Chapitre 1

Logique et ensembles

Sommaire

1.1 Rudiments de logique

1.1.1 Propositions, démonstrations, etc.

Définition 1.1.1
Une *proposition* est un énoncé dont on doit pouvoir dire qu'il est « vrai » ou « faux ».

On notera V et F (ou encore 1 et 0) les deux valeurs logiques possibles d'une proposition.

Exemples :
– « l'entier 2011 est premier » est une proposition vraie
– « l'entier 2012 est premier » est une proposition fausse
– « l'entier 2014 est une somme de deux carrés » est une proposition fausse (prouvez-le)
– « l'entier 2017 est somme de deux carrés » est une proposition vraie (en effet $2017 = 9^2 + 44^2$)

Définition 1.1.2
Certaines propositions sont déclarées vraies à priori : ce sont les *axiomes*. Sinon la véracité (ou la fausseté) d'une proposition doit résulter d'une *démonstration* (d'une *preuve*).

Remarque : dans le cadre d'un cours de mathématiques, quand on énonce une proposition, c'est pour affirmer qu'elle est vraie (et qu'on va la démontrer) !

Définition 1.1.3
Un *théorème* est une proposition vraie particulièrement importante.

Un *lemme* est une proposition vraie, utile à la démonstration d'une proposition plus importante.

Un *corollaire* est une proposition vraie, conséquence immédiate d'une autre proposition vraie.

Une *conjecture* est une proposition qu'on pense généralement vraie, sans en avoir de preuve.

Exemples :
– « l'axiome de récurrence » dans $\mathbb{N}$, « l'axiome de la borne supérieure » dans $\mathbb{R}$.
– « le théorème de Pythagore », le « théorème de Rolle », « le théorème de Bolzano-Weierstrass ».
– le « lemme des bergers », le « lemme de Gauss », le « lemme des noyaux ».
– la « conjecture de Syracuse », la « conjecture de Goldbach ».
– la « conjecture de Fermat » est devenue le « grand théorème de Fermat » en 1994.

© Jean-Michel Ferrard Ce cours accompagne la souscription au site mathprepa.fr
Sa diffusion en dehors de ce cadre n'est pas autorisée

1.1.2 Ensembles, éléments

On ne se risque pas à donner une définition précise de ces notions premières.

Définition 1.1.4

On dit qu'un *ensemble* E est constitué d'*éléments* et qu'un élément a *appartient* à E (on écrit : $a \in E$) ou n'appartient pas à E (on écrit : $a \notin E$).

Deux ensembles E, F sont dits *égaux* (on note $E = F$) s'ils sont constitués des mêmes éléments.

Par convention l'*ensemble vide*, noté $\emptyset$, est l'ensemble ne contenant aucun élément.

Quelques remarques

- Un même objet mathématique peut, selon les circonstances, être vu comme un ensemble, ou comme un élément d'un ensemble. Par exemple, l'intervalle $[0, 1]$ est un *ensemble* de nombres réels, mais c'est également un *élément* de l'ensemble des intervalles de $\mathbb{R}$.
- Un ensemble *fini* peut être défini en *extension*, c'est-à-dire par la liste (non ordonnée) de ses éléments. C'est le cas par exemple de l'ensemble $E = \{1, 3, 6, 10, 15, 21, 28, 36, 45, 55\}$.
  Dans une écriture comme $\{a, b, c, \ldots\}$ les éléments a, b, c, etc. sont à priori supposés distincts, et l'ordre dans lequel ils sont donnés n'a aucune importance.
- Un ensemble E peut être défini en *compréhension* (par une propriété caractérisant ses éléments). Ainsi $E = \left\{\frac{n(n+1)}{2},\ n \in \mathbb{N},\ 1 \leqslant n \leqslant 10\right\}$ est une autre définition de $\{1, 3, 6, 10, 15, 21, 28, 36, 45, 55\}$.
- Il y a bien d'autres conventions pour définir ou nommer des ensembles. Par exemple :
  · Si a, b sont deux réels, $[a, b[$ est l'ensemble des réels x qui vérifient $a \leqslant x < b$.
  · Si E est un ensemble, $\mathcal{P}(E)$ est l'ensemble des parties de E.
  · Certains ensembles ont des noms consacrés par l'usage : $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, ...

Définition 1.1.5

Par convention l'*ensemble vide*, noté $\emptyset$, est l'ensemble ne contenant aucun élément.

Un ensemble $\{a\}$, formé d'un seul élément, est appelé un *singleton*.

Un ensemble $\{a, b\}$, formé de deux éléments *distincts*, est appelé une *paire*.

1.1.3 Propriétés portant sur les éléments d'un ensemble

On sait que la proposition « *l'entier 2017 est somme de deux carrés* » est vraie ($2017 = 9^2 + 44^2$).

Mais l'énoncé « *l'entier n est une somme de deux carrés* », qui contient la variable *libre* n (c'est-à-dire à laquelle on n'a pas donné de contenu particulier) ne peut pas être considéré comme une proposition, car on ne peut lui attribuer la valeur « Vrai » ou « Faux » tant qu'on ne donne pas une valeur à n.

On parlera plutôt ici d'une propriété $\mathcal{P}$ portant sur les entiers naturels n.

Avec cette définition, la proposition $\mathcal{P}(2017)$ est vraie (ou encore : l'entier 2017 vérifie la propriété $\mathcal{P}$) et la proposition $\mathcal{P}(2014)$ est fausse (l'entier 2014 ne vérifie pas la propriété $\mathcal{P}$).

Soit $\mathcal{P}$ une propriété portant sur les éléments d'un ensemble E. Pour affirmer qu'un élément x de E vérifie (ou satisfait à) la propriété $\mathcal{P}$, on écrira simplement « $\mathcal{P}(x)$ » plutôt que « $\mathcal{P}(x)$ est vraie ».

Il nous arrivera de considérer des énoncés contenant plusieurs variables libres.

Par exemple, la propriété $\mathcal{P}$ suivante : « *l'entier n est la somme de k carrés* »

1.1.4 Opérations sur les propositions

On peut créer de nouvelles propositions à l'aide d'« opérations » sur des propositions existantes.

Définition 1.1.6

À partir des propositions $\mathcal{A}$, $\mathcal{B}$, on définit ainsi :

- la *négation* « non $\mathcal{A}$ » (ou encore $\overline{\mathcal{A}}$, ou encore $\neg\mathcal{A}$).
- la *disjonction* « $\mathcal{A}$ ou $\mathcal{B}$ » (notée également $\mathcal{A}\vee\mathcal{B}$).
- la *conjonction* « $\mathcal{A}$ et $\mathcal{B}$ » (notée également $\mathcal{A}\wedge\mathcal{B}$).
- l'*implication* : la proposition « $\mathcal{A}$ implique $\mathcal{B}$ » (notée $\mathcal{A}\Rightarrow\mathcal{B}$)
- l'*équivalence* : la proposition « $\mathcal{A}$ équivaut à $\mathcal{B}$ » (notée $\mathcal{A}\Leftrightarrow\mathcal{B}$)

La valeur des propositions précédentes est résumée dans les *tableaux de vérité* ci-dessous.

$\mathcal{A}$	$\overline{\mathcal{A}}$
V	F
F	V

$\mathcal{A}$	$\mathcal{B}$	$\mathcal{A}$ ou $\mathcal{B}$
V	V	V
V	F	V
F	V	V
F	F	F

$\mathcal{A}$	$\mathcal{B}$	$\mathcal{A}$ et $\mathcal{B}$
V	V	V
V	F	F
F	V	F
F	F	F

$\mathcal{A}$	$\mathcal{B}$	$\mathcal{A}\Rightarrow\mathcal{B}$
V	V	V
V	F	F
F	V	V
F	F	V

$\mathcal{A}$	$\mathcal{B}$	$\mathcal{A}\Leftrightarrow\mathcal{B}$
V	V	V
V	F	F
F	V	F
F	F	V

Au vu des tableaux de vérités précédents, on peut donc dire, d'une façon moins formelle :

- La proposition $\overline{\mathcal{A}}$ est vraie quand $\mathcal{A}$ est fausse, et fausse quand $\mathcal{A}$ est vraie.
- La proposition « $\mathcal{A}$ ou $\mathcal{B}$ » est vraie quand l'une au moins des deux propositions $\mathcal{A},\mathcal{B}$ est vraie.
- La proposition « $\mathcal{A}$ et $\mathcal{B}$ » est vraie quand les deux propositions $\mathcal{A},\mathcal{B}$ sont vraies.
- « $\mathcal{A}\Rightarrow\mathcal{B}$ » est vraie quand $\mathcal{A}$ est fausse (le « faux implique n'importe quoi ») ou quand $\mathcal{B}$ est vraie.
- « $\mathcal{A}\Leftrightarrow\mathcal{B}$ » est vraie quand $\mathcal{A},\mathcal{B}$ sont toutes les deux vraies ou toutes les deux fausses.

Les opérations précédentes peuvent être répétées pour former des propositions $\mathcal{P}(\mathcal{A},\mathcal{B},\mathcal{C},\ldots)$ dépendant de propositions initiales $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, etc.

Deux telles propositions $\mathcal{P}(\mathcal{A},\mathcal{B},\mathcal{C},\ldots)$ et $\mathcal{Q}(\mathcal{A},\mathcal{B},\mathcal{C},\ldots)$ sont dites *synonymes* si elles ont le même tableau de vérité, c'est-à-dire si l'équivalence $\mathcal{P}(\mathcal{A},\mathcal{B},\mathcal{C},\ldots)\Leftrightarrow\mathcal{Q}(\mathcal{A},\mathcal{B},\mathcal{C},\ldots)$ est *toujours* vraie (c'est-à-dire quelle que soit la valeur de vérité des propositions $\mathcal{A},\mathcal{B},\mathcal{C},\ldots$).

1.1.5 Quantificateurs

Définition 1.1.7

Soit $\mathcal{P}$ une propriété portant sur les éléments d'un ensemble E.

- La proposition « $\exists\, x\in E,\ \mathcal{P}(x)$ » dit qu'au moins un un élément x de E vérifie la propriété $\mathcal{P}$.
  On dit que « $\exists$ » est le *quantificateur existentiel*.
- La proposition « $\forall\, x\in E,\ \mathcal{P}(x)$ » exprime que tout élément x de E vérifie la propriété $\mathcal{P}$.
  On dit que « $\forall$ » est le *quantificateur universel*.
- La proposition « $\exists !\, x\in E,\ \mathcal{P}(x)$ » exprime qu'un et un seul élément x de E vérifie la propriété $\mathcal{P}$.

De l'importance de la chronologie dans une phrase à plusieurs quantificateurs

On peut former des propositions « à tiroirs » avec plusieurs quantificateurs, notamment sur des énoncés $\mathcal{P}(x,y,\cdots)$ à plusieurs variables. Dans ce cas, on prendra garde à l'ordre des quantificateurs, notamment dans les alternances de « $\forall$ » et de « $\exists$ ».

Ainsi les propositions $\begin{cases}\mathcal{A} : \forall x\in E,\, \exists y\in F,\, \mathcal{P}(x,y)\\ \mathcal{B} : \exists y\in F,\, \forall x\in E,\, \mathcal{P}(x,y)\end{cases}$ ont souvent des significations très différentes.

Le mieux est de penser à la traduction de ces deux propositions « en français ».

En effet, la proposition $\mathcal{A}$ exprime que pour tout x de E, il existe un élément de y (dont la valeur dépend a priori du x qu'on vient d'évoquer) tel que la proposition $\mathcal{P}(x,y)$ soit vraie.

Quant à la proposition $\mathcal{B}$, elle exprime qu'il existe un certain élément y de F tel que, pour tout x de E, la proposition $\mathcal{P}(x,y)$ soit vraie.

Par exemple, la proposition « $\forall x\in\mathbb{N},\ \exists y\in\mathbb{N},\ x\leqslant y$ » (qui exprime que pour tout x de $\mathbb{N}$, il existe un y dans $\mathbb{N}$ qui lui est supérieur ou égal) est évidemment vraie (prendre $y=x$, par exemple).

En revanche, la proposition « $\exists y\in\mathbb{N},\ \forall x\in\mathbb{N},\ x\leqslant y$ » (qui exprime qu'il existe un entier naturel y supérieur ou égal à tous les entiers naturels) est manifestement fausse.

Bien distinguer le « mode texte » et « mode mathématique »

Considérons la proposition suivante : « tout nombre réel est la puissance troisième d'un nombre réel ».

On pourra tout aussi bien écrire : « pour tout réel x, il existe un réel y tel que $y^3=x$ ».

En revanche, on n'écrira pas :

- « pour tout $x\in\mathbb{R}$, il existe $y\in\mathbb{R}$ tq $y^3=x$ »
- « $\forall x\in\mathbb{R}$, il existe $y\in\mathbb{R}$ tel que $y^3=x$ »

Le programme le dit explicitement : « *l'emploi de quantificateurs en guise d'abréviations est exclu* »

Le mieux est de bien distinguer dans quel mode on écrit : en « mode texte » (c'est-à-dire en bon français, sans utiliser de quantificateurs) ou en « mode mathématique ».

