Logique et ensembles

PCSI 2 Lycée Pasteur

17 septembre 2007

La logique est un domaine un peu à part au sein des mathématiques, qui sous-tend l'ensemble de la construction tout en en faisant partie. À notre petit niveau, nous nous contenterons de la voir comme une sorte de syntaxe de tout le langage mathématique. Pour bien comprendre le sens exact que l'on attribue à chaque énoncé que contient un texte mathématique, il est important de s'appuyer sur des bases rigoureuses.

1 Éléments de logique

1.1 Propositions, valeurs de vérité

Définition 1. Une proposition mathématique est un énoncé mathématique (ou non) pouvant être vrai ou faux. On note usuellement V et F (V comme vrai et F comme faux) les deux valeurs de vérité pouvant être prises par une proposition .

Exemples :
- « Le nombre π est un nombre entier » est une proposition mathématique fausse.
- « La terre est ronde » est une proposition habituellement considérée comme vraie bien que ce soit approximatif (et que sphérique soit un terme plus adapté que ronde).
- « Il pleut » est une proposition dont la vérité dépend du contexte mais facile à déterminer une fois ce contexte précisé.
- « Le prof de maths est sympa » est une proposition dont la valeur de vérité est subjective, et qui n'a donc pas grand sens mathématique.

En mathématiques, on s'efforcera la plupart du temps de ne considérer que des propositions qui s'appuient sur des objets suffisamment bien définis pour qu'on puisse leur associer une valeur de vérité de façon incontestable. Il existe toutefois quelques types de propositions un peu particulières :

Définition 2. Un axiome est une proposition qu'on admet comme étant vraie, et qui est à la base d'une théorie mathématique. Une conjecture est une proposition dont on soupçonne fortement la véracité mais qu'on n'a pas encore réussi à prouver.

Exemples
- Euclide a défini dans son livre *Les Éléments* les bases de la géométrie du plan en s'appuyant sur un certain nombre d'axiomes dont le plus célèbre est « Par un point donné passe une et une seule droite parallèle à une droite donnée ». Cet axiome ne peut pas se démontrer, il n'est d'ailleurs pas forcément vrai si on ne travaille pas dans le plan (sur une sphère, par exemple, deux droites ne sont jamais parallèles).
- La conjecture de Goldbach stipule que tout nombre pair (plus grand que 2) peut s'écrire comme une somme de deux nombres premiers. Bien qu'on soupçonne très fortement qu'elle soit vraie, elle résiste depuis plusieurs siècles aux assauts des mathématiciens.

La plupart des autres types d'énoncés que vous croiserez dans le cours de cette année sont des énoncés vrais : théorèmes, corollaires, lemmes, ou ce que j'appelle propositions. Tous sont démontrés (à partir d'axiomes que je me garderai bien d'expliciter, c'est beaucoup plus compliqué que ça n'en a l'air). Mais qu'est-ce qu'une preuve ? C'est une suite d'affirmations logiquement équivalentes qui permet de passer d'une proposition (l'hypothèse) à une autre (la conclusion). Si l'on sait que l'hypothèse est vraie, la conclusion le sera aussi. Reste à définir précisément ce qu'est l'équivalence logique.

Définition 3. Deux propositions A et B sont logiquement équivalentes si elles prennent toujours la même valeur de vérité. On le note $A \equiv B$.

1.2 Opérations logiques

À partir d'une ou de deux propositions, on est souvent amené en mathématiques à en construire de nouvelles.

Définition 4. Soit A une proposition, alors la proposition « non A » (notée $\rceil A$) est la négation de la proposition A. Elle prend la valeur de vérité opposée à celle de A.

Exemple : La négation de la proposition « 5 est pair » est la proposition « 5 est impair ».

Remarque 1. La proposition $\rceil(\rceil A)$ est logiquement équivalente à A.

Définition 5. À partir de deux propositions A et B, on peut construire les propositions « A et B », notée $A \wedge B$, qui est vraie lorsque A et B sont simultanément vraies, et « A ou B », notée $A \vee B$, qui est vrai dès qu'au moins une des deux propositions A et B est vraie.

Une autre façon de voir les choses est de former des tables de vérité :

Remarque 2. On peut aussi définir le ou à partir du et du non : $A \vee B \equiv \rceil(\rceil A \wedge \rceil B)$. Notons par ailleurs que le ou logique est un ou inclusif (les deux propositions peuvent être vraies simultanément) alors que le ou du langage courant est parfois exclusif (exemple classique, on vous propose au restaurant fromage ou dessert, il serait incongru d'essayer de manger des deux).

