UEO11 : Découverte des mathématiques
Année 2017-2018

Ce document et sa source LaTeX sont disponibles à l'adresse

http://github.com/dmegy/decouverteDesMaths

Version compilée le 23 janvier 2018

Table des matières

Chapitre 1

Logique et raisonnement

Sommaire

Retour à la table des matières principale

1.1 Préambule : vocabulaire et ensembles classiques

Afin de pouvoir illustrer les notions de ce chapitre dans le contexte des mathématiques, on part du principe qu'un certain nombre de choses sont connues :

1. Les ensembles classiques : $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, les mêmes privés de zéro : $\mathbb{N}^*$, ..., $\mathbb{C}^*$. Les lois de composition classiques sur ces ensembles : addition, multiplication, avec leurs règles de calcul.
2. L'égalité dans ces ensembles, la relation d'ordre dans $\mathbb{R}$: $x < y$ se lit « x est strictement inférieur à y », $x \leq y$ se lit « x est inférieur à y » (on précise parfois « inférieur ou égal » même si sans précision, une inégalité est toujours prise au sens large).
3. La relation de divisibilité dans $\mathbb{Z}$: la suite de symboles $a|b$ se lit « a divise b ».
4. Les notations d'appartenance d'un élément à un ensemble :on écrit $x \in E$ pour dire que x est un élément de l'ensemble E et $x \notin E$ sinon. Par exemple, $\frac{2}{3} \in \mathbb{Q}$, mais $\sqrt{2} \notin \mathbb{Q}$ (cela sera prouvé dans la suite du chapitre).
5. Les notations $\mathbb{R}_+$, $\mathbb{Q}_-$, etc pour des contraintes de signe (au sens large : 0 appartient à $\mathbb{Q}_+$ par exemple). On peut combiner : l'ensemble $\mathbb{R}_+^*$ est l'ensemble des réels strictement positifs.

6. Les fonctions classiques, comme la racine carrée et la valeur absolue.

Tout ceci sera revu en détail de toutes façons.

1.2 Propositions / assertions logiques

1.2.1 Définition. Une proposition (logique), ou assertion (logique) est une phrase à laquelle on peut attribuer le statut « VRAI » ou « FAUX ». La phrase peut en outre comporter des symboles qui désignent des objets mathématiques (comme des chiffres) et d'autres symboles qui désignent des relations mathématiques entre objets (par exemple l'égalité, inégalité, divisibilité, appartenance à un ensemble...)

Par exemple « $2+2=3$ » et « $2+3=5$ » sont des propositions (la première est fausse, la seconde vraie). La phrase « le nombre complexe i est positif » (ou encore « quelle heure est-il ? ») ne sont pas des propositions, on ne peut pas leur affecter de statut : la première n'a pas de sens (un nombre complexe n'a pas de signe), la seconde a un sens mais on ne peut pas lui affecter de statut VRAI ou FAUX.

Variables, paramètres, assertions ouvertes et fermées Une proposition peut dépendre d'un ou plusieurs paramètres, ou variables. Un paramètre est un symbole qui désigne un élément (explicité ou pas) d'un ensemble.

Les symboles nouveau doivent **toujours** être définis (ou déclarés) avec leur type (l'ensemble auquel appartient l'objet), de sorte à pouvoir être sûr du fait que la phrase est bien une assertion, c'est-à-dire possède un statut VRAI ou FAUX.

Par exemple : Dans « $x \geq 0$ », le symbole x n'est pas défini, on ne peut pas être sûr que la phrase ait un sens. Si x était un nombre complexe par exemple, la phrase n'aurait aucun sens. Le symbole x pourrait désigner beaucoup d'autres objets mathématiques, par exemple ... un cercle, les coordonnées d'un point du plan, auquel cas la phrase n'a pas non plus de sens.

D'autre part si x est un nombre naturel, la phrase a un sens mais elle est trivialement vraie car tous les naturels sont positifs. Tout ceci montre qu'il est crucial de déclarer clairement les variables et leur type *avant* de commencer à les utiliser.

Une assertion dont le statut ne dépend pas de la valeur d'un paramètre est dite *fermée*. Dans le cas contraire, elle est dite *ouverte*. Par exemple, « $2+2=5$ » est une assertion fermée, et $x^2+x+1 \leq 5$, qui dépend du paramètre $x \in \mathbb{R}$, est une assertion ouverte, son statut dépend de la valeur de x (par exemple, elle est fausse pour $x=2$ et vraie pour $x=1$).

On déclare des objets à l'aide de la locution « Soit ». La phrase « Soit x un réel. » déclare un réel, que l'on note x. La phrase « Soit $k \in \mathbb{Z}$. » déclare un entier relatif (l'usage de $\in$ comme abréviation pour « appartenant à »est toléré dans ce cas-là, même si en général on interdit d'utiliser les symboles mathématiques comme des abréviations).

La phrase « Soit x. » n'est pas une déclaration correcte d'objet mathématique : on doit préciser le type.

Si on précise que x est un nombre réel, « $x \geq 0$ »devient une assertion mathématique bien formée. Le statut de cette proposition dépend de la valeur de x : elle est vraie si $x \in \mathbb{R}_+$, elle est fausse si $x \in \mathbb{R}_-^*$. Le fait ne pas pouvoir connaître explicitement le statut n'est pas un problème. De fait que lorsqu'on déclare un réel x, on ne sait pas a priori lequel c'est.

1.3 Construction de propositions

Considérons deux propositions A et B. Dans les exemples qui suivent, sauf précision, x est un nombre réel.

Conjonction : « A et B » La proposition « A et B » est vraie si A et B sont vraies. Elle est fausse dès que l'une au moins des deux est fausse.

Exemple : « $x > 2$ et $x < 5$ » est vraie si $x \in]2,5[$. Elle est fausse sinon.

Disjonction : « A ou B » La proposition « A ou B » est vraie dès que l'une des deux est vraie, elle est fausse si les deux sont fausses. Lorsqu'on affirme que « A ou B »est vraie, l'un n'exclut pas l'autre.

Exemple : « $x > 2$ ou $x < 5$ » est vraie pour tout nombre réel x.

Négation : « non A » La proposition « non A » est vraie si A est fausse et inversement.

Implication logique : « $A \Rightarrow B$ » La proposition « $A \Rightarrow B$ »signifie par définition « B ou non-A ». Elle est vraie si A est fausse ou si B est vraie.
Exemples : $2+2=4 \Rightarrow 2\times 2=4$ est vraie. $2+2=5 \Rightarrow 2\times 2=4$ est vraie. $2+2=5 \Rightarrow 2\times 2=5$ est vraie. $2+2=4 \Rightarrow 2\times 2=5$ est fausse. Autre exemple : si x est un nombre réel, la proposition $x > 3 \Rightarrow x > 4$ est vraie pour $x \leq 3$ ou pour $x > 4$. Elle est fausse si $3 < x \leq 4$.

Attention : le symbole $\Rightarrow$ n'est en aucun cas une abréviation pour « donc ». La proposition $A \Rightarrow B$ ne veut pas dire « A est vraie donc B est vraie »!

Équivalence logique : « $A \Leftrightarrow B$ » La proposition « $A \Leftrightarrow B$ » signifie par définition « $A \Rightarrow B$ et $B \Rightarrow A$ ». Elle est vraie si A et B ont même statut, que ce soit vrai ou faux. Elle est fausse si A et B ont des statuts différents.
Exemples : $2+2=5 \Leftrightarrow 2\times 3=7$ est vraie. $1>0 \Leftrightarrow 2+2=4$ est vraie. Si x est un nombre réel, la proposition $x > 3 \Leftrightarrow x < 4$ est vraie pour $x \in]3,4[$. Elle est fausse sinon.

1.4 Quantificateurs

Soit $A(x)$ une proposition dépendant d'un paramètre x appartenant à un ensemble E (exemple : « $x > 3$ », où $x \in \mathbb{Z}$).

Quantificateur universel : $\forall$ (quelque soit/pour tout) La proposition « $\forall x \in E,\ A(x)$ » se lit « pour tout x dans E, $A(x)$ ». Elle est vraie si $A(x)$ est vraie pour toutes les valeurs que peut prendre x dans l'ensemble E. Elle est fausse dès qu'il existe une valeur spéciale de x pour laquelle $A(x)$ est fausse. Attention, contrairement à la proposition $A(x)$, la proposition $\forall x \in E,\ A(x)$ est une proposition qui ne dépend d'aucun paramètre : elle est soit vraie soit fausse : on dit que x est une variable muette, ou interne. Exemples : $\forall x \in R,\ x^2 > 1$ est fausse. La proposition $\forall x \in \mathbb{Z}^*,\ x^2 \geq 1$ est vraie.

Quantificateur existentiel : $\exists$ (il existe) La proposition « $\exists x \in E / A(x)$ » se lit « il existe x dans E tel que $A(x)$ ». Elle est vraie s'il y a une valeur de x dans l'ensemble E telle que $A(x)$ soit vraie. Elle est fausse si $A(x)$ est fausse pour toutes les valeurs de x.

1.4.1 Théorème. On a les équivalences suivantes :
non (non A) ⇔ A.
non (A ou B) ⇔ (non A) et (non B).
non (A et B) ⇔ (non A) ou (non B).
$(\forall x \in E,\ A(x)) \Leftrightarrow (\forall y \in E,\ A(y))$.
$\text{non}(\forall x \in E,\ A(x)) \Leftrightarrow \exists x \in E, \text{non}(A(x)))$.
$\text{non}(\exists x \in E,\ A(x)) \Leftrightarrow \forall x \in E, \text{non}(A(x)))$.

Démonstration : voir TD.

1.5 Méthodes de démonstration

1.5.1 Démonstration directe

Principe : pour montrer $A \implies B$, on suppose A vraie, et on montre que B est vraie.

Démonstration. En effet, si A est fausse, l'implication est vraie par définition donc il n'y a rien à prouver dans ce cas. □

1.5.1 Exemple. Soit $n \in \mathbb{Z}$; montrer que « n pair $\implies n^2$ pair ».

Exemple de rédaction:
Si n est pair, il existe $k \in Z$ tel que $n = 2k$. Alors, $n^2 = 4k^2 = 2(2k^2)$ est pair.

1.5.2 Démonstration par contraposée

Principe : $(A \implies B)$ est équivalente à (non-$B \implies$ non-A)

Démonstration. (non-$B \implies$ non-A) $\iff$ (non-A ou $non - non - B$) $\iff$ (B ou $non - A$). □

1.5.2 Exemple. Soit $n \in \mathbb{Z}$; montrer que n^2 pair $\implies n$ pair.

Exemple de rédaction:
On va montrer la contraposée, autrement dit on va montrer « n impair $\Rightarrow n^2$ impair », qui est équivalente, mais plus facile à montrer. Supposons donc n impair. Alors il existe $k \in \mathbb{Z}$ tel que $n = 2k+1$. Mais alors $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ est impair.

Note : en combinant avec le résultat précédent, on a donc prouvé, pour n un entier : « n^2 pair $\iff n$ pair. »

1.5.3 Démonstration par l'absurde

Principe : Si F désigne n'importe quelle proposition fausse, on a $A \iff$ (non-$A \implies F$).

Démonstration. (non-$A \implies F$) $\iff$ (F ou non-non-A) $\iff$ (F ou A) $\iff A$. □

Donc pour montrer A, il suffit de supposer A faux et d'en déduire une contradiction (c'est-à-dire n'importe quelle proposition fausse).

1.5.3 Exemple. Montrer que $\sqrt{2}$ n'est pas rationnel.

Exemple de rédaction:
Par l'absurde, supposons $\sqrt{2} \in \mathbb{Q}$. Alors il existe deux entiers p et q premiers entre eux tels que $\sqrt{2} = p/q$. Donc $p = q\sqrt{2}$ et donc $p^2 = 2q^2$, donc p^2 est pair, donc par l'exemple précédent p est pair. Donc il existe $k \in Z$ tel que $p = 2k$, d'où en remplacant $4k^2 = 2q^2$, donc en simplifiant q^2 est pair donc q est pair. Donc p et q sont tous les deux pairs, contradiction car ils sont premiers entre eux. Finalement cette contradiction prouve que $\sqrt{2} \notin \mathbb{Q}$.

1.5.4 Démonstrations par disjonction de cas

Principe : Pour démontrer $A \implies B$, on écrit A sous forme d'une disjonction : $A \iff A'$ ou A'', et on montre les deux implications $A' \implies B$ et $A'' \implies B$.
Démonstration.

$$\begin{aligned}(A \implies B) &\iff (B \text{ ou non-}A)\\ &\iff (B \text{ ou non-}(A' \text{ ou } A''))\\ &\iff (B \text{ ou } (non - A' et\, non - A''))\\ &\iff (B \text{ ou } non - A') \text{ et } (B \text{ ou } non - A'')\\ &\iff (A' \implies B \text{ et } A'' \implies B)\end{aligned}$$

□

1.5.4 Exemple. Soit $x \in \mathbb{R}$. Démontrer que $x^2 + \cos(x) > 0$.

Exemple de rédaction:
Soit $x \in \mathbb{R}$.
On distingue deux cas possibles suivant la valeur de x.
— Si $0 \leq |x| < \pi/2$, alors $x^2 \geq 0$ et $\cos(x) > 0$ donc $x^2 + \cos(x) > 0$.
— Si $\pi/2 \leq |x|$, alors $x^2 + \cos(x) \geq \pi^2/4 - 1 > 0$.
Finalement, dans tous les cas on a bien $x^2 + \cos(x) > 0$.

1.5.5 Démonstrations de propositions avec quantificateur universel

Pour démontrer $\forall x \in E,\ A(x)$, on écrit :
« Soit $x \in E$ un élément quelconque ».
Puis, on démontre $A(x)$.
Éventuellement, on écrit une phrase de conclusion, par exemple : « x étant pris quelconque dans E, la propriété est bien démontrée ».

1.5.5 Exemple. Montrer que $\forall x \in \mathbb{R}, x^2 + x + 1 > 0$ ».

Exemple de rédaction:
Soit $x \in \mathbb{R}$. (déclaration de x)
On a $x^2 + x + 1 = (x + \frac{1}{2})^2 + \frac{3}{4}$. (Début preuve de $A(x)$)
Comme un carré est toujours positif, on a $(x + \frac{1}{2})^2 \geq 0$
et donc $x^2 + x + 1 > 0$. (fin preuve de $A(x)$)
Ceci montre donc bien $\forall x \in \mathbb{R}, x^2 + x + 1 > 0$ (Conclusion)

1.5.6 Cas particulier : démonstrations par récurrence

Dans le cas particulier où le quantificateur universel porte sur l'ensemble $\mathbb{N}$, on peut utiliser une méthode de preuve spécifique, la récurrence. Cette méthode de démonstration s'appuie sur le fait que toute partie non vide de $\mathbb{N}$ admet un plus petit élément (ce qui est faux pour la plupart des autres ensembles classiques). Il suffit alors de montrer d'une part que $A(0)$ est vraie, ce qui est généralement facile, puis de montrer que pour tout $n \in \mathbb{N}$, on a $A(n) \Rightarrow A(n+1)$. La première étape est cruciale et le raisonnement est faux si on l'omet.

1.5.7 Démonstrations de propositions avec quantificateur existentiel

Pour démontrer « $\exists x \in E / A(x)$, il faut soit construire un élément x tel que $A(x)$ soit vrai, soit utiliser un théorème qui affirme dans sa conclusion l'existence d'un tel objet (ou qui affirme l'existence d'un objet à partir duquel on peut obtenir l'existence de x).

1.5.6 Exemple. Soit f une fonction croissante de $[0,1]$ dans $\mathbb{R}$. Montrer que f est majorée, autrement dit montrer que $(\exists M \in \mathbb{R} / (\forall x \in [0,1],\ f(x) \leq M))$.

Exemple de rédaction:
Posons $M = f(1)$. On a bien $\forall x \in [0,1],\ f(x) \leq f(1) = M$, car f est croissante.

1.5.7 Exemple. Montrer qu'il existe deux irrationnels a et b tels que a^b soit rationnel.

Exemple de rédaction:
Considérons le nombre réel $\sqrt{2}^{\sqrt{2}}$. Il est soit rationnel, soit irrationnel. Dans le premier cas, il suffit de poser $a = b = \sqrt{2}$ (irrationnels, voir exemple plus haut) et la preuve est terminée. Dans le second cas, il suffit de poser $a = \sqrt{2}^{\sqrt{2}}$ (qui est supposé irrationnel) et $b = \sqrt{2}$ On a alors $a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2 \in \mathbb{Q}$.

Ce deuxième exemple montre que parfois, on n'a pas besoin de construire explicitement l'objet, seulement de montrer que ça existe, soit par l'analyse de cas de figure complémentaires, soit en utilisant un théorème qui affirme l'existence d'un certain objet sans forcément l'expliciter. Cela dit, la plupart du temps, il faut construire l'objet.

1.6 Résolution des équations

Soit $A(x)$ une proposition portant sur $x \in E$. Résoudre $A(x)$, c'est déterminer exactement l'ensemble des x tels que $A(x)$ soit vrai. Cet ensemble est un sous-ensemble de E, on l'appelle l'ensemble des solutions. Il peut parfois être vide (aucune solution) ou égal à E (équation triviale).

Méthode par équivalence
$A(x) \iff B(x) \iff \ldots \iff C(x)$ et on sait facilement résoudre $C(x)$. Cette méthode ne s'applique que rarement, essentiellement qu'aux (systèmes d') équations linéaires.

1.6.1 Exemple. Résoudre $2x+3=5$, d'inconnue $x \in \mathbb{R}$.

Exemple de rédaction:
Soit $x \in \mathbb{R}$. On a

$$\begin{aligned} 2x+3=8 &\iff 2x=5 \\ &\iff x=\frac{5}{2}. \end{aligned}$$

L'ensemble des solutions de cette équation est donc $\left\{\frac{5}{2}\right\}$.

Méthode par conditions nécessaires et suffisantes Lorsque $A(x) \implies B(x)$, on dit que $B(x)$ est une condition nécessaire à $A(x)$, et $A(x)$ est une condition suffisante pour $B(x)$.
Dans la pratique, on écrit $A(x) \implies B(x) \implies \dots x \in \Omega$. Ensuite, parmi les éléments de Ω, on détermine ceux qui sont effectivement solution.

Exemple : résoudre $|x-1| = 2x+3$, d'inconnue $x \in \mathbb{R}$.

Exemple de rédaction:
Soit $x \in \mathbb{R}$. On a la chaîne d'implications $|x-1| = 2x+3 \Rightarrow |x-1|^2 = (2x+3)^2 \Leftrightarrow x^2 - 2x + 1 = 4x^2 + 12x + 9 \iff 3x^2 + 14x + 8 = 0 \iff (x \in \{-4; -2/3\})$. Réciproquement, on vérifie que -4 n'est pas solution mais que $-2/3$ est solution. Finalement, l'équation a une unique solution, $-2/3$.

Chapitre 2

Ensembles

Sommaire

Retour à la table des matières principale

2.1 Définitions (ou pas)

En mathématiques, le sens du mot *ensemble* est plus précis que celui donné par la langue française. Définir rigoureusement ce qu'est un ensemble (au sens mathématique du terme) est assez complexe et dans ce cours, on utilisera la définition intuitive suivante.

2.1.1 Définition. (Ensemble, définition intuitive)

1. Un *ensemble* E est une collection d'objets.
2. Les objets dont est constitué la collection définissant E sont les *éléments* de E.
3. On dit que x appartient à E et on note $x \in E$ si x est un élément de E. On note $x \notin E$ dans le cas contraire.
4. Deux ensembles E et F sont dits *égaux* s'ils ont les mêmes éléments. Dans ce cas on note $E = F$ (et $E \neq F$ dans le cas contraire).

(La définition donnée est insuffisante car en réalité, toutes les collections ne sont pas autorisées (pour éviter certains paradoxes). Mais la plupart de celles auxquelles on peut penser forment bien des ensembles au sens mathématique du terme).

2.1.2 Définition. (Manières de définir un ensemble)

1. Une définition *par énumération* d'un ensemble E est la donnée explicite de tous les éléments de l'ensemble, sous forme de liste entre accolades. Par exemple : $E = \left\{1, 3, \pi, 5, \sqrt{2}\right\}$.
2. Une définition *par compréhension* d'un ensemble E est la donnée d'une propriété qui caractérise les éléments de E parmi un ensemble plus gros F. Par exemple : $E = \{x \in \mathbb{R} \mid x^2 + x \leq 2\}$, qui se lit « E est l'ensemble des réels x tels que $x^2 + x \leq 2$ ».

Attention, dans une définition par énumération, il n'y a pas de notion d'ordre, ni de multiplicité (un élément ne peut pas appartenir « plusieurs fois » à un ensemble). Donc $\left\{1, 3, \pi, 5, \sqrt{2}\right\} = \left\{\sqrt{2}, 3, 5, 1, \pi\right\} = \left\{\sqrt{2}, 2, 2, 3, 3, 5, 1, 1, \pi\right\}$.

2.1.3 Définition. (Ensemble vide, singleton, paire)

1. L'*ensemble vide* est l'unique ensemble ne contenant aucun élément. On le note $\varnothing$ (la notation $\{\}$ est également correcte mais n'est pas utilisée). Une assertion du type « $\forall x \in \varnothing, A(x)$ » est toujours vraie par définition. L'ensemble vide est inclus dans tout ensemble, puisque l'assertion « $\forall x \in \varnothing, x \in E$ » est toujours vraie.
2. Un *singleton* est un ensemble contenant un unique élément. C'est donc un ensemble de la forme $\{x\}$.
3. Une *paire* est un ensemble de la forme $\{a, b\}$. Si $a = b$, alors il s'agit d'un singleton, mais la plupart des cas, les éléments sont différents et $\{a, b\}$ est donc un ensemble contenant deux éléments distincts.