Proposition 1.1.1 (négation d'une proposition avec quantificateurs)
Soit $\mathcal{P}$ une propriété portant sur les éléments d'un ensemble E.
La négation de la proposition « $\exists x\in E,\ \mathcal{P}(x)$ » est « $\forall x\in E,\ non\,\mathcal{P}(x)$ »
La négation de la proposition « $\forall x\in E,\ \mathcal{P}(x)$ » est « $\exists x\in E,\ non\,\mathcal{P}(x)$

1.1.6 Quelques synonymies classiques

Soit $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, etc. des propositions.

Les équivalences suivantes sont toujours vraies :

Double négation : $\text{non}\,(\text{non}\,\mathcal{A})\Leftrightarrow\mathcal{A}$ *Idempotence* : $\begin{cases}(\mathcal{A}\text{ et }\mathcal{A})\Leftrightarrow\mathcal{A}\\(\mathcal{A}\text{ ou }\mathcal{A})\Leftrightarrow\mathcal{A}\end{cases}$

Commutativité : $\begin{cases}(\mathcal{A}\text{ et }\mathcal{B})\Leftrightarrow(\mathcal{B}\text{ et }\mathcal{A})\\(\mathcal{A}\text{ ou }\mathcal{B})\Leftrightarrow(\mathcal{B}\text{ ou }\mathcal{A})\end{cases}$ *Associativité* : $\begin{cases}((\mathcal{A}\text{ et }\mathcal{B})\text{ et }\mathcal{C})\Leftrightarrow(\mathcal{A}\text{ et }(\mathcal{B}\text{ et }\mathcal{C}))\\((\mathcal{A}\text{ ou }\mathcal{B})\text{ ou }\mathcal{C})\Leftrightarrow(\mathcal{A}\text{ ou }(\mathcal{B}\text{ ou }\mathcal{C}))\end{cases}$

Dualité ou encore *Lois de De Morgan* : $\begin{cases}\text{non}\,(\mathcal{A}\text{ et }\mathcal{B})\Leftrightarrow((\text{non}\,\mathcal{A})\text{ ou }(\text{non}\,\mathcal{B}))\\\text{non}\,(\mathcal{A}\text{ ou }\mathcal{B})\Leftrightarrow((\text{non}\,\mathcal{A})\text{ et }(\text{non}\,\mathcal{B}))\end{cases}$

© Jean-Michel Ferrard Ce cours accompagne la souscription au site mathprepa.fr
Sa diffusion en dehors de ce cadre n'est pas autorisée

Double implication : $(\mathcal{A} \Leftrightarrow \mathcal{B}) \Leftrightarrow ((\mathcal{A} \Rightarrow \mathcal{B}) \text{ et } (\mathcal{B} \Rightarrow \mathcal{A}))$

Distributivité : $\begin{cases} (\mathcal{A} \text{ ou } (\mathcal{B} \text{ et } \mathcal{C})) \Leftrightarrow ((\mathcal{A} \text{ ou } \mathcal{B}) \text{ et } (\mathcal{A} \text{ ou } \mathcal{C})) \\ (\mathcal{A} \text{ et } (\mathcal{B} \text{ ou } \mathcal{C})) \Leftrightarrow ((\mathcal{A} \text{ et } \mathcal{B}) \text{ ou } (\mathcal{A} \text{ et } \mathcal{C})) \end{cases}$

1.1.7 Conditions nécessaires et/ou suffisantes

On considère deux propositions $\mathcal{A}$ et $\mathcal{B}$.

On suppose que « $\mathcal{A} \Rightarrow \mathcal{B}$ » est vraie.

Le tableau ci-contre illustre les trois cas possibles :

$\mathcal{A}$	$\mathcal{B}$	$\mathcal{A} \Rightarrow \mathcal{B}$
V	V	V
F	V	V
F	F	V

Définition 1.1.8

Soit $\mathcal{A}$ et $\mathcal{B}$ deux propositions.

Pour exprimer que la proposition « $\mathcal{A} \Rightarrow \mathcal{B}$ » est vraie, on dit indifféremment :

- La proposition $\mathcal{A}$ est une *condition suffisante* de la proposition $\mathcal{B}$.
- La proposition $\mathcal{B}$ est une *condition nécessaire* de la proposition $\mathcal{A}$.
- Pour que $\mathcal{A}$ (soit vraie) il *faut* que $\mathcal{B}$ (soit vraie).
- Pour que $\mathcal{B}$ (soit vraie), il *suffit* que $\mathcal{A}$ (soit vraie).
- $\mathcal{B}$ (est vraie) *si* $\mathcal{A}$ (est vraie).
- $\mathcal{A}$ (est vraie) *seulement si* $\mathcal{B}$ (est vraie).

Définition 1.1.9

Soit $\mathcal{A}$ et $\mathcal{B}$ deux propositions.

Pour exprimer que « $\mathcal{A} \Leftrightarrow \mathcal{B}$ » est vraie, on dit indifféremment :

- $\mathcal{A}$ est une condition *nécessaire et suffisante* (CNS) de $\mathcal{B}$.
- $\mathcal{A}$ (est vraie) *si et seulement si* $\mathcal{B}$ (est vraie).
- Pour que $\mathcal{A}$ (soit vraie), *il faut et il suffit* que $\mathcal{B}$ (soit vraie).

Dans ces énoncés on peut bien sûr échanger le rôle de $\mathcal{A}$ et $\mathcal{B}$.

1.2 Raisonnements classiques

1.2.1 Conseils appuyés pour bien rédiger

Dans le raisonnement logique, la syntaxe est primordiale. Elle va de pair avec la clarté du style.

Quelques bonnes habitudes doivent être prises :

- Indiquer clairement les hypothèses de la démonstration, et quel résultat on veut obtenir.
  Si par exemple, on doit prouver que l'implication $\mathcal{A} \Rightarrow \mathcal{B}$ est vraie, on commencera en général par dire : « supposons $\mathcal{A}$, et montrons $\mathcal{B}$ ». À partir de l'hypothèse sur $\mathcal{A}$, on procédera ensuite par conditions nécessaires, pour finalement prouver que $\mathcal{B}$ est vraie.

  Attention : on prouve ici que $\mathcal{B}$ est vraie *si* $\mathcal{A}$ *est vrai*, et pas que $\mathcal{B}$ est vrai dans l'absolu.

  À ce sujet, voir plus loin la règle de raisonnement dite du « modus ponens ».

- Mettre en évidence les liens logiques entre les phases successives de la démonstration.
  Le symbole « $\Rightarrow$ » n'est pas innocent. Son emploi doit être justifié.
- Ne pas mélanger les symboles « $\Rightarrow$ » et « $\Leftrightarrow$ ».
- Dans une proposition « à tiroirs », utiliser des parenthèses pour lever toute ambiguïté.
  Ainsi la proposition $(\mathcal{A} \Rightarrow \mathcal{B}) \Rightarrow \mathcal{C}$ n'est pas synonyme de $\mathcal{A} \Rightarrow (\mathcal{B} \Rightarrow \mathcal{C})$.
- Éviter d'utiliser exclusivement le langage de la logique formelle (propositions, quantificateurs) là où on peut s'exprimer « en français ». En particulier, on ne mélangera pas les deux styles. On évitera d'écrire, par exemple : « pour tout $x \in E$,... ».
- Varier le style, pour éviter toute sécheresse. Le mot « donc », par exemple, possède plusieurs synonymes : « on en déduit », « il s'ensuit », « par conséquent », etc.
- Soit $\mathcal{P}$ une propriété portant sur les éléments d'un ensemble E.
  Si on veut montrer la proposition « $\forall\, x \in E, \mathcal{P}(x)$ », on commencera souvent par écrire : « Soit x un élément de E, montrons que x vérifie la propriété $\mathcal{P}$ ». Le fait de fixer un élément de x n'est ici pas restrictif, tant que cet élément est quelconque dans E.
  Si on sait que la proposition « $\exists\, x \in E, \mathcal{P}(x)$ »est vraie, et si on veut en déduire quelque chose, on commencera en général par écrire « Soit x dans E, vérifiant la propriété $\mathcal{P}$ ».

  Le « Soit x » est un important car il installe dans la démonstration. Il crée et nomme un objet précis de E, sur lequel on va pouvoir travailler (le « $\exists\, x \in E$ » ne crée rien, lui).
- Soit $\mathcal{P}$ et $\mathcal{Q}$ deux propriétés portant sur les éléments d'un ensemble E.
  La proposition $(\exists\, x \in E, \mathcal{P}(x))$ et $(\exists\, x \in E, \mathcal{Q}(x))$ n'implique pas, en général $\exists\, x \in E, (\mathcal{P}(x)$ et $\mathcal{Q}(x))$
  La raison en est que le quantificateur $\exists$ est *mutificateur*. En d'autres termes, la variable x dont il est question dans $(\exists\, x \in E, \mathcal{P}(x))$ est *muette* : elle ne désigne aucun élément particulier de E.
  Il n'y a donc aucune raison de croire que les deux x de $(\exists\, x \in E, \mathcal{P}(x))$ et $(\exists\, x \in E, \mathcal{Q}(x))$ se réfèrent à un même élément de E.
  Si on doit déduire quelque chose de $(\exists\, x \in E, \mathcal{P}(x))$ et $(\exists\, x \in E, \mathcal{Q}(x))$, on pourra commencer par écrire : soit x dans E tel que $\mathcal{P}(x)$, et soit x' dans E tel que $\mathcal{Q}(x')$.

1.2.2 Quelques figures usuelles du raisonnement

Proposition 1.2.1 (la règle du « modus ponens »)
L'implication suivante est toujours vraie : $\Big((\mathcal{A} \Rightarrow \mathcal{B})$ et $\mathcal{A}\Big) \Rightarrow \mathcal{B}$

Proposition 1.2.2 (le raisonnement par contraposition)
L'équivalence suivante est toujours vraie : $(\mathcal{A} \Rightarrow \mathcal{B}) \;\Leftrightarrow\; ((\text{non}\,\mathcal{B}) \Rightarrow (\text{non}\,\mathcal{A}))$.

Proposition 1.2.3 (le raisonnement par l'absurde)
L'équivalence suivante est toujours vraie : $(\mathcal{A} \Rightarrow \mathcal{B}) \;\Leftrightarrow\; \text{non}\,(\mathcal{A}$ et $\text{non}\,\mathcal{B})$.

Proposition 1.2.4 (le syllogisme)
Soit $\mathcal{A}$, $\mathcal{B}$ et $\mathcal{C}$ trois propositions.
L'implication suivante est toujours vraie : $\Big((\mathcal{A} \Rightarrow \mathcal{B})$ et $(\mathcal{B} \Rightarrow \mathcal{C})\Big) \Rightarrow (\mathcal{A} \Rightarrow \mathcal{C})$.

Démonstration

C'est toujours la même méthode, à base de tableaux de vérité.

$\mathcal{A}$	$\mathcal{B}$	$\mathcal{C}$	$\mathcal{A}\Rightarrow\mathcal{B}$	$\mathcal{B}\Rightarrow\mathcal{C}$	$(\mathcal{A}\Rightarrow\mathcal{B})$ et $(\mathcal{B}\Rightarrow\mathcal{C})$	$\mathcal{A}\Rightarrow\mathcal{C}$	$((\mathcal{A}\Rightarrow\mathcal{B})$ et $(\mathcal{B}\Rightarrow\mathcal{C}))\Rightarrow(\mathcal{A}\Rightarrow\mathcal{C})$
V	V	V	V	V	V	V	V
V	V	F	V	F	F	F	V
V	F	V	F	V	F	V	V
V	F	F	F	V	F	F	V
F	V	V	V	V	V	V	V
F	V	F	V	F	F	V	V
F	F	V	V	V	V	V	V
F	F	F	V	V	V	V	V

On voit donc que la proposition $((\mathcal{A}\Rightarrow\mathcal{B})\text{ et }(\mathcal{B}\Rightarrow\mathcal{C}))\Rightarrow(\mathcal{A}\Rightarrow\mathcal{C})$ est toujours vraie : on exprime cette situation en disant que cette proposition est une *tautologie*

Proposition 1.2.5 (la disjonction des cas)
Soit $\mathcal{A}$, $\mathcal{B}$ et $\mathcal{C}$ trois propositions.
L'implication suivante est vraie : $\Big((\mathcal{A}\Rightarrow\mathcal{C})\text{ et }(\mathcal{B}\Rightarrow\mathcal{C})\Big)\Rightarrow\Big((\mathcal{A}\text{ ou }\mathcal{B})\Rightarrow\mathcal{C}\Big)$

1.2.3 L'axiome de récurrence

On admet l'existence et les propriétés de l'ensemble totalement ordonné $\mathbb{N}$, et notamment :

Axiome
Toute partie non vide de $\mathbb{N}$ possède un plus petit élément.

Proposition 1.2.6
Toute partie non vide majorée de $\mathbb{N}$ possède un plus grand élément.

Démonstration
Soit A une partie majorée non vide de $\mathbb{N}$. Soit B l'ensemble des majorants de A.
L'ensemble B est une partie non vide de $\mathbb{N}$ donc possède un plus petit élément b.
Pour tout élément a de A, on a l'inégalité $a\leqslant b$.
Si $b=0$, alors nécessairement $A=\{0\}$ et A possède bien un plus grand élément...
On suppose donc $b>0$. Par définition de b, l'entier $b-1$ n'est pas dans B.
Il existe donc un élément a de A tel que $b-1<a$.
On a alors $b-1<a\leqslant b$, ce qui implique $b=a$: l'entier b est donc dans A.
Ainsi b est un majorant de A qui appartient à A : c'est l'élément maximum de A

Remarques

– Soit n dans $\mathbb{N}$. L'ensemble $A=\{m\in\mathbb{N},\ m>n\}$ est non vide.
Le plus petit élément de A est bien sûr $n+1$ (c'est le *successeur* de n).
Autrement dit, pour tout n de $\mathbb{N}$, on a : $m>n\Leftrightarrow m\geqslant n+1$.

