Cours d'Algèbre Générale de l'Ecole Nationale Supérieure Polytechnique de Yaoundé

BOUETOU BOUETOU Thomas

17 septembre 2019

Objectifs :

Ce cours d'algèbre générale vise à donner les capacités de raisonnement et, de développer une base théorique qui est nécessaire pour le renforcement des aptitudes de conception utiles aux jeunes ingénieurs.

Who is great in calculus is a great man.

Tout comme la lumière éloigne les tenebres de l'obscurité alors, les mathématiques éloignent l'ignorance de la connaissance.

L'algèbre de manière particulière, tout comme La mathématque dans son entitée est le langage de la science.

Among mathematicians in general, three main categories may be distinguished; and perhaps the names logicians, formalists, and intuitionist may serve to characterize them,

1. (1) The word logician is here used, of course, without reference to the mathematical logic of Boole, Peirce, etc.; it is only intended to indicate that the main strength of the men belonging to this class lies in their logical and critical power, in their ability to give strict definitions, and to derive rigid deductions therefrom. The great and wholesome influence exerted for example in Germany is by Weierstrass in this direction is well known.
2. (2) The formalists among the mathematicians excel mainly in the skilful formal treatment of a given question, in devising for it an "algorithm." Gordan, or let us say Cayley and Sylvester, must be ranged in this group.
3. (3) To the intuitionists, finally, belong those who lay particular stress on geometrical intuition (Anschatmng), not in pure geometry only, but in all branches of mathematics. What Benjamin Peirce has called "geometrizing a mathematical question " seems to express the same idea. Lord Kelvin and von Standi may be mentioned as types of this category. Clebsch must be said to belong both to the second and third of these categories, and Felix Klein can classed with himself to the third, and also the first.

Classification of mathematical mind made by Felix Klein at the colloquium on mathematics from August 28th till September 9th prior After the adjournment of the International Congress of Mathematics in Chicago August, 1893.

Table des matières

Chapitre 1

THEORIE DES ENSEMBLES

Le développement de la mathématique nécessite lui même pratiquement l'usage de symboles abréviateur dont certains ont déjà été indiqués. La pluspart de ces symboles seront aussi utilisés en mathématque.

N. BOURBAKI

1.1 ELEMENTS DE LOGIQUE MATHEMATIQUE ET APPLICATIONS

En accord avec le dictionnaire, la logique est la science du raisonnement. La logique est un processus d'aide par lequel on arrive à une conclusion à partir d'un énoncé donné en utilisant des lois logiques. La logique joue un rôle important dans les études qui impliquent le raisonnement, similaire au traitement de la théorie des ensembles (connu comme théorie axiomatique des ensembles). Mais dans ce chapitre, nous allons aborder l'approche naive. L'approche axiomatique avait été donnée premièrement par le mathématicien anglais Georges Boole. C'est pourquoi, parfois on appelle logique booléenne. Ceci est aussi connu comme logique mathématique ou logique symbolique. La logique symbolique a gagné en importance avec l'avènement des ordinateurs.

1.1.1 Enoncé Logique

Nous pouvons exprimer nos pensées de deux manières :

- par les mots
- par la logique symbolique

Nous utilisons la logique symbolique pour des expressions claires de nos pensées parce que les symboles sont neutres et abstraits. Un énoncé ou proposition est toute phrase qui :

- a un sens
- est déclarative
- qui n'est pas ambigue.

Définition 1.1.1.1 *On appelle proposition logique toute relation p qui est soit vraie soit fausse.*

- *Quand la proposition est vraie, on lui affecte la valeur* 1.
- *Quand la proposition est fausse, on lui affecte la valeur* 0.

Ces valeurs sont appelées "Valeurs de vérité de la proposition".

Ainsi, pour définir une proposition logique, il suffit de donner ses valeurs de vérités. En général, on met ces valeurs dans un tableau qu'on nommera "Table de vérités" ou "Tableau de vérités".

La proposition est soit **vraie** ou **fausse**, ou ce qui est équivalent **valide** ou **invalide**. Une proposition ne peut pas être vraie et fausse en même temps. Ce fait est connu sous la **loi de la moitié exclu**. La véracité ou fausseté d'une proposition est appelé sa **vraie valeur**. Une phrase ouverte n'est pas une proposition par exemple $x + 6 = 8$. La véracité de ceci est ouverte jusqu'au moment où l'on trouve la valeur de x. De tels énoncés sont appelés phrases ouvertes.

Exemple 1.1.1.1 *:*

- *"$4 + 2 = 8$" c'est une proposition fausse. Sa vraie valeur est dénotée par F.*
- *" Mardi vient après Lundi " c'est une proposition vraie. Sa vraie valeur est dénotée par V.*
- *" pourquoi vas-tu au cinéma ? " ceci n'est pas un énoncé. La phrase n'est pas déclarative.*
- *" La mathématique est une matière difficile". Cette proposition est vraie ou fausse selon des personnes. La mathématique peut être difficile pour certains et facile pour d'autres. Ceci ne peut pas être vrai et faux pour la même personne.*
- *"aujourd'hui c'est jeudi". Cet énoncé est vrai le jeudi et faux les autres jours.*

1.1.2 Combinaison des propositions

Nous avons considéré des propositions ou énoncés simples. Nous pouvons convertir des propositions simples à propositions composées en utilisant des connecteurs logiques par exemple : **ET** , **OU** , **NON** , **SI** , **ALORS** , **SI ET SEULEMENT SI** , Dans une combinaison de proposition, les propositions simples sont appelées des composantes. En général, on note les propositions par des lettres minuscules : $p, q, r, \cdots$.

1.1.3 Tables de vérité

La table de vérité c'est ce qui donne la valeur vrai des propositions combinées. Elle a un nombre de lignes et de colonnes. Le nombre de lignes dépend du nombre de propositions simples.

Rémarque 1.1.3.1 *pour n propositions nous avons* 2^n *lignes.*

1.1.4 Equivalence logique

Deux combinaisons de propositions sont dites équivalentes ou égales si elles ont des valeurs vraies identiques. Dans ce cas on utilise les symboles "$\equiv$" ou "$=$".

1.1.5 Conjonction et disjonction

- (a) Conjonction
  Si deux propositions sont combinées par le connecteur " **ET** " pour former une combinaison de proposition alors la combinaison obtenue est appelée conjonction des deux propositions.
  Symbole : si p et q sont deux propositions, alors leur conjonction est dénotée par $p \wedge q$ et se lit " p et q".
  Par exemple : considérons les deux propositions "Il est un grand travailleur" ; " Il est intelligent", la conjonction est : " il est un grand travailleur et intelligent".
  Rémarque 1.1.5.1 *$p \wedge q$ est vraie quand p et q sont toutes vraies et, faux dans les autres cas.*
  Rémarque 1.1.5.2 *Etant données deux propositions logiques p et q, on appelle conjonction de p et q, la proposition logique $p \wedge q$ qui est Vraie quand p et q sont vraies à la fois. Sa table de vérités est donnée par :*
  Table de vérité : ici nous allons adopter $1 = V$, $0 = F$

p	q	$p \wedge q$
1	1	1
1	0	0
0	1	0
0	0	0

- (b) Disjonction
  Si deux propositions sont combinées par le connecteur **OU**. Pour former une combinaison de proposition alors la proposition obtenue est appelée disjonction des propositions p et q.
  Symbole : si p et q sont deux propositions alors leur disjonction est dénotée par $p \vee q$ et se lit "p ou q". Par exemple considérons les deux propositions : " Canon va jouer " ; " Tonnerre va jouer ". La disjonction est "Canon ou Tonnerre va jouer".
  Rémarque 1.1.5.3 *$p \vee q$ est fausse quand p et q sont toutes fausses.*
  Rémarque 1.1.5.4 *Etant données deux propositions logiques p et q, on appelle disjonction de p et q, la proposition logique $p \vee q$ qui est Vraie si l'une des propositions logiques p ou q est vraie. Sa table de vérités est donnée par :*

p	q	$p \vee q$
1	1	1
1	0	1
0	1	1
0	0	0

- (c) **Ou exclusif**
  Dans certains cas nous ne pouvons pas avoir toutes les alternatives, alors **OU** est utilisé dans le sens exclusif.
  Symbole : Nous écrivons **OR** dans le sens exclusif par $\veebar$ Par exemple : si p est une fille, alors p ne peut pas être les deux : fille et garçon Table de vérité.

p	q	$p \veebar q$
1	1	0
1	0	1
0	1	1
0	0	0

.

1.1.6 Négation

Définition 1.1.6.1 *Etant donnée une proposition logique p, on appelle négation de p la proposition logique $\bar{p}$, qu'on note aussi, $\neg p$ qui est fausse quand p est vraie et qui est vraie quand p est fausse.*

Ainsi, pour toute proposition, nous avons une proposition qui est sa négation. La négation n'est pas une proposition contraire mais sa négation.

Symbole : Négation de p se dénote $(\neg p)$ Par exemple si p est "Thomas est un bon garçon " alors $(\neg p)$ est soit "Thomas n'est pas un bon garçon " ou " ce n'est pas le cas que Thomas est un bon garçon".

Rémarque 1.1.6.1 *si p est vrai alors $(\neg p)$ est faux si p est faux alors $(\neg p)$ est vrai.*

Rémarque 1.1.6.2 *Le fait qu'une proposition ne peut prendre que les valeurs 0 ou 1 provient d'un principe fondamental de la logique "classique" qui est : Le principe du tiers exclu, à savoir qu'une proposition logique ne peut pas être vraie et fausse à la fois.*

Rémarque 1.1.6.3 *Pour définir une proposition logique p, il suffit de donner les situations où elle est Vraie, dans le reste des situations la proposition p étant Fausse et inversement si on connait les situations où p est Fausse, dans le reste des situations p est Vraie.*

Table de vérité.

p	$\neg p$
1	0
0	1

.

Propriété 1.1.6.1
- *(i)* $p \wedge p = p$
- *(ii)* $p \vee p = p$
- *(iii)* $p \wedge q = q \wedge p$
- *(iv)* $p \vee q = q \vee p$
- *(v)* $\neg(\neg p) = p$
- *(vi)* $\neg(p \wedge q) = \neg p \vee \neg q$
- *(vii)* $\neg(p \vee q) = \neg p \wedge \neg q$
- *(viii)* $(p \wedge q) \wedge r = p \wedge (q \wedge r)$
- *(ix)* $(p \vee q) \vee r = p \vee (q \vee r)$.

1.1.7 Implication et Bi-Implication (équivalence) de propositions

Implication de propositions

Si p et q sont deux propositions, alors l'énoncé de la forme "si p alors q " est appelée implication de propositions.

Symbole : si p alors q se dénote par $p \Longrightarrow q$ et se lit " p implique q "

Rémarque 1.1.7.1 *$p \Longrightarrow q$ est vrai dans tous les cas sauf quand p est vrai et q est faux.*

Table de vérité

p	q	$p \Longrightarrow q$
1	1	1
1	0	0
0	1	1
0	0	1

.

Propriété 1.1.7.1
- *(i)* $p \Longrightarrow q = \neg p \vee q$

  Solution 1.1.7.1 *On forme le tableau correspondant, on remarque que les deux dernières colonnes sont identiques*

p	q	$\neg p$	$p \Longrightarrow q$	$\neg p \vee q$
1	1	0	1	1
1	0	0	0	0
0	1	1	1	1
0	0	1	1	1

.

- *(ii)* $\neg(p \Longrightarrow q) = p \wedge \neg q$

Equivalence de propositions

Si p et q sont deux propositions, alors la proposition de la forme " p si et seulement si q " est appelée équivalence de propositions. On dit que deux propositions logiques p et q sont logiquement équivalentes, ou équivalentes, si elles ont les mêmes valeurs de vérité. On note : $p \Longleftrightarrow q$.

Symbole : " p si et seulement si q " se note par $p \Longleftrightarrow q$ et se lit comme :
- (a) p si et seulement si q
- (b) p implique q et q implique p
- (c) p nécessaire et q suffisant.

Rémarque 1.1.7.2 *$p \Longleftrightarrow q$ est vrai si p et q ont une même valeur de vérité et faux si p et q ont des valeurs de vérité contraires.*

p	q	$p \Longleftrightarrow q$
1	1	1
1	0	0
0	1	0
0	0	1

.

Propriété 1.1.7.2 $(p \Longleftrightarrow q) \Longleftrightarrow r = p \Longleftrightarrow (q \Longleftrightarrow r)$.

La contraposée

Le travail des scientifiques consiste à établir à partir de certaines données ou hypothèses d'autres propriétés. Si on note p les données ou hypothèses qu'on a et q les propriétés qu'on veut établir, alors tout revient à démontrer que $(p \Longrightarrow q)$ est vraie. Ce qui nous fait dire que la tâche des mathématiques consiste en la démonstration d'implications. Dans certaines situations, il est difficile de montrer directement l'implication $(p \Longrightarrow q)$ alors on essaye de donner une autre proposition équivalente qui pourrait être plus facile à établir.

Propriété 1.1.7.3 *Etant données deux proposotions logiques p et q, alors les propositions suivantes sont équivalentes :*
- $(p \Longrightarrow q)$
- $\overline{q} \Longrightarrow \overline{p}$.

La deuxième implication est appelée **Contraposée** *de la première implication.*

La réciproque

Etant données p et q deux propositions logiques, on appelle la réciroque de l'implication $(p \Longrightarrow q)$ la proposition $(q \Longrightarrow p)$.

Propriété 1.1.7.4 *Etant données trois proposotions logiques p, q et r alors les propositions suivantes sont équivalentes :*

1. $((p \vee q) \vee r) \Longleftrightarrow (p \vee (q \vee r))$ *(assiciativité de $\vee$)*
2. $((p \wedge q) \wedge r) \Longleftrightarrow (p \wedge (q \wedge r))$ *(assiciativité de $\wedge$)*
3. $((p \vee q) \wedge r) \Longleftrightarrow ((p \wedge r) \vee (q \wedge r))$ *(distributivité de $\wedge$ par rapport à $\vee$)*
4. $((p \wedge q) \vee r) \Longleftrightarrow ((p \vee r) \wedge (q \vee r))$ *(distributivité de $\vee$ par rapport à $\wedge$)*
5. $((p \Longrightarrow q) \wedge (q \Longrightarrow r)) \Longrightarrow (p \Longrightarrow r)$. *(transitivité de $\Longrightarrow$)*
6. $(p \Longleftrightarrow q) \Longleftrightarrow ((p \Longrightarrow q) \wedge (q \Longrightarrow p))$.

Démonstration 1.1.7.1 *Nous allons démontrer les propriétés* 3 *et* 5*, le reste est laissée à titre d'exercice.*
Pour montrer le 3 *nous allons utiliser la table de vérité suivante :*

p	q	r	$p \wedge r$	$q \wedge r$	$(p \wedge r) \vee (q \wedge r)$	$p \vee q$	$(p \vee q) \wedge r$
1	1	1	1	1	1	1	1
1	1	0	0	0	0	1	0
1	0	1	1	0	1	1	1
1	0	0	0	0	0	1	0
0	1	1	0	1	1	1	1
0	1	0	0	0	0	1	0
0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0

.

L'équivalence vient du fait que la sixième et huitième colonnes sont identiques.
Pour montrer la propriété 5*, posons que T est la proposition logique $[(p \Longrightarrow q) \wedge (q \Longrightarrow r) \Longrightarrow (p \Longrightarrow r)]$. En utilisant la définition de l'implication et les proriétés associées il vient :*

$$\begin{array}{rcl} T & \Longleftrightarrow & [(p \Longrightarrow q) \wedge (q \Longrightarrow r) \Longrightarrow (p \Longrightarrow r)] \\ & \Longleftrightarrow & [\overline{(p \Longrightarrow q) \wedge (q \Longrightarrow r)} \vee (p \Longrightarrow r)] \\ & \Longleftrightarrow & [\overline{(p \Longrightarrow q)} \vee \overline{(q \Longrightarrow r)} \vee (p \Longrightarrow r)] \\ & \Longleftrightarrow & [\overline{(\overline{p} \vee q)} \vee \overline{(\overline{q} \vee r)} \vee (\overline{p} \vee r)] \\ & \Longleftrightarrow & [(\overline{\overline{p}} \wedge \overline{q}) \vee (\overline{\overline{q}} \wedge \overline{r}) \vee (\overline{p} \vee r)] \\ & \Longleftrightarrow & [(p \wedge \overline{q}) \vee (q \wedge \overline{r}) \vee (\overline{p} \vee r)] \end{array}.$$

Alors, pour montrer que la proposition T est vraie, nous devons montrer que toutes les valeurs de vétité sont égales à 1. Il vient :

p	q	r	$\overline{p} \vee r$	$\overline{q} \wedge p$	$\overline{r} \wedge q$	T
1	1	1	1	0	0	1
1	1	0	0	0	1	1
1	0	1	1	1	0	1
1	0	0	0	1	0	1
0	1	1	1	0	0	1
0	1	0	1	0	1	1
0	0	1	1	0	0	1
0	0	0	1	0	0	1

.

Ce qui montre que la proposition T est vraie et entraine la transitivité de l'implication.

1.1.8 Tautologies et Contradictions

Tautologies

Définition 1.1.8.1 *la tautologie est un énoncé qui est toujours vrai pour toutes les valeurs vraies de ces composantes.*

Considérons par exemple la proposition suivante $p \vee \neg p$. La table de vérité de cette proposition donne :

p	$\neg p$	$p \vee \neg p$
1	0	1
0	1	1

.

On note que les valeurs de vérités de la troisiéme collonne sont égaux à 1.

Contradictions

Définition 1.1.8.2 *la contradiction est un énoncé qui est toujours faux pour toutes les valeurs vraies de ces composantes. Par exemple considérons $p \wedge \neg p$.*

p	$\neg p$	$p \wedge \neg p$
1	0	0
0	1	0

.

On note que les valeurs de vérités de la troisiéme collonne sont égaux à 0.

1.1.9 Arguments

Définition 1.1.9.1 *Un argument est une assertion telle que un énoncé, appelé conclusion fait suite à d'autres énoncés appelés hypothèses.*

Exemple 1.1.9.1 *Considérons les trois énoncés suivants :*

1. *Il travaille dur, il va réussir,*
2. *il n'est pas résultatif,*
3. *là, il n'a pas travaillé.*

Ces trois énoncés pris ensemble constituent un argument. Ici, les deux premiers sont des hypothèses et le dernier est une conclusion.
Supposons que p soit la proposition " il travaille dur", q : la proposition " il est résultatif". L'argument ci dessus peut être écrit :

$$[(p \Longrightarrow q) \wedge \neg q] \Longrightarrow \neg p.$$

Si un argument est une tautologie, alors c'est un argument valide.
Si un argument n'est pas une tautologie, alors ce n'est pas un argument valide.
Un argument est un énoncé tel que les différents énoncés (propositions) $p_1, p_2, \cdots, p_n$ prises ensemble donnent un autre énoncé P.
Symboliquement nous écrivons $p_1, p_2, \cdots, p_n/\text{-}P$. Le symbole " /- " est lu **tourniquet**. Les propositions $p_1, p_2, \cdots, p_n$ sont appelées **prémisses** ou **assumptions** (hypothèses) la proposition P est appelée **conclusion** .
Argument valide : l'argument $p_1, p_2, \cdots, p_n/\text{-}P$ est vrai si P est vraie soit, toutes les fois que les prémisses $p_1, p_2, \cdots, p_n$ sont vraies autrement il est faux.
L'argument vrai est appelé l'argument valide.

Rémarque 1.1.9.1 *$p_1, p_2, \cdots, p_n \rightarrow P$ est une tautologie.*

1.2 Notion d'ensemble et opérations sur les ensembles

1.2.1 Définitions fondamentales

En mathématique, on rencontre de manières différentes une variété d'ensembles. On peut donner des exemples : les sommets d'un polygone régulier ou non, les points d'une droite, l'ensemble des entiers naturels $\mathbb{N}$, l'ensemble des entiers relatifs $\mathbb{Z}$, l'ensembles des rationels $\mathbb{Q}$, l'ensemble des nombres réels $\mathbb{R}$, l'ensembles des nombres complexes $\mathbb{C}$ etc ...
La notion d'ensemble est si générale qu'il est très difficile d'en donner une définition appropriée. Mais, on s'accorde à dire qu'un ensemble est toute collection ou tout assemblage d'objets appelés éléments de l'ensemble.
Il convient de noter que les ensembles sont désignés par des lettres majuscules $A, B, C \cdots$ etc ...alors que les éléments d'un ensemble eux sont désignés par des lettres minuscules $a, b, c \cdots$.

La proposition «l'élément $< a >$ appartient à l'ensemble A» se note symboliquement

$$a \in A \text{ ou } A \ni a.$$

L'écriture

$$a \notin A$$

signifie que l'élément $< a >$ n'appartient pas à A. Si tous les éléments qui constituent A sont dans B on note

$$A \subset B$$

c'est- à -dire que A est un sous ensemble de B.
Si

$$(A \subset B \text{ et } B \subset A) \text{ alors } (A = B).$$

Parfois nous ne savons pas si un ensemble contient des éléments ou non. C'est pourquoi il serait donc logique d'introduire la notion d'ensemble vide, representée par le symbole $\emptyset$ ou $\{\ \}$.

Rémarque 1.2.1.1 *Un ensemble peut être représenté par extension, c'est-à-dire la donn ée explicite des élément de cet ensemble. Par exemple,* $A = \{1, 3, 3, 4, 5, 6, 7, 8, 9, 10\}$. *Où, il peux être représenté par compréhension, c'est-à-dire la donn ée d'une loi ou formule permettant de caractériser les éléments de cette formule.*

1.2.2 Opérations sur les ensembles.

Soient A et B deux ensembles quelconques.

Définition 1.2.2.1 *La* ***réunion*** *ou* ***somme*** *de* A *et* B *est l'ensemble noté* $C = A \cup B$ *et constitué des éléments qui appartiennent au moins à l'un de ces deux ensembles.*

$$C = A \cup B = \{x/x \in A \text{ ou } x \in B\}$$

De manière analogue, on définit la somme ou la réunion d'un nombre fini ou infini (dénombrable) d'ensembles. Si les A_α forment un système d'ensemble alors :

Définition 1.2.2.2 *La* ***somme*** *ou* ***reunion*** *des* A_α *est l'ensemble noté* $C = \cup_\alpha A_\alpha$ *et constitué des éléments qui appartiennent au moins à l'un de ces ensembles.*

Définition 1.2.2.3 *L'* ***intersection*** *de* A *et* B *est l'ensemble noté* $C = A \cap B$ *et constitué des éléments qui appartiennent à la fois à* A *et* B.

$$C = A \cap B = \{x/x \in A \text{ et } x \in B\}$$

De manière analogue, on définit l'intersection d'un nombre fini ou infini (dénombrable) d'ensembles. Si les A_α forment un système d'ensemble alors :

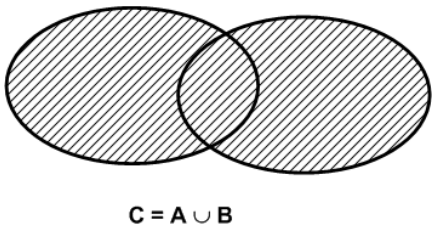


FIGURE 1.1 – $C = A \cup B$

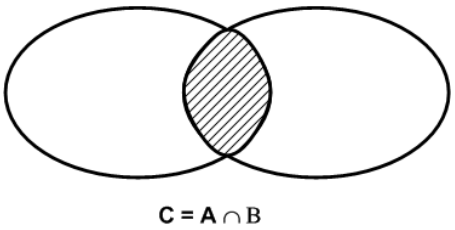


FIGURE 1.2 – $C = A \cap B$

Définition 1.2.2.4 *L' **intersection** des A_α est l'ensemble noté $C = \cap_\alpha A_\alpha$ et constitué des éléments qui appartiennent à la fois à tous ces ensembles.*

Proposition 1.2.2.1 – *La réunion et l'intersection des ensembles sont des opérations commutatives et associatives.*

$$\begin{aligned} A \cup B &= B \cup A \\ A \cap B &= B \cap A \\ (A \cup B) \cup C &= A \cup (B \cup C) \\ (A \cap B) \cap C &= A \cap (B \cap C) \end{aligned} \tag{1.1}$$

– *La réunion et l'intersection des ensembles sont des opérations distributives.*

$$\begin{aligned} (A \cup B) \cap C &= (A \cap C) \cup (B \cap C) \\ (A \cap B) \cup C &= (A \cup C) \cap (B \cup C) \end{aligned} \tag{1.2}$$

Preuve On va montrer que $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.
Montrons d'abord que $(A \cup B) \cap C \subseteq (A \cap C) \cup (B \cap C)$.

$$\begin{aligned} x \in (A \cup B) \cap C &\Rightarrow x \in (A \cup B) \text{ et } x \in C \\ &\Rightarrow (x \in A \text{ ou } x \in B) \text{ et } x \in C \\ &\Rightarrow (x \in A \text{ et } x \in C) \text{ ou } (x \in B \text{ et } x \in C) \\ &\Rightarrow x \in A \cap C \text{ ou } x \in A \cap B \\ &\Rightarrow x \in (A \cap C) \cup (A \cap B) \end{aligned}$$

On démontre de même que $(A \cap C) \cup (B \cap C) \subseteq (A \cup B) \cap C$.

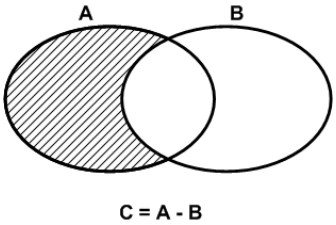


FIGURE 1.3 – $C = A\backslash B$

Définition 1.2.2.5 *On appelle* ***différence*** *de deux ensembles A et B l'ensemble noté $A\backslash B$ constitué des éléments qui, appartiennent à A et non à B*

$$A\backslash B = \{x/x \in A \text{ et } x \notin B\}.$$

Remarque :

$$A \cup B = (A\backslash B) \cup (A \cap B) \cup (B\backslash A).$$

Définition 1.2.2.6 *On appelle* ***différence symétrique*** *de deux ensembles A et B l'ensemble noté $A\Delta B$ et constitué de la collection des éléments qui, appartiennent à A uniquement ou des éléments qui appartiennent à B uniquement*

$$A\Delta B = \{x/x \in A\backslash B \text{ ou } x \in B\backslash A\}$$

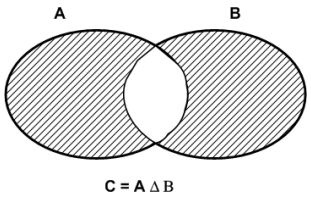


FIGURE 1.4 – $C = A\Delta B$

Remarque :

$$A\Delta B = (A\backslash B) \cup (B\backslash A) = (A \cup B)\backslash(A \cap B)$$

Proposition 1.2.2.2 *P1 :*

$$A\Delta B = B\Delta A \text{ et } (A\Delta B)\Delta C = A\Delta(B\Delta C).$$

P2 :

$$A\Delta\emptyset = A \text{ et } A\delta A = \emptyset$$

P3 :

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

Soit S l'ensemble universel.

Définition 1.2.2.7 *On appelle* ***complémentaire*** *de A (dans S) l'ensemble noté $S\backslash A$ (ou $\overline{A}$ ou A') et constitué des élément qui n'appartiennent pas à A*

$$S\backslash A = \{x/x \notin A\}$$

N.B

$$\overline{S} = \emptyset \text{ et } \overline{\emptyset} = S$$

En théorie des ensembles et des applications, un rôle important est joué par le principe de **dualité**, qui est basé sur les deux égalités suivantes :

$$S\backslash \cup_\alpha A_\alpha = \cap_\alpha (S\backslash A_\alpha)$$

et

$$S\backslash \cap_\alpha A_\alpha = \cup_\alpha (S\backslash A_\alpha)$$

Preuve : On va montrer la première égalité.
Supposons que $x \in S\backslash \cup_\alpha A_\alpha$

$$\begin{aligned} x \in S\backslash \cup_\alpha A_\alpha &\Rightarrow x \notin \cup_\alpha A_\alpha \\ &\Rightarrow x \notin A_\alpha \forall \alpha \\ &\Rightarrow x \in S\backslash A_\alpha \quad \forall \alpha \\ &\Rightarrow x \in \cap_\alpha (S\backslash A_\alpha). \end{aligned}$$

Inversement supposons que $x \in \cap_\alpha (S\backslash A_\alpha)$

$$\begin{aligned} x \in \cap_\alpha (S\backslash A_\alpha) &\Rightarrow x \notin A_\alpha \quad \forall \alpha \\ &\Rightarrow x \notin \cup_\alpha A_\alpha \\ &\Rightarrow x \in S\backslash \cup_\alpha A_\alpha. \end{aligned}$$

d'où le résultat.

Proposition 1.2.2.3

$\forall A, B$ et C les résultats suivants sont vérifiés :

$A \cap A = A$.
$A \cup A = A$.
$A \cap B = B \cap A$.
$A \cup B = B \cup A$.
$(A \cap B) \cap C = A \cap (B \cap C)$.
$(A \cup B) \cup C = A \cup (B \cup C)$.
$A \cap (A \cup B) = A$.
$A \cup (A \cap B) = A$.
$A \cap \emptyset = \emptyset$.
$A \cup \emptyset = A$.
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
$A \cup B = (A \backslash B) \cup (A \cap B) \cup (B \backslash A)$.
$A \cap B = (A \cup B) \backslash ((A \backslash B) \cup (B \backslash A))$.
$A \backslash B = A \backslash (A \cap B)$.
$A = (A \cap B) \cup (A \backslash B)$.
$(A \backslash B) \cap C = (A \cap C) \backslash (B \cap C)$.
$A \Delta B = (A \cup B) \backslash (A \cap B)$.
$A \Delta A = \emptyset,\ A - B = \emptyset \Leftrightarrow A \subseteq B$.
$A \cap (B - C) = (A \cap B) - C,\ \ A - B = (A \cup B) - B = A - (A \cap B)$.
$A \cap B = A - (A - B),\ \ A - (B - C) = (A - B) \cup (A \cap C)$.

$\overline{S} = \emptyset, \overline{\emptyset} = S$
$\overline{A \cup B} = \overline{A} \cap \overline{B}, \overline{A \cap B} = \overline{A} \cup \overline{B}, \overline{\overline{A}} = A$
$\overline{\cap\{A_\alpha / \alpha \in I\}} = \cup\{\overline{A}_\alpha / \alpha \in I\}$
$\overline{\cup\{A_\alpha / \alpha \in I\}} = \cap\{\overline{A}_\alpha / \alpha \in I\}$.

1.2.3 Produit cartésien de deux ensembles.

Définition 1.2.3.1 *On appelle ensemble des parties d'un ensemble A, l'ensemble de tous les sous-ensembles de l'ensemble A y compris l'ensemble vide et A lui-mêmese. L'ensemble des parties de l'ensemble A se note* $\wp(A)$ *et contient* $2^{|A|}$ *éléments.*

Définition 1.2.3.2 *La* ***paire ordonnée*** (a, b) *est l'ensemble* $\{\{a\}; \{a, b\}\}$. *Soit* $(a, b) = \{\{a\}; \{a, b\}\}$.

On voit immédiatement que si $a \neq b$ alors, $(a, b) \neq (b, a)$.

Définition 1.2.3.3 *On appelle* ***produit cartésien*** *des ensembles A et B notés* $A \times B$ *l'ensemble constitué de toutes les pairs ordonnées tel que le premier élément appartiènne au premier ensemble et le second élément appartiènne au second ensemble*

$$A \times B = \{(a, b) / a \in A, b \in B\}$$

De manière analogue

Définition 1.2.3.4 *On défini un* ***triplet ordonné*** *d'éléments* a, b, c *noté* (a, b, c) *par l'ensemble*

$$(a, b, c) = \{\{a\}, \{a, b\}, \{a, b, c\}\}.$$

Par suite

Définition 1.2.3.5 *Le* ***produit cartésien*** *de* A, B, C *est l'ensemble*

$$A \times B \times C = \{(a, b, c)/a \in A, b \in B, c \in C\}.$$

De même, on peut définir un quatriple ordonné par :

$$(a, b, c, d) = \{\{a\}, \{a, b\}, \{a, b, c\}, \{a, b, c, d\}\}.$$

Définition 1.2.3.6 *De manière générale nous pouvons définir le produit cartésien de n ensembles.*
On défini le ***produit cartésien*** *de* $A_{i=\overline{1,n}}$ *comme étant l'ensemble*

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n)/a_i \in A_i \ \ \forall i = 1, -, n\}.$$

si $A_i = A, \ \ \forall i$ *alors,*

$$A_1 \times A_2 \times \cdots \times A_n = \overbrace{A \times A \times \cdots \times A}^{n} = A^n$$

Définition 1.2.3.7 *Tout ensemble constitué d'un nombre fini d'éléments est appelé* ***ensemble fini****.*

Définition 1.2.3.8 *Pour les ensembles finis le nombre de ces éléments est appelé* ***cardinal****. et se note* $\mathbf{card}A$ *ou* $|A|$*si l'ensemble est A.*

Chapitre 2

APPLICATIONS ET FONCTIONS

The most distinct and beautiful statements of any truth must take at last the mathematical form. We might so simplify the roles of moral philosophy, as well as of arithmetic, that one formula would express them both.

H. D. THOREAU

2.1 Applications et fonctions

Définition 2.1.0.9 *Soient X, Y deux ensembles. L'application f de l'ensemble X vers Y ($f : X \to Y$) est la loi qui à chaque élément $x \in X$ fait correspondre exactement un élément $y \in Y$.*

X sera l'ensemble de départ de f et Y l'ensemble d'arrivée de f
Au niveau universitaire, les termes fonction, application, opérateur et transformation sont des synonymes. Mais toute fois dans certain cas, nous distinguerons la notion d'application à celle de fonction en disant qu'une fonction est toute correspondance qui fait associer à chaque élément de l'ensemble de départ au plus ou au moins un élément dans l'ensemble d'arrivé
Les notations suivantes :

$$f : X \to Y \qquad x \to^f y \qquad y = f(x) \qquad \forall x \in X$$

signifient que f est une fonction de X vers Y.

Définition 2.1.0.10 *On appelle digramme Sagittal tout schéma permettant de représenter une application, fonction ou bien une relation*

Définition 2.1.0.11 *L'élément y de Y dont l'application f fait correspondre un élément x de X est appelé* ***image*** *de x par f. L'ensemble X est appelé* ***domaine de définition*** *de f et se note $D(f)$ alors que, Y est l'****ensemble d'arrivée****.*

Définition 2.1.0.12 *L'ensemble*

$$R(f) = \{y / \exists x \in D(f) \quad f(x) = y\}$$

est encore appelé ***ensemble des valeurs*** *de l'application f ou* ***ensemble image****.*

Définition 2.1.0.13 *Les fonctions $f_1 : X_1 \to Y_1$ et $f_2 : X_2 \to Y_2$ sont égales si et seulement si*

- $X_1 = X_2$
- $\forall x \in X_1 \quad f_1(x) = f_2(x)$

et on note alors que $f_1 = f_2$

Supposons $f : X \to Y$ et qu'il existe $X_0 \subset X$. Définnissons la fonction $f_0 : X_0 \to Y$ en posant $\forall x \in X_0 \qquad f_0(x) = f(x)$.

Définition 2.1.0.14 *La fonction f_0 est appelé **restriction** de la fonction f sur X_0, et la fonction f le **prolongement** de f_0 sur X.*

Soit f une application $f : X \to Y, A \subseteq X$ et $B \subseteq Y$.

Définition 2.1.0.15 *L'ensemble*

$$\begin{aligned} f(A) &= \{y/\exists x \in A : f(x) = y\} \\ &= \{f(x)/x \in A\} \end{aligned}$$

*est appelé **ensemble image** par f de l'ensemble A.*

Définition 2.1.0.16 *L'image réciproque d'un ensemble B par la fonction f est l'ensemble noté $f^{-1}(B)$ et défini par :*

$$f^{-1}(B) = \{x/\exists y \in B : f(x) = y\}$$

N.B :

$$f(A) \subseteq Y \text{ et } f^{-1}(B) \subseteq X$$

Théorème 2.1.0.1 *Pour une fonction donnée l'image réciproque de la réunion de deux ensembles est égale à la somme des images réciproques de ces deux ensembles :*

$$f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$$

Preuve : Soit $x \in f^{-1}(A \cup B)$. Montrons que $x \in f^{-1}(A) \cup f^{-1}(B)$.

