UNIVERSITE CHEIKH ANTA DIOP DE DAKAR
FACULTE DES SCIENCES ET TECHNIQUES
DEPARTEMENT DE MATHEMATIQUE ET INFORMATIQUE

Première Année

Algèbre : 2019 - 2020

Pr. Mamadou BARRY

20 juillet 2020

Table des matières

Chapitre 1

Notions de Logique mathématique

Sommaire

La logique est la science qui traite des méthodes de raisonnement, en particulier elle nous offre des règles et techniques qui permettent de décider si une déduction est valide ou non.

1.1 Défintions et Exemples

Définition 1.1.1 *On appelle proposition tout énoncé qui est vrai dans certaines conditions et faux dans d'autres conditions mais dont on peut toujours dire s'il est vrai ou faux.*

La propriété essentielle d'une proposition P est donc d'être dotée de l'une des valeurs de vérité V (vrai) ou F (faux).

Exemple 1.1.1 *"n est entier et n est multiple de 2". Cette proposition est vraie si n est pair et fausse si n impair.*

Définition 1.1.2 *Une assertion est un énoncé dont on peut affirmer toujours sans ambiguité s'il est vrai ou s'il est faux.*

Autrement dit : Une assertion est une proposition qui est toujours vraie ou qui est toujours fausse.

Exemple 1.1.2

1. *"la neige est blanche"*
2. *"la terre est ronde"*
3. *"Sacramento est la capitale des USA"*
4. *"Si n est un entier alors $2n+1$ est un entier pair"*

Définition 1.1.3

1. *On appelle axiome, toute proposition à laquelle on attribue par convention la valeur Vrai.*
2. *On appelle théorème, toute proposition dont on démontre qu'elle a la valeur Vrai.*

Remarque 1.1.1 *Soit P une proposition. Le tableau suivant représente la table de vérité de P*

P
V
F

1.2 Connecteurs logiques

A partir des propositions P et Q ; on peut former d'autres propositions à l'aide des liaisons logiques appelées connecteurs logiques. Ses principaux connecteurs logiques sont : la négation, la conjonction, la disjonction, l'implication et l'équivalence.

1.2.1 La négation

La négation d'une proposition P est une proposition notée $\rceil P$ ou $\bar{P}$ ou encore "non P".

La proposition $\rceil P$ est vraie si P est fausse et $\rceil P$ est fausse si P est vraie

P	$\rceil P$
V	F
F	V

Table vérité de la négation

1.2.2 La conjonction

Etant données deux propositions P, Q. La conjonction de P, Q; est une proposition notée $P \wedge Q$ ou encore "P *et* Q".

La proposition $P \wedge Q$ est vraie si les deux propositions P, Q le sont simultanément. La proposition $P \wedge Q$ est fausse dans le cas contraire

P	Q	$P \wedge Q$
V	V	V
V	F	F
F	V	F
F	F	F

Table vérité de "*et*"

1.2.3 La disjonction

Etant données deux propositions P, Q. On appelle la disjonction de P et Q, la proposition notée $P \vee Q$ ou encore "P *ou* Q".

La proposition $P \vee Q$ est vraie si l'une au moins des propositions est vraie et $P \vee Q$ est fausse si P et Q sont simultanément fausses.

P	Q	$P \vee Q$
V	V	V
V	F	V
F	V	V
F	F	F

Table vérité de "*ou*"

1.2.4 L'implication

Etant données deux propositions P, Q.

La proposition $\rceil P \vee Q$ signifie "P implique Q" et se note "$P \Longrightarrow Q$".

La proposition "$P \Longrightarrow Q$" est fausse si P est vraie et Q est fausse.

La proposition "$P \Longrightarrow Q$" est vraie dans le cas contraire.

Remarque 1.2.1 "$P \Longrightarrow Q$" *signifie aussi "si* P *alors* Q*"*

P	Q	$P \Longrightarrow Q$
V	V	V
V	F	F
F	V	V
F	F	V

Table vérité de l'implication

1.2.5 L'équivalence

Etant données deux propositions P et Q.

La proposition $(P \Longrightarrow Q) \wedge (Q \Longrightarrow P)$ s'appelle l'équivalence de P et Q et se note "$P \Longleftrightarrow Q$" et on lit "P équivalente à Q".

La proposition "$P \Longleftrightarrow Q$" est vraie si P et Q ont même valeur de vérité.

Autrement dit : "$P \Longleftrightarrow Q$" est vraie si P et Q sont simultanément vraies ou simultanément fausses et $P \Longrightarrow Q$ est fausse dans le cas contraire $\big[$(P vraie et Q fausse) ou (P fausse et Q vraie)$\big]$.

Remarque 1.2.2 *Soient P, Q et R trois propositions. Les conditions suivantes sont équivalentes :*

1. *les propositions P, Q et R sont équivalentes.*
2. $(P \Longleftrightarrow Q) \wedge (Q \Longleftrightarrow R)$.
3. $(P \Longleftrightarrow R) \wedge (P \Longleftrightarrow Q)$.
4. $P \Longrightarrow Q \Longrightarrow R \Longrightarrow P$.

P	Q	$P \Longleftrightarrow Q$
V	V	V
V	F	F
F	V	F
F	F	V

Table de vérité de l'équivalence

1.2.6 Propriétés des connecteurs logiques

Soient P, Q *et* R trois propositions.

1. Commutativité
   - $P \wedge Q \Longleftrightarrow Q \wedge P$ (commutativité de "et")
   - $P \vee Q \Longleftrightarrow Q \vee P$ (commutativité de "ou")

2. Associativité
   - $(P \wedge Q) \wedge R \Longleftrightarrow P \wedge (Q \wedge R)$ (associativité de "et")
   - $(P \vee Q) \vee R \Longleftrightarrow P \vee (Q \vee R)$ (associativité de "ou")
3. Distributivité
   - Le connecteurs "ou" est distributif par rapport au connecteur "et"

   $$\left.\begin{array}{l} P \vee (Q \wedge R) \Longleftrightarrow (P \vee Q) \wedge (P \vee R) \\ (Q \wedge R) \vee P \Longleftrightarrow (Q \vee P) \wedge (R \vee P) \end{array}\right\} \text{(distributivité de "ou" par rapport à "et")}$$

   - Le connecteurs "et" est distributif par rapport au connecteur "ou"

   $$\left.\begin{array}{l} P \wedge (Q \vee R) \Longleftrightarrow (P \wedge Q) \vee (P \wedge R) \\ (Q \vee R) \wedge P \Longleftrightarrow (Q \wedge P) \vee (R \wedge P) \end{array}\right\} \text{(distributivité de "et" par rapport à "ou")}$$

4. Double négation : $\rceil(\rceil P) \Longleftrightarrow P$
5. Lois de Morgan
   - $\rceil(P \wedge Q) \Longleftrightarrow \rceil P \vee \rceil Q$
   - $\rceil(P \vee Q) \Longleftrightarrow \rceil P \wedge \rceil Q$
6. $(P \Longrightarrow Q) \Longleftrightarrow (\rceil Q \Longrightarrow \rceil P)$: contraposée
7. $\rceil(P \Longrightarrow Q) \Longleftrightarrow \rceil(\rceil P \vee Q) \Longleftrightarrow P \wedge \rceil Q$: négation de l'implication
8. Idempotence
   - Le connecteurs "et" est idempotent : $P \wedge P \Leftrightarrow P$
   - Le connecteurs "ou" est idempotent : $P \vee P \Leftrightarrow P$
9. $P \wedge \rceil P \Longleftrightarrow$ Faux : Règle de la contradiction
10. $P \vee \rceil P \Longleftrightarrow$ Vraie : Règle de l'évidence
11. $P \wedge$ Faux $\Leftrightarrow$ Faux et $P \vee$ Vrai $\Leftrightarrow P$
12. $P \vee$ Faux $\Leftrightarrow P$ et $P \vee$ Vrai $\Leftrightarrow$ Vrai

Exemple 1.2.1 *Soit R, S et T trois propositions. Vérifier de deux manière s que*

$$(R \Longrightarrow S) \Longrightarrow \Big[(S \Longrightarrow T) \Longrightarrow (R \Longrightarrow T)\Big] \qquad \textit{est vraie}$$

Méthode 1 : *Table de vérité. On pose* $a = R \Longrightarrow S$ *et* $b = (S \Longrightarrow T) \Longrightarrow (R \Longrightarrow T)$

R	S	T	$S \Rightarrow T$	$R \Rightarrow T$	$R \Rightarrow S$	$(S \Rightarrow T) \Rightarrow (R \Rightarrow T)$	$a \Rightarrow b$
V	V	V	V	V	V	V	V
V	V	F	F	F	V	V	V
V	F	V	V	V	F	V	V
V	F	F	V	F	F	F	V
F	V	V	V	F	F	F	V
F	V	F	F	V	V	V	V
F	F	V	V	V	V	V	V
F	F	F	V	V	V	V	V

Méthode 2 :

$$
\begin{aligned}
(R \Rightarrow S) \Rightarrow [(S \Rightarrow T) \Rightarrow (R \Rightarrow T)] &\Leftrightarrow (R \Rightarrow S) \Rightarrow [(\urcorner S \vee T) \Rightarrow (\urcorner R \vee T)] \\
&\Leftrightarrow (R \Rightarrow S) \Rightarrow [\urcorner(\urcorner S \vee T) \vee (\urcorner R \vee T)] \\
&\Leftrightarrow (R \Rightarrow S) \Rightarrow [(s \wedge \urcorner T) \vee (\urcorner R \vee T)] \\
&\Leftrightarrow (\urcorner R \vee S) \Rightarrow [(S \vee \urcorner R \vee T) \wedge (\urcorner T \vee \urcorner R \vee T)] \\
&\Leftrightarrow \urcorner(\urcorner R \vee S) \vee [(\vee \urcorner R \vee T) \wedge \ \mathit{Vrai} \vee \urcorner R)] \\
&\Leftrightarrow (R \wedge \urcorner S) \vee [(S \vee \urcorner R \vee T) \wedge \ \mathit{Vrai}] \\
&\Leftrightarrow (R \wedge \urcorner S) \vee (S \vee \urcorner R \vee T) \\
&\Leftrightarrow (R \vee S \vee \urcorner R \vee T) \wedge (\urcorner S \vee S \vee \urcorner R \vee T) \\
&\Leftrightarrow (\mathit{Vrai} \ \wedge S \vee T) \vee (\mathit{Vrai} \vee \urcorner R \vee T) \\
&\Leftrightarrow \mathit{Vrai} \ \wedge \ \mathit{Vrai} \\
&\Leftrightarrow \mathit{Vrai}.
\end{aligned}
$$

1.3 Quantificateurs

1.3.1 Définitions et exemples

Il y a en général deux types quantificateurs : le quantificateur universel et le quantificateur existentiel.

Notation 1.3.1 *1. Le quantificateur universel est noté "$\forall$" on lit "quel que soit"*

2. Le quantificateur existentiel est noté "$\exists$" on lit "il existe".
Soit $P(x)$ une proposition contenant un objet x appelé variable assujetti à appartenir à un ensemble E appelé référentiel.

3. Pour exprimer l'assertion "il existe au moins un objet x du référentiel E pour lequel $P(x)$ est vraie"; on convient d'écrire : $(\exists x \in E)\ P(x)$ ou $(\exists x)\ P(x)$.

4. Pour exprimer l'assertion "x est un élément quelconque de E pour lequel $P(x)$ est vraie"; on écrit "$\forall x \in E,\ P(x)$" on lit "pour tout x, $P(x)$".

Exemple 1.3.1 *1.* $(\exists x \in \mathbb{R})(x^2 - 3x + 2 = 0)$

2. $(\forall x \in \mathbb{R})(x^2 + 4 > 0)$.

1.3.2 Propriétés des quantificateurs

1. $\rceil[(\exists x)P(x)] \Longleftrightarrow (\forall x)(\rceil P(x))$
2. $\rceil[(\forall x)P(x)] \Longleftrightarrow (\exists x)(\rceil P(x))$
3. $\rceil[[(\forall x)(P(x) \Longrightarrow Q(x))] \Longleftrightarrow [(\exists x)(P(x) \wedge \rceil Q(x))]$
4. $[(\exists x)(\exists y)P(x,y)] \Longleftrightarrow [(\exists y)(\exists x)(P(x,y)]$
5. $[(\forall x)(\forall y)P(x,y)] \Longleftrightarrow [(\forall y)(\forall x)(P(x,y)]$
6. $[(\forall x)(\exists y)P(x,y)] \nLeftrightarrow [(\exists y)(\forall x)(P(x,y)]$
7. $[(\exists x)(\forall y)P(x,y)] \Longrightarrow [(\forall y)(\exists x)(P(x,y)]$
8. $[(\forall x)(P(x)\ et\ Q(x))] \Longleftrightarrow [((\forall x\ P(x))\ et\ (\forall x\ Q(x))]$
9. $[(\forall x)(P(x)\ ou\ Q(x))] \nLeftrightarrow [(\forall x\ P(x))\ ou\ (\forall x\ Q(x))]$

10. $[(\exists x)(P(x)\ ou\ Q(x))] \Longleftrightarrow \big[(\exists x\ P(x))\ ou\ (\exists x\ Q(x))\big]$
11. $[(\exists x)(P(x)\ et\ Q(x))] \Longrightarrow [((\exists x\ P(x))\ et\ (\exists x\ Q(x))]$.