– Soit n dans $\mathbb{N}^*$. L'ensemble A des m de $\mathbb{N}$ tel que $m < n$ est non vide (il contient 0).
Le plus grand élément de cet ensemble est bien sûr $n-1$ (c'est le *prédécesseur* de n).
Autrement dit, pour tout n de $\mathbb{N}$, on a : $m < n \iff m \leqslant n-1$.

Proposition 1.2.7 (principe de récurrence)
Soit A une partie de $\mathbb{N}$, contenant 0.
On suppose que si A contient un entier n, alors A contient $n+1$. Dans ces conditions, $A = \mathbb{N}$.

Démonstration
On raisonne par l'absurde, donc on suppose que le complémentaire B de A dans $\mathbb{N}$ n'est pas vide.
Soit b le plus petit élément de B (on utilise l'axiome du plus petit élément).
On trouve $b \geqslant 1$ (car 0 est dans A, donc pas dans B, et b est dans B).
On peut donc parler de l'entier $a = b-1$, et a est dans A.
Par hypothèse sur A, on en déduit que $b = a+1$ est dans A, et c'est absurde.

Remarque

On peut modifier légèrement l'énoncé précédent, en « démarrant » en un entier n_0 plutôt qu'en 0.
Soit A une partie de $\mathbb{N}$, contenant n_0.
On suppose que si A contient un entier $n \geqslant n_0$, alors A contient $n+1$.
Dans ces conditions, A contient $[n_0, +\infty[$.

1.2.4 Raisonnement par récurrence

Raisonnement par récurrence simple

Proposition 1.2.8 (récurrence simple)
Soit $\mathcal{P}$ une propriété portant sur les entiers naturels.
Soit n_0 un entier naturel. On suppose que $\mathcal{P}(n_0)$ est vraie.
On suppose également, pour tout entier $n \geqslant n_0$, que l'implication $\mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$ est vraie.
Alors la proposition $\mathcal{P}(n)$ est vraie pour tout entier $n \geqslant n_0$.

Démonstration
Notons A l'ensemble des entiers n de $\mathbb{N}$ pour lesquels $\mathcal{P}(n)$ est vraie.
Les deux hypothèses signifient que n_0 est dans A et que : $\forall n \in A,\ n+1 \in A$.
Le principe de récurrence nous dit alors que A contient l'intervalle $[n_0, +\infty[$: la propriété $\mathcal{P}$ est donc vraie pour tout $n \geqslant n_0$.

Voici donc comment montrer qu'une propriété $\mathcal{P}(n)$ est vraie pour tous les entiers naturels :
– On vérifie que l'entier n_0 satisfait à la propriété : c'est le *pas initial* de la récurrence.
La plupart du temps, on a bien sûr $n_0 = 0$, ou $n_0 = 1$...
– On se **donne** ensuite un entier $n \geqslant n_0$, et on suppose que $\mathcal{P}(n)$ est vraie (*hypothèse de récurrence*).
On démontre alors que $\mathcal{P}(n+1)$ est vraie (c'est le « *passage du rang n au rang $n+1$* »).
On exprime l'implication $\mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$ en disant que la propriété $\mathcal{P}$ est *héréditaire*.
– On conclut en annonçant que, par récurrence, la propriété est vraie pour tout entier $n \geqslant n_0$.

© Jean-Michel Ferrard Ce cours accompagne la souscription au site mathprepa.fr
Sa diffusion en dehors de ce cadre n'est pas autorisée

Variantes du raisonnement par récurrence

Une variante réside dans la manière d'avancer dans la récurrence. Il arrive en effet que l'hypothèse $\mathcal{P}(n)$ seule soit insuffisante pour démontrer $\mathcal{P}(n+1)$.

Le cas le plus fréquent est celui de la *récurrence double*, où le pas initial et l'hypothèse de récurrence portent sur deux entiers consécutifs.

Proposition 1.2.9 (récurrence de pas 2)

Soit $\mathcal{P}$ une propriété portant sur les entiers naturels.

Soit n_0 un entier naturel. On suppose que $\mathcal{P}(n_0)$ et $\mathcal{P}(n_0+1)$ sont vraies.

On suppose que pour tout $n \geqslant n_0$, l'implication « $(\mathcal{P}(n)$ et $\mathcal{P}(n+1)) \Rightarrow \mathcal{P}(n+2)$ » est vraie.

Alors la proposition $\mathcal{P}(n)$ est vraie pour tout $n \geqslant n_0$.

Il reste à voir une variante importante : le raisonnement par récurrence forte.

Pour prouver $\mathcal{P}(n+1)$, on peut en effet utiliser tout ou partie des hypothèses $\mathcal{P}(n_0), \mathcal{P}(n_0+1), \ldots, \mathcal{P}(n)$.

Proposition 1.2.10 (récurrence forte)

Soit $\mathcal{P}$ une propriété portant sur les entiers naturels.

Soit n_0 un entier naturel. On suppose que $\mathcal{P}(n_0)$ est vraie.

On suppose que pour tout $n \geqslant n_0$, l'implication $(\mathcal{P}(n_0)$ et $\mathcal{P}(n_0+1) \cdots$ et $\mathcal{P}(n)) \Rightarrow \mathcal{P}(n+1)$ est vraie.
Alors la proposition $\mathcal{P}(n)$ est vraie pour tout $n \geqslant n_0$.

Pratique du raisonnement par récurrence

Voici enfin quelques conseils pour « réussir » un raisonnement par récurrence :

- Ne pas oublier le « pas initial » (la propriété est souvent triviale, mais on **doit** la prouver).
- Ne **jamais** écrire : « *Supposons que pour* **tout** n, $\mathcal{P}(n)$. *Montrons* $\mathcal{P}(n+1)$ ».
  Il faut en fait écrire : « **Soit** n *un entier naturel ; on suppose* $\mathcal{P}(n)$. *Montrons* $\mathcal{P}(n+1)$ ».
- Bien articuler le pas initial et l'hypothèse de récurrence.
  Si le pas initial est n_0, et si on veut démontrer $\mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$, alors on doit fixer $n \geqslant n_0$.
  On peut tout à fait prouver $\mathcal{P}(n-1) \Rightarrow \mathcal{P}(n)$, mais dans ce cas on doit fixer $n > n_0$.
- Bien séparer le « passage du rang n au rang $n+1$ », où l'entier n est **fixé**, et la conclusion finale (qui est obligatoire, et qui doit porter sur **tous** les entiers $n \geqslant n_0$).
  Une phrase finale rituelle est « *ce qui prouve la propriété au rang* $n+1$ *et achève la récurrence* ».

1.2.5 Raisonnement par analyse-synthèse

Le *raisonnement par analyse-synthèse* est souvent utilisé quand on demande de prouver l'existence (ou la non existence) de solutions à un problème donné (et d'identifier la ou les solutions éventuelles).

Ce raisonnement se déroule alors en deux étapes (trois étapes avec la conclusion) :

- L'analyse : on suppose que le problème admet (au moins) une solution, et on procède par **conditions nécessaires**, en accumulant suffisamment de renseignements pour dégager un ou plusieurs « candidats-solutions ».
- La synthèse : on vérifie si les « candidats » sont *effectivement* solutions du problème.
- La conclusion : on donne la ou les solutions du problème (s'il y en a).

Sa diffusion en dehors de ce cadre n'est pas autorisée

1.2.6 Résolutions d'équations ou d'inéquations

Commençons par une définition banale :

Définition 1.2.1

Soit f une fonction définie sur une partie $\mathcal{D}$ de $\mathbb{R}$, à valeurs réelles.

Trouver l'ensemble $\mathcal{S}$ (éventuellement vide) des réels x de $\mathcal{D}$ tels que $f(x)$ soit nul (resp. positif ou nul, resp. strictement positif), c'est « résoudre » l'équation $f(x) = 0$ (resp. l'inéquation $f(x) \geqslant 0$, resp. l'inéquation $f(x) > 0$).

Les éléments x de $\mathcal{S}$ sont appelés les *solutions* de l'équation (resp. de l'inéquation).

Généralisations

- Bien sûr, les équations $f(x) = \lambda$, ou $f(x) \geqslant \lambda$, ou $f(x) > \lambda$ (avec λ réel), et plus généralement les équations $f(x) = g(x)$, ou les inéquations $f(x) \geqslant g(x)$, $f(x) > g(x)$, $f(x) \leqslant g(x)$ ou $f(x) < g(x)$ se ramènent instantanément à l'une des situations évoquées dans la définition précédente.
- Soient f et g sont deux fonctions à valeurs réelles, et définies respectivement sur $\mathcal{D}_f$ et $\mathcal{D}_g$.

  Résoudre le système $\begin{cases} f(x) = 0 \\ g(x) = 0 \end{cases}$ c'est trouver les solutions communes à $f(x) = 0$ et $g(x) = 0$.

  On généralise à la notion de système de n équations (ou inéquations, ou un mélange des deux).
- Plus généralement encore, et en introduisant des « fonctions de plusieurs variables », on peut être amené à considérer des systèmes d'équations (ou d'inéquations) à plusieurs inconnues x, y, z etc.
- Autre point de vue possible : on sera amené à résoudre des équations dont la ou les inconnues sont supposées appartenir à $\mathbb{N}$, ou à $\mathbb{Z}$, ou à $\mathbb{Q}$, ou à $\mathbb{C}$.
- Tout ça recouvre donc un grand nombre de situations différentes, et ça peut devenir très compliqué !

  Dans certains cas, par exemple, on prouvera qu'une équation possède une solution sans pouvoir la calculer explicitement (considérer par exemple l'équation $x^3 + x + 1 = 0$, avec x cherché dans $\mathbb{R}$).

Deux grandes méthodes de résolution

Il est impossible de dresser la liste des « méthodes », tant les situations peuvent être différentes.

Contentons-nous d'imaginer une « équation » (E) (en donnant un sens très général à ce terme).

On peut chercher à résoudre (E) « par équivalences », ou « par conditions nécessaires ».

- **Résoudre (E) par équivalences** :

  C'est former une succession d'équations (E), puis (E_2), (E_3), etc. possédant exactement le même ensemble de solutions (ce qu'il est bien sûr primordial et obligatoire de justifier, sauf pour les équivalences vraiment évidentes).

  On arrive alors à une dernière équation (E_n) dont l'ensemble des solutions est clair : on a ainsi obtenu l'ensemble des solutions de l'équation initiale (E).
- **Résoudre (E) par implications** (ou encore par « conditions nécessaires ») :

  C'est former des équations $(E), (E_2), (E_3)$, etc. telles qu'à chaque étape « (E_k) implique (E_{k+1}) ».

  En termes plus précis, il s'agit de justifier que l'ensemble des solutions $\mathcal{S}_k$ de (E_k) est inclus dans l'ensemble des solutions $\mathcal{S}_{k+1}$ de (E_{k+1}).

  On arrive alors à une dernière équation (E_n) dont l'ensemble des solutions $\mathcal{S}_n$ est clair.

© Jean-Michel Ferrard Ce cours accompagne la souscription au site mathprepa.fr
Sa diffusion en dehors de ce cadre n'est pas autorisée

Tout ce qu'on peut dire à ce stade est que l'ensemble $\mathcal{S}$ des solutions de (E) (c'est lui qui nous intéresse) est *inclus* dans l'ensemble $\mathcal{S}_n$. Il importe alors de procéder à une *réciproque*, c'est-à-dire de vérifier, parmi les éléments de $\mathcal{S}_n$, qui est *effectivement* élément de $\mathcal{S}$.

Le prix consenti à établir la réciproque est compensé par le fait qu'il est souvent beaucoup facile de prouver les implications « $(E_k) \Rightarrow (E_{k+1})$ » que les équivalences « $(E_k) \Leftrightarrow (E_{k+1})$ ».

Si l'une des étapes contient une implication $(E_k) \Rightarrow (E_{k+1})$ qui n'est pas une équivalence, il ne sert à rien d'écrire des équivalences ici ou là (autant n'écrire que des implications, c'est plus sûr).

– **La clarté du style** :

Ce qui a été dit à la section 1.2.1 (conseils pour bien rédiger) s'applique particulièrement à la résolution d'équations. Il est absolument primordial d'éviter les successions interminables d'implications ou d'équivalences. Il **faut**, aussi souvent que possible, aérer le style et faire des pauses dans les implications (construire des phrases terminées par un point).

On enchaînera notamment les implications par des formules du type « il en découle », « on en déduit ».

Pour les équivalences, on évitera l'utilisation abusive et répétée du symbole $\Leftrightarrow$, et on utilisera régulièrement des expressions comme « c'est-à-dire », ou « ce qui équivaut à », etc.

1.2.7 Équations ou inéquations à un paramètre

Définition 1.2.2

Soit $\mathcal{M}$ une partie de $\mathbb{R}$, appelée ici ensemble des valeurs du paramètre m.