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

Maintenant supposons l'inverse.

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

Ce qu'il fallait démontrer.

Rémarque 2.1.0.1 *De manière générale, soient donnée une collections d'ensembles* A_i, $\forall i$, *alors*

$$f^{-1}(\bigcup_i A_i) = \bigcup_i f^{-1}(A_i)$$

Théorème 2.1.0.2 *Pour une fonction ou application donnée, l'image réciproque de l'intersection de deux ensembles est l'intersection de ces des images réciproques de ces deux ensembles*

$$f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$$

Preuve : La preuve est laissée au lecteur. La démarche à suivre est identique à la précédente.

Rémarque 2.1.0.2 *De manière générale, soient donnée une collections d'ensembles* A_i, $\forall i$, *alors*

$$f^{-1}(\bigcap_i A_i) = \bigcap_i f^{-1}(A_i)$$

Théorème 2.1.0.3 *Pour une fonction donnée l'image de la somme (ou réunion) est la somme des images*

$$f(A \cup B) = f(A) \cup f(B)$$

Preuve : Laissée comme exercice.

Rémarque 2.1.0.3 *De manière générale, soient donnée une collections d'ensembles* A_i, $\forall i$, *alors*

$$f(\bigcup_i A_i) = \bigcup_i f(A_i)$$

Remarque : L'image de l'intersection de deux ensembles, ne coïncide pas toujours avec l'intersection des images.

$$f(A \cap B) \neq f(A) \cap f(B)$$

mais

$$f(A \cap B) \subset f(A) \cap f(B)$$

Rémarque 2.1.0.4 *De manière générale, soient donnée une collections d'ensembles* A_i, $\forall i$, *alors*

$$f(\bigcap_i A_i) \subseteq \bigcap_i f(A_i)$$

Définition 2.1.0.17 *Soit f une application de X vers Y.*
Le ***graphe*** *de la fonction f est l'ensemble noté $\boldsymbol{G}(f)$ defini par*

$$\boldsymbol{G}(f) = \{(x, y) \in X \times Y / x \in X, y = f(x)\}$$

ou bien

$$\boldsymbol{G}(f) = \{(x, f(x)) \in X \times Y / f(x) = y \in Y\}$$

Remarque :

$$\mathbf{G}(f) \subseteq X \times Y$$

Définition 2.1.0.18 *Soient les fonctions*

$$f : X \to Y \text{ et } g : Y \to Z.$$

La fonction $h : X \to Z$ *définie par la formule*

$$h(x) = g(f(x)) \qquad \forall x \in X$$

est appelée ***composition*** *ou* ***superposition*** *des fonctions* f *et* g.

Proposition 2.1.0.1 *Quelles que soient les applications*

$$f : X \longrightarrow Y,\ g : Y \longrightarrow Z,\ h : Z \longrightarrow T,$$

on a l'égalité

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Cette proposition permet de définir de manière générale l'expression suivante

$$f_1 \circ \cdots \circ f_n$$

Définition 2.1.0.19 *L'application* $f : X \to Y$ *est dite* ***surjective*** *si*

$$\forall y \in Y, \exists x \in X : f(x) = y.$$

Définition 2.1.0.20 *L'application* $f : X \to Y$ *est dite* ***injective*** *si*

$$\forall x_1 \in X, x_2 \in X \text{ tels que } x_1 \neq x_2 \Rightarrow \begin{cases} x_1 \neq x_2 & \Rightarrow \quad f(x_1) \neq f(x_2) \\ & ou \\ f(x_1) = f(x_2) & \Rightarrow \quad x_1 = x_2 \end{cases}$$

Définition 2.1.0.21 *L'application* $f : X \to Y$ *est dite* ***bijective*** *si elle est surjective et injective. Dans ce cas on dit que* f *est une* ***correspondance biunivoque*** *entre* X *et* Y.

Supposons que f est une application bijective de X vers Y. Alors

$$\forall y \in Y, \exists! x \in X : f(x) = y.$$

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

Définition 2.1.0.22 *La fonction* $f^{-1} : Y \to X$ *est appelée la* ***fonction réciproque*** *de* f.

Proposition 2.1.0.2 *Soient* X *et* Y *des ensembles non vides et* f *une application de* X *dans* Y. *Les propriétés suivantes sont équivalentes :*

– *(i) f est injective,*
– *(ii) il existe une application g de Y dans X telle que $g \circ f$ soit l'application identique de X dans X.*

Proposition 2.1.0.3 *Soient X et Y des ensembles non vides et f une application de X dans Y. Les propriétés suivantes sont équivalentes :*
– *(i) f est surjective,*
– *(ii) il existe une application h de Y dans X telle que $f \circ h$ soit l'application identique de Y dans Y.*

Proposition 2.1.0.4 *Soient X et Y des ensembles non vides et f une application de X dans Y. Les propriétés suivantes sont équivalentes :*
– *(i) f est bijective,*
– *(ii) il existe une application g et h de Y dans X telle que l'on ait $g \circ f = Id_X$ et $f \circ h = Id_Y$.*

De plus, si ces conditions sont vérifiées, les applications g et h sont uniques et coincident.

Définition 2.1.0.23 *Une application $f : \mathbb{N} \to X$ est appelée **suite** d'éléments de X. Cette suite sera représentée par $\{a_0, a_1, \ldots, a_n, \cdots\}$ ou par $(a_n)_{n\geq 1}$ on a $a_n = f(n)$.*

Chapitre 3

EQUIVALENCE ENTRE LES ENSEMBLES : NOTION DE PUISSANCE DES ENSEMBLES

3.1 Ensembles finis et infinis

De nos jours, il est impossible de faire quoi que ce soit en mathématiques sans utiliser la théorie des nombres entiers. Cet ensemble a toujours été considérer comme le point de départ de la construction des autres ensembles. Comme le disait Dedekind en son temps : **Dieu nous a donné les nombres entiers, tout le reste est l'œuvre de l'homme** En considérant la plus part des ensembles, on note que, parfois on peut déterminer le nombre d'éléments dans cet ensemble ; par exemple, le nombre de sommets dans un polygone, le nombre des nombres premiers dans un sous ensemble fini de $\mathbb{N} \cdots$ etc, $\cdots$ D'un autre côté, il existe des ensembles constitués d'un nombre infini d'éléments. Par exemple les ensembles usuels des nombres comme $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q} \cdots$ etc $\cdots$ ou l'ensemble de tous les points situés sur une droite, sur un cercle, dans un plan ou des polynômes ayant des coefficients rationnels. Dans ces cas on dit que l'ensemble est infini ; ayant en vue l'idée que de cet ensemble on peut retirer un élément, deux élément, mais après chaque retrait, il en reste toujours un nombre «considérable» d'éléments. On peut comparer deux ensembles finis par leur nombre d'éléments et dire s'il est le même ou pas soit conclure s'ils sont égaux ou non. La question que l'on se pose ici est de savoir si on peut le faire dans le cas des ensembles infinis ; ou bien la question de savoir lequel des ensembles est plus grand entre l'ensemble des cercles dans le plan ou l'ensemble des points des nombres rationnels dans une droite ou encore l'ensemble des fonctions définies dans le segment $[0, 1]$

Regardons par exemple comment on compare deux ensembles finis. On peut par exemple dans un premier temps constituer les éléments de chaque ensemble en suite les comparer mais on peut aussi s'en prendre autrement, en essayant d'établir si possible une bijection, c'est-à - dire une correspondance biunivoque entre les éléments de ces ensembles. Il est à noter que la correspondance biunivoque entre

deux ensemble finis peut être établi si et seulement si, ils ont le même nombre d'éléments. Par exemple, en prenant le cas d'une salle de classe, pour verifier qu'il y a le même nombre entre un groupe d'étudiants et l'ensemble des bancs, il faut tout simplement faire asseoir les étudiants. S'il ne reste pas de bancs vides et aucun étudiant debout c'est-à - dire si la bijection est établie entre ces deux ensembles, cela voudrait dire que le nombre d'éléments entre ces deux ensembles est égal. Dans le cas des ensembles infinis, la seule manière de comparer les ensembles est de pouvoir établir une bijection.

3.2 Ensembles denombrables

Parmi les ensembles infinis, le plus simple est l'ensemble des entiers naturels auquel nous allons rattacher la notion de dénombrabilité. On dira qu'un ensemble est dénombrable s'il est en bijection avec $\mathbb{N}$. En d'autre termes, un ensemble dénombrable est celui qui est constitué d'éléments que l'on peut numéroter comme une suite infinie $a_1, a_2, \ldots, a_n, \ldots$

3.2.1 Exemples

1. On peut établir une bijection entre $\mathbb{N}$ et $\mathbb{Z}$.
   En disposant les éléments de $\mathbb{Z}$ de manière á commencer par 0 et chaque successeur accompagné de son opposé comme l'indique les lignes suivantes :
   $0, \quad -1, \quad 1, \quad -2, \quad 2, \quad \ldots$
   $1, \quad 2, \quad 3, \quad 4, \quad 5, \quad \ldots$
   Si $n \geq 0$ les nombres impairs vont correspondre de la manière suivante $n \longleftrightarrow 2n+1$
   Si $n \leq 0$ les nombres pairs vont correspondre de la manière suivante $n \longleftrightarrow 2|n|$.
2. Dénombrement de l'ensemble de tous les pairs positifs $n \longleftrightarrow 2|n|$.
3. Dénombrement de l'ensemble de toutes les pussances de 2
   $2, 4, 8, \ldots, 2^n$ correspondant de la manière suivante $n \longleftrightarrow 2^n$.

Considérons un exemple plus complexe. Montrons que l'ensemble des nombres rationnels est dénombrable. Nous savons que chaque nombre rationnel peut s'écrire sous la forme $\alpha = \frac{p}{q} : \quad q > 0$. Désignons par la somme $|p| + q$ la «hauteur» du nombre rationnel α. Il est clair que le nombre des rationnels (fractions) ayant pour hauteur n est fini. Par exemple avec pour hauteur :

1	nous avons	$0/1$
2	nous avons	$1/1, -1/1$
3	nous avons	$2/1, 1/2, -2/1$
...		
etc.		

Nous allons énumerer tous les rationnels par rapport à leur hauteur. Ainsi pour hauteur 1 nous appellons 1., pour hauteur 2 ; 2, pour hauteur 3 ; 3, ainsi de suite ...Nous remarquerons que chaque rationnel sera lié à un numéro et nous allons établir une correspondance entre $\mathbb{N}$ et $\mathbb{Q}$.

Rémarque 3.2.1.1 *Les ensembles infinis qui ne sont pas dénombrables sont dit non dénombrables.*

Proposition 3.2.1.1 *Tout sous ensemble d'un ensemble dénombrable est soit fini ou dénombrable.*

Preuve : Supposons A dénombrable et $B \subset A$. Enumerons les élements de A par : $a_1, a_2, \ldots, a_n, \ldots$ Supposons $a_{n_1}, a_{n_2}, \ldots, a_{n_n}, \ldots$ ceux d'entre eux qui sont dans B. Si parmi les $n_1, n_2, \ldots$ il y' a un plus grand et fini alors, B est fini dans le cas contraire, B est infini, ce qui achève la preuve.

Proposition 3.2.1.2 *La reunion d'un nombre fini ou dénombrable d'ensermbles dénombrables est dénombrable.*

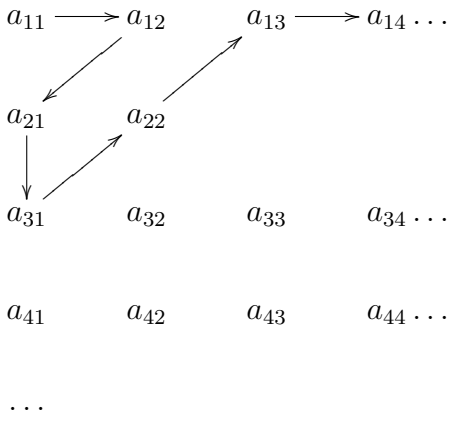
Preuve : Supposons $A_1, A_2, \ldots, A_n, \ldots$ des ensembles dénombrables. Nous allons supposer qu'ils sont deux à deux disjoints dans le cas contraire nous allons considerer la suite suivante :

$$A_1, \quad A_2 \setminus A_1, \quad A_3 \setminus (A_1 \cup A2) \ldots$$

chacun d'entre eux qui peut être dénombrable. Nous allons représenter les éléments de A_n par :

$$A_n = \{a_{n_1}, a_{n_2}, \ldots, a_{n_n}, \ldots\} \tag{3.1}$$

et la reunion $\bigcup_{n=1}^{\infty} A_n$ est l'ensemble constitué des éléments du tableau



que nous pouvons énumerer dans l'ordre indiqué par les flèches, d'où la preuve.

Proposition 3.2.1.3 *Tout ensemble infini contient un ensemble dénombrable.*

Preuve : Supposons M un ensemble infini, choisissons $a_1 \in M$. Puisque M est infini, on peut trouver a_2 different de a_1 ensuite a_3 different de a_1 et a_2. On continue ce processus qui ne va pas s'arrêter si non M est fini. Nous obtenons alors

$$A = \{a_1, a_2, \ldots, a_n, \ldots\} \tag{3.2}$$

3.3 Equivalence entre ensembles

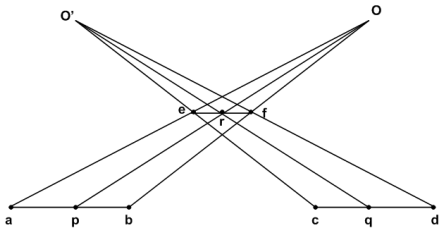
Définition 3.3.0.1 *Deux ensembles M et N sont appellés équivalents et noté ; $(M \sim N)$ s'il existe une correspondance biunivoque entre les éléments de ces ensembles.*

La notion déquivalence peut être employée sur n'importe quel ensemble. Par exemple, deux ensembles finis sont équivalents si et seulement si ils ont même nombre déléments ou même cardinal. Ainsi, la définition d'un ensemble dénombrable peut être formulée de la manière suivante :
Un ensemble est appellé ensemble dénombrable s'il est équivalent à l'ensemble des nombres naturels.

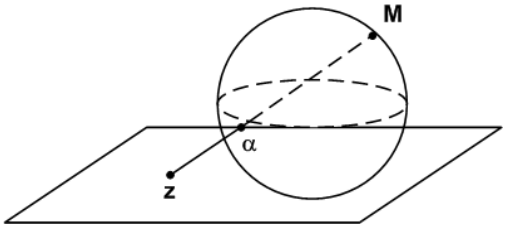
3.3.1 exemples

1. L'ensemble des points sur deux segments quelconque $[a, b]$ et $[c, d]$ sont équivalents entre eux.

   Il est clair que l'on peut établir une bijection entre eux. En effet les points p et q correspondent réciproquement s'ils sont des projections d'un même point r pris dans un intervalle temoin de reférence $[e, f]$.



2. L'ensemble des points dans le plan complexe est équivalent à l'ensemble des points sur la sphère. La bijection $\alpha \leftrightarrow z$ peut être établie à partir de la projection stériographique



3. L'ensemble de tous les nombres de l'intervalle $]0, 1[$ est équivalent à l'ensemble de tous les points sur la droite numérique réelle. La correspondance entre ces ensembles peut être établie à partir de la fonction $y = \frac{1}{\pi} \arctan x + \frac{1}{2}$.

Suite aux exemples que nous venons de donner, nous pouvons noter que, parfois les ensembles infinis peuvent être équivalents à leur sous ensembles propres. Par exemple, l'ensemble des nombres naturels à le même nombre déléments que l'ensemble des entiers relatifs et même que l'ensemble des nombres rationnels. De même l'intervalle $]0, 1[$ à même nombre de points que la droite numérique ...etc

... Ce phénomène est caractéristique aux ensembles infinis. En effet, nous avons montrer que, de chaque ensemble infini M, on peut extraire un sous ensemble dénombrable. Soit $A = \{a_1, a_2, \ldots, a_n, \ldots\}$ ce sous ensemble. séparons le en deux sous ensembles dénombrables.

$$A_1 = \{a_1, a_3, a_5 \ldots, a_{2k-1}, \ldots\} \text{ et } A_2 = \{a_2, a_4, a_6 \ldots, a_{2k}, \ldots\}$$

et établissons une correspondance entre A et A_1. Cette correspondance peut être prolongée jusqu'à la correspondance entre $M = A \cup (M \setminus A)$ et $A_1 \cup (M \setminus A) = M \setminus A_2$, c'est - à - dire rapportant chaque élément de $M \setminus A$ ce même élément. L'ensemble $M \setminus A_2$ ne coincide pas avec M c'est - à - dire est un sous ensemble propre de M. Nous avons ainsi obtenu le resultat suivant :

Proposition 3.3.1.1 *Chaque ensemble infini peut être équivalent à son sous ensemble propre. Ceci peut être pris pour définition d'ensemble propre.*

3.3.2 Non dénombrabilité de l'ensemble des nombres réels

Nous avons donné des exemples des ensembles dénombrables, leur nombre n'étant pas exhaustif. D'autre part, nous avions montré que la reunion d'un nombre fini ou dénombrable d'ensembles dénombrables est dénombrable. Il apparaît naturellement la question suivante : **est ce qu'il existe des ensembles non dénombrables ?** Le théorème suivant donne une réponse positive.

Théorème 3.3.2.1 *L'ensemble des nombres réels compris entre* 0 *et* 1, *soit le contenu du segment* $[0, 1]$, *est non-dénombrable.*

Preuve : Supposons qu'il existe un ensemble dénombrable de nombres réel α dans le segment $[0, 1]$ et énumerons les par :

$$\left.\begin{array}{lcr} \alpha_1 & = & 0, a_{11}a_{12}a_{13} \ldots a_{1n} \ldots \\ \alpha_2 & = & 0, a_{21}a_{22}a_{23} \ldots a_{2n} \ldots \\ \alpha_3 & = & 0, a_{31}a_{32}a_{33} \ldots a_{3n} \ldots \\ \ldots & \ldots & \ldots \\ \alpha_n & = & 0, a_{n1}a_{n2}a_{n3} \ldots a_{nn} \ldots \\ \ldots & \ldots & \ldots \end{array}\right\} \quad \sharp$$

Ici, a_{ik} est le k^{eme} chiffre décimal du nombre α_i. Construisons

$$\beta = 0, b_1 b_2 \ldots b_n \ldots$$

Par la procedure diagonale de Kantor ; c'est-à-dire par
- b_1 nous prenons un chiffre qui ne correspond pas avec a_{11},
- b_2 nous prenons un chiffre qui ne correspond pas avec a_{22},
- ...
- b_n nous prenons un chiffre qui ne correspond pas avec a_{nn},
- ...

En effet
$\alpha_1 \neq \beta$ car $b_1 \neq a_{11}$
$\alpha_2 \neq \beta$ car $b_2 \neq a_{22}$
d'une manière générale β est different de tous les α_i énumerés au $\sharp$ car $b_n \neq a_{nn}$. Nous avons donc trouvé un chiffre qui appartient à $[0, 1]$ mais, qui ne coincide avec aucun des chiffres qui ont été énumérés. La contradiction obtenu montre que les éléments de $[0, 1]$ ne peuvent être énumérés.

Théorème 3.3.2.2 *(De Kantor-Bernstein)*
Soient A et B deux ensembles quelconque. S'ils existent une application bijective f entre A et un sous- ensemble B_1 de B d'une part et une application bijective g entre B et un sous ensemble A_1 de A d'autre part alors, A et B sont équivalents.

Ce théorème peut être encore énoncé de la manière suivante : étant donné deux ensembles A et B, s'il existe une injection de A dans B et une injection de B dans A alors ces deux ensembles sont équipotents. Ce théorème a été conjecturé par Kantor en 1876 et, démontré par Bernstein en 1897. Ce théorème a un énoncé intuitivement simple même quand les ensembles A et B sont des ensembles finis. Nous conseillons 'a tout lecteur de reflechir vivement pour s'en convaincre. Le but étant d'établir le théorème et non de le justifier.

Démonstration 3.3.2.1 *:Sans se restreindre à la généralité, nous pouvons considerer que $A \bigcap B = \emptyset$. Soit x un élément quelconque de A. Posons $x = x_0$ et définissons la suite $\{x_n\}$ de la manière suivante :*
Supposons x_n deja défini alors si n est pair alors pour x_{n+1} on prend un élément de B qui verifie la condition $g(x_{n+1}) = x_n$ (si un tel élément existe bien sur). Mais si n est impair alors, x_{n+1} est un élément de A qui, vérifie la condition $f(x_{n+1}) = x_n$ (s'il existe biensûr).
Deux possibilités existent :

1. *si pour un certain n l'élément x_{n+1}, vérifiant les conditions données n'existe pas., alors le nombre n sera appellé l'ordre de l'élément x,*
2. *si la suite $\{x_n\}$ est infinie, alors x est appellé élément d'ordre infini.*

Décomposont maintenant A en trois ensembles A_E constitué d'éléments d'ordre pair, A_0-ensemble constitué d'éléments d'ordre impair et A_I-ensemble de tous les éléments d'ordre infini. De la même manière nous décomposons B. Nous notons que f fait correspondre A_E sur B_0 et A_I sur B_I et g^{-1} fait correspondre A_0 sur B_E. Ainsi la correspondance biunivoque Ψ qui coincide avec f sur $A_E \bigcup A_I$ et avec g^{-1} sur A_0 est la correspondance biunivoque qui fait correspondre A avec tout B.

3.3.3 Notion de puissance d'ensemble

Si deux ensembles finis sont équivalent alors, ils sont constitués d'un même nombre d'éléments. Si deux ensembles sont équivalents alors, on dit qu'ils ont une même puissance. Ainsi la puissance d'ensemble est ce dont les ensembles équivalents ont en commun. La puissance de l'ensemble $\mathbb{N}$ est $\aleph_0$(aleph-zéro) alors que la puissance du segment [0.1] est appellée la puissance du continu. Il se note c ou $\aleph_1$. La

question fondamentale de l'existence d'une puissance comprise entre $\aleph_0$ et c sera discutée dans la suite.
Soit A et B deux ensembles quelconques et $m(A)$ et $m(B)$ leur puissances respectives. Nous pouvons avoir les situations suivantes :

1. A est équivalent à une partie de B et B est équivalent à une partie de A.
2. A contient une partie équivalente à B mais B ne contient pas de partie équivalente à A.
3. B contient une partie équivalente à A mais A ne contient pas de partie équivalente à B.
4. aucun des ensembles A et B n' a pas de partie équivalente.

Dans le premier cas, avec le théorème de Kantor - Bernstein nous avons $m(A) = m(B)$. Dans le deuxième cas $m(A) > m(B)$ et le troisième cas $m(A) < m(B)$ par contre dans le quatrième cas, on dira que ces puissance ne sont pas comparables. Nous pouvons conclure que, à chaque deux ensembles A et B, on peut dire soit $m(A) = m(B)$ ou $m(A) > m(B)$ ou $m(A) < m(B)$.
Nous avons noté plus haut que les ensembles dénombrables sont les plus «petits» des ensembles infinis (ou forment une petite classe par rapport aux ensembles infinis)et, nous avons montré qu'il existe des ensembles qui ont la puissance du continu. Il apparaît logiquement une question : *est ce qu'il existe des puissances infinies qui dépasseraient la puissance du continu ?*
Le théorème suivant est verifié.

Théorème 3.3.3.1 *Soit M un ensemble quelconque et soit $\mathcal{M}$, l'ensemble des éléments qui sont les sous ensembles de l'ensemble M. Alors la puissance de $\mathcal{M}$, est plus grande que la puissance de M.*

Rémarque 3.3.3.1 *Nous allons noter que, la puissance de $\mathcal{M}$ est 2^m oú m est la puissance de M. On voit que $m < 2^m$. Si $m = \aleph_0$ alor, $\aleph_0 < 2^{\aleph_0}$. On montre que, $\aleph_1 = c = 2^{\aleph_0}$ et, ceci sera appellé plus tard la puissance du continu*

3.4 Ensembles Ordonnés : Nombres transfinites

3.4.1 Ensembles partiellement ordonnés

Soit M un ensemble et $\mathcal{R}$ une relation binaire définie dans M c'est - à dire la donnée d'un sous ensemble $T_{\mathcal{R}} \subset M \times M$. Nous dirons que cette relation est partiellement ordonnée si elle vérifie les propriètés suivantes :

1. Reflexivité : $\forall x \in M, \quad x\mathcal{R}x$.
2. Anti-symétrie :$\forall x, y \in M$ si $x\mathcal{R}y$ et $y\mathcal{R}x$ alors $x = y$.
3. Transitivité :$\forall x, y, z \in M$ si $x\mathcal{R}y$ et $y\mathcal{R}z$ alors $x\mathcal{R}z$.

Rémarque 3.4.1.1 *Nous disons que l'expression partiellement ordonnée ici utilisée est dans le sens algébrique propre. Mais en Analyse on parle tout simplement de relation d'ordre dans le cas où ces propriètés ou axiomes sont vérifiés.*

La notion d'ordonnencement partielle se note par le symbole $\leq$. Ainsi l'écriture $x \leq y$ veut dire que la paire (x, y) appartient à l'ensemble $T_{\mathcal{R}}$. Nous dirons de l'élément x qu'il ne dépasse pas y ou qu'il est surbordonné à y. L'ensemble dans lequel est définie une relation partiellement ordonnée est appellé ensemble partiellement ordonné.

Exemple d'ensembles partiellement ordonnés

1. Tout ensemble peut être considéré trivialement comme ensemble partiellement ordonné si nous introduisons la relation $x \leq y \Longleftrightarrow x = y$.
2. Soit M l'ensemble de toute les fonctions continues dans l'ensemble $[\alpha, \beta]$ la relation peut être posée par exemple comme $f \leq g \Longleftrightarrow f(t) \leq g(t) \quad \forall t \in [\alpha, \beta]$.
3. L'ensemble des sous ensembles d'un ensemble peut être vue comme ensemble partiellement ordonné par l'inclusion $M_1 \leq M_2 \Longleftrightarrow M_1 \subseteq M_2$.
4. L'ensemble des nombres naturels, par la relation $x \leq y \Longleftrightarrow y$ est divisible sans reste par x.

Soit M un ensemble partiellement ordonné. Dans le cas où $x \leq y$ et $x \neq y$ nous allons utiliser la relation $<$, c'est - à -dire $x < y$ et dire x est plus petit que y ou x est strictement subordonné à y. Similairement à partir de la relation $x \leq y$ nous allons utiliser la notation équivalente $x \geq y$ et dire que y n'est pas plus petit que x, dans le cas où $y \neq x$ nous dirons que y est plus grand que x, ou y succède à x.

– l'élément x est dit maximal si de $x \leq y \Rightarrow y = x$.
– l'élément x est dit minimal si de $z \leq x \Rightarrow z = x$.

3.4.2 Applications ou fonctions conservant l'ordre

Soient M et M' deux ensembles partiellement ordonnés et soit f une application de M vers M'. Nous dirons que cette application conserve l'ordre si $x \leq y$ ou $x, y \in M$ entraine que $f(x) \leq f(y)$ dans M'. L'application f est appellé isomorphisme d'ensembles partiellement ordonnés M et M' si elle est bijective et la relation $f(x) \leq f(y)$ est verifiée dans le cas où $x \leq y$. On dira alors que les ensembles M et M' sont isomorphes.

3.4.3 Type d'ordre ou ordinal et ensemble ordonné

Par isomorphisme d'ensembles partiellement ordonnés nous allons dire que les ensembles ont le même type d'ordre. Ainsi le type d'ordre est ce qui appartient á tous les ensembles partiellement ordonnés qui sont isomorphes. De même que la puissance des ensembles est ce qui est générale ou commun dans le cas des ensembles qui sont quivalents entre eux. Soit x et y deux éléments dans un ensemble partiellement ordonné. Il peut arriver que, aucune des relations suivantes, ne soit vérifiée $x \leq y$ et $y \leq x$. Dans ce cas on dit que x et y ne sont pas comparables. Dans un ensemble, s'il n'existe pas des éléments non comparables alors, on dit que cet ensemble est ordonné. Noter que le type d'ordre dans le cas de l'ensemble des entiers naturels est noté ω.

3.4.4 Somme ordonnée des ensembles ordonnés

Soient M_1 et M_2 deux ensembles disjoints avec pour ordinaux θ_1 et θ_2 respectivement. Dans la reunion $M_1 \bigcup M_2$ nous pouvons introduire l'ordre en considérant que, : deux éléments de M_1 sont ordonnés comme dans M_1, deux éléments de M_2 sont ordonnés comme dans M_2. Et que chaque élément de M_1 precède chaque élément de M_2. Nous laissons le soin au lecteur de montrer que c'est une relation d'ordre. Un tel ensemble ordonné sera appellé somme ordonnée des ensembles ordonnés M_1 et M_2 et noteé $M_1 + M_2$. Il est à noter que le plus important est l'ordre des termes sommés. Nous remarquerons que $M_1 + M_2$ n'est pas en général isomorphe à $M_2 + M_1$. Le type d'ordre de la somme $M_1 + M_2$ nous allons l'appeler la somme des types d'ordre θ_1 et θ_2 et noter $\theta_1 + \theta_2$

Rémarque 3.4.4.1 *La définition telle que donnée si dessus peut être étendue à une suite d'ensembles ayant pour ordres $\theta_1, \ldots, \theta_n$ respectivement.*

Exemples

1. Considérons deux ensembles de types d'ordre ω et n alors, leur somme correspondante $n + \omega = \omega$. Par contre $\omega + n \neq \omega$. En effet, si à gauche de l'ensemble des nombres naturels nous ajoutons un nombre fini d'élements alors, nous obtenons le type d'ordre ω.
2. Pour être plus précis, ω est l'ordinal de $\mathbb{N}$ muni de son ordre usuel.

$$\omega = \{1, 2, 3, \ldots\} \Rightarrow \omega + 1 = \{1, 2, 3, \ldots, \omega\}$$

$$\omega + 2 = \{1, 2, 3, \ldots, \omega, \omega + 1\}$$

nous voyons que $1 + \omega = \omega$ mais $\omega + 1 \neq \omega$.

3.4.5 Ensemble totalement ordonné :nombres transfinites

Définition 3.4.5.1 *Un ensemble ordonné est appellé totalement ordonné si chaque sous-ensemble non vide contient un plus petit élément, c'est-à-dire un élément qui precède tous les éléments de ce sous ensemble au sens de la relation d'orde.*

Si l'ensemble ordonné est fini alors il est totalement ordonné. L'exemple d'ensemble ordonné mais qui n'est pas totalement ordonné est le segment $[0, 1]$. Cet ensemble contient un plus petit élément qui est 0. Mais, $]0, 1]$ est un sous-ensemble de $[0, 1]$ qui ne contient pas de plus petit élément.

Rémarque 3.4.5.1 *Chaque sous ensemble non vide d'un ensemble totalement ordonné est totalement ordonné.*

Le type d'ordre, dans le cas des ensembles totalement ordonnés, est appellé type d'ordre transfinite ou tout simplement transfinite qui est tout simplement son ordinal. L'ensemble des entiers naturels avec l'ordre naturel a pour nombre transfinite ou ordinal ω.

Par exemple $\omega + k$ sera aussi un type d'ordre pour l'ensemble

$$\{1, 2, \ldots, n, \ldots, a_1, a_2, \ldots, a_k\}.$$

Mais l'ensemble $\{\ldots, -n, \ldots, -3, -2, -1\}$ est ordonné mais pas totalement par ce qu'il n' y a pas de plus petit élément.

La suite $\omega + n, \quad \omega + \omega, \quad \omega + \omega + n, \quad \omega + \omega + \omega \ldots$ etc sont des nombres transfinites(dans ce cas, on peut construire des ensembles qui satisfont à de tels nombres transfinites.)

Rémarque 3.4.5.2 *A côté de la somme on peut introduire la notion de produit* $\theta = \theta_1 \cdot \theta_2$

Nous laissons le soin au lecteur de faire cette construction.

Proposition 3.4.5.1 *La somme ordonnée d'un nombre fini d'ensembles totalement ordonnés est totalement ordonnée.*

Conséquence 3.4.5.1 *La somme ordonnée des nombres ordinaux est un nombre ordinal.*

Nous noterons que $\omega + \omega = \omega \cdot 2, \quad \omega + \omega + \omega = \omega \cdot 3$

A titre d'exercice, construire les ensembles qui ont pour ordres respectifs

$$\omega \cdot n, w^2, w^2 \cdot n, \omega^3, \ldots w^p \ldots$$

3.4.6 Comparaison des nombres ordinaux

Si n_1 et n_2 sont deux nombres ordinaux alors, ils sont égaux ou l'un d'eux est plus grand que l'autre. Soit α et β des nombres ordinaux et M et N des ensembles ayant pour ordinal α et β respectivement. Nous dirons que :

- $\alpha = \beta$ si les ensembles M et N sont isomorphes
- $\alpha < \beta$ si M est isomorphe à un sous ensemble de N
- $\alpha > \beta$ si N est isomorphe à un sous ensemble de M

Théorème 3.4.6.1 *Pour chaque deus nombres ordinaux* α *et* β*, une des relations suivantes est vérifiée :* $\alpha = \beta$*,* $\alpha < \beta$ *ou* $\alpha > \beta$*.*

Rémarque 3.4.6.1 *Si A et B sont deux ensembles totalement ordonnés alors ou bien ils sont équivalents (ont une même puissance) ou bien la puissance de l'un est plus grande que celle de l'autre.*

Rémarque 3.4.6.2 *Considérons la collection de tous les ordinaux qui correspondent à une puissance finie ou dénombrable, elle forme un ensemble ordonné. Cet ensemble n'est pas dénombrable, son ordinal est noté* $w_1 = \aleph_1$*, il n'existe pas de puissance m telle que* $\aleph_0 < m < \aleph_1$*.*

Proposition 3.4.6.1 *Soit A un ensemble de cardinaux. Il existe un et un seul cardinal* α *qui posséde les propriétés suivantes :*

- *(a) soit* $x \leq \alpha$*(respectivement* $x \geq \alpha$*) pour tout* $x \in A$*;*
- *(b) si on a un cardinal* β *tel que l'on ait* $x \leq \beta$*(respectivement* $x \geq \beta$*) pour tout* $x \in A$*, alors* $\beta \geq \alpha$*(respectivement* $\beta \leq \alpha$*).*

Cette proposition montre que si on a un ensemble de cardinaux A, il existe des cardinaux supérieurs et respectivement inférieurs à tout élément de l'ensemble A.

3.4.7 Axiome du choix : Théorème de Zermelo et autres propositions équivalentes

La comparaison des ensembles totalement ordonnés relativement à leurs puissances amène à se poser la question suivante : **ne peut - on pas ordonner totalement chaque ensemble d'une manière ou d'une autre ?**
Une reponse positive signifierait en particulier que les puissances non comparables en générale n'existent pas ; c'est la réponse qu'a donné Zermelo en démontrant que chaque ensemble peut être totalement ordonné.
A cause de la difficulté et du caractére fastidieux de la démostration de ce théorème, nous n'allons pas la présenter ici. Mais nous allons nous appuyer sur la proposition suivante appelée «axiome du choix».

Axiome du choix

Soit A un ensemble d'indice α et supposons que pour chaque α soit donné un ensemble quelconque M_α. Alors comme l'affirme l'axiome du choix, on peut construire une fonction φ sur A qui fait correspondre chaque $\alpha \in A$ un certain élément m_α de l'ensemble M_α. En dautres termes, on peut construire un ensemble en choisissant, dans chaque M_α, un et un seul élément.
Nous pouvons encore formuler cette proposition de la manière suivante : soit donné un ensemble M, il existe une fonction φ qui fait correspondre à chaque sous ensemble A de M un élément $\varphi(A)$ de ce sous ensemble, c'est l'axiome du choix.
Nous allons formuler quelques propositions qui sont ǫuivalentes à l'axiome du choix, c'est - à - dire chacune peut être démontrer, si on considère l'axiome du choix et, inversement, on peut démontrer l'axiome du choix si on accepte ces propositions. Nous noterons que le théorème de Zermelo est l'une de ces propositions.

