ENSEMBLES, STRUCTURES ALGEBRIQUES

PLAN

I : Vocabulaire

On rassemble ci-dessous un certain nombre de notions, introduites en cours d'année. Une étude exhaustive et directe de l'ensemble du chapitre serait particulièrement indigeste. Il vaut mieux se référer à tel ou tel paragraphe le moment venu.

1– Règles usuelles et notations

i) A, B et C étant les parties d'un ensemble E, on note :

$A \cup B = \{x \mid x \in A \text{ ou } x \in B\}$ (réunion de A et B)

$A \cap B = \{x \mid x \in A \text{ et } x \in B\}$ (intersection de A et B)

$\complement A = \{x \in E \mid x \notin A\}$ (complémentaire de A)

On prouvera en exercices les règles usuelles suivantes :

$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

$\complement (A \cap B) = \complement A \cup \complement B$

$\complement (A \cup B) = \complement A \cap \complement B$

$A \subset B \Leftrightarrow \complement B \subset \complement A$

Ces règles s'appliquent à une réunion ou une intersection quelconque, finie ou non. Si I désigne un ensemble quelconque d'indices, on pose :

$x \in \bigcup_{i \in I} A_i \Leftrightarrow \exists\, i,\ x \in A_i$ (x est dans l'un des A_i. $\exists$ signifie "il existe")

$x \in \bigcap_{i \in I} A_i \Leftrightarrow \forall\, i,\, x \in A_i$ (x est dans tous les A_i. $\forall$ signifie "quel que soit")

EXEMPLE :

$\bigcup_{n \in \mathbb{N}^*} [\frac{1}{n}, 1] =]0,1]$.

$\bigcap_{n \in \mathbb{N}^*} [1 - \frac{1}{n}, 1] = \{1\}$, alors que $\bigcap_{n \in \mathbb{N}^*} [1 - \frac{1}{n}, 1[= \varnothing$

$\varnothing$ désigne l'ensemble vide, ne possédant aucun élément.

ii) On appelle différence de A et B la partie notée A – B (ou A \ B) définie par $\{x \in E \mid x \in A \text{ et } x \notin B\}$. On a $A - B = A \cap \complement B$.

iii) Toutes les parties de E, depuis l'ensemble vide $\varnothing$ jusqu'à E lui–même, forment un ensemble appelé ensemble des parties de E et noté $\mathcal{P}(E)$. Par exemple, si E = {1, 2, 3}, $\mathcal{P}(E)$ = {$\varnothing$, {1}, {2}, {3}, {1, 2}, {1, 3}, {2, 3}, {1, 2, 3}}.
Si E possède n éléments, $\mathcal{P}(E)$ en possède 2^n. En effet, pour définir une partie A de E, il suffit de choisir si chaque élément de E appartient ou non à A, ce qui fait 2^n choix possibles (deux choix possibles par élément : il est dans A ou il n'est pas dans A). On a donc, en notant Card(E) le nombre d'éléments de E :

$$\text{Card}(\mathcal{P}(E)) = 2^{\text{Card}(E)}$$

iv) Etant donné deux ensembles E et F, on note $E \times F$ l'ensemble des couples (x, y), où x est élément de E et y élément de F. Par exemple, l'ensemble des couples de réels est noté $\mathbb{R} \times \mathbb{R}$, ou $\mathbb{R}^2$. L'ensemble des n-uplets ou n-listes $(x_1, x_2, ..., x_n)$ d'éléments de E est noté E^n. L'ensemble des suites $(x_i)_{i \in I}$ d'éléments de E, indicées par un ensemble I fini ou non, est noté E^I.

2- Logique

Une proposition mathématique P est une phrase pouvant prendre les valeurs *vrai* ou *faux*. Par exemple, dans les entiers :

P : $\forall\, n, \exists\, m,\, m = n^2$ est vrai
Q : $\forall\, n, \exists\, m,\, n = m^2$ est faux

Etant donné une proposition, le travail du mathématicien consiste à déterminer si elle est vraie ou fausse. S'il arrive à démontrer qu'elle est vraie, cette proposition est un théorème.

On est amené à regrouper diverses propositions de la façon suivante :

a) <u>la conjonction</u> : "P et Q" est une proposition qui sera vraie si et seulement si les deux propositions P et Q sont simultanément vraies.

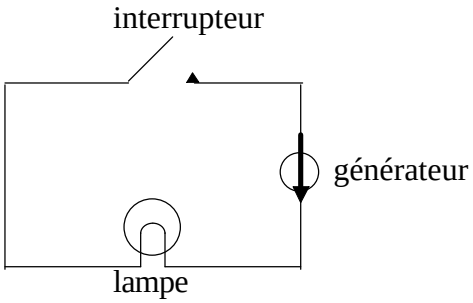
b) <u>la dijonction</u> : "P ou Q" est une proposition qui est vraie si et seulement si au moins une des deux propositions P ou Q est vraie. Les deux peuvent être vraies. le "ou" a un sens inclusif. (Il existe un "ou" exclusif, mais qui n'est pas utilisé de façon usuelle).

c) <u>l'équivalence</u> : "P $\Leftrightarrow$ Q" est vraie si et seulement si P et Q sont simultanément vraies ou simultanément fausses, autrement dit, si P et Q ont même valeurs de vérité. Par exemple :

$$x = e^y \Leftrightarrow x > 0 \text{ et } y = \ln(x)$$

L'équivalence peut s'appliquer à des propositions fausses. Par exemple, si on veut montrer qu'une proposition P est fausse, on peut chercher une proposition Q équivalente à P et montrer que Q est fausse.

d) <u>l'implication logique</u> : "P $\Rightarrow$ Q" est vraie si et seulement si P est fausse ou Q est vraie. Cette notion est la plus difficile à maîtriser, contrairement à ce qu'on peut penser au premier abord. Prenons un exemple pour illustrer ce fait. Considérons un circuit électrique en série constitué d'un générateur de courant, d'un interrupteur et d'une lampe.



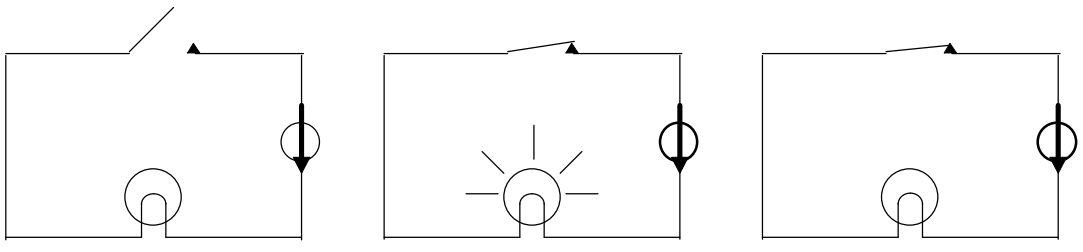
L'interrupteur peut être ouvert ou fermé ; la lampe peut être allumée ou éteinte.

Soit P la proposition : la lampe est allumée.

Soit Q la proposition : l'interrupteur est fermé.

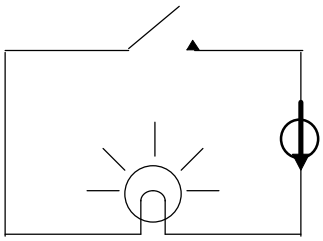
Quelle est la relation d'implication logique entre P et Q ? A-t-on P $\Rightarrow$ Q ? Q $\Rightarrow$ P ? A-t-on l'équivalence P $\Leftrightarrow$ Q ? Précisons qu'on ne recherche pas une relation causale, telle que le conçoit le physicien. Nous cherchons une relation logique permettant de faire une déduction.

Il y a trois situations possibles :



interrupteur ouvert lampe éteinte	interrupteur fermé lampe allumée	interrupteur fermé lampe éteinte
situations les plus courantes		situation inhabituelle mais pas impossible : lampe grillée, voltage trop faible, ...

Une seule situation est impossible :



interrupteur ouvert
lampe allumée.

La seule implication *logique* est la suivante :

P ⇒ Q : si la lampe est allumée, alors l'interrupteur est fermé.

L'implication Q ⇒ P (si l'interrupteur est fermé, alors la lampe est allumée) correspond certes à une explication *causale* de l'allumage de la lampe, mais n'est possible que dans un monde idéal et parfait où les lampes ne tombent jamais en panne, et ne constitue en rien une conséquence logique.

On réfléchira au fait que toutes les phrases qui suivent ont la même signification :

P ⇒ Q	lampe allumée ⇒ interrupteur fermé
non(Q) ⇒ non(P) (contraposée)	interrupteur ouvert ⇒ lampe éteinte
si P alors Q	si la lampe est allumée, alors on en déduit que l'interrupteur est fermé.
P est suffisant pour Q il suffit P pour avoir Q	il suffit que la lampe soit allumée pour conclure que l'interrupteur est fermé.
P seulement si Q	la lampe est allumée seulement si l'interrupteur est fermé.
Q est nécessaire pour P il faut Q pour avoir P	il faut que l'interrupteur soit fermé pour que la lampe soit allumée.
non(P) ou Q	la lampe est éteinte, ou l'interrupteur est fermé

Il résulte de cela que l'implication est vérifiée dans les trois cas suivants (correspondant à nos trois dessins) :

P est vrai et Q est vrai
P est faux et Q est vrai
P est faux et Q est faux

Ainsi, si P est faux, Q est quelconque et il n'y a rien à montrer. La seule chose à montrer est donc bien que, si P est vrai, alors Q est vrai.

L'implication est fausse dans le seul cas suivant :

P est vrai et Q est faux

Il ne peut y avoir d'implication, puisque l'hypothèse est vérifiée, mais pas la conclusion.

La réciproque de l'implication P ⇒ Q est Q ⇒ P. Elle peut être vraie ou fausse, indépendamment de la valeur de vérité de P ⇒ Q. Dans notre exemple, la réciproque est fausse. Toutes les phrases qui suivent sont équivalentes à Q ⇒ P. Elles sont donc fausses, le contre-exemple étant donné par le troisième dessin :

Q ⇒ P	interrupteur fermé ⇒ lampe allumée
non(P) ⇒ non(Q) (contraposée)	lampe éteinte ⇒ interrupteur ouvert
si Q alors P	si l'interrupteur est fermé, alors la lampe est allumée.
Q est suffisant pour P il suffit Q pour avoir P	il suffit que l'interrupteur soit fermé pour conclure que la lampe est allumée.
Q seulement si P	l'interrupteur est fermé seulement si la lampe est allumée.
P est nécessaire pour Q il faut P pour avoir Q	il faut que la lampe soit allumée pour conclure que l'interrupteur est fermé.
non(Q) ou P	l'interrupteur est ouvert, ou la lampe est allumée

Enfin, dire que P ⇒ Q et Q ⇒ P, c'est dire que P ⇔ Q.

e) la négation

La négation d'une proposition P est notée "non(P)". La négation d'une proposition P vraie sera fausse et la négation d'une proposition P fausse sera vraie.

La négation de "P et Q" est "non(P) ou non(Q)". En effet, dire que "P et Q" est fausse, c'est dire qu'une au moins des deux propositions est fausse.

La négation de "P ou Q" est "non(P) et non(Q)". En effet, nier le fait qu'au moins une des deux propositions est vraie, c'est dire qu'elles sont toutes deux fausses.