Remarque 1.3.1 *La réciproque de la dernière relation est en général fausse*

$$\big[(\exists x\ P(x))\ et\ (\exists x(Q(x))\big] \nRightarrow (\exists x)(P(x)\ etQ(x)).$$

Exemple 1.3.2 *"(il existe des hommes riches et honnêtes)" implique "il existe des hommes riches" et "il existe des hommes honnêtes"*

Alors que "il existe des hommes riches et il existe des hommes honnêtes" n'implique pas que "il existe des hommes riches et honnêtes".

Exemple 1.3.3 *1. Soit* $(u_n)_{n\in\mathbb{N}}$ *une suite numérique et* $\ell \in \mathbb{R}$

$(\forall \varepsilon \in \mathbb{R}_+^*)(\exists \eta \in \mathbb{N}^*)(\forall n \in \mathbb{N})(n \geq \eta \Longrightarrow |u_n - \ell| < \varepsilon)$.

2. $(\forall x \in \mathbb{N}^*, \exists y \in \mathbb{R}, x \geq y) \Longrightarrow (\exists z \in \mathbb{N}, xy = z)$

Négation :

1. $(\exists \varepsilon \in \mathbb{R}_+^*)(\forall \eta \in \mathbb{N}^*)(\exists n \in \mathbb{N}^*)(n \geq \eta$ et $|u_n - \ell| \geq \varepsilon)$
2. $(\forall x \in \mathbb{N}^*, \exists y \in \mathbb{R}, x \geq y)$ et $(\forall z \in \mathbb{N}, xy \neq z)$

1.4 Quelques méthodes usuelles de démonstrations

Démontrer une assertion P consiste à déduire logiquement P à partir d'un petit nombre d'assertions (ou axiomes).

1.4.1 Notion de contre - exemple

On considère l'assertion $(\exists x,\ A(x))$

On a $A(x)$ est un pédicat en une variable pour démontrer une assertion. Ce type on exhibe un objet du référentiel qui vérifie la propriété $A(x)$.

Pour démontrer par un contre - exemple que la propriété $[\forall x, A(x)]$ est fausse, il sjuffit d'exhiber un objet x du référentiel pour lequel $\rceil A(x)$ est vraie.

Exemple 1.4.1 $\forall x \in \mathbb{R}, \quad x \neq \sqrt{x}+6$ *est fausse. Pour* $x = 9 \qquad x = \sqrt{x}+6$ *est vraie.*

1.4.2 La Démonstration par contraposée

La démonstration par contraposée repose sur la règle logique suivante

$$\boxed{(P \Longrightarrow Q) \Longleftrightarrow (\rceil Q \Longrightarrow \rceil P)}$$

Exemple 1.4.2 *Soit* $x \in \mathbb{N}$
Montrer que $(x^2$ *impair*$) \Longrightarrow (x$ *impair*$)$.
Démontrons par contraposée x *pair* $\Longrightarrow x^2$ *pair.*
En effet : Supposons que x *est pair.*
Donc $\exists k \in \mathbb{N}$ *tel que* $x = 2k$; $x^2 = 4k^2 = 2(2k^2)$.
Ainsi x^2 *est pair.*
D'où x^2 *impair* $\Longrightarrow x$ *impair.*

Exemple 1.4.3 *Soient k et k' deux entiers naturels non nuls. Montrer que* $(kk' = 1 \Rightarrow k = k' = 1)$.

1.4.3 La Démonstration par l'absurde

La démonstration par l'absurde repose sur la règle logique suivante :

$$[\rceil P \Longrightarrow (Q \wedge \rceil Q)] \Longleftrightarrow P$$

Exemple 1.4.4 *Montrer que* $\sqrt{2}$ *est irrationnel.*

Supposons que $\sqrt{2}$ *est rationnel. Ainsi* $\sqrt{2} = \frac{p}{q}$, *avec pgcd(p, q) = 1.*

$$\begin{aligned}
\sqrt{2} = \frac{p}{q} &\Rightarrow 2 = \frac{p^2}{q^2} \\
&\Rightarrow p^2 = 2q^2 \\
&\Rightarrow p^2 \text{ est pair} \\
&\Rightarrow p \text{ est pair}(\star) \\
&\Rightarrow p = 2k \\
&\Rightarrow p^2 = 4k^2
\end{aligned}$$

On a alors

$$\begin{aligned}
2 = \frac{4k^2}{q^2} &\Rightarrow q^2 = 2k^2 \\
&\Rightarrow q^2 \text{ est pair} \\
&\Rightarrow q \text{ est pair}(\star\star)
\end{aligned}$$

Absurde d'aprés $(\star)$ *et* $(\star\star)$, *car pgcd(p, q) = 1.*

1.4.4 La démonstration par réccurence

1.4.4.1 Récurrence totale

La récurrene totale est basée sur la propriété suivante :

Soit X une partie de $\mathbb{N}$ s'il vérifie

1. $0 \in X$
2. si $\forall \in X$, $x + 1 \in X$

Alors $X = \mathbb{N}$.

La propriété de récurrence est sous la forme suivante :

Soit $\mathcal{P}(n)$ une relation dépendant de n.

$$\mathcal{P}(0) \wedge \big[\forall k \in \mathbb{N}, \big(\mathcal{P}(k) \Rightarrow \mathcal{P}(k+1)\big)\big] \Rightarrow \big(\forall n \in \mathbb{N}, \mathcal{P}(n)\big)$$

1.4.4.2 Récurrence incomplète

Elle est basée sur la règle suivante :

$$\exists n_0 \in \mathbb{N}, \mathcal{P}(n_0) \wedge \big[\forall k \geq n_0, \big(\mathcal{P}(k) \Rightarrow \mathcal{P}(k+1)\big)\big] \Rightarrow \big(\forall n \geq n_0, \mathcal{P}(n)\big)$$

Exemple 1.4.5 *Soit* $S_n = 1 + 3 + 5 + ... + (2n-1)$. *Montrer que* $\forall n \in \mathbb{N}^\star, S_n = n^2$.

Soit $\mathcal{P}(n) : S_n = n^2$
On a $\mathcal{P}(1) : S_1 = 1 = 1^2$
Supposons pour $k \geq 1$, on a $\mathcal{P}(k) : S_k = k^2$:
Montrons que $\mathcal{P}(k+1)$:

$$\begin{aligned} S_{k+1} &= 1 + 3 + 5 + ... + (2k-1) + [2(k+1) - 1] \\ &= S_k + 2k + 1 \\ &= k^2 + 2k + 1 \\ &= (k+1)^2 \end{aligned}$$

D'où $\mathcal{P}(k+1)$. Ainsi $\forall n \geq 1, \mathcal{P}(n)$. Par conséquent $\forall n \in \mathbb{N}^\star, S_n = n^2$.

1.5 Exercices

Exercice 1. Soient P, Q, R des propositions.
Dresser la table de vérité de la formule :

$$[(P \Rightarrow R) \vee (Q \Rightarrow R)] \Rightarrow [(P \vee Q) \Rightarrow R]$$

Exercice 2. Soient R, S et T trois assertions.
Montrer de deux manières différentes que les relations suivantes sont des tautologies :

1. $(R \Rightarrow S) \Rightarrow [(R \vee T) \Rightarrow (S \vee T)]$
2. $(R \Rightarrow S) \Rightarrow \big[(R \Rightarrow T) \Rightarrow [R \Rightarrow (S \wedge T)]\big]$

Exercice 3 : Donner la négation des propositions suivantes :

1. $(\forall x \in \mathbb{N}(\exists y \in \mathbb{N}^*)(\forall z \in\in \mathbb{N})(x = yz)$
2. Soit $(u_n)_{n\in\mathbb{N}}$ une suite réelle et $\ell \in \mathbb{R}$.

$$(\forall \varepsilon \in \mathbb{R}_+^* \ (\exists N \in \mathbb{N}) \ (\forall n \in \mathbb{N}) \ [(n > N) \Longrightarrow |u_n - \ell| < \varepsilon]$$

3. Soit f une application de $\mathbb{R}$ dans $\mathbb{R}$ et $x_o \in \mathbb{R}$

$$(\forall \varepsilon > 0) \ (\exists \rho > 0) \ (\forall x \in \mathbb{R}) \ [|x - x_o| < \rho \Longrightarrow |f(x)| < \varepsilon]$$

4. $[(\forall x \in \mathbb{R}) \ (x \leq 0)] \Longrightarrow [(\exists y \in \mathbb{R}^+) \ (x^2 = y)]$
5. $(\forall \epsilon > 0) \ (\exists \eta > 0) \ (\forall (x, y) \in I^2) \ \big[\mid x - y \mid \leq \eta \Rightarrow \mid f(x) - f(y) \mid \leq \epsilon\big]$
6. $(\forall \varepsilon > 0) \ (\exists \rho > 0) \ (\forall x \in \mathbb{R}) \ \big[|x - x_o| < \rho \Rightarrow |f(x) - f(x_0)| < \varepsilon\big]$

Exercice 4. Soient les quatres assertions suivantes :
i) $\exists x \in \mathbb{R} \ \forall y \in \mathbb{R} \ x + y < 0$ ii) $\forall x \in \mathbb{R} \ \exists y \in \mathbb{R} \ x + y < 0$
iii) $\forall x \in \mathbb{R} \ \forall y \in \mathbb{R} \ x + y < 0$ iv) $\exists x \in \mathbb{R} \ \forall y \in \mathbb{R} \ y^2 < x$.

1. Les assertions i), ii), iii), iv) sont-elles vraies ou fausses ?
2. Donner leur négation.

Exercice 5. Soient x, y et z trois réels parmi lesquels il y a 0 et deux réels non nuls de signe contraire. On suppose que les trois implications suivantes sont vraies.

1. $(x = 0) \Rightarrow (y > 0)$
2. $(x > 0) \Rightarrow (y < 0)$
3. $(y \neq 0) \Rightarrow (z > 0)$

Déterminer le signe de x, y et z.

Exercice 6. Soient $x_1, x_2, ..., x_n$ des entiers strictement positifs.

1. Montrer que $\frac{x_i}{x_j} + \frac{x_j}{x_i} \geq 2$.
2. Montrer par récurrence n que $(x_1 + x_2 + ... + x_n)(\frac{1}{x_1} + \frac{1}{x_2} + ... + \frac{1}{x_n}) \geq n^2$.

Exercice 7. Montrer par récurrence que :

1. $\frac{1}{1.2.3} + \frac{1}{2.3.4} + ... + \frac{1}{n(n+1)(n+2)} = \frac{n(n+3)}{4(n+1)(n+2)}$.
2. $\sum_{k=0}^{n} \frac{k}{(k+1)!} = 1 - \frac{1}{(n+1)!}$
3. $\sum_{k=0}^{n} k.k! = (n+1)! - 1$.

Exercice 8.

1. Montrer par contraposée que pour tout entier naturel n, si n^2 est pair alors n est pair.
2. Soit $n \in \mathbb{N}^\star$, démontrer par l'absurde que $n^2 + 1$ n'est pas le carré d'un entier.
3. Montrer que $\sqrt{2}$ et $\frac{ln(2)}{ln(3)}$ sont des irrationnels.

Chapitre 2

Ensembles - Applications - Relations

Sommaire

2.1 Ensembles

2.1.1 Définitions et exemples

Définition 2.1.1 *Un ensemble est une collection d'objets appelés éléments ou points.*

En général on désigne les ensembles par des lettres majuscules et les éléments par des lettres minuscules.

Remarque 2.1.1 *Si E est un ensemble. Si a un élément de E, on écrit "$a \in E$". On lit "a appartient à E".*
Pour exprimer que a n'appartient pas à E, on écrit "$a \notin E$".

Notation 2.1.1 *Un ensemble qui n'a pas d'élément est appelé par convention l'ensemble vide et est noté $\emptyset$.*

Parfois certains ensembles peuvent être définis à l'aide des propositions.