Théorème 3.4.7.1 *(Théorème de Zermelo)*
En effet si nous supposons que chaque ensemble M_α est totalement ordonné alors, pour construire la fonction $\varphi(A)$ dont l'axiome du choix affirme l'existence, il est suffisant de prendre dans chaque M_α le premier élément.

Pour donner la formulation des autres propositions, introduisons d'abord la définition suivante :

Définition 3.4.7.1 *soit M un ensemble partiellement ordonné, chaque sous ensemble de M dans lequel deux éléments sont comparables (en raison de l'ordre partiel introduite dans M) sera appellé chaîne.*

Une chaîne est maximale si elle n'est pas contenue comme sous ensemble dans n'importe quel autre chaîne de M.

Définition 3.4.7.2 *Appellons l'élément a Borne sup (borne supérieure) dans l'ensemble partiellement ordonné M du sous ensemble $M' \subset M$, si chaque élément $a' \in M$ est subordonné à a (soit si chaque a' precède a)*

Théorème 3.4.7.2 *(***de Hausdorff***)*
Dans un ensemble partiellement ordonné, chaque chaîne est contenu dans sa chaîne maximale.

Lemme 3.4.7.1 *(de Zorn)*
Si chaque chaîne dans un ensemble totalement ordonné M adment une Bornesup alors, chaque élément de M est inférieur ou égale à un certain élément maximal.

3.4.8 Induction transfinite (ou ordinal)

La méthode de démonstration par induction est très répandue, son principe est le suivant soit donnée une proposition $P(n)$ qui est formulée pour chaque n, nous supposons que :

1. la proposition $P(1)$ est vraie,
2. $\forall k \leq n \quad P(k)$ est vraie,
3. on montre que la proposition est aussi vraie pour $P(n+1)$.

Ainsi la proposition $P(n)$ est vraie $\forall n = 1, 2, \ldots$
En effet dans le cas contraire, parmi les n où la proposition $P(n)$ n'est pas vraie, on peut trouver un plus petit nombre n_1. Il est clair que $n_1 > 1$ c'est -à- dire $n_1 - 1$ est aussi un entier naturel et nous obtenons la contradiction de la condition 2.
De manière analogue nous pouvons utiliser le même raisonnement si on substitue l'ensemble $\mathbb{N}$ à n'importe quel autre ensemble totalement ordonné, dans ce cas il portera le nom d'induction transfinite. Ainsi la méthode d'induction transfinite se définit de la manière suivante :
Supposons que soit donné un ensemble totalement ordonné A et soit $P(a)$ une certaine proposition formulée pour chaque $a \in A$ tel que $P(a)$ soit vraie pour le premier élément de A et vraie pour a et pour chaque élément qui precède a. Alors, $P(a)$ est vraie $\forall a \in A$. En effet s'il existait dans A des éléments pour lesquels $P(a)$ ne soit pas vraie alors, dans l'ensemble de tels éléments, on retrouverait le premier disons par exemple $a^\star$ et nous obtiendrons une contradiction parce que $\forall a < a^\star$ la proposition ne serait pas vraie.
Une telle méthode de démonstration est appellée méthode de démostration par induction transfinite

3.4.9 Système d'ensembles

Définition 3.4.9.1 *Un système d'ensemble est chaque ensemble constitué des éléments qui sont eux même des ensembles.*

Définition 3.4.9.2 *Un système d'ensemble non vide $\mathfrak{K}$ est appellé anneau si*

$$\forall A, B \in \mathfrak{K} \Rightarrow A \Delta B \in \mathfrak{K} \qquad A \cap B \in \mathfrak{K}.$$

Comme $\forall A, B \in \mathfrak{K}$, $A \cup B = (A \Delta B) \cup (A \cap B)$ et
$A \setminus B = A \Delta (A \cap B) = A \setminus (A \cap B)$ donc du fait que $\forall A, B \in \mathfrak{K}$ alors implique l'appartenance á $\mathfrak{K}$ des ensembles $A \cup B$ et $A \setminus B$.
Ainsi nous pouvons dire que l'anneau des ensembles est un système qui est clos relativement á l'intersection, la reunion la différence et la différence symétrique des ensembles.

Définition 3.4.9.3 *Un système d'ensemble non vide* $\mathfrak{O}$ *est appellé semi- anneau s'il contient* $\emptyset$ *et est clos relativement á l'intersection et possède la propriété suivante : de l'appartenance á* $\mathfrak{O}$ *des ensembles* A *et* $A_1 \subset A$ *implique la possibilité de representer* $A = \bigcup_{k=1}^{n}$ *ou les* A_k *sont deux á deux disjoints et* A_1 *est le premier.*

Chapitre 4

Relations d'équivalence

4.1 Relations d'équivalence

Définition 4.1.0.4 *On appelle relation binaire définie dans un ensemble X et notée $\Re$, la donnée d'un ensemble $G(\Re) \subseteq X \times X$ et appellé graphe de la relation $\Re$ telle que :*

$$\forall x, y \in X, \quad x \Re y \leftrightarrow (x, y) \in G(\Re).$$

Définition 4.1.0.5 *Une relation $\Re$ dans un ensemble X est appelée relation d'équivalence si elle vérifie les propriétés suivantes :*

- $x \Re x \quad \forall x \in X \qquad$ *(reflexivité)*
- $\forall x, x' \in X, \quad x \Re x' \Rightarrow x' \Re x \qquad$ *(symétrie)*
- $\forall x, x', x'' \in X, \quad x \Re x' \text{ et } x' \Re x'' \Rightarrow x \Re x'' \qquad$ *(transitivité)*

Si x et x' correspondent par la relation d'équivalence, alors on dira que x est équivalent à x' modulo $\Re$. Et on note :

$$x \equiv x' \bmod (\Re)$$

La notation $x \not\Re x'$ signifie la négation de la relation d'équivalence des éléments x et x' appartenant à X.
Le sous-ensemble $\bar{x} = [x] = \dot{x} = \{x' \in X, \ x' \Re x\}$ de X de tous les éléments équivalents à x est appelé classe d'équivalence de l'élément x. Il est à noter que $x \in \bar{x}$ car $x \Re x$
Tout $x' \in \bar{x}$ se nomme représentant de la classe $\bar{x}$.
L'ensemble des classes d'équivalence par la relation $\Re$ forment une partition de l'ensemble X notée $\prod_{\Re}(X)$. X est donc la réunion de sous-ensembles disjoints.
Etant donné une partition quelconque $\prod(X)$ de l'ensemble X en sous-ensembles disjoints appelés C_x, les parties C_x sont des classes d'équivalence par une certaine relation $\Re$.

4.2 Factorisation d'applications

Comme nous l'avons établi ci-dessus, il existe une correspondance biunivoque entre relations d'équivalence et partitions de l'ensemble X. On conviendra d'appeler

ensemble quotient S par la relation d'équivalence $\Re$, on note $S = X/\Re$, l'ensemble constitué de toutes les classes d'équivalences par la relation $\Re$ dans X.

Application canonique et factorisation d'applications

L'application surjective :

$$\begin{array}{rccc} p: & X & \longrightarrow & X/\Re \\ & x & \mapsto & p(x) = \dot{x} \end{array}$$

est appelée application canonique de X sur $X/\Re$.
Soient X et Y deux ensembles et f une application de X vers Y. La relation binaire que nous allons noter O_f vérifiant :

$$\forall x, x' \in X,\ xO_f x' \Leftrightarrow f(x) = f(x')$$

est une relation d'équivalence. La preuve est laissée au lecteur.
La classe d'équivalence correspondant à l'élément x est définie ou notée par $\bar{x} = \{x';\ f(x') = f(x)\}$ elle désigne la fibre (ou l'orbite) de x par de la relation O_f.
L'application $f : X \longrightarrow Y$ induit une application notée $\bar{f}$ et définie par :

$$\begin{array}{rccc} \bar{f}: & X/O_f & \longrightarrow & Y \\ & \bar{x} & \mapsto & \bar{f}(\bar{x}) = f(x) \end{array}$$

de telle manière que :

$$\bar{f} \circ p(x) = f(x).$$

Ce qui est équivalent à

$$\bar{f}[p(x)] = f(x) \tag{4.1}$$

On sait que : $\bar{x} = [x] = \{x' \in X,\ x'\Re x\} = [x']$ car $x\Re x'$. Puisque $\bar{x} = \bar{x'} \Leftrightarrow f(x) = f(x')$, la relation 4.1 ne dépend pas du représentant x choisi dans la classe $\bar{x}$.Dans ce cas, on dit que $\bar{f}$ est bien définie et le diagramme :

$$\begin{array}{rccc} f: & X & \longrightarrow & Y \\ & \searrow & & \nearrow \\ & & X/O_f & \end{array}$$

illustre la factorisation suivante :

$$(\bar{f} \circ p)(x) = f(x).$$

Quelques propriétés de $\bar{f}$

$\bar{f}$ est **injective**. En effet, l'injectivité de $\bar{f}$ découle du fait que :

$$\bar{f}(\bar{x}_1) = \bar{f}(\bar{x}_2 \Leftrightarrow f(x_1) = f(x_2) \Leftrightarrow \bar{x_1} = \bar{x_2}$$

La surjectivité de $\bar{f}$ est équivalente à la surjectivité de f.
Si $f' : X/O_f \longrightarrow Y$ est une autre application pour laquelle est vérifiée la relation 4.1, alors :

$$(f' \circ p)(x) = f(x) \Rightarrow f'(\bar{x}) = f'(p(x)) = f(x) = \bar{f}(\bar{x}).$$

D'où $f' = \bar{f}$. Ainsi $\bar{f}$ est **unique**.

Définition 4.2.0.6 *Soient A, B, C et D des ensembles et $t : A \longrightarrow B$, $b : C \longrightarrow D$, $l : A \longrightarrow C$ et $r : B \longrightarrow D$ des applications. Nous dirons que le diagramme suivant est t'un diagramme commutatif si $r \circ t = b \circ l$*

$$\begin{array}{ccc} A & \xrightarrow{t} & B \\ {\scriptstyle l}\downarrow & & \downarrow{\scriptstyle r} \\ C & \xrightarrow{b} & D \end{array}$$

Définition 4.2.0.7 *Soit $f_1 : A_1 \longrightarrow B_1$ et $f_2 : A_2 \longrightarrow B_2$ deux applications. On appelle produit cartesien des applications f_1 et f_2 l'application définie par*

$$\begin{array}{rccc} f_1 \times f_2 : & A_1 \times A_2 & \longrightarrow & B_1 \times B_2 \\ & (a_1, a_2) & \mapsto & (f_1(a_1), f_2(a_2)) \end{array}$$

Théorème de la décomposition canonique

Théorème 4.2.0.1 (Théorème de la décomposition canonique) *Si φ est une application surjective de A sur B et $\Pi : A \longrightarrow A/\operatorname{Ker}\varphi$ la projection canonique, avec $\operatorname{Ker}\varphi = \{x \in A,\ \varphi(x) = 0_B\}$, le noyau de φ.*
Alors, il existe une application bijective $\chi : A/\operatorname{Ker}\varphi \longrightarrow B$ telle que :

$$\chi \circ \Pi = \varphi.$$

On a le diagramme ci-dessous :

$$\begin{array}{rccc} \varphi : & A & \longrightarrow & B \\ & \searrow^{\pi} & & \nearrow_{\chi} \\ & & A/\ker\varphi & \end{array}$$

Démonstration 4.2.0.1 *Il s'agit de pouvoir définir une fonction χ' bijective telle que $\chi' \circ \varphi = \Pi$, l'application χ du théorème correspondra alors à $(\chi')^{-1}$.*
Si $a \in A$ alors $a\Pi$ représente une classe d'équivalence dans la factorisation avec $\operatorname{Ker}\varphi$ à laquelle a appartient. Si $b \in B$, comme φ est une application surjective alors $b = a\varphi$ pour un certain $a \in A$.

Posons $b\chi' = a\Pi$. *L'application* χ' *est bien définie car* $b\chi'$ *ne dépend pas du choix de* a. *En effet, si* $b = a'\varphi$ *alors* $a\Pi = a'\Pi$ *par définition de la relation* $\operatorname{Ker}\varphi$, *on définit ainsi* $\chi' : B \to A/\operatorname{Ker}\varphi$.
Alors $\forall a \in A, a(\varphi\chi') = (a\varphi)\chi' = b\chi' = a\Pi$. *Donc* $\varphi\chi' = \Pi$.
D'autre part, si $b'\chi' = b''\chi'$, $b', b'' \in B$ *avec* $a', a'' \in A$ *tels que* $b' = a'\varphi$ *et* $b'' = a''\varphi$, *alors* $a'\Pi = a''\Pi$. *En raison de la définition de* $\operatorname{Ker}\varphi$, *on en déduit que* $b' = a'\varphi = a''\varphi = b''$. *Donc* χ' *est injective.*
Enfin, chaque élément de $A/\operatorname{Ker}\varphi$ *peut s'écrire* $a\Pi$, $a \in A$ *et on a* $a\Pi = (a\varphi)\chi'$. *Donc* χ' *est surjective.*
Par conséquent χ' *est bijective. Ce qui achève la preuve du théorème.*

Chapitre 5

Analyse combinatoire

5.1 Permutations, arrangements et combinaisons

5.2 Exemples de problèmes d'analyse combinatoire

- (a) Dans une classe de 30 étudiants combien de manières possibles on peut choisir un chef et un sous chef de classe si l'on suppose que chaque étudiant peut occuper ces postes.
  Solution 5.2.0.1 *D'après l'énoncé, chaque étudiant peut être chef donc il y a 30 possibilités. Pour le choix du sous chef, il reste* 29 *possibilités c'est pourquoi, en tout on a* $30x29$ *possibilités.*
- (b) Pour la permanence d'une salle de classe pendant une semaine sauf le dimanche, on a choisi 6 étudiants. Combien de manière possibles peut-on, organiser ces permanences si, on suppose que chaqu'un de ces étudiants surveille une fois.
  Solution 5.2.0.2 . *Au regard de ce problème, on voit que le lundi, chaqu'un des* 6 *étudiants choisi peut surveiller. Le mardi ne peut assurer la permanence que l'un des* 5 *restant puisque d'après l'hypothèse chaque étudiant surveille une fois. Donc, le nombre de possibilités de permanences lundi et mardi est* $6x5 = 30$*, le mercredi on ne peut que prendre parmi les* 4 *restant soit un nombre de possibilités* $6x5x4 = 120$*, le jeudi on prend* 1 *parmi les* 3 *restant soit* $6x5x4x3 = 360$ *et le samedi on prend* 1 *parmi les* 2 *restant soit* $6x5x4x3x1 = 720$ *possibilités.*
- (c) Pour faire passer un examen, on organise une commission constituée de deux enseignants. Combien de commissions possibles peut-on organiser à partir de 5 enseignants ?
  Solution 5.2.0.3 *Notons pour notre convenance que les enseignants sont représentés par les lettres* A, B, C, D, E*. il n'est pas difficile de représenter toutes les possibilités de ce choix soit :*

  AB, AC, AD, AE
  BC, BD, DE
  CD, CE
  DE

  .

Donc, on voit que le nombre de choix de ces commissions est 10
On note aussi que nous avions eu la possibilité de représenter ces différents cas, parce que le nombre d'enseignants n'était pas grand. Par exemple, s'il nous avait été demandé de constituer les commissions de 7 enseignants choisis parmi 14, alors , lister les commissions comme nous avons fait devrait être difficile et fastidieux, puisque dans ces conditions nous aurons 3432 commissions. Ce résultat pourra être obtenu quand nous allons ressortir la formule générale. Mais avant d'en arriver aux formules, essayons de voire ce qu'il ya de commun à ces trois exemples. Avant tout, nous remarquons qu'ici nous avons à faire à des ensembles constitués d'un nombre fini d'éléments et, qu'on nous demande de ressortir des sous ensembles de ces ensembles vérifiant certaines conditions. Par exemple, dans l'exemple (a), nous avions considérée l'ensemble des étudiants d'une classe constituée de 30 éléments et, on nous demandait de constituer les différents sous-ensembles de cet ensemble constitués de 2 éléments chacun(soit un chef et un sous chef). Dans l'exemple (b), nous avions considéré un ensemble de 6 éléments et nous devons les classifier (organiser) pour des permanences, nous devons donc ressortir les différents sous ensembles possible de cette classification. Dans l'ensemble (c) nous avions considéré un ensemble de 5 éléments qui sont des enseignants. Nous devons donc ressortir des sous ensembles de commissions constituées de 2 éléments . Il est à noter que, en considérant ces trois exemples, il ressort une différence certaine ; elle est basée sur le fait que dans les exemples (a), (b) et (c) l'expression **combien de manière possible** est comprise différemment. Si dans l'exemple (a) en constituant ces sous ensembles, il faut tenir compte de l'ordre. Alors que, dans l'exemple (c) on ne tient pas compte de l'ordre. Dans l'exemple (b) ici les sous ensembles sont constitués d'un même nombre d'éléments.

5.2.1 Arrangements

Définition 5.2.1.1 *On appelle arrangement de n éléments pris p à p (ou encore arrangement de rang p de n éléments) toute permutation formée avec p de ces n éléments. c'est -á-dire tout sous ensemble ordonné formé avec p des n éléments.*

Définition 5.2.1.2 *Soit donné un ensemble constitué de n éléments, chaque sous ensemble ordonné qui est constitué de p éléments est appelé arrangement de p éléments des n éléments ou arrangement de rang p.*

Rémarque 5.2.1.1 *De par la définition il vient que $n \geq p \geq o$*

Par exemple on obtient un arrangement de rang 13 cartes d'un jeu en extrayant 13 cartes quelconques de ce jeu et en les rangeant dans un ordre determiné
Nombre d'arrangements d'ordre p de n éléments , il est noté par A_n^p et est appellé nombre d'arrangement de n éléments pris p à p.
Soit F l'ensemble $\{1, 2, 3, \cdots, p\}$ de p premiers entiers et, E l'ensemble des n éléments donnés.
Toute application injective de F dans E permet de définir un arrangement de rang p des n éléments.
– l'image de 1 peut être l'un quelconque des n éléments de E

- l'image de 2 peut être l'un quelconque des $n-1$ éléments de E l'image de 1 étant choisi
- l'image de 3 peut être l'un quelconque des $n-2$ éléments de E les images de $1, 2$ étant fixées
- $\vdots$
- l'image de p peut être l'un quelconque des $n-(p-1)$ éléments de E les images de $1, 2, \cdots (p-1)$ étant fixées.

On obtient en définitive pour l'arrangement de rang p de n éléments

$$A_n^p = n(n-1)(n-2)\cdots(n-(p-1)).$$

On peut simplifier l'écriture de A_n^p en multipliant et divisant par $(n-p)(n-p-1)\times\cdots\times 2\times 1$ et il vient :

$$A_n^p = \frac{n(n-1)(n-2)\cdots(n-(p-1))(n-p)\times\cdots\times 2\times 1)}{(n-p)(n-p-1)\times\cdots\times 2\times 1} = \frac{n!}{(n-p)}$$

$$A_{52}^{13} = 52\times 51\times 50\times\cdots\times 41\times 40$$

5.2.2 Permutations

Définition 5.2.2.1 *On appelle permutation de n éléments tout ensemble strictement ordonné de ces n éléments*

Définition 5.2.2.2 *Tout arrangement de n éléments pris n à n est appelé permutation.*

Rémarque 5.2.2.1 *la permutation est un cas particulier de l'arrangement.*

Nombre de permutations de n éléments il est noté par P_n.
Il n'existe qu'une permutation formée à partir d'un et un seul élément soit a
Il n'existe que deux permutations formées à partir de deux éléments soit a, b et b, a
Il n'existe que 6 permutations formées à partir de trois éléments soit a, b, c

$$a,b,c \quad b,c,a \quad c,a,b$$

$$a,c,b \quad b,a,c \quad c,b,a.$$

Soit $1\times 2\times 3 = 6 = 3!$. Ainsi, le nombre de permutations de n éléments est $n!$.
Par exemple le nombre de manière de ranger les cartes d'un jeu de 52 cartes est 52!

5.2.3 Combinaisons

Définition 5.2.3.1 *On appelle combinaison de n éléments pris p à p (ou combinaison de rang p de n éléments ou encore, combinaison d'ordre n et de rang p) tout ensemble non ordonné formé de p de ces n éléments.*

Définition 5.2.3.2 *Soit donné un ensemble constitué de n éléments. Tout sous ensemble constitué de n pris de n éléments est appelé Combinaison.*

Par exemple toute donnée de 13 cartes extraites d'un jeu de 52 cartes indépendante de l'ordre dans lequel les cartes sont distribuées est une combinaison d'ordre 13 des ces 52 cartes.

Nombre de combinaisons de rang p de n éléments , il est noté C_n^p

Il est par définition lié par la formule $A_n^p = C_n^p \times p!$ soit

$$C_n^p = \frac{A_n^p}{p!} = \frac{n(n-1)(n-2)\cdots(n-(p-1))}{p!}$$

$$C_n^p = \frac{n!}{p!(n-p)}$$

Par exemple le nombre de combinaisons de 13 cartes dans un jeu de 52 cartes est

$$C_{52}^{13} = \frac{52 \times 51 \times \cdots \times 41 \times 40}{13!}$$

Propriétés

- (a) Relation entre le nombre de combinaison de rangs consécutifs le nombre de combinaison de rang $p+1$

$$C_n^{p+1} = \frac{n(n-1)(n-2)\cdots(n-(p-1))(n-p)}{(p+1)!} = C_n^p \times \frac{n-p}{p+1}$$

- (b) Triangle de Pascal
  Il s'agit de vérifier l'égalité suivante $C_{n+1}^p = C_n^p + C_n^{p-1}$.
  Ceci peut se faire par le biais de la table suivante

	0	1	2	3	4	...	$p-1$	p
0	1							
1	1	1						
2	1	2	1					
3	1	1	3	1				
4	1	4	6	4	1			
$\vdots$								
n	...	...	...		...	...	C_n^{p-1}	C_n^p
$n+1$	...	...	...		...	...		C_{n+1}^p

- (c) Combinaisons complémentaires $p \longrightarrow n-p$ soit $C_n^{n-p} = C_n^p$

Rémarque 5.2.3.1

$$C_n^0 = 1 \quad 0! = 1$$

5.2.4 Binôme de Newton

1. Formule du Binôme

   Soit P un polynôme défini par $P(x) = (x+a_1)(x+a_2)\ldots(x+a_n)$. Si nous posons $a_i = a \; \forall i$ alors on obtient $P(x) = (x+a)^n$. Qui devient aprés expansion :

$$(x+a)^n = C_n^0 x^n + C_n^1 x^{n-1} a + C_n^2 x^{n-2} a^2 + \ldots + C_n^p x^{n-p} a^p + \ldots + C_n^n a^n.$$

En explicitant les coefficients il vient :

$$(x+a)^n = x^n + nx^{n-1}a + \frac{n(n-1)}{2!}x^{n-2}a^2 + \ldots + \frac{n(n-1)\ldots(n-(p-1)}{p!}x^{n-p}a^p + \ldots + a^n.$$

2. Propriété des coefficients
   Dans la premiére formule précedante, si l'on pose $x = a = 1$ il vient :

$$2^n = C_n^0 + C_n^1 + C_n^2 + \ldots + C_n^p + \ldots + C_n^n.$$

Par contre si l'on pose $x = 1$ et $a = -1$ il vient :

$$0 = C_n^0 - C_n^1 + C_n^2 + \ldots + (-1)^p C_n^p + \ldots + (-1)^n C_n^n.$$

Si l'on pose $x = 2$ et $a = -1$ il vient :

$$1 = C_n^0 2^n - C_n^1 2^{n-1} + C_n^2 2^{n-2} + \ldots + C_n^p 2^{n-p}(-1)^p + \ldots + C_n^n(-1)^n.$$

Si Par contre l'on pose $x = 1$ et $a = -2$ il vient :

$$(-1)^n = C_n^0 - 2C_n^1 + 4C_n^2 + \ldots + C_n^p(-2)^p + \ldots + C_n^n(-2)^n.$$

5.3 Permutations, arrangements et combinaisons avec repétitons

5.3.1 Permutations avec repétitons

Définition 5.3.1.1 *On appelle permutation avec repétitions, toute permutation qui contient des éléments qui se repètent ou toute permutation qui contient des éléments en son sein qui sont identiques.*

En effet, considérons les éléments distincts $a, b, c, \ldots, l$ et supposons qu'on forme un assortiment de n éléments en utilisant α fois élément a, β fois élément b et γ fois élément $c \ldots$, λ fois élément l. En imaginant qu'on affecte des indices differents aux éléments identiques employés. Par exemple en désignant par $a_1, a_2, a_3 \ldots, a_\alpha$ les éléments identiques à a, on obtient $n!$ permutations possibles des n éléments ainsi distingués.
En réalité, les assortiments qui ne diffèrent que par l'ordre des a_i sont identiques ; or on peut former, à partir d'un assortiment donné $\alpha!$ assortiments ne differant que par l'ordre des a_i (nombre de permutations de α éléments.) En répetant le même raisonnement sur les autres éléments on obient en définitive

$$\frac{n!}{\alpha!\beta!\delta!\ldots\lambda!}$$

Permutations avec repétitions.

5.3.2 Arrangements avec repétitons

Définition 5.3.2.1 *On appelle arrangement avec repétitions, tout arrangement qui contient des éléments qui se repètent.*

Etant donnés n éléments distincts, on forme un assortment de p termes choisis parmi ces éléments, le même élément pouvant être repété. Il y'a dans ces conditions n possibilités pour le choix de chacun des p termes. Soit en tout n^p arrangements d'ordre p avec repétitions de n éléments.

5.3.3 Combinaisons avec repétitons

Définition 5.3.3.1 *On appelle combinaison avec repétitions, toute combinaison qui contient des éléments qui se repètent.*

Considérons maintenant n éléments distincts et proposons-nous de former des assortiments de p termes à partir de ces éléments qui peuvent être repétés(l'ordre des termes n'important pas). Désignons par $a, b, c, \ldots, l$ les n éléments donnés. Dans un assortiment quelconque, le même élément est répété au plus $(p-1)$ fois. Considérons l'ensemble des $n+p-1$ éléments $a, b, c, \ldots, l, 1, 2, 3, \ldots, (p-1)$ appellons le F. Cet ensemble contient C^p_{n+p-1} éléments qui sont des combinaisons des éléments de l'ensembles F.

Soit E l'ensemble des assotiments recherchés. Cherchons une bijection de l'ensemble E sur l'ensemble F.

Ecrivons chaque assortiment de E en l'ordonnant de la maniére suivante :Un élément de chaque type utilisé classé par ordre alphabétique, puis les éléments répétés eux même classés par ordre alphabétiques.

Pour illustrer l'exposé, consiérons le cas des assortiments de rang 5 de 6 éléments a, b, c, d, e, f. Nous écrirons par exemple les assortiments

$$a, c, d, a, a \quad (1)$$

$$b, c, b, c, c \quad (2).$$

L'ensemble F est alors formé des combinaisons de rang 5 des éléments $a, b, c, d, e, f, 1, 2, 3, 4$.

Associons á chaque assortiment définie de la manière suivanate :

- Les premiers termes sont les éléments distincts de l'assortiment ;
- Les termes répétés de l'assortiment sont remplacés par les chiffres $1, 2, 3, 4$ en ne tenant compte dans cette notation que des lettres figurant dans la partie diversifiée.

Par exemple, on associe á l'assortiment (1) la combinaison $a, c, d, 1, 2$ et à l'assortiment (2) la combinaison $b, c, 1, 3, 4$ (il nous a fallu en effet sauter le chiffre 2 pour indiquer que élément b n'etait répété qu'une fois).

De même on associerait à l'assortiment a, c, d, d, d la combinaison $a, c, d, 3, 4$, puisque les deux premiers éléments utilisés ne sont pas répétés.

Inversement, le même procedé permet d'associer à chaque combinaison un assortiment bien determiné.

Par exemple à la combinaison $a, c, d, 2, 4$ on associe l'assortiment a, c, d, c, d puisque :

- Le premier élément répété est le deuxième des éléments distincts ;
- Cet élément n'est répété qu'une seule fois (on saute le chiffre 3) l'autre élément ne peut être que d puisqu'il figure dans la partie diversifiée.

Ainsi, l'application proposée est une bijection et, les ensembles finis E et F se correspondent par une bijection comprenant le même nombre éléments qui est C_{n+p-1}^{p}.

Chapitre 6

Lois de composition

6.1 Lois de composition interne

6.1.1 Définition

On appelle loi de composition interne dans un ensemble E toute application $*$ de l'ensemble produit $E \times E$ vers E.

$$\begin{array}{rccc} * & : & E \times E & \longrightarrow & E \\ & & (x, y) & \mapsto & x * y \end{array}$$

Dans le cas où on applique $E \times E$ dans E, la loi est dite partout définie. On peut énoncer d'une manière moins abstraite la notion de loi de composition interne.
On appelle loi de composition interne dans un ensemble E, une correspondance $*$ associant à tout couple $(a, b) \in E \times E$ un élément c de E, bien déterminé. On écrit $a * b = c$.
Exemples de lois de composition interne : Dans $\mathbb{N}$, les opérations $+$ et $\cdot$ sont des lois de composition interne.

6.1.2 Propriétés d'une loi de composition interne

Commutativité

Une loi de composition interne $*$ dans un ensemble E est dite commutative si :

$$\forall a, b \in E, \quad a * b = b * a$$

Associativité

Une loi de composition interne $*$ dans un ensemble E est dite associative si :

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

Proposition 6.1.2.1 *Lorsque la loi $*$ sur E est associative on peut écrire les produits sans qu'il soit nécessaire de placer les parenthèses soit le résultat d'une telle procedure ne dépend pas de la manière dont sont disposées les parenthèses. En particulier, pour $x \in E$ et $n \in \mathbb{N}^\star$, on peut définir*

$$x^n = \underbrace{x * \cdots * x}_{n\ fois}$$

et on a les relations

$$\begin{cases} x^n * x^m &= x^{n+m} \quad (n, m \in \mathbb{N}^\star) \\ (x^n)^m &= x^{nm} \quad (n, m \in \mathbb{N}^\star). \end{cases}$$

Enfin, si, en plus d'être associative, la loi $*$ est aussi commutative, on peut permuter les éléments de $a_1 * a_2 * \cdots * a_n$ de manière arbitraire sans modifier le résultat.

Elément neutre

On dit qu'un élément $e \in E$ est neutre pour la loi $*$ si :

$$\forall a \in E,\ a * e = e * a = a$$

Rémarque 6.1.2.1 *Une loi interne admet au plus un élément neutre.*

Théorème 6.1.2.1 *S'il existe un élément neutre, alors il est unique.*

La démonstration est laissée au lecteur.

Elément symétrique

Soit $*$ une loi de composition interne d'élément neutre e. On dit que deux éléments a et a' sont symétriques si on a :

$$a * a' = a' * a = e$$

Théorème 6.1.2.2 *Si une loi est associative dans un ensemble et admet un élément neutre et, si un élément admet un symétrique alors ce dernier est unique.*

Démonstration 6.1.2.1 *Supposons que a admet deux symétriques qui sont a' et a''.*
Si a' est un symétrique de a alors : $a * a' = a' * a = e$ (1)
Si a'' est un symétrique de a alors : $a * a'' = a'' * a = e$ (2)
En composant chaque membre de (1) par a'', on a : $a'' * (a') = a'' * (a') = a'' * e$
$*$ étant associative, alors :
$(a'') * a' = (a'' * a') * a = a''$ car e est élément neutre.
D'après (2), on a $a'' * a = e$, on obtient alors : $e * a' = a''$. Soit $a' = a''$. Donc le symétrique est unique.

Théorème 6.1.2.3 (Symétrique d'une composée) *Si a et b admettent respectivement a' et b' pour symétriques par rapport à une loi associative $*$ définie sur E alors, la composée $a * b$ admet $b' * a'$ pour symétrique. C'est-à-dire :*

$$(a * b) * (b' * a') = e.$$

Table d'opération

Lorsqu'on est conduit à utiliser fréquemment une opération définie dans un ensemble E, on dresse une table de cette opération, c'est-à-dire une table où on retrouve les composées $a_i * a_j$ et $a_j * a_i$ préalablement déterminées. Si E contient un nombre fini d'éléments, on peut dresser une table complète de l'opération, dans le cas contraire, on établit une table partielle.
Disposition : Les éléments ayant été ordonnés, on les écrit en tête de chaque ligne et colonne du tableau carré et l'on reporte les composées $a_i * a_j$ dans la case située à l'intersection de la i-ème ligne et j-ème colonne.

$*$	a_1	a_2	a_3	$\dots$	a_i	$\dots$	a_j	$\dots$
a_1	$a_1 * a_1$	$a_1 * a_2$	$a_1 * a_3$	$\dots$	$a_1 * a_i$	$\dots$	$a_1 * a_j$	$\dots$
a_2	$a_2 * a_1$	$a_2 * a_2$	$a_2 * a_3$	$\dots$	$a_2 * a_i$	$\dots$	$a_2 * a_j$	$\dots$
a_3	$a_3 * a_1$	$a_3 * a_2$	$a_3 * a_3$	$\dots$	$a_3 * a_i$	$\dots$	$a_3 * a_j$	$\dots$
$\vdots$								
a_i	$a_i * a_1$	$a_i * a_2$	$a_i * a_3$	$\dots$	$a_i * a_i$	$\dots$	$a_i * a_j$	$\dots$
$\vdots$								
a_j	$a_j * a_1$	$a_j * a_2$	$a_j * a_3$	$\dots$	$a_j * a_i$	$\dots$	$a_j * a_j$	$\dots$
$\vdots$								

Si l'opération est commutative alors $a_i * a_j = a_j * a_j$.
La diagonale principale est la partie du tableau formée des cases intersections de lignes et colonnes de même indice.
Les composées $a_i * a_j$ et $a_j * a_i$ sont situées dans des cases symétriques par rapport à la diagonale principale.

Définition 6.1.2.1 *On appelle élément absorbant tout élément ν qui est telque*

$$\forall a \in E \quad a * \nu = \nu * a = \nu$$

Elément régulier

Un élément $a \in E$ est régulier pour la loi de composition interne $*$ définie sur E si :

$$\forall x, y \in E,\ a * x = a * y \Rightarrow x = y \text{ et } x * a = y * a \Rightarrow x = y$$

Si tout élément de E est régulier pour la loi $*$, on dit que cette loi est régulière.

Opération inverse

Soient $a, b, c \in E$ où est définie une opération (loi de composition) interne $*$.
On appelle opération inverse à droite de l'opération donnée, l'opération qui permet de déterminer $x \in E$ tel que $x * b = c$, en d'autres termes qui permet donc de résoudre cette équation.
On appelle opération inverse à gauche, l'opération qui permet de résoudre $a * y = c$.
Si l'opérateur $*$ est commutatif, les opérations à droite et à gauche se confondent.

Distributivité

Soient les lois $\top$ et $*$ deux lois de composition interne définies dans un ensemble E, a, b, c trois éléments quelconques de E. On dit que la loi $\top$ est distributive par rapport à la loi $*$ si on a :

$$\begin{array}{ll} (a * b)\top c = (a\top c) * (b\top c) & \text{distributivité à droite} \\ c\top(a * b) = (c\top a) * (c\top b) & \text{distributivité à gauche} \end{array}$$

Définition 6.1.2.2 *Soit $(G, \diamond)$ un ensemble muni d'une loi de composition interne et $\mathcal{R}$ une relation d'équivalence définie dans G. On dit que $\mathcal{R}$ est* **compatible** *avec la loi $\diamond$ si*

$$\forall a, b, c, d \in G \quad \left.\begin{array}{lll} a & \mathcal{R} & b \\ c & \mathcal{R} & d \end{array}\right\} \Rightarrow a \diamond c \ \mathcal{R} \ b \diamond d.$$

Equation dans E

Soit $f : E \to E$. Résoudre l'équation $f(x) = a$ avec $x, a \in E$, c'est chercher les éléments $x_0 \in E$ tels que $f(x_0) = a$.
Ce problème se présente sous un double aspect :

1. Vérifier si déterminer les x est possible ;
2. Dans le cas où c'est possible, déterminer les solutions, c'est-à-dire les éléments $x_0 \in E$ qui satisfont ou conviennent.