La négation de "P ⇒ Q" est "P et non(Q)". En effet, nous avons vu que "P ⇒ Q" est synonyme de "non(P) ou Q". La négation est donc bien "P et non(Q)". Dire que l'implication est fausse, c'est dire qu'on a l'hypothèse P, mais pas la conclusion Q.

La négation de "P ⇔ Q" est "(P et non(Q)) ou (Q et non(P))".

La négation de "∀ *x*, P(*x*)" est "∃ *x*, non(P(*x*))". En effet, dire qu'il est faux que P soit vraie pour tout *x*, c'est dire que P est faux pour au moins un *x*.

La négation de "∃ *x*, P(*x*)" est "∀ *x*, non(P(*x*))". En effet, dire qu'il n'existe aucun *x* vérifiant P, c'est dire que tous les *x* vérifient la négation de P.

Il résulte des deux derniers cas que, pour prendre la négation d'une proposition enchaînant les quantificateurs $\forall$ et $\exists$, il suffit de lire la proposition de gauche à droite, de changer les $\forall$ en $\exists$, de changer les $\exists$ en $\forall$ puis de prendre la négation de ce qui reste.
Exemple : la négation de :

$$\forall\, x,\ \forall\, \varepsilon > 0,\ \exists\, \delta > 0,\ \forall\, y,\ |y - x| < \delta \Rightarrow |f(x) - f(y)| < \varepsilon$$

est :

$$\exists\, x,\ \exists\, \varepsilon > 0,\ \forall\, \delta > 0,\ \exists\, y,\ |y - x| < \delta \text{ et } |f(x) - f(y)| \geq \varepsilon$$

(La première proposition si mystérieuse exprime la continuité d'une fonction f en tout point x. La deuxième exprime la non-continuité de f en un point x)

On notera enfin que :

$\forall\, x \in$ A, P(x) est une abréviation pour : $\forall\, x,\ x \in$ A $\Rightarrow$ P(x)

et a donc pour négation :

$\exists\, x,\ x \in$ A et non(P(x)), ce qu'on abrège en : $\exists\, x \in$ A, non(P(x))

De même, la négation de $\exists\, x \in$ A, P(x) est $\forall\, x \in$ A, non(P(x)).

On utilisera au besoin des parenthèses pour lever toute ambiguïté. Par exemple, dans les entiers, les deux propositions suivantes ont des sens différents. La première est vraie, la seconde est fausse.

$$\forall\, n,\ [(\forall\, m,\ mn \text{ pair}) \Rightarrow n \text{ pair}]$$

$$\forall\, n,\ [\forall\, m\ (mn \text{ pair} \Rightarrow n \text{ pair})]$$

En effet, dans la première proposition, n étant donné, on suppose que mn est pair pour tout entier m, en particulier pour $m = 1$. Donc n est pair. Dans la deuxième proposition, n étant donné, on suppose que c'est l'implication mn pair $\Rightarrow$ n pair qui est vraie pour tout m. Or cette implication est fausse pour $m = 2$ et $n = 3$ par exemple. $n = 3$ ne vérifie donc pas la condition demandée.

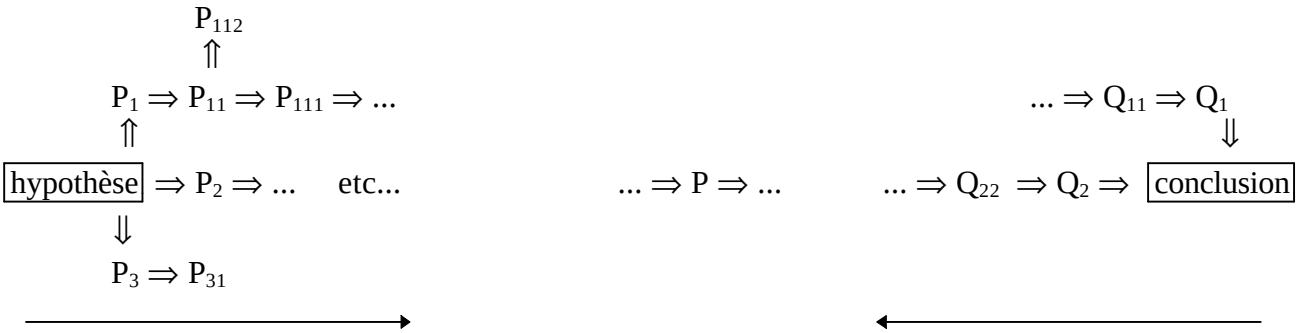
3- Introduction à la démonstration

Lorsqu'un mathématicien, après des heures, des jours, voire des années de labeur, pense qu'une propriété est vraie, il fait une conjecture. Pour être certain que cette propriété soit vraie et pour la faire valider par l'ensemble de la communauté mathématique ou scientifique, il faut une démonstration. La démonstration n'est donc pas la tâche essentielle du travail du mathématicien, mais son achèvement. Dans une moindre mesure, on demande la même chose à l'étudiant scientifique. Ce dernier, apprenti mathématicien, a parfois du mal à mettre en forme une démonstration. Ce paragraphe peut lui donner quelques procédés méthodiques.

La démarche démonstrative repose sur une liste de connaissances appelée à évoluer. Cette liste comprend tous les axiomes et théorèmes connus du démonstrateur, mais peut également évoluer par ajout de propriétés au cours de la démonstration. Le démonstration doit démontrer une proposition, c'est à dire une phrase mathématique que le démonstrateur pense être vraie. Nous avons vu dans le paragraphe précédent qu'une proposition peut être construite à partir de propriétés élémentaires en utilisant itérativement conjonction (et), disjonction (ou), implication ($\Rightarrow$), et négation (non). L'équivalence ($\Leftrightarrow$) quant à elle, n'est que la conjonction de deux implications ($\Rightarrow$ et $\Leftarrow$). A cela, on ajoute les quantificateurs existentiel ($\exists$) et universel ($\forall$).

Il convient d'abord de clairement séparer ce qu'on sait ou suppose vrai (théorèmes, définitions, mais aussi hypothèses diverses, qu'on regroupera sous le terme général de liste des connaissances), de la conclusion à laquelle on veut arriver. Par ailleurs, il convient de savoir qu'une démonstration ne consiste pas forcément à partir de l'hypothèse, puis par une suite de déductions logiques, à arriver à

la conclusion. On peut bien sûr partir de l'hypothèse pour en déduire diverses propriétés en espérant que l'une d'elles finira par être la conclusion cherchée, mais on peut aussi partir de la conclusion pour trouver des propriétés à partir desquelles la conclusion se déduit, en espérant ainsi remonter jusqu'aux hypothèses. On peut également opérer simultanément les deux démarches jusqu'à tomber sur une propriété faisant le lien entre les deux. Ci-dessous, P est une propriété pouvant servir de jonction entre une progression venant de l'hypothèse et une progression venant de la conclusion :



Sens dans lequel s'opère la recherche de nouvelles propriétés qui se déduisent de l'hypothèse

Sens dans lequel s'opère la recherche de nouvelles propriétés d'où découle la conclusion

Il convient également de distinguer ce qu'il faut faire pour **montrer** une conjecture, de ce qu'il faut faire pour **utiliser** une propriété déjà prouvée ou une hypothèse, et faisant donc partie de la liste des connaissances. On donne donc pour chaque connecteur logique (*et*, *ou*, *non*, *implique*) :
❑ d'une part une règle qui permet de **montrer** une propriété possédant ce connecteur, et donc d'ajouter cette propriété à la liste des connaissances (règle dite d'introduction).
❑ d'autre part une règle qui permet d'**utiliser** une propriété possédant ce connecteur et faisant partie de la liste de connaissances, soit pour montrer une autre propriété, soit pour remplacer dans la liste des connaissances la propriété par une ou d'autres propriétés. Une fois utilisée, la propriété en question peut en général être éliminée de la liste de connaissances (règle dite d'élimination), sauf si elle doit être utilisée plusieurs fois.
❑ Enfin, la règle énonçant le principe du raisonnement par l'absurde.

Certaines de ces règles paraîtront triviales. D'autres le sont beaucoup moins. Par ailleurs, plusieurs approches différentes peuvent être possibles pour aboutir à la même conclusion. Nous notons par A, B, C... des propriétés à prouver, et par P, Q, R... des propriétés déjà prouvées donc faisant partie de la liste des connaissances (la classification ci-dessous constitue le fondement de la logique classique. Une telle classification est par exemple utilisée par des logiciels d'assistants de preuves).

(Règles d'introduction) POUR MONTRER...
(i) ...une conjonction A et B : montrer A et montrer B.

(ii) ...une disjonction A ou B : montrer A ou montrer B.

(iii) ...une implication $A \Rightarrow B$: ajouter A comme hypothèse à sa liste de connaissances (autrement dit, supposer A) et montrer B.

(iv) ...une négation non(A) : ajouter A comme hypothèse à sa liste de connaissance et montrer qu'on aboutit à une contradiction. A est alors nécessairement faux. Autrement dit, non(A) est synonyme de $A \Rightarrow$ contradiction.

(v) ... $\exists x$ A(x) : exhiber un élément t bien choisi et montrer A(t).

(vi) ... $\forall x$ A(x) : montrer A(u), u étant un symbole quelconque non encore utilisé par ailleurs.

(Règles d'élimination) POUR UTILISER...
(a) ...une conjonction P et Q : ajouter P à la liste des connaissances et ajouter Q.

(b) ...une disjonction P ou Q : en déduire la validité de R en montrant P $\Rightarrow$ R **et** Q $\Rightarrow$ R (méthode de disjonction des cas). Pour montrer par exemple qu'une suite monotone (i.e. croissante **ou** décroissante) bornée converge, il suffit de montrer qu'une suite croissante bornée converge **et** qu'une suite décroissante bornée converge.

(c) ...une implication P $\Rightarrow$ Q : ajouter Q à la liste des connaissances à condition que P y soit déjà.

(d) ...une négation non(P) : déduire une contradiction si P fait également partie de la liste des connaissances. Autrement dit, une contradiction est un synonyme de (P et non(P)).

(e) ... $\exists x$ P(x), ajouter P(u) à la liste des connaissances, u étant un symbole quelconque non déjà utilisé par ailleurs. u désigne ici l'élément particulier qui vérifie la propriété P. On prendra garde à ne pas choisir un u intervenant dans une autre propriété.

(f) ... $\forall x$ P(x), ajouter P(t) à la liste des connaissances, t étant un objet choisi à notre gré.

LE RAISONNEMENT PAR L'ABSURDE
En logique classique, on ajoute la règle suivante, dite de raisonnement par l'absurde.
Pour montrer P, ajouter non(P) à la liste des connaissances et montrer une contradiction. Autrement dit, si non(P) $\Rightarrow$ contradiction, on a prouvé P. Cette règle s'appelle également simplification de la double négation, puisque non(P) $\Rightarrow$ contradiction est synonyme de non(non(P)).

Cette règle est utilisée implicitement dans :
❑ Le tiers exclu : pour toute propriété P, on a (P ou non(P)). En effet, dans le cas contraire, on aurait non (P ou non(P)), c'est-à-dire non(P) et non(non P) ce qui est contradictoire. Donc on a bien P ou non(P).