2.2 Parties d'un ensemble

2.2.1 Définition (Sous-ensemble / partie)**.** Soient E et F des ensembles. On dit que E est inclus dans F, ou que E est un sous-ensemble, ou une partie de F si tous les éléments de E sont des éléments de F, autrement dit si

$$\forall x \in E, x \in F.$$

Dans ce cas on note $E \subset F$ (notation la plus répandue) ou $E \subseteq F$ (dans ce cours, les deux notations sont synonymes et on privilégie la seconde). On note $E \not\subset F$ ou $E \nsubseteq F$ si E n'est pas un sous-ensemble de F, et $E \subsetneq F$ si c'est un sous-ensemble *strict* de F, c'est-à-dire $E \subseteq F$ et $E \neq F$.

2.2.2 Remarque (Principe de double-inclusion)**.** *Si E et F sont des ensembles, alors $E = F \iff (E \subseteq F \text{ et } F \subseteq E)$.*

2.2.3 Remarque. *Attention, les objets x et $\{x\}$ sont différents! Par exemple, $\varnothing$ et $\{\varnothing\}$ sont deux ensembles différents : le premier est l'ensemble vide, alors que $\{\varnothing\}$ est un ensemble non vide : c'est un ensemble contenant un élément (l'ensemble vide).*

2.2.4 Axiome et Définition (Ensemble des parties)**.** Soit E un ensemble. La collection de toutes les parties de E est un ensemble (au sens mathématique). On le note $\mathscr{P}(E)$.

Ainsi, si F est un ensemble, alors on a $F \in \mathscr{P}(E) \iff F \subseteq E$.

Remarque : cet ensemble n'est jamais vide car il contient toujours au moins $\varnothing$, qui est une partie de tout ensemble E.

2.2.5 Exemple. Un singleton $\{a\}$ contient deux parties : la partie vide $\varnothing$ et la partie $\{a\}$.

L'ensemble $\{1, 2\}$ a pour ensemble de parties : $\mathscr{P}(\{1, 2\}) = \{\varnothing, \{1\}, \{2\}, \{1, 2\}\}$.

2.3 Union, intersection, complémentaire, produit

2.3.1 Définition. (Union, intersection, complémentaire)

Soient A et B des ensembles. Leur *union*, notée $A \cup B$, est la collection formée par les éléments de A et de B. Leur *intersection*, notée $A \cap B$, est l'ensemble des éléments de A qui sont également des éléments de B (ou encore : l'ensemble des éléments de B qui sont aussi des éléments de A).

L'ensemble $A \setminus B$ est l'ensemble des éléments de A qui n'appartiennent pas à B.

Si A est un sous-ensemble d'un ensemble E, le complémentaire de A dans E est $E \setminus A$, on le note aussi $\complement A$ s'il n'y a pas d'ambiguïté sur l'ensemble E dans lequel on prend le complémentaire de A.

2.3.2 Proposition. Si A et B sont deux parties d'un ensemble E, on a :

$$\complement(A\cup B)=\complement A\cap\complement B;\quad \complement(A\cap B)=\complement A\cup\complement B.$$

Démonstration. Soit $x\in E$. Alors :

$$\begin{aligned} x\in\complement(A\cup B) &\iff \text{non}(x\in A\cup B)\\ &\iff \text{non}(x\in A \text{ ou } x\in B)\\ &\iff \text{non}(x\in A) \text{ et } \text{non}(x\in B)\\ &\iff \left(x\in\complement A\right) \text{ et } \left(x\in\complement B\right)\\ &\iff x\in\complement A\cap\complement B. \end{aligned}$$

□

2.3.3 Définition (Ensembles disjoints, unions disjointes)**.** Deux ensembles A et B sont *disjoints* si leur intersection est vide : $A\cap B=\varnothing$.

2.3.4 Définition (Produit cartésien)**.** Soient E et F deux ensembles. Le *produit cartésien*, ou simplement *produit*, noté $E\times F$, est la collection de tous les couples de la forme (x,y), avec $x\in E$ et $y\in F$. Si $E=F$, on note E^2 au lieu de $E\times E$.

On peut définir de même les produits finis du type $E_1\times E_2\times\ldots E_n$: leurs éléments sont les n-uplets de la forme $(x_1,x_2,\ldots x_n)$, avec $x_1\in E_1$, $x_2\in E_2$ etc.

2.3.5 Remarque. $E\times F=\varnothing \iff (E=\varnothing \text{ ou } F=\varnothing)$.

2.3.6 Définition (Diagonale)**.** Soit E un ensemble. La *diagonale* de $E\times E$ est l'ensemble des couples d'éléments identiques, c'est-à-dire l'ensemble

$$\Delta_E=\{(x,x)\mid x\in E\}$$

2.4 Familles indexées

2.4.1 Définition. Soient E et I des ensembles. Une famille d'éléments de E indexée par I est un objet de la forme $(x_i)_{i\in I}$, c'est-à-dire la donnée, pour tout élément $i\in I$, d'un élément de E noté x_i.

2.4.2 Exemple. Une suite réelle $(u_n)_{n\in\mathbb{N}}$ est une famille de réels indexée par $\mathbb{N}$.

L'ensemble I qui sert à indexer la famille peut être fini ou infini, et s'il est infini, il peut être plus gros que $\mathbb{N}$: il n'est pas nécessaire de pouvoir numéroter les éléments de la famille par des nombres : une famille peut être indexée par $\mathbb{R}$. Par exemple, si $a\in\mathbb{R}$, on peut définir la fonction $f_a:\mathbb{R}\to\mathbb{R}; x\mapsto e^{ax}$. Les fonctions f_a forment la famille $(f_a)_{a\in\mathbb{R}}$.

2.4.3 Définition (Unions et intersections indexées par un ensemble)**.** Soit E un ensemble, et $(E_i)_{i\in I}$ une famille de parties de E indexée par un ensemble I.

Leur *union*, notée $\bigcup\limits_{i\in I}E_i$, est l'ensemble $\{x\in E \mid \exists i\in I, x\in E_i\}$.

Leur *intersection*, notée $\bigcap\limits_{i\in I}E_i$, est l'ensemble $\{x\in E \mid \forall i\in I, x\in E_i\}$.

Chapitre 3

Applications

Sommaire

Retour à la table des matières principale

3.1 Applications, graphes

Résumé : applications, graphes, source, but, images, antécédents, ensemble des fonctions de E dans F, fonction caractéristique, point fixe d'une application

3.1.1 Définition (Graphe d'application)**.** Soient E et F deux ensembles, et $\Gamma \subseteq E \times F$. On dit que Γ est un *graphe d'application de E dans F* si la condition suivante est vérifiée :

$$\forall x \in E, \exists! y \in F, (x, y) \in \Gamma.$$

3.1.2 Exemple (Application directe de la définition)**.**

1. Si $E = \{1, 2, 3\}$ et $F = \{1, 4\}$, alors l'ensemble $\Gamma = \{(1, 4), (2, 1), (3, 1)\} \subseteq E \times F$ est un graphe d'application.
   L'ensemble $\Gamma' = \{(1, 1), (2, 4)\} \subseteq E \times F$ n'est pas un graphe d'application.
   L'ensemble $\Gamma'' = \{(1, 1), (2, 1), (2, 4), (3, 4)\} \subseteq E \times F$ non plus.
2. Si $E = F = \mathbb{R}$, l'ensemble $\Gamma = \{x, y) \in \mathbb{R}^2 \mid y = x^2\}$ est un graphe d'application, mais pas l'ensemble $\Gamma' = \{x, y) \in \mathbb{R}^2 :\mid x = y^2\}$. Par contre, si $E = F = (\mathbb{R}_+)^2$, l'ensemble $\Gamma'' = \{x, y) \in (\mathbb{R}_+)^2 :\mid x = y^2\}$ est un graphe d'application de E dans F.
3. Pour un sous-ensemble $\Gamma \subseteq E \times F$, être un graphe d'application de E dans F ne dépend pas que de l'ensemble Γ lui-même mais aussi de E et de F. Par exemple, si $E = \mathbb{R}_+$ et $F = \mathbb{R}_+$, alors $\Gamma = \{(x, y) \in \mathbb{R}_+ \times \mathbb{R}_+ \mid x = y^2\}$ est un graphe d'application de E dans F. Par contre, si $E = \mathbb{R}$ et $F = \mathbb{R}_+$, l'ensemble $\{(x, y) \in \mathbb{R} \times \mathbb{R}_+ \mid x = y^2\}$ (c'est le même que le précédent : les éléments sont les mêmes) n'est *pas* un graphe d'application de E dans F.

3.1.3 Définition (Applications/fonction entre ensembles)**.** Une *application* ou *fonction* (dans ce cours, les deux mots sont synonymes) f est la donnée de trois objets :

1. un ensemble E, appelé le *domaine* ou la *source*, ou encore l'*ensemble de départ* de f ;
2. un ensemble F, appelé le *codomaine* ou le *but* ou encore l'*ensemble d'arrivée* de f ;
3. une partie $\Gamma_f \subseteq E \times F$, appelée le *graphe de f* qui est un *graphe d'application* au sens de la définition précédente.

Ceci revient à donner E, F, et pour tout élément $x \in E$, un élément (unique) $y \in F$, appelé l'*image de x par f*. Cet élément est noté $f(x)$.

Deux fonctions sont égales si elles ont même source et but, et si les images des éléments sont les mêmes. (Et il n'est pas suffisant de demander que les images soient les mêmes.)

3.1.4 Définition (Image d'une application)**.** Soit $f : E \to F$. L'*image* de f est l'ensemble de toutes les images des éléments de E par f :

$$\{f(x) \mid x \in E\}$$

3.1.5 Remarque. 1. *Si f est une application de $\mathbb{R}$ dans $\mathbb{R}$, ce que l'on appelle souvent une « représentation graphique de f » est en fait une représentation graphique de son graphe. La représentation graphique n'est pas unique (l'échelle peut varier, on ne représente en général pas le domaine ni le codomaine en entier mais seulement une partie, etc) mais le graphe, lui, est un objet mathématique abstrait et unique.*

2. *Une fonction ne peut pas être uniquement définie par son graphe : la donnée du domaine et du codomaine sont nécessaires.*
3. *(Zérologie : application vide) Soit $E = \varnothing$ et F un ensemble. Il existe une (unique) application de E dans F, appelée* application vide*, celle dont le graphe Γ est la partie vide de $E \times F = \varnothing$. (Si $E = \varnothing$, l'assertion « $\forall x \in E, \exists! y \in F, (x, y) \in \Gamma$ » est effectivement vraie même si Γ est vide et donc Γ est bien un graphe d'application.)*

Pour définir une fonction de E dans F, on écrit « Soit $f : E \to F$ une fonction ». Pour définir une fonction particulière, plutôt que donner son graphe comme le demanderait la définition, on utilise le symbole « $\mapsto$ » qui se lit « est envoyé sur / s'envoie sur / est associé à » comme dans l'exemple suivant :

$$\text{Soit } f : \mathbb{Z} \to \mathbb{R},\ n \mapsto \sqrt{n^2 + n + 1}.$$

Ceci se lit par exemple « Soit f l'application de $\mathbb{Z}$ dans $\mathbb{R}$ qui à (un entier relatif) n associe (le réel) $\sqrt{n^2 + n + 1}$ ».

(Dans cet exemple, on devrait auparavant justifier que l'expression sous le radical désigne bien un réel positif, c'est bien le cas : exercice.)

On rencontre également la mise en forme du type suivant :

$$\text{Soit } f : \begin{cases} \mathbb{Z} \to \mathbb{R}, \\ n \mapsto \sqrt{n^2 + n + 1}. \end{cases}$$

3.1.6 Définition. Soient E et F des ensembles. L'ensemble des fonctions de E dans F est noté $\mathscr{F}(E, F)$ ou bien F^E (attention à l'ordre dans la seconde notation).

3.1.7 Remarque. *Un graphe de fonction n'est pas forcément défini par une formule simple du type $y = \sin(x)$, ou $y = x^2 + e^x$. Par exemple, on peut utiliser plusieurs formules suivant l'endroit du domaine où se trouve la variable :*

$$f : \mathbb{R} \to \mathbb{R}, x \mapsto \begin{cases} \sqrt{x} \text{ si } x \geq 0 \\ x^2 + x + e^x \text{ sinon.} \end{cases}$$

3.1.8 Définition (Antécédents d'un élément)**.** Soit $f : E \to F$ une fonction, et $y \in F$. On dit qu'un élément $x \in E$ est un *antécédent* de y si $f(x) = y$. En reformulant, l'ensemble des antécédents de y est donc l'ensemble des solutions de l'équation $f(x) = y$, d'inconnue $x \in E$.

3.1.9 Exemple. Un élément du codomaine peut ne pas avoir d'antécédents, ou en avoir plusieurs. Par exemple, si $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$, alors l'élément -1 n'a aucun antécédent (il n'existe pas de $x \in \mathbb{R}$ tel que $f(x) = x^2 = -1$). L'élément 0 a exactement un antécédent (0), et l'élément 4 a deux antécédents : 2 et -2.

3.1.10 Définition (Fonction caractéristique)**.** Soit E un ensemble et $A \in \mathscr{P}(E)$ une partie de E. La *fonction caractéristique* de A (sous-entendu, dans E) est la fonction

$$1_A : \begin{cases} E \to \{0,1\}, \\ x \mapsto \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{si } x \notin A \end{cases} \end{cases}$$

3.1.11 Définition (Point fixe)**.** Soit $f : E \to E$ une application d'un ensemble dans lui-même. Un élément $x \in E$ est dit *fixe par f* (ou simplement *fixe* s'il n'y a pas d'ambiguïté sur la fonction), si $f(x) = x$. On dit aussi que x est un *point fixe* de f.

Pour terminer ce paragraphe, on introduit un outil indispensable pour visualiser efficacement plusieurs ensembles et applications d'un seul coup : les diagrammes.

3.1.12 Définition (Diagramme)**.** Lorsque l'on est en présence de plusieurs ensembles et de plusieurs applications entre ces ensembles, il est classique de visualiser la situation à l'aide d'un diagramme. Un diagramme (d'applications entre ensembles) est un graphe orienté dont chaque sommet représente un ensemble et chaque arête (orientée) représente une application.

Attention, un tel graphe n'est pas simple, autrement dit il peut avoir des boucles (s'il y a des applications d'un ensemble dans lui-même) ou des arêtes multiples (s'il y a plusieurs applications distinctes entre deux ensembles donnés).

3.1.13 Exemple.

1. Étant donnés des ensembles A, B, C et D et des applications $f : A \to B$, $g : A \to C$, $h : D \to A$, $\phi : D \to C$, $\psi : B \to A$, on peut représenter la situation en donnant simplement diagramme suivant :

$$\begin{tikzcd} A \arrow[r, bend left, "f"] \arrow[d, "g"'] & B \arrow[l, bend left, "\psi"] \\ C & D \arrow[l, "\phi"] \arrow[ul, "h"] \end{tikzcd}$$

2. Étant donnés des ensembles E et F et des applications $f : E \to E$, $g : E \to F$ et $h : E \to F$, on peut représenter la situation par le diagramme :

$$\begin{tikzcd} E \arrow[loop left, "f"] \arrow[r, bend left, "g"] \arrow[r, bend right, "h"'] & F \end{tikzcd}$$

3.2 Composition

Résumé : composition, factorisation, la composition est associative, fonction identité, diagramme (commutatif ou pas),

3.2.1 Définition (Composition)**.** Soit $f : X \to Y$ et $g : Y \to Z$ deux fonctions. La composée de g et de f est la fonction $g \circ f$ (se lit « g rond f ») de X dans Z qui à $x \in X$ associe $g(f(x)) \in Z$. Autrement dit, par définition, $(g \circ f)(x) = g(f(x))$.

Une composition d'applications se visualise à l'aide du diagramme suivant (attention à l'ordre : appliquer la fonction $g \circ f$ consiste à appliquer f *suivie* de g) :

$$\begin{tikzcd} X \arrow[r, "f"'] \arrow[rr, bend left, "g\circ f"] & Y \arrow[r, "g"'] & Z \end{tikzcd}$$

Plus généralement, pour pouvoir composer deux fonctions il est suffisant que le codomaine de la première fonction (dans l'ordre de la composition) soit inclus dans le domaine de la seconde. (Cette condition est bien sûr également nécessaire, autrement l'écriture $g(f(x))$ n'a pas de sens. Deux fonctions quelconques ne sont donc en général pas composables.)

3.2.2 Définition (Factorisation d'une application comme composée d'autres applications)**.** Écrire une application f sous la forme d'une composition $f = g \circ h$, c'est la *factoriser*. Plusieurs factorisations sont possibles. Par exemple, si $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2 + 1$, on peut écrire $f : g \circ h$, avec

$$h : \mathbb{R} \to \mathbb{R}, x \mapsto x^2 \text{ et } g : \mathbb{R} \to \mathbb{R}, x \mapsto x + 1.$$

3.2.3 Mise en garde (La composition n'est pas commutative)**.** Attention, même si les domaines et codomaines permettent de composer deux fonctions dans les deux sens, les fonctions $g \circ f$ et $g \circ f$ obtenues sont en général distinctes. Par exemple, avec $f : \mathbb{R} \to R, x \mapsto x^2$ et $g : \mathbb{R} \to \mathbb{R}, x \mapsto x + 1$, on peut composer dans les deux sens mais on a :

$$\begin{aligned} g \circ f &: \mathbb{R} \to \mathbb{R}, x \mapsto g(f(x)) = g(x^2) = x^2 + 1, \\ f \circ g &: \mathbb{R} \to \mathbb{R}, x \mapsto f(g(x)) = f(x+1) = (x+1)^2 = x^2 + 2x + 1. \end{aligned}$$

3.2.4 Proposition (« La composition est associative »)**.** Soient $f : X \to Y$, $g : Y \to Z$, $h : Z \to T$ des fonctions. Alors $h \circ (g \circ f) = (h \circ g) \circ f$. Cette fonction est notée $h \circ g \circ f$.

Ce résultat se visualise à l'aide du diagramme :

$$\begin{tikzcd} X \arrow[r, "f"'] \arrow[rr, bend left, "g\circ f"] \arrow[rrr, bend left=50, "h\circ(g\circ f)"] \arrow[rrr, bend right=50, "(h\circ g)\circ f"'] & Y \arrow[r, "g"'] \arrow[rr, bend right, "h\circ g"'] & Z \arrow[r, "h"] & T \end{tikzcd}$$

Démonstration. Les domaines et codomaines sont les mêmes (X et T), et si $x \in X$, on a

$$\big(h \circ (g \circ f)\big)(x) = h((g \circ f)(x)) = h(g(f(x)) \text{ et}$$

$$\big((h \circ g) \circ f\big)(x) = (h \circ g)(f(x)) = h(g(f(x))$$

d'où l'égalité des deux fonctions. □

Cette proposition permet de ne pas avoir à noter les parenthèses lors de compositions successives, puisque toutes les possibilités de parenthésage donnent la même fonction.

3.2.5 Définition (Fonction identité)**.** Soit E un ensemble. La fonction identité sur E est la fonction $\mathrm{Id}_E : E \to E, x \mapsto x$. (En d'autres termes, la fonction identité de E est la fonction de E dans E dont tous les points sont fixes.)

3.2.6 Mise en garde. 1. Ne pas confondre la fonction identité avec une fonction constante (ou avec fonction nulle si le but est $\mathbb{R}$).

2. Si $\phi = E \to F$, alors $\phi = \phi \circ \mathrm{Id}_E = \mathrm{Id}_F \circ \phi$.

3.2.7 Définition (Diagramme commutatif)**.** Considérons un diagramme d'applications entre ensembles. En général, il y a plusieurs chemins entre deux sommets donnés, et ces chemins correspondent à différentes fonctions composées entre les deux ensembles.

On dit que le diagramme *est commutatif* (ou *qu'il commute*) lorsque pour tout couple de sommets, les différentes applications composées reliant ces ensembles sont égales.

3.2.8 Exemple. 1. Par exemple, dire que le diagramme
$$\begin{tikzcd} X \arrow[r, "h"] \arrow[d, "f"'] & Z \\ Y \arrow[ur, "g"'] & \end{tikzcd}$$
est commutatif revient à dire que $h = g \circ f$.

2. Dire que le diagramme
$$\begin{tikzcd} A \arrow[r, "\phi"] \arrow[d, "f"'] & B \arrow[d, "g"] \\ C \arrow[r, "\psi"] & D \end{tikzcd}$$
est commutatif revient à dire que $\psi \circ f = g \circ \phi$. Un tel diagramme est appelé *carré commutatif.*

3.2.9 Définition (Fonction involutive/involution)**.** Soit $f : E \to E$ une fonction ayant même source et but. On dit que f est *involutive*, ou que c'est une *involution*, si $f \circ f = \mathrm{Id}_E$.

3.2.10 Exemple. La fonction $f : \mathbb{R} \to \mathbb{R}, x \mapsto 1 - x$ est involutive.

3.3 Applications réciproques, sections et rétractions

Résumé : fonctions réciproque, unicité de la réciproque, sections et rétractions

3.3.1 Définition (Fonction réciproque)**.** Soient $f : E \to F$ et $g = F \to E$ deux fonctions. On dit qu'elles sont réciproques l'une de l'autre (ou que g est une réciproque de f, ou que f est une réciproque de g) si $g \circ f = \mathrm{Id}_E$ <u>et</u> $f \circ g = \mathrm{Id}_F$.

$$\begin{tikzcd} E \arrow[loop left, "\mathrm{Id}_E"] \arrow[loop right, "g\circ f"] \arrow[rr, bend left, "f"] & & F \arrow[loop left, "f\circ g"] \arrow[loop right, "\mathrm{Id}_F"] \arrow[ll, bend left, "g"] \end{tikzcd}$$

Attention, une fonction f n'a pas toujours de fonction réciproque !

3.3.2 Proposition. Soit $f : E \to F$ une fonction. Si elle admet une (fonction) réciproque, alors celle-ci est unique. Elle est notée généralement f^{-1}.