Proposition 1. On a les équivalences logiques suivantes :
- $(A \wedge A) \equiv A \equiv (A \vee A)$
- Les symboles $\wedge$ et $\vee$ sont commutatifs et associatifs, et distributifs l'un par rapport à l'autre.
- $A \vee \rceil A$ est toujours vraie (principe du tiers exclus).
- $\rceil(A \wedge B) \equiv \rceil A \vee \rceil B$ et $\rceil(A \vee B) \equiv \rceil A \wedge \rceil B$ (lois de de Morgan).

Démonstration. Pour la première propriété, il suffit de constater que $A \wedge A$ et $A \vee A$ sont vraies quand A est vraie, et fausses quand A est fausse. La commutativité des symboles découle de la symétrie de la table de vérité, l'associativité est évidente ($A \wedge B \wedge C$ est vrai uniquement si A, B et C sont vraies simultanément, ce qui ne dépend pas de l'ordre dans lequel on construit la proposition ; de même, $A \vee B \vee C$ est fausse uniquement si les trois propositions sont fausses). Le tiers exclus dit simplement la chose suivante : soit A, soit elle est fausse, auquel cas $\rceil A$ est vraie. Dans les deux cas, $A \vee \rceil A$ est vraie. Enfin, $\rceil A \vee \rceil B$ est fausse uniquement si $\rceil A$ et $\rceil B$ sont fausses, donc uniquement si A et B sont vraies, c'est-à-dire si $A \wedge B$ est vraie. On a donc bien $\rceil(A \wedge B) \equiv \rceil A \vee \rceil B$. □

Remarque 3. On parle parfois de conjonction pour désigner une proposition de la forme $A_1 \wedge \cdots \wedge A_n$ et de disjonction pour une proposition de la forme $A_1 \vee \ldots A_n$.

Exemple : Rien de très compliqué ici. La proposition « n est un nombre pair **ou** n est un nombre impair » est par exemple toujours vraie si n est un entier.

Définition 6. Soient A et B deux propositions logiques, alors la proposition $A \Rightarrow B$ (A implique B) est définie par $A \Rightarrow B \equiv \rceil A \vee B$. La proposition $A \Leftrightarrow B$ (A équivaut à B) est définie par $A \Rightarrow B \equiv (A \Rightarrow B) \wedge (B \rightarrow A)$.

Autrement dit, on a les tables de vérité suivantes :

Exemples : Les implications et équivalences sont les formes sous lesquelles on exprime implicitement la plupart des résultats d'un cours de maths, par exemple « Si une fonction est dérivable, elle est continue » (implication) ou « Un triangle de côtés respectifs a, b, c, avec $c \geqslant a$ et $c \geqslant b$ est rectangle ssi $c^2 = a^2 + b^2$ » (équivalence).

Attention tout de même, on a tendance dans le langage courant à supposer un lien de cause à effet dans les implications qui n'existe pas nécessairement en logique pure. La proposition « 2 est pair $\Leftrightarrow$ la dérivée de la fonction sinus est la fonction cosinus » est logiquement vraie. Autre particularité à retenir : une implication dont la prémisse (ce qui est à gauche) est fausse est toujours vraie, quelle que soit sa conclusion. Ainsi « 2 est impair $\Rightarrow$ la terre est carrée » est logiquement vraie.

Définition 7. La réciproque d'une implication logique $A \Rightarrow B$ est la proposition $B \Rightarrow A$. La contraposée d'une implication logique $A \Rightarrow B$ est la proposition $\rceil B \Rightarrow \rceil A$.

Proposition 2. Une implication et sa contraposée sont logiquement équivalentes.

Démonstration. En utilisant les résultats précédents, $(\rceil B \Rightarrow \rceil A) \equiv (B \vee \rceil A) \equiv (A \vee \rceil B) \equiv (A \Rightarrow B)$. □

Remarque 4. Il est évidemment très important de ne pas confondre réciproque et contraposée. La contraposition est souvent une façon utile de reformuler un résultat en vue d'une démonstration, par exemple « Tout nombre premier supérieur à 2 est impair ». La contraposée stipule que « Tout nombre pair supérieur à 2 n'est pas premier », ce qui est évident. NOtons au passage que pour prouver une équivalence, on démontre presque systématiquement les deux implications séparément.

Exemple : Il faut encore une fois faire attention, tenter de contraposer dans le langage courant donne souvent des résultats curieux. Prenons l'implication « S'il pleut, alors je prends mon parapluie ». Sa contraposée est la proposition « Si je ne prends pas mon parapluie, alors il ne pleut pas », qui est logiquement vraie (si je ne prends pas mon parapluie, c'est nécessairement qu'il ne pleut pas, puisque s'il pleuvait j'aurais pris mon parapluie, il faut juste éviter de voir un lien de cause à effet entre les deux).