❑ La contraposition : si (non(P) $\Rightarrow$ non(Q)) alors (Q $\Rightarrow$ P). En effet, supposons que l'on ait non(P) $\Rightarrow$ non(Q) et que Q soit vrai. Il s'agit de montrer que P est vrai. Raisonnons par l'absurde et supposons non(P). On a alors non(Q) d'après la première implication. Ayant Q et non(Q), on aboutit à une contradiction. Donc non(P) est absurde et P est vrai.

En mathématiques classiques, **toutes** les démonstrations mathématiques utilisent ces principes, et uniquement ces principes.

EXEMPLE 1 :
Montrer que : $\forall\, n \in \mathbb{N}$, [$n^2$ impair $\Rightarrow$ n impair]
D'après (vi), nous allons montrer que n^2 impair $\Rightarrow$ n impair, n étant un nombre quelconque. D'après (iii), nous allons supposer que n^2 est impair et montrer que n est impair.

On sait ou on suppose que :	On veut montrer que :
n^2 est impair	n est impair

Raisonnons par l'absurde. Nous allons supposer n non impair (i.e. n pair) et arriver à une contradiction. Si on y parvient, on aura prouvé que n est effectivement impair.

On sait ou on suppose que :	On veut montrer :
n^2 est impair n pair	une contradiction

On utilise la définition de la parité :

n pair $\Leftrightarrow \exists\, p \in \mathbb{N},\ n = 2p$ (définition de la propriété "être pair")

On sait ou on suppose que :	On veut montrer :
n^2 est impair $\exists\, p \in \mathbb{N},\ n = 2p$	une contradiction

On a $n = 2p$ (utilisation implicite de (e)) donc $n^2 = 4p^2$ qui est pair et non impair. On a bien obtenu une contradiction. CQFD.

On notera que la démonstration utilise le fait que n est pair. La plupart des étudiants partent de $n^2 = 2p + 1$, démarche généralement vouée à l'échec.

EXEMPLE 2 :
Toute suite réelle croissante majorée converge (il convient de lire cet exemple après avoir acquis les connaissances sur les réels et la notion de borne supérieure. cf le chapitre *Suites* dans le fichier SUITES.PDF). Bien entendu, dans le chapitre *Suites*, nous allons plus vite au but, mais on pourra se rendre compte que la démonstration est basée sur une application des principes (i) à (vi) et (a) à (f), ce que nous développons ci-dessous de façon outrageusement détaillée. Insistons sur le fait que le mathématicien ne développe jamais explicitement dans ses moindres détails une telle démarche. Ce développement a seulement pour but de mettre à jour les utilisations souvent implicites des dits principes.

Il s'agit de montrer que :

$\forall\, (u_n)$, [(u_n) est croissante et (u_n) est majorée $\Rightarrow$ (u_n) converge]

D'après (vi) et (iii), on a :

On sait ou on suppose que :	On veut montrer que :
(u_n) est croissante et (u_n) est majorée	(u_n) converge

On traduit chaque propriété (croissance, majoration, convergence) :

On sait ou on suppose que :	On veut montrer que :
$\forall n\ u_n \leq u_{n+1}$ $\exists M\ \forall n\ u_n \leq M$	$\exists l\ \forall \varepsilon > 0\ \exists N\ \forall n \geq N,\ l - \varepsilon < u_n < l + \varepsilon$

Nous avons un théorème d'existence de la borne supérieure (cf le chapitre *Suites* dans le fichier SUITES.PDF) qui dit : $\exists M\ \forall n\ u_n \leq M \Rightarrow \text{Sup}\ \{u_n,\ n \in \mathbb{N}\}$ existe. L'application de la règle (c) donne donc, en abrégeant la liste des connaissances (ce que nous ferons plusieurs fois pour alléger) :

On sait ou on suppose que :	On veut montrer que :
$\forall n\ u_n \leq u_{n+1}$ $\text{Sup}(u_n)$ existe	$\exists l\ \forall \varepsilon > 0\ \exists N\ \forall n \geq N,\ l - \varepsilon < u_n < l + \varepsilon$

Nous allons prendre $l = \text{Sup}\ \{u_n,\ n \in \mathbb{N}\}$ (application de la règle (v)). C'est évidemment le travail du mathématicien de faire le bon choix de l et il n'y a hélas aucune méthode automatique pour cela ☹). On peut simplement dire qu'on cherche un réel particulier l et que le seul dont on ait connaissance, à part les termes de la suite, c'est la borne supérieure. D'où l'idée de prendre $l = \text{Sup}(u_n)$.

On sait ou on suppose que :	On veut montrer que :
$\forall n\ u_n \leq u_{n+1}$ $l = \text{Sup}(u_n)$	$\forall \varepsilon > 0\ \exists N\ \forall n \geq N,\ l - \varepsilon < u_n < l + \varepsilon$

D'après la règle (vi), nous prenons $\varepsilon > 0$ quelconque. Comme la formulation $\forall\ \varepsilon > 0$ ... est une abréviation de $\forall\ \varepsilon,\ \varepsilon > 0 \Rightarrow$ ..., la règle (iii) ajoute la condition $\varepsilon > 0$ aux hypothèses. Nous remplaçons également $l = \text{Sup}(u_n)$ par la définition de la borne supérieure :

On sait ou on suppose que :	On veut montrer que :
$\forall n\ u_n \leq u_{n+1}$ $\forall n\ u_n \leq l$ $\forall \alpha > 0\ \exists m\ l - \alpha < u_m$ $\varepsilon > 0$	$\exists N\ \forall n \geq N,\ l - \varepsilon < u_n < l + \varepsilon$

Le α pouvant être choisi à notre gré selon la règle (f), nous prendrons $\alpha = \varepsilon$. Là aussi, le choix du α relève de l'intuition du mathématicien ...☹

On sait ou on suppose que :	On veut montrer que :
$\forall n\ u_n \leq u_{n+1}$ $\forall n\ u_n \leq l$ $\exists m\ l - \varepsilon < u_m$ $\varepsilon > 0$	$\exists N\ \forall n \geq N,\ l - \varepsilon < u_n < l + \varepsilon$

Nous appliquons la règle (v) en choisissant $N = m$ (le m de la liste des connaissances). ☹

On sait ou on suppose que :	On veut montrer que :
$\forall n\ u_n \leq u_{n+1}$ $\forall n\ u_n \leq l$ $\exists m\ l - \varepsilon < u_m$ $\varepsilon > 0$	$\forall n \geq m,\ l - \varepsilon < u_n < l + \varepsilon$

Nous prenons n quelconque supérieur ou égal à m en application de la règle (vi). Comme $\forall\ n \geq m$ ... est une abréviation de $\forall\ n,\ n \geq m \Rightarrow$ ..., d'après (iii), on ajoute $n \geq m$ à nos hypothèses, et plutôt que n dont le symbole est déjà utilisé dans la liste des connaissances, nous noterons cet entier p :

On sait ou on suppose que :	On veut montrer que :
$\forall n\ u_n \leq u_{n+1}$ $\forall n\ u_n \leq l$ $\exists m\ l - \varepsilon < u_m$ $\varepsilon > 0$ $p \geq m$	$l - \varepsilon < u_p < l + \varepsilon$

Dans la deuxième propriété de la liste des connaissances, nous choisissons (règle (f)) $n = p$.

On sait ou on suppose que :	On veut montrer que :
$\forall n\ u_n \leq u_{n+1}$ $u_p \leq l$ $\exists m\ l - \varepsilon < u_m$ $\varepsilon > 0$ $p \geq m$	$l - \varepsilon < u_p < l + \varepsilon$

Nous appliquons la règle (e) à la troisième propriété de la liste des connaissances. m désigne un élément sur lequel nous n'avons aucune possibilité de choix.

On sait ou on suppose que :	On veut montrer que :
$\forall n\ u_n \leq u_{n+1}$ $u_p \leq l$ $l - \varepsilon < u_m$ $\varepsilon > 0$ $p \geq m$	$l - \varepsilon < u_p < l + \varepsilon$

Enfin, dans la première propriété de la liste des connaissances, nous choisissons (règle (f) itérée plusieurs fois) $n = m$, $n = m+1$, ... $n = p-1$, $n = p$.

On sait ou on suppose que :	On veut montrer que :
$u_m \leq u_{m+1} \leq \ldots \leq u_{p-1} \leq u_p$ $u_p \leq l$ $l - \varepsilon < u_m$ $\varepsilon > 0$ $p \geq m$	$l - \varepsilon < u_p < l + \varepsilon$

Ce qu'on peut encore écrire :

On sait ou on suppose que :	On veut montrer que :
$l - \varepsilon < u_m \leq u_{m+1} \leq \ldots \leq u_{p-1} \leq u_p \leq l$ $\varepsilon > 0$	$l - \varepsilon < u_p < l + \varepsilon$

Ou encore plus brièvement :

On sait ou on suppose que :	On veut montrer que :
$l - \varepsilon < u_p \leq l$ $\varepsilon > 0$	$l - \varepsilon < u_p < l + \varepsilon$

La conclusion à montrer est bien vraie puisque $l \leq l + \varepsilon$.

On aura remarqué que le choix de tel ou tel élément x au gré du démonstrateur se manifeste :

ou bien dans la liste des connaissances sur une propriété du type $\forall x\ P(x)$ (règle (f))

ou bien dans la conclusion à montrer sur une propriété du type $\exists x\ A(x)$ (règle (v))

En effet, dans le premier cas, la propriété $P(x)$ étant vraie pour tout x, on est libre de l'appliquer au x que l'on veut.

Dans le second cas, puisqu'on doit montrer la propriété $A(x)$ pour un certain x, on peut choisir le x qui nous paraît répondre à la question (c'est là la partie la moins évidente), et, si notre choix a été judicieux, parvenir à prouver $A(x)$ pour ce x bien choisi.

A l'inverse, le démonstrateur n'a aucune liberté de choix sur l'élément *x* qui intervient :

dans la liste des connaissances sous la forme $\exists x\ P(x)$ (règle (e))

dans la conclusion à montrer sous la forme $\forall x\ A(x)$ (règle (vi))

Dans le premier cas, on suppose l'existence d'un x vérifiant $P(x)$ mais ce x nous est imposé.
Dans le second cas, on ne peut se contenter de montrer $A(x)$ pour un x de notre choix puisqu'il s'agit de montrer $A(x)$ pour tous les x.

La compréhension de ce mécanisme est essentielle pour mener à bien des démonstrations correctes et pour savoir sur quels éléments on peut faire un choix.

4– Fonctions, injections, surjections

a) Fonction :

Une fonction f (ou application) d'un ensemble E dans un ensemble F établit une relation entre les éléments de E et ceux de F. Tout élément x de E est associé à un unique élément de F, noté $f(x)$. $f(x)$ est l'image de x par f. Si y est dans F et s'il existe x dans E tel que $y = f(x)$, x est un antécédent de y par f. Certains éléments y de F peuvent n'être l'image d'aucun élément de E, et certains éléments y de F peuvent être l'image de plusieurs éléments de E, d'où les définitions d'injection et de surjection dans la suite du paragraphe.

La partie G de $E \times F$ égale à $\{(x, y), y = f(x)\}$ s'appelle graphe de f. On note $\mathcal{F}(E, F)$ (ou parfois F^E) l'ensemble des applications de E dans F.