Pour tout m de $\mathcal{M}$, soit f_m une fonction définie sur une partie $\mathcal{D}_m$ de $\mathbb{R}$, à valeurs réelles.

Trouver l'ensemble $\mathcal{S}_m$ (éventuellement vide) des réels x de $\mathcal{D}_m$ tels que $f_m(x)$ soit nul, c'est « résoudre » l'équation $f_m(x) = 0$. Les éléments x de $\mathcal{S}_m$ sont appelés les *solutions* de l'équation (resp. de l'inéquation), pour la valeur m du paramètre.

Remarques

– On peut bien sûr généraliser aux inéquations à un paramètre, ou aux systèmes d'équations/inéquations, ou même à des systèmes à plusieurs paramètres...

– Évidemment, le nom donné au paramètre n'est pas toujours m : on trouve souvent λ par exemple !

– L'important est de comprendre que le paramètre (appelons-le m) n'est pas une *inconnue* du problème. Ce paramètre possède en fait une valeur, que nous ne connaissons pas, et il est probable que cette valeur conditionne la résolution de l'équation $(E_m) : f(x) = 0$ de l'inconnue x.

– Il est donc possible que l'équation (E_m) (dont l'énoncé dépend de la valeur attribuée à m) ne possède pas de solutions en x pour certaines valeurs de m, et qu'elle en possède pour d'autres (dans ce cas, il est probable que cette ou ces solutions dépendent de la valeur atttibuée à m).

– Résoudre l'équation (E_m), d'inconnue x et de paramètre m, c'est donc déterminer les valeurs (ou les intervalles de valeurs de m) pour lesquelles l'équation (E_m) possède des solutions (et lesquelles). Cette résolution prend alors la forme d'une « discussion suivant les valeurs du paramètre m ».

– Cette discussion permet souvent de dégager des valeurs particulières de m, et des situations plus générales (toujours pour m). Il est recommandé de traiter les cas particuliers en premier. Il convient aussi de ne pas « inventer » de cas particuliers (qui n'apparaissent que parce qu'on a effectué tel calcul plutôt que tel autre) et qui ne sont pas des cas particuliers « intrinsèques » au problème posé.

© Jean-Michel Ferrard Ce cours accompagne la souscription au site mathprepa.fr Sa diffusion en dehors de ce cadre n'est pas autorisée

1.3 Ensembles

1.3.1 Opérations sur les ensembles

À partir de deux ensembles E et F, on peut en construire d'autres :

Définition 1.3.1 (intersection et réunion)
Soit E et F deux ensembles.
$E \cap F$ est l'ensemble formé des éléments qui sont à la fois dans E et dans F.
$E \cup F$ est l'ensemble formé des éléments qui sont dans l'un au moins des ensembles E et F.

Définition 1.3.2 (ensembles disjoints)
On dit que E, F sont *disjoints* si $E \cap F$ est vide.
Dans ce cas, on dit que $E \cup F$ est une d'*union disjointe*.

On ne confondra pas *distincts* et *disjoints* :
- Dire que E et F sont distincts, c'est dire : $(\exists\, x \in E, x \notin F)$ ou $(\exists\, x \in F, x \notin E)$.
- Dire que E et F sont disjoints, c'est dire : $(\forall\, x \in E, x \notin F)$ et $(\forall\, x \in F, x \notin E)$.

Définition 1.3.3 (différence et différence symétrique)
Soit E et F deux ensembles.
- *Différence* : l'ensemble $E \setminus F$ est formé des éléments qui sont dans E mais pas dans F.
- *Différence symétrique* : on note $E \Delta F$ l'ensemble $(E \cup F) \setminus (E \cap F)$.
  C'est l'ensemble des éléments qui sont dans un et un seul des deux ensembles E et F.

Remarques :
- On dit encore que $E \setminus F$ est le *complémentaire* de F dans E et on peut le noter $\complement_E F$.
- Une définition équivalente de la différence symétrique est :
  $E \Delta F = (E \setminus F) \cup (F \setminus E)$ (c'est une union disjointe).

1.3.2 Ensemble des parties d'un ensemble

Définition 1.3.4
On dit qu'un ensemble F est *inclus* dans un ensemble E, et on note $F \subset E$, pour exprimer que tout élément de F est également élément de E.
On dit encore que E *contient* F, ou que F est une *partie* (ou un *sous-ensemble*) de E.

Définition 1.3.5
Soit E un ensemble. On note $\mathcal{P}(E)$ l'ensemble des parties de E.

Remarques
- Évidemment, si $E \subset F$ et $F \subset G$, alors $E \subset G$.

© Jean-Michel Ferrard Ce cours accompagne la souscription au site mathprepa.fr
Sa diffusion en dehors de ce cadre n'est pas autorisée

– On a l'équivalence $A \in \mathcal{P}(E) \Leftrightarrow A \subset E$.

De même : $a \in E \Leftrightarrow \{a\} \subset E \Leftrightarrow \{a\} \in \mathcal{P}(E)$.

Les *ensembles* E et $\emptyset$ sont toujours des *éléments* de $\mathcal{P}(E)$.

– La réunion, l'intersection, la différence symétrique sont des *opérations binaires* sur $\mathcal{P}(E)$, en ce sens qu'à deux éléments de $\mathcal{P}(E)$ elles associent un élément de $\mathcal{P}(E)$.

– Si aucune confusion n'est à craindre sur l'ensemble E, on notera $\overline{A}$ le complémentaire d'une partie A de E : c'est encore une partie de E.

Le passage au complémentaire est donc une opération *unaire* sur $\mathcal{P}(E)$.

1.3.3 Opérations sur les parties d'un ensemble

On observe que si $\mathcal{A}(x)$ et $\mathcal{B}(x)$ sont deux prédicats basés sur E, alors :

– On a l'égalité $\{x \in E, \mathcal{A}(x)\} \cup \{x \in E, \mathcal{B}(x)\} = \{x \in E, \mathcal{A}(x) \text{ ou } \mathcal{B}(x)\}$.

– On a l'égalité $\{x \in E, \mathcal{A}(x)\} \cap \{x \in E, \mathcal{B}(x)\} = \{x \in E, \mathcal{A}(x) \text{ et } \mathcal{B}(x)\}$.

– Le complémentaire dans E de $\{x \in E, \mathcal{A}(x)\}$ est $\{x \in E, \text{non } \mathcal{A}(x)\}$.

De cette remarque et des propriétés des opérations sur les propositions, on déduit les propriétés suivantes des opérations sur $\mathcal{P}(E)$. A, B, C désignent ici trois parties quelconques de E.

– *Double passage au complémentaire* : $\overline{\overline{A}} = A$.

– *Idempotence* : $\begin{cases} A \cap A = A \\ A \cup A = A \end{cases}$

– *Commutativité* : $\begin{cases} A \cap B = B \cap A \\ A \cup B = B \cup A \end{cases}$

– *Associativité* : $\begin{cases} (A \cap B) \cap C = A \cap (B \cap C) \\ (A \cup B) \cup C = A \cup (B \cup C) \end{cases}$

– *Distributivité* : $\begin{cases} A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \\ A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \end{cases}$

– *Dualité* : $\begin{cases} \overline{A \cap B} = \overline{A} \cup \overline{B} \\ \overline{A \cup B} = \overline{A} \cap \overline{B} \end{cases}$

– *Partie vide et partie pleine* : $\begin{cases} A \cup \emptyset = A \quad A \cap \emptyset = \emptyset \\ A \cap B = \emptyset \Leftrightarrow A \subset \overline{B} \end{cases}$ $\qquad \begin{cases} A \cap E = A \quad A \cup E = E \\ A \cup B = E \Leftrightarrow \overline{B} \subset A \end{cases}$

Proposition 1.3.1 (propriétés de l'inclusion)
Soit A, B, C trois parties quelconques d'un ensemble E. Les équivalences suivantes sont vraies :

$$A = B \Leftrightarrow (A \subset B) \text{ et } (B \subset A) \qquad A \subset B \Leftrightarrow \overline{B} \subset \overline{A}$$
$$(A \cup B) \subset C \Leftrightarrow (A \subset C) \text{ et } (B \subset C) \qquad A \subset (B \cap C) \Leftrightarrow (A \subset B) \text{ et } (A \subset C)$$

Démonstration

Pour tout élément x de E, notons $\mathcal{A}$ et $\mathcal{B}$ les prédicats « $x \in A$ » et « $x \in B$ ».

L'inclusion $A \subset B$ est la traduction de l'implication $\mathcal{A} \Rightarrow \mathcal{B}$.

Plus généralement, l'équivalence $A = B \Leftrightarrow (A \subset B)$ et $(B \subset A)$ est la traduction de la synonymie $(\mathcal{A} \Leftrightarrow \mathcal{B}) \equiv (\mathcal{A} \Rightarrow \mathcal{B})$ et $(\mathcal{B} \Rightarrow \mathcal{A})$.

De même $A \subset B \Leftrightarrow \overline{B} \subset \overline{A}$ est la traduction de $(\mathcal{A} \Rightarrow \mathcal{B}) \equiv (\text{non } \mathcal{B} \Rightarrow \text{non } \mathcal{A})$.

Par ailleurs l'équivalence « $(A \cup B) \subset C \Leftrightarrow (A \subset C)$ et $(B \subset C)$ » n'est autre que la synonymie entre l'proposition « $(\mathcal{A}$ ou $\mathcal{B}) \Rightarrow \mathcal{C}$ » et l'proposition « $(\mathcal{A} \Rightarrow \mathcal{C})$ et $(\mathcal{B} \Rightarrow \mathcal{C})$ »

Enfin « $A \subset (B \cap C) \Leftrightarrow (A \subset B)$ et $(A \subset C)$ » traduit la synonymie « $(\mathcal{A} \Rightarrow (\mathcal{B}$ et $\mathcal{C})) \equiv ((\mathcal{A} \Rightarrow \mathcal{B})$ et $(\mathcal{A} \Rightarrow \mathcal{C}))$ »

Proposition 1.3.2 (propriétés de la différence symétrique)
Pour toutes parties A, B, C d'un ensemble E, on a les égalités suivantes :

$$A\Delta B = B\Delta A \qquad A\Delta A = \emptyset \qquad A\Delta E = \overline{A} \qquad A\Delta\emptyset = A$$
$$A\Delta(B\Delta C) = (A\Delta B)\Delta C \qquad A\cap(B\Delta C) = (A\cap B)\Delta(A\cap C)$$

Démonstration
On désigne par A, B, C trois parties quelconques de E.

– On a : $A\Delta B = (A\cup B)\setminus(A\cap B) = (B\cup A)\setminus(B\cap A) = B\Delta A$.

– On a facilement : $\begin{cases} A\Delta A = (A\cup A)\setminus(A\cap A) = A\setminus A = \emptyset \\ A\Delta E = (A\cup E)\setminus(A\cap E) = E\setminus A = \overline{A} \\ A\Delta\emptyset = (A\cup\emptyset)\setminus(A\cap\emptyset) = A\setminus\emptyset = A \end{cases}$

– Remarquons que pour toutes parties X, Y de E, $X\Delta Y$ est formé des éléments de E qui figurent dans l'un et dans l'un seulement des deux ensembles X et Y.
Dire que x est dans $A\Delta(B\Delta C)$, c'est donc dire qu'il est dans un et un seul des trois ensembles A, B, C, ou bien dans les trois à la fois. On arrive à la même caractérisation pour $(A\Delta B)\Delta C$, ce qui assure l'égalité de $A\Delta(B\Delta C)$ et de $(A\Delta B)\Delta C$.
On verra plus loin une autre démonstration, utilisant les fonctions caractéristiques.

– Dire qu'un élément x de E est dans $A\cap(B\Delta C)$, c'est dire qu'il est dans A et qu'il est dans l'un et l'un seulement des deux ensembles B et C.
Cela signifie qu'il est dans $A\cap B$ ou bien dans $A\cap C$, c'est-à-dire dans $(A\cap B)\Delta(A\cap C)$. On a donc l'égalité des deux ensembles $A\cap(B\Delta C)$ et $(A\cap B)\Delta(A\cap C)$.

Ceci termine la démonstration des propriétés de la différence symétrique

1.3.4 Produit cartésien d'un nombre fini d'ensembles

Définition 1.3.6 (n-uplets et produit cartésien)
Soit $E_1, E_2, \ldots, E_n$ n ensembles (non nécessairement distincts deux à deux), avec $n \geqslant 2$.

– Pour tout entier k (compris entre 1 et n), soit x_k un élément de l'ensemble E_k.
$(x_1, x_2, \ldots, x_n)$ est appelé un *n-uplet* de *composantes* $x_1, x_2, \ldots, x_n$ (dans cet ordre).

– On appelle *produit cartésien* de E_1, E_2, …, E_n, et on note $E_1\times E_2\times\ldots\times E_n$, l'ensemble des n-uplets $(x_1, x_2, \ldots, x_n)$. Par exemple, $E\times F = \{(a,b), a\in E, b\in F\}$.

Remarques :

– Un n-uplet est donc le moyen de regrouper n éléments dans un ordre bien défini.

– On parle de *couple* si $n=2$, de *triplet* si $n=3$, de *quadruplet* si $n=4$, etc.