Démonstration. Soient en effet $g = F \to E$ et $h : F \to E$ deux réciproques de f. Alors

$$g \circ f \circ h = (g \circ f) \circ h = \mathrm{Id}_E \circ h = h, \text{ et}$$

$$g \circ f \circ h = g \circ (f \circ h) = g \circ \mathrm{Id}_F = g$$

d'où $g = h$. □

3.3.3 Mise en garde.
1. On ne doit pas utiliser la notation f^{-1} avant d'avoir démontré que la fonction admet effectivement une réciproque.
2. Ne pas confondre fonction réciproque f^{-1} et fonction *inverse* $\dfrac{1}{f}$. La notion de fonction inverse concerne les fonctions à valeurs réelles qui ne s'annulent pas et n'a rien à voir avec la notion de réciproque.

3.3.4 Exemple. Les fonctions $f = \mathbb{R} \to \mathbb{R}_+^*, x \mapsto e^x$ et $g : \mathbb{R}_+^* \to R, x \mapsto \ln(x)$ sont réciproques l'une de l'autre.

3.3.5 Mise en garde. Dans la définition de réciproque, les conditions $g \circ f = \mathrm{Id}_E$ et $f \circ g = \mathrm{Id}_F$ sont toutes les deux nécessaires : il est en effet possible que l'une soit vérifiée et pas l'autre. Par exemple, les fonctions

$$f : \mathbb{R}_+ \to \mathbb{R}, x \mapsto \sqrt{x} \quad \text{et} \quad g : \mathbb{R} \to \mathbb{R}_+, x \mapsto x^2$$

vérifient $g \circ f = \mathrm{Id}_{\mathbb{R}_+}$, mais $f \circ g \neq \mathrm{Id}_{\mathbb{R}}$: en effet, on a $(f \circ g)(x) = \sqrt{x^2} = |x| \neq x$.

Dans ce type de cas, on n'est pas en présence de fonctions réciproques mais la situation porte tout de même un nom. C'est l'objet de la définition suivante.

3.3.6 Définition (Rétraction/inverse à gauche, section/inverse à droite)**.** Soit $f : E \to F$ une fonction.

1. Une *rétraction* (ou *inverse à gauche*) de f, est une fonction $r : F \to E$ telle que $r \circ f = \mathrm{Id}_E$.

$$\begin{tikzcd} E \arrow[loop left, "\mathrm{Id}_E"] \arrow[r, bend left, "f"] & F \arrow[l, bend left, "r"] \end{tikzcd}$$

2. Une *section* (ou *inverse à droite*) de f, est une fonction $s : F \to E$ telle que $f \circ s = \mathrm{Id}_F$.

$$\begin{tikzcd} E \arrow[r, bend left, "f"] & F \arrow[l, bend left, "s"] \arrow[loop right, "\mathrm{Id}_F"] \end{tikzcd}$$

3.3.7 Exemple. Soit $f = \mathbb{R} \to \mathbb{R}_+, x \mapsto x^2$. Alors les fonctions $s_1 : \mathbb{R}_+ \to \mathbb{R}, x \mapsto \sqrt{x}$ et $s_2 : \mathbb{R}_+ \to \mathbb{R}, x \mapsto -\sqrt{x}$ sont deux sections (inverses à droite) distinctes de f (on a bien $f \circ s_1 = \mathrm{Id}_{\mathbb{R}^+}$ et $f \circ s_2 = \mathrm{Id}_{\mathbb{R}^+}$). Par ailleurs, f est une rétraction de s_1 et de s_2. (Voir remarque ci-dessous.)

3.3.8 Remarque.
1. *Une fonction g est une rétraction de f si et seulement si f est une section de g puisque les deux assertions signifient* $g \circ f = \mathrm{Id}_E$ *: les deux notions sont « duales ».*
2. *Les sections et rétractions, lorsqu'elles existent, ne sont en général pas uniques (contrairement à la fonction réciproque qui est unique si elle existe).*
3. *Une fonction réciproque est à la fois une rétraction et une section (ou : à la fois un inverse à gauche et un inverse à droite).*
4. *De même que toutes les fonctions n'ont pas forcément de réciproque, toutes les fonctions n'admettent pas forcément une section ou une rétraction. Par exemple,* $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$ *n'admet ni section ni rétraction.*

3.4 Restriction, prolongement, corestriction

Résumé : restriction, prolongement, corestriction

3.4.1 Définition (Restriction)**.** Soit $f : E \to F$ et $A \in \mathscr{P}(E)$ une partie de E. La *restriction* de f à A, notée $f|_A$, est l'application de A dans F suivante :

$$f|_A : A \to F, x \mapsto f(x)$$

Attention, les fonctions $f|_A$ et f doivent être considérées comme distinctes car leurs domaines sont distincts (A au lieu de E).

3.4.2 Remarque. *Dans le contexte de la définition, si on note $i : A \to E, x \mapsto x$ l'inclusion de A dans E, alors la restriction $f|_A$ est simplement la composition $f \circ i$.*

$$\begin{tikzcd} A \arrow[r, "i"] \arrow[rr, bend right, "f\circ i = f|_A"'] & E \arrow[r, "f"] & F \end{tikzcd}$$

3.4.3 Définition (Prolongement)**.** Soient E et F des ensembles, $A \in \mathscr{P}(E)$ une partie de E et $f : A \to F$ une fonction. On dit qu'une application $g : E \to F$ est un *prolongement* de f si $g|_A = f$.

3.4.4 Mise en garde. Il existe en général plusieurs prolongements possibles d'une même fonction et même si la fonction f est donnée par une formule, un prolongement n'a aucune raison d'être défini par la même formule hors du domaine originel de f. Par exemple, si $f : \mathbb{R}_+^* \to \mathbb{R}, x \mapsto e^x$, alors les fonctions suivantes sont des prolongements de f (à divers domaines) :

$$g : \mathbb{R}^* \to \mathbb{R}, x \mapsto \begin{cases} e^x \text{ si } x > 0 \\ \sin(x) \text{ si } x < 0 \end{cases},$$

$$h : \mathbb{R}_+ \to \mathbb{R}, x \mapsto \begin{cases} e^x \text{ si } x > 0 \\ 10 \text{ si } x = 0 \end{cases}.$$

(Un prolongement ne doit pas non plus être forcément continu ni dérivable, etc.)

3.4.5 Définition (Corestriction)**.** Soit $f : E \to F$, et B une partie de F contenant toutes les images des éléments de E (autrement dit, $\forall x \in E, f(x) \in B$). La *corestriction* de f à B est l'application de domaine E, codomaine B et de même graphe que f, autrement dit c'est l'application

$$g : E \to B, x \mapsto f(x).$$

La corestriction de f à B se note $f|^B$ mais cette notation n'est pas aussi standard que celle pour la restriction

3.4.6 Exemple. Soit $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$. On peut la corestreindre à $[-3, +\infty[$ car cette partie de $\mathbb{R}$ contient toutes les images de f. La corestriction de f à $[-3, +\infty[$ est $g : \mathbb{R} \to [-3, +\infty[, x \mapsto x^2$.

3.4.7 Exercice. Dans le contexte de la définition, soit $i : B \to F$ l'inclusion de B dans F, et soit $r : F \to B$ une fonction définie comme suit : pour $y \in F$, on définit $r(y) = y$ si $y \in B$, et sinon, $r(y)$ est un élément arbitraire de B.

1. Vérifier que r est une rétraction de i.
2. Vérifier que la corestriction $f|^B$ est égale à la composée $r \circ f$.

3.5 Fonctions injectives et surjectives

Résumé : fonctions injectives, surjectives, bijectives, stabilité par composition, réciproques partielles, injectivité ssi rétractions, surjectivité ssi sections, bijectivité ssi réciproque

3.5.1 Définition (Fonction injective)**.** Soit $f : A \to B$ une application. On dit que f est *injective* (ou que c'est une *injection*) si les conditions équivalentes suivantes sont vérifiées.

1. $\forall (x, y) \in A^2, \quad f(x) = f(y) \Rightarrow x = y$.
2. $\forall (x, y) \in A^2, \quad x \neq y \Rightarrow f(x) \neq f(y)$. (La contraposée de la précédente.)
3. Deux éléments distincts de A ont des images distinctes.
4. Un élément de B admet au plus un antécédent par f.

Une formulation moins précise mais parlante est qu'une fonction injective « sépare les points ».

3.5.2 Exemple. $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$ n'est **pas** injective puisque $f(1) = f(-1)$.

3.5.3 Exercice. Montrer que $\sin : \mathbb{R} \to \mathbb{R}, x \mapsto \sin(x)$ n'est pas injective.

3.5.4 Définition (Fonction surjective)**.** Soit $f : A \to B$ une application. On dit que f est *surjective* (ou que c'est une *surjection*) si

$$\forall b \in B, \quad \exists a \in A / f(a) = b,$$

autrement dit tout élément $b \in B$ a (au moins) un antécédent par f. Une formulation moins précise mais parlante est qu'une fonction surjective « recouvre son codomaine ».

3.5.5 Exemple. $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$ n'est **pas** surjective puisque -1 n'a pas d'antécédent par f.

3.5.6 Exercice. Montrer que $\exp : \mathbb{R} \to \mathbb{R}, x \mapsto e^x$ n'est pas surjective.

3.5.7 Définition (Fonction bijective)**.** On dit que $f : A \to B$ est *bijective* (ou que c'est une *bijection*) si elle est injective et surjective. Autrement dit, f est bijective si tout élément $y \in B$ admet *exactement* un antécédent par f.

3.5.8 Exemple.

1. La fonction identité (d'un ensemble E dans lui-même) est bijective.
2. Si $A \subseteq B$, la fonction $i : A \to B, x \mapsto x$, appelée *l'inclusion de A dans B*, est injective. De même que les fonctions identité, les fonctions d'inclusion jouent souvent un rôle important malgré leur apparence anodine.
3. Si $f : E \to F$ est injective, sa restriction $f|_A$ à toute partie $A \subseteq E$ est injective.
4. On a déjà vu que $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$ n'est ni injective, ni surjective. La corestriction de f à $\mathbb{R}_+$ est $g : \mathbb{R} \to \mathbb{R}_+, x \mapsto x^2$. Elle n'est pas injective pour les mêmes raisons que f, mais elle est surjective : le codomaine est cette fois $\mathbb{R}_+$, et tout nombre réel positif $y \geq 0$ a au moins un antécédent, par exemple $-\sqrt{y}$.
5. La restriction de g à $\mathbb{R}_+$ est $h : \mathbb{R}_+ \to \mathbb{R}_+, x \mapsto x^2$. Elle est injective et surjective, donc bijective. Elle est injective car si x et y sont des réels positifs ayant même carré, ils sont forcément égaux (ils sont positifs donc il n'y a pas l'ambiguité de signe). Sa surjectivité ne découle pas directement de celle de g car le domaine a été restreint : elle est surjective car tout nombre réel positif $y \geq 0$ a au moins un antécédent *dans* $\mathbb{R}_+$, à savoir $\sqrt{y}$.
6. (Zérologie) L'unique fonction de $\varnothing$ dans $\varnothing$ est bijective. La fonction vide de $\varnothing$ dans n'importe quel ensemble est toujours injective.

3.5.9 Remarque. *En général, la surjectivité est plus difficile à montrer que l'injectivité, car il faut résoudre une équation à paramètre : l'équation $f(x) = y$, de paramètre y, et d'inconnue x, et ce pour tous les paramètres y. La non surjectivité est en revanche souvent plus facile à montrer, il suffit de trouver un élément qui n'a pas d'antécédent, en général cela se voit (éventuellement après un petit calcul / majoration / développement d'expression).*

3.5.10 Remarque. *Si $f : A \to B$ est injective, alors on peut parfois « identifier » A à un sous-ensemble de B grâce à f : un élément $a \in A$ est identifié à $f(a) \in B$. **Attention**, cette façon d'identifier A à une partie de B dépend de f et il existe en général plusieurs injections de A dans B, donc le choix de l'injection n'est pas anodin, ni canonique en général.*

3.5.11 Proposition (Stabilité à la composition de l'injectivité et de la surjectivité)**.** Soient $f : E \to F$ et $g : F \to G$ deux fonctions.

1. Si f et g sont injectives, alors $g \circ f$ l'est également.
2. Si f et g sont surjectives, alors $g \circ f$ l'est également.
3. Si f et g sont bijectives, alors $g \circ f$ l'est également.

Démonstration.

1. Soient $x, y \in E$ tels que $(g \circ f)(x) = (g \circ f)(y)$, c'est-à-dire tels que $g(f(x)) = g(f(y))$. Comme g est injective, on a $f(x) = f(y)$. Comme f est injective, on a alors $x = y$, ce qu'il fallait démontrer.
2. Soit $z \in G$. Comme g est surjective, z possède un antécédent par g c'est-à-dire qu'il existe $y \in F$ tel que $g(y) = z$. Ensuite, comme f est surjective, y possède un antécédent par f, c'est-à-dire qu'il existe $x \in E$ tel que $f(x) = y$. On a alors $g(f(x)) = g(y) = z$, donc x est un antécédent de z par $g \circ f$. Ceci montre que tout élément de G possède un antécédent par $g \circ f$, donc que $g \circ f$ est surjective.
3. Il suffit d'appliquer les deux premiers points.

□

3.5.12 Proposition (réciproques partielles)**.** Soient $f : E \to F$ et $g : F \to G$ deux fonctions.

1. Si $g \circ f$ est injective, alors f l'est également.
2. Si $g \circ f$ est surjective, alors g l'est également.

Démonstration.

1. Soient $x, y \in E$ tels que $f(x) = f(y)$. En appliquant g, il vient $g(f(x)) = g(f(y))$. Comme $g \circ f$ est injective, $x = y$.
2. Soit $z \in G$. Comme $g \circ f$ est surjective, il existe $x \in E$ tel que $g(f(x)) = z$. Posons $y = f(x)$. On a $g(y) = z$ donc y est un antécédent de z par g.

□

3.5.13 Corollaire (de la proposition)**.** Soit $f : E \to F$ une application.

1. Si elle admet une rétraction (inverse à gauche), alors elle est injective.
2. Si elle admet une section (inverse à droite), alors elle est surjective.
3. Si elle admet une fonction réciproque, alors elle est bijective.

Démonstration.

1. Soit r une rétraction de f. La composée $r \circ f = \mathrm{Id}_E$ est injective donc par la proposition précédente, f est injective.

2. Soit s une section de f. La composée $f \circ s = \mathrm{Id}_F$ est surjective donc par la proposition précédente, f est surjective.
3. Une réciproque étant à la fois une section et une rétraction, on applique les deux points précédents.

□

3.5.14 Remarque. ***Attention****, on peut avoir $g \circ f$ injective et g non injective, et on peut aussi avoir $g \circ f$ surjective et f non surjective. Considérons par exemple :*

$$f : \mathbb{N} \to \mathbb{N}, n \mapsto 2n \quad \textit{et} \quad g : \mathbb{N} \to \mathbb{N}, n \mapsto \lfloor n/2 \rfloor.$$

Alors $g \circ f = \mathrm{Id}_{\mathbb{N}}$ donc est bijective, mais f n'est pas surjective et g n'est pas injective.

On peut également considérer les fonctions

$$f : \mathbb{R}_+ \to \mathbb{R}, x \mapsto \sqrt{x} \quad \textit{et} \quad g : \mathbb{R} \to \mathbb{R}_+, x \mapsto x^2$$

qui vérifient également $g \circ f = \mathrm{Id}_{\mathbb{R}_+}$ sans que f soit surjective ni g injective.

On termine la section par la réciproque du corollaire précédent, qui établit entre autres l'équivalence entre bijectivité et existence d'une réciproque.

3.5.15 Proposition. Soit $f : E \to F$.

1. Elle est surjective ssi elle admet une section.
2. Elle est injective ssi elle admet une rétraction.
3. Elle est bijective ssi elle admet une réciproque.

Démonstration. Le sens « si » a été démontré dans le corollaire 3.5.13. Montrons le sens « seulement si ».

1. Pour tout $y \in F$, on choisit un antécédent de y par f, que l'on note x_y. On définit alors une fonction $g : F \to E$ par $g(y) = x_y$. Par construction, on a $f \circ g = \mathrm{Id}_F$ donc g est une section de f.
2. À tout $y \in F$ on associe soit son unique antécédent s'il en existe un, soit un élément de E arbitraire dans le cas contraire. Ceci définit une fonction $g : F \to E$ et par construction on a $g \circ f = \mathrm{Id}_E$.
3. D'une part, comme f est surjective, elle admet (d'après le premier point) une section s, qui vérifie donc $f \circ s = \mathrm{Id}_F$. Montrons que $s \circ f = \mathrm{Id}_E$. Soit $x \in E$ et soit $a = (s \circ f)(x)$. Alors $f(a) = (f \circ s \circ f)(x) = ((f \circ s) \circ f)(x) = f(x)$ et comme f est injective, $a = x$ c'est-à-dire $(s \circ f)(x) = x$. Donc $s \circ f = \mathrm{Id}_E$ et donc s est la réciproque de f.
4. *Preuve alternative du dernier point, en suivant le cheminement inverse.* D'une part, comme f est injective, elle admet (d'après le second point) une rétraction r, qui vérifie donc $r \circ f = \mathrm{Id}_E$. Montrons que $f \circ r = \mathrm{Id}_F$. Soit $y \in F$. Comme f est surjective, considérons x un antécédent de y. Alors, $(f \circ r)(y) = (f \circ r)(f(x)) = (f \circ (r \circ f))(x) = (f \circ \mathrm{Id}_E)(x) = f(x) = y$. D'où $f \circ r = \mathrm{Id}_F$ et donc r est la réciproque de f.

□

3.6 Images directes et réciproques de parties

Résumé : images directes et réciproques de parties, fibres d'une application, union et intersections d'images directes et réciproques.

3.6.1 Définition (Image directe d'une partie)**.** Soit $f : E \to F$ et $A \subseteq E$. On appelle image directe de A l'ensemble des images des éléments de A :

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

Autrement dit, pour un élément $y \in F$, on a $y \in f(A) \iff \big(\exists x \in A, y = f(x)\big)$.

3.6.2 Définition (Image réciproque d'une partie)**.** Soit $f : E \to F$ et $B \subseteq F$. On appelle image réciproque de B l'ensemble de tous les antécédents d'éléments de B :

$$f^{<-1>}(B) = \{x \in E \mid f(x) \in B\}.$$

Autrement dit, pour un élément $x \in E$, on a $x \in f^{<-1>}(B) \iff f(x) \in B$.

Attention, on voit très souvent la notation $f^{-1}(B)$ au lieu de $f^{<-1>}(B)$ mais cela peut prêter à confusion, la fonction f n'ayant pas forcément de réciproque. Dans ce chapitre, on utilise pour commencer la notation $f^{<-1>}(B)$. La notation $f^{-1}(B)$ sera adoptée progressivement dans les chapitres suivants.

3.6.3 Définition (Fibres d'une application)**.** Soit $f : A \to B$ et $b \in B$. La *fibre de f (au-dessus) de b* est l'ensemble des antécédents de b, c'est-à-dire $f^{<-1>}(\{b\}) = \{a \in A \mid f(a) = b\}$. De façon générale, les *fibres* de l'application f sont les images réciproques de singletons de B.

3.6.4 Proposition. Soit $f : E \to F$.

1. $f(\varnothing) = \varnothing$.
2. $f(E) \subseteq F$ avec égalité si et seulement si f est surjective. En général, $f(E) \neq F$.
3. Si $(A_i)_{i\in I}$ est une famille de parties de E, alors $f\left(\bigcup_{i\in I} A_i\right) = \bigcup_{i\in I} f(A_i)$.
4. Par contre, on a en général $f\left(\bigcap_{i\in I} A_i\right) \subseteq \bigcap_{i\in I} f(A_i)$ mais pas forcément égalité.

Démonstration.

1. Clair.
2. On a $f(E) = F \iff (\forall y \in F, y \in f(E))$ ce qui signifie par définition que tout élément $y \in F$ admet au moins un antécédent, et donc que f est surjective.
3. Soit $y \in F$. On a

$$\begin{aligned}
y \in f\left(\bigcup_{i\in I} A_i\right) &\iff \exists x \in \bigcup_{i\in I} A_i, y = f(x) \\
&\iff \exists x \in E, \left(x \in \bigcup_{i\in I} A_i \text{ et } y = f(x)\right) \\
&\iff \exists x \in E, \exists i \in I, (x \in A_i \text{ et } y = f(x)) \\
&\boxed{\iff \exists i \in I, \exists x \in E}, (x \in A_i \text{ et } y = f(x)) \\
&\iff \exists i \in I, \exists x \in A_i, y = f(x) \\
&\iff \exists i \in I, y \in f(A_i) \\
&\iff y \in \bigcup_{i\in I} f(A_i)
\end{aligned}$$

L'interversion de quantificateur signalée est licite car ce sont deux quantificateurs existentiels.

4. On a :

$$\begin{aligned} y\in f\left(\bigcap_{i\in I}A_i\right) &\iff \exists x\in\bigcap_{i\in I}A_i, y=f(x)\\ &\iff \exists x\in E, \left(x\in\bigcap_{i\in I}A_i \text{ et } y=f(x)\right)\\ &\iff \exists x\in E, \forall i\in I, (x\in A_i \text{ et } y=f(x))\\ &\boxed{\implies \forall i\in I, \exists x\in E}, (x\in A_i \text{ et } y=f(x)) \quad (*)\\ &\implies \forall i\in I, \exists x\in A_i, y=f(x)\\ &\implies \forall i\in I, y\in f(A_i)\\ &\implies y\in\bigcap_{i\in I}f(A_i)\end{aligned}$$

L'interversion des quantificateurs est licite **dans ce sens-là seulement :** $\exists x\forall i\ldots \implies \forall i\exists x\ldots$, et l'équivalence devient une implication. Ceci prouve l'inclusion. Pour montrer qu'il n'y a pas forcément égalité, il suffit de donner un contre-exemple, par exemple $\sin(\mathbb{R}_-^*\cap\mathbb{R}_+^*) = \sin(\varnothing)=\varnothing\subsetneq\sin(\mathbb{R}_+^*)\cap\sin(\mathbb{R}_-^*)=[-1,1]$.