Si on dispose d'une application f de E dans F et d'une application g de F dans H, on peut définir la composée $g \circ f$ de E dans H par : $(g \circ f)(x) = g(f(x))$.

L'application identique Id_E est l'application de E dans E définie par $Id_E(x) = x$.

Si A est inclus dans E, la restriction de f à A est l'application $f|_A$ de A dans F définie par $f|_A(x) = f(x)$. La seule différence entre f et $f|_A$ est l'ensemble de définition des applications : f est définie sur E alors que $f|_A$ est définie sur A.

Inversement, si E est inclus dans H et s'il existe une application g de H dans F telle que $g|_E = f$, on dit que g est un prolongement de f à H.

b) Injection :

Une fonction f d'un ensemble E dans un ensemble F est dite *injective* (one to one en anglais) si :

$$\forall x \in E, \forall x' \in E, x \neq x' \Rightarrow f(x) \neq f(x')$$

ou encore (ce qui est plus couramment utilisé) :

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

Si f est injective, l'équation $f(x) = y$ a au plus une solution, quel que soit y.

Si f et g sont injectives, alors $g \circ f$ l'est. En effet :

$(g \circ f)(x) = (g \circ f)(x')$
$\Rightarrow$ $(g(f(x)) = g(f(x'))$ (définition de $g \circ f$)
$\Rightarrow$ $f(x) = f(x')$ (injectivité de g)
$\Rightarrow$ $x = x'$ (injectivité de f)

c) Surjection :
Une fonction est dite *surjective* (onto) si :

$$\forall\, y \in \mathrm{F}, \exists\, x \in \mathrm{E},\ y = f(x)$$

Si f est surjective, l'équation $f(x) = y$ a au moins une solution, quel que soit y.

Si f et g sont surjectives, alors $g \circ f$ l'est. En effet :

$\forall\, z, \exists\, y,\ z = g(y)$ (surjectivité de g)
$\Rightarrow$ $\forall\, z, \exists\, y, \exists\, x,\ z = g(y)$ et $y = f(x)$ (surjectivité de f)
$\Rightarrow$ $\forall\, z, \exists\, x,\ z = g(f(x))$
$\Rightarrow$ $\forall\, z, \exists\, x,\ z = (g \circ f)(x)$ (définition de $g \circ f$)

d) bijection :
f surjective et injective est dite *bijective*.
Si f est bijective, l'équation $f(x) = y$ a exactement une solution x, quel que soit y. On peut alors définir la fonction réciproque f^{-1} de f par l'équivalence :

$$y = f(x) \Leftrightarrow x = f^{-1}(y).$$

On a alors $f(f^{-1}(y)) = f(x) = y$ ce qu'on écrit encore $f \circ f^{-1} = \mathrm{Id}_F$ et $f^{-1}(f(x)) = f^{-1}(y) = x$ ce qui s'écrit $f^{-1} \circ f = \mathrm{Id}_E$.

Si f et g sont bijectives, alors $g \circ f$ l'est et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. En effet :

$z = (g \circ f)(x)$
$\Rightarrow$ $z = g(f(x))$
$\Rightarrow$ $g^{-1}(z) = f(x)$
$\Rightarrow$ $f^{-1}(g^{-1}(z)) = x$
$\Rightarrow$ $x = (f^{-1} \circ g^{-1})(z)$

S'il existe une application g de F dans E telle que $f \circ g = \mathrm{Id}_F$ et $g \circ f = \mathrm{Id}_E$, alors f et g sont bijectives et réciproques l'une de l'autre. En effet, la seule solution x possible à l'équation $y = f(x)$ est $x = g(y)$. C'est bien une solution puisque $f(g(y)) = y$. Il n'y en a pas d'autre puisque :

$y = f(x) \Rightarrow g(y) = g(f(x)) = x$

On notera que l'on a besoin des deux relations $f \circ g = \mathrm{Id}_F$ et $g \circ f = \mathrm{Id}_E$ pour prouver l'existence et l'unicité. La première relation $f \circ g = \mathrm{Id}_F$ montre l'existence de la solution et prouve que f est surjective. La seconde relation $g \circ f = \mathrm{Id}_E$ montre l'unicité de la solution et prouve que f est injective.

EXEMPLE 1 : L'application $x \to \sin(x)$ est :

injective si l'ensemble de départ est $[-\frac{\pi}{2}, \frac{\pi}{2}]$
surjective si l'ensemble d'arrivée est $[-1,1]$

EXEMPLE 2 :
Pour n entier naturel, notons $[\![1, n]\!]$ l'ensemble des entiers de 1 à n. Alors il existe une bijection entre $[\![1, n]\!]$ et $[\![1, p]\!]$ si et seulement si $n = p$.

EXEMPLE 3 : il n'existe aucune bijection entre E et $\mathcal{P}(\mathrm{E})$, que E soit fini ou non. C'est clair si E est fini avec n éléments, puisque E et $\mathcal{P}(\mathrm{E})$ n'ont pas le même nombre d'éléments (n et 2^n respectivement), plus délicat à montrer si E est infini. Pour cela, nous allons montrer que, quelles que soient les fonctions f de E dans $\mathcal{P}(\mathrm{E})$ et g de $\mathcal{P}(\mathrm{E})$ dans E, on a $f \circ g \neq \mathrm{Id}_{\mathcal{P}(\mathrm{E})}$. Il est par contre tout à

fait possible d'avoir $g \circ f = \mathrm{Id}_E$. Il suffit pour cela de prendre $f(x) = \{x\}$ et $g(\mathrm{A})$ = un élément donné de A pour A non vide.

Pour montrer que :

(1) $f \circ g \neq \mathrm{Id}_{\mathcal{P}(E)}$

nous allons modifier cette proposition jusqu'à obtenir une affirmation manifestement vraie dont (1) découle. La difficulté essentielle est de bien comprendre qu'un *élément* de E a pour image par *f* une *partie* de E, et qu'une *partie* de E a pour image par *g* un *élément* de E. On peut déjà écrire que (1) équivaut à :

(2) $\exists\ \mathrm{A} \subset \mathrm{E},\ f \circ g(\mathrm{A}) \neq \mathrm{A}$

On écrit ensuite le fait que les deux parties A et $f \circ g(\mathrm{A})$ sont différentes, à savoir l'appartenance à la première partie ne saurait être équivalente à l'appartenance à l'autre partie :

(3) $\exists\ \mathrm{A} \subset \mathrm{E},\ \exists\ x,$ non $[x \in \mathrm{A} \Leftrightarrow x \in f \circ g(\mathrm{A})]$

(On aurait pu écrire aussi qu'il existe un *x* dans la première partie et pas dans la seconde, à moins que *x* soit dans la seconde et pas dans la première, ce qui est strictement identique à la formulation ci-dessus).

Comment trouver ce *x* à partir de A ? Nous ne connaissons qu'un seul élément de E en liaison avec A, c'est $x = g(\mathrm{A})$. Pour que (3) soit vérifié, il suffit donc d'avoir :

(4) $\exists\ \mathrm{A} \subset \mathrm{E},$ non $[g(\mathrm{A}) \in \mathrm{A} \Leftrightarrow g(\mathrm{A}) \in f \circ g(\mathrm{A})]$

La précédente proposition sera elle-même vérifiée si :

(5) $\exists\ \mathrm{A} \subset \mathrm{E},\ \forall\ x,$ non $[x \in \mathrm{A} \Leftrightarrow x \in f(x)]$

Il suffit en effet d'appliquer (5) au *x* particulier égal à $g(\mathrm{A})$ pour retrouver (4).

On peut aussi écrire (5) sous la forme équivalente :

(6) $\exists\ \mathrm{A} \subset \mathrm{E},\ \forall\ x,\ [x \in \mathrm{A} \Leftrightarrow x \notin f(x)]$

Or cette dernière proposition est vraie si l'on choisit précisément $\mathrm{A} = \{x \mid x \notin f(x)\}$. On a alors la chaîne de déduction suivante :

(6) vrai $\Leftrightarrow$ (5) $\Rightarrow$ (4) $\Rightarrow$ (3) $\Leftrightarrow$ (2) $\Leftrightarrow$ (1).

Une variante ainsi que des conséquences de cet exemple sont présentées en annexe.

e) image directe d'une partie :

Soit A une partie de E. *L'image de A par f* est l'ensemble noté $f(\mathrm{A})$ défini par :

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

Autrement dit :

$$y \in f(\mathrm{A}) \Leftrightarrow \exists\ x \in \mathrm{A},\ y = f(x)$$

$f(\mathrm{A})$ est l'ensemble des images des éléments de A.

EXEMPLE : si *f* est la fonction sinus, alors $f([0,\frac{3\pi}{4}]) = [0,1]$

f) image réciproque :

Soit B une partie de F. *L'image réciproque de B par f* est l'ensemble noté $f^{-1}(\mathrm{B})$ défini par :

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

Autrement dit :

$$x \in f^{-1}(B) \Leftrightarrow f(x) \in B$$

$f^{-1}(B)$ est l'ensemble des antécédents des éléments de B.

EXEMPLE : si f est la fonction sinus, $f^{-1}([0,1]) = \bigcup_{n\in\mathbb{Z}} [2n\pi, 2n\pi + \pi]$

On prendra garde que cette partie est définie même si f n'est pas bijective, que $f^{-1}(\{y\})$ est l'ensemble (éventuellement vide ou constitué de plus d'un élément) des antécédents de y, et que la notation $f^{-1}(y)$, elle, n'est tolérée que si f est bijective ; on désigne ainsi l'antécédent unique de y.

EXEMPLE :
Toujours avec $f = \sin$, $f^{-1}(\{0\}) = \{n\pi, n \in \mathbb{Z}\} = \pi\mathbb{Z}$.
$f^{-1}(0)$ n'existe pas.

EXERCICES :
i) Comparer $f(A \cap B)$ et $f(A) \cap f(B)$
On prouve que : $\forall A, \forall B, f(A \cap B) \subset f(A) \cap f(B)$

On pourra chercher à quelle condition on a :
$$\forall A, \forall B, f(A \cap B) = f(A) \cap f(B)$$
On trouvera qu'une condition nécessaire et suffisante est f injective.

ii) Comparer $f(A \cup B)$ et $f(A) \cup f(B)$
Il y a égalité

iii) Comparer $f(\complement A)$ et $\complement f(A)$
En général, ils sont différents. On prouve que :
$$f \text{ injective} \Leftrightarrow \forall A, f(\complement A) \subset \complement f(A)$$
$$f \text{ surjective} \Leftrightarrow \forall A, \complement f(A) \subset f(\complement A)$$

iv) Procéder de même pour les images réciproques.
Il y a toujours égalité.

v) Comparer B et $f(f^{-1}(B))$.
On a toujours $f(f^{-1}(B)) \subset B$
Une condition nécessaire et suffisante pour que :
$$\forall B, f(f^{-1}(B)) = B$$
est que f soit surjective

vi) Comparer A et $f^{-1}(f(A))$.
On a toujours $A \subset f^{-1}(f(A))$.
Une condition nécessaire et suffisante pour que :
$$\forall A, A = f^{-1}(f(A))$$
est que f soit injective

vii) Soit $f : E \to F$
$g : F \to G$

$h : G \to H$

Montrer que : $g \circ f$ surjectif $\Rightarrow g$ surjectif

$g \circ f$ injectif $\Rightarrow f$ injectif

$g \circ f$ et $h \circ g$ bijectifs $\Rightarrow$ f, g et h bijectifs

viii) Donnons un exemple d'application f et g telles que f et g soient non bijectives, mais où $g \circ f$ l'est.