Proposition 3. On a transitivité de l'implication et de l'équivalence, c'est-à-dire que $(A \Rightarrow B) \wedge (B \Rightarrow C) \Rightarrow (A \Rightarrow C)$ et $(A \Leftrightarrow B) \wedge (B \Leftrightarrow C) \Rightarrow (A \Leftrightarrow C)$

Démonstration. La conjonction de gauche est vraie seulement dans les cas ou A est fausse ou C est vraie. En effet, soit B est vraie, et il faut que C soit vraie, soit B est fausse et il faut que A soit fausse. Dans les deux cas, l'implicaion de droite sera vraie, donc l'implication globale est vraie. C'est encore plus facile pour les équivalences : la conjonction de gauche est vraie seulement si les trois propositions A, B et C sont logiquement équivalentes, mais dans ce cas, A et C le sont certainement ! □

1.3 Quantificateurs

Définition 8. Un prédicat $A(x)$ de référentiel E est une proposition faisant intervenir une variable x susceptible de varier à l'intérieur d'un ensemble E (plus précisement, le prédicat n'est une proposition qu'une fois x remplacé par un élément de E, ce qui permet de lui associer une valeur de vérité).

Exemple : « x est pair » est un prédicat dont le référentiel est l'ensemble $\mathbb{Z}$.

Définition 9. À tout prédicat $A(x)$ on associe les deux propositions $\forall x \in E\ A(x)$, qui est vraie si et seulement si les prositions $A(x)$ obtenues en remplaçant x par n'importe quel élément de E sont toutes vraies, et $\exists x \in E\ A(x)$, qui est vraie si et seulement si on peut trouver une valeur de x dans E rendant la proposition $A(x)$ vraie. Les symboles $\forall$ et $\exists$ sont appelés respectivement quantificateur universel et quentificateur existentiel (ils se lisent « quel que soit » et « il existe »).

Exemples : La proposition « $\forall x \in \mathbb{R}\ x^2 \geqslant 0$ » est vraie. La proposition « $\exists x \in \mathbb{Z}\ x^2 = 2$ » est fausse.

Proposition 4. On a $\rceil(\forall x \in E\ A(x)) \equiv (\exists x \in E,\ \rceil A(x))$ et $\rceil(\exists x \in E\ A(x)) \equiv (\forall x \in E,\ \rceil A(x))$.

Par ailleurs $(\forall x \in E\ A(x) \wedge B(x)) \equiv (\forall x \in E\ A(x)) \wedge (\forall x \in E\ B(x))$ et $(\exists x \in E\ A(x) \vee B(x)) \equiv (\exists x \in E\ A(x)) \vee (\exists x \in E\ B(x))$.

Démonstration. Ces résultats sont très intuitifs, on n'en donnera pas de démonstration formelle. □

Remarque 5. Attention, ces propriété sont à peu près les seules à être vraies sur les quantificateurs, il est très dangereux d'essayer d'en utiliser d'autres. De même, les inversions de quantificateurs sont à manipuler avec énormément de précaution.

Définition 10. Un exemple est une valeur de x pour laquelle un prédicat $A(x)$ est vrai. L'exemple permet de prouver des résultats de la forme $\exists x \in E\ A(x)$ (mais ne prouvera jamais un prédicat universel). Un contre-exemple est une valeur de x pour laquelle un prédicat $A(x)$ est faux. Le contre-exemple permet de prouver qu'un énoncé de la forme $\forall x \in E\ A(x)$ est faux.

1.4 Exemples de raisonnements mathématiques

Démonstration d'une implication On suppose la prémisse (ce qui se trouve à gauche de l'implication) vraie (si elle est fausse, l'implication sera de toute façon vérifiée) et on essaie d'aboutir à la vérité de la conclusion (ce qui se trouve à droite).

Montrons par exemple la proposition $x \geqslant 2 \Rightarrow x^2 - 3x + 2 \geqslant 0$. Supposons donc $x \geqslant 2$. On a alors $x - 2 \geqslant 0$ et $x - 1 \geqslant 0$, donc $(x-2)(x-1) = x^2 - 3x + 2 \geqslant 0$. On n'a aucune raison de s'intéresser aux cas où $x < 2$.

Démonstration d'une équivalence On procède généralement par doucle implication.

Exemple : on veut démontrer que $x \in \mathbb{Q} \Leftrightarrow (\exists p \in \mathbb{Z}, px \in \mathbb{N})$. En effet, si un tel entier p existe, alors on a $px = q$, donc $x = \dfrac{q}{p}$, avec p et q entiers (si jamais $q = 0$, $x = 0$ aussi, donc ça marche toujours), donc $x \in \mathbb{Q}$. Réciproquement, si $x \in \mathbb{Q}$, x peut s'écrire sous la forme $\dfrac{q}{p}$, où $q \in \mathbb{Z}$ et $p \in \mathbb{N}$ et on a bien $px \in \mathbb{N}$.