□

3.6.5 Proposition. Soit $f:E\to F$.

1. $f^{<-1>}(\varnothing)=\varnothing$.
2. $f^{<-1>}(F)=E$.
3. Si $(B_i)_{i\in I}$ est une famille de parties de F, alors $f^{<-1>}\left(\bigcup_{i\in I}B_i\right)=\bigcup_{i\in I}f^{<-1>}(B_i)$, ainsi que $f^{<-1>}\left(\bigcap_{i\in I}B_i\right)=\bigcap_{i\in I}f^{<-1>}(B_i)$.

Démonstration. Exercice. □

En conclusion, l'image réciproque se comporte un peu mieux que l'image directe.

3.6.6 Définition (Saturation, partie saturée)**.** Soit $f:E\to F$ une fonction et $A\in\mathscr{P}(E)$ une partie de la source de f. La *saturation* de A (relativement à la fonction f) est la partie $f^{<-1>}(f(A))$.

On dit que A est *saturée* (relativement à la fonction f) si elle est égale à sa saturation.

3.6.7 Exemple.

1. La saturation $\mathrm{Sat}_f(A)$ d'une partie A contient toujours A.
2. La saturation d'une partie A est saturée, autrement dit avec la notation plus haut on a $\mathrm{Sat}_f(\mathrm{Sat}_f(A))=\mathrm{Sat}_f(A)$.
3. Soit $f:\mathbb{R}\to\mathbb{R}_+, x\mapsto x^2$, et soit $A=\{2\}\subseteq\mathbb{R}$. La saturation de A est

$$f^{<-1>}(f(A))=f^{<-1>}(\{4\})=\{x\in\mathbb{R}\mid x^2=4\}=\{-2,2\}$$

La saturation de A contient donc strictement A, qui n'est donc pas saturée. Par contre, les parties $B=\{0\}$ et $C=\{-2,2\}$ sont saturées (relativement à f, toujours).

3.7 Compléments : principes de factorisation et exercices

Les définitions et résultats de cette section ne sont pas exigibles comme cours à l'examen mais sont néanmoins importants.

3.7.1 Proposition (Principe de factorisation à droite)**.** Soient $f : A \to B$ et $g : A \to C$. Rappelons que les trois assertions suivantes sont équivalentes :

1. g se factorise à droite par f ;
2. il existe une application $h : B \to C$ telle que $g = h \circ f$;
3. il existe une application $h : B \to C$ faisant commuter le diagramme $\begin{tikzcd} A \arrow[r, "g"] \arrow[d, "f"'] & C \\ B \arrow[ur, dashed, "\exists h"'] & \end{tikzcd}$.

Ces assertions sont vraies si et seulement si :

$$\forall x, y \in A, f(x) = f(y) \implies g(x) = g(y).$$

Démonstration. **Sens « seulement si ».** Supposons que g se factorise en $g = h \circ f$. Soient $x, y \in E$ tels que $f(x) = f(y)$. En composant à gauche par h, on obtient $h(f(x)) = h(f(y))$, c'est-à-dire $g(x) = g(y)$.
Sens « si ». Supposons que $\forall x, y \in A, f(x) = f(y) \implies g(x) = g(y)$. Construisons une fonction h vérifiant les conditions demandées. Soit $b \in B$. S'il existe $a \in A$ tel que $f(a) = b$, on définit $h(b)$ comme étant égal à $g(a)$. Sinon, on définit $h(b)$ comme étant un élément quelconque de C. En définissant ainsi un élément $h(b) \in C$ pour tout élément $b \in B$, on définit donc une fonction $h : B \to C$ et par construction, on a $g = h \circ f$. □

3.7.2 Remarque. *Si $A = C$ et $g = \mathrm{Id}_A$, cette proposition devient l'équivalence entre injectivité et existence d'une rétraction h (inverse à gauche).*

Cette proposition peut paraître abstraite mais en pratique elle est très facile à utiliser, comme le montre l'exemple suivant.

3.7.3 Exemple. Montrer que $g : \mathbb{R} \to \mathbb{R}, x \mapsto |x|$ se factorise à droite par $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$.

> *Exemple de rédaction:*
> Soient $x, y \in \mathbb{R}$. Supposons $f(x) = f(y)$ c'est-à-dire $x^2 = y^2$. Alors, $x = y$ ou $x = -y$, et donc on en déduit que $|x| = |y|$ c'est-à-dire $g(x) = g(y)$. D'après la proposition 3.7.1, il existe $h : \mathbb{R} \to \mathbb{R}$ telle que $g = h \circ f$, ou encore : $\forall x \in \mathbb{R}, |x| = h(x^2)$.

(Attention, dans l'exemple précédent h n'est pas exactement la racine carrée : en effet h doit être définie sur $\mathbb{R}$. D'ailleurs h n'est pas unique.)

3.7.4 Exercice. Dans le contexte de la proposition 3.7.1, montrer que si f est surjective, alors l'application h qui factorise g est forcément unique.

3.7.5 Proposition (Principe de factorisation à gauche)**.** Soient $f : A \to C$ et $g : B \to C$. Rappelons que les trois assertions suivantes sont équivalentes :

1. f se factorise à gauche par g ;
2. il existe une application $h : A \to B$ telle que $f = g \circ h$;
3. il existe une application $h : A \to B$ faisant commuter le diagramme $\begin{tikzcd} & B \arrow[d, "g"] \\ A \arrow[ur, dashed, "\exists h"] \arrow[r, "f"'] & C \end{tikzcd}$.

Ces assertions sont vraies si et seulement si $f(A) \subseteq g(B)$.

Démonstration. **Sens « seulement si ».** Supposons $f = g \circ h$, et soit $a \in A$. Alors $f(a) = g(h(a))$, donc $f(a) \in g(B)$. Ceci prouve que $f(A) \subseteq g(B)$.
Sens « si ». Supposons $f(A) \subseteq g(B)$. Construisons une application h vérifiant les conditions demandées. Soit $a \in A$. Comme $f(a) \in f(A) \subseteq g(B)$, $f(a) \in g(B)$ et donc $f(a)$ possède un antécédent par g. On définit $h(a)$ comme étant un tel antécédent. Par construction, on a $g \circ h = f$. □

3.7.6 Remarque. *Si $A = C$ et que $f = \mathrm{Id}_C$, on retombe sur l'équivalence entre surjectivité et existence d'une section (inverse à droite).*

Les deux exercices suivants montrent que l'ensemble des surjections et l'ensemble des injections forment ce qui est parfois appelé un *système orthogonal de factorisation*, une notion que l'on recroise dans plusieurs contextes en mathématiques.

3.7.7 Exercice (Factorisation en surjection puis injection)**.** Montrer que toute application se factorise en une surjection suivie d'une injection. Autrement dit, montrer que pour toute fonction $f : E \to F$, il existe un ensemble G, et des fonctions $\phi : E \to G$ et $\psi : G \to F$ telles que $f = \psi \circ \phi$, avec ϕ surjective et ψ injective.

3.7.8 Exercice (Propriété du relèvement)**.** Soient $e : A \to B$ et $m : C \to D$ deux applications. On dit que e est orthogonale (à gauche) à m (ou que m est orthogonale à droite à e), et on note $e \perp m$, si pour tout diagramme commutatif

$$\begin{tikzcd} A \arrow[r] \arrow[d, "e"'] & C \arrow[d, "m"] \\ B \arrow[r] & D \end{tikzcd},$$

il existe un relèvement c'est-à-dire une application $r : B \to C$ faisant commuter le diagramme :

$$\begin{tikzcd} A \arrow[r] \arrow[d, "e"'] & C \arrow[d, "m"] \\ B \arrow[r] \arrow[ur, "r"] & D \end{tikzcd}$$

Montrer que si e est surjective et m est injective, alors $e \perp m$.

Les deux exercices qui suivent donnent un éclairage alternatif sur le produit cartésien et sa contrepartie, l' « union disjointe ».

3.7.9 Exercice (Propriété universelle du produit)**.** Soient A et B des ensembles, et $A \times B$ leur produit (cartésien). On note $\mathrm{pr}_A : A \times B \to A, (a, b) \mapsto a$ et $\mathrm{pr}_B : A \times B \to B, (a, b) \mapsto b$. Ces deux applications sont appelées les *projections canoniques sur les facteurs du produit.*

Montrer que l'ensemble $A \times B$ ainsi que les deux projections vérifient la propriété suivante : pour tout ensemble D muni d'applications f et g vers (respectivement) A et B, il existe une unique application $h : D \to A \times B$ telle que $f = \mathrm{pr}_A \circ h$ et $g = \mathrm{pr}_B \circ h$, c'est-à-dire qu'il existe une unique application $h : D \to A \times B$ faisant commuter le diagramme suivant :

$$\begin{tikzcd} & & A \\ D \arrow[urr, "f"] \arrow[drr, "g"'] \arrow[r, dashed, "\exists! h"] & A \times B \arrow[ur, "pr_A"'] \arrow[dr, "pr_B"] & \\ & & B \end{tikzcd}$$

3.7.10 Exercice (Union disjointe/coproduit/somme cartésienne)**.** Soient A et B deux ensembles. On appelle *union disjointe de A et B* l'ensemble

$$A \biguplus B = (\{0\} \times A) \bigcup (\{1\} \times B)$$

Cet ensemble est muni de deux applications $i_A : A \to A \biguplus B, a \mapsto (0, a)$ et $i_B : B \to A \biguplus B, b \mapsto (1, b)$.

Montrer que $A \biguplus B$ ainsi que i_A et i_B vérifient la propriété suivante : pour tout ensemble C muni d'applications $f : A \to C$ et $g : B \to C$, il existe une unique application $h : A \biguplus B \to C$ telle que $f = h \circ i_A$ et $g = h \circ i_B$, autrement dit il existe une unique application h faisant commuter le diagramme suivant :

$$\begin{tikzcd}
A \arrow[dr, "i_A"'] \arrow[drr, "f"] & & \\
& A \biguplus B \arrow[r, dashed, "\exists ! h"] & C \\
B \arrow[ur, "i_B"] \arrow[urr, "g"'] & &
\end{tikzcd}$$

Chapitre 4

Entiers, ensembles finis et combinatoire

Sommaire

Retour à la table des matières principale

4.1 L'ensemble $\mathbb{N}$ et la récurrence

L'ensemble $\mathbb{N}$ est supposé connu. Il vérifie les propriétés suivantes (les ensembles ordonnés sont traités dans un chapitre ultérieur mais le vocabulaire devrait être connu) :

1. tout partie non vide majorée admet un plus grand élément ;
2. toute partie non vide admet un plus petit élément.

C'est la deuxième propriété qui permet de distinguer $\mathbb{N}$ de $\mathbb{Z}$ et qui fonde le principe de récurrence.

4.1.1 Définition (Propriété héréditaire)**.** Soit $A(n)$ une assertion dépendant d'un paramètre $n \in \mathbb{N}$. On dit qu'elle est *héréditaire* si :

$$\forall n \in \mathbb{N},\ A(n) \implies A(n+1).$$

(On définit de manière similaire l'hérédité à partir d'un certain rang n_0, au lieu du rang 0.)

4.1.2 Théorème (Principe de récurrence)**.** Soit $A(n)$ une propriété dépendant d'un paramètre $n \in \mathbb{N}$.

Si $A(0)$ est vraie et que la propriété est héréditaire, alors la propriété est vraie pour tout $n \in \mathbb{N}$, autrement dit :

$$\big(A(0) \text{ et } (\forall n \in \mathbb{N},\ A(n) \implies A(n+1))\big) \implies (\forall n \in \mathbb{N},\ A(n)).$$

Démonstration. Supposons la propriété vraie au rang 0 et héréditaire.

Montrons que la partie $A = \{n \in \mathbb{N} \mid A(n) \text{ est fausse}\} \subseteq \mathbb{N}$ est vide.

Si A est non-vide, elle possède un plus petit élément m avec $m \geq 1$ puisque $A(0)$ est vraie. Donc $m-1 \in \mathbb{N}$ et $A(m-1)$ est vraie par définition de m. Par hérédité, $A(m) = A((m-1)+1)$ est vraie, contradiction. Donc $A = \varnothing$ ce qui signifie exactement : $\forall \in \mathbb{N},\ A(n)$. □

4.1.3 Théorème (Récurrence forte)**.** Soit $A(n)$ une propriété dépendant d'un paramètre $n \in \mathbb{N}$.

Si $A(0)$ est vraie et que $\forall n \in \mathbb{N}, (\forall k \leq n, A(k)) \implies A(n+1)$, alors $A(n)$ est vraie pour tout $n \in N$.

Démonstration. Exercice. Appliquer le principe de récurrence simple à la propriété $B(n)$: « $\big(\forall k \leq n,\ A(k)\big)$ ». □

4.2 Ensembles finis

4.2.1 Ensembles $[\![a, b]\!]$

Si $a, b \in \mathbb{Z}$, on note $[\![a, b]\!]$ l'ensemble $\{n \in \mathbb{Z} \mid a \leq n \leq b\}$. Si $b < a$, cet ensemble est vide.

4.2.1 Lemme. Soient $m \geq 1$ et $a \in [\![1, m]\!]$. L'application

$$\phi : [\![1, m]\!] \setminus \{a\} \to [\![1, m-1]\!], x \mapsto \begin{cases} x & \text{si } x < a \\ x-1 & \text{si } x > a \end{cases}$$

est une bijection

Démonstration. Exercice. Remarquer que si $m = 1$, on obtient juste une bijection entre l'ensemble vide et lui-même. □

Les deux lemmes suivants établissent des résultats qui semblent « évident » mais qui doivent être démontrés rigoureusement afin d'asseoir la définition de cardinal sur des bases solides.

4.2.2 Lemme. Soient $m, n \in \mathbb{N}$. S'il existe une injection de $[\![1, m]\!]$ dans $[\![1, n]\!]$, alors $m \leq n$.

Démonstration. Pour m entier, notons $A(m)$ l'assertion

$$\forall n \in \mathbb{N}, \quad (\text{il existe une injection } [\![1, m]\!] \to [\![1, n]\!]) \implies m \leq n.$$

Montrons $\forall m, A(m)$ par récurrence, ce qui prouve la proposition.

Initialisation. $A(0)$ est vraie car pour tout n, $0 \leq n$ est vraie donc l'implication dans $A(0)$ est vraie.

Hérédité. Soit $m \in \mathbb{N}$ et supposons $A(m)$. Montrons $A(m+1)$.

Soit $n \in \mathbb{N}$ et soit $f : [\![1, m+1]\!] \to [\![1, n]\!]$ une injection. Alors la restriction $f|_{[\![1,m]\!]} : [\![1, m]\!] \to [\![1, n]\!] \setminus \{f(m+1)\}$ est également injective.

En composant avec une bijection $\phi : [\![1, n]\!] \setminus \{f(m+1)\} \to [\![1, n-1]\!]$ (par exemple celle fournie par le lemme), on obtient une injection $\phi \circ f|_{[\![1,m]\!]} : [\![1, m]\!] \to [\![1, n-1]\!]$.

Par hypothèse de récurrence, on a donc $m \leq n-1$, et donc $m+1 \leq n$, donc $A(m+1)$ est vraie. □

4.2.3 Lemme. Soient $m, n \in \mathbb{N}$. S'il existe une bijection entre $[\![1, m]\!]$ et $[\![1, n]\!]$, on a $m = n$

Démonstration. Soit f une telle bijection. Comme elle est injective, on a $m \leq n$.

Considérons alors la bijection réciproque $f^{-1} : [\![1, n]\!] \to [\![1, m]\!]$. Comme elle est également injective, on a $n \leq m$. D'où $m = n$. □

4.2.2 Ensembles finis et cardinal

4.2.4 Définition. Un ensemble E est *fini* s'il existe $n \in \mathbb{N}$ et une injection de E dans $[\![1,n]\!]$. Un ensemble qui n'est pas fini est *infini.*

4.2.5 Remarque. *a) On en déduit immédiatement qu'un ensemble qui s'injecte dans un ensemble fini est lui-même fini (la composée de deux injections est une injection).*

b) À priori, l'entier n de la définition n'est pas unique, car si n convient, alors $n+1$ aussi.

c) (Zérologie) L'ensemble vide est fini : il existe une (unique) application de l'ensemble dans tout ensemble F, c'est celle dont le graphe est la partie vide de $\varnothing \times F$ (cette partie vérifie bien les conditions pour être un graphe de fonction). On l'appelle « l'application vide ». On vérifie ensuite que cette application est injective (en appliquant la définition).

4.2.6 Proposition et Définition. Soit E un ensemble fini. Alors, il existe un unique $n \in \mathbb{N}$ tel que E soit en bijection avec $[\![1,n]\!]$.

Cet entier n est appelé le *cardinal* de E. Il est noté $\mathrm{Card}(A)$, ou $|A|$ ou $\sharp A$.

Démonstration. L'unicité découle des lemmes précédents.

Pour l'existence, Soit $n \in \mathbb{N}$ et soit $f : E \to [\![1,n]\!]$ une injection. Si $f(E) = [\![1,n]\!]$, l'application est surjective donc bijective. Sinon, il existe $a \in [\![1,n]\!] \setminus f(E)$, donc en composant f avec une injection $\phi : [\![1,n]\!] \setminus \{a\} \to [\![1,n-1]\!]$, on obtient une injection $\phi \circ f : E \to [\![1,n-1]\!]$. On itère ce processus tant que l'application n'est pas bijective, ce qui finit par se produire puisque l'ensemble d'arrivée des injections diminue strictement à chaque étape. □

4.2.7 Proposition.

1. Un ensemble en bijection avec un ensemble fini de cardinal n est également fini de cardinal n.
2. L'ensemble vide est fini de cardinal zéro. Réciproquement, un ensemble fini de cardinal zéro est vide.

Démonstration.

1. Soit $f : A \to B$ une bijection. Si B est fini de cardinal n, alors il existe une bijection $\phi : B \to [\![1,n]\!]$, et donc $\phi \circ f : A \to [\![1,n]\!]$ est une bijection.
2. On a déjà vu qu'il existe une (unique) application entre $\varnothing$ et $[\![1,0]\!] = \varnothing$ et qu'elle est injective. On peut vérifier qu'elle est surjective, toujours en appliquant la définition. Réciproquement, un ensemble de cardinal zéro est par définition en bijection avec $[\![1,0]\!] = \varnothing$, donc est vide.

□

4.2.8 Proposition.

1. Si A et B sont disjoints et finis, alors $A \cup B$ est fini et $|A \cup B| = |A| + |B|$.
2. Si A est fini et $B \subseteq A$, alors B est fini et $|B| \le |A|$.
3. Si de plus $|B| = |A|$, alors $B = A$.
4. Si A et B sont finis, alors $|A \cup B| = |A| + |B| - |A \cap B|$.

Démonstration.

1. Soient n et m des entiers et $f : A \to [\![1,m]\!]$, $g : B \to [\![1,n]\!]$ des bijections. L'application

$$\phi : A \cup B \to [\![1,m+n]\!], \quad x \mapsto \begin{cases} f(x) & \text{si } x \in A \\ m + g(x) & \text{si } x \in B \end{cases}$$

est bien définie, et c'est une bijection de $A \cup B$ dans $[\![1,m+n]\!]$.

2. Si A est fini, alors B s'injecte dans un ensemble fini donc est fini. De même, la partie $A \setminus B$ de A est également finie. On peut alors écrire A comme l'union disjointe d'ensembles finis $A = B \cup (A \setminus B)$ et par ce qui précède, on a $|A| = |B| + |A \setminus B|$. On en déduit que $|B| \leq A$ et que s'il y a égalité, $A \setminus B$ est de cardinal 0, donc vide, d'où $A = B$.
3. On a l'union disjointe $A = A \cup (B \setminus A)$ donc $|A \cup B| = |A| + |B \setminus A|$. D'autre part, on a l'union disjointe $B = (B \cap A) \cup (B \setminus A)$, donc $|B| = |B \cap A| + |B \setminus A|$. En remplaçant $|B \setminus A|$ par $|B| - |B \cap A|$ dans la première égalité, on obtient le résultat.

□

4.2.3 Applications et ensembles finis

4.2.9 Proposition. Soit $f : A \to B$ une application.

1. Si B est fini, alors $|f(A)| \leq |B|$ et si de plus $|f(A)| = |B|$ alors f est surjective.
2. Si A est fini et f est injective, alors $|f(A)| = |A|$.

Démonstration.

1. On a $f(A) \subseteq B$ donc $f(A)$ est fini et $|f(A)| \leq |B|$. S'il y a égalité des cardinaux, alors on a $f(A) = B$ ce qui signifie que f est surjective.
2. Soit $g : A \to f(A)$ l'application déduite de f en remplaçant le codomaine B par $f(A)$. L'application g est surjective par construction, que A soit fini ou pas.
   Si f est injective, g l'est également. On en déduit que A et $f(A)$ sont en bijection. Si de plus A est fini, ils ont donc le même cardinal.

□

4.2.10 Proposition. Soit $f : A \to B$ une application.

1. Si B est fini et f est injective, alors A est fini et $|A| \leq |B|$.
2. Si A est fini et f est surjective, alors B est fini et $|A| \geq |B|$.

Démonstration.

1. Si B est fini, alors A s'injecte dans un ensemble fini donc est fini. De plus, on a $|A| = |f(A)| \leq |B|$.
2. Soit $g : B \to A$ une *section* de f, c'est-à-dire une application qui à $y \in B$ associe un antécédent quelconque de y. Par construction, on a $f \circ g = \mathrm{Id}_B$ donc g est injective, et par le premier point B est fini et $|B| \leq |A|$.

□

4.2.11 Théorème (IMPORTANT)**.** Soient A et B finis **de même cardinal**, et soit $f : A \to B$. Alors, on a les équivalences suivantes :

$$f \text{ est injective} \iff f \text{ est surjective} \iff f \text{ est bijective.}$$

Démonstration. Il suffit de prouver la première équivalence.

Sens $\Longrightarrow$: Si f est injective, on a $|f(A)| = |A| = |B|$, et comme $f(A) \subseteq B$, l'égalité des cardinaux force $f(A) = B$ c'est-à-dire que f est surjective.