$\mathbb{N} \to \mathbb{N}$

$f : n \to n+1$

$g : 0 \to 0$

$n \to n-1$ pour n non nul.

5– Ensembles finis

Nous énonçons ci-dessous un certain nombre de propriétés sur les ensembles finis, sans chercher à les justifier outre mesure.

E est un ensemble fini s'il existe une bijection de $[\![1, n]\!]$ sur E, où l'on note $[\![1, n]\!]$ l'ensemble des entiers de 1 à n. n est le cardinal de E, noté Card(E).

Une partie de $\mathbb{N}$ est finie si et seulement si elle est majorée. Si n est le cardinal de cette partie, il existe une bijection strictement croissante et une seule entre cette partie et $[\![1, n]\!]$. 1 est l'image de l'élément le plus petit, 2 l'image du suivant, etc...

$\text{Card}(\varnothing) = 0$

Si E' est inclus dans E, alors $\text{Card}(E') \leq \text{Card}(E)$, avec égalité si et seulement si E' = E.

Si f est une application de E dans F et si Card(E) = Card(F) (fini), alors, il y a équivalence entre injective, surjective et bijective. En effet, compte tenu de l'égalité entre Card(F) et Card(E), on a :

f injective $\Rightarrow \text{Card}(E) = \text{Card}(f(E)) \Rightarrow \text{Card}(F) = \text{Card}(f(E))$

or f(E) est inclus dans F, donc f(E) = F puisqu'ils ont même nombre d'éléments, et f est surjective.

De même :

f surjective $\Rightarrow f(E) = F \Rightarrow \text{Card}(F) = \text{Card}(f(E)) \Rightarrow \text{Card}(E) = \text{Card}(f(E))$

donc deux éléments distincts de E ne peuvent avoir deux images identiques. f est donc injective.

Ces remarques sont fausses si E et F sont des ensembles infinis.

La réunion de deux parties finies est finie et l'on a :

$$\text{Card}(A \cup B) = \text{Card}(A) + \text{Card}(B) - \text{Card}(A \cap B)$$

puisque la somme Card(A) + Card(B) compte deux fois (une fois de trop) les éléments de $\text{Card}(A \cap B)$. Evidemment, si A et B sont disjoints (i.e. $A \cap B = \varnothing$), on a $\text{Card}(A \cup B) = \text{Card}(A) + \text{Card}(B)$.

On pourra de même réfléchir que :

$$\text{Card}(A \cup B \cup C) = \text{Card}(A) + \text{Card}(B) + \text{Card}(C) - \text{Card}(A \cap B) - \text{Card}(A \cap C) - \text{Card}(B \cap C) + \text{Card}(A \cap B \cap C)$$

On a :

$$\text{Card}(E \times F) = \text{Card}(E) \times \text{Card}(F)$$

Le cardinal de l'ensemble $\mathcal{F}(E, F)$ des applications de E dans F est égal à $(\text{Card}(F))^{\text{Card}(E)}$. En effet, pour chaque élément de E, il y a Card(F) choix possibles pour son image. Ainsi, le nombre d'applications de E dans {0, 1} est égal à $2^{\text{Card}(E)}$ de même que $\text{Card}(\mathcal{P}(E))$, ce qui s'explique par le fait que chaque partie A de E est caractérisée par une unique application de E dans {0,1}, appelée sa fonction indicatrice, que nous noterons $\mathbf{1}_A$. Cette fonction est définie par :

$\mathbf{1}_A(x) = 1$ si $x \in A$
$= 0$ si $x \notin A$

Il y a donc autant de parties dans E que de fonctions de E dans {0,1}.

Si Card(E) = *n*, le nombre de bijections de E est égal à *n*!. En effet, il y a *n* choix possibles pour l'image du premier élément de E, mais seulement *n*–1 pour le suivant, *n*–2 pour le suivant, etc... jusqu'au dernier où il ne restera plus qu'un seul choix possible. Les bijections d'un ensemble fini s'appellent aussi permutations de cet ensemble.

6- Relation d'équivalence

Soit E un ensemble. Une relation binaire $\mathcal{R}$ sur E est une fonction de $E \times E$ à valeurs booléennes (vrai ou faux). Si *x* et *y* sont deux éléments de E, $x\mathcal{R}y$ peut être vrai ou faux. Un exemple fréquent est constitué des relations permettant de relier des éléments partageant une propriété commune. Il s'agit des relations d'équivalence.

a) Exemples et définition :
Voici des exemples de relations d'équivalence :

❑ Dans un ensemble quelconque, l'égalité est une relation d'équivalence triviale. La propriété commune est d'être identique.

❑ Dans l'ensemble des droites affines du plan, D // D' (D est parallèle à D') si et seulement si D et D' ont même vecteur directeur. La propriété commune à D et D' est d'avoir une même direction.

❑ Dans $\mathbb{Z}$, soit *p* un nombre donné. Pour tout couple (*n*, *m*) de $\mathbb{Z}^2$, on pose :

$n \equiv m \bmod p \Leftrightarrow \exists\, k,\ n = m + kp$

On dit que *n* est congru à *m* modulo *p*. La propriété commune à *n* et *m* est d'avoir même reste dans la division euclidienne par *p*.

❑ Dans $\mathbb{R}$, soit α un réel. On dispose d'une définition analogue :

$x \equiv y \bmod \alpha \Leftrightarrow \exists\, k,\ n = m + k\alpha$

Un exemple classique intervient avec $\alpha = 2\pi$ pour les mesures des angles.

❑ Dans $\mathbb{Z} \times \mathbb{Z}^*$, on considère la relation $ab' = ba'$ entre deux couples (a, b) et (a', b'). La propriété commune est de représenter le même rationnel $\frac{a}{b} = \frac{a'}{b'}$.

Formellement, une relation $\mathcal{R}$ sur un ensemble E sera une relation d'équivalence si elle vérifie les propriétés suivantes. Elle est :

- réflexive
- symétrique

- transitive

i) *La réflexivité* s'applique aux relations vérifiant :

$$\forall x \in E, x \mathcal{R} \quad x$$

ii) *La symétrie* s'applique aux relations vérifiant :

$$\forall x \in E, \forall y \in E, x \mathcal{R} y \Rightarrow y \mathcal{R} x$$

iii) *La transitivité* s'applique aux relations vérifiant :

$$\forall x \in E, \forall y \in E, \forall z \in E, [x \mathcal{R} \ y \text{ et } y \mathcal{R} \ z] \Rightarrow x \mathcal{R} \ z$$

EXERCICE :
Vérifier que les relations données dans les exemples sont toutes des relations d'équivalence.

b) Partition et classes d'équivalence :
Une partition d'un ensemble E est une famille $(A_i)_{i \in I}$ vérifiant :

$\forall i, A_i \neq \varnothing$

$\forall i, \forall j, i \neq j \Rightarrow A_i \cap A_j = \varnothing$

$\bigcup_{i \in I} A_i = E$

Une partition permet de définir une relation $\mathcal{R}$ de la façon suivante :

$x \mathcal{R} y \Leftrightarrow \exists i, x \in A_i$ et $y \in A_i$

$\mathcal{R}$ définit la relation "appartenir au même A_i". Une telle relation

Réciproquement, une relation d'équivalence permet de définir une partition de E.

DEFINITION

Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E. *La classe d'équivalence* C_x *d'un élément x est l'ensemble* $\{y \in E \mid y \mathcal{R} x\}$.

La classe de *x* rassemble tous les éléments en relation avec *x* (qui ont même propriété que *x* pour la relation donnée). On peut vérifier que :

a) $x \in C_x$

b) $x \mathcal{R} y \Leftrightarrow C_x = C_y$

c) non$(x \mathcal{R} y) \Leftrightarrow C_x \cap C_y = \varnothing$

En effet :

a) résulte de la réflexivité.

b) $\Rightarrow$ résulte de la transitivité et de la symétrie

$\Leftarrow$ résulte du a) et de la définition des classes d'équivalence

c) $\Rightarrow$ se prouve par l'absurde. Si *z* est élément de $C_x \cap C_y$, alors on a $z \mathcal{R} x$ et $z \mathcal{R} y$, donc, en utilisant la symétrie et la transitivité, $x \mathcal{R} y$.

$\Leftarrow$ est évident.

En conséquence, les classes d'équivalences sont non vides, disjointes deux à deux, et leur réunion est égale à E. Elles forment une partition de E.

EXEMPLE : Un exemple fondamental de relation d'équivalence intervient en Physique dans le domaine de la thermodynamique. Il est tellement banal qu'il faut se forcer à se poser la question de savoir pourquoi cette propriété est vérifiée. Considérons trois corps A, B et C, chacun en équilibre thermique. On dira que A et B ont même température si, lorsque A et B sont mis en contact, aucun échange thermique n'a lieu entre eux. Supposons que A et B aient même température, et que B et C aient même température. Peut-on dire que A et C ont même température ? On doit prendre conscience que la réponse oui donnée à cette question ne doit pas reposer sur une utilisation syntaxique du vocabulaire (A et B ont même température, B et C ont même température donc A et C ont même température), mais sur des expériences physiques répétées. Ces expériences, nous les effectuons plus ou moins consciemment tous les jours, et la réponse à ces expériences est positive. Le physicien pose alors comme principe que cette règle est universellement respectée. C'est le principe zéro de la thermodynamique, qui exprime donc le fait que la propriété "avoir même température" est une relation d'équivalence. Ce principe, pour être énoncé, n'a pas besoin de définir ce qu'est la température. Il énonce simplement le résultat attendu d'un protocole expérimental entre trois corps A, B et C. C'est seulement une fois ce principe posé qu'on peut définir la température comme représentant la classe d'équivalence de corps mutuellement en équilibre thermique. Pour définir précisément et mesurer cette température, on choisit un corps de référence A (en général modélisé par un gaz parfait) à partir duquel on définit la température de A, puis la température de tout corps en équilibre thermique avec A. Ainsi, la notion de température devient une notion dérivée d'un principe premier basé sur l'existence a priori d'une relation d'équivalence entre corps, postulée sur des résultats expérimentaux.

7– Relation d'ordre

La suite du paragraphe est réservée aux MPSI

Un autre exemple de relation est donné par les relations permettant de classer les éléments entre eux. Il s'agit des relations d'ordre.

a) Exemple et définition :

Considérons les trois exemples suivants

i)	dans $\mathbb{R}$	l'infériorité	$x \leq y$
ii)	dans $\mathcal{P}$(E)	l'inclusion	$A \subset B$
iii)	dans $\mathbb{N}^*$	la divisibilité	n divise p, noté $n \mid p$, i.e., $\exists\, k \in \mathbb{N}, p = nk$

Il s'agit de trois relations d'ordre. Une relation est dite relation d'ordre si elle est :

- réflexive
- antisymétrique
- transitive

L'antisymétrie s'applique aux relations vérifiant :

$$\forall\, x \in \text{E}, \forall\, y \in \text{E}, [\, x \mathcal{R}\, y \text{ et } y \mathcal{R}\, x\,] \Rightarrow x = y$$

Comme son nom l'indique, une relation d'ordre sert à établir une hiérarchie parmi les éléments de E. Si $x \mathcal{R}\, y$, x sera le plus souvent considéré comme plus petit que y (la convention inverse aurait pu être également être prise). $x \mathcal{R}\, y$ doit être compris comme une phrase du type x est plus petit que y,

ou bien x est avant y (et éventuellement, $x = y$). Du fait de l'antisymétrie et de la transitivité, il est impossible d'avoir un cycle d'éléments distincts vérifiant $x_1 \mathcal{R} x_2$, $x_2 \mathcal{R} x_3$, ..., $x_{n-1} \mathcal{R} x_n$, $x_n \mathcal{R} x_1$.