Démonstration d'un prédicat existentiel Il suffit d'exhiber un exemple vérifiant le prédicat.

Exemple : on veut démontrer $\exists f : \mathbb{R} \to \mathbb{R}, f'(x) = \cos x$. Il suffit de remarquer que la fonction sin vérifie $f' = \cos$ (si on cerchait à trouver toutes les fonctions vérifiant ce résultat, ce serait une autre histoire, mais ce n'est pas le cas ici).

Démonstration d'un prédicat universel La démonstration de ce type de prédicat commence à peu près systématiquement par une phrase du type « Soit $x \in E$ ». Il s'agit en effet de montrer une propriété pour une valeur quelconque choisie dans l'ensemble E.

Exemple : on veut démontrer $\forall n \in \mathbb{N}^*, \displaystyle\int_n^{n+1} \frac{1}{x}\, dx \leqslant \frac{1}{n}$. Soit $n \in \mathbb{N}^*$. on a $\forall x \in [n, n+1], \dfrac{1}{n+1} \leqslant \dfrac{1}{x} \leqslant \dfrac{1}{n}$, donc $\displaystyle\int_n^{n+1} \frac{1}{x}\, dx \leqslant \int_n^{n+1} \frac{1}{n}\, dx = \frac{n+1-n}{n} = \frac{1}{n}$.

Démonstration par l'absurde C'est un type particulier de démonstration où on suppose le résultat faux. On cherche à démontrer à partir de hypothèse une proposition dont on sait qu'elle est fausse. On en déduit alors que notre hypothèse ne peut être que vraie (puisqu'elle implique une absurdité).

Un exemple classique : on va démontrer par l'absurde qu'il existe une infinité de nombre premiers (démonstration due à Euclide). Supposons donc le contraire, c'est-à-dire qu'il n'y en ait qu'un nombre fini, et notons-les $p_1, p_2, \dots, p_n$. Considérons alors l'entier $p_1 p_2 \dots p_n + 1$. Il ne peut pas être divisible par p_1 puisque le reste de sa division par p_1 vaut 1 par construction. De même il n'est divisible par aucun nombre premier de notre liste. Il peut cependant, comme tout nombre entier, s'écrire comme un produit de nombres premiers (éventuellement réduit à lui-même). Ceux-ci ne feront alors pas partir de notre liste, ce qui prouve que notre hypothèse de départ est absurde. Il y a donc une infinité de nombres premiers.

Un autre exemple pour la route : montrons que $\sqrt{2}$ est irrationnel. On suppose le contraire, c'est-à-dire que $\sqrt{2} = \frac{p}{q}$, avec pgcd $(p, q) = 1$ (on peut toujours faire cette supposition supplémentaire, quitte à rendre la fraction irréductible). On a alors en élevant au carré $2 = \frac{p^2}{q^2}$, d'où $p^2 = 2q^2$. Or, un entier dont le carré est pair est aussi pair (ça se démotre facilement par contraposée : si n est impair, n^2 est un produit de deux impairs, donc impair). On en déduit que $p = 2p'$, avec $p' \in \mathbb{N}$. Mais alors $p^2 = 4p'^2$ et $q^2 = \frac{1}{2}p^2 = 2p'^2$. L'entier q est alors également pair (pour la même raison que p l'était), et la fraction $\frac{p}{q}$. Cela est en contradiction avec notre hypothèse, qui est donc absurde. Le nombre $\sqrt{2}$ est donc irrationnel.

Démonstration par analyse et synthèse Un nom un peu compliqué pour un type de raisonnement assez particulier, qui intervient lorsqu'on veut démontrer l'existence de certains objets. On commence par étudier les propriétés de l'objet en question en supposant qu'il existe, jusqu'à en déduire la ou les seules valeurs qu'il peut prendre. Il suffit ensuite de vérifier si ces valeurs vérifient en effet les propriétés attendues ou non.

Exemple : on veut démontrer que tout fonction $f : \mathbb{R} \to \mathbb{R}$ peut s'écrire comme somme d'une fonction paire et d'une fonction impaire. Supposons donc $f = g + h$, avec g paire et h impaire. On a donc $g(-x) = g(x)$ et $h(-x) = -h(x)$ pour tout réel x. On a alors, en faisant la somme de $f(x)$ et de $f(-x)$, $2g(x) = f(x) + f(-x)$, donc g est nécessairement la fonction $x \mapsto \frac{f(x) + f(-x)}{2}$. De même, en faisant la différence de $f(x)$ et de $f(-x)$, on obtient $h : x \mapsto \frac{f(x) - f(-x)}{2}$. Il suffit maintenant de vérifier que les deux fonxtions qu'on vient de définir conviennent. Elles sont bien respectivement paire et impaire, et leur somme vaut bien f. La proposition est donc démontrée. On a même démontré l'unicité de la décomposition au passage.