Sens $\Longleftarrow$, par contraposée : Si f n'est pas injective, soient x et y distincts tels que $f(x) = f(y)$. Alors $f(A) = f(A \setminus \{y\})$, donc

$$|f(A)| \leq |A \setminus \{y\}| = |A| - 1 = |B| - 1,$$

donc $f(A) \neq B$ et donc f n'est pas surjective. □

Ce théorème est à retenir, il est indispensable dans tous les domaines des mathématiques. En particulier, il est crucial pour la théorie de la dimension des espaces vectoriels, au prochain semestre.

4.2.12 Corollaire. Soit $f : A \to B$ entre ensembles finis. Alors f est injective si et seulement si $|f(A)| = |A|$.

Démonstration. On a déjà prouvé le sens « seulement si ».

Si $|f(A)| = |A|$, alors la corestriction $g : A \to f(A), x \mapsto f(x)$ qui est par définition surjective, est également injective par le précédent théorème. Donc f est injective. □

4.2.4 Remarque sur les définitions équivalentes

Il existe d'autres définitions (équivalentes) d'ensemble fini et de cardinal. Par exemple, on aurait pu donner comme définition : un ensemble E est fini s'il existe $n \in \mathbb{N}$ et une surjection de $[\![1,n]\!]$ dans E.

Dans ce cas, on aurait commencé par prouver le lemme suivant : « s'il existe une surjection de $[\![1,m]\!]$ dans $[\![1,n]\!]$, alors $m \geq n$ », et l'ordre des résultats établis, ainsi que les preuves, auraient été différents.

4.2.13 Exercice. Établir tous les résultats du cours en prenant cette définition pour base, au lieu de celle avec les injections.

On peut aussi définir les ensembles finis en utilisant $\mathbb{N}$.

4.2.14 Exercice. Soit E un ensemble. Prouver que E est fini si et seulement si aucune application de $\mathbb{N}$ dans E n'est injective. Établir une formulation équivalente avec des surjections.

L'essentiel est d'avoir une définition équivalente, mais surtout une définition maniable et efficace pour prouver les résultats du cours.

4.3 Sommes et produits

4.3.1 Définition (Notation $\sum$ et $\prod$)**.** Soit E un ensemble fini, et $f : E \to \mathbb{C}$ (ou autre codomaine que $\mathbb{C}$, l'essentiel étant de pouvoir sommer et multiplier).

On note $\sum_{x\in E} f(x)$ le nombre 0 auquel on ajoute la somme des valeurs prises par $f(x)$ lorsque x parcourt E.

On note $\prod_{x\in E} f(x)$ le nombre 1 que l'on multiplie par le produit des valeurs prises par $f(x)$ lorsque x parcourt E.

4.3.2 Remarque (« Un produit vide vaut 1, une somme vide vaut 0 »)**.** *Faire intervenir* 0 *et* 1 *sert à avoir les propriétés :* $\sum_{x\in\varnothing}(\dots) = 0$ *et* $\prod_{x\in\varnothing}(\dots) = 1$.

4.3.3 Remarque. *Dans la définition, si* $E = A\cup B$ *et* $A\cap B = \varnothing$, *alors* $\sum_{x\in E} f(x) = \sum_{x\in A} f(x) + \sum_{x\in B} f(x)$.

Si I est un ensemble fini et $(u_i)_{i\in I}$ est une famille de complexes, on note $\sum_{i\in I} u_i$ la somme de (zéro plus) tous ces complexes.

4.3.4 Définition. La notation $\sum_{i=0}^{n} u_i$ signifie par définition $\sum_{i\in[\![0,n]\!]} u_i$, et plus généralement, $\sum_{i=a}^{b} u_i$ signifie par définition $\sum_{i\in[\![a,b]\!]} u_i$.

4.3.5 Proposition (Linéarité de la somme)**.** Soit A un ensemble fini, f, g deux fonctions de A dans $\mathbb{C}$ et λ, μ deux complexes. Alors :

$$\sum_{x\in A}(\lambda f(x)+\mu g(x)) = \lambda\sum_{x\in A} f(x)+\mu\sum_{x\in A} g(x).$$

4.3.6 Exemple. Soit $n\in N$. On peut écrire

$$\sum_{k=0}^{n}(2k+3) = 2\sum_{k=0}^{n} k+3\sum_{k=0}^{n} 1 = 2\frac{n(n+1)}{2}+3(n+1) = (n+1)(n+3).$$

4.3.7 Théorème (Théorème de Fubini pour les sommes finies)**.** Soient A et B des ensembles finis et $f : A\times B \to \mathbb{C}$. On a les égalités :

$$\sum_{x\in A}\left(\sum_{y\in B} f(x,y)\right) = \sum_{(x,y)\in A\times B} f(x,y) = \sum_{y\in B}\left(\sum_{x\in A} f(x,y)\right)$$

Démonstration. Par récurrence sur $|B|$.
Initialisation. Si $|B|=0$, alors B est vide, et les sommes indexées par B sont nulles. D'autre part, $A\times B=\varnothing$, donc au final les trois sommes sont nulles.
Hérédité. Soit $n\in\mathbb{N}$, et supposons que pour toute partie B de cardinal n et tout ensemble fini A, les égalités soient vraies. Soit B un ensemble de cardinal $n+1$. Écrivons $B=B'\cup\{b\}$, avec $b\notin B'$, et B' de cardinal n. On a alors une union disjointe $A\times B = A\times B'\cup A\times\{b\}$ et donc

$$\sum_{(x,y)\in A\times B} f(x,y) = \sum_{(x,y)\in A\times B'} f(x,y)+\sum_{(x,y)\in A\times\{b\}} f(x,y) = \sum_{(x,y)\in A\times B'} f(x,y)+\sum_{x\in A} f(x,b).$$

D'autre part, on a

$$\begin{aligned}\sum_{x\in A}\left(\sum_{y\in B} f(x,y)\right) &= \sum_{x\in A}\left(\sum_{y\in B'} f(x,y)+\sum_{y=b} f(x,y)\right)\\ &= \sum_{x\in A}\sum_{y\in B'} f(x,y)+\sum_{x\in A} f(x,b)\\ &= \sum_{(x,y)\in A\times B'} f(x,y)+\sum_{x\in A} f(x,b) \text{ par hypothèse de récurrence}\\ &= \sum_{(x,y)\in A\times B} f(x,y) \text{ par la rémarque précédente.}\end{aligned}$$

La deuxième égalité se prouve de la même façon en échangeant les rôles de A et B. □

4.3.8 Définition (Factorielle)**.** Soit $n\in\mathbb{N}$. La factorielle de n, notée $n!$, est le produit de tous les entiers strictement positifs et inférieurs à n. Autrement dit, $n! = \prod_{k\in[\![1,n]\!]} k$. En particulier, si $n=0$, le produit est vide et donc $0!=1$ par définition d'un produit vide.

4.4 Combinatoire

4.4.1 Principes élémentaires de combinatoire

4.4.1 Proposition. Soient E et F finis de cardinal n et p. Alors $E\times F$ est de cardinal np.

Démonstration. L'application

$$\phi : [\![1,n]\!] \times [\![1,p]\!] \to [\![1,np]\!], \quad (x,y) \mapsto (x-1)p + y$$

est bijective. □

4.4.2 Corollaire. Soit E un ensemble fini. Alors pour tout $k \in \mathbb{N}^*$, $|E^k| = |E|^k$.

Démonstration. Par récurrence sur k. **Initialisation.** Lorsque $k = 1$, on a bien $|E^1| = |E| = |E|^1$.
Hérédité. Soit $k \in \mathbb{N}^*$ et supposons que $|E^k| = |E|^k$. On a $|E^{k+1}| = |E^k \times E| = |E^k| \cdot |E|$ par la proposition précédente, et d'autre part par hypothèse de récurrence, on a $|E^k| = |E|^k$. Finalement, $|E^{k+1}| = |E|^{k+1}$. □

4.4.3 Corollaire. Soient $E \neq \varnothing$ et F des ensembles finis de cardinal n et p. L'ensemble $\mathscr{F}(E,F)$ des fonctions de E dans F est de cardinal p^n.

Démonstration. L'ensemble $\mathscr{F}(E,F)$ est en bijection avec F^n. (Une fonction correspond au choix d'un élément de F pour chacun des n éléments de E.) □

4.4.4 Remarque.

1. *Si E est vide, il existe une unique application de E dans n'importe quel ensemble, fût-il vide : l'application vide. Donc $|\mathscr{F}(E,F)| = 1$, ce qui permet d'étendre la formule lorsque E est vide. Lorsque E et F sont tous deux vides, on pose $0^0 = 1$ (ou plutôt on démontre, si on a la « bonne » définition de a^b) et la formule reste valable.*
2. *L'ensemble $\mathscr{F}(E,F)$ est également noté F^E. Avec cette notation, on a la formule $\left|F^E\right| = |F|^{|E|}$.*

4.4.5 Proposition. Soient $n, p \in \mathbb{N}$ avec $p \leq n$.

1. Il y a $n(n-1)(n-2)\ldots(n-p+1) = \dfrac{n!}{(n-p)!}$ injections de $[\![1,p]\!]$ dans $[\![1,n]\!]$.
2. En particulier, il y a $n!$ bijections de $[\![1,n]\!]$ dans lui-même.

Une bijection de $[\![1,n]\!]$ dans lui-même s'appelle une *permutation* $[\![1,n]\!]$.

4.4.6 Proposition. Soit E un ensemble fini. L'ensemble $\mathscr{P}(E)$ des parties de E est fini, de cardinal $2^{|E|}$.

Démonstration. Il y a une bijection entre $\mathscr{P}(E)$ et $\mathscr{F}(E,\{0,1\})$, donnée par $A \mapsto \mathbf{1}_A$, l'application qui à une partie A associe sa fonction caractéristique. Or, on a $|\mathscr{F}(E,\{0,1\})| = |\{0,1\}|^{|E|} = 2^{|E|}$. □

4.4.2 Coefficients binomiaux

4.4.7 Définition. Soit $n \in \mathbb{N}$, et $k \in \mathbb{Z}$.
On note $\mathscr{P}_k([\![1,n]\!])$ ou même $\mathscr{P}_k(n)$ l'ensemble des parties de $[\![1,n]\!]$ qui sont de cardinal k.
On note $\dbinom{n}{k}$ le nombre de parties de $[\![1,n]\!]$ de cardinal k, c'est-à-dire $\dbinom{n}{k} = |\mathscr{P}_k(n)|$.

Remarque : si $k < 0$ ou si $k > n$, $\dbinom{n}{k} = 0$ car il n'y a aucune partie de $[\![1,n]\!]$ de cardinal k.

4.4.8 Proposition. On a $\dbinom{n}{k} = \dbinom{n}{n-k}$.

Démonstration. L'application $\phi : \mathscr{P}_k(n) \to \mathscr{P}_{n-k}(n)$, $A \mapsto \complement A$, est une bijection. □

4.4.9 Proposition. Soit $n \in \mathbb{N}$. On a $\displaystyle\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

Démonstration. On classe les parties de $P([\![1,n]\!])$ suivant leur cardinal k, c'est-à-dire qu'on écrit $\mathscr{P}([\![1,n]\!]) = \displaystyle\bigcup_{k=0}^{n} \mathscr{P}_k(n)$, l'union étant disjointe. En prenant le cardinal des deux membres on obtient $2^n = |P([\![1,n]\!])| = \displaystyle\sum_{k=0}^{n} |\mathscr{P}_k(n)| = \sum_{k=0}^{n} \binom{n}{k}$. □

4.4.10 Proposition (Formule de Pascal)**.** Soient $k, n \in \mathbb{N}$. Alors $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$.

Démonstration. On compte les parties à $k+1$ éléments de $[\![1,n+1]\!]$ selon qu'elles contiennent ou non $n+1$. Celles qui ne contiennent pas $n+1$ sont en bijection avec $\mathscr{P}_{k+1}(n)$, et celles qui contiennent $n+1$ contiennent k autres éléments de $[\![1,n]\!]$ et sont donc en bijection avec $\mathscr{P}_k(n)$. □

4.4.11 Proposition (Formule du binôme de Newton)**.** Soient $a, b \in \mathbb{C}$ et $n \in \mathbb{N}$. Alors $(a+b)^n = \displaystyle\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$.

Démonstration. On développe le produit $(a+b)^n = (a+b)(a+b)\dots(a+b)$, ce qui donne 2^n termes tous de la forme $a^k b^{n-k}$, pour certains $0 \le k \le n$. À chaque façon de choisir un terme (a ou b) dans chaque parenthèse, on associe une partie $X \in [\![1,n]\!]$ qui correspond aux parenthèses où on choisit a au lieu de b. On peut alors écrire :

$$
\begin{aligned}
(a+b)^n &= \sum_{X \in \mathscr{P}([\![1,n]\!])} a^{|X|} b^{n-|X|} \\
&= \sum_{k=0}^{n} \left(\sum_{X \in \mathscr{P}_k(n)} a^{|X|} b^{n-|X|} \right) \\
&= \sum_{k=0}^{n} \left(\sum_{X \in \mathscr{P}_k(n)} a^k b^{n-k} \right) \\
&= \sum_{k=0}^{n} a^k b^{n-k} |\mathscr{P}_k(n)| \\
&= \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}
\end{aligned}
$$

□

Remarque : il existe aussi une preuve par récurrence sur n qui utilise la formule de Pascal, qui est moins parlante du point de vue combinatoire.

4.4.12 Proposition. Soient $n, k \in \mathbb{N}$. Alors $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$.

La preuve qui suit est la version rigoureuse de la phrase « pour compter le nombre de parties de cardinal k de $[\![1,n]\!]$, on compte le nombre de listes ordonnées de cardinal k, c'est-à-dire

$\dfrac{n!}{(n-k)!}$, puis on divise par le nombre de façons de désordonner ces listes, c'est-à-dire $k!$, puisqu'on ne s'occupe pas de l'ordre ». (La fin de la phrase est floue et non justifiée : pourquoi est-il correct de « diviser » lorsqu'on ne « s'occupe pas » de quelque chose ?)

Démonstration.

Soit I l'ensemble des injections de $[\![1,k]\!]$ dans $[\![1,n]\!]$ (en bijection avec les listes ordonnées de k éléments de $[\![1,k]\!]$). Il est de cardinal $\dfrac{n!}{(n-k)!}$. Montrer le résultat revient à montrer que $|I| = k!|\mathscr{P}_k(n)|$.

Or, on peut écrire $|I| = \sum_{X\in\mathscr{P}_k(n)} \left|\{f\in I\,,\ f([\![1,k]\!]) = X\}\right|$. Mais si X est de cardinal k, une injection $f\in I$ telle que $f([\![1,k]\!]) = X$ est forcément une bijection, et on sait qu'il y a $k!$ telles bijections.

Donc, $|I| = \sum_{X\in\mathscr{P}_k(n)} k! = k!|\mathscr{P}_k(n)|$, ce qu'il fallait démontrer. □

4.4.13 Remarque. *Le principe combinatoire général derrière cette preuve est le suivant : Si ϕ : $A\to B$ entre ensembles finis, alors $|A| = \sum_{b\in B}\left|f^{-1}(\{b\})\right|$. Cela revient à compter le nombre d'éléments de a en les classant d'abord selon leur image dans B, puis en sommant, pour chaque b, le nombre d'antécédents de b. Ici, ce principe serait appliqué avec $A = I$, $B = \mathscr{P}_k(n)$, et ϕ serait l'application qui à $f\in I$ associe son image, qui est un élément de $\mathscr{P}_k(n)$. Dans ce cas particulier, toutes les images réciproques ont le même cardinal $k!$.*

4.4.14 Remarque. *On peut trouver d'autres preuves des résultats présentés ici : des preuves par récurrence, ou bien des preuves calculatoires utilisant la formule $\dbinom{n}{k} = \dfrac{n!}{k!(n-k)!}$ qui doit alors être démontrée le plus tôt possible. Les preuves combinatoires sont souvent plus riches de sens.*

Chapitre 5

Arithmétique

Sommaire

Retour à la table des matières principale

Attention, la présentation qui suit diffère sans doute beaucoup de celle vue en terminale : il faut faire l'effort de l'étudier en détail même si l'ordre dans lequel les notions sont introduites semble « mauvais » : en fait, c'est plutôt le « bon » ordre (si tant est qu'il en existe un).

Le cours d'arithmétique des polynômes suivra le même canevas (définitions semblables, mêmes lemmes aux mêmes endroits, mêmes preuves), de même que le cours d'algèbre générale sur les anneaux par la suite.

5.1 Préliminaires

5.1.1 Division euclidienne

5.1.1 Proposition (Division euclidienne)**.** Soit $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$. Il existe un unique couple $(b, r) \in \mathbb{N}^2$ vérifiant les deux propriétés suivantes :

1. $a = bq + r$;
2. $r < b$.

L'entier b est le *quotient* de la division euclidienne de a par b, et r est le *reste*. Effectuer la division euclidienne de a par b, c'est écrire $a = bq + r$ avec b et q comme plus haut.

5.1.2 Exemple. $17 = 5 \times 3 + 2$ est la division euclidienne de 17 par 5. Le quotient est 3 et il reste 2. Par contre, l'écriture $17 = 5 \times 2 + 7$ bien que correcte n'est pas une division euclidienne, car dans une division euclidienne, le reste *doit* être strictement inférieur à 5.

5.1.2 Idéaux de $\mathbb{Z}$

5.1.3 Définition (Ensembles $\alpha\mathbb{Z}$ et générateur principal)**.** Soit α un entier relatif.

1. On note $\alpha\mathbb{Z}$ l'ensemble $\{\alpha k \mid k \in \mathbb{Z}\} = \{\dots, -2\alpha, -\alpha, 0, \alpha, 2\alpha, 3\alpha, \dots\}$. C'est l'ensemble des multiples de α. Les ensembles $\alpha\mathbb{Z}$ et $(-\alpha)\mathbb{Z}$ sont identiques.
2. Le *générateur principal* de $\alpha\mathbb{Z}$ est $|\alpha|$.

5.1.4 Exemple. $3\mathbb{Z} = \{\dots, -6, -3, 0, 3, 6, 9, 12, \dots\}$. Si $\alpha = 0$, alors $\alpha\mathbb{Z} = \{0\}$. On a $\alpha\mathbb{Z} = \mathbb{Z}$ ssi α est égal à 1 ou -1. Plus généralement, on a $a\mathbb{Z} = b\mathbb{Z}$ ssi $a = b$ ou $a = -b$.

5.1.5 Définition. Un *sous-groupe de* $\mathbb{Z}$ est une partie $G \subseteq \mathbb{Z}$ vérifiant les trois propriétés suivantes :

1. G contient 0.
2. G est stable par somme :$\forall x, y \in G,\ x + y \in G$.
3. G est stable par opposé :$\forall x \in G,\ -x \in G$.

Un ensemble de la forme $\alpha\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ (exercice). La proposition qui suit affirme que la réciproque est vraie.

5.1.6 Proposition. Soit $G \subseteq \mathbb{Z}$ un sous-groupe de $\mathbb{Z}$. Alors, il existe $\alpha \in \mathbb{Z}$ tel que $G = \alpha\mathbb{Z}$.

Démonstration. Soit $G \subseteq \mathbb{Z}$ un sous-groupe de $\mathbb{Z}$. Soit $G_+^* = G \cap \mathbb{N}^*$. Il y a deux cas :

1. Si G_+^* est vide, cela signifie que G ne possède aucun élément strictement positif. Comme G est stable par opposé, il ne peut pas non plus contenir d'éléments strictement négatifs. Cela signifie que $G = \{0\} = 0\mathbb{Z}$.
2. Sinon, c'est une partie non vide de $\mathbb{N}$, qui possède donc un plus petit élément, notons-le α. Par définition, G est stable par somme et opposé, donc $2\alpha \in G$ et $-\alpha \in G$ et plus généralement, pour tout $k \in \mathbb{Z}$, on a $k\alpha \in G$. Donc $\alpha\mathbb{Z} \subseteq G$. Montrons l'inclusion inverse. Soit $x \in G$, positif. Écrivons la division euclidienne de x par α. On a $x = \alpha q + r$, avec $r < \alpha$. Comme G est stable par somme et différence et que $\alpha q \in G$, on en déduit que $r = x - \alpha q$ est également dans G. Or, $r < \alpha$, donc par minimalité de α, $r = 0$, ce qui montre que $x = \alpha q$, donc que $x \in \alpha\mathbb{Z}$. Si x est négatif, ce qui précède montre que $-x \in \alpha\mathbb{Z}$, donc que $x \in \alpha\mathbb{Z}$.

□

5.1.7 Proposition. Un sous-groupe G de $\mathbb{Z}$ est automatiquement *absorbant pour la multiplication*, c'est-à-dire :

$$\forall g \in G, \forall n \in \mathbb{Z}, ng \in G.$$

Pour cette raison et d'autres qui deviendront claires dans un futur cours d'algèbre, on utilise la dénomination « idéal de $\mathbb{Z}$ » au lieu de « sous-groupe de $\mathbb{Z}$ ». Les deux terminologies sont parfaitement équivalentes, dire *idéal* sert à rappeler la propriété supplémentaire d'être absorbant par multiplication.

5.2 Pgcd

5.2.1 Proposition. Soient a et b deux entiers. Alors :

1. L'ensemble $\{ak + bl \mid k, l \in \mathbb{Z}\}$ noté par définition $a\mathbb{Z} + b\mathbb{Z}$, est un idéal de $\mathbb{Z}$.
2. C'est le plus petit idéal de $\mathbb{Z}$ contenant a et b.

3. Il contient $a\mathbb{Z}$ et $b\mathbb{Z}$, donc également $a\mathbb{Z} \cup b\mathbb{Z}$, mais il est en général strictement plus grand que $a\mathbb{Z} \cup b\mathbb{Z}$.

Démonstration.