6.2 Lois de composition externe

6.2.1 Définition

On appelle loi de composition externe $(\cdot)$ sur les ensembles E et F toute application de $E \times F$ dans E ou encore toute application de $E \times F$ dans F.
Exemple :
Le produit d'un scalaire par un vecteur :

$$\forall \alpha \in \mathbb{K},\ \forall \vec{X} \in V,\ (\alpha, \vec{X}) \mapsto \alpha\vec{X} \in V.$$

6.2.2 Parties fermées de E

Considérons une loi de composition externe notée $\cdot : E \times F \to E$ pour tout E et F.
Une partie E' de E est dite stable ou fermée pour cette loi si :

$$\forall a \in E',\ \forall k \in F,\ a \cdot k \in E'.$$

6.3 Homomorphismes et isomorphismes

6.3.1 Définition d'un homomorphisme

Soient E et F deux ensembles munis respectivement des lois de composition interne $*$ et $\top$. Une application $f : E \to F$ est un homomorphisme pour les lois $*$ et $\top$ si :

$$\forall x_1, x_2 \in E,\ f(x_1 * x_2) = f(x_1) \top f(x_2)$$

6.3.2 Définition d'un isomorphisme

Soient E et F deux ensembles munis respectivement des lois de composition interne $*$ et $\top$. Une bijection $f : E \to F$ est dite régulière pour les lois $*$ et $\top$ si :

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

f est appelé isomorphisme.
En d'autres termes, f est un isomorphisme signifie que f est un homomorphisme bijectif.

Définition 6.3.2.1 *soit $(E, *), (F, \top)$ une bijection f de E dans F est dite régulière par la loi $*$ et $\top$ si*
$a * b = c \Rightarrow f(a) \top f(b) = f(c) \forall a, b, c \in E$
on dit alors que f est un isomorphisme de E sur F.

Rémarque 6.3.2.1 Un peu de terminologie
- *Un* **Morphisme** *est aussi appelé homomorphisme.*
- *Lorsque les ensembles de départ et d'arrvivée sont les mêmes on parle* **d'endomorphisme**.
- *Un morphisme bijectif est appelé isomorphisme.*
- *Un isomorphisme bijectif d'un ensemble vers lui même s'appelle* **automorphisme**.

Chapitre 7

Semi-groupe et Groupes

7.1 Quasigroupes et Semi-groupes

Définition 7.1.0.2 *On appelle magma, tout couple $(E, *)$ où E est un ensemble et $*$ une loi de composition interne sur E.*

Rémarque 7.1.0.2 *Si $*$ est associatif(resp. commutatif) le magma est dit associatif (resp. commutatif)*

Définition 7.1.0.3 *On appelle monoide tout magma, associatif et unitaire.*

Rémarque 7.1.0.3 *Si la loi est commutative alors le monoide commutatif.*

Définition 7.1.0.4 *On appelle quasigroupe tout ensemble Q muni de deux lois $(\cdot)$ et $(\setminus)$ vérifiant les propriétés suivantes :*
$\forall a, b \in Q; \quad a \cdot (a \setminus b) = b, \quad a \setminus (a \cdot b) = b.$

En d'autres termes, un quasigroupe c'est un magma $(Q, \cdot)$ où l'on peut resoudre les équations $a \cdot x = b$ et $y \cdot a = c$ et on trouve comme solution respectivement
$x = a \setminus b = a^{-1}b$, $y = a^{-1}((a \cdot c) \cdot a^{-1})$

Définition 7.1.0.5 *On appelle boucle tout quasigroupe admettant un élément neutre.*

Définition 7.1.0.6 *Un ensemble non vide avec une opération associative est appelé semi-groupe.*

Théorème 7.1.0.1 *Le produit de quelques éléments du semi-groupe ne dépend pas de la disposition des parenthèses. Ce résultat permet d'utiliser $a_1 a_2 \dots a_n$ sans mettre les parenthéses.*

Théorème 7.1.0.2 *Si les $a_1, \dots, a_n$ sont les éléments d'un semi-groupe tels que $a_i a_j = a_j a_i |; \forall i, j$ alors,*

$$a_1 a_2 \dots a_n = a_{\sigma(1)} a_{\sigma(2)} \dots a_{\sigma(n)}$$

où σ est une permutation quelconque des éléments de l'ensemble $1, 2, \dots, n$.

Démonstration 7.1.0.1 *Démonstration : Par récurrence pour $n = 2$ le théorème est vraie par hypothèse.*
Suppososns que la proposition est vraie jusqu'à l'ordre $(n-1)$.
Si $\sigma(n) = n$ alors en considérant le théorème 7.1.0.1 et l'hypothèse de récurrence nous avons :

$$a_{\sigma(1)} \cdots a_{\sigma(n-1)} \cdot a_n = (a_{\sigma(1)} \ldots a_{\sigma(n-1)}) \cdot a_n = a_n \cdots a_{n-1} \cdot a_n.$$

Si
$n = \sigma(k)$ où $k < n$ alors

$$\begin{aligned} a_{\sigma(1)} \cdots a_{\sigma(n-1)} \cdot a_{\sigma(n)} &= (a_{\sigma_{(1)}} \cdots a_{\sigma(k-1)})(a_{\sigma(n)}(a_{\sigma(k+1)} \cdots a_{\sigma(n)})) \\ &= a_{\sigma_{(1)}} \cdots a_{\sigma(k-1)} a_n a_{\sigma(k+1)} \cdots a_{\sigma(n)} \\ &= (a_{\sigma(1)} \cdots a_{\sigma(k-1)})(a_n(a_{\sigma(k+1)} \cdots a_{\sigma(n)})) \\ &= (a_{\sigma(1)} \cdots a_{\sigma(k-1)})((a_{\sigma(k+1)} \cdots a_{\sigma(n)})a_n) \\ &= a_{\sigma(1)} \cdots a_{\sigma(k-1)} a_{\sigma(k+1)} \cdots a_{\sigma(n)} a_n = a_1 \cdots a_n. \end{aligned}$$

Conséquence 7.1.0.1 *Pour tout élément $a_1, a_2, \cdots, a_n$ d'un semi-groupe commutatif et pour toute permutation σ de l'ensemble $1, 2, \cdots, n$ légalité suivante est vérifiée :*

$$a_1 a_2 \cdots a_n = a_{\sigma(1)} \cdot a_{\sigma(2)} \cdots a_{\sigma(n)}. \tag{7.1}$$

Définition 7.1.0.7 *Le sous-ensemble H non vide d'un semi-groupe est appelé sous-semi-groupe si le produit de chaque 2 éléments de H appartient à H. C'est -à-dire chaque sous-semi-groupe est un semi-groupe.*

Théorème 7.1.0.3 *Toute intersection non vide de sous-semi-groupe est un sous-semi-groupe.*

Démonstration 7.1.0.2 *soit $\bigcup$ l'intersection de sous-semi-groupes. Si $x, y \in \bigcup$ alors x et y appartiennent à chaque sous-semi-groupe entrant dans l'intersection. Alors xy appartient à chaque sous-semi-groupe c'est-á-dire $x \cdot y \in \bigcup$.*

Définition 7.1.0.8 *L'application φ du semi groupe A vers le semi-groupe B est appelé homomorphisme si $\varphi(xy) = \varphi(x)\varphi(y)$ $\forall x, y \in A$. (Nous soulignons que $x \cdot y$ représente l'opération dans A et $\varphi(x)\varphi(y)$ dans B).*

Théorème 7.1.0.4 *$\varphi : A \to B$ est un homomorphisme de semi-groupe surjectif et e neutre dans A alors $\varphi(e)$ est neutre dans B.*

Théorème 7.1.0.5 *Si $\varphi : A \to B$ homomorphisme de semi-groupe surjectif $a \in A$ et, $a^{(-1)}$ existe alors $\varphi(a^{(-1)}) = (\varphi(a))^{(-1)}$.*

Théorème 7.1.0.6 *Si $\varphi : A \to B$ est un homorphisme de semi-groupe alors $Im\varphi$ est un sous-semi-groupe du semi-groupe B.*

Théorème 7.1.0.7 *Si $\varphi : A \to B$ est un homorphisme de semi-groupe alors le noyau $Ker\varphi$ partitionne A.*

Démonstration 7.1.0.3 *Si x et u sont dans la même classe d'équivalence dans cette partition, de même que y et v, alors en raison de la définition de la partition $Ker\varphi$ nous avons $\varphi(x) = \varphi(u)$ et $\varphi(y) = \varphi(v)$. Comme φ est un homomorphisme alors $\varphi(xy) = \varphi(x)\varphi(y) = \varphi(u)\varphi(v) = \varphi(uv)$ soit xy et uv sont dans la même classe d'équivalence.*

Théorème 7.1.0.8 *Supposons que $\varphi : A \to B$ homomorphisme surjectif de semi-groupe et $\pi : A \to A/Ker\varphi$ l'application canonique alors il existe un isomorphisme $\chi : B \to A/Ker\varphi$ tel que $\varphi\chi = \pi$.*

7.2 Groupes

Groupe

Définition 7.2.0.9 *Le semi-groupe est appelé groupe s'il contient un élément neutre et que chaque élément admet un symétrique.*

Définition 7.2.0.10 *La structure algébrique $(G, \star)$ est appelé groupe si :*
- *$\star$ est associative dans G*
- *$\star$ admet un élément neutre dans G*
- *chaque élément de G admet un symétrique qui est dans G.*

Si en plus $\star$ est commutative dans G, alors on dit que G est un groupe commutatif ou groupe abelien, ou encore G admet une structure de groupe abelienne ou une structure de groupe commutatif.

Rémarque 7.2.0.4 *Dans un groupe tout élément admet toujours un unique élément symétrique.*

L'unique élément symétrique de a est noté a^{-1}. Nous avons
- e^{-1}. L'élément neutre est son propre symétrique.
- $(a^{-1})^{-1} = a$.
- $(a * b)^{-1} = b^{-1} * a^{-1}$. Le symétrique d'un produit est le produit inverse des symétriques.
- De manière générale, $(a_1 * a_2 * \cdots * a_n)^{-1} = a_n^{-1} * \cdots * a_1^{-1}$.

En particulier on a $(a^n)^{-1} = (a^{-1})^n$ pour tout $n \in \mathbb{N}$. On notera alors que $a^{-n} = (a^n)^{-1}$, ce qui permet de définir a^n pour tout $n \in \mathbb{Z}$ en convenant que $a^0 = e$.

Exemple 7.2.0.1
- *L'ensemble des nombres complexes de module 1 muni de la multiplication $(\cdot)$ est un groupe abélien noté $(U, \cdot)$*
- *L'ensemble des entiers relatifs muni de l'addition usuelle $+$ noté $(\mathbb{Z}, +)$. Lélément neutre est 0, le symétrique de chaque élément est son opposé. C'est un groupe abélien.*
- *L'ensemble des racines $n-$iéme de l'unité dans $(\mathbb{C})$, avec pour loi la multiplication est un groupe abélien noté $(\mathbf{U}_n, \cdot)$. L'élément neutre est 1. C'est un groupe abélien fini, il contient n éléments.*

- *L'ensemble des matrices inversibles à n lignes et n colonnes à coefficient dans un corps ou champ $\mathbb{K}$ muni de la multiplication des matrices est un groupe noté $(\mathbf{GL}_n(\mathbb{K}), \times)$. L'élément neutre est la matrice identité, l'élément symétrique de chaque matrice est son inverse. C'est un groupe non abélien dès que $n > 1$*
- *Soit Ω un ensemble quelconque non vide et $S(\Omega)$ l'ensemble des bijections de Ω dans Ω muni de la composition des applications $(\circ)$. c'est un groupe noté $(\mathbf{S}(\Omega), \circ)$. Si Ω est un ensemble fini, alors $\mathbf{S}(\Omega)$ est groupe fini et a pour cardinal $n!$ si $card(\Omega) = n$. Dans le cas contraire, c'est un groupe infini. Ce groupe est non abélien dès que $card(\Omega) > 2$.*
- *L'ensemble des isométries affines du plan euclidien P muni de la composition des fonctions est un groupe noté $\mathbf{Is}(P)$. Ce groupe est infini et non abélien contenant des translations, des rotations, des réflexions.*
- *Construisons un autre exemple de la manière suivante. Soient $(E, *)$ et $(F, \circ)$ deux groupes. Définissons dans $E \times F$ une loi de la manière suivante*

$$(a, b) \star (c, d) = (a * c, b \circ d).$$

Alors $(E \times F, \star)$ est un groupe, appelé produit directe de $(E, *)$ par $(F, \circ)$. Si $(E, *) = (F, \circ)$ alors, on notere ce groupe E^2. De même on peut définir le produit de n groupes et noté E^n.

Définition 7.2.0.11 *Le sous-ensemble H du groupe G est appelé sous-groupe si H est un sous-semi-groupe et que chaque élément admet un inverse.*

Définition 7.2.0.12 *Le sous-ensemble H du groupe G est appelé sous-groupe si :*
- $H \neq \emptyset$
- $\forall x, y \in H, x * y \in H$
- $\forall x, y \in H, x * y^{-1} \in H$

Rémarque 7.2.0.5 *Chaque sous-groupe H du groupe G contient l'élément neutre. En effet $\forall h \in H; h^{-1} \in H$ alors $hh^{-1} = 1 \in H$.*

Rémarque 7.2.0.6 *Parfois la notation $H < G$ est utilisée pour dire que H est un sous groupe de G. Dans le cas où on n'exclut pas la possibilité que H soit égal à G on note $H \leq G$.*

Exemple 7.2.0.2 – *Relativement à l'addition nous avons $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$*
- *$n\mathbb{Z} < \mathbb{Z}$ relativement à $+$ oú $n\mathbb{Z}$ est l'ensemble des multiples de n*
- *$\mathbf{U}_n < \mathbf{U} < (\mathbb{C}^\star)$ relativement à la multiplication.*
- *$\mathbf{GL}_n(\mathbb{Q}) < \mathbf{GL}_n(\mathbb{R}) < \mathbf{GL}_n(\mathbb{C})$ relativement à la multiplication.*
- *Soit $\mathbf{T}$ l'ensemble des translations du plan euclidien alors, $\mathbf{T} < \mathbf{Is}(P) < \mathbf{S}(P)$ relativement à la composition des applications (transformations).*
- *Notons par $\mathfrak{R}_A$ l'ensemble des rotations de centre A du plan euclidien alors, $\mathfrak{R}_A < \mathbf{Is}(P)$.*

Théorème 7.2.0.9 *L'intersection d'une famille de sous-groupe est un sous-groupe.*

Soient $(G, \times)$ un groupe et $\mathfrak{F}$ une famille non vide de sous groupes de G (ici $\mathfrak{F}$ peut être en nombre fini ou non). Notons par I l'intersection de tous les éléments de $\mathfrak{F}$, soit $I = \bigcap_{H \in \mathfrak{F}} H$. D'après le théorème précedant, I lui même est un groupe.

7.2.1 Sous groupe engendré par une partie

Soit $(G, \times)$ un groupe et A un sous ensemble non vide de G.

Définition 7.2.1.1 *On appelle sous groupe engendré par A c'est l'intersection de tous les sous groupes contenant A. Il est noté par $\langle A \rangle$. Soit $\mathfrak{T}$ l'ensemble de tous les sous groupes de G contenant A alors,*

$$\langle A \rangle = \bigcap_{H \in \mathfrak{T}} H.$$

Rémarque 7.2.1.1 *$\mathfrak{T}$ n'est pas vide car il contient G.*

Proposition 7.2.1.1 *Le sous groupe $\langle A \rangle$ est le plus petit sous groupe de G contenant A. Soit $\langle A \rangle$ est caractérisé par les deux conditions suivantes*
– $\langle A \rangle$ est un sous groupe de G contenant A.
– Si K est un autre sous groupe de G contenant A alors, $\langle A \rangle \subseteq K$.

Proposition 7.2.1.2 *Soit $(G, \times)$ un groupe et, A un sous ensemble non vide de G et $x \in \langle A \rangle$. Ii existe $n \in \mathbb{N}^\star$ et des éléments $y_1, y_2, \cdots, y_n$ où $y_i \in A$ et $y_i^{-1} \in A$ pour $i \in \{1, 2, \cdots, n\}$ tels que $x = y_1 \times y_2 \times \cdots \times y_n$.*

Définition 7.2.1.2 *Soient $(G_1, *)$ et $(G_2, \circ)$ deux groupes et ψ une application de G_1 dans G_2. On dit que ψ est un homomorphisme ou encore un morphisme de groupe ou tout simplement un morphisme, lorsqu'elle vérifie la condition suivante*

$$\forall x, y \in G_1 \;\; \phi(x * y) = \phi(x) \circ \phi(y).$$

Proposition 7.2.1.3 *L'image de l'élément neutre du groupe de départ par un morphisme est lélément neutre du groupe d'arrivée. Soit $\phi(e_{G_1}) = e_{G_2}$.*

Proposition 7.2.1.4 *Par un morphisme l'image du symétrie d'un élément est le symétrie de l'image de cet élément. Soit $\phi(a^{-1}) = [\phi(a)]^{-1}$.*

Définition 7.2.1.3 *On appelle l'image de H par $\phi(H)$ l'ensemble défini par $\phi(H) = \{\phi(h) : h \in H\}$.*

Proposition 7.2.1.5 *Soient ϕ un morphisme de G_1 dans G_2 et H un sous groupe de G_1 alors, $\phi(H)$ est sous groupe de G_2. En particulier $\phi(G_1)$ est un sous groupe de G_2 . Soit $H \leq G_1 \Rightarrow \phi(H) \leq G_2$.*

Définition 7.2.1.4 *On appelle noyau de ϕ et l'on note $ker\phi$ l'ensemble défini par $ker\phi = \{g \in G_1 : \phi(g) = e_{G_2}\}$.*

Proposition 7.2.1.6 *Le noyau d'un morphisme est un sous groupe du groupe de départ. Soit $ker\phi \leq G_1$.*

Proposition 7.2.1.7 *Pour qu'un morphisme soit injectif il faut et il suffit que son noyau se réduise á l'élément neutre. Soit ϕ injectif $\Leftrightarrow ker\phi = \{e_{G_1}\}$.*

Conséquence 7.2.1.1 *Soient G_1 et G_2 deux groupes finis de même cardinal et ϕ un morphisme de G_1 dans G_2. Pour que ϕ soit un isomorphisme il faut et il suffit que $ker\phi$ soit réduit á l'élément neutre.*

Exemple 7.2.1.1 Quelques exemples de morphisme
– *(i)*

$$\begin{array}{rccc} \exp & : & (\mathbb{R},+) & \longrightarrow & (\mathbb{R}^{\star+},\cdot) \\ & & x & \mapsto & \exp x \end{array},$$

– *(ii)*

$$\begin{array}{rccc} \exp & : & (\mathbb{R},+) & \longrightarrow & (\mathbf{U},\cdot) \\ & & x & \mapsto & \exp ix \end{array},$$

– *(iii)*

$$\begin{array}{rccc} \det & : & \mathbf{GL}_n(\mathbb{K}) & \longrightarrow & (\mathbb{K}^{\star+},\cdot) \\ & & A & \mapsto & \det A \end{array},$$

– *(iv) Soit $(G,\cdot)$ un groupe et $x \in G$. L'ápplication*

$$\begin{array}{rccc} \exp & : & (G,\cdot) & \longrightarrow & (G,\cdot) \\ & & a & \mapsto & x^{-1}ax \end{array},$$

est un automorphisme. Les automorphismes construits de cette manières s'appellent automorphismes intérieur. L'ensemble des automorphismes intérieures, noté $\mathbf{Int}(G)$, forme un groupe relativement á la loi de composition des applications.
– *(v) Soit $(G,\circ)$ un groupe quelconque et $x \in G$. L'application suivante est un morphisme de groupe.*

$$\begin{array}{rccc} f_g & : & (\mathbb{Z},+) & \longrightarrow & ((G,\circ) \\ & & n & \mapsto & g^n. \end{array}$$

7.2.2 Relation déquivalence induite dans un groupe par un sous groupe

Rémarque 7.2.2.1 *Soit $(G,\times)$ un groupe et H un sous groupe de $(G,\times)$ alors, H peut induire dans $(G,\times)$ deux relations d'équivalences telle que l'une soit une relation d'équivalence à droite et l'autre une relation d'équivalence à gauche définies de la manière suivante.*

Définition 7.2.2.1 *Soit $(G,\times)$ et H un sous groupe de $(G,\times)$ on appelle relation d'équivalence à gauche par le sous groupe H dans $(G,\times)$ la relation définie et notée par $(\mathcal{R}_{gch})_H$ telle que*

$$x\ (\mathcal{R}_{gch})_H\ y \Leftrightarrow x^{-1} \times y \in H.$$

De même nous avons

Définition 7.2.2.2 *Soit $(G, \times)$ et H un sous groupe de $(G, \times)$ on appelle relation d'équivalence à droite par le sous groupe H dans $(G, \times)$ la relation définie et notée par $(\mathcal{R}_{dr})_H$ telle que*

$$x\ (\mathcal{R}_{dr})_H\ y \Leftrightarrow y \times x^{-1} \in H.$$

Théorème 7.2.2.1 *Les relations $(\mathcal{R}_{dr})_H$ et $(\mathcal{R}_{gch})_H$ sont des relations d'équivalences.*

La classe déquivalence de $x \in G$ sera noté $cl(x)$ ou $\bar{x}$, $\dot{x}$ ou encore $[x]$. C'est l'ensemble constitué des éléments de G qui sont en relation avec x soit

$$\bar{x} = \{g \in G : x\ (\mathcal{R}_{gch})_H\ g\}.$$

L'ensemble de toutes les classes d'équivalence est noté G/H et est appelé le quotient de G par H. Quand $y \in [x]$, on dit que y est un représentant de $[x]$. Nous avons toujours que x est le représentant de sa propre classe d'équivalence $[x]$, il est à noter que $[x]$ admet aussi d'autres représentants.
Il est à noter que les classes d'équivalences à gauche définie par $(\mathcal{R}_{gch})_H$ peuvent être aussi interpretées par

$$[x] = x \times H$$

avec

$$x \times H = \{x \times h : h \in H\}.$$

Soit H un sous groupe du groupe G et $g \in G$, l'ensemble de tous les produits gh où $h \in H$ forme une classe á gauche du sous-groupe H et, est notée gH. De même on définit l'ensemble Hg.
Si $g \in H$ alors $gH = H$. En effet $gH \subset H$ car H est un sous-groupe. Maintenant soit $h \in H$ alors comme H est un sous-groupe, nous avons $g^{-1}h \in H$ ce qui entraîne que $h = g(g^{-1}h) \in gH$. c'est-á-dire $H \subset gH$. D'oú $gH = H$.

Théorème 7.2.2.2 *L'ensemble de toutes les classes à gauche forme une partition du groupe G pour le sous groupe H.*

Démonstration 7.2.2.1 *Si $g \in G$ alors $g = g.1$ comme $1 \in H$ nous avons $g \in gH$. Pour démontrer le théorème, il serait suffisant d'établir que deux classes à gauche différentes on une intersection vide. Pour cela nous devons supposer le contraire à savoir montrer que deux classes à gauche qui ont des éléments en communs coïncident. Soit si $x \in aH \cap bH$ oú $a, b \in G$ alors $x = ah_1 = bh_2$ avec $h_1, h_2 \in H$. D'ici il vient que $a = (bh_2)h_1^{-1}$. Si en suite $g \in aH$ alors $g = ah$ où $h \in H$. C'est pourquoi $g = ah = ((bh_2)h_1^{-1})h = b(h_2h_1^{-1}h)$ or le produit $h_2h_1^{-1}h \in H$ puisque H est un sous-groupe alors $g \in bH$.*
Nous avons montrer que $aH \subset bH$. On montre de la même manière que $bH \in aH$ et on conclu.

La partition du groupe G par les classes à gauche du sous-groupe H est appelée Partition gauche pour le sous-groupe H. De même on démontre ce théorème en considérant les classes à droite.

Théorème 7.2.2.3 *(LAGRANGE)*
Si H est un sous-groupe du groupe fini G, alors le cardinal du sous-groupe H divise le cardinal du groupe G (soit la puissance du groupe $G = |G|(G : e)$

(Parfois le cardinal d'un groupe est appelé l'ordre) donc ce théorème peut être reformulé de la manière suivante l'ordre du sous-groupe H qui divise l'ordre du groupe G.

Théorème 7.2.2.4 *Si n est le cardinal du groupe G et $m = cardH$ et $k = card\chi$ où χ l'ensemble des classes à droite par le sous-groupe H, alors $n = km$.*

Démonstration 7.2.2.2 *Soient $h_1, \cdots, h_m$ les éléments de H. Le sous-ensemble Hg contient les éléments $h_1g, \cdots, h_mg$. Si $h_ig = h_jg$ alors $h_i = (h_jg)g^{-1} = h_j(gg^{-1}) = h_j$. Ainsi les éléments $h_1g, \cdots, h_mg$ sont tous différents. C'est-à-dire chaque classe à gauche par H contient exactement m éléments. En raison du théorème* 7.2.0.11*, $n = km$.*

Théorème 7.2.2.5 *Si $\varphi : G \to G'$ est un homomorphisme de groupe et 1 le neutre du groupe G alors $\varphi(1)$ neutre dans G' et $\varphi(g^{-1}) = (\varphi(y))^{-1}$.*

Théorème 7.2.2.6 *Si $\varphi : G \to G'$ Homomorphisme de semi-groupe et G un groupe alors $Im\varphi$ est un groupe.*

Conséquence 7.2.2.1 *Si $\varphi : G \to G'$ est un homomorphisme surjectif de semi-groupe et G groupe alors G' est un groupe.*

Définition 7.2.2.3 *Le sous groupe H de G est normal ou distingué G si $\forall h \in H, g \in G$ on a $ghg^{-1} \in H$.*

Définition 7.2.2.4 *Soit $(G, \times)$ un groupe et soit H un sous groupe de G. On dit que H est normal ou distingué dans G ou encore invariant si*

$$\forall g \in G, \;\; g^{-1} \times H \times g \subset H.$$

soit

$$\forall g \in G \;\; \forall h \in H \;\; g^{-1} \times h \times g \in H.$$

De ces définitions nous pouvont prendre cette relation plus forte à savoir H invariant dans G si

$$\forall g \in G, \;\; g^{-1} \times H \times g = H.$$

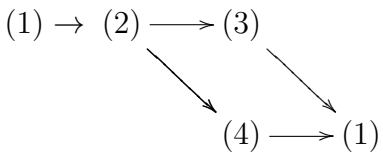
Rémarque 7.2.2.2 *Dire que H est normal ou distingué dans G ce note symboliquement $H \lhd G$. Lorsqu'on exclu pas le fait que H puisse être égal à G alors on note $H \trianglelefteq G$.*

Si le groupe est commutatif alors $ghg^{-1} = h(gg^{-1}) = h \cdot 1 = h$ c'est - à - dire tout sous groupe d'un groupe commutatif est normal.

Théorème 7.2.2.7 *Si H est un sous groupe du groupe du G. Les propositions suivantes sont équivalentes :*

1. *H est un sous groupe normal.*
2. *$gH = Hg \; \forall g \in G$ cette propriété veut dire que la partition à gauche et à droite par le sous groupe normal quoincide.*
3. *La partition á gauche par le sous groupe H de G est admissible.*
4. *La partition á droite par le sous groupe H de G est admissible.*

Démonstration 7.2.2.3 *Il est suffisant de démontrer ce théorème suivant le diagramme suivant :*



(1) $\Rightarrow$ (2) *Si $x \in gH$, alors $x = gh$ pour un certain $h \in H$ écrivons ou représentons x de la manière suivante $x = (ghg^{-1})g$, or par hypothèse nous avons que $ghg^{-1} \in H$. Ainsi $x \in Hg$ du fait que x soit arbitraire nous concluons que $gH \subseteq Hg$. On démontre de la mme manière l'inclusion inverse.*
(2) $\Rightarrow$ (3) *Supposons que $x, u \in aH$ et $y, v \in bH$ où $a, b \in G$ alors ils existent $h_1, h_2, h_3, h_4 \in H$ tels que $x = ah_1$, $u = ah_2$, $y = bh_3$, $v = bh_4$. Il vient que $xy = ah_1bh_3$ et $uv = ah_2bh_4$. Comme $Hb = bH$, il existe $h' \in H$ et $h'' \in H$ tels que $h_1b = bh'$ et $h_2b = bh''$, ainsi*

$$xy = abh'h_3 \in (ab)H$$

et

$$uv = abh''h_4 \in (ab)H.$$

Ce qui montre que nous sommes en présence des classes d'équivalencen et par dela, démontre la possibilité du partitionnement à gauche par H.
(2) $\Rightarrow$ (4) *Se démontre de manière analogue.*
(3) $\Rightarrow$ (1) *Il est clair que $\forall h \in H$ les éléments gh et g appartiennent à une même classe d'équivalence de la partition à gauche par H. De par la possibilité ou l'admissibilité de ce partitionnement, les éléments ghg^{-1} et $gg^{-1} = 1$ doivent aussi appartenir à la même classe d'équivalence. Nous voyons que $1 \in H$ alors $ghg^{-1} \in H$*
(4) $\Rightarrow$ (1) *Se démontre de manière analogue.*

Exemple 7.2.2.1 Sous groupes normaux
- *Soit $(G, \times)$ un groupe abélien alors, tout sous groupe de G sera normal dans G.*
- *si ϕ est un homomorphisme de $(G_1, \times)$ dans $(G_2, \circ)$ alors, $\ker \phi$ sera un sous groupe invariant de G_1 et l'on pourra alors écrire $\ker \phi \trianglelefteq G_1$.*
- *Soit $\mathbf{GL}_n(\mathbb{R})$ l'ensemble des matrices régulières muni de la multiplication des matrices. Et soit l'ensemble H défini par $H = \{\lambda Id : \lambda \in \mathbb{R}^\star\}$ où Id est la matrice identité de $\mathbf{GL}_n$. Alors, $H \trianglelefteq \mathbf{GL}_n(\mathbb{R})$.*

Rémarque 7.2.2.3 *Dans cette remarque nous allons noter tout simplement* $(\mathcal{R})_H$ *en lieu et place de relation á droite ou à gauche. Nous allons parler de la compatibilité de la relation* $(\mathcal{R})_H$ *avec la loi du groupe* G *lorsque* $H \trianglelefteq G$. *Soit* $(G, \times)$ *un groupe et* $H \trianglelefteq G$, *la relation d'équivalence* $(\mathcal{R})_H$ *définie par le sous groupe invariant* H *a la propriété dêtre compatible avec la loi* $\times$ *soit*

$$\left.\begin{array}{lll} a_1 & (\mathcal{R})_H & a_2 \\ b_1 & (\mathcal{R})_H & b_2 \end{array}\right\} \Rightarrow a_1 \times b_1 \ \ (\mathcal{R})_H \ \ a_2 \times b_2.$$

Rémarque 7.2.2.4 *On peut aussi faire de l'opération sur les classes. Ainsi soit,* $(G, \times)$ *un groupe et* H *un sous groupe distingué de* G. *Nous rappelons que l'écriture* G/H *est l'ensemble des classes d'équivalences par la relation* $(\mathcal{R})_H$. *On peut ainsi définir une loi* $\bar{\times}$ *sur* G/H *de la manière suivante*

$$\begin{array}{rccl} \bar{\times} & : & G/H \times G/H & \longrightarrow & G/H \\ & & (\bar{a}_1, \bar{a}_2) & \mapsto & cl(represent.\ quelconque\ de\ a_1, represent.\ quelconque\ de\ a_2). \end{array}$$

Proposition 7.2.2.1 *Soit* $(G, \times)$ *un groupe et* $H \trianglelefteq G$ *alors,* $(G/H, \bar{\times})$ *est un groupe.*

Proposition 7.2.2.2 *Soit* $(G, \times)$ *un groupe et* $H \trianglelefteq G$ *alors, l'application* p *définie par*

$$\begin{array}{rccl} p & : & (G, \times) & \longrightarrow & (G/H, \bar{\times}) \\ & & x & \mapsto & cl(x) \end{array}$$

est un homomorphisme de groupe. Il est surjectif et, son noyau est égal H.

Proposition 7.2.2.3 *Soient* $(G_1, \times)$ *et* $(G_2, \diamond)$ *deux groupes* ϕ *un homorphisme de* $(G_1, \times)$ *dans* $(G_2, \circ)$. *Il existe un isomorphisme* χ *de* $G_1/\ker\phi$ *sur* $\Phi(G_1)$ *tel que* $\phi = \chi \circ p$ *où* p *est la surjection canonique de* G_1 *sur* $G_1/\ker\phi$. *On a donc*

$$G_1/\ker\phi \cong \Phi(G_1)$$

et le diagramme commutatif suivant est vérifié

$$\begin{array}{rccc} \phi : & G_1 & \longrightarrow & \phi(G_1) \subseteq G_2 \\ & \searrow^{p} & & \nearrow_{\chi} \\ & & G_1/\ker\Phi & \end{array}.$$

Exemple 7.2.2.2 Exemple de groupes où peut être appliqué le théorème d'isomorphisme
- *(i)* $(\mathbb{R}/2\pi) \cong \mathbf{U}$
- *(ii)* $\mathbf{GL}_n(\mathbb{K})/\mathbf{SL}_n(\mathbb{K}) \cong \mathbb{K}^\star$
- *(iii) Tout groupe fini d'ordre* n *est isomorphe à* $\mathbb{Z}/n\mathbb{Z}$.

Théorème 7.2.2.8 *Toute admissibilité de partitionnement du groupe* G *est une partition gauche par un sous-groupe normal quelconque. Ce sous-groupe normal est constitué des classes d'équivalence de cette partition contenant l'élément unité.*

Démonstration 7.2.2.4 *Supposons que $\sum$ est une partition quelconque admissible du groupe G par H et constitue l'ensemble des classes d'équivalence de cette partition contenant l'élément unité. Si $h_1, h_2 \in H$ alors en notant $[x]$ la classe d'équivalence de $\sum$ contenant x nous aurons $[h_1] = [h_2] = [1]$. De part la possibilité du partitionnement $\sum$ il vient que $[h_1h_2] = [h_1][h_2] = [1][1] = [1.1] = [1] = H$. Ainsi $h_1h_2 \in H$ c'est-à-dire H est un sous-semi-groupe. Si $h \in H$ alors $[h] = [1]$. De part la possibilité du partitionnement $\sum$ il vient que $[h^{-1}] = [1.h^{-1}] = [1][h^{-1}] = [h][h^{-1}] = [hh^{-1}] = [1] = H$ c'est-à-dire $h^{-1} \in H$. Ainsi H est un sous-groupe. Si K est une certaine classe de la partition $\sum$ alors fixons dans K un certain élément k. Ainsi $[k] = K$ et pour tout $h \in H$ nous avons que $[kh] = [k][h] = [k][1] = [k.1] = [k]$ c'est-à-dire $kh \in K$ ce qui entraîne que $kH \subset K$. Si $x \in K$ alors $[k] = [x]$ et nous aurons $[k^{-1}][k] = [k^{-1}][x] = [k^{-1}k] = [1]$. Ceci entraîne que $k^{-1}x = h \in H$. D'où $x = kh \in kH$. Soit $K \subseteq kH$ donc $K = kH$. Ceci démontre que la partition $\sum$ coincide avec la partition par le sous-groupe H. Sa normalité provient du théorème 7.2.2.7.*

Le théorème 7.2.2.8 nous montre qu'au lieu de parler de Facteur de groupe par une partition possible, on peut tout simplement parler de Facteur de groupe par le sous-groupe normal H.