Exemple 2.1.1 *1.* $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}^*$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{C}^*$ *sont des ensembles.*

2. $\emptyset = \{x \ : \ x \neq x\}$.

3. Si $P(x)$ est une proposition $E = \{x \ : \ x$ vérifie $P(x)\}$

4. $\mathbb{R}_+ = \{x \in \mathbb{R} \ / \ x \geq 0\}$.

2.1.2 Partie d'un ensemble

Définition 2.1.2 *Soient E et F deux ensembles. On dit que E est inclus dans F si tout élément de E est aussi un élément de F.*

Remarque 2.1.2 *E inclus dans F signifie : $\forall x, (x \in E \Longrightarrow x \in F)$.*

Notation 2.1.2 *Si E est inclus dans F on écrit $E \subset F$ ou encore $F \supset E$.*

Définition 2.1.3 *On dit qu'un ensemble A est une partie de E si A est inclus dans E ou encore A est un sous-ensemble de E.*

Exemple 2.1.2 *1. On a* $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

2. $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ *sont des sous-ensembles de* $\mathbb{C}$.

Remarque 2.1.3 *Soient* E *et* F *deux ensembles on dit que* $(E = F)$ *ssi* $(E \subset F)$ *et* $(F \subset E)$.

Définition 2.1.4 *On appelle l'ensemble des parties de* E*, l'ensemble noté* $\mathcal{P}(E)$ *dont les éléments sont les sous-ensembles de* E.

Remarque 2.1.4 *Si* E *est un ensemble à* n *éléments alors* $\mathcal{P}(E)$ *admet* 2^n *éléments.*

Exemple 2.1.3 *1.* $\emptyset$ *est une partie de* E*,* E *est aussi une partie de* E*.* $\emptyset$ *et* E *sont appelés les parties triviales de* E.

2. Si $E = \{a, b, c\}$. $\mathcal{P}(E) = \{\emptyset, E, \{a\}\ ;\ \{b\}\ ;\ \{c\}\ ;\ \{a, b\}; \{a, c\}\{b, c\}\}$.

2.1.3 Opérations sur les ensembles

Soient E et F deux ensembles et A, B, C des parties de E.

2.1.3.1 Intersection

Définition 2.1.5 *On appelle intersection de* E *et* F *et l'on note* $E \cap F$ *; l'ensemble des éléments* x *tels que* $x \in E$ *et* $x \in F$. $E \cap F = \{x : x \in E \ \ et \ \ x \in F\}$

Remarque 2.1.5 *1. Si* $E \cap F = \emptyset$*, on dit que* E *et* F *sont disjoints.*

2. $E \cap F \subset E$ *et* $E \cap F \subset F$.

2.1.3.1 Réunion

Définition 2.1.6 *On appelle réunion de* E *et* F *et l'on note* $E \cup F$ *; l'ensemble des éléments* x *tels que* $x \in E$ *ou* $x \in F$*. On a donc* $E \cup F = \{x : x \in E \ \ ou \ \ x \in F\}$

Remarque 2.1.6 *1.* $E \cup \emptyset = E$

2. $E \cup F = \emptyset \Longrightarrow E = \emptyset$ *et* $F = \emptyset$

3. *Si* $E \subset F$, *alors* $E \cup F = F$

4. $E \subset E \cup F$ *et* $F \subset E \cup F$.

2.1.3.1 Complémentaire d'un ensemble

Définition 2.1.7 *On appelle complémentaire de* A *dans* E, *l'ensemble des éléments de* E *qui n'appartiennent pas à* A.

Notation 2.1.3 $\mathcal{C}_E A$ *ou* $E - A$ *ou* $\bar{A} = \{x \in E : x \notin A\}$.

Remarque 2.1.7 *Soit* $A \subset E$.

1. $\mathcal{C}_E A \subset E$
2. $\mathcal{C}_E(\mathcal{C}_E\ A) = A$
3. $\mathcal{C}_E E = \emptyset$ *et* $C_E\emptyset = E$
4. $\mathcal{C}_E A \cap A = \emptyset$ *et* $\mathcal{C}_E A \cup A = E$

Propriété 2.1.1

1. *Commutativité*
   (a) *L'intersection est commutative :*
   $$A \cap B = B \cap A \quad \forall A, B \in \mathcal{P}(E).$$
   (b) *La réunion est commutative*
   $$A \cup B = B \cup A \quad \forall A, B \in \mathcal{P}(E).$$
2. *Associativité*
   (a) *L'intersection est associative*
   $$(A \cap B) \cap C = A \cap (B \cap C) \ \ \forall A, B, C \in \mathcal{P}(E).$$
   (b) *La réunion est associative*
   $$(A \cup B) \cup C = A \cup (B \cup C) \ \ \forall A, B, C \in \mathcal{P}(E).$$

3. Distributivité

(a) L'intersection est distributive par rapport à la réunion

$$\left.\begin{array}{l} A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \\ (B \cup C) \cap A = (B \cap A) \cup (C \cap A) \end{array}\right\} \forall A, B, C \in \mathcal{P}(E)$$

(b) La réunion est distributive par rapport à l'intersection

$$\left.\begin{array}{l} A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \\ (B \cap C) \cup A = (B \cup A) \cap (C \cup A) \end{array}\right\} \forall (A, B, C) \in (\mathcal{P}(E))^3$$

4. Idempotence : $\forall A \in \mathcal{P}(E)$ *: on a* $A \cap A = A$ *et* $A \cup A = A$.

Preuve :

• Montrons que $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

$$\begin{array}{rcl} x \in A \cap (B \cup C) & \Leftrightarrow & (x \in A) \wedge (x \in B \cup C) \\ & \Leftrightarrow & (x \in A) \wedge [(x \in B) \vee (x \in C)] \\ & \Leftrightarrow & [(x \in A) \wedge (x \in B)] \vee [(x \in A) \wedge (x \in C)] \\ & \Leftrightarrow & [x \in (A \cap B)] \vee [x \in (A \cap C)] \\ & \Leftrightarrow & x \in (A \cap B) \cup (A \cap C) \end{array}$$

Par conséquent $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

On peut ainsi de la même façon traiter les autres points pour achever la preuve.

Théorème 2.1.1 *Soient* $A, B \in \mathcal{P}(E)$

1. $\mathcal{C}_E(A \cap B) = (\mathcal{C}_E A) \cup (\mathcal{C}_E B)$
2. $\mathcal{C}_E(A \cup B) = (\mathcal{C}_E A) \cap (\mathcal{C}_E B)$.

Preuve :

• Montrons que $\mathcal{C}_E(A \cap B) = (\mathcal{C}_E A) \cup (\mathcal{C}_E B)$

$$\begin{aligned} x \in \mathcal{C}_E(A \cap B) &\Leftrightarrow x \notin (A \cap B) \\ &\Leftrightarrow \rceil(x \in A \cap B) \\ &\Leftrightarrow \rceil[(x \in A) \wedge (x \in B)] \\ &\Leftrightarrow \rceil(x \in A) \vee \rceil(x \in B) \\ &\Leftrightarrow (x \in \mathcal{C}_E A) \vee (x \in \mathcal{C}_E B) \\ &\Leftrightarrow x \in (\mathcal{C}_E A) \cup (\mathcal{C}_E B) \end{aligned}$$

Par conséquent $\mathcal{C}_E(A \cap B) = (\mathcal{C}_E A) \cup (\mathcal{C}_E B)$.

• Montrons que $\mathcal{C}_E(A \cup B) = (\mathcal{C}_E A) \cap (\mathcal{C}_E B)$.

$$\begin{aligned} x \in \mathcal{C}_E(A \cup B) &\Leftrightarrow x \notin (A \cup B) \\ &\Leftrightarrow \rceil(x \in A \cup B) \\ &\Leftrightarrow \rceil[(x \in A) \vee (x \in B)] \\ &\Leftrightarrow \rceil(x \in A) \wedge \rceil(x \in B) \\ &\Leftrightarrow (x \in \mathcal{C}_E A) \wedge (x \in \mathcal{C}_E B) \\ &\Leftrightarrow x \in (\mathcal{C}_E A) \cap (\mathcal{C}_E B) \end{aligned}$$

Par conséquent $\mathcal{C}_E(A \cup B) = (\mathcal{C}_E A) \cap (\mathcal{C}_E B)$.

Définition 2.1.8 *Produit d'ensembles*
On appelle produit cartésien des ensembles E et F, l'ensemble des éléments (x, y) tels que $x \in E$ et $y \in F$.

Notation 2.1.4 $E \times F = \{(x, y) : x \in E \text{ et } y \in F\}$.

Remarque 2.1.8

1. *$E \times F \neq F \times E$ si $E \neq F$.*
2. *Si E a n éléments et F a m éléments alors $E \times F$ et $F \times E$ ont $n \times m$ éléments.*

Exemple 2.1.4 *Soient* $E = \{\alpha, \beta\}$ *et* $F = \{1, 2, 2\}$. *Alors on a*

$E \times F = \{(x, y) : x \in E \text{ et } y \in F\} = \{(\alpha, 1)\ ;\ (\alpha, 2)\ ;\ (\alpha, 3)\ ;\ (\beta, 1)\ ;\ (\beta, 2)\ ;\ (\beta, 3)\}$

Propriété 2.1.2 *1. Si* $A \subset E$ *et* $B \subset F$ *alors* $A \times B \subset E \times F$.

2. $E \times F = \emptyset \Longleftrightarrow E = \emptyset$ *ou* $F = \emptyset$.

3. Soient E, F *et* G *3 ensembles :*

(i) $E \times (F \cap G) = (E \times F) \cap (E \times G)$

(ii) $E \times (F \cup G) = (E \times F) \cup (E \times G)$.

Remarque 2.1.9 *1. Lorsque* $E = F$, $E \times E$ *se note* E^2 *et on appelle diagonale de* E^2 *l'ensemble des couples* (x, x) *avec* $x \in E$.

2. Plus généralement, le produit cartésien de n ensembles $E_1, E_2, ..., E_n$ *est l'ensemble* $E_1 \times E_2 \times \ldots \times E_n$ *encore noté* $\prod_{i=1}^{n} E_i$

$E_1 \times E_2 \times \ldots \times E_n = \{(x_1, \ldots x_n) : x_i \in E_i,\ i \leq i \leq n\}$.

On dit que $(x_1, x_2, ..., x_n)$ *est un n-uple. Si* $E_1 = E_2 = \ldots = E_n = E$, *on note* E^n *au lieu de* $E \times E \times E \ldots \times E$.

Par exemple $\mathbb{R} \times \mathbb{R} \times \mathbb{R} = \mathbb{R}^3$ *et* $\underbrace{\mathbb{R} \times \mathbb{R} \times \ldots \times \mathbb{R} = \mathbb{R}}_{n\ fois} = \mathbb{R}^n$.

2.2 Applications

2.2.1 Définitions et exemples

Définition 2.2.1 *Soient* E *et* F *deux ensembles. On appelle graphe de* E *vers* F, *toute partie non vide* G *de* $E \times F$.

Autrement dit tout élément de G *est un couple ordonné* (x, y) *où* $x \in E$ *et* $y \in F$.

Définition 2.2.2 *On appelle application de* E *dans* F, *toute relation* f *qui associe à chaque élément* x *de* E *un et un seul élément* y *de* F.

Notation 2.2.1

$$\begin{array}{rccc} f: & E & \longrightarrow & F \\ & x & \longmapsto & y = f(x) \end{array} \quad ou \quad \begin{array}{ccc} E & \xrightarrow{f} & F \\ x & \longmapsto & y = f(x) \end{array}$$

où E est appelé l'ensemble de départ de f. F est appelé l'ensemble d'arrivée de f. L'élément y est appelé image de l'élément x par f.

Autrement dit *: Une application est un triplet*

$$f = (E, F, G) \quad où \quad G = \{(x, f(x)\ ;\ x \in E\}$$

est appelé le graphe de f.

Remarque 2.2.1 *Soient $f_1 = (E_1, E_1, G_1)$ $f_2 = (E_2, F_2, G_2)$ deux applications. On dit que $f_1 = f_2$ ssi* $\begin{cases} E_1 = E_2 \\ F_1 = F_2 \\ G_1 = G_2 \end{cases}$.

Exemple 2.2.1 *1.* $\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & sin(x) \end{array}$ *est une application.*

2. $\begin{array}{rccc} I_{d_E}: & E & \longrightarrow & E \\ & x & \longmapsto & I_{d_E}(x) = x \end{array}$ *est une application appelée identité.*

3. $\begin{array}{rccc} f: & \mathbb{N} & \longrightarrow & \mathbb{Z} \\ & n & \longmapsto & 2n \end{array}$ *est une application.*

4. Soient E et F deux ensembles les applications :

$$\begin{array}{rccc} \pi_1: & E \times F & \longrightarrow & E \\ & (x, y) & \longmapsto & x \end{array}.$$

$$\begin{array}{rccc} \pi_2: & E \times F & \longrightarrow & F \\ & (x, y) & \longmapsto & y \end{array}$$

s'appellent respectivement la 1^{re} projection et la deuxième projection.