– On ne confondra pas (par exemple) la *paire* $\{a,b\}$ avec le *couple* (a,b) :
  · Si a et b sont différents, les couples (a,b) et (b,a) désignent en effet deux objets différents, alors que $\{a,b\}$ et $\{b,a\}$ désignent le même ensemble.
  · De même si $a=b$: l'ensemble $\{a,b\}$ se réduit au singleton $\{a\}$, alors que (a,a) est toujours un couple (mais dont les deux composantes sont égales).

– Si $E_1, E_2, \ldots, E_n$ sont égaux à un même ensemble E, on note E^n plutôt que $E\times E\times\cdots\times E$.

– Par définition, la *diagonale* de E^2 est l'ensemble $\Delta = \{(x,x), x\in E\}$.

1.4 Applications

1.4.1 Applications entres ensembles non vides

Définition 1.4.1

Soient E et F deux ensembles non vides.

Une *application* (on dit aussi une *fonction*) f de E vers F est le moyen d'associer, à chaque élément x de E, un unique élément y de F. On note alors $y = f(x)$.

On exprime l'égalité $y = f(x)$ est *l'image* de x par f, ou que x est *un antécédent* de y par f.

On dit que E est l'*ensemble de départ* et que F l'*ensemble d'arrivée* de f.

Définition 1.4.2

Soit E et F deux ensembles.

On note $\mathcal{F}(E,F)$, ou encore F^E l'ensemble de toutes les applications de E vers F.

Si les deux ensembles E et F sont égaux, on note plus simplement $\mathcal{F}(E)$ (ou E^E).

Notations et remarques :

– Une application f de E vers F est souvent notée $E \xrightarrow{f} F$ ou $f : \begin{array}{ccc} E & \longrightarrow & F \\ x & \mapsto & y=f(x) \end{array}$

– Si E est fini, on peut représenter $f : E \to F$ par la donnée de chacune des images par f.
On définit par exemple une application f de $E = \{a,b,c,d,e\}$ vers $F = \{t,u,v,w\}$ par :

$$f(a) = t,\ f(b) = t,\ f(c) = v,\ f(d) = w,\ f(e) = w$$

Comme on le voit sur cet exemple, tout élément de E possède une image et une seule (c'est la définition même d'une application) mais un élément donné de F peut très bien :

· ne posséder aucun antécédent (l'élément u n'en a pas)

· ou posséder un seul antécédent (celui de v est c)

· ou en posséder plusieurs (t et w en ont chacun deux) ou une infinité (pas ici... !)

– Deux applications f et g sont *égales* si :

· elles ont le même ensemble de départ E et le même ensemble d'arrivée F.

· pour tous x de E, on a $f(x) = g(x)$.

Définition 1.4.3 (application Identité)

Soit E un ensemble.

On définit l'application *identité* de E dans E, notée Id_E, par : $\forall\, x \in E, \mathrm{Id}_E(x) = x$.

Définition 1.4.4 (applications constantes)

Une application f de E dans F est dite *constante* s'il existe un élément α de F, tel que, pour tout x de E, $f(x)$ soit égal à α.

1.4.2 Famille indexée par un ensemble non vide

Définition 1.4.5 (familles d'éléments d'un ensemble)

Soit I un ensemble non vide dont les éléments seront appelés *indices*. Soit E un ensemble.

Toute application x de I vers E est appelée une *famille d'éléments* de E, *indicée* par I.

On note x_i plutôt que $x(i)$, et on écrit $(x_i)_{i\in I}$ cette famille d'éléments.

On note E^I l'ensemble des familles d'éléments de E indicées par I : c'est donc une autre manière de désigner l'ensemble $\mathcal{F}(I,E)$.

Remarques et notations :

- La famille $(x_i)_{i\in I}$ est dite *finie* ou *infinie*, selon que l'ensemble I est fini ou infini.
- On ne confondra pas la famille $(x_i)_{i\in I}$, c'est-à-dire l'application x, avec l'ensemble $\{x_i, i\in I\}$ c'est-à-dire l'ensemble image de cette application.
  En particulier, une famille infinie peut n'être constituée que d'un nombre fini d'éléments (et par exemple un seul si l'application x est constante !)
- Si I est un intervalle d'entiers $[m,n]$, où $m\leqslant n$, la famille est notée $(x_i)_{m\leqslant i\leqslant n}$.
- Si les x_i sont dans $\mathbb{R}$ ou dans $\mathbb{C}$, leur somme et leur produit sont notés respectivement $\sum_{i=m}^{n} x_i$ et $\prod_{i=m}^{n} x_i$.

Définition 1.4.6 (famille de parties d'un ensemble)

Toute application de I vers $\mathcal{P}(E)$ est appelée une *famille de parties* de E, indicée par I.

Une telle famille s'écrit par exemple $(E_i)_{i\in I}$ (si on appelle E_i l'image de i par l'application).

Soit $(E_i)_{i\in I}$ une famille de parties de l'ensemble E.

La réunion et l'intersection de cette famille sont les parties de E définies par :

· $\bigcup_{i\in I} E_i = \{x\in E, \exists\, i\in I, x\in E_i\}$ (éléments de E appartenant à au moins un E_i)

· $\bigcap_{i\in I} E_i = \{x\in E, \forall\, i\in I, x\in E_i\}$ (éléments de E appartenant à tous les E_i).

Si I est un intervalle d'entiers $[m,n]$, avec $m\leqslant n$, on notera plutôt $\bigcup_{i=m}^{n} E_i$ et $\bigcap_{i=m}^{n} E_i$.

Définition 1.4.7 (partitions d'un ensemble)

On dit qu'une famille $(E_i)_{i\in I}$ de parties de E constitue une *partition* de E si :

- Aucun des ensembles E_i n'est vide : $\forall\, i\in I, E_i\neq\emptyset$.
- Les E_i sont disjoints deux à deux : $\forall\,(i,j)\in I^2$, avec $i\neq j$, $E_i\cap E_j=\emptyset$.
- La réunion des ensembles E_i est égale à E tout entier : $\bigcup_{i\in I} E_i = E$.

Dans ces conditions, tout élément x de E appartient à un sous-ensemble E_i unique.

1.4.3 Fonction indicatrice d'une partie

Définition 1.4.8

Soit A une partie d'un ensemble E. On appelle *fonction indicatrice* (ou *fonction caractéristique*) de A, et on note $\mathbb{1}_A$, la fonction définie sur E par : $\begin{cases}\mathbb{1}_A(x)=1 & \text{si } x\in A\\ \mathbb{1}_A(x)=0 & \text{si } x\notin A\end{cases}$

– Opérations sur les applications numériques :
Soit f, g deux applications définies sur un ensemble E, à valeurs réelles.
Soit α un nombre réel.
On définit les applications $f+g$, fg et αf de la manière suivante :
· pour tout x de E, $(f+g)(x)=f(x)+g(x)$
· pour tout x de E, $(fg)(x)=f(x)g(x)$
· pour tout x de E, $(\alpha f)(x)=\alpha f(x)$
Par abus de langage, on note encore α l'application constante prenant la valeur α.
En particulier $\mathbb{1}_E=1$ et $\mathbb{1}_\emptyset=0$.

– Propriétés :
L'application $\mathbb{1}$, qui envoie A sur $\mathbb{1}_A$, est une bijection de $\mathcal{P}(E)$ sur $\mathcal{F}(E,\{0,1\})$.
Toute application f de E vers $\{0,1\}$ est en effet la fonction indicatrice d'une unique partie A de E, définie par : $A=\{x\in E, f(x)=1\}$.
En particulier, deux parties A et B de E sont égales si et seulement si leurs fonctions indicatrices $\mathbb{1}_A$ et $\mathbb{1}_B$ sont identiques : c'est parfois un bon moyen de démontrer l'égalité entre deux parties d'un ensemble.

Proposition 1.4.1

Soit A et B deux parties de E. On a les égalités suivantes :

$$\mathbb{1}_{\overline{A}}=1-\mathbb{1}_A \qquad \mathbb{1}_{A\cap B}=\mathbb{1}_A\mathbb{1}_B$$
$$\mathbb{1}_{A\cup B}=\mathbb{1}_A+\mathbb{1}_B-\mathbb{1}_A\mathbb{1}_B \qquad \mathbb{1}_{A\setminus B}=\mathbb{1}_A(1-\mathbb{1}_B)$$

Les parties A et B sont disjointes si et seulement si $\mathbb{1}_{A\cup B}=\mathbb{1}_A+\mathbb{1}_B$.
Enfin, on a $\mathbb{1}_{A\Delta B}=\mathbb{1}_A+\mathbb{1}_B-2\mathbb{1}_A\mathbb{1}_B=(\mathbb{1}_A-\mathbb{1}_B)^2=|\mathbb{1}_A-\mathbb{1}_B|$

Démonstration

◇ On a $A\cup B=(A\Delta B)\cup(A\cap B)$ et cette union est disjointe.
On en déduit $\mathbb{1}_{A\Delta B}=\mathbb{1}_{A\cup B}-\mathbb{1}_{A\cap B}=\mathbb{1}_A+\mathbb{1}_B-2\mathbb{1}_A\mathbb{1}_B=(\mathbb{1}_A-\mathbb{1}_B)^2$.
Remarquons que $\mathbb{1}_A-\mathbb{1}_B$ ne peut prendre que les valeurs -1, 0 ou 1.
Or $\forall x\in\{-1,0,1\}$, $|x|=x^2$. On peut donc écrire $\mathbb{1}_{A\Delta B}=|\mathbb{1}_A-\mathbb{1}_B|$.

◇ Voici par exemple comment retrouver l'associativité de l'opération Δ.
Posons $X=A\Delta B$ et $Y=B\Delta C$. Il faut montrer que $X\Delta C=A\Delta Y$.
Pour cela on prouve l'égalité des fonctions indicatrices de ces ensembles.

$$\begin{aligned}\mathbb{1}_{X\Delta C}&=\mathbb{1}_X(1-2\mathbb{1}_C)+\mathbb{1}_C=(\mathbb{1}_A+\mathbb{1}_B-2\mathbb{1}_A\mathbb{1}_B)(1-2\mathbb{1}_C)+\mathbb{1}_C\\&=\mathbb{1}_A+\mathbb{1}_B+\mathbb{1}_C-2\mathbb{1}_A\mathbb{1}_B-2\mathbb{1}_A\mathbb{1}_C-2\mathbb{1}_B\mathbb{1}_C+4\mathbb{1}_A\mathbb{1}_B\mathbb{1}_C\\ \mathbb{1}_{A\Delta Y}&=\mathbb{1}_Y(1-2\mathbb{1}_A)+\mathbb{1}_A=(\mathbb{1}_B+\mathbb{1}_C-2\mathbb{1}_B\mathbb{1}_C)(1-2\mathbb{1}_A)+\mathbb{1}_A\\&=\mathbb{1}_A+\mathbb{1}_B+\mathbb{1}_C-2\mathbb{1}_A\mathbb{1}_B-2\mathbb{1}_A\mathbb{1}_C-2\mathbb{1}_B\mathbb{1}_C+4\mathbb{1}_A\mathbb{1}_B\mathbb{1}_C=\mathbb{1}_{X\Delta C}\end{aligned}$$

1.4.4 Restriction et prolongement

Soit f une application d'un ensemble E vers un ensemble F.

Il y a plusieurs moyens de créer de nouvelles applications en ne modifiant que l'ensemble de départ ou l'ensemble d'arrivée de f.

- Extension de l'ensemble d'arrivée :
  Pour tout ensemble F' contenant F, on peut encore dire que f est une application de E vers F' (ce n'est pas vrai si F' est une partie de F, sauf si F' contient l'image de f, c'est-à-dire tous les éléments de F qui ont au moins un antécédent).

- Restriction d'une application :
  Soit E' une partie de E.
  On définit une application g, de E' vers F, en posant : $\forall\, x \in E', g(x) = f(x)$.
  On dit que g est *la restriction* de f à E'.

- Prolongements d'une application :
  Soit E'' un ensemble contenant E.
  On dit qu'une application h de E'' vers F est *un prolongement* de f si f est la restriction de h à E, c'est-à-dire si : $\forall\, x \in E, h(x) = f(x)$.

On notera qu'on parle de *la* restriction et d'*un* prolongement.

Par exemple, si f est l'identité de $\mathbb{R}^+$ dans lui-même, elle possède une infinité de prolongements à $\mathbb{R}$ tout entier, parmi lesquels :

- L'application identité de $\mathbb{R}$.
- L'application « valeur absolue », de $\mathbb{R}$ dans lui-même.
- L'application h définie par : $h(x) = \frac{1}{2}(x + |x|)$, et qui est identiquement nulle sur $\mathbb{R}^-$.

1.4.5 Image directe d'une partie par une application

Soit E, F deux ensembles, et f une application de E vers F.

Définition 1.4.9

Soit $A \subset E$. On appelle *image* de A par f le sous-ensemble $f(A) = \{f(a), a \in A\}$ de F.

$f(A)$ est donc l'ensemble des images par f des éléments de A.

On peut écrire : $y \in f(A) \;\Leftrightarrow\; \exists\, x \in A,\, f(x) = y$.

On définit ainsi une nouvelle application de $\mathcal{P}(E)$ vers $\mathcal{P}(F)$: à toute partie de E on associe en effet une partie de F.

Cette application est encore notée f. On ne confondra pas ces deux significations de f !