2 Ensembles

Les ensembles sont les objets les plus basiques que l'on puisse manipuler en mathématiques. En effet, tout objet mathématique est un ensemble, auquel on ajoute éventuellement d'autre propriétés qui en font une fonction, une matrice ou plus simplement un entier (oui, un entier est un ensemble comme un autre, même si je ne m'étendrai pas là-dessus ici). Et pourtant, on ne définit jamais ce qu'est un ensemble mathématique. En effet, la notion d'ensemble est tellement élémentaire qu'on ne pas s'appuyer sur une autre notion pour la décrire.

2.1 Définitions

Définition 11. Un ensemble E est une collection d'objets. On peut définir un ensemble mathématique par extensionnalité, c'est-à-dire en nommant tous les objets le constituant, par exemple $E = \{4; 5; 6; 7; 8\}$ ou par compréhension, c'est-à-dire en caractérisant ses éléments par une propriété commune, par exemple $E = \{n \in \mathbb{N} \mid 4 \leqslant n \leqslant 8\}$. Ce deuxième type de définition fait souvent intervenir un autre ensemble. On utilisera toujours le symbole | pour signifier « tels que ».

Définition 12. Deux ensemble sont égaux s'ils sont constitués des mêmes éléments. Un ensemble E est inclus dans un ensemble F si tous les éléments de E appartiennent à F, ce qu'on note $E \subset F$. On dit aussi que E est un sous-ensemble de F, et on parle de sous-ensemble propre lorsqu'en plus $E \neq F$.

Remarque 6. Pour prouver que $E \subset F$, on considère généralement un élément quelconque de E, et on essaie de prouver qu'il appartient à F. Pour montrer l'égalité de deux ensembles, on procèdera souvent par double inclusion : on prouve séparément $E \subset F$ et $F \subset E$.

Définition 13. L'ensemble ne contenant aucun élément, appelé ensemble vide, est noté $\emptyset$.

Définition 14. Soient A et B deux ensembles inclus dans un même ensemble E. On définit l'ensemble A union B par $A \cup B = \{x \in E \mid x \in A \,\mathbf{ou}\, x \in B\}$; l'ensemble A inter B par $A \cap B = \{x \in E \mid x \in A \,\mathbf{et}\, x \in B\}$, et le complementaire de A par $\overline{A} = \{x \in E \mid x \notin A\}$. Plus généralement, on peut définir le complémentaire de B dans A par $A \backslash B = \{x \in A \mid x \notin B\} = A \cap \overline{B}$.

Proposition 5. Les propriétés suivantes devraient vous rappeler celles vues dans la première partie de ce cours sur les opérateurs logiques :

- $A \cup A = A \cap A = A$
- Les opérations $\cap$ et $\cup$ sont commutatives, associatives, et distributives l'une par rapport à l'autre. L'ensemble vide est un élément neutre pour l'opération d'union.
- $\overline{A \cup B} = \overline{A} \cap \overline{B}$ et $\overline{A \cap B} = \overline{A} \cup \overline{B}$ (lois de de Morgan).

Démonstration. La première propriété, ainsi que la commutativité et l'associativité des opérations, sont évidentes. Montrons que $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. Soit $x \in A \cap (B \cup C)$, on a donc $x \in A$ et soit $x \in B$, soit $x \in C$. dans le premier cas, $x \in A \cap B$, dans le deuxième $x \in A \cap B$, donc dans les deux cas $x \in (A \cap B) \cup (A \cap C)$, donc la première inclusion est vraie. Dans l'autre sens, si $x \in (A \cap B) \cup (A \cap C)$, on a soit $x \in A \cap B$, soit $x \in A \cap C$. Dans les deux cas, $x \in A$, et x appartient à l'un des deux ensembles B et C, donc $x \in A \cap (B \cup C)$, ce qui montre la deuxième inclusion. La deuxième propriété de distributivité se montre de façon similaire.

Enfin, les lois de De Morgan découlent des lois du même nom sur les opérations logiques. $\square$

Définition 15. Une partition d'un ensemble E est un ensembles de sous-ensembles A_1, ..., A_n de E tels que $\bigcup_{i=1}^{n} A_i = E$ et $\forall (i,j) \in \{1; \dots; n\}^2$, $A_i \cap A_j = \emptyset$. Autrement dit, tout élément de E appartient à un et un seul des ensembles A_i.

Exemple : Si on note $A = \{n \in \mathbb{N} \mid n \text{ est pair }\}$ et $B = \{n \in \mathbb{N} \mid n \text{ est impair }\}$, les ensembles A et B forment une partition de $\mathbb{N}$.