Définition 2.2.3 *Soit f une application de E dans F et A une partie de E. On appelle restriction de f à A, et on note f/A, l'application h de A dans F telle $h(x) = f(x)$ pour tout $x \in A$.*

Remarque 2.2.2 *Si $Card(E) = n$ et $card(F) = p$. Le nombre total d'applications de E dans F est p^n.*

2.2.2 Composition d'applications

Soient E, F et H trois ensembles $f : E \longrightarrow F$ et $g : F \longrightarrow H$ deux applications.

A chaque élément $x \in E$, on associe un élément et un seul élément de H. On obtient ainsi une application de E dans H appelée application composée de g et de f et est notée gof.

$$E \xrightarrow{f} F \xrightarrow{g} H$$

$$gof$$

on a : $(gof)(x) = g(f(x))$.

si $x \in E$, on a : $(gof)(x) = g(f(x))$.

Remarque 2.2.3

1. *La composition d'application n'est pas commutative c'est-à-dire $fog \neq gof$.*

2. *La composition d'applications est associative c'est-à-dire si $f : E_1 \longrightarrow E_2$, $g : E_2 \longrightarrow E_3$ et $h : E_3 \longrightarrow E_4$, alors $(hog)of = ho(gof)$.*

Exemple 2.2.2

$$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & x^2 \end{array}$$

$$\begin{array}{rccc} g: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & |x-1| \end{array}$$

$$(gof)(x) = g(f(x)) = g(x^2) = |x^2 - 1|$$

$$(fog)(x) = f(g(x)) = f(|x-1|) = (x-1)^2.$$

2.2.3 Fonction indicatrice

Soit E un ensemble. Pour tout $A \in \mathcal{P}(E)$, on définit l'application

$$\begin{array}{rccc} \varphi_A: & E & \longrightarrow & \{0,1\} \\ & x & \longmapsto & \varphi_A(x) = \begin{cases} 1, & si\ x \in A \\ 0, & si\ x \notin A \end{cases} \end{array}$$

appelée fonction indicatrice de A ou fonction caractéristique de A.
Une fonction indicatrice caractérise complètement une partie de E dans le sens où si $A, B \in \mathcal{P}(E)$,

$$\varphi_A = \varphi_B \Leftrightarrow A = B$$

On a les relations suivantes :

1. $\varphi_A^2 = \varphi_A$.
2. $\varphi_{\overline{A}} = 1 - \varphi_A$.
3. $\varphi_{A\cap B} = \varphi_A \varphi_B$
4. $\varphi_{A\cup B} = \varphi_A + \varphi_B - \varphi_A \varphi_B$.

2.2.4 Injection - Surjection - Bijection

Soit $f : E \longrightarrow F$ une application.

2.3.4.1 Injection

Définition 2.2.4 *L'application f est dite injective ou que c'est une injection si l'une des propositions équivalentes suivantes est vraie :*

1. $\forall x, x' \in E$, *la relation* $f(x) = f(x') \Rightarrow x = x'$.
2. $\forall x, x' \in E$, $x \neq x' \Rightarrow f(x) \neq f(x')$.
3. *tout élément de* F *admet au plus un antécédent dans* E.

Exemple 2.2.3 *1.*
$$\begin{array}{ccc} \mathbb{R} & \xrightarrow{\varphi} & \mathbb{R} \\ x & \longmapsto & 3x \end{array}$$

2.
$$\begin{array}{ccc} \mathbb{R} & \xrightarrow{\psi} & \mathbb{R}^2 \\ x & \longmapsto & (x, 2x) \end{array}$$

3. Soit E *un ensemble et* $A \subset E$
$$\begin{array}{rccl} j: & A & \longrightarrow & E \\ & x & \longmapsto & j(x) = x \end{array} \quad \text{est une injection appelée injection canonique}$$

Proposition 2.2.1 *Soient* $f : E \to F$ *et* $g : F \to G$ *deux applications.*

1. *Si* f *et* g *sont injectives, alors* $g \circ f$ *est injective.*
2. *Si* $g \circ f$ *est injective, alors* f *est injective.*

Preuve. Exercice

Théorème 2.2.1 *Caractérisation des applications injectives*
Soient E *et* F *deux ensembles non vide et* $f : E \to F$ *une application. Les conditions suivantes sont équivalentes :*

1. f *est injective.*
2. *il existe une application* $r : F \to E$ *tel que* $r \circ f = Id_E$.

L'application r *est appelée rétraction de* f.

Preuve. Exercice

2.3.4.2 Surjection

Définition 2.2.5 *L'application* f *est dite surjective ou que c'est une surjection si l'une des propositions équivalentes suivantes est vraie :*

1. $\forall y \in F, \exists x \in E : y = f(x)$.
2. $Im(f) = F$
3. *tout élément de F admet au moins un antécédent dans E.*

Exemple 2.2.4 *1.*
$$\begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R}^+ \\ x & \longmapsto & x^2 \end{array}$$

2. *Soit E un ensemble et $A \subset E$*
$$\begin{array}{rccc} \pi_1 : & \mathbb{R} \times \mathbb{R} & \longrightarrow & \mathbb{R} \\ & (x, y) & \longmapsto & x \ . \\ \pi_2 : & \mathbb{R} \times \mathbb{R} & \longrightarrow & \mathbb{R} \\ & (x, y) & \longmapsto & y \ . \end{array}$$

Proposition 2.2.2 *Soient $f : E \to F$ et $g : F \to G$ deux applications.*

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

Preuve. Exercice

Théorème 2.2.2 *Caractérisation des applications surjectives*
Soient E et F deux ensembles non vide et $f : E \to F$ une application. Les conditions suivantes sont équivalentes :

1. *f est surjective.*
2. *il existe une application $s : F \to E$ tel que $f \circ s = Id_F$.*

L'application s est appelée section de f.

Preuve. Exercice

2.3.4.3 Bijection

Définition 2.2.6 *L'application f est dite bijective e ou que c'est une bijection si l'une des propositions équivalentes suivantes est vraie :*

1. *f est injective et surjective.*

2. $\forall y \in F, \exists!\ x \in E : y = f(x)$.

3. *tout élément de F possède un unique antécédent dans E.*

Exemple 2.2.5 1. $\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & x^5 \end{array}$ *est une bijection*

2. $\begin{array}{lcl} \mathbb{R}^3 & \longrightarrow & \mathbb{R}^3 \\ (x,y,z) & \longmapsto & (x, x-y, x+y-z) \end{array}$ *est une bijection*

Conséquences.

1. Si f est une injection alors $card(E) \leq card(F)$
2. Si f est une surjection alors $card(E) \geq card(F)$
3. Si f est une bijection alors $card(E) = card(F)$.

Théorème 2.2.3 *Soient E, F deux ensembles finis de même cardinal et $f : E \longrightarrow F$ une application. Alors les conditions suivantes sont équivalentes :*

1. *Si f est injective.*
2. *Si f est surjective.*
3. *Si f est bijective.*

Preuve.

- Il est clair que 3) $\Longrightarrow$ 1).
- Montrons que 1) $\Longrightarrow$ 2).

Supposons $f : E \longrightarrow F$ soit injective.

Si $Z = Imf$; on a $card(E) = card(Z)$. Par conséquent $card(Z) = card(F)$ et comme $Z \subseteq F$, on en conclut que $Z = F$; c'est-à-dire que f est surjective.

- Montrons enfin que 2) implique 3).

Supposons que $f : E \longrightarrow F$ soit surjective. Pour tout $y \in F$, posons $E_y = \{x \in E \ / \ f(x) = y\}$. Comme f est surjective, $E_y \neq \emptyset$ quelque soit $y \in F$, par conséquent $card(E_y) \geq 1$.

D'autre part $E = \bigcup_{y \in F} E_y$ et $E_y \cap E_{y'} = \emptyset$ si $y \neq y'$. On en conclut donc que $card(E) = \sum_{y \in F} card(E_y)$. Mais comme $card(F) = card(E)$ et $card(E_y) \geq 1$, on en déduit que $card(E_y) = 1$ quel que soit $y \in F$. Cela signifie que f est injective donc f est bijective.

Théorème 2.2.4 *(de Cantor - Bernstein)*
Soient E et F deux ensembles. S'il existe une injection de E dans F et une injection de F dans E, alors il existe une bijection de E dans F.

2.2.5 Image directe - Image réciproque

Théorème 2.2.5 *Soient $f : E \longrightarrow F$ une application et A et A' deux parties de E.*

1. *Si $A \subset A'$ alors $f(A) \subset f(A')$.*
2. *$f(A \cup A') = f(A) \cup f(A')$.*
3. *$f(A \cap A') \subset f(A) \cap f(A')$.*
4. *$f(A \cap A') = f(A) \cap f(A') \Longleftrightarrow f$ est injective.*
5. *$f^{-1}[f(A)] = A \Leftrightarrow f$ est surjective.*

Preuve

1. Soit $y \in f(A)$. Donc il existe $x \in A$ tel que $y = f(x)$ or $A \subset A'$ donc $x \in A'$. Ainsi $f(x) \in f(A')$, c'est-à-dire $y \in f(A')$. D'où $f(A) \subset f(A')$.
2. On a $A \subset A \cup A'$ d'après 1) $f(A) \subset f(A \cup A')$n et $A' \subset A \cup A'$ d'après 1) $f(A') \subset f(A \cup A')$. Donc $f(A) \cup f(A') \subset f(A \cup A')$. Soit maintenant $y \in f(A \cup A')$. Il existe ainsi $x \in A \cup A'$ tel que $y = f(x)$. Comme $x \in A \cup A'$, alors on a $x \in A$ ou $x \in A'$. Donc $y = f(x) \in f(A)$ ou $y = f(x) \in f(A')$, c'est-à-dire $y \in f(A) \cup f(A')$. On a alors $f(A \cup A') \subset f(A) \cup f(A')$. Par conséquent $f(A \cup A') = f(A) \cup f(A')$.
3. Soit $y \in f(A \cap A')$. Donc $\exists x \in A \cap A'$ tel que $y = f(x)$. Comme $x \in A \cap A'$, alors on a $x \in A$ et $x \in A'$. Donc $y = f(x) \in f(A)$ et $y = f(x) \in f(A')$, c'est-à-dire $y \in f(A) \cap f(A')$. On a ainsi $f(A \cap A') \subset f(A) \cap f(A')$.
4. laisser au soin de l'étudiant

5. laisser au soin de l'étudiant

Exemple 2.2.6 *Soit la fonction f définie sur $\mathbb{R}$ telle que : $x \longmapsto x^2$. On pose $A = [-2, 0]$ et $A' = [0, 2]$. $A \cap A' = \{0\}$, donc $f(A \cap A') = f(\{0\}) = \{f(x) : x \in \{0\}\} = \{f(0)\} = 0$. Par contre, $f(A) = [0, 4] = f(A')$, alors $f(A) \cap f(A') = [0, 4]$. Notons que dans cet exemple, $f(A \cap A') \neq f(A) \cap f(A')$.*

Théorème 2.2.6 *Soient $f : E \longrightarrow F$ une application et B et B' deux parties de F.*

1. *Si $B \subset B'$ alors $f^{-1}(B) \subset f^{-1}(B')$.*
2. *$f^{-1}(B \cup B') = f^{-1}(B) \cup f^{-1}(B')$.*
3. *$f(B \cap B') = f^{-1}(B) \cap f^{-1}(B')$.*
4. *$f^{-1}(C_F B) = C_E(f^{-1}(B)$.*
5. *$f[f^{-1}(B)] = B \Leftrightarrow f$ est surjective.*

Preuve.