Théorème 7.2.2.9 *[Théoréme d'homomorphisme pour les groupe] Si $\varphi : G \to G'$ un homomorphisme surjectif de groupe, $Ker\varphi$ le noyau de φ est un sous-groupe normal et $\pi : G \to G/Ker\varphi$ une application canonique (homomorphisme naturel) alors il existe un isomorphisme $\chi : G' \to G/Ker\varphi$ tel que $\varphi\chi = \pi$.*

La démonstration de ce théorème est laissée en exercice

Dans la suite nous allons définir les opérations suivantes :

Soit $g \in G$ et $n \in \mathbb{Z}$ alors posons

$$g^n = \begin{cases} \underbrace{g \cdots g}_{n\ fois} & \text{si n}>0 \\ 1 & \text{si n}=0 \\ \underbrace{g^{-1} \cdots g^{-1}}_{|n|\ fois} & \text{si n}<0 \end{cases}$$

$$ng = \begin{cases} \underbrace{g + g \cdots + g}_{n\ fois} & \text{si n}>0 \\ 0 & \text{si n}=0 \\ \underbrace{(-g) + (-g) + \cdots + (-g)}_{|n|\ fois} & \text{si n}<0 \end{cases}$$

Théorème 7.2.2.10 $g^m.g^n = g^{m+n}$

Démonstration 7.2.2.5 *Si $m = 0$ alors $g^0.g^n = 1.g^n = g^n = g^{0+n}$. De même si $n = 0$.*

Si $m, n \neq 0$ alors les différents cas suivants sont possibles.

	m	n
1	>0	>0
2	>0	<0
3	<0	>0
4	<0	<0

cas 1 :
$g^m.g^n = \underbrace{(g\cdots g)}_{m\ fois}\underbrace{(g\cdots g)}_{n\ fois} = \underbrace{g\cdots g}_{n+n\ fois} = g^{m+n}$.
cas 2 :
on casse en trois cas : a) $m > |n|$, b) $m = |n|$, c) $m < |n|$ en raison de l'addition dans $\mathbb{Z}$.
$m+n = m-|n|$, $m+n = 0$ et $m+n = -(|n|-m)$ correspondament. Alors comme $gg^{-1} = g^0 = 1$ nous aurons : $g^m.g^n = g^{m+n}$.
Le cas 3 est analogue au cas 2.
Cas 4 :
nous avons $m+n = -(|m|+|n|)$ ce qui entraine $g^m.g^n = \underbrace{(g^{-1}\cdots g^{-1})}_{|m|\ fois} \times \underbrace{(g^{-1}\cdots g^{-1})}_{|m|\ fois} =$

$\underbrace{(g^{-1}\cdots g^{-1})}_{|m|+|n|\ fois} = g^{-(|m|+|n|)} = g^{m+n}$.

Théorème 7.2.2.11 $(g^m)^n = g^{mn}$

Démonstration 7.2.2.6 *Si $m = 0$ alors $(g^0)^n = 1^n = 1 = g^0 = g^{0.n}$ de même si $n = 0$ alors $(g^m)^0 = 1 = g^0 = g^{m\times 0}$.*
Supposons maintenant que $m, n > 0$ alors
$(g^m)^n = \underbrace{\underbrace{(g\cdots g)}_{|m|\ fois}\cdots\underbrace{(g\cdots g)}_{|m|\ fois}}_{|n|\ fois} = \underbrace{g\cdots g}_{m\times n\ fois} = g^{mn}$.
En suite nous savons à partir du théorème 7.2.0.18 que
$\forall k$, $g^k\cdots g^{-k} = g^{-k}\cdots g^k = 1$ donc $(g^k)^{-1} = g^{-k}$.
C'est pourquoi si $n > 0$ implique que $n = -|n|$ alors pour tout entier relatif nous avons $(g^m)^n = (g^m)^{(-|n|)} = g^{m(-|n|)} = ((g^m)^{|n|})^{-1} = (g^{m|n|})^{-1} = g^{-m|n|} = g^{mn}$.
Si $m < 0$ et $n > 0$ alors $(g^m)^n = (g^{|m|})^n = \underbrace{(g^{-1}\cdots g^{-1})^n}_{|m|\ fois} = ((g^{-1})^{|m|})^n = (g^{-1})^{|m|n} =$

$g^{-|m|n} = g^{mn}$.

Définition 7.2.2.5 *Le groupe G est appelé groupe monogène s'il existe dans G un élément g tel que $\forall x \in G, \exists n \in \mathbb{Z} : x = g^n$ l'élément g est appelé élément engendrant ou générateur du groupe G.*

Définition 7.2.2.6 *Le groupe G est appelé groupe cyclique s'il existe dans G un élément g tel que $\forall x \in G, \exists n \in \mathbb{Z} : g^n = e$ l'élément g est appelé élément engendrant ou générateur du groupe G.*

Rémarque 7.2.2.5 *On voit que chaque groupe monogène ou cyclique est un groupe qui est engendré par un seul élément.*

Rémarque 7.2.2.6 *On voit que chaque groupe cyclique est un groupe monogène.*

Rémarque 7.2.2.7 *A partir du théoréme 7.2.2.10. On voit que chaque groupe monogène ou cyclique est commutatif.*

l'ensemble $\mathbb{Z}$ est un groupe monogène pour l'addition engendré par 1 ou -1. Si $m \in \mathbb{N}$ alors l'ensemble $m\mathbb{Z}$ de tous les entiers relatifs qui sont divisibles par m est un sous-groupe. Puisque $(\mathbb{Z}, +)$ est commutatif alors $(m\mathbb{Z}, +)$ est un sous-groupe normal, c'est pourquoi on peut considérer le facteur de groupe $\mathbb{Z}/m\mathbb{Z}$ qui est appelé groupe de résidu modulo m. Le groupe de résidu modulo m contient les classes d'équivalence $[0], [1], [2], \cdots, [m-1]$. Toutes ces classes sont différentes. En effets $i - j \notin m\mathbb{Z}$ si $0 \leq j < i < m$ assurons-nous qu'il n'y a pas plus de m éléments (où qu'il n'y a pas d'autres éléments). En effet $\forall u \in \mathbb{Z}$ nous pouvons écrire $u = mq + r$ où $0 \leq r < m$ comme $[mq] = [0]$ du fait que $mq \in m\mathbb{Z}$ et de la définition l'opération dans le groupe. Nous obtenons $[u] = [mq + r] = [mq] + [r] = [0] + [r] = [r]$. Donc le groupe de résidu modulo m contient exactement m éléments. Et la classe d'équivalence [1] est la classe qui engendre ce groupe.

Proposition 7.2.2.4 *Soit $(G, \times)$ un groupe monogène engendré par $a \in G$. Il y a deux possibilités. Ou bien a est d'ordre fini $d \in \mathbb{N}^\star$ et on a $G = \{a^i, i = 0, 1, \cdots, d-1\}$ ou bien a n'est pas d'ordre fini, on dit alors qu'il est d'ordre infini et $G = \{a^n, n \in \mathbb{Z}\}$. Dans chaque cas les éléments des ensembles indiqués sont deux á deux distincts.*

Rémarque 7.2.2.8 *On voit que l'ordre d'un élement qui engendre un groupe cyclique ou monogène est égal au cardinal de ce groupe.*

Exemple 7.2.2.3 *Sous groupe engendrés*
- $\langle m \rangle = m\mathbb{Z}$.
- $\langle m, n \rangle = pgdc(m, n)\mathbb{Z}$.
- $\mathbf{U}_k = \langle exp(2ik\pi/n) \rangle$.
- *On montre en géometrie que toute isometrie du plan s'écrit comme la composée d'au plus trois réflexions (symétries orthogonales) nous pouvons donc poser*

$$\mathbf{Is}(p) = \langle S_D : \rangle$$

où D est une droite du plan.

Théorème 7.2.2.12 *La classe $[k]$ où $0 \leq k < m$, engendre le groupe de résidu modulo m si et seulement si k et m sont premiers entre eux.*

Pour démontrer ce théorème donnons d'abord le lemme suivant.

Lemme 7.2.2.1 *Tout sous-groupe non nul du groupe $\mathbb{Z}$ coincide avec $m\mathbb{Z}$ pour un certain m.*

Démonstration 7.2.2.7 *Soit H sous groupe non nul de $\mathbb{Z}$ alors H contient des entiers relatifs positifs. Soit m le plus petit d'entre eux alors $m\mathbb{Z} \subset H$. Supposons x un élément quelconque de H alors en divisant x par m avec le reste nous obtenons $x = qm + r$ où $0 \leq r < m$.il est clair que $r = x - mq \in H$. Si $r \neq 0$ alors nous obtenons une contradiction du choix dem (car m était le plus petit) ainsi $r = 0$. Donc $n = qm \in m\mathbb{Z}$ soit $H \subseteq m\mathbb{Z}$ Ainsi $H = m\mathbb{Z}$.*

Démonstration du théorème 7.2.2.12.

Démonstration 7.2.2.8 *Supposons que la classe $[k]$ est génératrice du groupe des résidus modulo m. Si k et m ne sont pas irréductibles (premiers entre eux)alors $k = k'd$ et $m = m'd$ avec $d > 1$ alors $[m'k] = [m'k'd] = [mk'] = [0]$ car $[mk'] \in m\mathbb{Z}$ ensuite considérons les classes $[0], [k], [2k], \cdots, [(m'-1)k]$. Comme $d > 1$ alors elles sont inférieures à m. De l'autre côté $\forall s \in \mathbb{Z}$, nous avons $s = qm' + r$ avec $q \in \mathbb{Z}$ et $0 \leq r < m'$ de là nous avons $[sk] = [(qm' + r)k] = [qm'k] + [rk] = [qm'k'd] + [rk] = [qk'm] + [rk] = [0] + [rk]$ puisque $[qk'm] \in m\mathbb{Z}$. Ainsi les classes que nous avons énumérées couvrent complètement toutes les classes modulo m, ce qui est impossible. Supposons maintenant que k et m sont premiers entre eux alors il existe u et v tel que $um + vk = 1$ d'ici [1]=[um]+[vk]=[0]+[vk]=[vk]. C'est pourquoi $\forall [s] \in \mathbb{Z}/m\mathbb{Z}$(nous rappelons que $0 \leq s < m$) $[s] = s[1] = s[vk] = [svk] = (sv)[k]$ c'est à dire $[k]$ est générateur.*

La construction des groupes monogène ou cycliques est définie par le théorème suivant :

Théorème 7.2.2.13 *Tout groupe cyclique ou monogène est isomorphe au groupe des entiers relatifs par l'addition ou au groupe des résidus modulo un certain m.*

Démonstration : soit G un groupe cyclique avec pour générateur g. Considérons l'application :

$$\varphi : \mathbb{Z} \to G \quad m \mapsto g^m$$

Puisque G est un groupe cyclique alors φ est surjective. A partir du théorème 7.2.0.18 nous avons : $\varphi(k + l) = g^{k+l} = g^k.g^l = \varphi(k)\varphi(l)$ donc φ : homomorphisme. A partir du théorème 7.2.0.17 le groupe G est isomorphe à $\mathbb{Z}/Ker\varphi$. Si $Ker\varphi = \{0\}$ alors toutes les classes d'équivalences par le sous groupe $ker\varphi$ sont constituées d'un seul élément chacune. Ainsi $\mathbb{Z}/Ker\varphi$ coïncide avec $\mathbb{Z}$ soit G isomorphe à Z. Si$Ker\varphi \neq \{0\}$ alors à partir du lemme de la démonstration du théorème 7.2.2.9, $Ker\varphi = m\mathbb{Z}$ pour un certain m alors $\mathbb{Z}/Ker\varphi$ est un groupe résidu modulo m qui est isomorphe au groupe G.

Théorème 7.2.2.14 *[Théorème de Cayley] Pour tout groupe G, il existe un homomorphisme injectif du groupe G dans le groupe Q constitué des applications bijectives du groupe G vers G.*

(faire remarquer que l'on peut prendre un S á la place de G).

Démonstration 7.2.2.9 *Démonstration : Si $g \in G$ alors désignons par $\varphi(g)$ l'application de G vers G définie par l'égalité $x(\varphi(g)) = xg$ pour tout $x \in G$ comme $x = (xg^{-1}g) = (xg^{-1})(\varphi(g))$, alors $\varphi(g)$ est surjective. Montrons maintenant que $\varphi(g)$ est injective pour cela montrons que $\forall x, y \in G$ alors $x(\varphi(g)) = y(\varphi(g)) \Longrightarrow x = y$ Si $x(\varphi(g)) = y(\varphi(g))$ alors $x = (xg)g^{-1} = (x(\varphi(g)))g^{-1} = (y(\varphi(g)))g^{-1} = (yg)g^{-1} = y$*

c'est-à-dire $\varphi(g)$ est une application injective de $G \to G$. Ainsi, $\varphi(g)$ est une application bijective de $G \to G$ c'est-à-dire φ est une application de G vers Q. Si $\varphi(g_1) = \varphi(g_2)$ alors $g_1 = 1(\varphi(g_1)) = 1(\varphi(g_2)) = g_2$ c'est-á-dire φ est injective. De l'égalité $x(\varphi(g_1)\varphi(g_2)) = (x(\varphi(g_1)))(\varphi(g_2)) = (xg_1)g_2 = x(g_1g_2) = x(\varphi(g_1g_2))$ oú x est un élément quelconque de G entraine que $\varphi(g_1)\varphi(g_2) = \varphi(g_1g_2)$ donc φ homomorphisme. C'est ce qu'il fallait démontrer.

7.2.3 Générateurs d'un groupe monogène

Générateurs d'un groupe monogène Soit $G =< a >$ un groupe cyclique d'ordre n. Les générateurs de G sont les éléments a^k où k et n sont premières entre eux. Le nombre de générateurs de G est donc le nombre des entiers k vérifiant $1 \leq k \leq n$ et $k \wedge n = 1$. Ce nombre est noté par $\varphi_{(n)}$ L'application $\varphi : \mathbb{N}^\star \to \mathbb{N}^\star$ ainsi définie s'appelle Indicateur d'Euler.

Rémarque 7.2.3.1 *: Un groupe cyclique est un groupe monogène fini.*

Exemple : Soit $G = \mathbb{Z}/3\mathbb{Z}$ alors le groupe $\mathcal{Q}$ considéré au Théorème 7.2.0.22 est le groupe de permutation de l'ensemble {0,1,2} et l'application φ décrit dans le théorème est :

$$\varphi([0]) = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix},$$

$$\varphi([1]) = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix},$$

$$\varphi([2]) = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix}.$$

A partir de la démonstration des théorèmes précédants on voit que chaque groupe fini s'applique sur le groupe des applications bijectives d'un ensemble fini vers lui-même c'est-à-dire le groupe des permutations de l'ensemble $\{1, 2, \cdots, n\}$ pour un certain n et se note $\mathcal{O}_n$. le groupe symétrique d'ordre n contient $n!$ éléments.

Considérons quelques unes de ses propriétés :

Définition 7.2.3.1 *Appelons cycle et notons $(i_1, i_2, \cdots, i_k)$ où $i_1, i_2, \cdots, i_k$ sont des nombres différents de l'ensemble $\{1, 2, \cdots, n\}$ une permutation σ telle que*

$$\sigma(i) = \begin{cases} i & si\ i \notin \{i_1, \cdots, i_k\} \\ i_{h+1} & si\ i = i_h\ et\ h \neq k \\ i_1 & si\ i = i_k \end{cases}.$$

Rémarque 7.2.3.2 *l'ensemble $\{1, 2, \cdots, n\}$ s'appelle le support du cycle σ.*

Exemple dans le groupe $\mathcal{O}_6$ nous avons :

$$(135) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 4 & 1 & 6 \end{pmatrix}.$$

Rémarque 7.2.3.3 *Un cycle constitué de deux éléments est appelé transposition.*

Exemple :

$$(35) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 5 & 4 & 3 & 6 \end{pmatrix}.$$

Deux cycles qui ne contiennent pas les mêmes éléments sont libres ou indépendants.

Théorème 7.2.3.1 *Si ρ et σ sont deux cycles indépendants, alors $\rho\sigma = \sigma\rho$.*

Démonstration 7.2.3.1 *: notons que si $i \in \rho$ entraîne $i\rho \in \rho, i\rho \notin \sigma$ et $i \notin \sigma$ de même $i\sigma \in \sigma, i\sigma \notin \rho$ et $i \notin \rho$ si $i \in \sigma$. C'est pourquoi*

$$i(\rho\sigma) = (i\rho)\sigma = \begin{cases} i\rho = i & si\ i \notin \rho \cup \sigma \\ = i\rho & si\ i \in \rho \\ = i\sigma & si\ i \in \sigma \end{cases},$$

et

$$i(\sigma\rho) = (i\sigma)\rho = \begin{cases} i\rho = i & si\ i \notin \rho \cup \sigma \\ = i\rho & si\ i \in \rho \\ = i\sigma & si\ i \in \sigma \end{cases}.$$

Ainsi $i(\rho\sigma) = i(\sigma\rho) \qquad \forall i \to \rho\sigma = \sigma\rho$.

Théorème 7.2.3.2 *Si les cycles $\sigma_1, \sigma_2, \cdots, \sigma_m$ sont deux à deux disjoints ou indépendants, alors $\sigma_1\sigma_2\cdots\sigma_m = \sigma_{\pi(1)}\sigma_{\pi(2)}\cdots\sigma_{\pi(m)}$ pour toute permutation $\pi \in O_m$ ou S_m.*

Groupe opérant sur un ensemble

Définition 7.2.3.2 *Soit E un ensemble non vide, soit G un groupe noté multiplicativement. On dit que le groupe G* **opère à gauche** *sur E si l'on peut définir sur E la loi externe à gauche*

$$\begin{array}{rccc} (\cdot) & : & G \times E & \longrightarrow & E \\ & & (g, x) & \mapsto & g \cdot x \end{array},$$

de domaine G telle que :
– O1 $\forall g_1, g_2 \in G$ et $\forall x \in E \quad (g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$
– O1 $e \cdot x = x \quad \forall x \in E$ où e est le neutre dans G.

Proposition 7.2.3.1 *Soit G opérant à gauche sur E alors, l'application*

$$\begin{array}{rccc} f & : & G & \longrightarrow & \sigma_E \\ & & g & \mapsto & f_g : f_g(x) = g \cdot x \end{array},$$

est un homomorphisme. Avec σ_E groupe de permutations de l'ensemble E.
Réciproquement *si*

$$\begin{array}{rccc} f & : & G & \longrightarrow & \sigma_E \\ & & g & \mapsto & f_g \end{array}$$

est un homomorphisme de groupes alors, l'application

$$\begin{array}{rccc} \cdot & : & G \times E & \longrightarrow & E \\ & & (g,x) & \mapsto & g \cdot x = f_g(x) \end{array}$$

définit une opération à gauche de G sur E.

En d'autres mots, la donnée d'une opération à gauche de G sur E équivaut à la donnée d'un homomorphisme.

Démonstration 7.2.3.2 *: Montrons que $\forall g \in G$, f_g est dans σ_E il revient à montrer que f_g est bijective. En effet considérons $x, x' \in E$ il vient :*

$$g \cdot x = g \cdot x' \Leftrightarrow f_g(x) = f_g(x')$$

puisque G est un groupe en composant de part et d'autre par g^{-1} et en uitlisant O1 il vient :

$$g^{-1}(g \cdot x) = g^{-1}(g \cdot x') \Leftrightarrow (g^{-1}g) \cdot x = (g^{-1}g) \cdot x' \Leftrightarrow e \cdot x = e \cdot x',$$

en Appliquant O2 nous obtenons $x = x'$.
Pour montrer la surjection, soit $y \in E$, montrons qu'il existe $x \in E$ tel que $y = f_g(x)$ soit $y = g \cdot x$. On verifie sans peine que $x = g^{-1} \cdot y$ est une solution de cette équation. Montrons maintenant que f est un homomorphisme c'est - à - dire $f_{g_1 g_2} = f_{g_1} \circ f_{g_2}$ en effet

$$\forall x \in E \quad f_{g_1 g_2}(x) = (g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x) = f_{g_1}(f_{g_2}(x)) = f_{g_1} \circ f_{g_2}(x).$$

Conséquence 7.2.3.1
1. $f_e(x) = x \quad \forall x \in E$,
2. $f_{g^{-1}} = (f_g)^{-1} \quad \forall g \in G$.

Réciproquement f étant donné, montrons que

$$\begin{array}{rccc} & G \times E & \longrightarrow & E \\ & (g,x) & \mapsto & g \cdot x = f_g(x) \end{array} \text{ ,}$$

est une opération à gauche de G sur E, c'est - à - dire c'est une loi externe par définition. En effet :

nous obtenons $O1$ par $\quad (g_1 g_2) \cdot x = f_{g_1 g_2}(x) = f_{g_1} \circ f_{g_2}(x) = f_{g_1}[f_{g_2}(x)] = g_1 \cdot (g_2 \cdot x),$

nous obtenons $O2$ par $\quad e \cdot x = (gg^{-1}) \cdot x = g \cdot (g^{-1} \cdot x) = f_g(f_{g^{-1}}(x)) = f_g[(f_g)^{-1}(x)] = x.$

Puisque $f_{g^{-1}}(x) = [f_g(x)]^{-1}$.

Exemple 7.2.3.1 *Soit E un ensemble non vide et, soit σ_E le groupe de permutations de E et soit G un groupe quelconque de permutation (c'est - à - dire G est un sous - groupe de σ_E) On peut faire operer à gauche G sur E par la loi suivante :*

$$\begin{array}{rccc} & G \times E & \longrightarrow & E \\ & (g,x) & \mapsto & g(x). \end{array}$$

On vérifie que l'on a bien O1 et O2. C'est l'opération canonique ou naturelle de G sur E.

Sous-groupes d'isotropie et orbites

Définition 7.2.3.3 *Soit $a \in E$ avec a fixé, définissons l'ensemble $G_a = \{g \in G / g \cdot a = a\}$ où l'on rappelle que G est un groupe qui opère à gauche sur E.*

Proposition 7.2.3.2 *G_a est un sous groupe de G.*

Preuve : en effet $G_a \neq \emptyset$ car $e \in G_a$ puisque $e \cdot a = a$
- $g_1, g_2 \in G_a$ on a $(g_1 g_2) \cdot a = g_1 \cdot (g_2 \cdot a) = g_1 \cdot a = a$
- soit $g \in G_a$ on a $g^{-1} \cdot a = g^{-1}(g \cdot a) = (g^{-1}g) \cdot a = e \cdot a = a$.

Ce qui montre que G_a est un sous goupe de G il s'appelle le sous-groupe d'isotrope.

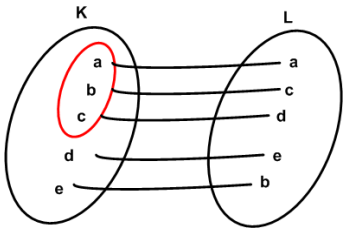
Définition 7.2.3.4 *G_a s'appelle le sous-groupe d'isotropie de a ou stabilisateur de a.*

Exemple

Soit E un ensemble quelconque non vide et, considérons σ_E l'ensemble des permutations de E. Soit G un sous-groupe de σ_E. Comme nous l'avons noté, ceci induit une opération canonique de G sur E. Pour $a \in E$, $\quad G_a = \{g \in G / g(a) = a\}$ ceci est le sous groupe d'isotropie de a, c'est- à- dire l'ensemble des permutations de G, qui l'aissent invariant le point a. Soit A une partie de E, posons $H_A = \bigcap_{a \in A} G_a$. En effet on montre que H_A est un sous-groupe de G comme intersection de sous groupes. Posons d'autre part $B = E \setminus A$ et considérons l'application

$$\begin{array}{rccc} \theta & : & H_A & \longrightarrow & \sigma_B \\ & & g & \mapsto & \theta(g) = g/B. \end{array}$$

θ est un isomorphisme de groupe. Dans la suite, montrons que si $g \in H_A$ on a $g/B \in \sigma_B$.
Illustration nous allons poser dans la figure qui suit $K = L = E = \{a, b, c, d, e\}$ et $B = \{a, b, c\}$.



On voit que g/B est deja une bijection de B sur $g(B)$. Or $g(B) = B$ donc $\theta(g) = g/B \in \sigma_B$

$$(g \circ h)/B = g/B \circ h/B \quad a \in \sigma_B \qquad g_\sigma(x) = \begin{cases} x & \text{si } x \in A \\ \sigma(x) & \text{si } x \in B \end{cases}.$$

Nous venons de montrer que : pour $E \neq \emptyset$ en considérant σ_E et $B \subset E$ avec $(B \neq \emptyset)$ alors, l'application

$$\begin{array}{rccc} j_{A,B} & : & \sigma_B & \longrightarrow & \sigma_E \\ & & g & \mapsto & j_{A,B}(g) = (\diamondsuit) \end{array}$$

$(\diamondsuit)$ la permutation de E qui coincide avec g sur B et laisse invariant chaque élément de $E \setminus B$ est un homomorphisme injectif.

orbites

Soit G opérant à gauche sur l'ensemble E, associons à G la relation :

$$x\mathcal{R}_G y \Leftrightarrow \exists g \in G : y = g \cdot x.$$

Nous laissons le soins au lecteur de montrer que c'est une relation d'équivalence. Pour $x \in E$, posons $G_x = \{y \in E / \exists g \in G : y = g \cdot x\}$. En effet nous avons $x\mathcal{R}_G y \Leftrightarrow y \in G_x \quad (\star)$.

Définition 7.2.3.5 *On appelle orbite de E suivant G (ou encore une G-orbite de E) une classe d'équivalence quelconque modulo $\mathcal{R}_G$.*

D'après $(\star)$ une partie Ω de E est une G-orbite si et seulement si $\exists x \in E : \Omega = G \cdot x$.

Définition 7.2.3.6 *Soit G un groupe opérant à gauche sur un ensemble E. On dit que G opère transitivement si E possède une et une seule G-orbite. Dans le cas contraire, on dit que G opère intransitivement.*

Soit G opérant à gauche sur E. Soit Ω une G-orbite de E. Considerons $a, b \in \Omega$, on voudrait comparer G_a, G_b c'est - à - dire les sous groupes d'isotropie de a et b.

Définition 7.2.3.7 *Deux sous groupes H_1 et H_2 d'un groupe G sont dits conjugués s'il existe $s \in G$ tel que $H_2 = sH_1s^{-1}$.*

Théorème 7.2.3.3 *Soit G opérant à gauche sur E, soit Ω une G-orbite de E, alors $\forall a, b \in \Omega$, alors G_a et G_b sont conjugués.*

Démonstration 7.2.3.3 *Comme Ω est une G-orbite, alors il existe $s \in G$ tel que $b = s \cdot a$. Pour tout g, $g \in G_b \Leftrightarrow g \cdot b = b \Leftrightarrow g \cdot (s \cdot a) = s \cdot a \Leftrightarrow (gs) \cdot a = s \cdot a \Leftrightarrow s^{-1}[(g \cdot s) \cdot a] = a \Leftrightarrow (s^{-1} \cdot g \cdot s) \cdot a = a \Leftrightarrow G_a \Leftrightarrow g \in sG_as^{-1} \Leftrightarrow G_b = sG_as^{-1}$.*

Théorème 7.2.3.4 *Soit G opérant à gauche sur E. Soit Ω une G-orbite, soit $a \in \Omega$(a fixé). Pour tout $x \in \Omega$, considérons $C_x = \{g \in G / g \cdot x = x\}$. Alors l'application $x \longrightarrow C_x$ est une bijection de Ω sur $(G/G_a)_g$.*

Soit $\mathcal{R}_g$ la relation déquivalemce sur G définie comme suit :
$r\mathcal{R}_g s \Leftrightarrow s^{-1}r \in G_a$. On pose alors $G/\mathcal{R}_g = (G/G_a))_g$ comme ensemble des classes à gauche. D'autre part, si sG_a est une classe à gauche qui est égale à gG_a alors, pour tout g, $g \in sG_a$. Montrons que, pour tout $x \in \Omega$ on a $C_x \in (G/G_a))_g$. C'est - à - dire si $x \in \Omega, \exists s \in G : C_x = sG_a$. Soit $s \in C_x$ c'est- à - dire $s \cdot a = x$.

$$g \in C_x \Leftrightarrow g \cdot a = x \Leftrightarrow g \cdot a = s \cdot a \Leftrightarrow s^{-1}(g \cdot a) = a \Leftrightarrow S^{-1}g \in G_a \Leftrightarrow g \in sG_a$$

Rémarque 7.2.3.4 *S'il existe $a \in \Omega$ tel que G_a soit un sous- groupe distingué de G alors, $G_b = G_a \forall \quad b \in \Omega$.*

Conséquence 7.2.3.2 *Si Ω est fini, alors $(G/G_a))_g$ est fini et $Card \quad \Omega = [G : G_a]$.*

Rémarque 7.2.3.5 – *Si $x\mathcal{R}_g y \Leftrightarrow x^{-1}y \in H$ où H est un sous-groupe d'un groupe G et, $(G/H)_g = G/\mathcal{R}_g$ si $x \in G$ la classe (à gauche) de x est xH.*
– *Si les classes à gauche sont finies alors, elles ont toute le même cardinal qui est $Card \quad H$.*

Théorème 7.2.3.5 *Chaque permutation τ se présente sous la forme d'un produit de cycles deux à deux disjoints ou indépendants.*

Démonstration 7.2.3.4 *: pour tout i considérons l'ensemble $\{i = i\tau^0, i\tau, i\tau^2, i\tau^3, \cdots\}$. Comme $i\tau^k \in \{1, 2, \cdots, n\}$, alors il existe un m tel que $i\tau^m = i\tau^{m+h}$ pour un certain $h > 0$. En considérant les théorèmes 7.2.2.10 et 7.2.2.11 nous obtenons $i = (i\tau^m)(\tau^m)^{-1} = i(\tau^{m+h-m}) = i\tau^h$. Nous pouvons considérer que h est choisi de tel manière que les cycles $i, i\tau, \cdots, i\tau^{h-1}$ sont différents. Le cycle $\sigma = (i(i\tau) \cdots (i\tau^{h-1})$ sera l'orbite de la permutation τ engendré par l'élément i. Si "u" un élément entier relatif quelconque alors en écrivant $u = hq + r$ où $0 \leq r < h$ nous obtenons $i\tau^u = i(\tau^{hq}\tau^r) = (i((\tau^h)^q)\tau^r = i\tau^r \in \sigma$. Pour bien parachever la démonstration du théorème, établissons d'abord les deux lemmes suivants :*

Lemme 7.2.3.1 *Deux orbites de la permutation τ sont soit disjoints ou coïncidents.*

Démonstration 7.2.3.5 *En effet si les orbites $\sigma = (i(i\tau) \cdots (i\tau^{h-1}))$ et $\rho = (j(j\tau) \cdots (j\tau^{l-1}))$ contiennent d alors $d = i\tau^s = j\tau^t$ où $t \geq s$ dans ce cas $i = (j\tau^l)(\tau^s)^{-1} = j\tau^{t-s} \in \rho$. Soit $\sigma \leq \rho$. De même on démontre que $\rho \leq \sigma$. Ainsi $\sigma = \rho$.*

Lemme 7.2.3.2 *Si σ est l'orbite de la permutation τ et $i \in \sigma$ alors $i\tau = i\sigma$.*

En effet supposons que $\sigma = (k(k\tau) \cdots (k\tau^{r-1}))$ alors $i = k\tau^h$ où $0 \leq h < r$ d'ici

$$i\sigma = (k\tau^h)\sigma = \begin{cases} k = k\tau^r = (k\tau^{r-1})\tau = i\tau & si \quad h = r - 1 \\ k\tau^{h+1} = (k\tau^h)\tau & si \quad 0 \leq h < r - 1. \end{cases}$$

En retournant á la démonstration du théorème 7.2.3.5, supposons que $\tau_1 \cdots \tau_m$ sont des orbites de la permutations τ qui ne sont pas constituées d'un élément. Si $i \notin \sigma_1 \cup \cdots \cup \sigma_m$ alors $i\sigma_k = i \quad \forall k$ où $i\sigma_1 \cdots \sigma_m = i\tau$. Dans le cas contraire en raison du Lemme 7.2.3.1, $i \in \sigma_s$ pour une orbite près de σ_s. C'est pourquoi $i \notin \sigma_1 \cup \cdots \cup \sigma_{s-1}$ c'est-à-dire $i\sigma_1 = \cdots = i\sigma_{s-1} = i$. Outre cela nous avons $i\tau \in \sigma_s$ où

$i\tau \notin \sigma_{s+1} \cup \cdots \cup \sigma_m$ et ceci entraîne $(i\tau)\sigma_{s+1} = \cdots = (i\tau)\sigma_m = i\tau$. D'ici en considérant le lemme 7.2.3.2 nous obtenons : $i\sigma_1 \cdots \sigma_{s-1}\sigma_s\sigma_{s+1} \cdots \sigma_m = (i\sigma_s)\sigma_{s+1} \cdots \sigma_m = (i\tau)\sigma_{s+1} \cdots \sigma_m = i\tau$. Ainsi $i\tau = i(\sigma_1 \cdots \sigma_m)$ $\forall i$ c'est-à-dire $\tau = \sigma_1 \cdots \sigma_m$. L'indépendance des cycles $\sigma_1, \sigma_2, \cdots, \sigma_m$ provient des lemmes.

Théorème 7.2.3.6 *Chaque permutaion se présente sous forme de produit de transpositions.*

Démonstration 7.2.3.6 *Démonstration : En raison du théorème 7.2.3.5, il suffit d'établir l'égalité $(i_1 \cdots i_k) = (i_1 i_2)(i_1 i_3) \cdots (i_1 i_k)\sharp$*
Mais $i((i_1 i_2) \cdots (i_1 i_k)) = i$ si $i \neq i_1, \cdots, i_k$. si $i = i_k$ alors $i((i_1 i_1) \cdots (i_1 i_k)) = i_k(i_1 i_k) = i_1$. Mais $i = i_s$ où $1 \leq s < k$
alors

$$\begin{aligned} i((i_1 i_2) \cdots (i_1 i_k)) &= i_s((i_1 i_s)(i_1 i_{s+1}) \cdots (i_1 i_k)) = \\ i_1((i_1 i_{s+1}) \cdots (i_1 i_k)) &= i_{s+1}((i_1 i_{s+2}) \cdots (i_1 i_k)) = i_{s+1}. \end{aligned}$$

Ainsi $i((i_1 i_2) \cdots (i_1 i_k)) = i(i_1 \cdots i_k)$ $\forall i$ c'est-à-dire que l'égalité $\sharp$ est vérifiée.

Puisque les orbites des permutations sont définies de manière unique, dans la démonstration du théorème 7.2.3.5 on peut voir ou noter que chaque permutation se présente de manière unique sous forme de produit de cycles indépendants ou deux à deux disjoint à ordre de multiplicité près. Pour représenter une permutation comme produit de transpositions, cela ne se fait pas de manière unique parce que de l'égalité ($\sharp$) il vient :$(13)(15) = (135) = (351) = (35)(31)$ il est vrai que $(13) = (31)$ mais $(15) \neq (35)$. Une certaine consolation peut servir de théorème le résultat suivant :

Théorème 7.2.3.7 *La parité de la permutation est égale à la parité du nombre de transposition qui entre dans sa représentation.*

Deux permutations σ et τ de l'ensemble $\{1, 2, \cdots, n\}$ sont égales si $\sigma(i) = \tau(i)$ $\forall i$. La permutations σ se présente sous la forme

$$\begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix},$$

le nombre

$$Sgn\sigma = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{1 - j} =$$

$$= \frac{(\sigma(1) - \sigma(2)) \cdots (\sigma(1) - \sigma(n))(\sigma(2) - \sigma(3)) \cdots (\sigma(2) - \sigma(n)) \cdots \sigma(n-1) - \sigma(n)}{(1-2) \cdots (1-n)(2-3) \cdots (2-n) \cdots ((n-1) - n)}$$

est appelé le signe **signature** de la permutation. En général il est égal à 1 ou -1 dans le premier il est appelé paire et dans le deuxième car impaire.
Par exemple considérons la permutation suivante :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}.$$

Sa signature est :

$$Sgn\sigma = \frac{3.1.2(-2)-(-1)(1)}{(-1)(-2)(-3)(-1)(-2)(-1)} = 1 \quad \text{soit} \quad \sigma \quad est \quad \text{paire}$$

Nous disons que les permutations σ et τ diffèrent par la transposition (i,j) si

$$\sigma(k) = \begin{cases} \tau(k) & \text{si } k \neq i,j \\ \tau(j) & \text{si } k = i \\ \tau(i) & \text{si } k = j \end{cases}$$

En écrivant ces permutations sous forme de tableau il n'est pas difficile de voir que, une de ces permutations s'obtient de l'autre par un changement de position i^{ime} et j^{ime} place.