Définition 16. Le produit cartésien de deux ensembles E et F est l'ensemble constitué de tous les couples d'éléments (x, y), avec $x \in E$ et $y \in F$. On le note $E \times F$.

Remarque 7. Les notations sont très importantes : l'ensemble $\{2; 3\}$ est constitué de deux éléments (les entiers 2 et 3), alors que l'ensemble $\{(2, 3)\}$ est constitué d'un seule élément, la paire d'entiers $(2, 3)$.

Remarque 8. On peut très bien définir une union, une intersection ou un produit cartésien de plus de deux ensembles, en gardant les mêmes notations. On peut même généraliser sans difficulté à une union ou une intersection d'une infinité de sous-ensembles, on parle alors d'une famille de sous-ensembles et on note $\bigcup_{i \in I} A_i$ et $\bigcap_{i \in I} A_i$.

Remarque 9. Lorsque $E = F$, on note E^2 plutôt que $E \times E$, et plus généralement $\underbrace{E \times E \times \cdots \times E}_{n \text{ fois}} = E^n$.

Définition 17. L'ensemble des parties d'un ensemble E, noté $\mathcal{P}(E)$, est l'ensemble dont les éléments sont les sous-ensembles de E.

Exemple : Si $E = \{1; 2; 3\}$, $\mathcal{P}(E) = \{\emptyset; \{1\}; \{2\}; \{3\}; \{1; 2\}; \{1; 3\}; \{2; 3\}; \{1; 2; 3\}\}$.

2.2 Applications

Une application est en gros ce que vous avez l'habitude d'appeler une fonction (mais on n'utilise pas ce terme en théorie des ensembles, il y a en fait de subtiles distinctions).

Définition 18. Une application est la donnée d'un ensemble E, appelé ensemble de départ, d'un ensemble F appelé ensemble d'arrivée, et d'un sous-ensemble G de $E \times F$, appelé graphe, vérifiant la propriété suivante : $\forall x \in E, \exists ! y \in F, (x, y) \in G$.

Remarque 10. Cette définition est affreusement formelle. En pratique, si $x \in E$, on note $f(x)$ l'unique élément de F tel que $(x, y) \in G$, et on a bien défini une fonction de E dans F, qu'on notera comme on en a l'habitude $f : E \to F$ ou $E \xrightarrow{f} F$.

Exemple : L'application $x \to x$, définie sur un quelconque ensemble E, est appelée application idéntité, notée id_E.

Définition 19. On note $\mathcal{F}(E, F)$ ou E^F l'ensemble des applications de E dans F.

Remarque 11. Deux applications sont identiques si elles ont même ensemble de départ, ensemble d'arrivée et graphe. Par exemple, les fonctions d'une variable réelle $f : x \mapsto x - 4$ et $g : x \mapsto \dfrac{x^2 - 5x + 4}{x - 1}$ sont différentes, même si elles coïncident sur $\mathbb{R}\backslash\{1\}$: elles n'ont pas le même ensemble de définition.

Définition 20. Soit $f : E \to F$ une application et E' un sous-ensemble de E. L'application $g : E' \to F$ définie par $\forall x \in E'$, $g(x) = f(x)$ est appelée restriction de f au sous-ensemble E' et notée $f_{|E'}$. On dit egalement que f est un prolongement de f à E.

Exemple : La fonction $x \to x \ln x$, définie sur R_+^*, peut se prolonger en une fonction $\tilde{f}$ définie et continue sur R_+ en posant $\tilde{f}(0) = 0$. En pratique, on utilise souvent la même notation pour désigner le prolongement que pour la fonction d'origine, même si c'est un abus de notation.

Définition 21. Soient $f : E \to F$ et $g : F \to G$ deux applications, alors la composée de g et de f est l'application $g \circ f : E \to G$ définie par $g \circ f(x) = g(f(x))$.

Remarque 12. La composition n'est bien sûr pas commutative ; en général, $f \circ g$ n'est même pas définie quand $g \circ f$ l'est. Par contre, la composition est une opération associative. Par ailleurs, l'application identité est un élément neutre pour la composition.

Exemple : On considère les fonctions $f : \mathbb{R} \to \mathbb{R}_+$ et $g : \mathbb{R}_+ \to \mathbb{R}$ définies par $f(x) = x^2$ et $g(x) = \sqrt{x}$; alors $g \circ f(x) = |x|$ et $f \circ g(x) =^x$ (la première composée étant définie sur $\mathbb{R}$ et la deuxième sur $\mathbb{R}_+$.

Définition 22. Soit $f : E \to F$ une application, f est dite injective si $\forall (x, x') \in E^2, f(x) = f(x') \Rightarrow x = y$; f est dite surjective si $\forall y \in F, \exists x \in E, f(x) = y$; enfin, f est dite bijective si elle est à la fois injective et surjective.

