est-à-dire : pour tout n et pour toute application $f : \{1, \ldots, n+1\} \to \{1, \ldots, n\}$, il existe k et k' dans $\{1, \ldots, n+1\}$ tels que $f(k) = f(k')$ et $k \neq k'$; en termes imagés : si on range $n+1$ objets dans n tiroirs, au moins un des tiroirs ($f(k)$) contient au moins deux objets (k et k').)
Corollaire : si $n < p$, il n'existe pas d'injection $\{1, \ldots, p\}$ dans $\{1, \ldots, n\}$.
Par suite, si un ensemble E est fini, il existe un unique n tel que $E \simeq \{1, \ldots, n\}$. On appelle cet entier n le cardinal de E ; notation : $n = \operatorname{card} E$.
Propriété importante : si E et F sont deux ensembles finis *de même cardinal* et f est une application de E dans F, alors f est injective SSI f est surjective SSI f est bijective.

6. Ce lemme n'est pas neutre du point de vue épistémologique : il utilise l'axiome du choix.

Dénombrabilité

Lemme : si un ensemble E n'est pas fini, il existe une injection de $\mathbb{N}$ dans E.
On dit qu'un ensemble infini E est *dénombrable* s'il existe une bijection de E sur $\mathbb{N}$.
Exemples d'ensembles dénombrables : $\mathbb{N}$, $\mathbb{N}^*$, $\mathbb{Z}$, $\mathbb{N}^2$, $\mathbb{Q}$.
Exemples d'ensembles non dénombrables : $\mathcal{P}(\mathbb{N})$, $\mathbb{R}$, $\mathbb{R}^2$, $\mathcal{P}(\mathbb{R})$...

Dénombrements

La *factorielle* $n!$ d'un entier naturel n est définie par récurrence par : $0! = 1$ et, pour tout n entier naturel, $(n+1)! = n! \times (n+1)$.
Théorème. Soit E et F deux ensembles de cardinaux finis respectifs n et p. Alors :

(i) On a : $\mathrm{card}(E \cup F) = \mathrm{card}(E) + \mathrm{card}(F) - \mathrm{card}(E \cap F)$.

(ii) On a : $\mathrm{card}(E \times F) = \mathrm{card}(E)\,\mathrm{card}(F)$.

(iii) Soit F^E l'ensemble des applications de E dans F. Alors : $\mathrm{card}(F^E) = \mathrm{card}(F)^{\mathrm{card}(E)} = p^n$.

(iv) Le nombre d'applications *injectives* de F dans E est :

$$\mathbf{A}_n^p = \begin{cases} \dfrac{n!}{p!} = n(n-1)\cdots(n-p+1) & \text{si } 0 \leq p \leq n \\ 0 & \text{si } p > n, \end{cases}$$

(v) En particulier, le nombre de bijections de E dans E est : $n!$.

(vi) Le nombre de parties à p éléments de E est :

$$\binom{n}{p} = \begin{cases} \dfrac{n!}{p!(n-p)!} & \text{si } 0 \leq p \leq n. \\ 0 & \text{si } p > n. \end{cases}$$