Lemme 7.2.3.3 *Si les permutations σ et τ différent par la transposition (i,j) alors $Sgn\sigma = -Sgn\tau$.*

En regroupant les produits nous obtenons :

$$Sgn\sigma = \prod_{1\leq k<l<n} \frac{\sigma(k)-\sigma(l)}{k-l} \times \prod_{1\leq k\leq n; k\neq i,j} \left(\frac{\sigma(i)-\sigma(k)}{i-k} \times \frac{\sigma(j)-\sigma(k)}{j-k}\right)\left(\frac{\sigma(i)-\sigma(j)}{i-j}\right)$$

$$=$$

$$= \prod_{\substack{1\leq k<l<n; \\ \text{k}\neq i,j; \\ \text{l}\neq i,j}} \frac{\tau(k)-\tau(l)}{k-l} \times \prod_{\substack{1\leq k\leq n; \\ \text{k}\neq i,j}} \left(\frac{\tau(j)-\tau(k)}{i-k} \times \frac{\tau(i)-\tau(k)}{j-k}\right) \times \left(\frac{\tau(j)-\tau(i)}{i-j}\right)$$

$$= \prod_{\substack{1\leq k<l<n; \\ \text{k}\neq i,j; \\ \text{l}\neq i,j}} \frac{\tau(k)-\tau(l)}{k-l} \times \prod_{\substack{1\leq k\leq n; \\ \text{k}\neq i,j}} \left(\frac{\tau(j)-\tau(k)}{j-k} \times \frac{\tau(i)-\tau(k)}{i-k}\right) \times \frac{\tau(i)-\tau(j)}{i-j} \times (-1)$$

$$= (-1)sgn\tau.$$

Pour démontrer le théorème 7.2.3.7, établissons d'abord le lemme suivant :

Lemme 7.2.3.4 *pour toute permutation τ et transposition (i,j) les permutations τ et $(i,j)\tau$ ont une parité différente.*

En effet

$$k((ij)\tau) = \begin{cases} k\tau & \text{si } k \neq i,j \\ j\tau & \text{si } k = i \\ i\tau & \text{si } k = j \end{cases}.$$

Ainsi si

$$\tau = \begin{pmatrix} 1 & 2 & \cdots & n \\ \tau(1) & \tau(2) & \cdots & \tau(n) \end{pmatrix}.$$

Alors

$$(ij)\tau = \begin{pmatrix} 1 & i & j & n \\ \tau(1) & \tau(j) & \tau(i) & \tau(n) \end{pmatrix}.$$

D'après le Lemme 7.2.3.3 d'où le résultat.
Maintenant en revenant au théorème 7.2.3.7, si $\tau = \tau_1 \cdots \tau_m$ où τ_h sont des transpositions, la proposition requise vient de l'égalité $\tau = \tau_1 \cdots \tau_m \epsilon$ où ϵ=permutation identité qui est fini et paire. Il faut prendre en considération que en raison du Lemme 7.2.3.4, dans la multiplication avec chaque τ_h, la parité change.
CQFD.

Proposition 7.2.3.3 *L'application $Sgn : (S_n, \cdot) \longrightarrow (\{-1,1\}, \cdot)$ est un morphisme de groupe. Autrement dit, quelles que soient σ et ρ dans S_n, on a*

$$Sgn(\sigma \cdot \rho) = Sgn(\sigma) \cdot Sgn(\rho).$$

Conséquence 7.2.3.3 *La signature d'une transposition quelconque est égale à -1.*

Conséquence 7.2.3.4 *La signature d'un cycle de longueur k est égale á $(-1)^{k-1}$.*

Théorème 7.2.3.8 *Les permutations paires forment un sous groupe normale $\mathcal{U}_n$ du groupe $\mathcal{O}_n$ appellé n-ième groupe alterné.*

Démonstration 7.2.3.7 *: Soit $\mathcal{U}_n$ la collection de toutes les permutations paires de σ_n. Si $\sigma, \tau \in \mathcal{U}_n$ alors $\sigma\tau \in \mathcal{U}_n$ en raison des théorèmes 7.2.3.6 et 7.2.3.7.*

Pour continuer la d'emonstration de ce th'erème, établissons d'abord le lemme suivant.

Lemme 7.2.3.5 *Si les $\sigma_1, \cdots, \sigma_m$ sont des transpositions alors $(\sigma_1 \cdots \sigma_m)^{-1} = \sigma_m \cdots \sigma_1$.*

Pour démontrer ce lemme remarquons d'abord que $\sigma_i^2 = \epsilon$ où ϵ est la permutation identité. D'ici nous avons $\sigma_1 \cdots \sigma_m \cdot \sigma_m \cdots \sigma_1 = \epsilon = \sigma_m \cdots \sigma_1 \sigma_1 \cdots \sigma_m$.
En revenant au théorème 7.2.3.8, si maintenant $\sigma \in \mathcal{U}$ en raison des lemmes établis dans les démonstrations des théorèmes 7.2.3.6 et 7.2.3.7 entrainent que $\sigma^{-1} \in \mathcal{U}_n$. Ainsi $\mathcal{U}_n$ est un sous groupe de S_n. Si enfin $\sigma \in \mathcal{U}_n$ et $\rho = \rho_1 \cdots \rho_n$ où ρ_i- transposition alors en raison du lemme précédent

$$Sgn(\rho\sigma\rho^{-1}) = Sgn(\rho_1 \cdots \rho_m \sigma \rho_m \cdots \rho_1) = Sgn\sigma = +1$$

en raison du théorème 7.2.3.7 il vient alors que

$$(la \quad parite \quad \rho\sigma\rho^{-1}) = (la \quad parite\sigma) + 2m = (la \quad parite\sigma).$$

C'est-à-dire $\rho\sigma\rho^{-1} \in \mathcal{U}_n$ si $\sigma \in \mathcal{U}_n$.

Proposition 7.2.3.4 *Si σ est un cycle de longeur k ou un k-cycle alors, σ est d'ordre k soit $\sigma^k = Id$ et $\sigma^{k-1} \neq Id$.*

Définition 7.2.3.8 *un élément $z \in G$ est appellé central si $zg = gz \qquad \forall g \in G$. L'ensemble de tous les éléments centraux est appelé centre.*

Théorème 7.2.3.9 *Le centre $\mathcal{Z}$ d'un groupe G est un sous groupe. Et chaque sous-groupe du groupe $\mathcal{Z}$ est un sous groupe normal de G.*

Démonstration 7.2.3.8 *: Il est clair que l'élément neutre est dans $\mathbb{Z}$. Si $z', z'' \in \mathcal{Z}$ alors $\forall g \in G$ nous avons $(z'z'')g = z'(z''g) = z'(gz'') = (z'g)z'' = (gz')z'' = g(z'z'')$ c'est-à-dire $z'z'' \in \mathcal{Z}$. Si $z \in \mathcal{Z}$ alors $gz = zg \qquad \forall g \in G, \quad z^{-1}g = z^{-1}gzz^{-1} = z^{-1}zgz^{-1} = gz^{-1}$ c'est-à-dire $z^{-1} \in \mathcal{Z}$ d'où $\mathcal{Z}$ est un sous groupe. Enfin si H est un sous groupe dans $\mathcal{Z}$, soit $g \in G$ et $h \in H$ alors $ghg^{-1} = hgg^{-1} = h \in H$. D'où chaque sous groupe de $\mathcal{Z}$ est un sous groupe normal.*

Si $a \in G$ alors pour tout élément de la forme gag^{-1} où $g \in G$ on dira qu'il est adjoint avec l'élément a (ou conjugué de l'élément a), l'ensemble de tous les l'éléments adjoints à l'élément a (ou conjugué de l'élément a) est appelé classe adjointe. Il est claire que chaque élément est contenu dans sa classe adjointe (il suffit de prendre $g = 1$)

Théorème 7.2.3.10 *Deux classes adjointes du groupe G sont soit non sécantes ou coïncident c'est-à-dire les classes adjointes forment une partition du groupe G.*

Démonstration 7.2.3.9 *: <u>Démonstration</u> : Soient K et L deux classes adjointes des éléments a et b correspondant et soit $u \in K \cap L$ alors $u = gag^{-1} = hbh^{-1}$ où $g, h \in G$. Si $v \in K$ alors $v = cac^{-1}$ pour un certain $c \in G$ d'ici il vient que $v = cg^{-1}ugc^{-1} = cg^{-1}hbh^{-1}gc^{-1} = (cg^{-1}h)b(cg^{-1}h)^{-1} \in L$ ainsi $K \subseteq L$. De même on démontre l'autre inclusion.*

Exemple : Un calcul immédiat montre que le groupe S_3 se décompose suivant les trois classes adjointes suivantes :

$$\left\{\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\right\},\left\{\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\right\}$$
$$\left\{\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right\}.$$

Théorème 7.2.3.11 *Supposons qu'un groupe fini G contient n éléments et $g \in G$. Alors $g^n = 1$ et si $g^m = 1$ mais que $g^k \neq 1$ pour $1 \leq k < m$, alors m divise n.*

Démonstration 7.2.3.10 *: Supposons $g \in G$, $g^m = 1$ et $g^k \neq 1$, si $1 \leq k < m$. Pour tout entier s nous avons $s = qm + r$ où $0 \leq r < m$. En vertu des théorèmes 9 et 10 on a : $g^s = (g^m)^q g^r = 1 \cdot g^r = g^r$. Outre cela, si $0 < k < m$ alors $g^k g^{m-k} = 1$ et $0 < m - k < m$. Ainsi $\{1, g, g^2, \cdots, g^{m-1}\}$ est un sous groupe de G qui contient m éléments. En raison du théorème 7.2.0.11, m divise n. Ceci démontre la deuxième affirmation du théorème. Pour démontrer la première, considérons l'ensemble $\{g, g^2, g^3, \cdots\}$. En raison du fait que G soit fini, il existe m tel que $g^k = g^{k+m}$ pour tout $m > 0$. On peut supposer que les $g^k, g^{k+1}, \cdots, g^{k+m-1}$ sont tous distincts. En raison des théorèmes 7.2.2.10 et 7.2.2.11, il vient que $1 = g^k g^{-k} = g^{k+m}.g^{-k} = g^m$ et que les éléments $1, g, g^2, \cdots, g^{m-1}$ sont tous différents. Comme il a été montré ci-dessus, il vient que $n = qm$ pour un certain q et $g^m = (g^m)^q = 1^q = 1$ en raison du théorème 7.2.2.11.*

Dans la suite nous allons noter $|X|$ le nombre d'éléments de l'ensemble X ou encore l'ordre du groupe X (qu'il ne faut pas confondre avec la notation du déterminant).

Théorème 7.2.3.12 *supposons que $K(g)$ est la classe adjointe de l'élément g du groupe G et $C(G)$ l'ensemble des éléments $x \in G$ tels que $xg = gx$. Alors $C(G)$ est un sous- groupe du groupe G et $|K(g)||C(G)| = |G|$.*

Démonstration 7.2.3.11 *: Posons $L = C(g)$, il est clair que $1 \in L$ donc $L \neq \emptyset$ Montrons que si $x, y \in L$ alors $xy \in L$. En effet $(xy)g = x(yg) = x(gy) = (xg)y = (gx)y = g(xy)$ ce qui entraîne $xy \in L$. De même si $x \in L$ alors $x^{-1} \in L$; puisque $x^{-1}g = x^{-1}g(xx^{-1}) = (x^{-1}(gx))x^{-1} = (x^{-1}(xg))x^{-1} = ((x^{-1}x)g)x^{-1} = gx^{-1}$. D'où $x^{-1} \in L$. Donc L est un sous-groupe.*
Notons G/L l'ensemble quotient des classes d'équivalences à droite du groupe G par L. (Rémarquons que comme le sous-groupe L n'est pas supposé normale, alors ce n'est pas un facteur de groupe). Définnisons l'application $\varphi : K(g) \longrightarrow G/L$ en posant $\varphi(u^{-1}gu) = Lu$. Si $u^{-1}gu = v^{-1}gv$ pour $u, v \in G$, alors $(vu^{-1})g = (gvu^{-1})$, d'ici il vient que $vu^{-1} \in L$. C'est pourquoi $v \in Lu$, soit $Lu = Lv$. Ceci montre que l'application φ est bien définie. Il est claire qu'elle est surjective. En effet si $\varphi(u^{-1}gu) = \varphi(v^{-1}gv)$, alors $Lu = Lv$ ceci implique que $u = lv$ pour un certain $l \in L$. Ce qui signifie que

$$u^{-1}gu = v^{-1}l^{-1}glv = v^{-1}l^{-1}lgv = v^{-1}gv.$$

Ainsi φ est injective, donc bijective. En considérant le théorème de Lagrange abregé. Nous obtenons

$$|K(g)||L| = |G/L||L| = |G|.$$

Théorème 7.2.3.13 *Le centre du groupe G où $|G| = p^k$ avec p premier et $k \geq 1$, contient au moins un élément.*

Démonstration 7.2.3.12 *Supposons que* 1 *est l'unique élément central du groupe G et $g_1, \cdots, g_t$ les réprésentants des autres classes adjointes. Posons $L_i = C(g_i)$ En raison du théorème* 7.2.0.32*, nous obtenons $|K(g_i)||L_i| = p^k$, il vient $|L_i| = p^{k_i}$, où $0 \leq k_i \leq k$ c'est-à-dire $|K(g_i)| = p^{k-k_i}$.*
Si $k = k_i$ pour un certain i alors $|L_i| = |G|$, soit $L_i = G$ c'est-à-dire g_i est l'élément central en raison de son choix. Ainsi $k - k_i \geq 1, \quad \forall i$.
En representant le groupe G sous forme d'union des classes adjointes nous obtenons :

$$\begin{array}{rcl} p^k = |G| & = & 1 + |K(g_1)| + \cdots + |K(g_t)| \\ & = & 1 + p^{k-k_1} + \cdots + p^{k-k_t} \end{array}$$

c'est-à-dire $1 = p(p^{k-1} - p^{k-k_1-1} - \cdots - p^{k-k_t-1})$

Construction de l'ensemble Q

Nous savons que $(\mathbb{N}, \times)$ n'admet pas de structure de groupe. Mais que $\times$ est associative, commutative et admet un élément noutre qui est 1, mais aussi chaque élément de $\mathbb{N}$ autre que 1 n'admet pas de symétrique. Nous allons construire un ensemble, plus grand que $\mathbb{N}$ et où les points que nous venons d'évoquer seront vérifiés. Comme $\mathbb{Z}$ a été construit à partir de $\mathbb{N} \times \mathbb{N}$. Nous allons reprendre $\mathbb{N} \times \mathbb{N}$ et enlever le couple $(0, 0)$. Plus précisement, nous allons écrire $\mathbb{N}^\star \times \mathbb{N}^\star$. Dans $\mathbb{N}^\star \times \mathbb{N}^\star$ nous allons définir la relation

$$(x, y)\mathcal{R}(z, t) \Longleftrightarrow xt = yz.$$

Nous laissons le soin au lecteur de vérifier que c'est une relation d'équivalence. Déterminons $\mathbb{N}^\star \times \mathbb{N}^\star/\mathcal{R} = \mathbb{Q}$ l'ensemble quotient. L'élément neutre dans $\mathbb{Q}$ est

$$\overline{(1,1)} = \overline{(a,a)} \quad a \in \mathbb{N}^\star$$

Chapitre 8

Anneaux, Corps et espaces vectoriels

8.1 Anneaux et Corps

8.1.1 Anneaux

Définition 8.1.1.1 *Un ensemble non vide A muni de deux lois de composition interne $(+)$ pour la première et $(\cdot)$ pour la deuxième est appelé anneau s'il vérifie les trois conditions suivantes :*

$1\cdot$ $(A,+)$*est un groupe abélien*
$2\cdot$ *la loi* $\cdot$ *est associative*
$3\cdot$ $\forall a,b,c\in A,\quad \Big((a+b).c=a.c+b.c \;\; et \;\; a.(b+c)=a.b+b.c\Big)$
la deuxième loi est distributive par rapport à la première

ou encore

Définition 8.1.1.2 *Un ensemble non vide A muni de deux lois de composition interne $+$ et $(\cdot)$ est appelé anneau s'il vérifie les trois conditions suivantes :*

$1\cdot$ $(A,+)$*est un groupe abélien*
$2\cdot$ $(A,.)$*est en semi-groupe*
$3\cdot$ $\forall a,b,c\in A,\quad \Big((a+b).c=a.c+b.c \;\; et \;\; a.(b+c)=a.b+b.c\Big)$
la deuxième loi est distributive par rapport à la première

Si la 2^{ime} loi admet un élément neutre alors l'anneau A est dit unitaire.
Si la 2^{ime} loi est commutative, l'anneau est dit **commutatif**.

Exemple 8.1.1.1

(i) $(\mathbb{Z},+,.)$ *;* $(\mathbb{Q},+,\times)$ *sont des anneaux commutatifs et unitaires.*

(ii)Chaque groupe abélien B peut être transformé en un anneau en définissant la 2^{ime} opération $a.b=0 \quad \forall a,b\in B$. Cet anneau est appelé ***anneau avec pour multiplication nulle****. Il est commutatif mais n'admet pas d'unité.*

(iii) La structure algébrique $\mathfrak{M}_n(\mathbb{K})$ qui dénote l'ensemble des matrices d'ordre n avec, $(\mathbb{K}=\mathbb{Q},\mathbb{R},\mathbb{C})$ est un anneau unitaire non commutatif et non intègre.

(iv) Soit I un intervalle de $\mathbb{R}$ et $\mathcal{F}(I)$ l'ensemble des fonctions d'éfinies sur I à valeurs réelle alors, $(\mathcal{F}(I), +, \cdot)$ est un anneau commutatif unitaire non intègre. Les lois $(+)$ et $(\cdot)$ sont l'addition et la multiplication usuelle. Par contre l'ensemble $\mathfrak{C}(I)$ des fonctions continues sur I est un sous anneau de $\mathcal{F}(I)$.

De la définition de l'anneau, nous pouvons obtenir les propriétés suivantes :

$$a.0 = 0.a = 0$$
$$a.(-b) = (-a).b = -a.b$$
$$(a-b).c = a.c - a.b \qquad \text{et} \quad a.(b-c) = a.b - a.c$$

Définition 8.1.1.3 *le sous ensemble Hde A est appelé sous-anneau si H est un sous groupe abélien de $(A, +)$ et si H est un semi-groupe de $(A, .)$.*

ou encore

Définition 8.1.1.4 *Soit $(A, +, \cdot)$ un anneau et H un sous ensemble non vide de A. H est un sous anneau de A si*
– $\forall x, y \in H, x - y \in H$
– $\forall x, y \in H, x \cdot y \in H$.

Théorème 8.1.1.1 *L'intersection de sous - anneaux est un sous - anneau.*

Définition 8.1.1.5 *L'application$\varphi : A \to A'$ est appelé homomorphisme d'**anneaux** si :*

$$\varphi(x+y) = \varphi(x) + \varphi(y) \quad \forall x, y \in A$$
$$\varphi(x.y) = \varphi(x).\varphi(y).$$

Ainsi l'hompomorphisme d'anneaux est un homomorphisme pour la première loi et la deuxième loi.

Tout homomorphisme biunivoque est appelé isomorphisme. S'il existe un isomorphisme entre l'anneau A et l'anneau A', on dit que A et A' sont isomorphes.

Théorème 8.1.1.2 *Si $\varphi : A \to A'$ est un homomorphisme d'anneaux, alors $Im\varphi$ est un sous - anneau de A'.*

La partition de l'anneau A est admissible si elle est admissible comme groupe additif aussi bien comme semi groupe. En d'autres mots, la partition Σ d'un anneau A est admissible si du fait que x et y, tout comme u et v, appartiennent à la même classe d'équivalence ; il en est de même de $x + y$ et $u + v$ ainsi que xy et uv.
Si Σ est une partition admissible de l'anneau A alors dans l'ensemble quotient A/Σ,on peut définir les opérations :

$$1.[x] + [y] = [x + y]$$
$$2.[u].[v] = [u.v]$$

l'admissibilité de la partition permet de démontrer que ces opérations sont bien définies. Ainsi il ne serait pas difficile de vérifier que la véracité des conditions 1 et 3 de la définition d'un anneau.
Le facteur quotient A/Σ est un anneau. Cet anneau est appelé facteur d'anneau A pour la partition Σ.
L'application qui met en correspondance chaque élément de A contenu dans sa classe d'équivalence de la partition est un homomorphisme d'anneaux. Cet homomorphisme est dit **naturel.** En accord avec les résultats des théorème sur le chapitre des groupes la future admissibilité du groupe additif sera une partition sur les classes d'équivalence sur un certain groupe.

Définition 8.1.1.6 *Considérons le sous - anneau I de l'anneau A. Ce sous - anneau est un idéal de A si les produits xa et ax appartiennent à $I \quad \forall x \in I, \quad \forall a \in A$.*

Théorème 8.1.1.3 *La partition Σ de l'anneau A est admissible si et seulement si elle est la partition par rapport à un groupe additif relativement à un certain idéal. Cet idéal apparait être la classe d'équivalence de la partition Σ contenant l'élément 0.*

preuve :

Démonstration 8.1.1.1 *Comme l'idéal est une conséquence du groupe commutatif de l'anneau alors il sera un sous groupe normal,en accord avec le théorème 6 sur le chapitre des groupes,la partition en classe d'équivalence par l'idéal sera une partition admissible pour le groupe additif.Comme a et c de même que b et d sont dans la même classe d'équivalence alors, $a = c + x$ et $b = d + y$ avec $x, y \in I$.*
$ab = (c + x)(d + y) = cd + (cy + xd + xy)$.
Donc ab et cd appartiennent à la même classe d'équivalence. Ainsi la partition par l'idéal apparaît comme étant admissible et même pour le semi groupe multiplicatif. Supposons maintenant que Σ est une partition admissible pour l'anneau A. En raison du théorème 7 sur le chapitre des groupes, ce type de partition sera une partition par rapport à un certain sous groupe I du groupe additif de l'anneau A.
Si $x \in I$ alors x et 0 appartiennent à la même classe d'équivalence de la partition Σ.
Considérons $a \in A$. Comme a appartient à sa classe d'équivalence de la partition Σ admissible alors nous aurons $x.a = 0$ et $0.a = 0$ qui vont appartenir à la même classe de la partition Σ alors $x.a \in I$.De même on vérifie que $a.x \in I$.Donc I est un idéal CQFD.
*Le théorème 8.1.1.3 montre qu'au lieu de parler de facteur d'anneau de A par une partition admissible, on peut parler de **facteur d'anneau de A par un certain idéal**. Le théorème 8.1.1.3 montre aussi que cet idéal coincide avec la classe de la partition contenant 0.*
Si $\varphi : \quad A \to A'$ épimorphisme d'anneaux, alors la partition par rapport à $Ker\varphi$ pour la même raison definie pour un idéal K constitués de toutes les images inverses de 0 c'est-à-dire que $K = \{a \in A \backslash \varphi(a) = 0\}$.
C'est pourquoi dans la théorie des anneaux,le noyau de l'homomorphisme est appelé cet idéal et par $Ker\varphi$.On le note $Ker\varphi = I$

Nous noterons une fois de plus que si I est l'idéal alors la classe d'équivalence définissant l'élément a se présente sous la forme $a + I$.

Théorème 8.1.1.4 Théorème des homomorphismes d'anneaux
Si $\varphi : \quad A \to A'$ *est un homomorphisme d'anneaux surjectif, alors* $Ker\varphi$ *sera un idéal et si l'on considére*$\Pi : \quad A \to A/Ker\varphi$ *appellée application naturelle,alors il existe un isomorphisme* $\chi : \quad A' \to A/Ker\varphi$ *tel que* $\chi \circ \varphi = \Pi$.

On vérifie aisement que le sous groupe $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$.
C'est pourquoi $\mathbb{Z}/n\mathbb{Z}$ est anneau qui est appelé **anneau des résidus modulo n.**
On vérifie rapidement que si $\varphi : \quad A \to A'$ est un épimorphisme d'anneaux et l'anneau A est commutatif alors A' sera commutatif. En particulier le facteur d'anneau de l'anneau commutatif est commutatif. C'est pourquoi tous les anneaux formés par des résidus quelquonques sont commutatifs.

Définition 8.1.1.7 *On appelle diviseur de zéro dans l'anneau* A *tout élément* $a \in A - \{0\}$ *tel que* $ab = 0$ *ou* $ba = 0$, *pour un certain élément* $b \in A$.
Si A *est un anneau unitaire alors* a *est appelé* <u>inverse</u> *pour un certain élément* b *tel que* $ab = ba = 1$.

Théorème 8.1.1.5 *L'élément inverse dans un anneau ne peut être un diviseur de zéro.*

Démonstration 8.1.1.2 ***<u>preuve :</u>***
Supposons que l'élément inversible de l'anneau est un diviseur de zéro. Alors pour un certain $b \in A, \exists a \in A ab = ba = 1$. *Supposons maitenant que pour un certain* $c \neq 0, ac = 0 \quad ou \quad ca = 0$. *En considérant la condition 2 dans la définition de l'anneau, nous avons* $c = (ba)c = b(ac) = b.0 = 0$ *ou bien* $c = c(ab) = (ca)b = 0.b = 0 \Rightarrow c = 0$ *absurde.CQFD*

Proposition 8.1.1.1 *Soit* A° *l'ensemble des éléments inversibles de l'anneau unitaire* $(A, +, \cdot)$ *alors,* $(A^\circ, \cdot)$ *est un groupe.*

8.1.2 Corps et Champs

Définition 8.1.2.1 *Un ensemble non vide* A *muni de deux lois de composition interne* $+$ *pour la première et* $\cdot$ *pour la deuxième est appelé* <u>corps</u> *s'il vérifie les trois conditions suivantes :*

$1 \cdot \quad (A, +)$ *est un groupe abélien*
$2 \cdot \quad (A^*, \cdot)$ *est un groupe*
$3 \cdot \quad \forall a, b, c \in A, \quad \Big((a + b).c = a.c + b.c \quad et \quad a.(b + c) = a.b + b.c\Big)$
la deuxième loi est distributive par rapport à la première

Rémarque 8.1.2.1 *De cette définition, si la deuxième loi est commutative alors, ce corps est appelé champ. Nous pouvons aussi avoir cette autre définition.*

Définition 8.1.2.2 *L'anneau commutatif F est appelé champ s'il contient un élément unité différent de 0 et chaque élément de F est inversible.*

En raison du théorème 8.1.1.5 dans les anneaux il n'y a pas de diviseur de zéro. Ainsi nous obtenons de la définition du champ que les éléments non nuls du champ forment un groupe multiplicatif.

Exemple : $(\mathbb{Q}, +, \times)$ *et* $(\mathbb{R}, +, \times)$

Théorème 8.1.2.1 *L'anneau des résidus modulo m est un champ si et seulement si m est premier.*

preuve :

Soit A l'anneau des résidus modulo m. Supposons que A est un champ.
-Si m n'est pas premier i.e on peut le décomposer en produits de facteurs premiers $m = kl$ où $0 < k, l < m$. Alors les classes de k ($[k]$) et les classes de l ($[l]$) sont toutes différentes de $[0]$. $[m] = [k][l] = [0]$
Ainsi k est un diviseur de zéro (ce qui est absurde) car dans un champ il n'y a pas de diviseur de zéro.
-Si m est premier, supposons $[k] \neq 0$ alors $0 < k < m$. Comme m est divisible seulement par 1 et m alors le PGCD i.e $(k, m) = 1$. Ainsi, il
$\exists u, v \in \mathbb{Z}$ tel que $uk + mv = 1$. D'ici, il vient que
$[u][k] = [uk] + [0] = [uk] + [mv] = [uk + mv] = [1]$. Donc tout élément non nul de A est inversible. CQFD

Définition 8.1.2.3 *Soit K un champ et $p \in K$ est appelé caractéristique si*

$$\underbrace{1 + 1 + \cdots + 1 = 0}_{p\ fois}$$

et tout élément positif inférieur à p ne vérifie pas cette identité.

Si dans un champ il n'existe pas d'élément p tel que

$$\underbrace{1 + 1 + \cdots + 1}_{p\ fois} = 0$$

alors on dit que ce champ est de caractéristique nulle.

Exemple : $(\mathbb{R}, +, \times)$ est un champ de caractéristique nulle.

Théorème 8.1.2.2 *la caractéristique peut être zéro ou un nombre premier.*

preuve :

Si $n = kl$ où $1 < k, l < n$ avec n la caractéristique du champ K. Alors

$$a = \underbrace{1 + 1 + \cdots + 1}_{k\ fois} \neq 0$$

et

$$b = \underbrace{1 + 1 + \cdots + 1}_{l\ fois} \neq 0.$$

$$ab = \underbrace{1+1+\cdots+1}_{kl\ fois} = 0$$

ce qui est absurde car a ou b est un diviseur de zéro c'est à dire $a = 0$ ou $b = 0$ (ce qui est absurde) car $a \neq 0$ ou $b \neq 0$. D'où n est premier.

Théorème 8.1.2.3 *Tout anneau commutatif unitaire sans diviseur de zéro s'injecte dans un champ.*

Démonstration 8.1.2.1 *Soit A un anneau commutatif unitaire sans diviseur de zéro et notons*

$$Q = \{\frac{a}{b}, a, b \in A \quad et \quad b \neq 0\}.$$

Posons $\left[\frac{a}{b}\right] = \left\{\frac{x}{y}/\frac{x}{y} \in Q, ay = bx\right\}$
Vérifions que les sous ensembles $\left[\frac{a}{b}\right]$ *forment une partition de Q. Comme* $\frac{a}{b} \in \left[\frac{a}{b}\right]$, *pour cela il suffit d'établir que deux ensembles de ce type qui ont un élément en commun coincident.*
Pour le montrer supposons que $\frac{u}{v} \in \left[\frac{a}{b}\right] \cap \left[\frac{c}{d}\right]$, *alors $av = bu$ et $cv = du$.*
Si $\frac{x}{y} \in \left[\frac{a}{b}\right] \Rightarrow ay = bx$. *Montrons que $cy = dx$.*
En effet, $(bv)(cy - dx) = bduy - vdya = avdy - vdya = 0$. *Comme dans A il n'y a pas de diviseur de zéro et $bv \neq 0$, il vient que $(bv)(cy - dx) = 0$ ce qui revient à soit $cy - dx = 0$ soit $cy = dx$*
c'est à dire $\frac{x}{y} \subseteq \left[\frac{c}{d}\right]$. *Ainsi,* $\left[\frac{a}{b}\right] \subseteq \left[\frac{c}{d}\right]$.
De même, on montre que $\left[\frac{c}{d}\right] \subseteq \left[\frac{a}{b}\right]$ *donc* $\left[\frac{a}{b}\right] = \left[\frac{c}{d}\right]$.
Notons Σ la partition obtenue et considérons le facteur d'ensemble Q/Σ et définissons dans un ensemble les opérations $+$ et $\cdot$ en posant
$\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] = \left[\frac{ad+bc}{bd}\right]$; $\left[\frac{a}{b}\right]\left[\frac{a}{b}\right] = \left[\frac{ac}{bd}\right]$.
Comme il n'y a pas de diviseur de zéro dans A car A est un champ, la partition droite de ces égalités à un sens. Vérifions qu'elles sont bien définies.
Supposons $\left[\frac{a}{b}\right] = \left[\frac{u}{v}\right]$ *et* $\left[\frac{c}{d}\right] = \left[\frac{w}{z}\right]$. *Il suffit de vérifier que*

$$\left[\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] = \left[\frac{u}{v}\right] + \left[\frac{w}{z}\right] et \left[\frac{a}{b}\right]\left[\frac{c}{d}\right] = \left[\frac{u}{v}\right]\left[\frac{w}{z}\right]\right]. (1)$$

Mais par l'hypothèse on a $av = bu$ et $cz = dw$; d'ici il vient que

$$(bd)(uz + wv) = bduz + bdwv = advz + bczv$$
$$(bd)(uz + wv) = (vz)(ad + bc) et (ac)(vz) = budw = (bd)(uw)$$

D'où (1).
Après, on vérifie facilement que la multiplication et l'addition sont associatives et commutatives et qu'en fait l'associativité et la commutativité proviennent de l'égalité

$$\left(\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right]\right) + \left[\frac{u}{v}\right] = \left[\frac{ad+bc}{bd}\right] + \left[\frac{u}{v}\right] = \left[\frac{adv + bcv + bdu}{bdv}\right]$$

et

$$\left[\frac{a}{b}\right]+\left(\left[\frac{c}{d}\right]+\left[\frac{u}{v}\right]\right)=\left[\frac{a}{b}\right]+\left[\frac{cv+du}{dv}\right]=\left[\frac{adv+bcv+bdu}{bdv}\right].$$

En suite, $\left[\frac{a}{b}\right]+\left[\frac{0}{1}\right]=\left[\frac{a.1+b.0}{b}\right]=\left[\frac{a}{b}\right]$
$\left[\frac{a}{b}\right]+\left[\frac{-a}{b}\right]=\left[\frac{ab-ba}{b^2}\right]=\left[\frac{0}{b^2}\right]=\left[\frac{0}{1}\right].$
Donc $(Q/\Sigma,+)$ *est un groupe commutatif.*
En outre,

$$\left(\left[\frac{a}{b}\right]+\left[\frac{c}{d}\right]\right)\left[\frac{u}{v}\right]=\left[\frac{(ad+bc)u}{bdv}\right]=\left[\frac{(ad+bc)uv}{bdv^2}\right]=\left[\frac{au}{bv}\right]+\left[\frac{cu}{dv}\right]=\left[\frac{a}{b}\right]\left[\frac{u}{v}\right]+\left[\frac{c}{d}\right]\left[\frac{u}{v}\right].$$

Donc Q/Σ *est un anneau commutatif.*
$\left[\frac{a}{b}\right]\left[\frac{1}{1}\right]=\left[\frac{a}{b}\right]$ *soit* $\left[\frac{1}{1}\right]$ *est l'unité de l'anneau* Q/Σ. *Si* $\left[\frac{a}{b}\right]\neq\left[\frac{0}{1}\right]$ *alors* $a\neq 0\Rightarrow$
$\left[\frac{b}{a}\right]\in Q/\Sigma$. *D'autre part,* $\left[\frac{a}{b}\right]\left[\frac{b}{a}\right]=\left[\frac{1}{1}\right]\Rightarrow(Q/\Sigma,+,\cdot)$ *est un champ.*
Définissons l'application

$$\begin{aligned}\varphi:\quad & A\to Q/\Sigma\\ & a\varphi\mapsto\left[\frac{a}{b}\right]\end{aligned}$$

Comme $\left[\frac{a}{1}\right]=\left[\frac{b}{1}\right]\Rightarrow a=b.$*Cette application est injective et des égalités* $(a+b)\varphi=$
$\left[\frac{a+b}{1}\right]=\left[\frac{a}{1}\right]+\left[\frac{b}{1}\right]=a\varphi+b\varphi$
$(ab)\varphi=\left[\frac{ab}{1}\right]=\left[\frac{a}{1}\right]\left[\frac{b}{1}\right]=a\varphi b\varphi\Rightarrow\varphi$ *est un homomorphisme injectif et* φ *injecte* A
dans Q/Σ *CQFD.*

Construisons un autre corps

Soit $\mathbb{C}$ l'ensemble des matrices de la forme

$$\begin{pmatrix} a & -b\\ b & a\end{pmatrix}.$$

Définissons sur $\mathbb{C}$ l'addition et la multiplication de la manière suivante :

$$\begin{pmatrix} a & -b\\ b & a\end{pmatrix}+\begin{pmatrix} c & -d\\ d & c\end{pmatrix}=\begin{pmatrix} a+c & -(b+d)\\ b+d & a+c\end{pmatrix}$$

$$\begin{pmatrix} a & -b\\ b & a\end{pmatrix}\times\begin{pmatrix} c & -d\\ d & c\end{pmatrix}=\begin{pmatrix} ac-bd & -(bc+ad)\\ bc+ad & ac-bd\end{pmatrix}$$

$$I=\begin{pmatrix} 1 & 0\\ 0 & 1\end{pmatrix};\begin{pmatrix} a & -b\\ b & a\end{pmatrix}\neq\begin{pmatrix} 0 & 0\\ 0 & 0\end{pmatrix}$$

si et seulement si, $\delta=a^2+b^2\neq 0$

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} \frac{a}{\delta} & \frac{b}{\delta} \\ \frac{-b}{\delta} & \frac{a}{\delta} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

les éléments de $\mathbb{C}$ excepté

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

sont inversibles. $\mathbb{C}$ est un champ appelé champs des **nombres** complexes. Les nombres réels s'injectent dans $\mathbb{C}$.