Remarque 13. Autrement dit, f est injective si tout élément de F a au plus un antécédent par f, surjective si tout élément de F a au moins un antécédent de F, et bijective si tout élément de F a exactement un antécédent par f. Par contraposition, on peut aussi définir une application injective de la façon suivante : $x \neq x' \Rightarrow f(x) \neq f(x')$.

Proposition 6. Soient $f : E \to F$ et $g : F \to G$ deux applications. Si f et g sont injectives alors $g \circ f$ est injective. Si f et g sont surjectives, alors $g \circ f$ est surjective.

Démonstration. Supposons g et f injectives, et soient $x, x' \in E^2$ tels que $g(f(x)) = g(f(x'))$. Par injectivité de g, on a alors nécessairement $f(x) = f(x')$, puis par injectivité de f, $x = x'$, ce qui prouve l'injectivité de $g \circ f$. Supposons désormais g et f surjectives et soit $z \in G$. Par surjectivité de g, $\exists y \in F$, $z = g(y)$, puis par surjectivité de f, $\exists x \in E$, $y = f(x)$. Mais alors $z = g \circ f(x)$, donc z a un antécédent par $g \circ f$, ce qui prouve sa surjectivité. $\square$

Remarque 14. La réciproque de ces propriétés est totalement fausse, voir la feuille d'exerices pour quelques exemples.

Proposition 7. Une application $f : E \to F$ est bijective si et seulement si il existe $g : F \to E$ telle que $g \circ f = id_E$ et $f \circ g = id_F$. L'application g est alors appelée bijection réciproque de f (ou réciproque tout court) et notée f^{-1}.

Remarque 15. Cette réciproque, bien que notée f^{-1}, n'a rien à voir avec la fonction inverse de f, que pour cette raison on notera toujours $\frac{1}{f}$. Notons au passage que f^{-1} est effectivement bijective, de réciproque f.

Démonstration. Supposons f bijective et soit $y \in F$. Il existe un unique antécédent x de y par f, on pose $g(y) = x$. On a alors par construction $f \circ g(x) = x$, donc $f \circ g = id_F$. De plus, si $x \in E$, $g(f(x))$ est un antécédent de $f(x)$, mais comme il n'y en qu'un ça ne peut être que x, donc on a aussi $g \circ f = id_E$.

Réciproquement, si $g \circ f = id_E$ et $f \circ g = id_F$, considérons x et x' tels que $f(x) = f(x')$, on a alors $g \circ f(x) = g \circ f(x')$, donc $x' = x$, ce qui prouve l'injectivité de f. Soit maintenant $y \in F$, alors $g(y)$ est un antécédent de y par f puisque $f \circ g(y) = y$, donc f est sujective. L'application f est donc bijective. □

Proposition 8. Soient $f : E \to F$ et $g : F \to G$ deux applications bijectives, alors $g \circ f : E \to G$ est une application bijective et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Démonstration. f et g étant à la fois injectives et surjectives, $g \circ f$ est à la fois injective et surjective (cf plus haut) donc bijective. De plus, $\forall x \in E$, $f^{-1} \circ g^{-1} \circ g \circ f(x) = f^{-1}(g^{-1} \circ g)(f(x)) = f^{-1}(f(x)) = x$ et de même $\forall x \in G$, $g \circ f \circ f^{-1} \circ g^{-1}(x) = x$. □

Définition 23. Soit $f : E \to F$ une application et $A \subset E$. On appelle image (directe) de A l'ensemble des images des éléments de A : $f(A) = \{y \in F \mid \exists x \in A, f(x) = y\}$. Soit maintenant $B \subset F$, on appelle image réciproque de B par F l'ensemble des antécédents d'élements de B : $f^{-1}(B) = \{x \in E \mid f(x) \in B\}$.

Remarque 16. La deuxième notation n'a pas été choisie de façon contradictoire avec la définition d'application réciproque (encore heureux). Si f est bijective, l'image réciproque d'une partie B de F est confondue avec son image directe par f^{-1}.

2.3 Relations

Définition 24. Une relation binaire R sur un ensemble E est un sous-ensemble de $E \times E$. On note habituellement xRy si $(x, y) \in R$.

Exemple : Une fois de plus, cette définition absconse peut laisser perplexe, alors que vous connaissez énormément d'exemple très simples. Par exemple, $\leqslant$ est une relation binaire sur $\mathbb{R}$. On a par exemple $(3,4) \in \leqslant$, mais $(4,3) \notin \leqslant$ (ce qu'on note plutôt $3 \leqslant 4$ et $4 \nleqslant 3$), ce qui prouve l'importance de l'ordre des deux arguments dans une relation binaire.