1. Si, $B \subset B'$ alors $f^{-1}(B) \subset f^{-1}(B')$. Soit $x \in f^{-1}(B)$, donc $f(x) \in B$. Or, $B \subset B'$, donc $f(x) \in B'$. D'où, $x \in f^{-1}(B')$, ainsi on obtient $f^{-1}(B) \subset f^{-1}(B')$.
2. Pour $f^{-1}(B \cup B') = f^{-1}(B) \cup f^{-1}(B')$, on a :

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

   Ainsi $f^{-1}(B \cup B') = f^{-1}(B) \cup f^{-1}(B')$.
3. Montrons $f^{-1}(B \cap B') = f^{-1}(B) \cap f^{-1}(B')$.

$$\begin{aligned} x \in f^{-1}(B \cap B') &\Leftrightarrow f(x) \in B \cap B' \\ &\Leftrightarrow f(x) \in B \text{ et } f(x) \in B' \\ &\Leftrightarrow x \in f^{-1}(B) \text{ et } x \in f^{-1}(B') \\ &\Leftrightarrow x \in f^{-1}(B) \cap f^{-1}(B') \end{aligned}$$

4. Montons que $f^{-1}(C_F B) = C_E(f^{-1}(B)$.

$$\begin{aligned} x \in f^{-1}(C_F B) &\Leftrightarrow f(x) \in C_F B \\ &\Leftrightarrow x \notin f^{-1}(B) \\ &\Leftrightarrow x \in C_E(f^{-1}(B) \end{aligned}$$

   Par conséquent $f^{-1}(C_F B) = C_E(f^{-1}(B)$.

5. laisser au soin de l'étudiant

2.3 Notion de familles

2.3.1 Familles d'éléments d'un ensemble

Définition 2.3.1 *Soient I et E deux ensembles non vides. Une famille d'éléments de E indexée par I est une application*

$$\begin{aligned} f: \ I &\longrightarrow E \\ i \quad &\mapsto f(i) = x_i \end{aligned}$$

On note $(x_i)_{i\in I}$.

Exemple 2.3.1 *1. Une suite numériques est une famille d'éléments de $\mathbb{R}$*

$$\begin{aligned} (x_n)_{n\in\mathbb{N}} := \quad f: \ \mathbb{N} &\longrightarrow \mathbb{R} \\ n \quad &\mapsto f(n) = x_n \end{aligned}$$

2. Une suite complexe est une famille d'éléments de $\mathbb{C}$

$$\begin{aligned} (z_n)_{n\in\mathbb{N}} := \quad f: \ \mathbb{N} &\longrightarrow \mathbb{C} \\ n \quad &\mapsto f(n) = z_n \end{aligned}$$

Remarque 2.3.1 *Soient $(x_i)_{i\in I}$ une famille d'éléments de E indexée par I et $J \subset I$. La famille $(x_i)_{i\in J}$ est une sous famille de la famille $(x_i)_{i\in I}$.*

2.3.2 Famille d'ensembles

Définition 2.3.2 *Soit I un ensemble non vide. On appelle famille d'ensembles indexée par I, la donnée pour chaque $i \in I$, d'un ensemble E_i. On note $(E_i)_{i\in I}$.*

Définition 2.3.3 *Soient E un ensemble et I un ensemble non vide. On appelle famille de parties de E indexée par I, toute application*

$$\begin{aligned} \varphi : \ I &\longrightarrow \mathcal{P}(E) \\ i &\longmapsto \varphi(i) = E_i \end{aligned}$$

Exemple 2.3.2 *1. Soient $I = \{1, 2\}$ et E un ensemble*

$$\begin{aligned} f : \ I &\longrightarrow \mathcal{P}(E) \\ 1 &\longmapsto f(1) = E_1 \\ 2 &\longmapsto f(2) = E_2 \end{aligned}$$

On a $(E_i)_{i\in I} = \{E_1, E_2\}$.

2. Soient $I = \{1, 2, ..., p\}$ et E un ensemble. Alors on a $(E_i)_{i\in I} = \{E_1, E_2, ..., E_p\}$.

Remarque 2.3.2 *Soient I un ensemble non vide et $(E_i)_{i\in I}$ une famille d'ensemble indexée par I.*

1. ***Réunion.***
   Il existe un unique ensemble G tel que
   $$x \in G \Leftrightarrow \exists k \in I : x \in E_k$$
   G est appelé réunion des E_i et on note $G = \cup_{i\in I} E_i$.
2. ***Intersection.***
   Il existe un unique ensemble H tel que
   $$x \in H \Leftrightarrow x \in E_k, \forall k \in I$$
   H est appelé intersection des E_i et on note $H = \cap_{i\in I} E_i$.

Propriété 2.3.1 *Soient E un ensemble et I, J deux ensembles non vides. Pour tous $(A_i)_{i\in I}$ une famille de E indexée par I et $(B_i)_{i\in I}$ une famille de E indexée par J, on a les assertions suivantes ;*

1. $\overline{\cup_{i\in I} A_i} = \cap_{i\in I}\overline{A_i}$ *et* $\overline{\cap_{i\in I} A_i} = \cup_{i\in I}\overline{A_i}$
2. $\left(\cup_{i\in I}\ A_i\right) \cap \left(\cup_{i\in I}\ B_i\right) = \cup(A_i \cap_{(i,j)\in I\times J} B_j)$
3. $\left(\cap_{i\in I}\ A_i\right) \cup \left(\cap_{i\in I}\ B_i\right) = \cap(A_i \cup_{(i,j)\in I\times J} B_j)$

Définition 2.3.4 *Soient F une partie d'un ensemble E et $(E_i)_{i\in I}$ une famille de parties de E indexée par I. On dit que la famille $(E_i)_{i\in I}$ est un recourement de F si et seulement si $F \subset \cup_{i\in I} E_i$.*
On dit que la famille $(E_i)_{i\in I}$ est un recourement si et seulement si $E = \cup_{i\in I} E_i$

Définition 2.3.5 *Soit $(E_i)_{i\in I}$ une famille de parties de E indexée par I. On dit que $(E_i)_{i\in I}$ est une partition de E si :*

1. $E = \cup_{i\in I} E_i$.
2. $E_i \cap E_j = \emptyset$, *si* $i \neq j$.

2.4 Relations binaires

2.4.1 Définitions et exemples

Définition 2.4.1 *Soit E un ensemble. On appelle relation binaire sur E, tout couple $\mathcal{R} = (E, \Gamma)$, où Γ est une partie de $E \times E$, appelée graphe de Γ. Si $(x, y) \in \Gamma$, on dit que x est en relation avec y et on note $x\mathcal{R}y$.*

Exemple 2.4.1
1. *Dans E, la relation d'égalité est une relation binaire.*
2. *Dans $\mathbb{R}$, la relation " $\leq$ " est une relation binaire.*
3. *Dans $\mathcal{P}(E)$ où E est un ensemble, la relation d'inclusion est une relation binaire sur $\mathcal{P}(E)$.*
4. *Dans $\mathbb{N}^*$, la relation de divisibilité est une relation binaire.*

Définition 2.4.2 *Soit $\mathcal{R}$ une relation binaire sur E.*

1. *On dit que $\mathcal{R}$ est réflexive, si $\forall x \in E, x\mathcal{R}x$.*
2. *On dit que $\mathcal{R}$ est symétrique si $\forall x, y \in E, \big(x\mathcal{R}y \Rightarrow y\mathcal{R}x\big)$.*
3. *On dit que $\mathcal{R}$ est anti-symétrique si, $\forall x, y \in E, \big(x\mathcal{R}y$ et $y\mathcal{R}x \Rightarrow x = y\big)$.*
4. *On dit que $\Re$ est transitive si :*

$$\forall x, y, z \in E, \left.\begin{array}{c} x\mathcal{R}y \\ y\mathcal{R}z \end{array}\right\} \Rightarrow x\mathcal{R}z$$

2.4.2 Relation d'équivalence

Définition 2.4.3 *Soit $\mathcal{R}$ une relation binaire sur E. On dit que $\mathcal{R}$ est une relation d'équivalence sur E, si $\mathcal{R}$ est à la fois réflexive, symétrique et transitive.*

Exemple 2.4.2
1. *La relation d'égalité est une relation d'équivalence sur E.*
2. *Soit p un entier positif. Dans $\mathbb{Z}$, on définit la relation $\mathcal{R}$ par $x\mathcal{R}y \Longleftrightarrow \exists k \in \mathbb{Z} : x - y = kp$. $\mathcal{R}$ est une relation d'équivalence sur $\mathbb{Z}$.*
3. *Soit $f : E \longrightarrow F$ une application. On définit sur E la relation binaire par $x\mathcal{R}y \Longleftrightarrow f(x) = f(y)$. $\mathcal{R}$ est une relation d'équivalence sur E, appelée relation d'équivalence associée à f.*
4. *Dans $\mathcal{R}$, on définit : $x\mathcal{R}y \Longleftrightarrow \sin x = \sin y$. $\mathcal{R}$ est une relation d'équivalence.*

Définition 2.4.4 *Soit $\mathcal{R}$ une relation d'équivalence sur E. On appelle classe d'équivalence modulo $\mathcal{R}$ d'un élément a de E, l'ensemble des éléments x de E qui sont en relation avec a. On la note $\bar{a}$ ou $\mathcal{C}(a)$ ou $\dot{a}$.*

$$\dot{a} = \bar{a} = \mathcal{C}(a) = \{x \in E / x\mathcal{R}a\}$$

.

Définition 2.4.5 *L'ensemble des classes d'équivalence modulo $\mathcal{R}$ s'appelle l'ensemble quotient de E par $\mathcal{R}$. On le note $E/\mathcal{R} = \{\dot{x} : x \in E\}$.*

Exemple 2.4.3 *1. Soit* $E = \{-10, -5, -3, -2, -1, 0, 1, 2, 3, 10, 19\}$. *On définit la relation* $x\mathcal{R}y \Longleftrightarrow |x| = |y|$. $\mathcal{R}$ *est une relation d'équivalence sur* E.

(a) $\dot{0} = \{x \in E : |x| = 0\} = \{0\}$.

(b) $\dot{1} = \{x \in E : |x| = 1\} = \{-1, 1\}$.

(c) $\dot{2} = \{x \in E : |x| = 2\} = \{-2, 2\}$

(d) $\dot{3} = \{x \in E : |x| = 3\} = \{-3, 3\}$.

(e) $\dot{10} = \{x \in E : |x| = 10\} = \{-10, 10\}$.

(f) $-\dot{5} = \{x \in E : |x| = 5\} = \{-5\}$.

(g) $\dot{19} = \{x \in E : |x| = 19\} = \{19\}$.

(h) $E/\mathcal{R} = \{\dot{x} : x \in E\} = \{\{-5\}, \{19\}, \{-10, 10\}, \{-3, 3\}, \{-2, 2\}, \{-1, 1\}\}$.

2. Dans $\mathbb{Z}$, *on définit la relation* $x\mathcal{R}y \Longleftrightarrow x - y \in 2\mathbb{Z}$. *Soit* $a \in \mathbb{Z}$.

$$\begin{aligned} \dot{a} &= \{x \in \mathbb{Z} : x\mathcal{R}a\} && (2.1)\\ &= \{x \in \mathbb{Z} : x - a \in 2\mathbb{Z}\} && (2.2)\\ &= \{x \in \mathbb{Z} : \exists k \in \mathbb{Z}, x - a = 2k\} && (2.3)\\ &= \{x \in \mathbb{Z} : \exists k \in \mathbb{Z}, x = 2k + a\} && (2.4) \end{aligned}$$

D'où $\dot{a} = \{x \in \mathbb{Z} : \exists k \in \mathbb{Z}, x = 2k + a\}$. *Donc, dans la classe d'un élément a, a n'est que la classe du reste de la division euclidienne par 2. 0, 1 étant les restes de la division par 2, on a deux classes :* $\dot{0} = \{x \in \mathbb{Z} : x\mathcal{R}0\} = \{x \in \mathbb{Z} : \exists k \in \mathbb{Z}, x = 2k\}$. *Donc la classe de 0 est l'ensemble des entiers pairs.* $\dot{1} = \{x \in \mathbb{Z} : \exists k \in \mathbb{Z}, x = 2k + 1\}$, *la classe de 1 est l'ensemble des entiers impairs.*

Propriété 2.4.1 *Soit* $\mathcal{R}$ *une relation d'équivalence sur* E.

1. $\forall x \in E, x \in \dot{x}$.
2. $\forall x, y \in E, (x\mathcal{R}y \Longleftrightarrow \dot{x} = \dot{y})$.
3. $\forall (x, y) \in E^2, (x \not\mathcal{R}y \Rightarrow \dot{x} \cap \dot{y} = \emptyset)$.
4. *Les classes d'équivalence modulo* $\mathcal{R}$ *de* E *réalisent une partition de* E : $E = \bigcup_{x \in E} \dot{x}$.