Considérons l'application $\varphi(a)$ qui à tout a associe $\varphi(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \sim a$

$$i = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad i^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -1$$

$$bi = \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} \times \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -b \\ b & 0 \end{pmatrix}$$

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} 0 & -b \\ b & 0 \end{pmatrix} = a + ib$$

Donc $z = a + ib$ et son conjugué est $\overline{z} = a - ib$

Théorème 8.1.2.4 *l'application*

$$\begin{aligned} \varphi : \quad & \mathbb{C} \to \mathbb{C} \\ & z \mapsto \overline{z} \end{aligned}$$

est un isomorphisme.

$$z\overline{z} = a^2 + b^2$$

$$| z | = \sqrt{a^2 + b^2} \quad \text{qui est le module de z}$$

$$1) |u| = 0 \Leftrightarrow u = 0$$
$$2) |uv| = |u||v|$$
$$3) |u + v| \leq |u| + |v|$$

Construisons un corps non commutatif en considérant l'ensemble $\mathbb{K}$ des matrices de la forme $\begin{pmatrix} u & v \\ -\overline{v} & \overline{u} \end{pmatrix} \qquad u, v \in \mathbb{C}$

Comme dans le cas de $\mathbb{C}$, $\mathbb{K}$ est un sous anneau de l'anneau des matrices. Il n'est pas commutatif.

Comme

$\overline{i} = -i$, on a :

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

Cependant, $I \in \mathbb{K}$ et si $u = a + ib$ et $v = c + id$, alors
$u\overline{u} + v\overline{v} = a^2 + b^2 + c^2 + d^2 \in \mathbb{R}_+^*$
C'est pourquoi

$$\begin{pmatrix} u & v \\ -\overline{v} & \overline{u} \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

D' où $\lambda = u\overline{u} + v\overline{v} \neq 0$. Ainsi nous avons :

$$\begin{pmatrix} u & v \\ -\overline{v} & \overline{u} \end{pmatrix} \begin{pmatrix} \frac{\overline{u}}{\lambda} & \frac{v}{\lambda} \\ -\frac{\overline{v}}{\lambda} & \frac{\overline{u}}{\lambda} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

c'est-à-dire chaque élément de $\mathbb{K}$ admet un inverse dans $\mathbb{K}$. Donc $\mathbb{K}$ est un corps qui est appelé corps des quaternions.
On vérifie que l'application
$\varphi(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ où $a \in \mathbb{R}$ est un homomorphisme injectif de $\mathbb{R}$ dans $\mathbb{K}$ en faisant correspondre a avec $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ et en posant

$$i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \qquad j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

on obtient le tableau suivant :

$*$	1	i	j	k
1	1	i	j	k
i	i	-1	k	-j
j	j	-k	-1	i
k	k	j	-i	-1

Si $a \in \mathbb{R}, \overline{a} = a$. C'est pourquoi

$$a \begin{pmatrix} u & v \\ -\overline{v} & \overline{u} \end{pmatrix} = \begin{pmatrix} au & av \\ -a\overline{v} & a\overline{u} \end{pmatrix}$$

En posant $u = a + ib$, $v = c + id$, nous obtenons $\begin{pmatrix} u & v \\ -\overline{v} & \overline{u} \end{pmatrix} = a + bi + cj + dk$

Proposition 8.1.2.1 *Quel que soit $n \in \mathbb{N}$, $n \geq 2$, alors, $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau commutatif.*

Proposition 8.1.2.2 *Quel que soit $p \in \mathbb{N}$, p, premier alors, $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ est un corps commutatif.*

Proposition 8.1.2.3 Petit théorème de Fermat
Soit p, premier et pour tout $x \in \mathbb{Z}$ tel que $p \nmid x$. Alors, est vérifiée la relation suivante

$$x^{p-1} \equiv 1[p].$$

Soit p divise toujours $x^{p-1} - 1$.

Proposition 8.1.2.4 *$(\mathbb{Z}, +, \cdot)$ est un anneau principal.*

Proposition 8.1.2.5 *Soit $(A, +, \cdot)$ un anneau commutatif et I un ideal de A alors, $(A/I, +, \cdot)$ est un anneau commutatif; où $+$ et $\cdot$ sont définies dans les classes. Si A est unitaire alors, A/I est un anneau unitaire et on a $1_{A/I} = cl(1_A)$.*

Proposition 8.1.2.6 *Soient $(A_1, +, \cdot)$ et $(A_2, +, \cdot)$ deux anneaux commutatifs et $f : A_1 \longrightarrow A_2$ un morphisme d'anneaux. Il existe un unique isomorphisme $\chi : A_1/\ker f \longrightarrow f(A_1)$ tel que $f = \chi \circ p$ où p est la projection canonique de A_1 sur $A_1/\ker f$. Nous aurons alors*

$$A_1/\ker f \simeq f(A_1).$$

8.1.3 Anneaux de Polynômes

Définition 8.1.3.1 Construction de $A[x]$ avec A un anneau commutatif et unitaire
Soit $(A, +, \cdot)$ un anneau commutatif et unitaire, fixons $x \in A$ et proposons-nous de former une collection des éléments de la forme $a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$, où $a_i \in A$ pour $i \in \{0, 2, \cdots, n\}$. Cette collection délément sera notée $A[x]$. Nous aurons $A[x] = \{a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n / a_i \in A \text{ et } i \in \{0, 2, \cdots, n\}\}$. Nous allons pour le moment admettre cette collection forme un anneau qui, sera appellé anneau des polynômes.

Rémarque 8.1.3.1 *Les 'eléments de $A[x]$ qui sont des polynômes sont notés par P avec $P = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ avec $a_i \in A$*

Exemple 8.1.3.1 Exemples de polynômes
– *$P = 6x^5 + -75x^3 + 3x - 6$ est un polynôme à coefficients dans $\mathbb{Z}$*
– *$Q = a_{\sqrt{5}}x^3 - 6x^2 + 9x - 7$ est un polynôme à coefficients dans $\mathbb{R}$*

Définition 8.1.3.2 *On appelle degré du polynôme $P = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ et noté $deg(P)$ le plus grand exposant en x figurant dans ce polynôme.*

ou nous pouvons encore dire

Définition 8.1.3.3 *Le degré d'un polynôme est l'exposant i le plus élevé des termes x^i de coefficient a_i non nul.*

Exemple 8.1.3.2 – *Le degré de $P = 6x^5 + -75x^3 + 3x - 6$ est $deg(P) = 5$.*
– *Le degré de $Q = a_{\sqrt{5}}x^3 - 6x^2 + 9x - 7$ est $deg(Q) = 3$.*

Définition 8.1.3.4 *La valuation d'un polynôme est l'exposant i le moins élevé des termes x^i de coefficient a_i non nul. Elle est notée par $val(P)$.*

Exemple 8.1.3.3 – *La valuation de $P = 6x^5 + -75x^3 + 3x - 6$ est $val(P) = 0$.*
– *La valuation de $Q = a_{\sqrt{5}}x^3 - 6x^2 + 9x - 7$ est $val(P) = 0$.*

Rémarque 8.1.3.2 *Le degré de $P = 0$ est $deg(P) = -\infty$, alors que la valuation de $P = 0$ est $val(P) = +\infty$.*

Rémarque 8.1.3.3 *En algèbre il existe un théorème appelé théorème fondamental de l'algèbre et qui dit : "tout polynôme de degré n dans $\mathbb{C}$ admet n racine " ce résultat peut aussi être généralisé par tout polynôme de degré n dans $\mathbb{C}$ admet n racines.*

8.1.4 Recherche des zéros

Généralement pour chercher les zéros(racines) d'un polynôme on prend tous les diviseurs du terme constant ; c'est- à- dire, si le polynôme s'écrit $P = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ alors, a_n est le terme et, les zéros du polynôme sont les diviseurs de a_n .

Exemple 8.1.4.1 *Considérons le polynôme* $P = x^4 + 5x^3 + 5x^2 - 5x - 6$. *Dans ce polynôme* $a_n = a_4 = -6$. *Cherchons les diviseurs de* -6 *ils sont* $-6, -3, -2, 1, 2, 3, 6$. *Après subtitution de ces valeurs par* x *dans le polynôme on note sont* -1, -2, -3 *et* 1.

Dans le recherche des zéros d'un polynôme, il existe plusieurs techniques. Nous laissons le soin au lecteur de consulter d'autres ouvrages. Mais nous avons le resultat suivant.

Proposition 8.1.4.1 *pour que* a *soit racine de* P *il faut et il suffit que le polynôme* $x - a$ *divise* P, *soit qu'il existe* $Q \in A[X]$, *tel que* $P = (X - a) \cdot Q$.

Cette proposition montre que pour que a soit une racine d'ordre ou zéro d'ordre k ou de multiplicité k du polynôme P il faut que $(x - a)^k$ divise P. Soit $P = (x - a)^k \cdot Q$, pour un certain $Q \in A[X]$ mais $P = (x - a)^{k+1}$ ne divisant pas P.

Proposition 8.1.4.2 *Soit* A *est un anneau commutatif unitaire que* a *soit racine de* P *il faut et il suffit que le polynôme* $x - a$ *divise* P, *soit qu'il existe* $Q \in A[X]$, *tel que* $P = (X - a) \cdot Q$.

Proposition 8.1.4.3 *Si* A *est un anneau commutatif unitaire et* $QP \in A[X]$. *Si* A *est intègre et* $a_1, a_2, \cdots, a_r$ *sont les racines de* P *alors,*

$$P = (x - a_1)^{k_1}(x - a_2)^{k_2} \cdots (x - a_r)^{k_r} Q$$

où k_i *est la multiplicité de* a_i $(1 \leq i \leq r)$ *et aucun des* a_i *n'est racine de du polynôme* $Q \in A[X]$.

Rémarque 8.1.4.1 *Ce résultat n'est pas vrai si* A *n'est pas intègre.*

Equation linéaire de premier ordre

Définition 8.1.4.1 *On appelle équation de premier ordre, tout équation qui se présente sous la forme :*

$$ax + b = 0, \quad (1)$$

avec $a \neq 0$.

L'expression $x = -\frac{b}{a}$ est solution de (1).

Equation linéaire de second ordre (Equation quadratique)

Définition 8.1.4.2 *On appelle équation linéaire de second ordre tout équation qui se présente sous la forme :*

$$ax^2 + bx + c = 0, \quad (2)$$

avec $a \neq 0$.

Pour résoudre cette équation on utilise le discriminent $\Delta = b^2 - 4ac$.
- Si $\Delta \leq 0$, alors (2) n'admet pas de racines réelles.
- Si $\Delta \geq 0$, alors (2) admet deux racines distinctes :

$$x_1 = \frac{-b + \sqrt{\Delta}}{2a}, \quad x_2 = \frac{-b - \sqrt{\Delta}}{2a}.$$

- Si $\Delta = 0$, alors (2) admet une racine double

$$x_1 = x_2 = -\frac{b}{2a}$$

Exemple 8.1.4.2 *Résoudre l'équation* $(a+1)x^2 + 2(a+1)x + a - 2 = 0$, *suivant le paramètre* a.

Théorème 8.1.4.1 *(Viete)*
Soit donnée l'équation $ax^2 + bx + c = 0$, *alors la somme et le produit des racices donnent :*

$$x_1 + x_2 = -\frac{b}{a} \quad x_1 x_2 = \frac{c}{a}.$$

Théorème 8.1.4.2 *Si* x_1 *et* x_2 *sont les racines de l'équation* $x^2 + px + q = 0$, *et* $S_n = x_1^n + x_2^n$, *avec* $(n \geq 2)$, $n \in \mathbb{N}$. *Alors la formule récurrente suivante est vérifiée :*

$$S_(n+1) = -pS_n - qS_(n-1); \quad S_1 = -p; \quad S_2 = p^2 - 2q.$$

En effet, comme x_1 et x_2 sont racines de l'équation quadratique, alors nous avons $x_1^2 + px_1 + q = 0$ et $x_2^2 + px_2 + q = 0$. En multipliant la prmière équation par x_1^{n-1} et la seconde par x_2^{n-1}, en faisant la somme, on obtient la formule récurrente.

Exemple 8.1.4.3 *Déterminer l'équation quadratique dont une des solutions est connue* $\frac{\sqrt{3}-\sqrt{5}}{\sqrt{3}+\sqrt{5}}$

Solution 8.1.4.1 *Supposons que* $x^2 + px + q = 0 \quad (3)$ *soit cette équation avec* p, q *des nombres rationnelles, il vient que en rationalisant le dénominateur on a :*

$$\frac{\sqrt{3}-\sqrt{5}}{\sqrt{3}+\sqrt{5}} = \frac{(\sqrt{3}-\sqrt{5})(\sqrt{3}-\sqrt{5})}{(\sqrt{3}+\sqrt{5})(\sqrt{3}-\sqrt{5})} = -4 + \sqrt{15},$$

cette racine doit vérifier (3), *soit* $(-4+\sqrt{15})^2 + p(-4+\sqrt{15}) + q = 0$ *après développement, il vient que :* $(31 - 4p + q) + (p - 8)\sqrt{15} = 0$, *par identification, on trouve* $31 - 4p + q = 0$ *et* $p - 8 = 0$, *après résolution du sytème on trouve* $p = 8$ *et* $q = 1$. *En défitive on trouve comme équation* $x^2 + 8x + 1 = 0$.

Exemple 8.1.4.4 *Montrer que deux équation quadratiques* $x^2 + p_1x + q_1 = 0$ *et* $x^2 + p_2x + q_2 = 0$, *de discriminant positif, admettent au moins une racine commune, si et seulement si,*

$$(q_2 - q_1)^2 = (p_2 - p_1)(p_1q_2 - q_1p_2).$$

Solution 8.1.4.2 *Considérons les deux fonctions* $f_1(x) = x^2 + p_1x + q_1$ *et* $f_1(x) = x^2 + p_2x + q_2$. *Supposons que* x_1, x_2 *sont des solutions de l'équation* $f_1(x) = 0$. *Pour que les équations* $f_1(x) = 0$ *et* $f_2(x) = 0$, *aient au moins une racine commune, il faut et il suffit que* $f_2(x) \times f_2(x) = 0$. *Soit* $(x_1^2 + p_2x_1 + q_2)(x_2^2 + p_2x_2 + q_2) = 0$. *En re écrivant cette expression sous la forme*

$$(x_1^2 + p_1x_1 + q_1 + (p_2 - p_1)x_1 + q_2 - q_1)(x_2^2 + p_1x_2 + q_1 + (p_2 - p_1)x_2 + q_2 - q_1) = 0.$$

Comme par hypothèse $x_1^2 + p_1x_1 + q_1 = 0$ *et* $x_2^2 + p_1x_2 + q_1 = 0$, *il vient que*

$$((p_2 - p_1)x_1 + q_2 - q_1)((p_2 - p_1)x_2 + q_2 - q_1) = 0.$$

En développant on obtient :

$$(p_2 - p_1)^2x_1x_2 + (p_2 - p_1)(q_2 - q_1)x_1 + (q_2 - q_1)(p_2 - p_1)x_2 + (q_2 - q_1)^2 = 0,$$

qu'on peut encore présenter sous la forme

$$(p_2 - p_1)^2x_1x_2 + (p_2 - p_1)(q_2 - q_1)(x_1 + x_2) + (q_2 - q_1)^2 = 0.$$

Comme $x_1 + x_2 = -p_1$ *et* $x_1x_2 = q_1$ *d'après le théorème de Viete.En substituants ces valeurs dans cette dernière expression, on obtient :*

$$(p_2 - p_1)^2q_1 + (p_2 - p_1)(q_2 - q_1)(-p_1) + (q_2 - q_1)^2 = 0.$$

En développant

$$\begin{aligned}(q_2 - q_1)^2 &= (p_2 - p_1)(q_2 - q_1)(p_1) - (p_2 - p_1)^2q_1 \\ &= (p_2 - p_1)[q_2p_1 - q_1p_1 - p_2q_1 + p_1q_1] \\ &= (p_2 - p_1)(q_2p_1 - p_2q_1)\end{aligned}$$

CQFD

Equation de la forme $ax^{2n} + bx^n + c = 0$**,** $a \neq 0$, $n \geq 2$ $n \in \mathbb{N}$

Pour $n = 2$, cette équation est dite biquadratique.pour résoudre une telle équation, on pose un changement de variable. Soit y^n et, l'équation se transforme sous la forme d'une équation quadratique suivante : $ay^2 + by + c$. Qui peut être résolu en utilisant le discriminant.

Equation pouvant être ramenée sous la forme quadratique

Considérons l'équation $ax^3 + bx^2 + bx + a = 0$, avec $a \neq 0$, elle est appellée équation symétrique d'ordre 3. Puisque $ax^3 + bx^2 + bx + a = (x+1)(ax^2 + (b-a)x + a)$ et elle devient facilement résoluble. Les équations de la forme

$$ax^4 + bx^3 + cx^2 + bx + a = 0,$$

$$ax^4 + bx^3 + cx^2 - bx + a = 0,$$

avec $a \neq 0$, sont appellées des équations symétriques d'ordre 4. Pour les résoudre, on divise chacune des équations par x^2, on obtient :

$$a(x^2 + \frac{1}{x^2}) + b(x + \frac{1}{x}) + c = 0.$$

Dans ce cas on pose comme changement de variable : $y = x + \frac{1}{x}$,pour la première équation.

$$a(x^2 + \frac{1}{x^2}) + b(x - \frac{1}{x}) + = 0c.$$

Dans ce cas on pose comme changement de variable : $y = x - \frac{1}{x}$,pour la deuxième équation.

Recherche de manière générale des zéros d'un polynôme

Pour résoudre les équations algébriques à coefficients entiers, on utilise le théorème suivant :

Théorème 8.1.4.3 *Pour que la fraction irréductible $\frac{p}{q}$, $q \neq 0$ soit racine de l'équation*

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n = 0, \quad *$$

il est nécessaire que p soit un diviseur de a_n et q un diviseur de a_0.

Conséquence 8.1.4.1 *Si l'équation $*$ est à coefficients relatifs et, $a_0 = 1$ alors, les racines rationnelles de cette équation ne peuvent que être des entièrs qui sont les diviseurs de a_n.*

Exemple 8.1.4.5 *Résoudre l'équation $2x^4 + 7x^3 - 12x^2 - 38x + 21 = 0$.*

Les divisiseurs de 21 sont : $\pm1, \pm3, \pm7, \pm21$ et ceux de 2 sont : $\pm1, \pm2$. Constituons toutes les fractions de la forme $\frac{p}{q}$, 1, 3, 7, 21, -1, -3, -7, -21, $\frac{1}{2}$, $\frac{3}{2}$, $\frac{7}{2}$, $\frac{21}{2}$, $-\frac{1}{2}$, $-\frac{3}{2}$, $-\frac{7}{2}$, $-\frac{21}{2}$. Toute racine rationnelle de cette équation appartient à cette collection.

Théorème 8.1.4.4 *Si une fraction rationnelle non négative* $\frac{p}{q}$, $q \neq 0$ *est solution de léquation à coefficient relatifs* $P(x) = a_0x^n + a_1x^{n-1}.\cdots + a_{n-1}x + a_n = 0$, *alors pour tout entier relatif* m, *le nombre* $P(m)$ *est divisible par* $p - mq$

Exemple 8.1.4.6 *Chercher toute les racines rationnelles de l'équation* $2x^4 + 7x^3 - 12x^2 - 38x + 21 = 0$.

Solution 8.1.4.3 *Déterminons la collection des nombres pouvant être racine de cette équation on a :* ± 1, ± 3, ± 7, ± 21, $\pm\frac{1}{2}$, $\pm\frac{3}{2}$, $\pm\frac{7}{2}$, $\pm\frac{21}{2}$. *En prenant* $x = +1$ *et en calculant sa valeur en* $P(x)$ *on trouve que* $P(+1) = -20$. *Soit* $x = +1$ *n'est pas racine de cette équation en raison du thérème défini précédemme. Si* $\frac{p}{q}$ *est racine de l'équation* $P(x) = 0$, *alors le nombre* $P(1)$ *est divisible par* $p - q$. *Or le nombre* -20 *est divisible par* $3 - 1 = 2$. *c'est pourquoi le nombre* $+3$ *peut être considéré comme racine. Mais le nombre* -20 *n'est pas divisible par* $7 - 1 = 6$. *c'est pourquoi,* 7 *n'est pas racine de l'équation. En raisonnant ainsi, on réduit le nombre d'éléments entrant dans la collection. Ainsi on trouve pour la suite de la vérification les nombres :* 3, 21, -1, -3, $\frac{1}{2}$, $\frac{3}{2}$, $\frac{7}{2}$, $*\frac{3}{2}$. *On v'erifie que :* $P(3) \neq 0$, $P(-3) = 0$, $P(\frac{1}{2}) = 0$, $P(\frac{3}{2} \neq 0$, $P(\frac{7}{2}) \neq 0$. *Comme solution on a* -3, $\frac{1}{2}$.

Rémarque 8.1.4.2 *Parfois pour rechercher les racines de l'équation* $P(x) = a_0x^n + a_1x^{n-1}.\cdots + a_{n-1}x + a_n = 0$. *On peut réduire le degré du polynôme, associé à cette équation, dans le cas où nous connaissons une racine* α *de cette équation, de la manière suivante :* $P(x) = (x - \alpha)Q(x)$ *où* $Q(x)$ *est un polynôme de degré* $n - 1$.

Exemple 8.1.4.7 *Résoudre l'équation* $x^4 + 2x^3 - 2x^2 - 6x + 5 = 0$.

Solution 8.1.4.4 *Comme* $a_0 = 1$, *alors* 1, -1, -5, 5. *En calculant la valeur de ce polynôme sur ces éléments on* $P(1) = 0$, $P(-1) \neq 0$, $P(-5) \neq 0$, $P(5) \neq 0$. *Donc* $P(x) = (x - 1)Q(x)$ *où* $Q(x)$ *est un polynôme de degré* 3.

8.1.5 Opérations sur les polynômes

Soient deux polynômes P et Q définies par :

$$P = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$$

$$Q = b_0x^m + b_1x^{m-1} + \cdots + b_{nm-1}x + b_m$$

Somme et soustraction de polynômes

La somme ou la soustraction des polynômes P et Q est l'expression définie par $P \pm Q$ et est égale :

- (a) si $n = m$ alors $P \pm Q = (a_0 \pm b_0)x^n + (a_1 \pm b_1)x^{n-1} + \cdots + (a_{n-1} \pm b_{n-1})x + (a_n \pm b_n)$,
- (b) si $n \neq m$ par exemple si $n > m$, on complète les coefficients de en ajoutant simplement des zéros jusqu'à obtenir un même degré fictif que n et on applique le résultat du cas précédent $(m = n)$.

Proposition 8.1.5.1 *pour tout* $P, Q \in A[X]$, $deg\ (P + Q) \leq \max(deg\ P, deg\ Q)$ *et l'égalité a lieu à moins que* P *et* Q *soient de même degré.*

Produit de deux polynômes

Le produit de deux polynômes P et Q est l'expression définie par $P \cdot Q$ et s'écrit

$$P \cdot Q = c_0 x^{n+m} + c_1 x^{n+m-1} + \cdots + c_{n+m-1} x + c_{n+m}.$$

Si nous utilisons le signe de la sommation on peut l'écrire

$$P \cdot Q = \sum_{p=0}^{n+m} c_p x^{n+m-p}$$

avec

$$c_p = \sum_{i+j=p} a_i b_j$$

Théorème 8.1.5.1 *Soit $(A, +, \cdot)$ un anneau commutatif unitaire alors, $(A[X]+, \cdot)$ est aussi un anneau commutatif unitaire avec $0_{A[X]} = 0_A$ et $1_{A[X]} = 1_A$*

Proposition 8.1.5.2 *pour tout $P, Q \in A[X]$, deg $(P \cdot Q)$ = deg P + deg Q. On supposera que $A[X]$ est un anneau commutatif et unitaire et intègre.*

Division de polynômes

La division du polynôme P par le polynôme Q est l'expression définie par $\frac{P}{Q}$ avec la condition que $Q \neq 0$

Définition 8.1.5.1 *soient P et Q deux polynômes de degré n et m respectivement. La relation $\frac{P}{Q}$ avec $Q \neq 0$ est appelée fraction rationnelle. Si deg $P >$ deg Q alors la fraction est impropre. Si deg $P <$ deg Q alors la fraction est propre.*

Division Euclidienne

Soient D et d deux polynômes avec *deg* $D = n$ et *deg* $d = m$. Supposons que *deg* $D >$ *deg* d alors il existe deux polynômes Q et R tels que $D = Q \cdot d + R$ avec *deg* $R <$ *deg* d

Théorème 8.1.5.2 *Soit A un anneau commutatif unitaire intègre et $P \in A[X]$ un polynôme dont le coefficient dominant est inversible soit $dom(P) \in A^\star$. Quel que soit $H \in A[X]$, il existe un et un seul couple de polynômes (Q, R) tels que deg $R <$ deg P et $T = Q \cdot P + R$. On dit dans ce cas que Q est le quotient de la division euclidienne de T par P et R est le reste.*

Théorème 8.1.5.3 *Soit $P \in A[X]$. Il existe $n \in \mathbb{N}$ et des éléments $a_0, a_1, \cdots, a_{n-1}, a_n \in A$ tels que P sécrive*

$$P = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = \sum_{p=0}^{n} a_p x^{n-p}.$$

De plus si

$$P = \sum_{p=0}^{n} a_p x^{n-p} \text{ et } P = \sum_{p=0}^{m} b_p x^{m-p}$$

sont deux écritures de $P \in A[X]$, *avec par exemple* $n \leq m$, *alors il vient que*

$$a_i = b_i \text{ pour } 0 \leq i \leq n \; b_i = 0_A \text{ pour} n < i \leq m$$

où 0_A *est l'élément neutre par rapport à la première loi dans l'anneau* $(A, +, \cdot)$.

Proposition 8.1.5.3 *Si* $\mathbb{K}$ *est un corps alors, l'anneau* $\mathbb{K}[X]$ *est principal.*

8.2 Espaces Vectoriels

8.2.1 Espaces Vectoriels

Définition 8.2.1.1 *Soit* $(\mathbb{K}, \sharp, *)$ *un corps ou un champ et soit* $(E, \top, \perp)$ *un ensemble muni de deux lois dont la première* $(\top)$ *est une loi de composition interne, et la seconde* $(\perp)$ *une loi de composition externe. On dit que* E *est un espace vectoriel sur* $\mathbb{K}$ *ou tout simplement un* $\mathbb{K}$*-espace vectoriel si :*

1. $(E, \top)$ *est un groupe abelien,*
2. $\forall \alpha, \beta \in \mathbb{K}, \forall x \in E, (\alpha * \beta) \perp x = \alpha \perp (\beta \perp x)$ *c'est l'associativité mixte,*
3. $\forall \alpha, \beta \in \mathbb{K}, \forall x \in E, (\alpha \sharp \beta) \perp x = (\alpha \perp x) \top (\beta \perp x)$ *c'est la distributivité par rapport aux éléments de* $\mathbb{K}$,
4. $\forall \alpha \in \mathbb{K}, \forall x, y \in E, \alpha \perp (x \top y) = (\alpha \perp x) \top (\alpha \perp x)$ *c'est la distributivité par rapport aux éléments de* E,
5. $\forall x \in E, 1_{\mathbb{K}} \perp x = x$),

où $1_{\mathbb{K}}$ *est le neutre par rapport à la deuxième loi dans* $\mathbb{K}$.

Nous pouvons donner cette autre définition moins abstraite que la précedante à savoir :

Définition 8.2.1.2 *Soit* $(\mathbb{K}, +, \times)$ *un corps ou un champ et soit* $(E, +, \cdot)$ *un ensemble muni de deux lois dont la première* $(+)$ *est une loi de composition interne, et la seconde* $(\cdot)$ *une loi de composition externe. On dit que* E *est un espace vectoriel sur* $\mathbb{K}$ *ou tout simplement un* $\mathbb{K}$*-espace vectoriel si :*

1. $(E, +)$ *est un groupe abelien,*
2. $\forall \alpha, \beta \in \mathbb{K}, \forall x \in E, (\alpha \times \beta) \perp x = \alpha \cdot (\beta \cdot x)$ *c'est l'associativité mixte,*
3. $\forall \alpha, \beta \in \mathbb{K}, \forall x \in E, (\alpha + \beta) \cdot x = (\alpha \cdot x) + (\beta \cdot x)$ *c'est la distributivité par rapport aux éléments de* $\mathbb{K}$,
4. $\forall \alpha \in \mathbb{K}, \forall x, y \in E, \alpha \cdot (x + y) = (\alpha \cdot x) + (\alpha \cdot x)$ *c'est la distributivité par rapport aux éléments de* E,
5. $\forall x \in E, 1_{\mathbb{K}} \cdot x = x$),

où $1_{\mathbb{K}}$ *est le neutre par rapport à* $(\times)$ *dans* $\mathbb{K}$.

Rémarque 8.2.1.1 *Si $\mathbb{K} = \mathbb{R}$, alors on dit que E est un espace vectoriel réel ou un $\mathbb{R}$-espace vectoriel.*

Rémarque 8.2.1.2 *Les éléments de $\mathbb{K}$ seront appellés les scalaires, alors que ceux de E seront les vecteurs. En général on distingue les vecteurs des scalaires en mettant une féche au dessus des vecteurs.*

Convention :

Il est convenu décrire le scalaire avant le vecteur, soit ou c'est-à-dire si α est un scalaire et $\overrightarrow{x}$ un vecteur, alors il est convenable d'écrire $\alpha\overrightarrow{x}$. Puisque l'ériture $\overrightarrow{x}\alpha$ peut tout avoir un autre sens mathématique.

Rémarque 8.2.1.3 *L'élément neutre de la loi interne de E est noté 0 et est appelé vecteur nul. Ainsi pour éviter les confusions, on note le vecteur nul 0_E et, l'élément neutre dans $\mathbb{K}$ sera noté $0_{\mathbb{K}}$.*

Exemple 8.2.1.1

1. *$\mathbb{R}$ est un $\mathbb{R}$-espace vectoriel.*
2. *$\mathbb{R}^2$ est un $\mathbb{R}$-espace vectoriel.*
3. *de manière générale $\mathbb{R}^n$ est un $\mathbb{R}$-espace vectoriel.*
4. *$\mathbb{C}$ est un $\mathbb{R}$-espace vectoriel.*
5. *de manière générale $\mathbb{C}^n$ est un $\mathbb{R}$-espace vectoriel.*
6. *Le produit $\mathbb{K}^n$ qui, est un ensemble constitué de n-uplets de scalaires $(a_1, a_2, \cdots, a_n)$ avec l'addition définie par*

$$(a_1, a_2, \cdots, a_n) + (b_1, b_2, \cdots, b_n) = (a_1 + b_1, a_2 + b_2, \cdots, a_n + b_n)$$

et la multiplication par un scalaire définie par

$$\lambda(a_1, a_2, \cdots, a_n) = (\lambda a_1, \lambda a_2, \cdots, \lambda a_n)$$

est un $\mathbb{R}$ ou un $\mathbb{C}$-espace vectoriel.

7. *L'ensemble des fonctions $\mathbb{R}$ dans $\mathbb{R}$ noté $\mathfrak{F}(\mathbb{R}, \mathbb{R})$ peut être muni d'une structure de $\mathbb{R}$-espace vectoriel de la manière*

$$\forall f, g \in \mathfrak{F}(\mathbb{R}, \mathbb{R}) \ \ \forall x \in \mathbb{R} \ \ (f + g)(x) = f(x) + g(x) \ \ et \ \ (\lambda f)(x) = \lambda f(x).$$

8. *De manière générale considérons l'ensemble $\mathbb{K}^A$ de toutes les fonctions définies sur un ensemble quelconque A et à valeurs dans $\mathbb{K}$ avec pour addition déninie par*

$$(\varphi + \psi)(x) = \varphi(x) + \psi(x)$$

et pour multiplication

$$(\lambda\varphi)(x) = \lambda\varphi(x)$$

est un $\mathbb{R}$ ou un $\mathbb{C}$-espace vectoriel.

9. *L'ensemble noté* $\mathfrak{F}(\mathbb{N},\mathbb{R})$ *de toutes les suites numériques peut être muni d'une structure d'espace vectoriel en définissant l'addition et la multiplication de la manière suivante : soit* $\mathcal{U}=(\mathcal{U}_n)_n$ *et* $\mathcal{V}=(\mathcal{V}_n)_n$ *deux éléments de* $\mathfrak{F}(\mathbb{N},\mathbb{R})$ *alors la somme*
$$(\mathcal{U}_n)+(\mathcal{V}_n)=^{def}(U+V)_n$$
et la multiplication
$$(\alpha\mathcal{U}_n)=^{def}(\alpha U)_n.$$
Ainsi l'ensemble $\mathfrak{F}(\mathbb{N},\mathbb{R})$ *muni de ces deux opérations est un* $\mathbb{R}$ *ou un* $\mathbb{C}$*-espace vectoriel.*

10. *L'ensemble noté* $\mathfrak{P}[X]$ *des fonctions polynômes sur* $\mathbb{R}$ *peut être muni d'une structure d'espace vectoriel de la manière suivante pour tout* f *et* g *de* $\mathfrak{P}[X]$ *on a* $f(x)=a_0x^k+a_1x^{k-1}+\cdots+a_{k-1}x+a_k$ *et* $g(x)=b_0x^k+b_1x^{k-1}+\cdots+b_{k-1}x+b_k$ *alors pour addition nous avons*
$$(f(x)\pm g(x))=(f\pm g)(x)=(a_0\pm b_0)x^k+(a_1\pm b_1)x^{k-1}+\cdots+(a_{k-1}\pm b_{k-1})x+(a_k\pm b_k)$$
et pour multiplication
$$\lambda f(x)=(\lambda f)(x)=(\lambda a_0)x^k+(\lambda a_1)x^{k-1}+\cdots+(\lambda a_{k-1})x+(\lambda a_k)$$

Propriété 8.2.1.1 *Les égalités suivantes sont valides*
$$0\cdot x=0_E\ \ (-x)=(-1)\cdot x\ \ \lambda\cdot 0_E=0_E.$$
Soit le produit $\alpha\cdot x$ *ne peut s'annuler que si l'un des facteurs est nul.*

Propriété 8.2.1.2 *L'addition est régulière. Soit*
$$\forall x,y,z\in E,\ \ alors\ \ x+z=y+z\Longrightarrow x=y$$

Propriété 8.2.1.3 *nous avons* $\forall\alpha,\beta\in\mathbb{R},\ \forall x,y\in E$
$$\alpha(x-y)=\alpha x-\alpha y$$
$$(\alpha-\beta)x=\alpha x-\beta x$$

Propriété 8.2.1.4 *L'addition est régulière. Soit*
$$\forall x,y,z\in E,\ \ alors\ \ x+z=y+z\Longrightarrow x=y$$

Proposition 8.2.1.1 *Si* E *et* F *sont deux espaces vectoriels sur* $\mathbb{K}$*, alors leur produit cartésien* $E\times F$ *admet une structure naturelle d'espace vectoriel sur* $\mathbb{K}$ *définie par :* $\forall(x_1,y_1)\in\mathbb{K}^2$ *and* $\forall(x_2,y_2)\in\mathbb{K}^2$*, nous avons*
$$(x_1,y_1)+(x_2,y_2)=(x_1+x_2,y_1+y_2),$$
$$\lambda(x_1,y_1)=(\lambda x_1,\lambda y_1).$$

Proposition 8.2.1.2 *Si E est un espaces vectoriels sur $\mathbb{K}$, alors l'ensemble E^A de toutes les fonctions définies sur un ensemble quelconque A à valeurs dans E a une structure d'espace vectoriel.*

Définition 8.2.1.3 *On appelle combinaison linéaire des n vecteurs $x_1, \cdots, x_n$ toute expression qui se présente sous la forme suivante*

$$\alpha_1 x_1 + \cdots + \alpha_n x_n$$

ou simplement toute expression qui s'écrit comme $\sum_{i=1}^{n} \alpha_i x_i$ pour certain scalaires donnés α_i $i \in \{1, \cdots n\}$

Exemple 8.2.1.2 *Dans $\mathbb{R}^2$, considérons les vecteurs suivsnts $X_1 = (1, -1)$ et $X_2 = (-3, 0)$. Une conbinaison linéaire de X_1 et X_2 sera $\alpha X_1 + \beta X_2$ avec $\alpha, \beta \in \mathbb{R}$ on aura*

$$\alpha X_1 + \beta X_2 = (\alpha - 3\beta, -\alpha)$$

Exemple 8.2.1.3 *Soit $\mathfrak{F}$ le $\mathbb{R}$-espace vectoriel des fonctions polynômes réelles.*

f_0 *le polynôme* $x \longmapsto 1$
f_1 *le polynôme* $x \longmapsto x$
f_2 *le polynôme* $x \longmapsto x^2$
f_3 *le polynôme* $x \longmapsto x^3$.