Cas particuliers et exemples :

- L'image de l'ensemble vide par f est l'ensemble vide : $f(\emptyset) = \emptyset$.
  Pour tout a de E, $f(\{a\}) = \{f(a)\}$ (on a là les deux acceptations de f).
- $f(E)$ est l'ensemble de toutes les images par f. On dit que c'est l'*ensemble image* de f.
  Si on reprend l'exemple vu en 1.C.1 $f(\{a, b, c\}) = \{t, v\}$ et $f(\{d, e\}) = \{w\}$.

Proposition 1.4.2

Soit f une application d'un ensemble E vers un ensemble F.

Soit A et B deux parties quelconques de E. On a

- ◇ $A \subset B \Rightarrow f(A) \subset f(B)$
- ◇ $f(A \cup B) = f(A) \cup f(B)$
- ◇ $f(A \cap B) \subset f(A) \cap f(B)$

En revanche, il n'y a pas de règle générale permettant de comparer $f(\overline{A})$ et $\overline{f(A)}$.

Démonstration ◇ Vérifions l'implication $A \subset B \Rightarrow f(A) \subset f(B)$:
Supposons $A \subset B$, et soit y un élément de $f(A)$.
Il existe x dans A tel que $y = f(x)$.
Bien sûr x appartient aussi à B, donc y est dans $f(B)$. Ainsi $f(A) \subset f(B)$.

◇ On a les inclusions $\begin{cases} A \subset A \cup B \\ B \subset A \cup B \end{cases}$ donc $\begin{cases} f(A) \subset f(A \cup B) \\ f(B) \subset f(A \cup B) \end{cases}$
On en déduit l'inclusion $f(A) \cup f(B) \subset f(A \cup B)$.
Réciproquement, soit y dans $f(A \cup B)$.
Par définition, il existe x dans $A \cup B$ tel que $y = f(x)$.
Si x est dans A (resp. dans B), y est dans $f(A)$ (resp. dans $f(B)$).
Ainsi y est toujours dans $f(A) \cup f(B)$.
On en déduit l'inclusion $f(A \cup B) \subset f(A) \cup f(B)$.
Finalement, on a bien l'égalité $f(A \cup B) = f(A) \cup f(B)$.

◇ On a $\begin{cases} A \cap B \subset A \\ A \cap B \subset B \end{cases}$ donc $\begin{cases} f(A \cap B) \subset f(A) \\ f(A \cap B) \subset f(B) \end{cases}$ donc $f(A \cap B) \subset f(A) \cap f(B)$

1.4.6 Image réciproque d'une partie par une application

Définition 1.4.10

Soit f une application d'un ensemble E vers un ensemble F.

Soit B une partie de F. L'*image réciproque* de B par f, notée $\overset{-1}{f}(B)$, est l'ensemble des éléments de E dont l'image est dans B : Autrement dit : $\overset{-1}{f}(B) = \{x \in E, f(x) \in B\}$.
C'est la partie de E formée par les antécédents des éléments de B.

On peut donc écrire : $x \in \overset{-1}{f}(B) \Leftrightarrow f(x) \in B$.

Remarques :

- On définit ainsi une application $\overset{-1}{f}$ de $\mathcal{P}(F)$ vers $\mathcal{P}(E)$: à toute partie de F on associe en effet une partie de E. Mais cette application ne doit pas être confondue (quand f est bijective) avec la bijection réciproque f^{-1} (voir plus loin).
- Soit f une application d'un ensemble E vers un ensemble F. Alors on a :
  $\overset{-1}{f}(\emptyset) = \emptyset$; $\overset{-1}{f}(F) = E$; $\forall b \in F, \overset{-1}{f}(\{b\}) = \{x \in E, f(x) = b\}$.
- Si on reprend l'exemple donné en 1.3.1,
  $\overset{-1}{f}(\{u\}) = \emptyset$, $\overset{-1}{f}(\{v\}) = \{c\}$, $\overset{-1}{f}(\{w\}) = \{d, e\}$ et $\overset{-1}{f}(\{t, w\}) = \{a, b, d, e\}$.

Proposition 1.4.3

Soit f une application d'un ensemble E vers un ensemble F.

Pour deux parties quelconques A et B de F, on a les égalités :

$$\overset{-1}{f}(A\cup B)=\overset{-1}{f}(A)\cup\overset{-1}{f}(B),\qquad \overset{-1}{f}(\overline{A})=\overline{\overset{-1}{f}(A)},\qquad \overset{-1}{f}(A\cap B)=\overset{-1}{f}(A)\cap\overset{-1}{f}(B)$$

Démonstration ◇ Soit x un élément de E. On a les équivalences :

$$\begin{aligned} x\in\overset{-1}{f}(A\cup B) &\Leftrightarrow f(x)\in A\cup B \Leftrightarrow (f(x)\in A) \text{ ou } (f(x)\in B)\\ &\Leftrightarrow (x\in\overset{-1}{f}(A)) \text{ ou } (x\in\overset{-1}{f}(B)) \Leftrightarrow x\in\overset{-1}{f}(A)\cup\overset{-1}{f}(B)\end{aligned}$$

On en déduit l'égalité : $\overset{-1}{f}(A\cup B)=\overset{-1}{f}(A)\cup\overset{-1}{f}(B)$.

◇ Soit x un élément de E. On a les équivalences :

$$x\in\overset{-1}{f}(\overline{A}) \Leftrightarrow f(x)\in\overline{A} \Leftrightarrow \text{non } (f(x)\in A) \Leftrightarrow \text{non } (x\in\overset{-1}{f}(A)) \Leftrightarrow x\in\overline{\overset{-1}{f}(A)}.$$

◇ On peut utiliser les deux résultats précédents, et le fait que $A\cap B=\overline{\overline{A}\cup\overline{B}}$:

$$\begin{aligned}\overset{-1}{f}(A\cap B) &= \overset{-1}{f}\left(\overline{\overline{A}\cup\overline{B}}\right)=\overline{\overset{-1}{f}\left(\overline{A}\cup\overline{B}\right)}=\overline{\overset{-1}{f}\left(\overline{A}\right)\cup\overset{-1}{f}\left(\overline{B}\right)}\\ &=\overline{\overline{\overset{-1}{f}(A)}\cup\overline{\overset{-1}{f}(B)}}=\overline{\overline{\overset{-1}{f}(A)}\cap\overline{\overset{-1}{f}(B)}}=\overset{-1}{f}(A)\cap\overset{-1}{f}(B)\end{aligned}$$

1.4.7 Composition d'applications

Définition 1.4.11

Soit E, F, G trois ensembles. Soit f dans $\mathcal{F}(E,F)$ et g dans $\mathcal{F}(F,G)$.

La *composée* de f par g, notée $g\circ f$, est l'application de E vers G, définie par :

$\forall\, x\in E, g\circ f(x)=g(f(x))$.

Proposition 1.4.4

Soit E,F,G,H quatre ensembles.

Soit f dans $\mathcal{F}(E,F)$, g dans $\mathcal{F}(F,G)$ et h dans $\mathcal{F}(G,H)$.

Alors on a l'égalité $h\circ(g\circ f)=(h\circ g)\circ f$.

Démonstration

Pour tout élément x de E, en notant $y=f(x)$ et $z=g(y)$, on a en effet :

$$\begin{cases}(h\circ(g\circ f))(x)=h((g\circ f)(x))=h(g(f(x)))=h(g(y))=h(z)\\ ((h\circ g)\circ f)(x)=(h\circ g)(f(x))=(h\circ g)(y)=h(g(y))=h(z)\end{cases}$$

Les applications $h\circ(g\circ f)$ et $(h\circ g)\circ f$ sont donc égales

Remarques et propriétés :

– On exprime cette propriété (qui ne devra jamais être redémontrée) en disant que *la loi de composition des applications est associative.*

De cette propriéte il découle qu'une composition répétée, comme $f_n\circ f_{n-1}\circ\cdots\circ f_2\circ f_1$, ne nécessite pas de parenthèses.

– Soit f dans $\mathcal{F}(E,F)$. Alors $\mathrm{Id}_F \circ f = f$ et $f \circ \mathrm{Id}_E = f$.
– Si f appartient à $\mathcal{F}(E)$, on pose par convention $f^0 = \mathrm{Id}_E$.
On définit alors : $\forall\, n \in \mathbb{N}^*,\ f^n = f^{n-1} \circ f = f \circ f \circ \cdots \circ f \circ f$ (n fois).
– Soit f dans $\mathcal{F}(E,F)$ et g dans $\mathcal{F}(F,E)$.
On peut donc former à la fois $g \circ f$ (de E dans E) et $f \circ g$ (de F dans F).
Ces deux applications sont en général distinctes (notamment si $E \neq F$!).
– Si f et g appartiennent à $\mathcal{F}(E)$, on dit que f et g *commutent* si $g \circ f = f \circ g$.
On note que Id_E commute avec toute application de E dans E.
De même, les « puissances » f^n d'une application f commutent entre elles (on vérifie en effet par une récurrence évidente sur l'entier naturel n qu'on a toujours l'égalité : $f^n \circ f^p = f^p \circ f^n = f^{n+p}$)

1.5 Injections, surjections, bijections

1.5.1 Applications injectives

Définition 1.5.1
Soit f une application de E dans F. On dit que f est une application *injective* (ou encore une *injection*) si tout élément y de F possède *au plus un antécédent* par f.

Remarques :
– Une définition équivalente de l'injectivité de f est : $\forall\,(x,x') \in E^2, x \neq x' \Rightarrow f(x) \neq f(x')$.
Autrement dit, une application est injective si elle « conserve les différences ».
– Une autre définition équivalente (très utile) est : $\forall\,(x,x') \in E^2,\ f(x) = f(x') \Rightarrow x = x'$

Proposition 1.5.1
Soit f dans $\mathcal{F}(E,F)$ et g dans $\mathcal{F}(F,G)$.
– *Si f et g sont injectives, alors $g \circ f$ est injective.*
– *Si $g \circ f$ est injective, alors f est injective.*

Démonstration – Supposons que les applications f et g soient injectives.
Soit a, b dans E tels que $(g \circ f)(a) = (g \circ f)(b)$. Il faut montrer que $a = b$. Or :
$$\begin{aligned} g \circ f(a) &= g \circ f(b) \Rightarrow g(f(a)) = g(f(b)) \\ &\Rightarrow f(a) = f(b) \quad \text{(injectivité de } g\text{)} \\ &\Rightarrow a = b \quad \text{(injectivité de } f\text{)} \end{aligned}$$
Ainsi l'application $g \circ f$ est également injective.
– On suppose que $g \circ f$ est injective. Soit a, b dans E tels que $f(a) = f(b)$.
Cette égalité implique $g(f(a)) = g(f(b))$ c'est-à-dire $(g \circ f)(a) = (g \circ f)(b)$.
On en déduit $a = b$ car $g \circ f$ est injective. L'injectivité de f en découle.

1.5.2 Applications surjectives

Définition 1.5.2

Soit f une application de E dans F.

On dit que f est une application *surjective* (ou encore une *surjection*) si tout élément y de F possède *au moins un antécédent* par f, autrement dit si : $\forall\, y \in F, \exists\, x \in E, f(x) = y$.

Une définition équivalente de la surjectivité de $f : E \to F$ est : $f(E) = F$.

On dit souvent que f est une surjection de E *sur* F (plutôt que *dans* F).

Proposition 1.5.2

Soit f dans $\mathcal{F}(E,F)$ et g dans $\mathcal{F}(F,G)$.

- *Si f et g sont surjectives, alors $g \circ f$ est surjective.*
- *Si $g \circ f$ est surjective, alors g est surjective.*

Démonstration – Supposons maintenant que les applications f et g soient surjectives.
Soit z un élément de G. Il faut prouver l'existence de x dans E tel que $z = (g \circ f)(x)$.
Or il existe y dans F tel que $z = g(y)$, car g est surjective.
De même, il existe x dans E tel que $y = f(x)$, car f est surjective.
On en déduit $z = g(y) = g(f(x)) = (g \circ f)(x)$.

– On suppose que $g \circ f$ est surjective. Soit z un élément de G.
Il existe donc un élément x de E tel que $z = (g \circ f)(x)$.
Mais cette égalité s'écrit $z = g(y)$, avec $y = f(x)$, élément de F.
Ainsi tout z de G a au moins un antécédent dans F par g : g est surjective.

1.5.3 Applications bijectives

Définition 1.5.3

Soit f une application de E dans F. On dit que f est une application *bijective* (ou encore une *bijection*) si f est à la fois injective et surjective, c'est-à-dire si tout élément y de l'ensemble F possède *un antécédent x et un seul* dans E : $\forall\, y \in F, \exists\,! x \in E,\ f(x) = y$.

Proposition 1.5.3 (bijection réciproque)

Soit f une bijection de l'ensemble E sur l'ensemble F.

On définit une application de F vers E en associant à tout y de F son seul antécédent x.

Cette application, notée f^{-1}, vérifie donc : $\forall\, x \in E, \forall\, y \in F,\ x = f^{-1}(y) \ \Leftrightarrow\ y = f(x)$.

On a alors les égalités : $f^{-1} \circ f = \mathrm{Id}_E$, et $f \circ f^{-1} = \mathrm{Id}_F$.

L'application f^{-1} est également bijective : on l'appelle la bijection réciproque *de f.*

On a enfin l'égalité $(f^{-1})^{-1} = f$: l'application f est la bijection réciproque de f^{-1}.