Théorème 2.4.1 (Décomposition canonique d'applications) *Soient E, F deux ensembles, f une application. Alors les assertions suivantes sont vérifiées :*

1. *La relation binaire $\mathcal{R}$ définie sur E par $x\mathcal{R}y \Longleftrightarrow f(x) = f(y)$ est une relation d'équivalence sur E, dite relation d'équivalence associée à f.*
2. *Soit $\pi : E \longrightarrow E/\mathcal{R}$ la surjection canonique $x \longmapsto \pi(x) = \dot{x}$ et $j : Im(f) \longrightarrow F \quad x \longmapsto j(x) = x$ est l'injection canonique. Il existe une bijection unique $\bar{f} : E/\mathcal{R} \longrightarrow Im(f)$ telle que $f = j \circ \bar{f} \circ \pi$. On a le diagramme suivant :*

$$\begin{array}{ccc} E & \xrightarrow{f} & F \\ \pi \downarrow & & \uparrow j \\ E/\mathcal{R} & \xrightarrow{\bar{f}} & Im(f) \end{array}$$

Preuve.

1. Homework
2. Montrons que $\bar{f}$ est une application. En effet, soit $\bar{x}, \bar{x}' \notin E/\mathcal{R}$ tel que $\dot{x} = \dot{x}'$

$$\begin{array}{rcl} \dot{x} = \dot{x}' & \Rightarrow & x\mathcal{R}x' \\ & \Rightarrow & f(x) = f(x') \\ & \Rightarrow & \bar{f}(\dot{x}) = \bar{f}(\dot{x}') \end{array}$$

   Donc f est une application. Ainsi, $\bar{f}(\dot{x}) = \bar{f}(\dot{x}') \Rightarrow x\mathcal{R}x' \Rightarrow \dot{x} = \dot{x}'$. Donc $\bar{f}$ est injective. Par ailleurs, soit $y \in Im(f)$. On a $y \in f(E)$. Donc $\exists x \in E : y = f(x) = \bar{f}(\dot{x})$. $\bar{f}$ est donc surjective. D'où le résultat : $\bar{f}$ est une bijection.

3. Montrons $f = j \circ \bar{f} \circ \pi$. Soit $x \in E$,

$$\begin{array}{rcl} (j \circ \bar{f} \circ \pi)(x) & = & (j \circ \bar{f})(\pi(x)) \\ & = & \big(j \circ \bar{f}\big)(\dot{x}) \\ & = & j[\bar{f}(\dot{x})] \\ & = & j(f(x)) \\ & = & f(x) \end{array}$$

   D'où $j \circ \bar{f} \circ \pi = f$, ce qui finit la démonstration.

2.4.3 Relation d'ordre

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

Définition 2.4.6 *On dit que $\mathcal{R}$ est une relation d'ordre sur E, si $\mathcal{R}$ est à la fois réflexive , antisymétrique et transitive.*

Remarque 2.4.1 *Soit $\mathcal{R}$ une relation d'ordr sur E.*

1. *$\mathcal{R}$ est dite relation d'ordre total si $\forall x, y \in E$, $\big(x\mathcal{R}y$ ou $y\mathcal{R}x\big)$.*
2. *$\mathcal{R}$ est dite relation d'ordre partiel s'il existe au moins $(x, y) \in E^2$, tel que $x \not\mathcal{R}y$ et $y\mathcal{R}x$.*
3. *Le couple $(E, \mathcal{R})$ est appelé ensemble ordonné.*

Exemple 2.4.4

1. *Dans $\mathbb{R}$, la relation " $\leq$ " est une relation d'ordre total.*
2. *Dans $\mathbb{N}^*$, la relation binaire suivante : $x\mathcal{R}y \Longleftrightarrow x$ divise y est une relation d'ordre partiel.*
3. *Soit X un ensemble. Sur $\mathcal{P}(X)$, la relation binaire suivante : $A\mathcal{R}B \Longleftrightarrow A \subset B$ est une relation d'ordre partiel.*

Définition 2.4.7 *Soient $(E, \leq)$ un ensemble ordonné, $a \in E$ et $A \subset E$.*

1. *On dit que a est un majorant de A si $x \leq a$ pour tout $x \in A$. Si de plus $a \in A$, il est dit le plus grand élément de A. L'ensemble A est dit majoré s'il admet un majorant, il est dit minoré s'il admet un minorant c'est-à-dire un élément $b \in E$, vérifiant $b \leq x$, pour tout $x \in A$.*
   L'ensemble A est dit borné s'il est à la fois majoré et minoré.
2. *Un élément a est dit :*
   (a) maximal de E si $a \leq x$, $x \in E \Rightarrow x = a$.
   (b) minimal de E si $x \leq a$, $x \in E \Rightarrow x = a$.

Exemple 2.4.5

1. *Le sous ensemble $A = \{x \in \mathbb{Q} : 0 \leq x^2 < 1\}$ de $\mathbb{R}$ est borné mais admet pas de plus grand élément.*

2. *Un plus grand élément, s'il existe, d'un ensemble ordonné est maximal.*
3. *Soit F un ensemble. Alors l'ensemble ordonné $(\mathcal{P}(F), \subset)$ admet un élément maximal F.*
4. *Les nombres premiers constituent des éléments maximaux pour l'ensemble ordonné $\mathbb{N}^*$ muni de la relation de divisibilité.*

2.5 Ensembles dénombrables

Définition 2.5.1 *1. Deux ensembles E et F sont dit équipotents s'il existe une bijection de E sur F.*

2. Un ensemble est dit dénombrable s'il est équipotent à $\mathbb{N}$.

Proposition 2.5.1 *Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.*

Preuve. Soit A une partie non vide de $\mathbb{N}$. Il est clair que A est minoré par 0. Si A n'admet pas de plus petit élément, alors pour tout $a \in A$, il existe $a' \in A$ tel que $a' < a$. Soit $a_0 \in A$, il existe alors $a_1 \in A$ tel que $a_1 < a_0$. On peut trouver également $a_2 \in A$ vérifiant $a_2 < a_1$. On construit ainsi une suite $(a_n)_{n\in\mathbb{N}}$ strictement décroissante de nombres entiers naturels inférieurs à a_0. Ce qui est absurde car $\{0, 1, ..., a_0\}$ est fini. Par conséquent A possède un plus petit élément que l'on note $inf(A)$.

Proposition 2.5.2 *Toute partie d'un ensemble fini ou dénombrable est finie ou dénombrable.*

Preuve. Il suffit de démontrer que toute partie infinie d'un ensemble dénombrable est dénombrable. De façon équivalente, on peut simplement prouver que toute partie infinie de $\mathbb{N}$ est équipotente à $\mathbb{N}$. Soit A une telle partie, on pose $a_0 = inf(A)$ et pour $n \geq 1$: $a_n = inf\big(A\backslash\{a_0, ..., a_{n-1}\}\big)$. Il est clair que tous les éléments de A sont indexés et on définit une bijection

$$\begin{aligned} \Psi : \ \mathbb{N} &\longrightarrow A \\ n &\longmapsto a_n \end{aligned}$$

Proposition 2.5.3 *Soient E et F deux ensembles et $f : E \to F$ une application surjective. Si E est fini ou dénombrable, alors F est fini ou dénombrable.*

Preuve. Soit $y \in F$, il existe $x \in E$ tel que $y = f(x)$. Pour chaque $y \in F$, on fixe un unique $x_y \in E$ tel que $f(x_y) = y$, ce qui définit une application injective

$$\begin{array}{rccc} g: & F & \longrightarrow & E \\ & y & \longmapsto & g(y) = x_y \end{array}$$

En effet, $g(y) = g(y') = x_y \Rightarrow y = f(x_y) = y'$. Ainsi F et $g(F)$ sont équipotent. Comme E est fini ou dénombrable, alors $g(F) \subset E$ est fini ou dénombrable. Par conséquent F est fini ou dénombrable.

Corollaire 2.5.1 *Un ensemble E est fini ou dénombrable si et seulement si il existe une surjection de $\mathbb{N}$ sur E c'est-à-dire si l'on peut ranger les éléments de E en une suite indexée par $\mathbb{N}$.*

Preuve.

Condition nécessaire

1. Si E est fini à n_0 éléments $a_1, a_2, ..., a_{n_0}$. On définit une application surjective

$$\begin{array}{rccc} \varphi: & \mathbb{N} & \longrightarrow & E \\ & n & \longmapsto \varphi(n) = \begin{cases} a_{n+1}, & si\ n \in \{0, ..., n_0 - 1\} \\ a_{n_0}, & si\ n \geq n_0 \end{cases} \end{array}$$

2. Si E est infini, il existe une bijection de $\mathbb{N}$ sur E, donc une surjection.

Condition suffisante

Réciproquement, s'il existe une surjection $\varphi : \mathbb{N} \to E$, alors E est fini ou dénombrable. En outre $E = \varphi(\mathbb{N}) = \{\varphi(n) : n \in \mathbb{N}\} = \big(\varphi(n)\big)_{n\in\mathbb{N}}$.

Beaucoup de résultats importants de la théorie des ensembles dépendent de l'axiome du choix.

Axiome du choix.

Soit $(A_i)_{i\in I}$ une famille de sous-ensembles non vides d'un ensemble E telle que $A_i \cap A_j = \emptyset$, si $i \neq j$. Alors il existe un sous-ensemble A de E, tel que $A \cap A_i = \{a_i\}$, $\forall i \in I$.
Cet axiome du choix n'est pas évident si I n'est pas dénombrable et il est équivalent au lemme de Zorn.

Lemme 2.5.1 *(de Zorn)*
Soit $(E, \leq)$ un ensemble ordonné tel que tout sous-ensemble totalement ordonné admet un majorant. Alors E possède au moins un élément maximal.

Chapitre 3

Structures algébriques : Groupes -Anneaux - Corps

Sommaire

3.1 Généralités

3.1.1 Lois de compositions internes

Définition 3.1.1 *Soit E un ensemble. On appelle loi de composition interne sur E, toute application de $E \times E$ dans E.*

Notation 3.1.1

$$\begin{aligned} \bullet : \quad E \times E &\longrightarrow E \\ (x, y) &\longmapsto x \bullet y \end{aligned}$$

$$\begin{aligned} \star : \quad E \times E &\longrightarrow E \\ (x, y) &\longmapsto x \star y \end{aligned}$$

$$\begin{aligned} \perp : \quad E \times E &\longrightarrow E \\ (x, y) &\longmapsto x \perp y \end{aligned}$$

Remarque 3.1.1 *$x * y$ est le composé de x et y pour la loi $*$.*

Exemple 3.1.1 *1. Dans $\mathbb{N}$, le pgcd et le ppcm sont des lois de composition internes. En effet,*

$$\begin{aligned} pgcd : \quad \mathbb{N} \times \mathbb{N} &\longrightarrow \mathbb{N} \\ (m, n) &\longmapsto pgcd(m, n) \end{aligned}$$

est une application.

De même que,

$$\begin{aligned} ppcm : \quad \mathbb{N} \times \mathbb{N} &\longrightarrow \mathbb{N} \\ (m, n) &\longmapsto ppcm(m, n) \end{aligned}$$

2. *Dans $\mathbb{Z}$, l'addition et la multiplication sont des lois de composition internes, car*

$$\begin{aligned} + : \quad \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z} \\ (m, n) &\longmapsto m + n \end{aligned}$$

est une application.

$$\begin{aligned} \times : \quad \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z} \\ (m, n) &\longmapsto m \times n \end{aligned}$$

est une application.

3. *Dans $\mathbb{R}$, on définit $a * b = \sqrt[5]{a^5 + b^5}$. $*$ est une loi de composition interne sur $\mathbb{R}$.*

4. *Soit X un ensemble quelconque. L'intersection et la réunion sont des lois de composition internes sur $\mathcal{P}(X)$. Car, on a les applications suivantes :*

$$\begin{aligned} \cup : \quad \mathcal{P} \times \mathcal{P} &\longrightarrow \mathcal{P} \\ (A, B) &\longmapsto A \cup B \end{aligned}$$

$$\begin{aligned} \cap : \quad \mathcal{P} \times \mathcal{P} &\longrightarrow \mathcal{P} \\ (A, B) &\longmapsto A \cap B \end{aligned}$$

5. *Soit X un ensemble. On pose : $E = \mathcal{F}(X, X)$, l'ensemble des applications de X dans X. La composition des applications est une loi de composition interne sur E. Car*

$$\begin{aligned} \circ : \quad E \times E &\longrightarrow E \\ (f, g) &\longmapsto g \circ f \end{aligned}$$

est une application.

3.1.2 Propriétés des lois de composition internes

Soient E un ensemble muni d'une loi de composition interne notée $\star$.

3.1.2.1 Associativité

La loi $*$ est associative si et seulement si $(x \star y) \star z = x \star (y \star z), \forall (x, y, z) \in E^2$.

Exemple 3.1.2 *Dans $\mathbb{R}$ l'addition et la multiplication sont associatives.*

3.1.2.2 Commutativité

La loi $*$ est commutative si et seulement si $x \star y = y \star x, \forall (x, y) \in E^2$.