Alors les fonctions polynômes f et g définies par

$$f \longmapsto 2x^3 - 3x^2 - 6x - 5$$

$$g \longmapsto 3x^2 - 6x - 5,$$

sont des combinaisons linéaires des fonctions f_0, f_1, f_2, f_3. Puisque on peut poser

$$f = 2f_3 - 3f_2 - 6f_1 - 5f_0,$$

$$f = 3f_2 - f_1 + 2f_0.$$

Par contre la fonction $h \longmapsto x^4 + 2x^2$, n'est pas une combinaison linéaire des fonctions f_0, f_1, f_2, f_3 car, il n'existe pas de $(\alpha, \beta, \gamma, \delta,) \in \mathbb{R}^4$ tel que

$$h(x) = (\alpha f_3 + \beta f_2 + \gamma f_1 + \delta f_0)(x).$$

8.2.2 Sous espaces vectoriels

Définition 8.2.2.1 *Soit E un $\mathbb{K}$-espace vectoriel et F un sous ensemble de E. F est un sous espace vectoriel de E si : F est non vide et est stable par rapport à première et deuxième loi dans E. Soit :*
– $\forall x, y \in F,\ \ x + y \in F$
– $\forall \alpha \in \mathbb{K},\ \forall x \in F,\ \ \alpha \cdot x \in F$.

Exemple 8.2.2.1 *D'après la proposition 8.2.1.2 si $E = \mathbb{R}$ et $A =]0, 1$, alors $\mathbb{R}^{[0,1]}$ est un espace vectoriel. Ainsi l'ensemble $\mathcal{C}[0, 1]$ des fonctions réelles continues sue le segment $[0, 1]$, est un sous espace vectoriel de $\mathbb{R}^{[0,1]}$.*

Théorème 8.2.2.1 *Soit E un $\mathbb{K}$-espace vectoriel et F un sous ensemble de E. F est un sous espace vectoriel de E si et seulement si :*
- *F est non vide,*
- *toute combinaison linéaire de deux éléments de F est un élément de F soit $\forall \alpha, \beta \in \mathbb{K}$, $\forall x, y \in F \;\; \alpha \cdot x + \beta \cdot y \in F$.*

Conséquence 8.2.2.1 *Une partie non vide F d'un $\mathbb{K}$-espace vectoriel E est un sous espace vectoriel de E si et seulement si elle est stable par combinaison linéaire.*

Conséquence 8.2.2.2 *Si F est un sous espace vectoriel de E, alors la restriction des opérations dfinies dans E sur F lui confère une structure d'espace vectoriel.*

Définition 8.2.2.2 *On appele sous espace vectoriel propre d'un espace vectoriel E, tout sous espace vectoriel qui est différent du vecteur nul 0_E et de E lui même. Dans le cas contraire on dit que ce sous espace vectoriel est trivial.*

Opérations sur les sous espaces vectoriels

1. **Intersection de deux sous espaces vectoriels**

   Définition 8.2.2.3 *Soit F_1 et F_2 deux sous espaces vectoriels de E. On appelle intersection de deux sous espaces vectoriels F_1 et F_2 et noté $F_1 \cap F_2$, c'est l'ensemble constitué des vecteurs qui appartiennent à la fois à F_1 et F_2, soit*

   $$F_1 \cap F_2 = \{x / x \in F_1 \text{ et } x \in F_2\}.$$

   Proposition 8.2.2.1 *L'intersection de deux sous espaces vectoriels est un sous espace vectoriel.*

   Démonstration 8.2.2.1 *Soient F_1 et F_2 deux sous espaces vectoriels. Montrons que $F_1 \cap F_2$ est un sous espace vectoriel.*
   - *En effet $F_1 \cap F_2 \neq \emptyset$ car $0_E \in F_1$ et $0_E \in F_2$ donc $0_E \in F_1 \cap F_2$*
   - *$\forall x, y \in F_1 \cap F_2$ montrons que $x + y \in F_1 \cap F_2$.*
     Comme $x \in F_1 \cap F_2$ alors $x \in F_1$ et $x \in F_2$,
     comme $y \in F_1 \cap F_2$ alors $y \in F_1$ et $y \in F_2$.
     Puisque $x \in F_1$ et $y \in F_1$, alors $x + y \in F_1$ puisque F_1 est un sous espace vectoriel,
     puisque $x \in F_2$ et $y \in F_2$, alors $x + y \in F_2$ puisque F_2 est un sous espace vectoriel.
     Donc $x + y \in F_1 \cap F_2$.
   - *Montrons que $\forall \alpha \in \mathbb{K}$ et $\forall x \in F_1 \cap F_2$, alors $\alpha x \in F_1 \cap F_2$*
     $x \in F_1 \cap F_2$, alors $x \in F_1$ et $x \in F_2$, comme F_1 et F_2 sont des sous espaces vectoriels, alors $\alpha x \in F_1$ et $\alpha x \in F_2$, soit $\alpha x \in F_1 \cap F_2$

   Rémarque 8.2.2.1 *On peut aussi définir l'intersection d'un nombre quelconque de sous espaces vectoriels. Soient $F_i, i \in I$ où I peut être fini ou non. On appelle l'intersection de ces sous espaces vectoriels F_i, l'ensemble noté $\bigcap_{i \in I} F_i$.*

2. **Reunion de deux sous espaces vectoriels**

Définition 8.2.2.4 *Soit F_1 et F_2 deux sous espaces vectoriels de E. On appelle reunion de deux sous espaces vectoriels F_1 et F_2 et noté $F_1 \cup F_2$, c'est l'ensemble constitué des vecteurs qui appartiennent à F_1 ou à F_2, soit*

$$F_1 \cup F_2 = \{x / x \in F_1 \text{ ou } x \in F_2\}.$$

Rémarque 8.2.2.2 *En général la reunion de deux sous espaces vectoriels n'est pas un sous espace vectoriel.*

Rémarque 8.2.2.3 *On peut aussi définir la reunion d'un nombre quelconque de sous espaces vectoriels. Soient $F_i, i \in I$ où I peut être fini ou non. On appelle reunion de ces sous espaces vectoriels F_i, l'ensemble noté $\bigcup_{i \in I} F_i$.*

3. **Somme de deux sous espaces vectoriels**

Définition 8.2.2.5 *Soit F_1 et F_2 deux sous espaces vectoriels de E. On appelle somme de deux sous espaces vectoriels F_1 et F_2 et noté $F_1 + F_2$, c'est l'ensemble constitué des vecteurs sommes y tel qu'il existe $x_1 \in F_1$ et $x_2 \in F_2$, afin que $y = x_1 + x_2$*

$$F_1 + F_2 = \{y = x_1 + x_2 / x_1 \in F_1 \text{ et } x_2 \in F_2\}.$$

Proposition 8.2.2.2 *La somme de deux sous espaces vectoriels est un sous espace vectoriel. C'est le plus petit sous espace vectoriel (au sens de l'inclusion) qui contienne F_1 et F_2.*

Nous laissons la démonstration en exercice.

Définition 8.2.2.6 *On appelle systeme ou famille de vecteurs ou encore partie de vecteur tout ensemble constitué de vecteurs.*

Rémarque 8.2.2.4 *Si un système ou une famille ou une partie de vecteur est constituée d'un nombre finie de vecteurs, alors on dit que c'est un système ou une famille ou encore une partie finie de vecteurs. Dans le cas contraire on dit que c'est un système infini.*

Théorème 8.2.2.2 *Soit $\{x_1, x_2, \cdots, x_n\}$ une partie ou un système fini de vecteurs. Alors l'ensemble des combinaisons lineaires de $\{x_1, x_2, \cdots, x_n\}$ noté $\mathcal{L}(x_1, x_2, \cdots, x_n)$, est un sous espace vectoriel de E ; c'est le plus petit sous espace vectoriel de E(au sens de l'inclusion) contenant les vecteurs $x_1, x_2, \cdots, x_n$. En d'autres termes, il est inclus dans tout autre sous espace vectoriel contenant $\{x_1, x_2, \cdots, x_n\}$.*

Démonstration 8.2.2.2 *Soit $\mathcal{L}(x_1, x_2, \cdots, x_n)$ l'ensemble des combinaisons linéaire des vecteurs $x_1, x_2, \cdots, x_n$. Cet ensemble est non vide, car il contient la combinaison triviale soit $0.x_1 + 0.x_2 + \cdots + 0.x_n = 0_E$.*
On peut aussi vérifier que $x_1, x_2, \cdots, x_n$ appartiennent à $\mathcal{L}(x_1, x_2, \cdots, x_n)$, en effet pour tout k compris entre 1 et n, x_k est combinaison linéaire de $x_1, x_2, \cdots, x_n$ (pour cela, il suffit de considerer la combinaison linéaire où tous les coefficients sont nuls sauf le k^{ime} qui est égal à 1.)

Montrons maintenant que $\mathcal{L}(x_1, x_2, \cdots, x_n)$ est stable par combinaison linéaire. Soit $x \in \mathcal{L}(x_1, x_2, \cdots, x_n)$, alors il existe des scalaires $\lambda_1, \lambda_2, \cdots, \lambda_n$ tels que

$$x = \lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_n x_n = \sum_{i=1}^{n} \lambda_i x_i.$$

De même $y \in \mathcal{L}(x_1, x_2, \cdots, x_n)$, alors il existe des scalaires $\gamma_1, \gamma_2, \cdots, \gamma_n$ tels que

$$y = \gamma_1 x_1 + \gamma_2 x_2 + \cdots + \gamma_n x_n = \sum_{i=1}^{n} \gamma_i x_i.$$

Ainsi

$$\begin{array}{rcl} \alpha x + \beta y & = & \alpha(\lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_n x_n) + \beta(\gamma_1 x_1 + \gamma_2 x_2 + \cdots + \gamma_n x_n) \\ & = & (\alpha\lambda_1 + \beta\gamma_1)x_1 + (\alpha\lambda_2 + \beta\gamma_2)x_2 + \cdots + (\alpha\lambda_n + \beta\gamma_n)x_n. \end{array}$$

Soit c'est une combinaison linéaire de $\{x_1, x_2, \cdots, x_n\}$, donc un élément de $\mathcal{L}(x_1, x_2, \cdots, x_n)$. Supposons maintenant que H soit un autre sous espace vectoriel contenant $\{x_1, x_2, \cdots, x_n\}$, alors il est stable par combinaison linéaire, il contient donc toute combinaison linéaire des vecteurs de $\{x_1, x_2, \cdots, x_n\}$. Par conséquent $\mathcal{L}(x_1, x_2, \cdots, x_n)$ est inclu dans H soit $\mathcal{L}(x_1, x_2, \cdots, x_n) \subseteq H$ et $\mathcal{L}(x_1, x_2, \cdots, x_n)$ est le plus petit sous espace (au sens de l'inclusion) contenant $\{x_1, x_2, \cdots, x_n\}$.

Notation Ce sous espace vectoriel est appellśous espace engendré par $x_1, x_2, \cdots, x_n$. Il est parfois noté $Vect(x_1, x_2, \cdots, x_n)$ ou $< x_1, x_2, \cdots, x_n >$ ou encore $\overline{(x_1, x_2, \cdots, x_n)}$.
Ainsi $x \in Vect(x_1, x_2, \cdots, x_n) \Leftrightarrow \exists(\lambda_1, \cdots, \lambda_n) \in \mathbb{K}^n / x = \lambda_1 x_1 + \cdots + \lambda_n x_n$.

Propriété 8.2.2.1 (De Transitivité)
Soit F un sous espace engendré par n $x_1, x_2, \cdots, x_n$. On suppose qu'il existe p vecteurs $y_1, y_2, \cdots, y_p$ appartenant à F tels que pour tout i, $1 \leq i \leq n$, x_i soit une combinaison linéaire de $y_1, y_2, \cdots, y_p$. Alors F est engendré par $y_1, y_2, \cdots, y_p$.

Sous espaces engendés par une partie quelconque d'un sous espace vectoriel

Une construction analogue peut ître faite en prenant une partie A quelconque non vide d'un espace vectoriel E en lieu et place d'une partie finie.

Définition 8.2.2.7 *Soit A une partie non vide d'un $\mathbb{K}$-espace vectoriel E. On définit le sous espace vectoriel engendré par A, comme étan l'ensemble des combinaisons linéaires des élément de A : soit*

$$u \in Vect(A) \Leftrightarrow \exists n \in \mathbb{N}^\star, \exists(x_1, \cdots, x_n) \in A^n,\ \exists(\lambda_1, \cdots, \lambda_n) \in \mathbb{K}^n / u = \lambda_1 x_1 + \cdots + \lambda_n x_n.$$

Nous le soin au lecteur de démontrer que $Vect(A)$ est un sous espace vectoriel de E et, c'est le plus petit sous espace vectoriel de E contenant A (au sens de l'inclusion bien sur.)

Exemple 8.2.2.2 *Considérons $k \in \mathbb{N}$ et, notons par e_k la fonction polynôme définie sur $\mathbb{R}$ par $x \longmapsto x^k$. Dans ce cas, le sous espace vectoriel engendré par la partie $A = \{e_k / \ k \in \mathbb{N}\}$ est l'ensemble des fonctions polynômes réeles.*

Rémarque 8.2.2.5 *Si F est un sous espace vectoriel de E, alors $Vect(F) = F$.*

Rémarque 8.2.2.6 *Pour toute partie A d'un espace vectoriel E, on $Vect(Vect(A)) = Vect(A)$.*

Construction d'un sous espace vectoriel engendré par une partie

Théorème 8.2.2.3 *Soit A une partie quelconque d'un espace vectoriel E. Il existe des sous espaces vectoriels contenant A, par exemple E lui même. Soit S l'ensemble des sous espaces vectoriels contenant A. Alors le sous espace vectoriel engendre par A est égal à l'intersection des éléments de S, soit $\bigcap_{F_i \in S} F_i$.*

Définition 8.2.2.8 (Système libre)
Soit $(x_1, \cdots, x_n)$ un système de n vecteurs. Ce système est dit libre ou linéairement indépendant, si pour toute combinaison linéaire triviale de vecteurs implique la trivialité de tous les coefficients. Soit :

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = 0_E \Longrightarrow \alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$$

Exemple 8.2.2.3 *Soit $\mathbb{R}^2$ un $\mathbb{R}$-espace vectoriel. Considérons le system (X_1, X_2) définit par $X_1 = (-1, 2)$ et $X_2 = (1, 1)$. Montrons que le syxtème (X_1, X_2) est libre dans $\mathbb{R}^2$.*
En effet, $\alpha_1 X_1 + \alpha_2 X_2 = 0_{\mathbb{R}^2} \Longleftrightarrow \alpha_1(-, 2) + \alpha_2(1, 1) = (0, 0)$. Par identification on a

$$\begin{cases} -\alpha_1 + \alpha_2 &= 0 \\ 2\alpha_1 + \alpha_2 &= 0 \end{cases}, \tag{8.1}$$

qui est un système de deux équations à deux inconnues. Après résolution on trouve $\alpha_1 = \alpha_2 = 0$. Soit (X_1, X_2) est un syxtème libre dans $\mathbb{R}^2$.

Définition 8.2.2.9 (Système lié)
Un système lié est le contraire d'un système libre. En d'autres termes un système lié est un système qui n'est pas libre.

Définition 8.2.2.10 *Soit $(x_1, \cdots, x_n)$ un système de n vecteurs. Ce système est dit lié ou linéairement dépendant, si pour toute combinaison linéaire triviale de vecteurs, on peut trouver des coefficient non tous nuls associés à cette combinaison. Soit :*

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = 0_E \Longrightarrow \exists \alpha_i / \alpha_i \neq 0.$$

Exemple 8.2.2.4 *Soit $\mathbb{R}^3$ un $\mathbb{R}$-espace vectoriel. Considérons le system (X_1, X_2, X_3) définit par $X_1 = (-1, 2, 1)$, $X_2 = (0, -1, 2)$ et $X_3 = -2, 4, 2)$. On montrons que le syxtème (X_1, X_2, X_3) est libé dans $\mathbb{R}^3$.*

Définition 8.2.2.11 (Système générateur)
Soit $(x_1, \cdots, x_n)$ un système de n vecteurs. Ce système est dit générateur de (ou engendrant l'espace) E, si tout vecteur de cet espace s'exprime comme une combinaison linéaire de vecteurs de ce systeème. Soit :

$$\forall x \in E \exists (\lambda_1, \cdots, \lambda_n) \in \mathbb{R}^n \text{ tel que } x = \lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_n x_n.$$

Exemple 8.2.2.5 *Considérons l'exemple donné 8.2.2.3, ce système est un systeme générateur de $\mathbb{R}^2$, car pour tout $(a, b) \in \mathbb{R}^2$ on*

$$(a, b) = (\frac{b-a}{3})\alpha_1 + (\frac{b+2a}{3})\alpha_2.$$

Définition 8.2.2.12 (Base)
Un système de n vecteurs $(x_1, \cdots, x_n)$, est une base s'il est à la fois libre et générateur ou soit tout vecteur de cet espace s'exprime de manière unique comme une combinaison linéaire de vecteurs de ce systeème. Soit :

$$\forall x \in E \exists ! (\lambda_1, \cdots, \lambda_n) \in \mathbb{R}^n \text{ tel que } x = \lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_n x_n.$$

Exemple 8.2.2.6 *Le système de vecteurs de l'exemple 8.2.2.3, est une base de $\mathbb{R}^2$.*

Définition 8.2.2.13 (Dimension)
On appelle dimension d'un espace vectoriel E et noté $\dim E$ le nombre maxima de vecteurs contenu dans sa base.

Rémarque 8.2.2.7 *Le nombre de vecteurs peut être fini ou non. Dans ce cas ont dit que E est de dimension fini ou infini.*

Proposition 8.2.2.3 *Dans un espace vectoriel de dimension n, tout système de moins de n vecteurs est libre.*

Proposition 8.2.2.4 *Dans un espace vectoriel de dimension n, tout système de plus de n vecteurs est lié.*

Proposition 8.2.2.5 *Dans un espace vectoriel de dimension n, tout système de n vecteurs est une base.*

Proposition 8.2.2.6 *Soit E un $\mathbb{K}$-espace vectoriel. On suppose que E est de dimension finie. Alors E possède une base. De plus cette base est de cardinal fini.*

Théorème 8.2.2.4 *Soient H un système libre ayant p éléments et T un système générateur ayant q éléments. Alors $p \leq q$, et l'on peut remplacer p éléments de T par les p éléments de H de manière que le nouveau système M obtenu soit toujours un système générateur.*

Conséquence 8.2.2.3 *Tout espace vectoriel de dimension finie possède une base fini, et toutes les bases d'un espace vectoriel ont le même nombre d'éléments qui, est dimension de cet espace vectoriel.*

Définition 8.2.2.14 *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n, et soit $\mathfrak{B} = (e_1, \cdots, e_n)$, une base de E. Tout vecteur x appartenant à E s'exprime de manière unique sous la forme*

$$x = x_1e_1 + x_2e_2 + \cdots + x_ne_n = \sum_{i=1}^{n} x_ie_i.$$

Les scalaires x_i s'appellent les coordonnées dex dans la base $\mathfrak{B}$.

Théorème 8.2.2.5 (de la base incomplète)
Soit E un $\mathbb{K}$-espace vectoriel. Supposont que $\dim E = n$, et soit $(e_1, \cdots, e_m)$, une famille libre de E. Supposons en suite que $m < n$. Alors, on peut trouver des vecteurs $(e_m+1, \cdots, e_n)$ dans E tels que $(e_1, \cdots, e_m, e_m+1 \cdots, e_n)$, soit une base de E. Dans ce cas on dit que, on a completé la famille $(e_1, \cdots, e_m)$ en une base de E.

Rémarque 8.2.2.8 *Soit E un $\mathbb{K}$-espace vectoriel et, soit F un sous espace vectoriel de E. Une base du sous espace vectoriel F est une base de F en tant qu'espace vectoriel.*

Définition 8.2.2.15 *On dit qu'un sous espace vectoriel est de dimension finie si, il est engendré en tant qu'espasce vectoriel par une famille de cardinal fini.*

Définition 8.2.2.16 *La dimension d'un sous espace vectoriel de dimension finie est le cardinal d'une base de ce sous espace vectoriel.*

Sous espaces vectoriels supplémentaires et somme directe de sous espaces vectoriels

Définition 8.2.2.17 (somme directe de deux sous espaces vectoriels)
Soit E un $\mathbb{K}$-espace vectoriel et, soit F_1 et F_2 deux sous espaces vectoriels de E. On dit que F_1 et F_2 sont en sommes directe si $F_1 \cap F_2 = \{0_E\}$. On note alors cette $F_1 \oplus F_2$ le sous espace somme de deux sous espaces vectoriels supplémentaires

Définition 8.2.2.18 (Sous espaces vectoriels supplémentaires)
Soient F_1 et F_2 deux sous espaces vectoriels d'un $\mathbb{K}$-espace vectoriel E. On suppose que F_1 et F_2 sont en sommes directe dans E et que $F_1 \oplus F_2 = E$, alors F_1 et F_2 sont dit supplémentaires dans E. On dit alors que F_1 est un supplémentaire de F_2 dans E.

Théorème 8.2.2.6 *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie. Soit F un sous espace vectoriel de E. Alors F possède un sous espace supplémentaire dans E.*

Démonstration 8.2.2.3 *Supposons $\dim E = n$. Comme F est un sous espace vectoriel de E, il est aussi de dimension finie. Posons $\dim F = k$. Soient $e_1, ..., e_k$ des vecteurs de F qui définissent une base deF. Cette famille qui, est libre dans F, lŠest aussi dans E. LŠutilisation du théorème de la base incomplète nous permet dŠêtre assurer de lŠexistence de $n - k$ vecteurs $e_{k+1}, ..., e_n$ tels que la famille $(e_1, ..., e_n)$ forme une base de E. Soit F' le sous espace vectoriel engendré par $e_{k+1}, ..., e_n$. Il est clair que $F \cap F' = \{0_E\}$ et que $F \oplus F' = E$. F' est donc bien un sous espace supplémentaire au sous espace F.*

Définition 8.2.2.19 *Un sous espace vectoriel de dimension un est appelé une droite vectorielle.*

Définition 8.2.2.20 *Un sous espace vectoriel de dimension deux est appelé une plan vectoriel.*

Théorème 8.2.2.7 *Si F et F' sont deux sous espaces vectoriels de dimension finie du $\mathbb{K}$-espace vectoriel E alors* $\dim F + \dim F = \dim(F + F) + \dim(F \cap F')$

Démonstration 8.2.2.4 *Notons que $F \cap F'$ est un sous espace vectoriel de F et F' . Posons* $\dim F = m$, $\dim F' = l$ *et* $\dim(F \cap F') = k$. *Supposons aussi* $(e_1, ..., e_m)$ *une base de F, que lŠon complète en une base* $(e_1, ..., e_k, f_{k+1}, ..., f_m)$ *de F et en une base* $(e_1, ..., e_k, f'_{k+1}, ..., f'_l)$ *de F'. La famille* $(e_1, ..., e_k, f_{k+1}, ..., f_m, f'_{k+1}, ..., f'_l)$ *est donc une base de $F + F'$. On peut alors dans ce cas écrire les ǵalités suivantes :* $\dim(F + F') = k + m - k + l - k = m + l - k = \dim F + \dim F - \dim(F \cap F')$.

Comme nous l'avons vue, si les vecteurs $x_1, ..., x_m$ sont en nombre fini,alors la dimension du sous espace vectoriel quŠils engendrent est nécessairement de dimension finie. Nous pouvons avoir la définition suivante.

Définition 8.2.2.21 *Soit m un entier positif. On appelle rang dŠun système de vecteurs $x_1, ..., x_m$ du $\mathbb{K}$-espace vectoriel E la dimension de $Vect(x_1, ..., x_m)$.*

Espaces vectoriels de dimension infinie

Comme nous l'avons déjà mentionné, les propriétés d'existence d'un supplémentaire pour un sous espace vectoriel, d'existence d'une base et le théorème de la base incomplète sont vraies en dimension infinie. Nous allons maintenant établir ces 3 propriétés.

Théorème 8.2.2.8 *Soit E un espace vectoriel sur le corps $\mathbb{K}$. Soit F un sous espace vectoriel de E . Soient H un autre sous espace vectoriel de E tel que $F \cap H = \{0_E\}$ et L aussi un autre sous espace vectoriel de E tel que $F + L = E$. Alors il existe un supplémentaire W de F contenu dans W et contenant H.*

Démonstration 8.2.2.5 *Considérons l'ensemble A des sous espaces vectoriels de E contenant H et contenus dans L. A n'est pas vide car H est élément de A. A est partiellement ordonné par la relation* **être inclu dans ou être égal à :** $\subseteq$ *. Considérons une partie totalement ordonné de A. Considérons ensuite la réunion des éléments de cette partie et notons la U. Comme la partie est totalement ordonnée, cette réunion est encore un sous espace vectoriel de E qui contient H et qui est contenu dans L. Cette réunion a comme seul élément commun avec F le vecteur nul de E. U est de plus un majorant de cette partie pour la relation d'ordre donné par l'inclusion. A est donc un ensemble inductif. Appliquons le lemme de Zorn. Il existe un élément maximal pour A. Notons le W. W vérifie :*

1. $F \cap W = \{0_E\}$
2. $H \subseteq W \subseteq L$

3. $\forall T \in A,\ T \subseteq W$.

Montrons que W *est un supplémentaire à* F. *Au regard de ce que l'on sait déjà, il suffit de pouver que* $F+W = E$. *Soit* $E = F+L$. *Alors* x *s'écrit :* $x = f+l$ *où* $f \in F$ *et où* $l \in L$. *Si on trouve* $w \in W$ *et* $f \in F$ *tels que* $x = f + w$ *alors c'est gagné. Si* $l \in W$, *alors* w *est trouvé. Sinon, on considére le sous espace vectoriel* X *engendré par* W *et* l. *Ce sous epace vectoriel contient strictement* W. *Par conséquent, comme* W *est maximale dans* A, X *n'appartient pas à* A. *Mais* X *vérifie les points* 2 *et* 3 *précédents. Il ne vérifie donc pas le point* 1. *Cela signifie qu'il existe un vecteur* $y \in X \cap F$. y *y est donc d'une part élément de* F *mais a d'autre part une écriture de la forme* $y = a + \lambda l$ *où* $\lambda \in \mathbb{K}$ *et où* $a \in W$. *Si* $\lambda = 0$, *alors* y *est un élément de* F, *qui est aussi un élément de* W. *C'est impossible car* $W \in A$. *Donc* $\lambda \neq 0$. *Alors* $l = \frac{1}{\lambda}(y-a)$. *Cela entraine que* $x = f + \frac{1}{\lambda}y - \frac{1}{\lambda}a$. *On n'a bien* $f + \frac{1}{\lambda}y \in F$ *et* $\frac{1}{\lambda}a \in W$ *Nous avons ainsi obtenu la décomposition posé dans le théorème.*

De ce théorème nous avons la conséquence suivante.

Conséquence 8.2.2.4 *Soit* E *un espace vectoriel sur le corps* $\mathbb{K}$. *Soit* F *un sous espace vectoriel de* E . *Alors* F *possède un supplémentaire dans* E.

Proposition 8.2.2.7 *Soit* E *un espace vectoriel non trivial sur le corps* $\mathbb{K}$, *alors* E *possède une base.*

Démonstration 8.2.2.6 *Soit* $\mathcal{F}$ *l'ensemble de toute les familles libres de* E. $\mathcal{F}$ *est non vide car si* x *est un vecteur non nul de* E *alors* $\{x\}$ *est une famille libre dans* E. $\mathcal{F}$ *est un ensemble partiellement ordonné par l'inclusion. Soit* $\mathcal{A}$ *une partie de* $\mathcal{F}$ *totalement ordonnée non vide. Alors la réunion des éléments de cette famille est encore un élément de* $\mathcal{F}$. *Cette réunion, de plus, est un majorant de* $\mathcal{F}$. *Donc* $\mathcal{F}$ *est inductif. Et* $\mathcal{F}$ *possède alors un élément maximal. Notons* F *cette famille libre de vecteurs de* E *et élément maximal de* $\mathcal{F}$. *Cette famille est libre maximale dans* E. *C'est par conséquent une base de* E.

Théorème 8.2.2.9 Théorème de la base incomplete en dimension infinie *Soit* $(e_i)_{i\in I}$ *une partie génératrice de* E. *Soit* J *un sous ensemble de* I *tel que* $(e_i)_{i\in J}$ *une système libre dans* E. *Alors il existe* K *de sorte que* $J \subseteq K \subseteq I$ *tel que* $(e_i)_{i\in K}$ *soit une base de* E.

Démonstration 8.2.2.7 *Remarquons d'abord que l'on a présupposer l'existence de partie génératrice dans* E. *Ceci est, d'après la propriété précédente, évident. Considérons cette fois ci l'ensemble* $\mathcal{F}$ *des familles libres* $(e_i)_{i\in L}$ *avec* $J \subseteq L \subseteq I$. $\mathcal{F}$ *est ordonné partiellement par l'inclusion. Si* $\mathcal{A}$ *est une partie de* $\mathcal{F}$ *totalement ordonnée pour lŠinclusion, alors la famille réunion des éléments de* $\mathcal{A}$ *est encore élément de* $\mathcal{F}$ *. De plus, cette réunion majore* $\mathcal{A}$. *On en déduit que* $\mathcal{F}$ *est inductif. D'après le lemme de Zorn,* $\mathcal{F}$ *possède un élément maximal. Soit* $J \subseteq L \subseteq I$. $\mathcal{F}$ *tel que* $(e_i)_{i\in L}$ *soit l'élément maximal de* $\mathcal{F}$. *Cette famille est libre. Montrons qu'elle est aussi génératrice. Il suffit pour cela de remarquer que pour tout vecteur* e_k, *avec* k *n'appartenant pas à* L, *la famille* $(e_i)_{i\in L} \cup \{e_k\}$ *est liée dans* E. *Par conséquent, comme* $(e_i)_{i\in I}$ *engendre* E *et que* $(e_i)_{i\in I} \subseteq Vect((e_i)_{i\in L})$, *alors* $(e_i)_{i\in L}$ *engendre* E. *C'est donc bien une base de* E.

Bibliographie

[1] R.P. Burn Groups, a path to geometry, Cambridge university press, Cambridge, 1985.

[2] M. I. Gelfand Lecture on linear algebra, Interscience Puplishers, New York, 1961.

[3] R. Godement Cours d'a'gébrebre, Collection Enseignement des Sciences , 5. Hermann, Paris, 1987. 671 pp.

[4] M. Kargapolov et I. Merzliakov Eléments de la théorie des groupes, Mir, Moscou, 1985.

[5] A. Kostrikin Introduction à l'algèbre, Mir, Moscou, 1981.

[6] A. Kurosh Cours d'algèbre supérieure, Mir, Moscou, 1973.

[7] B.L. Van der Waerden, Modern algebra 2 vol., Springer, Berlin, 1955.

[8] O. Zariski and P. Samuel, 2 vol. Commutative Algebra, D. Van Nostrand Cy., Princeton, 1958.

[9] Michel Demazure Cours d'algèbre Nouvelle Bibliothèque Mathématique Cassini, Paris, 1997. xviii+302 pp.

[10] Joseph-Alfred Serret, Cours d'algèbre supérieure Tome I et II. Les Grands Classiques Gauthier-Villars Editions Jacques Gabay, Sceaux, 1992. xii+695 pp.

[11] Daniel Perrin, Cours d'algébre. Collection de l'Ecole Normale Supérieure de Jeunes Filles, 18. Ecole Normale Supérieure de Jeunes Filles, Paris, 1982. 212 pp.

[12] J. Querré, Cours d'algébre. Maîtrise de Mathématiques. Masson, Paris-New York-Barcelona, 1976. x+240 pp.

[13] Marc Zamansky, Introduction à l'algébre et l'analyse modernes. Troisième édition. Collection Universitaire de Mathématiques, No. 1 Dunod, Paris 1967 xviii+435 pp.

[14] Jacqueline Lelong-Ferrand ; Jean-Marie Arnaudiès, Cours de mathématiques. Tome 1. Algébre. Troisième édition. 1er Cycle Universitaire. Classes Préparatoires. Mathématiques. Dunod, Paris, 1977. x+534 pp.

[15] Jacques Dixmier, Cours de mathématiques du premier cycle. Première année. Deuxième édition. Avec la collaboration de Pierre Dugac. Cahiers Scientifiques, Fasc. 30. Gauthier-Villars, Paris, 1976. ix+630 pp

[16] Bernard Charles, Algèbre générale. Mathématiques. Presses Universitaires de France, Paris, 1984. 336 pp.

[17] Léonce Lesieur ; Yves Meyer ; Claude Joulain ; Jean Lefebvre, Algèbre générale. Collection U, Série Mathématiques. Librairie Armand Colin, Paris, 1975. viii+243 pp.

[18] Michel ALESSANDRI. Thèmes de Géométrie. Dunod, 1999.

[19] Marcel BERGER. Géométrie. Cedic-Nathan, 1973.

[20] Claude CARREGA. Théorie des corps. Hermann, 1975.
[21] H.S.M. COXETER. Introduction to Geometry. John Wiley Sons, 1989.
[22] Jean de BIASI. Mathématiques pour le CAPES et l'Agrégation Interne. Ellipses, 1995.
[23] Jean DELCOURT. Théorie des Groupes. Dunod, 2001.
[24] Jean DELCOURT. Problèmes de Mathématiques. Dunod, 2004.
[25] Michel DEMAZURE. Cours dŠAlgèbre. Cassini, 1997.
[26] Alain BOUVIER et Denis RICHARD. Groupes. Hermann, 1968.
[27] Marie-Noëlle GRAS et Georges GRAS. Algèbre fondamentale, Arithmétique. Ellipses, 2004.
[28] Serge FRANCINOU et Hervé GIANELLA. Exercices de Mathématiques pour l'Agrégation. Masson, 1993.
[29] Jean-Marie ARNAUDIES et José BERTIN. Groupes et Géométrie. Ellipses, 1996.
[30] H.S.M. COXETER et S.L. GREITZER. Redécouvrons la Géométrie. Dunod, 1971.
[31] Jean FRESNEL. Méthodes Modernes en Géométrie. Hermann, 1996.
[32] Rémi GOBLOT. Algèbre linéaire. Masson, 1995.
[33] Rémi GOBLOT. Thèmes de géométrie. Masson, 1998.
[34] Rémi GOBLOT. Algèbre commutative. Dunod, 2001.
[35] Paul HALMOS. Naive set theory. Springer, 1986. [19] Rached MNEIMNE. Éléments de Géométrie. Cassini, 1997.
[36] Jean-Marie MONIER. Géométrie, MPSI, MP. Dunod, 3 e édition, 2003.
[37] Daniel PERRIN. Cours d'algèbre. Ellipses, 1996.
[38] Marc ROGALSKI. Carrefours entre Analyse, Algèbre et Géométrie. Ellipses, 2001.
[39] Romain VIDONNE. Groupe circulaire, rotations et quaternions. Ellipses, 2001.