Voici un dernier exemple : dans l'ensemble des mots sur un alphabet (un mot est une suite finie de lettres de l'alphabet), l'ordre alphabétique ou lexicographique est une relation d'ordre. Cette relation existe dans de nombreux langages de programmation :

'ABBC' ≤ 'ABC' est vrai
'ABBC' ≤ 'ABB' est faux

Remarque : si on définit une relation ≤ dans $\mathbb{N}$, $\mathbb{Z}$ ou $\mathbb{R}$, il n'en est pas de même dans $\mathbb{C}$. Pourquoi ? Les relations définies sur les ensembles de nombres présentent une certaine compatibilité avec les lois + et × définies sur ces ensembles. En particulier, on a :

$$a \geq 0 \text{ et } b \geq 0 \Rightarrow a + b \geq 0 \text{ et } ab \geq 0.$$

Si l'on avait, sur $\mathbb{C}$, une relation du type $i \geq 0$, alors, en effectuant le produit avec lui-même, on obtiendrait $-1 \geq 0$, Puis en multipliant de nouveau par i, on aurait $-i \geq 0$, ce qui est contradictoire Cela ne veut pas dire qu'il est impossible de définir une relation d'ordre sur $\mathbb{C}$, mais que cette relation ne présentera aucun caractère de compatibilité avec les lois + et ×.

Exercice : définir une relation d'ordre sur $\mathbb{C}$.

b) Ordre total, ordre partiel :

On remarquera une différence entre d'une part la relation d'inégalité dans $\mathbb{R}$ ou l'ordre lexicographique, et d'autre part, l'inclusion ou la relation de divisibilté.

Dans le premier cas, pour tout élément x et y, l'une des deux propriétés $x \mathcal{R} y$ ou $y \mathcal{R} x$ est vérifiée, ce qui n'est pas vrai dans le second cas. Par exemple, on n'a pas 2 | 3, ni 3 | 2. De même {1,2} n'est pas inclus dans {3}, pas plus que {3} n'est inclus dans {1,2}. On parle respectivement d'ordre total et partiel.

Une relation d'ordre $\mathcal{R}$ sur un ensemble E est dit d'ordre total si :

$$\forall x \in \text{E}, \forall y \in \text{E}, x \mathcal{R} y \text{ ou } y \mathcal{R} x$$

Dans le cas contraire, $\mathcal{R}$ est une relation d'ordre partiel :

$$\exists x \in \text{E}, \exists y \in \text{E}, \text{non}(x \mathcal{R} y) \text{ et non}(y \mathcal{R} x)$$

c) Majorant, minorant, maximum, minimum :

❑ Soit E muni d'une relation d'ordre $\mathcal{R}$. Une partie A de E est *minorée* par a (a est un *minorant* de A) si :

$$\forall x \in \text{A}, a \mathcal{R} x$$

A est *majorée* par b (b est un *majorant* de A) si :

$$\forall x \in \text{A}, x \mathcal{R} b$$

Exemple : [0,1] est majoré par 2, et minoré par –1.

❑ Soit E muni d'une relation d'ordre $\mathcal{R}$. Une partie A de E admet un *minimum a* (ou plus petit élément) si :

$$a \in A \text{ et } \forall x \in A,\ a\ \mathcal{R}\ x$$

a est donc un minorant de A, lui–même élément de A.

A admet un *maximum b* (ou plus grand élément) si :

$$b \in A \text{ et } \forall x \in A,\ x\ \mathcal{R}\ b$$

b est donc un majorant de A, lui–même élément de A.

Exemples :

0 est le minimum de [0,1] (avec la relation usuelle) et 1 est son maximum.
]0,1] n'admet pas de minimum, mais admet 1 comme maximum.
]0,1[n'admet ni maximum ni minimum.

$\varnothing$ est le minimum de $\mathcal{P}(E)$ pour la relation d'inclusion. E est le maximum.
Si A est l'ensemble de tous les singletons de E, A n'admet ni minimum, ni maximum.

Pour la relation de divisibilité de $\mathbb{N}$, 1 est le minimum, il n'y a pas de maximum.

Fin de partie réservée aux MPSI

II : Structures algébriques

Début de partie réservée aux MPSI

1– Loi de composition interne

a) Définition :

Soit E un ensemble. On appelle loi de composition interne de E, notée par exemple $*$, une opération qui permet d'associer, à deux éléments quelconques de E *a* et *b*, un troisième élément noté $a * b$.

Exemples : Les lois de compositions internes les plus courantes sont :

- \+ dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.
- – dans les mêmes ensembles.
- $\times$ dans les mêmes ensembles.
- / dans $\mathbb{Q}^*$, $\mathbb{R}^*$, ou $\mathbb{C}^*$.
- div (division entière) dans $\mathbb{N}^*$ ou $\mathbb{Z}^*$.
- o dans l'ensemble des applications de E dans E.
- $\cap$ dans l'ensemble E = $\mathcal{P}(\Omega)$ des parties d'un ensemble Ω.
- $\cup$ dans l'ensemble des parties d'un ensemble.
- $\wedge$ (produit vectoriel) dans l'espace euclidien orienté de dimension 3

b) Associativité :

Soit E un ensemble muni d'une loi de composition interne notée $*$. Cette loi est dite associative si :

$$\forall a \in E, \forall b \in E, \forall c \in E, (a * b) * c = a * (b * c)$$

L'intérêt d'une telle notion est que les parenthèses deviennent inutiles, la notation $a * b * c$ valant indifféremment l'une ou l'autre des expressions. Les lois suivantes, dans les ensembles du paragraphe précédent, sont associatives : +, $\times$, o, $\cap$, $\cup$. Les lois suivantes ne le sont pas : –, /, div, $\wedge$.

On notera que l'absence de parenthèses dans l'écriture :

$$7 - 5 - 1 = 1$$

signifie implicitement qu'une convention est adoptée pour distinguer entre $(7 - 5) - 1$ et $7 - (5 - 1)$, la convention étant ici *que le calcul se fait de gauche à droite*, mais rien ne nous aurait empêché de prendre la convention inverse : faire les calculs de droite à gauche. Ce qui aurait conduit au résultat, qui nous paraît faux : $7 - 5 - 1 = 3$!!
Quant à la notation *a*/*b*/*c*, elle est à éviter, aucune convention n'ayant été définie à son sujet.

c) Commutativité :
Soit E un ensemble muni d'une loi de composition interne notée $*$. Cette loi est dite commutative si :

$$\forall\, a \in \mathrm{E},\ \forall\, b \in \mathrm{E},\ a * b = b * a$$

L'intérêt d'une telle notion est que l'ordre dans lequel les éléments sont placés est indifférent. Les lois suivantes, dans les ensembles du paragraphe précédent, sont commutatives : +, $\times$, $\cap$, $\cup$. Les lois suivantes ne le sont pas : o (sauf si les fonctions sont définies sur un ensemble possédant un seul élément), –, /, div, $\wedge$.

Dans le cas d'une loi $*$ commutative et associative, l'expression suivante possède un sens :

$$\mathop{\Large *}_{i \in \mathrm{I}} x_i$$

où I est un ensemble fini d'indices. Par exemple, si $\mathrm{I} = \{1,...,n\}$, l'expression précédente est égale à $x_1 * x_2 * ... * x_n$, l'ordre des termes étant indifférent.

Exemples :

$\sum_{i=1}^{n} x_i$ désigne la somme des éléments x_i

$\prod_{i=1}^{n} x_i$ désigne le produit des éléments x_i

$\bigcap_{i \in \mathrm{I}} \mathrm{A}_i$ désigne l'intersection des parties A_i

$\bigcup_{i \in \mathrm{I}} \mathrm{A}_i$ désigne la réunion des parties A_i

On notera, que, si I et J sont deux ensembles disjoints d'indices, on a :

$$\mathop{\Large *}_{i \in \mathrm{I} \cup \mathrm{J}} x_i = \mathop{\Large *}_{i \in \mathrm{I}} x_i * \mathop{\Large *}_{i \in \mathrm{J}} x_i \qquad \text{(i)}$$

Quelle formule donner si I et J ne sont pas disjoints ? Si l'un des ensembles est vide ? Où retrouve–t–on des conventions analogues ? (penser à 0! par exemple)

d) Elément neutre :
Soit E muni d'une loi interne $*$. On dit que e est élément neutre de la loi $*$ si :

$\forall\, a \in \mathrm{E},\ a * e = e * a = a$

EXEMPLES :
Le neutre de + est 0. Celui de $\times$ est 1. Celui de $\circ$ est Id. Celui de $\cap$ est Ω (l'ensemble entier). Celui de $\cup$ est $\varnothing$. – et / n'ont pas d'éléments neutres. Si $*$ est associative, commutative, et admet un élément neutre *e*, alors la formule (i) nous conduit à poser :

$$\mathop{\Large *}_{i \in \varnothing} x_i = e$$

Le neutre, s'il existe est unique. En effet, si *e* et *e*' sont deux neutres, on a :
$e * e' = e$ car *e*' est neutre
$e * e' = e'$ car *e* est neutre
donc $e = e'$.

e) Elément symétrique :
Soit E muni d'une loi $*$, et d'un élément neutre *e*. On appelle symétrique d'un élément *x* un élément *x*' tel que :
$x * x' = x' * x = e$

EXEMPLES :
Le symétrique de *x* pour + est $-x$ (appelé opposé de *x*).
Le symétrique de *x* non nul pour $\times$ est $\frac{1}{x}$ (appelé inverse de *x*)
Le symétrique de *f* bijective pour $\circ$ est f^{-1} (appelé réciproque)

Il n'y a en général pas de symétrique pour $\cap$ et $\cup$.

– et /, n'ayant aucune propriété particulière, apparaissent ici comme symétrisations des opérations + et $\times$.

Le symétrique, s'il existe, et si la loi est associative, est unique. En effet, si *x*' et *x*'' sont deux symétriques de *x*, alors on a :
$x' * x * x'' = (x' * x) * x'' = e * x'' = x''$
$= x' * (x * x'') = x' * e = x'$.
donc $x' = x''$. Ce symétrique est souvent noté x^{-1}.