Exemple 3.1.3 *Dans $\mathbb{R}$ l'addition et la multiplication sont commutatives.*

3.1.2.3 Elément neutre

On dit que e est élément neutre de E pour la loi $\star$ si et seulement si $\forall x \in E, e \star x = x \star e = x$.

Si $e \star x = x$, on dit que e est un élément neutre à gauche.

Si $x \star e = x$, on dit que e est un élément neutre à droite.

Exemple 3.1.4 *Dans $\mathcal{P}(X)$, on a $\emptyset \cup A = A \cup \emptyset = A$. $\emptyset$ est l'élément neutre de $\mathcal{P}(X)$ pour la loi $\cup$. De même, $X \cap A = A \cap X = A$. Ainsi X est l'élément de neutre de $\mathcal{P}(X)$ pour la loi $\cap$.*

3.1.2.4 Elément symétrique

Soit e l'élément neutre de E pour la loi $\star$. Soit $x \in E$. On dit que x admet un élémént symétrique pour la loi $\star$ s'il existe $x' \in E$ tel que $x \star x' = x' \star x = e$.

Si $x \star x' = e$, on dit que x' est le symétrique à droite de x.

Si $x' \star x = e$, on dit que x' est le symétrique à gauche de x.

Exemple 3.1.5

1. *Dans $\mathbb{R}$, le symétrique x' de x pour la loi $+$ s'appelle opposé de x, et est noté $-x$. $(x + x' = x' + x = 0 \Rightarrow x' = -x)$.*
2. *Dans $\mathbb{R}^*$, le symétrique de x pour la loi $\times$ s'appelle inverse de x, et est noté $\frac{1}{x}$. $(x \times x' = x' \times x = 1 \Rightarrow x' = \frac{1}{x})$.*

3.1.2.5 Distributivité

Soient $\star$ et $\perp$ deux lois de composition internes sur E. On dit que la loi $\star$ est distributive par rapport à la loi $\perp$, si pour tous $(x, y, z) \in E^3$, on a :

$$x \star (y \perp z) = (x \star y) \perp (x \perp z) \text{ et } (y \perp z) \star x = (y \star x) \perp (z \star x)$$

Exemple 3.1.6 *1. Dans $\mathbb{R}$, la multiplication est distributive par rapport à l'addition. En effet, $x \times (y + z) = (x \times y) + (x \times z)$ et $(y + z) \times x = (y \times x) + (z \times x)$.*

2. Dans $\mathcal{P}(X)$, la réunion est distributive par rapport à l'intersection et vice -versa.

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

3.2 Groupes

3.2.1 Définitions et exemples

Définition 3.2.1 *On appelle groupe tout ensemble G muni d'une loi de composition interne notée $\star$ possédant les propriétés suivantes :*

1. *La loi $*$ est associative ;*
2. *G admet e comme un élément neutre pour la loi $\star$.*
3. *Tout élément de G admet un symétrique pour la loi $\star$.*

Si de plus la loi $\star$ est commutative, on dit que G est commutatif ou abélien

Remarque 3.2.1 *1. Si $+$ est la loi du groupe G, lélément neutre est noté 0. Dans ce cas, l'élément symétrique x' est noté -x, pour tout $x \in G$.*

2. Si $\times$ est la loi de G, alors l'élément neutre est noté 1, et l'élément symétrique d'un élément x, est noté x^{-1}.

3. Si $(G, \cdot)$ est un groupe, on notera le symétrique d'un élément x de G par x^{-1}.

Exemple 3.2.1 *1. $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{Z}/n\mathbb{Z}, +)$ sont des groupes abéliens pour l'addition.*

2. $(\mathbb{Q}^*, \times), (\mathbb{R}^*, \times), (\mathbb{C}^*, \times), (\{-1, 1\}, \times)$ *sont des groupes abéliens.*

3. *Soit E une ensemble quelconque. $(\mathcal{S}(E), \circ)$ est un groupe, non nécessairement commutatif. En particulier, si $E = \{1, 2, ..., n\}$. Dans ce cas, $\mathcal{S}(E)$ se note $\mathcal{S}_n$, soit $(\mathcal{S}_n, \circ)$, et s'appelle le groupe des permutations d'ordre n.*

   $\mathcal{S}_n$ a $n!$ éléments. Pour $n = 3$, $\mathcal{S}_3$ a 6 éléments. $\mathcal{S}_3 = \{Id, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$

$$Id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$
$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$
$$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

   Le lecteur pourra compléter le tableau suivant :

$\overset{\curvearrowright}{\circ}$	Id	σ_1	σ_2	σ_3	σ_4	σ_5
Id	Id	σ_1	σ_2	σ_3	σ_4	σ_5
σ_1						
σ_2						
σ_3						
σ_4						
σ_5						

4. $(\mathbb{R}^n, +)$ *est un groupe abélien.*

3.2.2 Sous-groupes

Définition 3.2.2 *Soit $(G, \star)$ un groupe et H une partie de G. On dit que H est un sous-groupe de G si :*

1. $\forall (x, y) \in H^2, x * y \in H$. *On dit que H est stable par la loi $*$.*
2. $\forall x \in H, x^{-1} \in H$.

Remarque 3.2.2 1. *Une partie H de G est un sous-groupe de G si et seulement si $H \neq \emptyset$ et, $\forall (x, y) \in H^2, x * y^{-1} \in H$.*

2. *Si $(G,\star)$ est un groupe d'élément neutre e ; alors une partie H de G est un sous-groupe si et seulement si $e \in H$ et $\forall (x,y) \in H^2, x * y^{-1} \in H$.*

Exemple 3.2.2 1. *Soit $(G,\star)$ un groupe d'élément neutre e. Alors, $\{e\}$ et G sont des sous-groupes de G.*

2. *$\mathbb{Z}$ et $\mathbb{Q}$ sont des sous-groupes de $(\mathbb{R},+)$.*

3. *$H = \{z \in \mathbb{C}^* / |z| = 1\}$ est un sous-groupe de $(\mathbb{C}^*,\star)$.*
   En effet, on a : $1 \in H, H \neq \emptyset$. Soient $z, z' \in H . z \cdot z'^{-1} \in H$. Car $|z| = 1, |z'| = 1$, $|z \cdot z'^{-1}| = |z| \cdot |z'^{-1}| = |z| \times \frac{1}{|z'|} = 1$.

4. *$U_n = \{z \in \mathbb{C}^* : z^n = 1\}$ est un sous-groupe de $(\mathbb{C}^*,\star)$.*

5. *Les sous-groupes de $(\mathbb{Z},+)$ sont de la forme $n\mathbb{Z}$, $n \in \mathbb{N}$.*

Proposition 3.2.1 *Soit $(G,\star)$ un groupe d'élément neutre e, et soit $(H_i)_{i\in I}$ une famille quelconque de sous-groupe, alors $\bigcap_{i\in I} H_i$ est un sous-groupe de G.*

Preuve. Posons $H = \bigcap_{i\in I} H_i$.
On a $e \in H_i, \forall i \in I$, car H_i est un sous-groupe de G. Comme $e \in H_i, e \in \bigcap_{i\in I} H_i$, donc $e \in H$. Soit $(x,y) \in H^2$, $x \in H \Rightarrow \forall i \in I, x \in H_I$, $y \in H \Rightarrow \forall i \in I, y \in H_I$. Donc, $x * y^{-1} \in H_I, \forall i \in I$. Ainsi, $x * y^{-1} \in H$. D'où le résultat : H est une sous-groupe de G.

Proposition 3.2.2 *Soit $(G,\star)$ un groupe.*

1. *En général, la réunion de deux sous-groupes de G, n'est pas un sous-groupe de G.*

2. *Soient H_1 et H_2 deux sous-groupes de G. Alors $H_1 \cup H_2$ est un sous-groupe de G si et seulement si $H_1 \subset H_2$ ou $H_2 \subset H_1$.*

Preuve.

1. Il suffit de prendre $H_1 = 8\mathbb{Z}$ et $H_2 = 3\mathbb{Z}$, deux sous-groupes de $(\mathbb{Z},+)$. $H_1 \cup H_2 = 8\mathbb{Z} \cup 3\mathbb{Z}$ n'est pas un sous-groupe de $(\mathbb{Z},+)$. En effet, $8 \in 8\mathbb{Z}$ et $3 \in 3\mathbb{Z}$; mais $8 + 3 = 11 \notin 8\mathbb{Z} \cup 3\mathbb{Z}$.

2. Laisser au soin de l'étudiant.

Définition 3.2.3 *Soit A une partie non vide de G, un groupe muni de la loi $\star$. On appelle sous-groupe engendré par A le plus petit sous-groupe de G contenant A. On le note $< A >$.*

Remarque 3.2.3 *1. Si A est un sous-groupe de A, alors $< A >= A$.*

2. A est l'ensemble des produits finis d'éléments de $A \cup A^{-1}$, i.e $< A >= \{x = x_1 \star x_2 \star ... \star x_s : x_i \in A \cup A^{-1}\}$, A^{-1} est l'ensemble des symétriques des éléments de A.

Exemple 3.2.3 *Dans $(\mathbb{Z}, +)$, $< \{1\} >= \mathbb{Z}$, en effet*

$$< \{1\} >= \{m \in \mathbb{Z}/m = \begin{cases} \overbrace{1+1+\cdots+1}^{m \text{ fois}} & si\ m \geq 0 \\ \overbrace{-1-1-\cdots-1}^{|m| \text{ fois}} & si\ m \leq 0 \end{cases} \}$$

Remarque 3.2.4 *Soit $(G, \star)$ un groupe. On pose $A = \{a\}$.*

1. $< A >=< a >= \{a^k/k \in \mathbb{Z}\}$ si la loi est multiplicative.

2. $< A >=< a >= \{ka/k \in \mathbb{Z}\}$ si la loi est additive.

3. Dans le groupe $\mathcal{S}_3$, $< \sigma_1 >= \{\sigma_1^k/k \in \mathbb{Z}\}$.

Proposition 3.2.3 *Soit $(G, \star)$ un groupe et H_1 et H_2 deux sous-groupes de G. Les assertions suivantes sont vérifiées :*

1. $H_1 \star H_1 = H_1$.

2. $H_1 \star H_2$ n'est pas en général un sous-groupe de G.

3. $H_1 \star H_2$ est un sous-groupe de G équivaut à $H_2 \star H_1 = H_1 \star H_2$.

Preuve. (Homework).

3.2.3 Homomorphismes de groupes

Définition 3.2.4 *Soient $(G, \star)$ et $(G', \perp)$ deux groupes. On appelle homomorphisme de G dans G', toute application f de G dans G vérifiant : $f(x \star y) = f(x) \perp f(y), \forall (x, y) \in G^2$. On note :*

$$\begin{array}{rccc} f: & (G, \star) & \longrightarrow & (G', \perp) \\ & x & \longmapsto & f(x) \end{array}$$

Exemple 3.2.4 *1.*

$$\begin{array}{rccc} f: & (\mathbb{C}, +) & \longrightarrow & (\mathbb{C}, \times) \\ & z & \longmapsto & f(z) = e^z \end{array}$$

En effet, $f(z + z') = f(z) \times f(z')$. f est un homomorphisme.

2.

$$\begin{array}{rccc} g: & (\mathbb{R}_+^*, \times) & \longrightarrow & (\mathbb{R}, +) \\ & x & \longmapsto & g(x) = lnx \end{array}$$

est un homomorphisme de groupe car $g(x \times x') = g(x) + g(x')$.

3.

$$\begin{array}{rccc} h: & (\mathcal{S}_n, \circ) & \longrightarrow & (\{-1; 1\}, \times) \\ & \sigma & \longmapsto & (-1)^{i(\sigma)} \end{array}$$

est un homomorphisme ($i(\sigma)$ est le nombre d'inversion de σ). $h(\sigma)$ est la signature de σ .

Définition 3.2.5 *Soient $(G, \star)$ et $(G', \perp)$ deux groupes et $f : G \longrightarrow G'$ un homomorphisme de groupes.*

1. *On dit que f est un isomorphisme de groupes, si f est bijective.*
2. *On dit que f est un monomorphisme de groupe, si f est injectif.*

3. *On dit que f est un épimorphisme de groupe, si f est surjectif.*
4. *On dit que f est un endomorphisme du groupe G si $G = G'$.*
5. *On dit que f automorphisme de G, si f est un endomorphisme de G et f est bijectif.*

Exemple 3.2.5 *1. $(\mathbb{R}, +)$ est un groupe abélien. De même, $(\mathbb{R}, \star)$ est un groupe abélien avec $x \star y = \sqrt[3]{x^3 + y^3}$ Vérifions que $(\mathbb{R}, +)$ et $(\mathbb{R}, \star)$ sont isomorphes. Soit*

$$\begin{aligned} g : \ (\mathbb{R}, \star) &\longrightarrow (\mathbb{R}, +) \\ t &\longmapsto g(x) = t^3 \end{aligned}$$

Soient $(a, b) \in \mathbb{R}^2$. $f(a \star b) = (\sqrt[3]{a^3 + b^3})^3 = a^3 + b^3 = f(a) + f(b)$. Donc f est homomorphisme de groupe. D'où le résultat.
Soit $y \in \mathbb{R}$ tel que

$$\begin{aligned} f(x) = y &\Rightarrow x^3 = y \\ &\Rightarrow x = \sqrt[3]{y}. \end{aligned}$$

Il y a une unique solution, donc f est bijective : f est un isomorphisme de groupes.