1. Il suffit de vérifier que c'est un sous-groupe de $\mathbb{Z}$.
2. Si un idéal I de $\mathbb{Z}$ contient a et b, comme il est stable par somme et opposé, il contient $-a$, $-b$, $a + (-a) = 0$, $a + a = 2a$, $a + b$ et plus généralement tous les $ka + lb$ pour $k, l \in \mathbb{Z}$. Donc I contient $a\mathbb{Z} + b\mathbb{Z}$.
3. Il est clair que $a\mathbb{Z} + b\mathbb{Z} = \{ka + bl \mid k, l \in Z\}$ contient $\{ka \mid k \in Z\} = a\mathbb{Z}$ (prendre $l = 0$) ainsi que $b\mathbb{Z}$, et donc contient l'union $a\mathbb{Z} \cup b\mathbb{Z}$. Pour voir que l'inclusion peut être stricte, prenons $a = 4$ et $b = 6$. On a $4\mathbb{Z} \cup 6\mathbb{Z} = \{..., -6, -4, 0, 4, 6, 8, 12, 16, 18, 20, 24, 28, ...\}$. Cet ensemble ne contient pas 2, alors que $2 = 6 - 4 \in 4\mathbb{Z} + 6\mathbb{Z}$.

□

5.2.2 Définition. Soient a et b des entiers. Le générateur principal de $a\mathbb{Z}+b\mathbb{Z}$ est appelé le *pgcd* (pour *plus grand commun diviseur*) de a et b, il est noté $\mathrm{pgcd}(a, b)$.

5.2.3 Remarque. *À ce stade, le nom de* plus grand commun diviseur *est juste une notation. Les deux propositions qui suivent montrent que le pgcd est effectivement un diviseur commun, et que c'est le plus grand tel diviseur positif, en un sens précis.*

5.2.4 Proposition. Soient a et b des entiers, et $d = \mathrm{pgcd}(a, b)$. On a les propriétés suivantes

1. L'entier a est dans $a\mathbb{Z} + b\mathbb{Z}$, donc d divise a. De même, d divise b. C'est donc un *diviseur commun* de a et b, ce qui commence à justifier son nom.
2. L'entier d est dans $d\mathbb{Z}$, donc il existe k et l dans $\mathbb{Z}$, tels que $d = ak + bl$. On dit que (k, l) est un couple (ou paire, par abus de langage) de Bézout pour a et b. L'égalité $d = ak + bl$ est appelée *relation de Bézout*.
3. Si m est un diviseur commun de a et b et que $ak+bl = d$ est une relation de Bézout, alors on voit que m divise $ak + bl$ donc m divise d. C'est en ce sens que d est le *plus grand* diviseur commun.
4. Si $d = 0$, alors $a = b = 0$. En effet, si $d = 0$ alors $\{0\} = a\mathbb{Z} + b\mathbb{Z} \supseteq a\mathbb{Z}$, d'où $a = 0$ et de même $b = 0$.
5. On a $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(b, a) = \mathrm{pgcd}(a, -b)$, car $a\mathbb{Z} + b\mathbb{Z} = b\mathbb{Z} + a\mathbb{Z} = a\mathbb{Z} + (-b)\mathbb{Z}$.
6. $\mathrm{pgcd}(a, 0) = |a|$, car $a\mathbb{Z} + 0\mathbb{Z} = a\mathbb{Z}$.
7. $\mathrm{pgcd}(a, 1) = 1$, car $a\mathbb{Z} + \mathbb{Z} = \mathbb{Z}$.

5.2.5 Proposition. Si $x > 0$, $x|a$ et $x|b$, et $\forall m, m|a$ et $m|b \implies m|x$, alors $x = d$.

Démonstration. Si $x|a$ et $x|b$, alors $x|d$. D'autre part, $d|a$ et $d|a$, donc $d|x$. Donc finalement, $d = x$. Attention, la condition $x > 0$ est indispensable pour ce raisonnement. Deux entiers relatifs peuvent se diviser l'un l'autre, comme 1 et -1, sans être égaux. □

5.2.6 Proposition. Soit $k > 0$. On a $\mathrm{pgcd}(ka, kb) = k\,\mathrm{pgcd}(a, b)$.

Démonstration. Notons provisoirement $d_1 = \mathrm{pgcd}(a, b)$ et $d_2 = \mathrm{pgcd}(ka, kb)$.

Comme $d_1|a$ et $d_1|b$, on a $kd_1|ka$ et $kd_1|kb$ donc finalement $kd_1|d_2$. En particulier, $k|d_2$ donc $\dfrac{d_2}{k}$ est un entier.

D'autre part, $d_2|ka$ et $d_2|kb$, donc en divisant par k et en utilisant la remarque précédente, on a $\dfrac{d_2}{k}|a$ et $\dfrac{d_2}{k}|b$ donc $\dfrac{d_2}{k}|d_1$, d'où $d_2|kd_1$.

Comme kd_1 et d_2 sont positifs, on en déduit $d_2 = kd_1$. □

5.2.1 Algorithme d'Euclide

5.2.7 Lemme (d'Euclide)**.** Soient a, b et k des entiers relatifs. Alors :

$$\text{pgcd}(a,b) = \text{pgcd}(a+kb,b).$$

Démonstration. Ils y a au moins deux façons de prouver le résultat : on peut montrer que les idéaux $a\mathbb{Z}+b\mathbb{Z}$ et $(a+kb)\mathbb{Z}+b\mathbb{Z}$ sont les mêmes, ce qui implique qu'ils ont le même générateur principal, ou alors on peut montrer que (a,b) et $(a+kb,b)$ ont les mêmes diviseurs communs, donc le même plus grand diviseur commun.
Première preuve (mêmes idéaux). D'une part, $(a+kb)\mathbb{Z}+b\mathbb{Z} \subseteq a\mathbb{Z}+b\mathbb{Z}$ car si i et j sont des entiers, alors $i(a+kb)+jb = ia+(iK+j)b \in a\mathbb{Z}+b\mathbb{Z}$. D'autre part, $a\mathbb{Z}+b\mathbb{Z} \subseteq (a+kb)\mathbb{Z}+b\mathbb{Z}$ car si i et j sont des entiers, alors $ia+jb = i(a+kb)+(j-ik)b \in (a+kb)\mathbb{Z}+b\mathbb{Z}$. Finalement, les idéaux $a\mathbb{Z}+b\mathbb{Z}$ et $(a+kb)\mathbb{Z}+b\mathbb{Z}$ sont identiques donc ont le même générateur principal.
Deuxième preuve (mêmes diviseurs). Si $m|a$ et $m|b$, alors $m|a+kb$ et $m|b$.
Si $m|a+kb$ et $m|b$, alors $m|a+kb-kb$ et $m|b$, donc m divise a et b.
On en déduit que les couples (a,b) et $(a+kb,b)$ ont les mêmes diviseurs communs. Ils ont donc le même pgcd. □

5.2.8 Corollaire. En particulier, si $a = bq+r$ (division euclidienne ou pas), alors :

$$\text{pgcd}(a,b) = \text{pgcd}(b,r).$$

5.2.9 Théorème (Algorithme d'Euclide)**.** Appliquer l'algorithme d'Euclide aux entiers naturels a et b, c'est effectuer une suite de divisions euclidiennes :

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\dots \\ r_{n-2} &= q_n r_{n-1} + r_n \end{aligned}$$

en continuant tant que r_n n'est pas nul. Alors, on a les résultats suivants :

1. (terminaison de l'algorithme) Au bout d'un certain nombre d'étapes, on a $r_n = 0$, donc l'algorithme termine en un nombre fini d'étapes.
2. Le dernier reste non nul r_{n-1} est le pgcd de a et b.

Démonstration.

1. (Preuve de terminaison) Il s'agit de montrer que l'on ne peut pas continuer indéfiniment à faire des divisions euclidiennes. Par définition de ce qu'est une division euclidienne, on a : $b > r_1$, $r_1 > r_2$ et plus généralement $r_i > r_{i+1}$. La suite des restes est une suite strictement décroissante d'entiers positifs, elle ne peut pas être infinie.
2. (Preuve de correction du calcul de pgcd) Par le lemme d'Euclide et son corollaire appliqués à chaque étape, on a

$$\text{pgcd}(a,b) = \text{pgcd}(b,r_1) = \text{pgcd}(r_1,r_2) = \dots = \text{pgcd}(r_{n-1},r_n) = \text{pgcd}(r_{n-1},0) = r_{n-1}.$$

□

On remarque qu'il n'est pas nécessaire que $a > b$ dans l'algorithme : si ce n'est pas le cas, l'algorithme les replace dans le bon ordre au cours de la première étape.

L'algorithme d'Euclide permet également d'obtenir une relation de Bézout en « remontant » les étapes de l'algorithme :

$$d = r_{n-1} = r_{n-3} - q_{n-1}r_{n-2} = r_{n-3} - q_{n-1}(r_{n-4} - q_{n-2}r_{n-3})\dots = au+bv.$$

5.2.2 Nombres premiers entre eux, théorème de Gauß

5.2.10 Définition. Deux nombres relatifs a et b sont premiers entre eux si $\operatorname{pgcd}(a,b) = 1$. On note : $a \wedge b = 1$.

5.2.11 Proposition. Soient a et b des entiers. On a

$$a \wedge b = 1 \iff (\exists u, v \in \mathbb{Z} \mid au + bv = 1)$$

Démonstration. Sens $\Longrightarrow$: il existe une relation de Bézout.
Sens $\Longleftarrow$: si $au + bv = 1$, alors $\operatorname{pgcd}(a,b)$ divise 1, donc vaut 1. □

5.2.12 Proposition. Soient a et b des entiers. Si $a \wedge b = 1$ et $a \wedge c = 1$, alors $a \wedge bc = 1$.

Démonstration. Si $au + bv = 1$ et $au' + cv' = 1$ sont des relations de Bézout, on a en multipliant les deux :

$$1 = (au + bv)(au' + cv') = a(auu' + bvu' + ucv') + bcvv'.$$

□

5.2.13 Corollaire. Soient a, b et $n > 0$, $m > 0$ des entiers. Si $a \wedge b = 1$, alors $a^n \wedge b^m = 1$.

Démonstration. On a $a \wedge b = 1 \implies a \wedge b^2 = ... = a \wedge b^m = 1$, puis $b^m \wedge a \implies b^m \wedge a^2 = ... = b^m \wedge a^n = 1$. □

Attention, ceci n'est **pas** un résultat de passage au produit avec le symbole $\wedge$! Si on a $a \wedge b = 1$ et $c \wedge d = 1$, on n'a **pas** $ac \wedge bd = 1$. Exemple : $2 \wedge 3 = 1$ et $3 \wedge 2 = 1$ et pourtant $6 \wedge 6 \neq 1$.

5.2.14 Théorème (« théorème de Gauß »)**.** Soient a, b et c des entiers. Si $a \wedge b = 1$ et $a|bc$, alors $a|c$.

Démonstration. Soit $ak + bl = 1$ une relation de Bézout pour a et b. Si a divise bc, alors il divise également blc. D'autre part, a divise akc. Donc $a|(bl + ak)c$ c'est-à-dire $a|c$. □

5.2.3 Résolution des équations diophantiennes du type $ax + by = c$

5.2.15 Définition. Une équation diophantienne est une équation du type $F(x_1, x_2, ...x_k) = 0$, les inconnues x_1, ... x_k appartiennent à $\mathbb{Z}$, ou une partie de $\mathbb{Z}$.

Exemples :
$12x + 3y = 8$, d'inconnues x et y dans $\mathbb{Z}$.
$2^n - 3^m = 7$ d'inconnues n et m dans $\mathbb{N}$.
$x^n + y^n = z^n$ d'inconnues x, y, z, n dans $\mathbb{N}$. (C'est l'équation de Fermat ; il a été démontré en 1994 après trois siècles d'efforts que l'équation n'admet des solutions que si $n = 2$.)

Dans ce cours, on s'intéresse aux équations du type $ax + by = c$ d'inconnues x et y dans $\mathbb{Z}$, et avec a, b et c des paramètres entiers.

Géométriquement, cela revient à trouver les points à coordonnées entières de la droite du plan d'équation cartésienne $ax + by = c$.

La méthode de résolution consiste, comme pour les équations différentielles linéaires, à trouver une solution particulière de l'équation, puis à y ajouter les solutions de l'équation homogène associée, qui est par définition l'équation obtenue en remplaçant le second membre par zéro : $ax + by = 0$. C'est le contenu de la proposition suivante :

5.2.16 Proposition. Soient a, b des entiers non tous deux nuls, c un entier. On considère l'équation $(E) : ax + by = c$ d'inconnue $(x, y) \in \mathbb{Z}^2$, ainsi que l'équation homogène associée $(E_h) : ax + by = 0$.

Si (x_p, y_p) est une solution particulière de (E), alors son ensemble de solutions est

$$\left\{(x_p, y_p) + (s, t) \mid (s, t) \text{ solution de } E_h\right\}$$

Démonstration. Soit (x, y) un couple d'entiers.

$$\begin{aligned} ax + by = c &\iff ax + by = ax_p + by_p \\ &\iff a(x - x_p) + b(y - y_p) = c - c = 0, \end{aligned}$$

donc (x, y) est solution de (E) si et seulement si $(x - x_p, y - y_p)$ est solution de l'équation homogène (E_h) associée à (E). On en déduit le résultat. □

Il reste donc à établir un critère pour l'existence de solutions, et à donner une méthode pour trouver des solutions particulières, et pour résoudre les équations homogènes.

5.2.17 Proposition (Existence de solutions et solution particulière)**.** Soient a, b et c des entiers.

1. L'équation $(E) : ax + by = c$ d'inconnue $(x, y) \in \mathbb{Z}^2$ admet des solutions si et seulement si $\operatorname{pgcd}(a, b) | c$.
2. Dans ce cas, en notant $k = c / \operatorname{pgcd}(a, b)$ et $au + bv = \operatorname{pgcd}(a, b)$ une relation de Bézout, une solution particulière est (ku, kv).

Démonstration. Montrons d'abord que la condition est nécessaire. S'il existe une solution (x, y), alors $ax + by = c$ et donc tout diviseur commun de a et b divise aussi $ax + by$ et donc c. En particulier $\operatorname{pgcd}(a, b) | c$.

Réciproquement, montrons que la condition est suffisante en prouvant que le couple fourni est bien solution. En multipliant par k la relation de Bézout on obtient $auk + bvk = \operatorname{pgcd}(a, b)k = c$ donc (uk, vk) est bien une solution de (E). □

5.2.18 Proposition (Résolution des équations homogènes)**.** Soient a, b des entiers non tous deux nuls, et notons $d = \operatorname{pgcd}(a, b)$. L'équation $ax + by = 0$ d'inconnue $(x, y) \in \mathbb{Z}^2$ a pour ensemble de solutions :

$$\left\{k\left(\frac{-b}{d}, \frac{a}{d}\right), k \in \mathbb{Z}\right\}$$

(Remarque : si a et b sont nuls, alors l'ensemble des solutions est $\mathbb{Z}^2$ tout entier...)

Démonstration. (de la proposition) Écrivons $a = da'$ et $b = db'$. L'équation s'écrit donc $da'x + db'y = 0$ et en simplifiant par d qui est non nul, on obtient l'équation équivalente $a'x + b'y = 0$, avec $a' \wedge b' = 1$.

Si un des deux entiers a ou b est nul, le résultat est facile.

Sinon, le théorème de Gauß donne alors $a' | y$, donc il existe $k \in \mathbb{Z}$ tel que $y = ka'$. On trouve alors $x = -kb'$ en simplifiant par a'. □

5.2.19 Exemple. L'ensemble des solutions entières de l'équation $2x + 6y = 0$ est $\{k(3, -1) \mid k \in \mathbb{Z}\}$.

5.3 Ppcm

5.3.1 Proposition. Soient $a, b \in \mathbb{Z}$. L'ensemble $a\mathbb{Z} \cap b\mathbb{Z}$ (qui est par définition l'ensemble des entiers qui sont à la fois multiples de a et multiples de b, c'est-à-dire l'ensemble des multiples communs de a et b) est un idéal de $\mathbb{Z}$.

Démonstration. On a déjà vu qu'il suffit de montrer que c'est un sous-groupe de $\mathbb{Z}$, donc que $a\mathbb{Z} \cap b\mathbb{Z}$ contient 0, est stable par somme et par opposé.

1. $0 \in a\mathbb{Z}$ et $0 \in b\mathbb{Z}$, donc $0 \in a\mathbb{Z} \cap b\mathbb{Z}$.
2. Soient x, y dans $a\mathbb{Z} \cap b\mathbb{Z}$. Comme x et y sont dans $a\mathbb{Z}$, $x + y \in a\mathbb{Z}$ car $a\mathbb{Z}$ est stable par somme. On montre de même que $x + y \in b\mathbb{Z}$. Donc $x + y \in a\mathbb{Z} \cap b\mathbb{Z}$.
3. Soit $x \in a\mathbb{Z} \cap b\mathbb{Z}$. Comme $x \in a\mathbb{Z}$, on a $-x \in a\mathbb{Z}$ car $a\mathbb{Z}$ est stable par opposé. On montre de même que $-x \in b\mathbb{Z}$. Donc $-x \in a\mathbb{Z} \cap b\mathbb{Z}$.

De façon générale et en anticipant sur un futur cours d'algèbre, l'intersection de deux sous-groupes est un sous-groupe. □

5.3.2 Définition. Soient $a, b \in \mathbb{Z}$. Le générateur principal de l'idéal $a\mathbb{Z} \cap b\mathbb{Z}$ est appelé *plus petit commun multiple* (sous-entendu, le plus petit parmi ceux strictement positifs) et noté $\mathrm{ppcm}(a, b)$.

5.3.3 Proposition. Soient a, $b \in \mathbb{Z}$. On a :

1. $\mathrm{ppcm}(a, 1) = |a|$.
2. $\mathrm{ppcm}(a, 0) = 0$.
3. Si M est un multiple de a et de b, alors c'est un multiple de $\mathrm{ppcm}(a, b)$.

5.3.4 Proposition. Soient a et b des naturels non nuls. On a :

$$\mathrm{pgcd}(a, b) \times \mathrm{ppcm}(a, b) = ab.$$

Démonstration.

— Premier cas : $a \wedge b = 1$. Soit $m = \mathrm{ppcm}(a, b)$. Alors a divise m donc on peut écrire $m = ka$. D'autre part b divise m, donc b divise ka, par le théorème de Gauss, comme b est premier avec a, on en déduit que b divise k. Donc $ab|m$. D'autre part, ab est un multiple commun de a et de b, donc $m|ab$. Finalement, $m = ab$.

— Deuxième cas : $d = \mathrm{pgcd}(a, b) \geq 1$. Écrivons $a = da'$ et $b = db'$. On a donc $a' \wedge b' = 1$. Donc $\mathrm{ppcm}(a', b') = a'b'$, puis $\mathrm{ppcm}(da', db') = da'b' = ab/d$.

□

5.4 Nombres premiers

5.4.1 Définition

5.4.1 Définition. Un entier naturel p est dit *premier* s'il possède exactement deux diviseurs positifs distincts : 1 et p. En particulier, un nombre premier est toujours ≥ 2.

Le nombre 1 n'est pas premier. Les nombres premiers sont 2, 3, 5, 7, 11, 13, 17, 19, 23 etc.

5.4.2 Proposition. Soit p un nombre premier et $a \in \mathbb{Z}$. Alors $a \wedge p = 1$ ou $p|a$.

Démonstration. On a $\mathrm{pgcd}(a, p)|p$ donc $\mathrm{pgcd}(a, p)$ vaut 1 ou p. □

5.4.3 Définition. Un entier naturel $n \geq 2$ qui n'est pas premier est dit *composé*. Cela revient à :

$$\exists a, b \in [\![2, n-1]\!] \mid n = ab.$$

5.4.4 Proposition (Test de primalité)**.** Un entier n est premier si $\forall a \leq \sqrt{n}$ entier, a ne divise pas n.

Démonstration. Si n est composé, alors $n = ab$ avec $a, b \in [\![2, n-1]\!]$, donc au moins un des deux entiers a ou b est $\leq \sqrt{n}$ (sinon on aurait $n = ab > \sqrt{n}^2 = n$, absurde). L'autre sens de l'équivalence est évident. □

5.4.2 Décomposition en produit de nombres premiers

Soit $\mathscr{P}$ l'ensemble des nombres premiers.

5.4.5 Proposition.

$$\forall n \geq 1, \exists !(\alpha_p)_{p\in\mathscr{P}},\ n = \prod_{p\in\mathscr{P}} p^{\alpha_p}.$$

En fait, seul un nombre fini des α_p sont non nuls.

Démonstration. On montre l'existence par récurrence forte sur n. Pour $n \geq 1$, notons $A(n)$ l'assertion $\exists(\alpha_p)_{p\in\mathscr{P}},\ n = \prod_{p\in\mathscr{P}} p^{\alpha_p}$.

Initialisation. Pour $n = 1$, la suite nulle $\alpha_p = 0$ (pour tout p) convient.

Hérédité sous hypothèse de récurrence forte. Soit $n \geq 1$, et supposons $A(k)$ vraie pour tout $k \leq n$. Montrons $A(k+1)$. Si $n+1$ est premier, alors la suite $\alpha_{n+1} = 1$ et $\alpha_i = 0$ pour $i \neq n+1$ convient. Si $n+1$ est composé, écrivons $n = bc$ avec $b, c \leq n$. Par hypothèse de récurrence appliquée à b et c, on peut écrire $b = \prod_{p\in\mathscr{P}} p^{\beta_p}$ et $c = \prod_{p\in\mathscr{P}} p^{\gamma_p}$. On a donc

$$bc = \prod_{p\in\mathscr{P}} p^{\beta_p} \cdot \prod_{p\in\mathscr{P}} p^{\gamma_p} = \prod_{p\in\mathscr{P}} p^{\beta_p+\gamma_p}$$

et la suite $\alpha_p = \beta_p + \gamma_p$ convient.

L'unicité de la décomposition est laissée en exercice. □

5.4.6 Définition (Valuation p-adique)**.** Soit n un entier et p un nombre premier. On appelle *valuation p-adique de n* et on note $v_p(n)$ l'exposant de p dans la décomposition de n en facteurs premiers. On peut donc écrire

$$n = \prod_{p\in\mathscr{P}} p^{v_p(n)}.$$

Exemples : $v_2(16) = 4$, $v_3(17) = 0$, $v_2(18) = 1$.