EXERCICE : Si $*$ est associative, commutative, admet un élément neutre *e*, et si tout élément admet un symétrique, alors on a, avec I et J quelconques :

$$\mathop{\Large *}_{i \in I \cup J} x_i = \mathop{\Large *}_{i \in I} x_i * \mathop{\Large *}_{i \in J} x_i * \left[\mathop{\Large *}_{i \in I \cap J} x_i\right]^{-1}$$

2– Définition d'un groupe
Un ensemble $(G,*)$ est un groupe si :
i) G est non vide.
ii) $*$ est une loi de composition interne.
iii) $*$ est associative.
iv) $*$ admet un élément neutre *e*.

v) tout x de G admet un symétrique x'.

Si, en outre, $*$ est commutative, le groupe est dit commutatif ou abélien (Niels Abel, mathématicien norvégien, 1802-1829).

On note parfois la loi du groupe multiplicativement (ab au lieu de $a * b$) ou additivement ($a + b$ au lieu de $a * b$), mais la notation additive est réservée aux groupes commutatifs. $a * a * ... * a$ est alors noté a^n dans le cas multiplicatif ou na dans le cas additif.

Les axiomes des groupes permettent de simplifier les équations. Ainsi :

$a * x = a * y \Rightarrow x = y$ (composer à gauche par le symétrique de a)

$x * a = y * a \Rightarrow x = y$ (composer à droite par le symétrique de a)

EXEMPLE 1 :
On peut citer le groupe des complexes de module 1, le groupe des racines $n^{ème}$ complexes de l'unité, le groupe des similitudes directes du plan. Voici d'autres exemples.

EXEMPLE 2 :
Voici quelques groupes à deux éléments :

{σ,Id} où σ est une symétrie, muni de la loi o.

U_2 = {+1,–1} muni du produit (groupe des racines carrées de l'unité, ou règle des signes).

$\mathbb{Z}/2\mathbb{Z}$ = {0,1} muni de la loi +. Dans cet ensemble, on pose 1 + 1 = 0.

{Croissance, Decroissance} muni de la loi o, et de la règle donnant le sens de variation de la composée de deux fonctions monotones.

{true,false} (en programmation), muni de la loi xor (ou exclusif).

Tous ces groupes sont en fait identiques au suivant :
Groupe à deux éléments {a,e}. La table d'opération de ce groupe est :

*	a	e
a	e	a
e	a	e

On a nécessairement $a^2 = e$ car si $a^2 = a$, en simplifiant par a, on obtient $a = e$.

La correspondance se fait de la façon suivante :

Groupe	*	a	e
{σ,Id}	o	σ	Id
{+1,–1}	×	–1	+1
$\mathbb{Z}/2\mathbb{Z}$	+	1	0
{Croissance, Décroissance}	o	Decroissante	Croissante
{true,false}	xor	true	false

Tous ces groupes sont dits isomorphes. Un théorème démontré pour l'un d'entre eux l'est pour tous.

Par exemple : la valeur d'un produit en fonction de la parité du nombre de a est a si ce nombre est impair, e si ce nombre est pair. Ce résultat se traduit de la façon suivante dans quelques situations courantes :

$\sigma^{2p} = Id$ et $\sigma^{2p+1} = \sigma$ pour une symétrie σ

Le produit d'un nombre pair de termes négatifs est positif, le produit d'un nombre impair de termes négatifs est négatif.

La composée d'un nombre pair de fonctions décroissantes et d'un nombre quelconque de fonctions croissantes est croissante ; La composée d'un nombre impair de fonctions décroissantes et d'un nombre quelconque de fonctions croissantes est décroissante.

EXEMPLE 3 :
L'exemple suivant n'est pas un groupe :

*	*a*	*e*
a	*a*	*a*
e	*a*	*e*

On trouve cependant cette situation dans les cas suivants :

{*a*, *e*}	*	*a*	*e*
$\mathbb{Z}/2\mathbb{Z}$	×	0	1
{*f* paire, *f* impaire}	o	paire	impaire
{true, false}	or	true	false
{false, true}	and	false	true
{Ω, ∅}	∩	∅	Ω
{∅, Ω}	∪	Ω	∅

Ici, *a* est dit absorbant.

EXEMPLE 4 : Groupes à trois éléments :
Quels sont les groupes à trois éléments ?
Il n'y en a qu'un :

*	*a*	*b*	*e*
a	*b*	*e*	*a*
b	*e*	*a*	*b*
e	*a*	*b*	*e*

Pour le remplir, on remarque que, pour chaque élément *y*, l'application : $x \in G \to yx \in G$ est bijective. Chaque élément du groupe apparaît donc une fois et une seule dans chaque ligne *y*. De même, l'application $x \to xy$ est bijective, donc chaque élément du groupe apparaît une fois et une seule dans chaque colonne *y*. En outre $ab = b$ est impossible car cela implique, en simplifiant par *b*, que $a = e$. De même $ab = a$ est impossible, donc $ab = e$, etc... Il est alors facile de compléter le tableau.

Tous les groupes à trois éléments sont donc isomorphes. En voici quelques exemples :

G	*	*a*	*b*	*e*
$\mathbb{U}_3 = \{1, j, j^2\}$	×	*j*	j^2	1

où *j* est une racine cubique complexe de l'unité. $\mathbb{U}_3$ est le groupe des racines cubiques de l'unité.

$\{1, \sigma, \sigma^2\}$	o	σ	σ^2	Id

où σ est une rotation de $2\pi/3$

$\mathbb{Z}/3\mathbb{Z}$	+	1	2	0

constitué des éléments {0,1,2} où le calcul se fait modulo 3 (i.e. à un multiple de 3 près).

EXEMPLE 5 :
Quels sont les groupes à 4 éléments ?
On n'en trouve que deux :

*	*a*	*b*	*c*	*e*
a	*e*	*c*	*b*	*a*
b	*c*	*a*	*e*	*b*
c	*b*	*e*	*a*	*c*
e	*a*	*b*	*c*	*e*

*	*a*	*b*	*c*	*e*
a	*e*	*c*	*b*	*a*
b	*c*	*e*	*a*	*b*
c	*b*	*a*	*e*	*c*
e	*a*	*b*	*c*	*e*

Le premier n'est autre que $(\mathbb{Z}/4\mathbb{Z},+)$, c'est à dire le groupe des éléments {0,1,2,3} où les calculs se font modulo 4, ou encore le groupe $\mathbb{U}_4$ des racines quatrièmes complexes de l'unité :

G	*	*c*	*a*	*b*	*e*
$\mathbb{U}_4 = \{1,-1,i,-i\}$	×	*i*	–1	*–i*	1

groupe des racines quatrième de l'unité.

$\mathbb{Z}/4\mathbb{Z}$	+	1	2	3	0

Le second est $(\mathbb{Z}/2\mathbb{Z})^2$:

G	*	*a*	*b*	*c*	*e*
$(\mathbb{Z}/2\mathbb{Z})^2$	+	(1,0)	(0,1)	(1,1)	(0,0)

Ce dernier groupe se trouve également dans la situation suivante : considérons un matelas. Il peut être laissé dans la position initiale (Id). On peut le tourner dans le sens de la longueur (σ). On peut le tourner dans le sens de la largeur (θ). On peut lui faire un demi–tour à plat (φ). {Id,σ,θ,φ} n'est autre que le second groupe.

EXEMPLE 6 :

$\mathbb{U}_n$ groupe des racines $n^{\text{ème}}$ de l'unité dans $\mathbb{C}$, muni du produit

$\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, ..., n–1\}$ où les calculs se font modulo n.

3– Sous-groupe

Définition : Soit (G,∗) un groupe et G' une partie de G. On dit que G' est un sous–groupe de G si, muni de la loi ∗, (G',∗) est un groupe. Il suffit de vérifier les propriétés suivantes :

- ❑ G' est non vide
- ❑ G' est stable pour ∗ (ce qui signifie que ∗ est une loi interne à G') :

$$\forall x \in G', \forall y \in G', x * y \in G'$$

❑ G' est stable par passage au symétrique : $\forall x \in G', x^{-1} \in G'$

Il est inutile de vérifier que G' dispose d'un élément neutre. En effet, si e est le neutre de G, on montre que e est également neutre de G'. En effet :

G' est non vide, donc il existe x élément de G'

$x \in G'$ donc $x^{-1} \in G'$

$x \in G'$ et $x^{-1} \in G'$ donc $x * x^{-1} \in G'$ donc $e \in G'$

$\forall x \in G, e * x = x * e = x$ donc ceci reste vrai a fortiori pour x dans G'

L'associativité étant vraie dans G est a fortiori vraie dans G'. Il en est de même de l'éventuelle commutativité.

On montre aisément que l'intersection de deux ou plusieurs sous–groupes est lui–même un sous–groupe.

EXEMPLE 1 : Dans le plan $\mathbb{R}^2$, considérons les applications qui au vecteur (x,y) associe le vecteur $(x',y') = (ax + by, cx + dy)$, avec $ad - bc \neq 0$, ce qu'on note :

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

L'ensemble de ces applications, muni de la loi de composition o, forme un groupe appelé groupe linéaire.

L'ensemble des applications pour lesquelles $ad - bc = \pm 1$ en forme un sous–groupe.

L'ensemble des applications orthogonales (rotations et symétries) forme un sous–groupe de ce sous-groupe appelé groupe orthogonal.

L'ensemble des rotations forme lui–même un sous–groupe du groupe orthogonal.

EXEMPLE 2 : l'ensemble des nombres pairs forme un sous–groupe de $(\mathbb{Z},+)$.

4– Anneaux et corps

Un **anneau** $(A, +, \times)$ est un ensemble non vide muni de deux lois + et $\times$ vérifiant les propriétés suivantes :

$(A, +)$ est un groupe commutatif. Son neutre est noté 0.

$\times$ est une loi associative possédant un élément neutre, et distributive par rapport à l'addition, i.e. :

$$\forall a, \forall b, \forall c, a \times (b + c) = ab + ac \text{ et } (b + c) \times a = ba + ca$$

Le produit $\times$ peut ne pas être commutatif. Un exemple non commutatif est donné par l'anneau des matrices carrées.

0 est nécessairement absorbant. Soit x un élément quelconque. On a :

$x \times 0 = x \times (0 + 0) = x \times 0 + x \times 0$

$\Rightarrow$ $0 = x \times 0$ en simplifiant par $x \times 0$

De même, $0 \times x = 0$.

0 ne peut donc avoir de symétrique pour le produit. Si tout élément non nul admet un symétrique pour le produit, l'ensemble considéré est un **corps** ; on réserve en général cette appellation au cas où, de plus, le produit $\times$ est commutatif.

A' est un sous-anneau de A si A' est inclus dans A, si (A', +, ×) est un anneau ; on convient également que le neutre de A et de A' est identique.