Rappel : on ne confondra pas l'application f^{-1} (bijection réciproque de f), de F vers E, avec l'application $\overset{-1}{f}$ de $\mathcal{P}(F)$ vers $\mathcal{P}(E)$, qui existe même quand f n'est pas bijective.

Proposition 1.5.4

Soit f dans $\mathcal{F}(E,F)$. Pour montrer que l'application f est bijective, il suffit de trouver g dans $\mathcal{F}(F,E)$ telle que : $g\circ f=\mathrm{Id}_E$, et $f\circ g=\mathrm{Id}_F$. On a alors $g=f^{-1}$.

Démonstration

Supposons que $g\circ f=\mathrm{Id}_E$ et $f\circ g=\mathrm{Id}_F$.

L'application Id_E étant bijective donc injective, on en déduit que f est injective.

De même, Id_F est bijective donc surjective. Il s'ensuit que f est surjective.

Ainsi l'application f est bijective. On trouve alors :

$$f^{-1}=\mathrm{Id}_E\circ f^{-1}=(g\circ f)\circ f^{-1}=g\circ(f\circ f^{-1})=g\circ\mathrm{Id}_F=g$$

L'application g est donc bien la bijection réciproque de f

Proposition 1.5.5

Soit f dans $\mathcal{F}(E,F)$ et g dans $\mathcal{F}(F,G)$.

Si f et g sont bijectives, alors $g\circ f$ est bijective, et $(g\circ f)^{-1}=f^{-1}\circ g^{-1}$.

Démonstration

Si f et g sont bijectives, elles sont à la fois injectives et surjectives. Les résultats précédents montrent alors que $g\circ f$ est injective et surjective, donc bijective.

Soit z un élément de G et x un élément de E. On a les équivalences :

$$\begin{aligned}x &= (g\circ f)^{-1}(z) \Leftrightarrow z=(g\circ f)(x) \Leftrightarrow z=g(f(x)) \Leftrightarrow f(x)=g^{-1}(z)\\ &\Leftrightarrow x=f^{-1}(g^{-1}(z)) \Leftrightarrow x=(f^{-1}\circ g^{-1})(z)\end{aligned}$$

Ainsi les applications $(g\circ f)^{-1}$ et $f^{-1}\circ g^{-1}$ sont identiques.

Définition 1.5.4 (applications involutives)

Soit f dans $\mathcal{F}(E)$. On dit que f est *involutive* si $f\circ f=\mathrm{Id}_E$.

Cela équivaut à dire que f est bijective et que $f^{-1}=f$.

Exemples

- L'application Id_E est involutive, ou encore les symétries dans un espace affine.
- L'application $x\mapsto\dfrac{1}{x}$ est une involution de $\mathbb{R}^*$.
- L'application $A\mapsto\overline{A}$ est une involution de $\mathcal{P}(E)$.
- L'application $z\mapsto\bar{z}$ est une involution de $\mathbb{C}$.

1.6 Relations binaires

1.6.1 Généralités

Soit E et F deux ensembles.

Définition 1.6.1

On appelle *relation* $\mathcal{R}$ de E vers F la donnée d'une partie R du produit cartésien $E \times F$.

La partie R est appelée le *graphe* de la relation $\mathcal{R}$.

On dit qu'un élément x de E est *en relation* avec un élément y de F, pour la relation $\mathcal{R}$, si le couple (x, y) appartient au graphe R.

On exprime cette situation en écrivant $x\,\mathcal{R}\,y$.

Si $E = F$ (cas fréquent) on dit que $\mathcal{R}$ est une relation *sur* E.

Exemples :

- La relation d'inclusion dans l'ensemble des parties de E : $A\,\mathcal{R}\,B \Leftrightarrow A \subset B$.
- La relation de divisibilité sur les entiers relatifs : $m\,\mathcal{R}\,n \Leftrightarrow m$ divise n.
- Dans $\mathbb{Z}$, et si a non nul, on définit la relation de *congruence modulo* a :
  $m\,\mathcal{R}\,n \Leftrightarrow m - n$ est divisible par a. On note le plus souvent $m \equiv n\ (a)$.
- Sur tout ensemble E, on peut définir la *relation égalité* : $x\,\mathcal{R}\,y \Leftrightarrow x = y$.
  Le graphe de cette relation est la diagonale $\Delta(E) = \{(x, x), x \in E\}$.
- Soit E et F deux ensembles quelconques.
  On définit la *relation universelle* de E vers F par : $\forall (x, y) \in E \times F, x\,\mathcal{R}\,y$.
  Le graphe de cette relation est l'ensemble $E \times F$ tout entier.
- Soit E un ensemble *fini* et $\mathcal{R}$ une relation sur E.
  On peut représenter $\mathcal{R}$ en donnant la liste de tous les couples (x, y) de E^2 tels que $x\,\mathcal{R}\,y$.
  Voici par exemple la description d'une relation sur $E = \{a, b, c, d, e, f\}$.

	a	b	c	d	e	f
a	$\star$					
b	$\star$					$\star$
c			$\star$			
d		$\star$		$\star$	$\star$	$\star$
e	$\star$				$\star$	
f				$\star$		

ce qui équivaut à $\begin{cases} a\,\mathcal{R}\,a \\ b\,\mathcal{R}\,a, \quad b\,\mathcal{R}\,f \\ c\,\mathcal{R}\,c \\ d\,\mathcal{R}\,b, \quad d\,\mathcal{R}\,d, \quad d\,\mathcal{R}\,e, \quad d\,\mathcal{R}\,f \\ e\,\mathcal{R}\,a, \quad e\,\mathcal{R}\,e \\ f\,\mathcal{R}\,d \end{cases}$

- Restriction d'une relation :
  Si $\mathcal{R}$ est une relation binaire sur E, et si F est une partie de E, alors on peut définir la restriction $\mathcal{S}$ de $\mathcal{R}$ à l'ensemble F.
  Le graphe de $\mathcal{S}$ est l'intersection de $F \times F$ et du graphe de $\mathcal{R}$.
  Par exemple, Si P est l'ensemble des entiers naturels premiers, la restriction à P de la relation de divisibilité n'est autre que la relation d'égalité sur P.

1.6.2 Propriétés éventuelles des relations binaires

Définition 1.6.2

Soit $\mathcal{R}$ une relation binaire sur l'ensemble E.

- $\mathcal{R}$ est dite *réflexive* si : $\forall\, x \in E, x\,\mathcal{R}\,x$.
- $\mathcal{R}$ est dite *symétrique* si : $\forall\,(x,y) \in E^2, x\,\mathcal{R}\,y \Rightarrow y\,\mathcal{R}\,x$.
- $\mathcal{R}$ est dite *transitive* si : $\forall\,(x,y,z) \in E^3, (x\,\mathcal{R}\,y \text{ et } y\,\mathcal{R}\,z) \Rightarrow x\,\mathcal{R}\,z$.
- $\mathcal{R}$ est dite *antisymétrique* si : $\forall\,(x,y) \in E^2, (x\,\mathcal{R}\,y \text{ et } y\,\mathcal{R}\,x) \Rightarrow x = y$.

Remarques :

- L'antisymétrie s'écrit aussi : $\forall\,(x,y) \in E^2, (x\,\mathcal{R}\,y \text{ et } x \neq y) \Rightarrow \text{non}\,(y\,\mathcal{R}\,x)$
- Si $\mathcal{R}$ est symétrique, on dira de deux éléments x, y de E qu'ils sont ou qu'ils ne sont pas en relation (x et y ayant alors des rôles identiques).
- L'antisymétrie n'est pas le contraire de la symétrie : la relation « égalité », par exemple, possède les deux propriétés, alors que la relation donnée en exemple sur $\{a,b,c,d,e,f\}$ n'est ni symétrique (e est en relation avec a mais a n'est pas en relation avec e) ni antisymétrique (les éléments d et f sont en relation l'un avec l'autre, bien qu'ils soient distincts).
- A titre d'exercice, on pourra vérifier que si une relation est à la fois symétrique, antisymétrique, et réflexive, alors c'est la relation d'égalité.

1.6.3 Relations d'ordre

Définition 1.6.3

On dit qu'une relation $\mathcal{R}$ sur un ensemble E est une *relation d'ordre* si $\mathcal{R}$ est à la fois réflexive, antisymétrique et transitive. On note souvent $\leqslant$ une telle relation.

On dit alors que $(E, \leqslant)$ est un *ensemble ordonné*.

Une relation d'ordre sur E est donc caractérisée par :

- $\forall\, x \in E,\ x \leqslant x$
- $\forall\, x,y,z \in E,\ (x \leqslant y \text{ et } y \leqslant z) \Rightarrow x \leqslant z$
- $\forall\, x,y \in E,\ (x \leqslant y) \text{ et } (y \leqslant x) \Rightarrow x = y$

Définition 1.6.4 (ordre total ou ordre partiel)

Soit $\mathcal{R}$ une relation d'ordre sur E.

- Deux éléments x et y de E sont dits *comparables* (pour $\leqslant$) si $x \leqslant y$ ou si $y \leqslant x$.
- Si deux éléments quelconques x et y sont toujours comparables, on dit que $\leqslant$ est une relation d'*ordre total* : l'ensemble E est dit *totalement ordonné* par $\leqslant$.
- Sinon (c'est-à-dire s'il existe au moins deux éléments non comparables x et y) on dit que $\leqslant$ est une relation d'*ordre partiel* (l'ensemble E est dit *partiellement ordonné* par $\leqslant$).

Exemple et remarques

- Sur les ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, on dispose d'une relation d'ordre total, notée $\leqslant$.
  Si m et n sont deux entiers relatifs, avec $m \leqslant n$, on note souvent $[\![m, n]\!] = \{p \in \mathbb{Z}, m \leqslant p \leqslant n\}$.
- *Relation d'ordre inverse*
  Si $\leqslant$ est une relation d'ordre sur E, on définit encore une relation d'ordre sur E, notée $\geqslant$, en posant : $\forall\,(x, y) \in E^2, x \geqslant y \;\Leftrightarrow\; y \leqslant x$.
- Si on pose : $x < y \;\Leftrightarrow\; (x \leqslant y)$ et $x \neq y$, on définit une nouvelle relation (appelée souvent ordre strict) qui en fait n'est pas une relation d'ordre (elle n'est pas réflexive).
- Soit $(E, \leqslant)$ un ensemble ordonné.
  La négation de la proposition $x \leqslant y$ est : « (x et y ne sont pas comparables) ou $(y < x)$ ».
  Bien sûr, si E est totalement ordonné, la négation de $x \leqslant y$ est $y < x$.
- On définit une relation d'ordre sur $\mathcal{P}(E)$ en posant : $A \leqslant B \;\Leftrightarrow\; A \subset B$.
  Il s'agit d'un ordre partiel, sauf si E est vide ou se réduit à un élément.
  Par exemple, si a et b sont distincts dans E, $\{a\}$ et $\{b\}$ ne sont pas comparables.
- Sur $\mathbb{R}^2$, on peut poser : $(x, y) \leqslant (x', y') \;\Leftrightarrow\; (x \leqslant x')$ et $(y \leqslant y')$.
  C'est un ordre partiel : les couples $(1, 2)$ et $(4, 0)$, par exemple, ne sont pas comparables.

Relation de divisibilité dans $\mathbb{N}$

Définition 1.6.5
On dit que n *divise* m (ou que m est un *multiple* de n) si : $\exists\, q \in \mathbb{N}, m = nq$.
On note alors $n \mid m$. On définit ainsi une relation d'ordre partiel sur $\mathbb{N}$.
Pour cette relation, 1 est le minimum de $\mathbb{N}$.

Démonstration

Pour tout entier n, on a $n = n \cdot 1$ donc $\begin{cases} n \mid n & \text{(la relation est réflexive)} \\ 1 \mid n & \text{(l'entier 1 est minimum)} \end{cases}$

La relation est transitive car $\begin{cases} n \mid n' \\ n' \mid n'' \end{cases} \Rightarrow \begin{cases} n' = nq \\ n'' = n'q' \end{cases} \Rightarrow n'' = n(qq') \Rightarrow n \mid n''$.

$\begin{cases} n \mid m \\ m \mid n \end{cases} \Rightarrow \begin{cases} m = nq \\ n = mp \end{cases} \Rightarrow n = n(qp) \Rightarrow \begin{cases} n = 0 \text{ ou} \\ pq = 1 \end{cases} \Rightarrow \begin{cases} m = n = 0 \text{ ou} \\ p = q = 1 \end{cases} \Rightarrow m = n$

C'est un ordre partiel car par exemple 2 et 3 ne sont pas comparables

Remarque : la divisibilité ne définit pas une relation d'ordre sur $\mathbb{Z}$; en effet si m est un entier relatif non nul, les entiers m et $-m$ se divisent mutuellement (le quotient vaut -1) bien qu'ils soient distincts : la relation n'est donc pas antisymétrique.

Ordre lexicographique sur $\mathbb{R}^2$

Sur l'ensemble $\mathbb{R}^2$, on peut poser : $(x, y) \leqslant (x', y')$ si $\begin{cases} x < x' \text{ ou} \\ (x = x') \text{ et } (y \leqslant y') \end{cases}$
on définit ainsi une relation d'ordre total sur $\mathbb{R}^2$.
Cette relation (dont le modèle se généralise facilement à $\mathbb{R}^n$) est appelée *ordre lexicographique*, en référence à la relation d'ordre total qui permet de classer les mots du dictionnaire.