5.4.7 Proposition (Propriétés fondamentales de la valuation p-adique)**.**

$$v_p(n) \geq 1 \iff p|n.$$

$$v_p(nm) = v_p(n) + v_p(m).$$

5.4.8 Proposition (Critère de divisibilité en termes de valuations p-adiques)**.**

$$n|m \iff \left(\forall p \in \mathscr{P},\ v_p(n) \leq v_p(m)\right)$$

Démonstration. Si $m = kn$, alors pour tout $p \in \mathscr{P}$, $v_p(m) = v_p(k) + v_p(n) \geq v_p(n)$.
Réciproquement, on a

$$m = \prod_{p\in\mathscr{P}} p^{v_p(m)} = \prod_{p\in\mathscr{P}} p^{v_p(n)} \cdot \prod_{p\in\mathscr{P}} p^{v_p(m)-v_p(n)}$$

donc $n|m$. □

5.4.9 Corollaire (pgcd et ppcm en termes de valuations p-adiques)**.**

$$\operatorname{pgcd}(n,m) = \prod_{p\in\mathscr{P}} p^{\min(v_p(n),v_p(m))},$$

$$\operatorname{ppcm}(n,m) = \prod_{p\in\mathscr{P}} p^{\max(v_p(n),v_p(m))}.$$

Démonstration. Notons $d = \mathrm{pgcd}(n, m)$ et $a = \prod_{p\in\mathscr{P}} p^{\min(v_p(n),v_p(m))}$.

Pour tout $p \in \mathscr{P}$, on a $v_p(a) \leq v_p(n)$ donc $a|n$. De même, $a|m$. Donc a est un diviseur commun de m et n, et il divise donc leur pgcd : $a|d$.

D'autre part, soit $\in \mathscr{P}$. On a $d|m$ donc $v_p(d) \leq v_p(m)$, et de même, $d|n$ donc $v_p(d) \leq v_p(n)$. On en déduit que $v_p(d) \leq \min(v_p(n), v_p(m)) = v_p(a)$. Comme ceci vaut pour tout $p \in \mathscr{P}$, on a $d|a$.

Finalement on a $a|d$ et $d|a$, donc $\boxed{d = a}$.

Le résultat sur le ppcm se démontre de la même manière. □

5.4.10 Exemple. $\mathrm{pgcd}(120, 252) = \mathrm{pgcd}(2^3 \cdot 3 \cdot 5, 2^2 \cdot 3^2 \cdot 7) = 2^2 \cdot 3 = 12$. Pour les nombres faciles à factoriser, c'est toujours comme cela que l'on procède, l'algorithme d'Euclide est à réserver aux cas difficiles, ou aux calculs de relations de Bézout.

5.4.3 Infinitude des nombres premiers

5.4.11 Proposition. L'ensemble $\mathscr{P}$ des nombres premiers est infini.

Démonstration. Supposons par l'absurde qu'il soit fini, et soir M son plus grand élément. Pour tout $k \leq M$, k divise $M!$, donc le reste par la division euclidienne de $M! + 1$ par k est 1. On en déduit que k ne divise pas $M! + 1$. En particulier, aucun nombre premier ne divise $M! + 1$, qui ne possède donc pas de décomposition en facteurs premiers, absurde. □

Chapitre 6

Relations d'ordre, relations d'équivalence

Sommaire

Retour à la table des matières principale

6.1 Relations binaires

6.1.1 Définition. Soit E un ensemble. Une *relation binaire* $\mathscr{R}$ sur E est une application de $E\times E$ dans $\{\text{vrai}, \text{faux}\}$.

Une relation $\mathscr{R}$ est caractérisée par la partie de $E\times E$ constituée des couples (x,y) tels que $\mathscr{R}(x,y) = \text{vrai}$. On notera « $x\mathscr{R}y$ » au lieu de « $\mathscr{R}(x,y) = \text{vrai}$ » et « $x \not\mathscr{R} y$ » au lieu de « $\mathscr{R}(x,y) = \text{faux}$ »

6.1.2 Exemple. Si E est fini de cardinal n, il existe 2^{n^2} relations binaires sur E. En effet, d'après 4.4.1 on a $|E\times E| = n^2$ et donc d'après 4.4.6 on obtient $|\mathscr{P}(E\times E)| = 2^{n^2}$.

6.1.3 Exemples. Les symboles $=$, $\leq$, $<$, $\geq$, $>$, $|$ (divise), $//$ (parallèle à), $\perp$ (perpendiculaire à), $\subseteq$ (inclus dans) désignent des relations binaires sur des ensembles. La relation d'égalité $=$ correspond à la partie diagonale de $E\to E$, c'est-à-dire à la partie

$$\Delta_E = \{(x,x) \mid x\in E\}$$

6.1.4 Exemple (Zérologie)**.** La relation vide est celle qui correspond à la partie vide de $E \times E$: pour cette relation, aucun élément n'est relié à aucun autre : $x\mathscr{R}y$ est toujours faux. À l'autre extrême, la partie plein de $E \times E$ est une relation binaire, pour laquelle tout élément est relié à tout autre élément : $x\mathscr{R}y$ est toujours vrai.

6.1.5 Définition. Soit E un ensemble. Une relation binaire $\mathscr{R}$ sur E est :

1. réflexive ssi $\forall x \in E, x\mathscr{R}x$;
2. transitive ssi $\forall x, y, z \in E, x\mathscr{R}y$ et $y\mathscr{R}z \implies x\mathscr{R}z$;
3. antisymétrique ssi $\forall x, y \in E, x\mathscr{R}y$ et $y\mathscr{R}x \implies x = y$.
4. symétrique ssi $\forall x, y \in E, x\mathscr{R}y \implies y\mathscr{R}x$.

6.1.6 Mise en garde. Contrairement à ce qu'on peut croire, une relation peut être à la fois symétrique et antisymétrique, comme par exemple la relation =. (Si la relation est de plus supposée réflexive, c'est le seul exemple.)

Le tableau suivant résume sans preuve quelques propriétés des relations classiques. (Certains points seront détaillés par la suite.)

relation	réflexive	transitive	symétrique	antisymétrique
$=$	oui	oui	oui	oui
$\neq$	non	non	oui	non
$\leq$ sur $\mathbb{R}$	oui	oui	non	oui
$<$ sur $\mathbb{R}$	non	oui	non	oui [1]
$\mid$ sur $\mathbb{N}$	oui	oui	non	oui
$\nmid$ sur $\mathbb{N}$	non	non	non	non
$\mid$ sur $\mathbb{Z}$	oui	oui	non	non
$\subseteq$ sur $\mathscr{P}(E)$	oui	oui	non	oui
$//$ sur les droites du plan	oui	oui	oui	non
$\perp$ sur les droites du plan	non	non	oui	non

6.1.7 Définition (Raffinement d'une relation)**.** Soient $\mathscr{R}$ et $\mathscr{S}$ des relations binaires sur E. On dit que $\mathscr{R}$ est plus fine que $\mathscr{S}$, ou encore que c'est est un raffinement, si $\forall x, y \in E, x\mathscr{R}y \implies x\mathscr{S}y$.

6.1.8 Définition. Soit E un ensemble muni d'une relation binaire $\mathscr{R}$. La relation *réciproque* ou *transposée*, notée ${}^t\mathscr{R}$, est définie par : $x\,{}^t\mathscr{R}y \iff y\mathscr{R}x$.

6.1.9 Exercice. Montrer qu'une relation $\mathscr{R}$ est symétrique si et seulement si $\mathscr{R} = {}^t\mathscr{R}$.

6.1.10 Exercice. Montrer qu'un ensemble fini de cardinal n possède 2^{n^2-n} relations réflexives et $2^{n(n+1)/2}$ relations symétriques.

6.2 Relations d'ordre

6.2.1 Définitions et vocabulaire

6.2.1 Définition. Une relation est une *relation d'ordre* ssi elle est réflexive, transitive et antisymétrique.

Un ensemble E muni d'une relation d'ordre $\mathscr{R}$ est appelé *ensemble ordonné*.

6.2.2 Exemples. a) La relation $\leq$ est une relation d'ordre sur $\mathbb{N}$, ou sur $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$. (Mais pas sur $\mathbb{C}$: la relation $\leq$ n'est même pas *définie* sur $\mathbb{C}$.)

b) La relation $\subseteq$ est une relation d'ordre sur $\mathscr{P}(E)$. L'antisymétrie est exactement le principe de double inclusion.

c) La relation $|$ (« divise ») est une relation d'ordre sur $\mathbb{N}^*$, ainsi que sur l'ensemble $\mathbb{N}$. Attention : dans $\mathbb{N}$, tout entier divise 0 !

6.2.3 Mise en garde. 1. La relation $<$ n'est pas une relation d'ordre sur $\mathbb{R}$ (ni sur $\mathbb{N}$, $\mathbb{Z}$ ou $\mathbb{Q}$), car elle n'est pas réflexive, et la relation de divisibilité $|$ n'est pas une relation d'ordre sur $\mathbb{Z}^*$ ni sur $\mathbb{Z}$, car elle n'est pas antisymétrique : $1|-1$ et $-1|1$ et pourtant $1 \neq -1$.

2. il faut systématiquement préciser l'ordre auquel on se réfère, même pour un ensemble « connu ». Par exemple, il faut éviter de parler de « l'ensemble ordonné $\mathbb{N}$ » : en effet $\mathbb{N}$ peut être muni de l'ordre usuel $\leq$ ou bien de la divisibilité $|$ et les deux ordres sont fréquemment utilisés.

6.2.4 Définition. Si $\mathscr{R}$ est une relation d'ordre sur E, on peut lui associer une relation d'*ordre strict*, définie par « $x\mathscr{R}y$ et $x \neq y$ ». (Remarque : une relation d'ordre strict n'est pas une relation d'ordre puisqu'elle n'est pas réflexive.)

6.2.5 Exemple. Sur $\mathbb{R}$, l'ordre strict associé à la relation d'ordre $\leq$ est l'inégalité stricte $<$.

Dans ce cours, on notera en général $\leq_E$ au lieu de $\mathscr{R}$ une relation d'ordre générique sur E (même si la relation n'a rien à voir avec l'inégalité $\leq$ sur $\mathbb{R}$), afin de distinguer les relations d'ordre des relations binaires générales. On notera $<_E$ la relation d'*ordre strict* qui lui est associée.

Enfin, les notations $\geq_E$ et $>_E$ désignent les relations transposées de $\leq_E$ et $<_E$. Autrement dit $x \geq_E y$ et $x >_E y$ sont synonymes de $y \leq_E x$ et $y <_E x$.

6.2.6 Mise en garde. Contrairement au cas particulier de $(\mathbb{R}, \leq)$, dans un ensemble ordonné général $(E, \leq_E)$ la négation de « $x \leq_E y$ » n'est **pas** « $y <_E x$ ». Par exemple, le contraire de « $2|n$ » n'est pas « n divise strictement 2. »

6.2.7 Définition. Une relation d'ordre $\leq_E$ sur un ensemble E est *totale* si tous les éléments sont comparables, c'est-à-dire si :

$$\forall x, y \in E, x \leq_E y \text{ ou } y \leq_E x.$$

Un ensemble muni d'un ordre total est appelé *ensemble totalement ordonné* . Une relation d'ordre qui n'est pas totale est dite d'ordre *partiel*.

6.2.8 Remarque. *Si x et y sont deux éléments d'un ensemble totalement ordonné $(E, \leq_E)$, alors le contraire de $x \leq_E y$ est $x >_E y$. Comme remarqué plus haut, ceci est **faux** si l'ordre n'est pas total, justement à cause d'éventuels éléments non comparables.*

6.2.9 Exemples. La relation d'ordre $\leq$ sur $\mathbb{R}$ (ou $\mathbb{N}$, $\mathbb{Q}$ ou $\mathbb{Z}$) est totale. Par contre, $\subseteq$ et $|$ ne sont pas totales. Par exemple, dans $\mathscr{P}(\mathbb{R})$, les parties $\mathbb{R}_+$ et $]-3, 6]$ ne sont pas comparables pour l'inclusion. Dans $\mathbb{N}^*$, les éléments 2 et 3 ne sont pas comparables pour la divisibilité.

6.2.10 Exercice. Soit E un ensemble. Montrer que « est plus fine que » est une relation d'ordre sur l'ensemble des relations binaires sur E.

6.2.2 Applications croissantes, décroissantes, monotones

6.2.11 Définition. Soient $(E, \leq_E)$ et $(F, \leq_F)$ des ensembles ordonnés et $f : E \to F$. On dit que f est

1. *croissante* si $\forall x, y \in E, x \leq_E y \implies f(x) \leq_F f(y)$;

2. *décroissante* si $\forall x, y \in E, x \leq_E y \implies f(x) \geq_F f(y)$;
3. *monotone* si elle est croissante ou décroissante ;
4. *strictement croissante* si $\forall x, y \in E, x <_E y \implies f(x) <_F f(y)$;
5. *strictement décroissante* si $\forall x, y \in E, x <_E y \implies f(x) >_F f(y)$;
6. *strictement monotone* si elle est strictement croissante ou strictement décroissante.

(Remarque : dans cette situation, il est important de distinguer les relations d'ordre sur E et sur F.)

6.2.12 Exemple. 1. L'application $f : \mathbb{R} \to \mathbb{R}, x \mapsto x + e^x$ est croissante pour l'ordre usuel $\leq$ sur $\mathbb{R}$.

2. Si E est fini, l'application $f : \mathscr{P}(E) \to \mathbb{N}$, $A \mapsto \mathrm{Card}(A)$ est croissante entre les ensembles ordonnés $(\mathscr{P}(E), \subseteq)$ et $(\mathbb{N}, \leq)$.
3. L'application $f : \mathscr{P}(E) \to \mathscr{P}(E)$, $A \mapsto \complement A$ est décroissante pour l'inclusion, car $A \subseteq B \implies \complement B \subseteq \complement A$.
4. Une application *décroissante* entre $(E, \leq_E)$ et $(F, \leq_F)$ est la même chose qu'une application *croissante* entre $(E, \leq_E)$ et $(F, \geq_F)$.

6.2.13 Exercice. Montrer qu'une application strictement croissante entre ensembles totalement ordonnés est injective.

6.2.14 Proposition. 1. La composée de deux applications croissantes est croissante.

2. La composée de deux applications décroissantes est croissante.
3. La composée d'une application décroissante et d'une croissante est décroissante.

Démonstration. Application directe de la définition. □

6.2.3 Plus grand et plus petit élément

6.2.15 Définition. Soit $(E, \leq_E)$ un ensemble ordonné et $A \subseteq E$ une partie non vide.

1. Un élément $m \in E$ est un *majorant* de A si $\forall a \in A, a \leq_E m$.
2. La partie A est *majorée* si elle possède des majorants.
3. Un élément $m \in A$ qui est un majorant de A est appelé un *plus grand élément de* A, ou *maximum* de A.
4. On définit de même les *minorants*, les parties minorées et les plus petits éléments.

6.2.16 Exemple. a) Dans l'ensemble ordonné $(\mathbb{R}, \leq)$, la partie $[2, 5]$ est majorée par 5, mais aussi par 6, 10 etc. La partie $\mathbb{R}_+$ est minorée, mais pas majorée. La partie $\mathbb{Z}$ n'est ni minorée ni majorée.

b) Toute partie non vide de $\mathbb{N}$ admet un plus petit élément pour l'ordre usuel $\leq$ (c'est la propriété fondamentale de $\mathbb{N}$), mais pas forcément de plus grand élément.

c) Dans un ensemble ordonné non vide $(E, \leq_E)$, la partie vide est majorée : tout élément m est un majorant, car l'assertion $\forall x \in \varnothing, x \leq_E m$ est vraie. De la même façon, dans un ensemble non-vide, la partie vide est minorée par n'importe quel élément.

6.2.17 Remarque. *Attention aux reformulations hâtives. Si $x \in E$ est un élément qui ne possède aucun majorant strict, on ne peut pas pour autant en conclure que x est un plus grand élément de E. Par exemple, dans l'ensemble ordonné $\{2, 3, 4\}$ muni de la divisibilité, l'élément 4 ne possède aucun majorant strict, pourtant il ne majore pas 3 : encore une fois, cela est dû au fait que l'ordre n'est pas forcément total, et que le contraire de $x \geq y$ n'est pas $x < y$.*

6.2.18 Proposition (Unicité du plus grand élément, s'il existe)**.** Si $A \subseteq E$ possède un plus grand élément, il est unique. On le note alors $\max(A)$. De même, si $A \subseteq E$ possède un plus petit élément, il est unique. On le note alors $\min(A)$.

Démonstration. Soient m et m' deux plus grands éléments de A. Comme m est un plus grand élément, on a par définition $\forall x \in A, x \leq_E m$ et donc en particulier $m' \leq_E m$. De même, comme m' est un plus grand élément, on a $m \leq_E m'$. Par antisymétrie de la relation d'ordre, on a $m = m'$.

On prouve le résultat pour le plus petit élément de la même manière. □

6.2.19 Exemples.
a) La partie $[0,1]$ est majorée dans $\mathbb{R}$ car 1, 2 ou encore 5 sont des majorants. Elle possède un plus grand élément : 1.
b) La partie $]3,+\infty[$ de $\mathbb{R}$ n'a pas de plus grand élément car elle n'est pas majorée.
c) La partie $A = [0,1[$ de $\mathbb{R}$ est majorée. Par contre, elle n'a pas de plus grand élément.
d) La partie $B = \{x \in \mathbb{Q} \mid x^2 \leq 2\}$ est majorée (par $\sqrt{2}$ par exemple), mais n'admet pas de plus grand élément (rappel : $\sqrt{2} \notin \mathbb{Q}$).
e) Si E est un ensemble, alors $\mathscr{P}(E)$ muni de l'inclusion possède un plus grand élément : E, et un plus petit élément : $\varnothing$.
f) Dans l'ensemble ordonné $(\mathbb{N}^*, |)$, la partie $\{2,3,4\}$ n'a pas de plus grand élément.
g) Dans l'ensemble ordonné $(\mathbb{N}, |)$, il y a un plus petit élément au sens de la divisibilité, c'est 1 (et non zéro). D'autre part, l'élément 0 est en fait le plus grand élément au sens de la divisibilité : tout nombre entier k divise 0.

6.2.4 Borne supérieure, borne inférieure

6.2.20 Définition (Borne supérieure)**.** La partie $A \subseteq E$ admet une borne supérieure $s \in E$ ssi :

1. s est un majorant de A;
2. tout majorant de A majore s.

(En d'autres termes, s est le plus petit des majorants de A, ou encore : l'ensemble de tous les majorants de A possède un plus petit élément s.)

Attention, contrairement à un plus grand élément, une borne supérieure de A, s'il en existe, n'appartient pas forcément à A.

6.2.21 Proposition (Unicité de la borne supérieure, s'il en existe une)**.** Soit $(E, \leq_E)$ un ensemble ordonné, et $A \subseteq E$. Si A possède une borne supérieure, elle est unique et on la note $\sup(A)$.

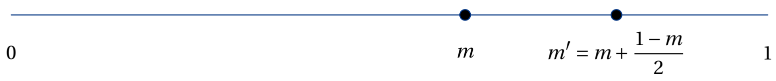
Démonstration. Soient s et s' deux bornes supérieures de A. Comme s est une borne supérieure et s' un majorant, on a $s \leq_E s'$. Un raisonnement symétrique montre que $s' \leq_E s$, et finalement $s' = s$. □

6.2.22 Exemple. La partie $\mathbb{R}_+ \subseteq \mathbb{R}$ n'a pas de borne supérieure. La partie $A = [0,1[\subseteq \mathbb{R}$ n'a pas de plus grand élément, mais possède une borne supérieure : 1.

Démonstration. Pour le premier point, la partie n'a même pas de majorant donc c'est clair. D'une part, il est clair que 1 est un majorant de $[0,1[$, c'est-à-dire que $\forall x \in [0,1[$, $x \leq 1$.

Vérifions la seconde partie de la définition. Il s'agit de montrer qu'un élément m de $[0,1[$ ne peut pas être un majorant de $[0,1[$. Mais si $m \in [0,1[$, alors on peut considérer le réel $m' = m + \frac{1-m}{2}$. Comme $0 \leq m < 1$, on a l'encadrement $0 < \frac{1-m}{2} < 1-m$ et donc en sommant m on obtient

$$m < m' < 1$$



Ceci montre que m ne majore pas m', qui est dans $[0,1[$. Donc m n'est pas un majorant de $[0,1[$. □

Autre exemple important de borne supérieure qui n'est pas un plus grand élément : la partie $\{x \in \mathbb{Q}, x^2 < 2\}$ de $\mathbb{R}$ est majorée et admet une borne supérieure égale à $\sqrt{2}$ et qui n'appartient pas à A car $\sqrt{2} \notin \mathbb{Q}$.

6.2.23 Proposition. Soit $(E, \leq_E)$ un ensemble ordonné $A \subseteq E$. Si A admet une borne supérieure et que $\sup(A) \in A$, alors c'est son plus grand élément. Si A admet un plus grand élément, c'est aussi sa borne supérieure.

Démonstration. Exercice, appliquer les définitions. □

Enfin, on définit de même ce qu'est une *borne inférieure*, et on montre que si une partie admet une borne inférieure, alors celle-ci est unique. On la note $\inf(A)$.

La borne inférieure d'une partie, même si elle existe, n'appartient pas forcément à la partie. Par exemple, 0 est la borne inférieure de $]0,1]$.

6.2.24 Théorème ($\mathbb{R}$ possède la propriété de la borne supérieure)**.** Dans $(\mathbb{R}, \leq)$, toute partie non vide et majorée admet une borne supérieure.

Démonstration. Admis provisoirement. Pour prouver ce théorème, il faut disposer d'une définition rigoureuse de l'ensemble $\mathbb{R}$. Voir le cours d'analyse de second semestre. □

Il existe des ensembles ordonnés ne possédant pas la propriété de la borne supérieure, c'est-à-dire possédant des parties non-vides, majorées, et sans borne supérieure. C'est le cas de $(\mathbb{Q}, \leq)$, si l'on considère la partie $\{x \in \mathbb{Q} \mid x^2 \leq 2\}$: il n'existe pas de borne supérieure de cette partie dans $\mathbb{Q}$.