EXEMPLES :

- $(\mathbb{Z}, +, \times)$ est un anneau. Les matrices carrées munies de la somme et du produit des matrices forment un anneau.
- $(\mathbb{Q}, +, \times)$ est un corps, sous-corps de $\mathbb{R}$, lui-même sous-corps de $\mathbb{C}$. Les fractions rationnelles de polynômes, de la forme $\frac{P}{Q}$ où P et Q sont des polynômes (avec $Q \neq 0$) forment un corps.
- Considérons les quatres opérations élémentaires +, –, × et /, ainsi que la fonction $\sqrt{}$. Partant des rationnels, construisons de proche en proche de nouveaux nombres en itérant les opérations précédentes. On obtient ainsi par exemple les nombres $\sqrt{2}$ ou $\frac{1+\sqrt{5}}{2}$ ou $\sqrt{2-\sqrt{2+\sqrt{2+\sqrt{2+\sqrt{2}}}}}$. En continuant indéfiniment, on forme un corps appelé corps des nombres constructibles. On peut montrer que, dans le plan, les points à coordonnées constructibles dans un repère orthonormé sont précisément les points constructibles à la règle et au compas à partir de l'origine du repère et des vecteurs de base. (Cela résulte du fait que l'intersection d'un cercle et d'une droite conduit à une équation du second degré, dont la résolution ne fait appel qu'aux opérations +, –, ×, / et $\sqrt{}$). On a montré au XIXème que les nombres π, $\sqrt[3]{2}$ ou $\cos(\frac{\pi}{9})$ ne sont pas constructibles, rendant impossible la résolution de problèmes millénaires posés pas les Grecs Anciens, celui de la quadrature du cercle, de la duplication du cube ou de la trisection de l'angle.
- Considérons l'ensemble $\mathbb{F}_4 = \{0, 1, \alpha, \beta\}$ avec les lois commutatives + et × définies comme suit :

  0 est le neutre de la somme
  1 est le neutre du produit
  $\alpha^2 = \beta$ $\quad \alpha\beta = 1$ $\quad \beta^2 = \alpha$
  $1 + \alpha = \beta$ $\quad 1 + \beta = \alpha$ $\quad \alpha + \beta = 1$

  Ces opérations donnent à $\mathbb{F}_4$ une structure de corps. $\mathbb{F}_4$ est le seul corps à quatre éléments. En ce qui concerne la somme, sa structure de groupe est isomorphe à celle de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ avec l'isomorphisme suivant :

  $\mathbb{F}_4 \rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
  $0 \rightarrow (0,0)$
  $1 \rightarrow (1,1)$
  $\alpha \rightarrow (0,1)$
  $\beta \rightarrow (1,0)$

  mais il n'y a pas d'isomorphisme pour le produit. $\mathbb{F}_4$ est un corps, ce que n'est pas $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
  (On a $\alpha\beta = 1$ mais $(0,1) \times (1,0) = (0,0)$ et non $(1,1)$).

Fin de partie réservée aux MPSI

L'annexe qui suit ne fait pas partie du programme de mathématiques de CPGE. Elle est destinée à des étudiants (plutôt de deuxième année ou au-delà) qui s'intéresseraient aux fondements des mathématiques.

Annexe : les axiomes

Qu'est-ce qu'un axiome ?

D'Alembert écrit, dans son Encyclopédie (1788) :

> ***Axiome*** *: En Mathématiques, on appelle axiomes des propositions évidentes par elles-mêmes, et qui n'ont pas besoin de démonstrations. Telles sont les propositions suivantes : le tout est plus grand que la partie ; si à deux grandeurs égales on ajoute des grandeurs égales, les sommes seront égales ; si deux figures étant appliquées l'une sur l'autre se couvrent parfaitement, ces deux figures sont égales en tout.*
>
> ***Théorème*** *: c'est une proposition qui énonce et démontre une vérité.*

Notre conception moderne des axiomes ne correspond plus à des notions déclarées évidentes par elles-mêmes. On fait actuellement reposer une théorie mathématique sur des notions primitives (non définies) et les axiomes ne servent qu'à décrire les règles d'utilisation de ces notions primitives. Voici des exemples modernes d'axiomes et de notions primitives :

i) La notion d'ensemble et d'appartenance est une notion primitive. On ne cherchera à définir ni l'une ni l'autre.

ii) Frege, en 1893, avait proposé comme axiome le suivant : Φ étant un prédicat quelconque, il existe un ensemble A tel que, pour tout x, x appartient à A si et seulement si $\Phi(x)$ est vrai. Russel, en 1902, proposa de prendre comme prédicat : $\Phi(x) \Leftrightarrow x \notin x$. D'après Frege, il existe alors un ensemble A tel que :

$$\forall\, x,\ x \in \mathrm{A} \Leftrightarrow x \notin x$$

Cette équivalence est vraie en particulier lorsque x = A, ce qui donne :

$$\mathrm{A} \in \mathrm{A} \Leftrightarrow \mathrm{A} \notin \mathrm{A}$$

ce qui contradictoire. Cet exemple prouve qu'on ne peut pas prendre n'importe quoi pour axiome, en particulier en ce qui concerne la construction des ensembles.

Voici quelques axiomes actuellement en vigueur :

❑ La réunion d'une famille d'ensemble (indicée par un ensemble) est un ensemble.

❑ La famille constituée des parties d'un ensemble est un ensemble.

❑ Il existe un ensemble infini

❑ Le principe de récurrence dans $\mathbb{N}$

❑ Le $5^{\text{ème}}$ postulat d'Euclide en géométrie euclidienne : par un point donné, il passe une parallèle à une droite donnée et une seule. Le rejet de cet axiome conduit à d'autres types de géométries.

❑ L'existence de la borne supérieure dans $\mathbb{R}$

Un axiome curieux, l'axiome du choix :

Considérons la proposition suivante :

Soit f une application injective de E dans F. Alors il existe une application surjective g de F dans E telle que g o f = Id.

Démonstration :

❑ Soit a un élément quelconque de E. On pose :

i) si y appartient à f(E), $g(y) = x$ où x est l'unique élément tel que $y = f(x)$.

ii) si y n'appartient pas à f(E), on pose $g(y) = a$.

On alors g surjective et g o f = Id

Considérons maintenant la proposition suivante :

Soit f une application surjective de E dans F. Alors il existe une application injective g de F dans E telle que f o g = Id.

Démonstration :
❑ Pour tout y de F, $f^{-1}(\{y\})$ est non vide. Soit $g(y)$ un élément de cette partie. Alors g est injective et $f \circ g = \mathrm{Id}$

Il y a une différence fondamentale entre ces deux démonstrations. La première ne fait appel qu'au choix arbitraire d'un unique élément *a*, alors que la seconde fait appel au choix simultané et arbitraire d'un nombre quelconque et éventuellement infini d'éléments $g(y)$. La possibilité d'un tel choix a été vivement contesté au début du XXème siècle et nécessite un axiome : l'axiome du choix. Ce dernier est également lié à la question de munir un ensemble d'un "bon ordre" ; un ensemble est dit bien ordonné si toute partie non vide admet un plus petit élément. Un exemple typique d'ensemble bien ordonné est $\mathbb{N}$. Par contre, $\mathbb{R}$ n'est pas bien ordonné avec l'ordre usuel. Cantor pensait que tout ensemble pouvait être muni d'un bon ordre, et la nécessité d'une démonstration s'est posé. On peut se demander en effet comment il peut être possible de munir par exemple $\mathbb{R}$ d'un bon ordre. Au début du siècle, on pensa avoir montré l'impossibilité de munir $\mathbb{R}$ d'un bon ordre. Mais Zermelo prouva le contraire en utilisant pour la première fois ce qui allait devenir l'axiome du choix :
Soit $(A_i)_{i \in I}$ une famille d'ensembles non vides, indicée par un ensemble I quelconque et soit A la réunion des A_i. Alors il existe une application f de I dans A telle que :

$$\forall\, i \in I,\ f(i) \in A_i.$$

La fonction f permet de choisir un élément noté $f(i)$ dans chaque A_i. D'autres formulations équivalentes sont possibles. Par exemple, le produit $\prod_{i \in I} A_i$ est non vide.

On montre que cet axiome permet de munir $\mathbb{R}$ d'un bon ordre, sans qu'on puisse cependant l'expliciter, et ceci choqua bon nombre de mathématiciens qui le rejetèrent. Cependant, d'autres théorèmes, dont les énoncés paraissaient vraisemblables à la communauté mathématique nécessitent l'axiome du choix. En voici quelques-uns :
❑ Soit E et F deux ensembles. Alors ou bien il existe une injection de E dans F ou bien il existe une injection de F dans E. (Théorème de Cantor, équivalent à l'axiome du choix)
❑ Soit E un espace vectoriel. Alors il existe une base sur E.
❑ Tout ensemble inductif admet un élément maximal. (Un ensemble est inductif si toute partie totalement ordonnée est majorée). (Théorème de Zorn, équivalent à l'axiome du choix).

Certains résultats cependant sont prouvés au moyen de l'axiome du choix et fortement contraires à l'intuition :
❑ Lebesgue a développé une théorie de l'intégration très puissante. Toutes les fonctions usuelles sont mesurables au sens de Lebesgue. Les seuls exemples non mesurables qui ont été découverts nécessitent l'axiome du choix.
❑ La sphère unité peut être décomposée en quatre parties isométriques A, B, C, D avec D également isométrique à $A \cup B$. (D est donc à la fois le quart et la moitié de la sphère). (Théorème de Hausdorf, extrêmement choquant).
❑ Dans le même ordre d'idée, deux ensembles bornés quelconques de $\mathbb{R}^3$ d'intérieur non vide peuvent être partitionnés en deux familles finies respectives (A_i) et (B_i) de façon que A_i soit isométrique à B_i. (Théorème de Banach-Tarski).

❑ Il existe des fonctions de $\mathbb{R}$ dans $\mathbb{R}$ telle que $f(x + y) = f(x) + f(y)$, avec f différente des fonctions linéaires ax. Cependant aucune de ces fonctions ne peut être explicitée.

La nature de l'axiome du choix est donc complexe. Affirmant l'existence d'un objet, il ne peut cependant définir explicitement cet objet. Bien plus, une telle explicitation est impossible puisque le rejet de l'axiome supprimerait la seule possibilité de valider son existence.

Ces questions sont liées à la nature de la notion de l'existence en mathématiques. Il y a deux notions différentes, l'une est l'existence explicite, fournissant le moyen de construire l'objet (par exemple, étant donnés deux entiers, on peut déterminer explicitement le plus petit multiple commun de ces deux entiers), l'autre est une existence purement formelle ne fournissant aucun moyen de définir explicitement l'objet (des exemples ont été donnés précédemment). Les mathématiques usuelles ne font aucune distinction entre ces deux notions d'existence, ce qu'on peut juger regrettable car l'existence formelle a une utilité et une efficacité bien moins grande que l'existence explicite. Avouons cependant que les branches des mathématiques cherchant à apporter une distinction entre ces deux notions d'existence (logique intuitionniste, analyse constructive) sont difficiles à aborder.

On peut néanmoins reconnaître cette qualité à l'existence formelle : elle prouve qu'il est vain de dépenser ces efforts à montrer l'inexistence de l'objet considéré. Considérons par exemple une propriété donnée sur les entiers (par exemple, celle d'être un nombre parfait [égal à la somme de ses diviseurs autres que lui-même] impair et posons-nous la question de savoir si cette propriété est vérifiée par au moins un entier. Il y a alors trois possibilités.

i) Aucun entier ne vérifie la propriété

ii) Il existe au moins un entier vérifiant la propriété et on peut donner sa valeur (existence explicite)

iii) Il existe au moins un entier vérifiant la propriété mais on ne peut donner sa valeur (existence formelle), soit parce que cette valeur est trop grande pour pouvoir être calculée, soit parce qu'on ignore un procédé de calcul de cette valeur, soit même parce que cette existence repose sur un axiome. Si on se trouve dans ce cas, cela montre qu'il est inutile de chercher à prouver i).

◆