Définition 25. Une relation est dite réflexive si $\forall x \in E$, $(x, x) \in R$ (autrement dit, on a xRx). Elle est dite symétrique si $\forall (x, y) \in E^2$, $(x, y) \in R \ \Rightarrow\ (y, x) \in R$, et antisymétrique si $\forall (x, y) \in E^2$, $((x, y) \in R) \wedge ((y, x) \in R) \ \Rightarrow\ y = x$. Enfin, elle est dite transitive si $((x, y) \in R) \wedge ((y, z) \in R) \ \Rightarrow\ (x, z) \in R$.

Exemples : Sur $\mathbb{R}$, la relation $\leqslant$ est réflexive mais pas la relation $<$. La relation $\leqslant$ est par ailleurs l'exemple type d'une relation antisymétrique. Au contraire, la relation R définie sur $\mathbb{N}$ par : « $xRy \ \Leftrightarrow\ x$ et y ont même reste modulo 18 » est symétrique. Toutes les relations qu'on vient de définir sont transitives.

Définition 26. Une relation binaire qui est réflexive, symétrique et transitive est appelée relation d'équivalence sur un ensemble E. On appelle dans ce cas classe d'équivalence d'un élément x l'ensemble $C_x = \{y \in E \mid (x, y) \in R\}$.

Remarque 17. La plus simple des relations d'équivalences est la relation d'égalité. La classe d'équivalence d'un élément x est alors réduite à x lui-même.

Proposition 9. L'ensemble des classes d'équivalences d'une relation d'équivalence définie sur un ensemble E forme une parition de l'ensemble E.

Démonstration. Soit $x \in E$. On a par réflexivité xRx donc x appartient à une classe d'équivalence, la sienne. La réunion des classes d'équivalence est donc bien E tout entier. De plus, supposons que deux classes d'équivalence de deux élément y et z ne soient pas disjointes, et soit x un élément appartenant à ces deux classes. Comme on a xRy (ou yRx, peu importe, la relation est symétrique) et zRx, on a aussi zRy par transitivité, donc y appartient à la classe d'équivalence de z, et les deux classes considérées sont en fait la même. Les classes forment donc une partition de E. $\square$

Remarque 18. Réciproquement, si on a une partition de'un ensemble E sous la forme $E = \bigcup_{i \in I} A_i$, on peut définir une relation d'équivalence par $xRy \Leftrightarrow \exists i \in I, (x, y) \in A_i^2$. Les classes d'équivalence de la relation R sont alors exactement les sous-ensembles A_i.

Exemple : On considère E l'ensemble des couples de points du plan et on note R la relation $(A, B)R(C, D) \Leftrightarrow ABDC$ est un parallélogramme. Les classes d'équivalence pour cette relation s'identifient naturellement aux vecteurs du plan.

Définition 27. Une relation binaire est une relation d'ordre sur un ensemble E si elle est réflexive, antisymétrique et transitive. On dit que c'est un ordre total si de plus on a $\forall (x, y) \in E^2$, xRy ou yRx.

Exemple : On définit les deux relations suivantes sur $\mathbb{R}^2$: $(x, y) \leqslant (x', y')$ si $x \leqslant x'$ et $y \leqslant y'$; et $(x, y) \preceq (x', y')$ si $x \leqslant x'$ ou $x = x'$ et $y \leqslant y'$. La première relation est un ordre partiel sur $\mathbb{R}^2$ (appelée ordre produit) et le deuxième une relation d'ordre total, appelée ordre lexicographique (réfléchissez, c'est la même chose que pour le dictionnaire).

Définition 28. On appelle ensemble ordonné un couple (E, R) constitué d'un ensemble E et d'une relation d'ordre R sur celui-ci.

Définition 29. Soit (E, R) un ensemble ordonnée et A un sous-ensemble de E. Un élément $x \in E$ est un majorant (respectivement minorant) de A si $\forall y \in A$, yRx (resp. xRy). Si de plus $x \in A$, x est appelé plus grand élément (ou maximum) (resp. plus petit élément ou minimum) de la partie A.

Exemple : Soit $A = \{x \in \mathbb{R} \mid x^2 < 2\}$. La partie A admet tout un tas de majorants pour l'ordre usuel ($\sqrt{2}$, mais aussi 15, $38\pi^5$ et bien d'autres) mais pas de plus grand élément.

Proposition 10. Si une partie A admet un plus petit ou un plus grand élément pour une relation d'ordre R, celui-ci est unique.

Démonstration. En effet, supposons qu'il existe deux plus grands (par exemple) éléments x_1 et x_2 dans A. On a donc $x_1 R x_2$ et $x_2 R x_1$, mais alors par antisymétrie de la relation R, $x_1 = x_2$. $\square$