6.2.5 Ordre produit et ordre lexicographique

6.2.25 Proposition et Définition. Soient $(E \leq_E)$ et $(F, \leq_F)$ des ensembles ordonnés. L'*ordre produit* sur $E \times F$ est défini par :

$$(x, y) \leq_{E\times F} (x', y') \iff \left(x \leq_E x' \text{ et } y \leq_F y'\right).$$

Démonstration. Il s'agit de prouver que la relation binaire définie est bien une relation d'ordre donc réflexive, antisymétrique et transitive. Exercice. □

Attention, même si $\leq_E$ et $\leq_F$ sont totales, l'ordre produit n'est pas forcément un ordre total. Par exemple, pour $E = F = \mathbb{R}$ et l'ordre usuel sur $\mathbb{R}$ qui est bien total, on remarque que l'ordre produit $\leq_{\mathbb{R}\times\mathbb{R}}$ sur $\mathbb{R} \times \mathbb{R}$ n'est pas total car $(1,2)$ et $(2,1)$ ne sont pas comparables.

6.2.26 Proposition et Définition. Soient $(E \leq_E)$ et $F, \leq_F)$ des ensembles **totalement** ordonnés. L'ordre lexicographique sur $E \times F$ est défini par :

$$(x, y) \leq_{E\times F} (x', y') \iff \left(x <_E x' \text{ ou } (x = x' \text{ et } y \leq_F y')\right).$$

C'est un ordre total.

Démonstration. La propriété de relation d'ordre est laissée en exercice. Prouvons que l'ordre est total.

Soient en effet (x, y) et (x', y') distincts. Si $x \neq x'$, alors comme $\leq_E$ est un ordre total, on a forcément $x <_E x'$ ou bien $x' <_E x$. Si $x = x'$, alors on a forcément $y \neq y'$ et comme $\leq_F$ est un ordre total, on a forcément $y <_F y'$ ou bien $y' <_F y$.

En conclusion, on a bien soit $(x, y) \leq_{E\times F} (x', y')$, soit $(x', y') \leq_{E\times F} (x, y)$. □

6.2.27 Exemple. Avec l'ordre usuel sur l'alphabet, l'ordre lexicographique sur les mots est l'ordre dans lequel les mots sont classés dans un dictionnaire.

6.3 Relations d'équivalence

6.3.1 Définitions

6.3.1 Définition (Relation d'équivalence)**.** Une relation binaire $\mathscr{R}$ sur un ensemble E est une *relation d'équivalence* ssi elle est :

1. réflexive (rappel : $\forall x \in E, x\mathscr{R}x$) ;
2. transitive (rappel : $\forall x, y, z \in E, x\mathscr{R}y$ et $y\mathscr{R}z \implies x\mathscr{R}z$) ;
3. symétrique (rappel : $\forall x, y \in E, x\mathscr{R}y \implies yRx$).

6.3.2 Exemples. a) Les relations $=$, $//$ (parallélisme), sont des relations d'équivalence.

b) La relation $\perp$ (perpendiculaire) n'est **pas** une relation d'équivalence car elle n'est pas réflexive, ni transitive.

c) Tout ensemble possède la relation d'équivalence triviale : celle où tous les éléments sont équivalents.

d) Sur $\mathbb{R}$, la relation $x\mathscr{R}y \iff (x = y \text{ ou } x = -y)$ est une relation d'équivalence.

e) L'ensemble vide possède une seule relation d'équivalence, la relation vide (la seule fonction de $\varnothing \times \varnothing$ dans $\{\text{vrai}, \ \text{faux}\}$ à savoir la fonction vide : on vérifie qu'elle définit bien une relation d'équivalence).

f) Un singleton, c'est-à-dire un ensemble contenant un unique élément, possède une seule relation d'équivalence (celle où l'unique élément est relié à lui-même).

g) Un ensemble $\{a, b\}$ à deux éléments possède deux relations d'équivalence distinctes : la première est l'*égalité*, la seconde est la *relation d'équivalence triviale*, celle où a et b sont équivalents.

h) Un ensemble à trois éléments possède cinq relations d'équivalence (exercice).

6.3.3 Proposition (Relation donnée par les fibres d'une application)**.** Si $f : E \to F$ est une application, alors la relation

$$x\mathscr{R}y \iff (x \text{ et } y \text{ sont dans la même fibre de } f)$$

est une relation d'équivalence sur E.

(Rappelons que par définition de ce que sont les fibres d'une application, on peut reformuler la définition de cette relation en : $x\mathscr{R}y \iff f(x) = f(y)$.)

Démonstration. Soit $x \in E$. Alors on a bien $f(x) = f(x)$ donc $x\mathscr{R}x$, donc $\mathscr{R}$ est réflexive. Si $x, y \in E$, on a bien $x\mathscr{R}y \iff f(x) = f(y) \iff f(y) = f(x) \iff y$§ donc $\mathscr{R}$ est symétrique. Et enfin, Si $x, y, z \in E$ et que $x\mathscr{R}y$ et $y\mathscr{R}z$, alors $f(x) = f(y)$ et $f(y) = f(z)$, donc $f(x) = f(z)$ et donc $x\mathscr{R}z$, donc $\mathscr{R}$ est transitive. Ceci montre que $\mathscr{R}$ est bien une relation d'équivalence.

On verra dans la dernière section que toutes les relations d'équivalence sont de ce type, pour une application f bien choisie : la *surjection canonique sur le quotient.* □

6.3.4 Exemple. La proposition précédente implique que les relations suivantes sont des relations d'équivalence :

1. Sur $\mathbb{R}$, la relation définie par $x\mathscr{R}y \iff \sin(x) = \sin(y)$;
2. Sur $\mathbb{C}$, la relation définie par $z\mathscr{R}z' \iff |z| = |z'|$.
3. Sur $\mathbb{R}$, la relation définie par $x\mathscr{R}y \iff xe^y = ye^x$. (Dans ce cas, la fonction est $f : \mathbb{R} \to \mathbb{R}, t \mapsto te^{-t}$.)

D'autres exemples importants de relations d'équivalence sont les congruences. Commençons par rappeler les définitions.

6.3.5 Proposition et Définition. Soit $a \in \mathbb{R}^*$ et $x, y \in \mathbb{R}$. On a :

$$\frac{x-y}{a} \in \mathbb{Z} \iff x - y \in a\mathbb{Z} \iff (\exists k \in \mathbb{Z} \mid x = y + ka).$$

Si ces conditions équivalentes sont vérifiées, on dit que x et y sont *congrus modulo a* et on note

$$x \equiv y \quad [a].$$

La relation de congruence modulo a entre deux réels x et y est une relation d'équivalence.

Démonstration. Exercice. □

De toutes ces formulations, la plus efficace pour rédiger des preuves est en général la première.

Les relations de congruence les plus courantes sont celles modulo des entiers, ou bien modulo π ou 2π etc.

6.3.6 Exemples.
a) $1 \equiv 5\,[2]$, car $1 - 5 = -4$ est un multiple de 2.
b) $4 \equiv -9\sqrt{3} + 4\,[\sqrt{3}]$, car $4 - (-9\sqrt{3} + 4) = 9\sqrt{3}$ est un multiple de $\sqrt{3}$.
c) $\pi/3 \equiv 7\pi/3\,[2\pi]$, car $\pi/3 - 13\pi/3 = -12\pi/3 = -4\pi$ est un multiple de 2π.

Les congruences se comportent relativement bien par rapport aux opération algébriques, comme le montre la proposition suivante (avec un bémol pour la multiplication, voir l'énoncé et la remarque qui suit).

6.3.7 Proposition. Soit $a \neq 0$ et $b \neq 0$ des réels non nuls, et x, y, x', y' des réels tels que $x \equiv y\,[a]$ et $x' \equiv y'\,[a]$. Alors :

i) $x + x' \equiv y + y'\,[a]$.
ii) $bx \equiv by\,[ba]$.

Démonstration.

i) Si $\dfrac{x-y}{a} \in \mathbb{Z}$ et $\dfrac{x'-y'}{a} \in \mathbb{Z}$, alors $\dfrac{x-y}{a} + \dfrac{x'-y'}{a} \in \mathbb{Z}$.
On a donc $\dfrac{(x+x')-(y+y')}{a} \in \mathbb{Z}$, c'est-à-dire $x + x' \equiv y + y'\,[a]$.

ii) On a :

$$\big(x \equiv y\,[a]\big) \Leftrightarrow \left(\frac{x-y}{a} \in \mathbb{Z}\right) \Leftrightarrow \left(\frac{bx-by}{ba} \in \mathbb{Z}\right) \Leftrightarrow \big(bx \equiv by\,[ba]\big).$$

□

6.3.8 Remarque. *Attention au second point, multiplier une congruence par b change la base de congruence, qui est également multipliée par b.*

6.3.9 Définition. Si $a \in \mathbb{Z}^*$, la relation de congruence modulo a sur $\mathbb{Z}$ induit une relation d'équivalence sur $\mathbb{Z}$, également appelée la relation de congruence modulo a sur $\mathbb{Z}$, et notée de la même façon.

6.3.2 Classes d'équivalence

6.3.10 Définition (Classe d'équivalence)**.** Soit E un ensemble muni d'une relation d'équivalence $\mathscr{R}$. Soit $x \in E$. On note $\overline{x}$ (ou parfois $Cl(x)$) et on appelle la *classe d'équivalence de x modulo $\mathscr{R}$ (ou : sous $\mathscr{R}$)* l'ensemble de tous les éléments qui sont équivalents à x, c'est-à-dire l'ensemble :

$$\overline{x} = \{y \in E \mid y\mathscr{R}x\}$$

Soit $A \in \mathscr{P}(E)$ une partie de E. On dit que A est une *classe d'équivalence modulo $\mathscr{R}$* si c'est la classe d'équivalence d'un certain élément, c'est-à-dire si : $\exists x \in E,\ A = \overline{x}$.

Attention au type des objets : $x \in E$, mais $\overline{x} \subseteq E$.

6.3.11 Proposition.

1. $\forall x \in E, x \in \overline{x}$ (en particulier une classe d'équivalence n'est jamais vide).
2. $\forall x, y \in E, x\mathscr{R}y \iff \overline{x} = \overline{y}$.
3. $\forall x, y \in E, \overline{x} = \overline{y}$ ou $\overline{x} \cap \overline{y} = \varnothing$. (Deux classes sont égales ou disjointes.)

Démonstration.

1. Découle de la réflexivité.
2. Sens $\Longleftarrow$: Supposons $\overline{x} = \overline{y}$. Comme $y \in \overline{y}$, on a $y \in \overline{x}$, donc $y\mathscr{R}x$.
   Sens $\Longrightarrow$: Soit $z \in \overline{x}$. Alors $z\mathscr{R}x$ et comme $x\mathscr{R}y$, on a $z\mathscr{R}y$ par transitivité, et donc $z \in \overline{y}$. Ceci montre $\overline{x} \subseteq \overline{y}$. Pour montrer l'inclusion réciproque, on a $y\mathscr{R}x$ par symétrie de R puis on termine de la même manière.
3. Soient x et y, et supposons $\overline{x} \cap \overline{y} \neq \varnothing$. Soit $z \in \overline{x} \cap \overline{y}$. Alors $z\mathscr{R}x$ et $z\mathscr{R}y$, donc par symétrie et transitivité, $x\mathscr{R}y$, d'où $\overline{x} = \overline{y}$.

□

6.3.12 Définition (Partie saturée)**.** Soit E un ensemble muni d'une relation d'équivalence $\mathscr{R}$ et soit $A \in \mathscr{P}(E)$. La *saturation* de A relativement à la relation $\mathscr{R}$ est la partie

$$\{y \in E \mid \exists x \in A, y\mathscr{R}x\}$$

On dit qu'une partie est *saturée* (relativement à $\mathscr{R}$), si elle est égale à sa saturation.

6.3.13 Remarque. *La saturation de A est égale à $\bigcup_{x \in A} \overline{x}$. En effet, si $y \in E$, alors*

$$\exists x \in A, y\mathscr{R}x \iff \exists x \in A, y \in \overline{x} \iff y \in \bigcup_{x \in A} \overline{x}$$

6.3.14 Exercice. Montrer qu'une classe d'équivalence est saturée, mais que la réciproque est fausse en général. Montrer que les classes d'équivalence sont exactement les parties saturées minimales pour l'inclusion.

L'outil principal pour manipuler les classes d'équivalence est l'*ensemble quotient*, que l'on définit maintenant.

6.3.15 Définition. L'ensemble des classes d'équivalence est appelé *ensemble quotient de E par $\mathscr{R}$* et est noté $E/\mathscr{R}$.

L'application $p : E \to E/\mathscr{R}, x \mapsto \overline{x}$ qui à un élément de E lui associe sa classe d'équivalence est appelée *application de passage au quotient*, ou *projection canonique sur le quotient*. (Cette application étant surjective, on l'appelle aussi la *surjection canonique sur le quotient*.)

6.3.16 Exemple. Pour l'ensemble E des droites du plan $\mathbb{R}^2$ muni de la relation d'équivalence $//$, les classes d'équivalence sont appelées *directions* : deux droites sont parallèles si et seulement si elles ont la même *direction*. L'ensemble quotient de E par la relation de parallélisme est l'ensemble des directions du plan. On le note $\mathbb{P}^1(\mathbb{R})$ et on l'appelle la droite projective.

6.3.17 Proposition. Soit E un ensemble muni d'une relation d'équivalence $\mathscr{R}$ et $p = E \to E/\mathscr{R}$ la projection sur le quotient. Alors

1. p est surjective.
2. $x\mathscr{R}y \iff p(x) = p(y)$.
3. Les fibres sont exactement les classes d'équivalence modulo la relation $\mathscr{R}$.

Démonstration.

1. Soit A une classe d'équivalence. Par définition, il existe $x \in E$ tel que $A = \overline{x} = p(x)$. Donc p est surjective.
2. On a $x\mathscr{R}y \iff \overline{x} = \overline{y} \iff p(x) = p(y)$.
3. C'est une relation du deuxième point, puisque par définition de la fibre d'une application quelconque f, deux éléments x et y sont dans la même fibre si et seulement $f(x) = f(y)$.

$\square$

6.3.3 Partitions et classes d'équivalence

6.3.18 Définition (Partition d'un ensemble)**.** Soit E un ensemble, et $\mathscr{A}$ un ensemble de parties de E, c'est-à-dire $\mathscr{A} \subset \mathscr{P}(E)$. L'ensemble $\mathscr{A}$ est une *partition de E en ensembles non vides*, ou simplement *partition*[2] *de* E, si :

1. les parties sont non vides c'est-à-dire $\forall A \in \mathscr{A},\ A \neq \varnothing$.
2. les parties recouvrent E c'est-à-dire que leur union égale E, autrement dit $\bigcup_{A\in\mathscr{A}} A = E$.
3. Les parties sont deux à deux disjointes, c'est-à-dire $\forall A, A' \in \mathscr{A},\ A \cap A' = \varnothing$.

6.3.19 Exemple (Partition définie par une famille)**.** Soit E un ensemble, et soit $(A_i)_{i\in I}$ une famille de parties de E. Cette famille définit une partition de E si :

1. Les A_i sont toutes non vides.
2. On a $\bigcup_{i\in I} A_i = E$.
3. Les parties A_i sont deux à deux disjointes : $\forall i, j \in I, i \neq j \implies A_i \cap A_j = \varnothing$.

6.3.20 Exemple.

1. L'ensemble vide possède une seule partition, la partition vide qui ne contient aucune partie (car les parties elles, doivent être non-vides).
2. Un ensemble $\{a, b\}$ à deux éléments possède deux partitions : la partition triviale $\{\{a, b\}\}$ et la partition en deux singletons $\{\{a\}, \{b\}\}$.
3. Un ensemble à trois éléments possède cinq partitions distinctes (exercice).
4. Tout ensemble possède la partition $\{\{x\} \mid x \in E\}$ qui est la partition en singletons inclus dans E. (Si E est vide, la partition est vide).
5. Tout ensemble non-vide E possède toujours au moins la partition triviale en une seule partie, l'ensemble lui-même. C'est bien une partition car E est non-vide. Cette partition s'écrit donc $\{E\}$.

2. Notation adoptée dans tout ce cours

6. L'ensemble $\mathbb{Z}$ possède la partition en deux parties suivante : $\{2\mathbb{Z}, 2\mathbb{Z}+1\}$. C'est la partition en nombres pairs et nombres impairs.

6.3.21 Définition (Raffinement d'une partition)**.** Soient $\mathscr{A}$ et $\mathscr{B}$ deux partitions de E. On dit que $\mathscr{A}$ est *plus fine* que $\mathscr{B}$ (ou : qu'elle est un raffinement de $\mathscr{B}$) si les éléments de $\mathscr{B}$ sont des unions d'éléments de $\mathscr{A}$, autrement dit si $\mathscr{A}$ fractionne les éléments de $\mathscr{B}$ en sous-parties.

6.3.22 Exercice. Soient $\mathscr{R}$ et $\mathscr{S}$ deux relations d'équivalence sur E. Montrer que $\mathscr{R}$ est plus fine que $\mathscr{S}$ si et seulement si la partition en classes d'équivalence modulo $\mathscr{R}$ est plus fine que la partition en classe d'équivalence modulo $\mathscr{S}$.

6.3.23 Exercice. Montrer que la relation binaire « être plus fine que » est une relation d'ordre sur l'ensemble de toutes les partitions de E, et que l'ordre n'est en général pas total.

Si E est un ensemble à trois éléments, dire, parmi les cinq partitions possibles, lesquelles sont comparables.

6.3.24 Remarque. *Le plus grand élément de cet ensemble ordonné est la partition la plus fine : c'est la partition en singletons, c'est-à-dire l'ensemble de tous les singletons inclus dans E. Cette partition est plus fine que toute autre. Si E est non-vide, la partition la moins fine est la partition triviale (celle à une seule partie).*

6.3.25 Proposition (Partition en classes d'équivalence)**.** Soit $\mathscr{R}$ une relation d'équivalence sur E. Alors $E/\mathscr{R}$ est une partition de E.

Démonstration.

1. Une classe d'équivalence n'est jamais vide, puisque qu'elle est toujours de la forme $\overline{x}$ et donc contient un élément x.
2. Soit $a \in E$. On a $\overline{a} \in E/\mathscr{R}$, et $a \in \overline{a}$. Donc $a \in \bigcup_{A \in E/\mathscr{R}} A$. On en déduit que $E \subseteq \bigcup_{A \in E/\mathscr{R}} A$.
3. On a déjà montré que deux classes d'équivalence sont soit égales soit disjointes.

□

6.3.26 Remarque (Zérologie)**.** *Le quotient de l'ensemble vide par son unique relation d'équivalence est l'ensemble des classes d'équivalence : comme il n'y a aucune classe d'équivalence, l'ensemble quotient est vide. La projection canonique est l'application $p : \varnothing \to \varnothing$ (dite application vide). Elle est bien surjective...*

Ce résultat admet une « réciproque » :

6.3.27 Proposition. Soit $\{A_i \mid i \in I\}$ une partition d'un ensemble E. Alors la relation

$$x \mathscr{R} y \iff \left(\exists i \in I, x \in A_i \text{ et } y \in A_i\right)$$

est une relation d'équivalence.

Démonstration. Voir TD. □

Ces deux propositions permettent de montrer qu'« une relation d'équivalence sur E est la même chose qu'une partition de E » : attention, à proprement parler ce ne sont pas les mêmes objets (pas le même type), mais le sens précis de cette phrase est qu'il existe une bijection entre d'une part l'ensemble des relations d'équivalence sur E, et d'autre part, l'ensemble des partitions de E.

6.3.28 Corollaire (Application à la combinatoire)**.** Si $\mathscr{R}$ est une relation d'équivalence sur un ensemble fini E, alors $|E| = \sum_{A \in E/\mathscr{R}} |A|$.

Démonstration. On a $E = \bigcup_{A \in E/\mathscr{R}} A$ et l'union est disjointe, donc on obtient le résultat en prenant le cardinal des deux membres. □

6.3.29 Exercice. Soit E un ensemble fini et $f : E \to E$ une involution, c'est-à-dire vérifiant $f \circ f = \mathrm{Id}_E$.

1. Montrer que si f n'a pas de point fixes, alors $|E|$ est pair.
2. Plus généralement, montrer que $|E|$ a la même parité que le nombre de points fixes de f.

6.4 Compléments sur les quotients

6.4.1 Proposition et Définition (Passage au/factorisation par le quotient)**.** Soit $f : E \to F$ une application, $\mathscr{R}$ une relation d'équivalence sur E et $p : E \to E/\mathscr{R}$ la projection canonique sur le quotient. On dit que f *passe (ou descend) au quotient* si elle se factorise à droite par p, autrement dit s'il existe une application $\overline{f} : E/\mathscr{R} \to F$ telle que $f = \overline{f} \circ p$, autrement dit telle que le diagramme suivant commute :

$$\begin{tikzcd} E \arrow[r, "f"] \arrow[d, "p"] & F \\ E/\mathscr{R} \arrow[ur, "\overline{f}"'] & \end{tikzcd}$$

Si une telle application $\overline{f}$ existe, elle est unique.

Démonstration. (de l'unicité). Soit $\alpha \in E/\mathscr{R}$. Comme la projection canonique $p : E \to E/\mathscr{R}$ est surjective, il existe $x \in E$ tel que $\alpha = p(x)$. Or par hypothèse, on a $f = \overline{f} \circ p$, donc $\overline{f}(\alpha) = \overline{f}(p(x)) = f(x)$. Ceci montre que les valeurs de $\overline{f}$ sont déterminées par la fonction f. □

6.4.2 Proposition (Condition nécessaire et suffisante de passage au quotient)**.** Soit $f : E \to F$ une application, et $\mathscr{R}$ une relation d'équivalence sur E.

Alors, f descend au quotient en une application $\overline{f} : E/\mathscr{R} \to F$ si et seulement si elle est constante sur les classes d'équivalence, c'est-à-dire si et seulement si :

$$\forall x, y \in E, x \mathscr{R} y \implies f(x) = f(y).$$