Démonstration

– Pour tout couple (x,y), on a bien $(x,y) \leqslant (x,y)$: la relation est réflexive.
– Remarquons d'abord que $(a,b) \leqslant (a',b') \Rightarrow a \leqslant a'$, et que $(a,b) \leqslant (a,b') \Leftrightarrow b \leqslant b'$.
Dans ces conditions $\begin{cases}(x,y) \leqslant (x',y')\\(x',y') \leqslant (x,y)\end{cases} \Rightarrow (x=x') \Rightarrow \begin{cases}(x,y) \leqslant (x,y')\\(x,y') \leqslant (x,y)\end{cases} \Rightarrow \begin{cases}x=x'\\y=y'\end{cases}$
La relation est antisymétrique.
– Le système (S) $\begin{cases}(x,y) \leqslant (x',y')\\(x',y') \leqslant (x'',y'')\end{cases}$ implique $\begin{cases}x \leqslant x'\\x' \leqslant x''\end{cases}$ donc $x \leqslant x''$.
Si on a l'inégalité stricte $x < x''$ alors $(x,y) \leqslant (x'',y'')$.
Sinon $x = x' = x''$, donc (S) $\Rightarrow \begin{cases}(x,y) \leqslant (x,y')\\(x,y') \leqslant (x,y'')\end{cases} \Rightarrow (y \leqslant y' \leqslant y'')$.
On voit là encore que $(x,y) \leqslant (x'',y'')$: la relation est transitive.
– Soit (x,y) et (x',y') deux éléments de $\mathbb{R}^2$.
Si $x < x'$, alors on a $(x,y) \leqslant (x',y')$. Si $x' < x$ on a $(x',y') \leqslant (x,y)$.
Il reste le cas $x = x'$. Il suffit alors de comparer y et y' : $\begin{cases}y \leqslant y' \Rightarrow (x,y) \leqslant (x',y')\\y' \leqslant y \Rightarrow (x',y') \leqslant (x,y)\end{cases}$
Dans tous les cas, les couples (x,y) et (x',y') sont donc comparables.
– Conclusion : la relation $\leqslant$ est une relation d'ordre total sur $\mathbb{R}^2$

1.6.4 Relations d'équivalence, classes d'équivalence

Définition 1.6.6
On dit qu'une relation $\mathcal{R}$ sur un ensemble E est une *relation d'équivalence* si $\mathcal{R}$ est à la fois réflexive, symétrique et transitive.
Pour tout x de E, l'ensemble des éléments en relation avec x est appelé la *classe d'équivalence* de x, et notée $\mathcal{C}(x)$ (ou $\dot{x}$, ou $\overline{x}$) : $\mathcal{C}(x) = \{y \in E, x\,\mathcal{R}\,y\}$.

Conséquences de la définition :
– La relation $\mathcal{R}$ étant réflexive, tout élément x de E appartient à sa propre classe d'équivalence. En particulier, aucune classe d'équivalence n'est vide.
– Soit x et y dans E : si $x\,\mathcal{R}\,y$, alors $\mathcal{C}(x) = \mathcal{C}(y)$. Sinon $\mathcal{C}(x) \cap \mathcal{C}(y) = \emptyset$.
Deux classes d'équivalence sont donc ou bien identiques ou bien disjointes.

Démonstration
Si $\mathcal{C}(x) \cap \mathcal{C}(y) = \emptyset$ alors $y \notin \mathcal{C}(x)$. On n'a donc pas $x\,\mathcal{R}\,y$.
Sinon soit $z \in \mathcal{C}(x) \cap \mathcal{C}(y)$. On a $x\,\mathcal{R}\,z$ et $z\,\mathcal{R}\,y$ donc $x\,\mathcal{R}\,y$.
Pour tout t de $\mathcal{C}(x)$ on a ainsi $t\,\mathcal{R}\,x$ et $x\,\mathcal{R}\,y$ donc $t\,\mathcal{R}\,y$, c'est-à-dire $t \in \mathcal{C}(y)$.
Ainsi $\mathcal{C}(x) \subset \mathcal{C}(y)$ (puis l'égalité en changeant les rôles)

– Une classe d'équivalence $\mathcal{C}$ est entièrement déterminée par la donnée de l'un quelconque de ses éléments x (on dira que x est un *représentant* de $\mathcal{C}$).

Proposition 1.6.1 (partitions et relations d'équivalence)
Soit E un ensemble.

- *Soit $\mathcal{R}$ une relation d'équivalence sur E.*
  Soit Ω un sous-ensemble de E obtenu en choisissant dans chaque classe d'équivalence $\mathcal{C}$ un représentant x unique : la famille $(\mathcal{C}(x))_{x\in\Omega}$ est une partition de l'ensemble E. Autrement dit, les différentes classes d'équivalence pour la relation $\mathcal{R}$ définissent une partition de E.
- *Réciproquement, soit $(E_i)_{i\in I}$ une partition de E.*
  Soit $\mathcal{R}$ la relation définie sur E par : $\forall\,(x,y)\in E^2,\ x\,\mathcal{R}\,y \Leftrightarrow \exists\, i\in I,\ \{x,y\}\subset E_i$
  Alors $\mathcal{R}$ est une relation d'équivalence sur E, et les sous-ensembles E_i sont les classes d'équivalence de E pour $\mathcal{R}$.

Démonstration

En effet, aucune classe n'est vide, les classes sont deux à deux disjointes et leur réunion est égale à E tout entier (car chaque x de E est dans sa propre classe d'équivalence)

— Puisque E est la réunion des E_i, tout x de E est dans l'un des E_i.
Ainsi $\{x,x\}=\{x\}\subset E_i$ et donc $x\,\mathcal{R}\,x$: la relation $\mathcal{R}$ est réflexive.

— Par sa définition même, la relation $\mathcal{R}$ est symétrique (x et y jouent le même rôle).

— Soit x,y,z dans E tels que $x\,\mathcal{R}\,y$ et $y\,\mathcal{R}\,z$.
Il existe donc (i,j) dans I^2 tels que $\{x,y\}\subset E_i$ et $\{y,z\}\subset E_j$.
Ainsi l'intersection $E_i\cap E_j$ est non vide car elle contient y.
En vertu des hypothèses, on a donc $E_i=E_j$. Ainsi $x\,\mathcal{R}\,z$ car $\{x,z\}\subset E_i$.
La relation $\mathcal{R}$ est donc transitive : finalement c'est une relation d'équivalence

— Soit x un élément de E. Il existe un unique x de I tel que x appartienne à E_i.
On a alors $y\in\mathcal{C}(x) \Leftrightarrow \{x,y\}\subset E_i \Leftrightarrow y\in E_i$. Autrement dit $\mathcal{C}(x)=E_i$.
Ainsi toute classe d'équivalence est un E_i et réciproquement chaque E_i est la classe d'équivalence de l'un quelconque de ses éléments.

Exemples de relations d'équivalence

- Soit $f:E\to F$ une application.
  On définit une relation d'équivalence sur E en posant : $x\,\mathcal{R}\,y \Leftrightarrow f(x)=f(y)$.
  La classe d'équivalence de x est l'image réciproque par f du singleton $\{f(x)\}$.
- Par exemple, si Ω est un point fixé du plan, on définit une relation sur ce plan en posant $M\,\mathcal{R}\,N \Leftrightarrow d(\Omega,M)=d(\Omega,N)$: l'ensemble des classes d'équivalence est l'ensemble des cercles de centre Ω.
- La relation définie sur l'ensemble $\mathcal{D}$ des droites du plan affine par : $D\,\mathcal{R}\,\Delta \Leftrightarrow D/\!/\Delta$.
  Les classes d'équivalence correspondent aux différentes "directions" de droites.

1.6.5 Congruence modulo un réel strictement positif

Définition 1.6.7 (congruence modulo un réel $a > 0$)
Soit a un réel strictement positif. Les réels x et y sont dits *congrus* modulo a, et on note $x \equiv y\ (a)$, s'il existe un entier relatif q tel que $x - y = qa$.

Remarques

- La relation de congruence modulo a est une relation d'équivalence sur $\mathbb{R}$.
- Chaque classe a un représentant unique dans $[0, a[$ ou encore dans $\left[-\frac{a}{2}, \frac{a}{2}\right[$.
- Pour tout réel λ, on a : $x \equiv y\ (a) \ \Leftrightarrow\ x + \lambda \equiv y + \lambda\ (a)$
- Pour tout réel non nul λ, on a : $x \equiv y\ (a) \ \Leftrightarrow\ \lambda x \equiv \lambda y\ (\lambda a)$
- On a les équivalences classiques suivantes :

$$\cos y = \cos x \ \Leftrightarrow\ \begin{cases} y = x\ (2\pi) \\ \text{ou} \\ y = -x\ (2\pi) \end{cases} \qquad \sin y = \sin y \ \Leftrightarrow\ \begin{cases} y = x\ (2\pi) \\ \text{ou} \\ y = \pi - x\ (2\pi) \end{cases}$$

Par exemple : $\cos x = 1 \ \Leftrightarrow\ x \equiv 0\ (2\pi)$; $\sin(2x) = 0 \ \Leftrightarrow\ x = 0\ (\pi/2)$

1.6.6 Division euclidienne et congruence modulo un entier

Définition 1.6.8
Soit (a, b) dans $\mathbb{Z} \times \mathbb{N}^*$.
Il existe un unique couple (q, r) de $\mathbb{Z} \times N$ tel que : $(a = bq + r)$ et $(r \leqslant b - 1)$
Le passage du couple (a, b) au couple (q, r) s'appelle *division euclidienne* de a par b.
Dans cette division, a est le *dividende*, b le *diviseur*, q le *quotient*, et r le *reste*.

Démonstration

- On prouve l'existence d'une division $a = bq + r$ en supposant tout d'abord que a est dans $\mathbb{N}$.
  Soit A le sous-ensemble de $\mathbb{N}^*$ formé des entiers k tels que $kb > a$.
  Notons que $k = a + 1$ convient toujours car $(a + 1)b - a = a(b - 1) + b \geqslant b \geqslant 1$.
  L'ensemble A, partie non vide de $\mathbb{N}^*$, possède un minimum, que nous pouvons noter $q + 1$, avec q dans $\mathbb{N}$.
  Par définition $\begin{cases} q \notin A \\ q + 1 \in A \end{cases}$ c'est-à-dire $\begin{cases} qb \leqslant a \\ a < (q + 1)b \end{cases}$
  Ainsi $r = a - bq$ est un entier naturel strictement inférieur à b.
  On a donc trouvé un couple $(q, r) \in \mathbb{N}^2$ tel que $a = bq + r$, avec $0 \leqslant r \leqslant n - 1$.
- On suppose maintenant que a est un entier strictement négatif.
  Si a est un multiple de b, alors on a une égalité $a = bq + r$ avec $r = 0$.
  Si a (donc $-a$) n'est pas un multiple de b, on sait qu'on peut écrire $-a = q'b + r'$, avec $1 \leqslant r' \leqslant n - 1$, donc $a = -q'b - r' = -(q' + 1)b + b - r' = qb + r$ avec $q = -q - 1'$ et $r = b - r'$ (donc $1 \leqslant r = b - r' \leqslant n - 1$).
- Il reste à prouver *l'unicité* de l'écriture $a = bq + r$, avec q dans $\mathbb{Z}$, et $0 \leqslant r \leqslant n - 1$.
  Supposons alors qu'on ait aussi $a = bq' + r'$, avec $(q', r') \in \mathbb{N}^2$ et $r' \leqslant n - 1$.
  On doit montrer que les couples (q, r) et (q', r') sont égaux.
  On voit que $b(q' - q) = r - r'$, mais $-b < r - r' < b$. La seule possibilité est $q' - q = 0$.
  On trouve donc $q' = q$, puis $r' = r$. Le couple (q, r) obtenu plus haut est donc unique.

Remarque (divisibilité et division euclidienne) :
Soit a et b deux entiers relatifs. La proposition « b divise a » équivaut à dire que « $a = b = 0$ ou le reste dans la division de a par $|b|$ est nul ».

Définition 1.6.9 (congruence modulo un entier n de $\mathbb{N}^*$)
Soit n un entier naturel strictement positif. Les entiers relatifs a et b sont dits *congrus* modulo n, et on note $a \equiv b\ (n)$, s'il existe un entier relatif q tel que $a - b = qn$.

Remarques

- La relation de congruence modulo l'entier n est une relation d'équivalence sur $\mathbb{Z}$.
- Dire que les deux entiers a et b sont congrus module n, c'est dire que a et b ont le même reste dans la division euclidienne par n.
- Comme il y a n restes possibles dans la division par n, il y a exactement n classes d'équivalence.
  Les entiers $0, 1, 2, \ldots, n-1$ constituent une famille de représentants de chaque classe.
  L'ensemble des différentes classes d'équivalence s'écrit donc : $\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$.
- On a les propriétés suivantes (a, b, c sont dans $\mathbb{Z}$, m, n sont dans $\mathbb{N}^*$)
  $$\begin{cases} a \equiv b\ (n) \Leftrightarrow a + c \equiv b + c\ (n) \\ a \equiv b\ (n) \Rightarrow ma \equiv mb\ (mn) \Rightarrow ma \equiv mb\ (n) \\ a \equiv b\ (n) \Rightarrow a^m \equiv b^m\ (n) \end{cases}$$