2. *Soit $(G, .)$ un groupe, et $a \in G$, e l'élément neutre de G. L'application $g : (G, .) \longrightarrow (G, .)$, $x \longmapsto g(x) = a \, . \, x \, . \, a^{-1}$. g est un automorphisme de G dit automorphisme intérieur. En effet, $g(x \, . \, x') = g(x) \, . \, g(x'), \forall x, x' \in G$, et g est bijectif (à montrer).*

Définition 3.2.6 *Soit $f : (G, \times) \longrightarrow (G', \perp)$ est homomorphisme de groupes et e' l'élément neutre de G'. On appelle noyau de f, le sous-groupe de G, noté $Ker(f)$ défini par : $Ker(f) = f^{-1}(\{e'\}) = \{x \in G / f(x) = e'\}$*

Proposition 3.2.4 *Soient $f : (G, \star) \longrightarrow (G', \perp)$ un homomorphisme de groupes, e et e' les élément neutres respectifs de G et C'. Alors on a les assertions suivantes :*

1. *$Ker(f)$ est un sous-groupre de $(G, \star)$.*
2. *$Im(f)$ est un sous - groupe de $(G', \perp)$.*

3. *f est injective* $\Longleftrightarrow Ker(f) = \{e\}$.
4. *f est surjective* $\Longleftrightarrow Im(f) = G'$.
5. $\forall x \in G, f(x^{-1}) = [f(x)]^{-1}$.
6. *Si H' est un sous-groupe de G', alors* $f^{-1}(H')$ *est un sous-groupe de G.*

Preuve.

1. On a : $f(e) = f(e \star e) = f(e) \perp f(e)$. En composant par $(f(e))^{-1}$ à droite, on a $f(e) \perp (f(e))^{-1} = f(e) \perp (f(e) \perp (f(e))^{-1})$, qui implique $e' = f(e) \perp e'$, d'où le résultat : $e' = f(e)$, donc $e \in Ker(f)$; Montrons que $x \star y^{-1} \in Ker(f), \forall x, y \in Ker(f)$.

$$\begin{aligned} f(x \star y^{-1}) &= f(x) \perp f(y^{-1}) \\ &= f(x) \perp [f(y)]^{-1} \\ &= e' \perp e^{-1} \ \ (car\ f(x) = e' = f(y)) \\ &= e' \ \ (car\ e'^{-1} = e) \end{aligned}$$

   D'où $f(x \star y^{-1}) = e'$. Par suite, $x \star y^1 \in Ker(f)$; $Ker(f)$ est un sous-groupe de G.

2. Montrons $[f(x)]^{-1} = f(x^{-1})$. Soit $x \in G$. On a : $x \star x^{-1} = x^{-1} \star x = e$.

$$\begin{aligned} x \star x^{-1} = e &\Rightarrow f(x * x^{-1}) = f(e) \\ &\Rightarrow f(x) \perp f(x^{-1}) = f(e) \\ &\Rightarrow f(x) \perp f(x^{-1}) = e' \end{aligned}$$

   D'où $[f(x)]^{-1} = f(x^{-1})$, ce qui achève la démonstration.

3.2.4 Ordre d'un groupe

Soit $(G, \star)$ un groupe d'élément neutre e.

Définition 3.2.7 *On appelle ordre de G, le cardinal de G. On le note :* $o(G) = Card(G) =\mid G \mid$.

Remarque 3.2.5 *L'ordre d'un groupe G est le plus petit entier n tel que $\forall x \in G, x^n = e$, avec $x^n = x \star x \star ... \star x$, (si la loi du groupe est notée $\star$).*

Définition 3.2.8 *Soit $(G, \star)$ un groupe et $a \in G$. On appelle ordre de a le cardinal du sous-groupe engendré par a. On le note $o(a) = o(< a >) = Card(< a >)$.*

Exemple 3.2.6

1. *Soit $(G, \times)$ un groupe, avec $G = \{-1; 1\}$, on a : $o(G) = 2$, i.e , $\forall x \in G, x^2 = 1$.*
2. *$(\mathcal{S}_n, \circ)$ le groupe des permutations, on a $o(\mathcal{S}_n) = n!$.*
3. *Soit $(K, \cdot)$ le groupe d'ordre 4 appelé groupe de Klein. $K = \{e, a, b, c\}$. On a : $a^2 = e; b^2 = e; c^2 = e; a \cdot b = b \cdot a = c; a \cdot c = c \cdot a = b; b \cdot c = c \cdot b = a$.*

$\overset{\curvearrowright}{\circ}$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Théorème 3.2.1 (De Lagrange)
Soit $(G, \star)$ un groupe et H un sous-groupe de G. Alors $o(H)$ divise $o(G)$, i.e l'ordre de H divise l'ordre de G.

Remarque 3.2.6 *On dit qu'un groupe G est fini si son cardinal est fini.*

3.2.5 Groupe-quotient

Soit $(G, \cdot)$ un groupe d'élément neutre.

Proposition 3.2.5 *Soit H un sous-groupe de G. Alors les assertions suivantes sont vérifiées :*

1. *La relation binaire $\mathcal{R}$ définie sur G par $\forall (x, y) \in G^2$, $x\mathcal{R}y \iff x^{-1} \cdot y \in H$, est une relation d'équivalence sur G.*

2. *La relation binaire $\mathcal{R}'$ définie sur G par : $\forall (x,y) \in G^2, x\mathcal{R}'y \Longleftrightarrow y\cdot x^{-1} \in H$, est une relation d'équivalence sur G.*
3. *La classe d'équivalence d'un élément $x \in G$ modulo $\mathcal{R}$ est $\overline{x} = x\cdot H$.*
4. *La classe d'équivalence d'un élément $x \in G$ modulo $\mathcal{R}'$ est $\overline{x} = H\cdot x$.*

Preuve.

1. Montrons que $\mathcal{R}$ est une relation d'équivalence sur G.
   (a) Réflexibilité
   Soit $x \in G$, on a $x^{-1}\cdot x = e \in H$, i.e $x^{-1}\cdot x \in H$, d'où $x\mathcal{R}x$. Donc $\Re$ est réflexive.
   (b) Symétrie
   Soient $(x,y) \in G : x\mathcal{R}y$

$$\begin{aligned} x\mathcal{R}y &\Rightarrow x^{-1}\cdot y \in H \\ &\Rightarrow (x^{-1}\cdot y)^{-1} \in H \\ &\Rightarrow y^{-1}\cdot (x^{-1})^{-1} \in H \\ &\Rightarrow y^{-1}\cdot x \in H \\ &\Rightarrow y\mathcal{R}x \\ &\Rightarrow \mathcal{R} \textit{ est symtrique.} \end{aligned}$$

   (c) Transitivité
   Soient $(x,y,z) \in G^3 : x\mathcal{R}y$ et $y\mathcal{R}z$. $x\mathcal{R}y \Longleftrightarrow x^{-1}\cdot y \in H$ et $y\mathcal{R}z \Longleftrightarrow y^{-1}\cdot z \in H$.

$$\begin{aligned} \textit{Ainsi } x^{-1}\cdot y\cdot y^{-1}\cdot z \in H &\Rightarrow x^{-1}\cdot e\cdot z \in H \\ &\Rightarrow x^{-1}\cdot z \in H \\ &\Rightarrow x\mathcal{R}z \\ &\Rightarrow \mathcal{R} \textit{ est une relation transitive.} \end{aligned}$$

   Par conséquent, $\mathcal{R}$ est une relation d'équivalence, d'après tout ce qui précède.

2. Montrons que la classe d'équivalence modulo $\mathcal{R}$ est $\overline{x} = x\cdot H$. Soit $x \in G$.

$$\begin{aligned}\overline{x} &= \{y \in G / x\mathcal{R}y\}\\ &= \{y \in G / x^{-1}\cdot y \in H\}\\ &= \{y \in G / x\cdot x^{-1}\cdot y \in x\cdot H\}\\ &= \{y \in G / y \in x\cdot H\}\\ &= x\cdot H\end{aligned}$$

Ce qui achève la démonstration.

On a $G/\mathcal{R} = \{\overline{x} : x \in G\} = \{x \cdot H / x \in G\}$ appelé ensemble-quotient modulo $\mathcal{R}$.

Remarque 3.2.7 *1. $G/\mathcal{R}$ est noté aussi G/H.*

2. *Les classes modulo $\mathcal{R}$ sont dites classes à gauche modulo H. Soit $x \in G, \overline{x} = x\cdot H$. $\overline{x}$ est l'ensemble des classes de x à gauche modulo H.*
3. *Les classes d'équivalence modulo $\mathcal{R}'$ sont dites classes à droite modulo H, $x \in G, \overline{x} = H \cdot x$ (classe de x à droite modulo H). On le note $G/\mathcal{R}' = \{H\cdot x / x \in G\}$.*
4. *Si $(G, \cdot)$ est commutatif, alors $H \cdot x = x \cdot H, \forall x \in G$.*
5. *$\overline{e} = e\cdot H = H\cdot e = H$.*
6. *$(G, +)$ un groupe. Soit $x \in G, \overline{x} = x + H$ (classe de x modulo H).*
7. *On rappelle que $x\cdot H = \{x\cdot h : h \in H\}$.*

Définition 3.2.9 *Soit $(G, \cdot)$ un groupe et H un sous-groupe de G. On dit que : H est invariant, ou distingué, ou normal dans G, si $\forall x \in G, x\cdot H = H\cdot x$.*

Proposition 3.2.6 *Soit H un sous-groupe de G. Alors, les conditions suivantes sont équivalentes :*

1. *H est normal,*
2. *$\forall x \in G, x\cdot H\cdot x^{-1} = H$,*
3. *$\forall x \in G, x\cdot H\cdot x^{-1} \subset H$.*

Exemple 3.2.7 *1. Dans un groupe abélien, tous les sous-groupes sont invariants.*

2. Dans $(\mathbb{Z}, +)$, tous les sous-groupes sont invariants (on rappelle que tous les sous-groupes ici sont de la forme $p\mathbb{Z}$: $p > 0$.

Théorème 3.2.2 *Soit $(G, \cdot)$ un groupe, H un sous-groupe invariant de G. Alors, les assertions suivantes sont vérifiées :*

1. *La relation d'équivalence $\mathcal{R}$ définie sur G par $x\mathcal{R}y \Longleftrightarrow x^{-1}\cdot y \in H$ est compatible avec la structure du groupe G.*
2. *La loi $\cdot$ définie par G/H par :*

$$\begin{array}{ccc} G/H \times G/H & \longrightarrow & G/H \\ (\overline{x}, \overline{y}) & \longmapsto & \overline{x}\cdot\overline{y} = \overline{x\cdot y} \end{array}$$

est une loi de composition interne sur G/H.

3. *$(G/H, \cdot)$ est un groupe appelé le groupe quotient de G par H.*

Remarque 3.2.8 *1. La relation $\mathcal{R}$ est compatible avec la loi du groupe G si $\forall (x, y) \in G^2, \forall (x', y') \in G^2$, on a $x\mathcal{R}y$ et $x'\mathcal{R}y' \Rightarrow x\cdot x'\mathcal{R}y\cdot y'$*

2. Soit e l'élément neutre de G. $\overline{e} = e\cdot H = H$ est l'élément neutre de G/H.

3.

$$\begin{aligned} \overline{x}\cdot\overline{y} &= (x\cdot H)\cdot(y\cdot H) \\ &= x\cdot(H\cdot y)\cdot H \\ &= x\cdot y\cdot H\cdot H \\ &= x\cdot y\cdot H \\ &= (x\cdot y)\cdot H \\ &= \overline{x\cdot y} \end{aligned}$$

Exemple 3.2.8 *1. $(\mathbb{Z}, +)$ est un groupe abélien. Soit $p > 0$, $H = p\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$. $x\mathcal{R}y \Longleftrightarrow x + y^{-1} \in H \Longleftrightarrow x - y \in p\mathbb{Z}$ $\mathcal{R}$ est une relation d'équivalence sur $\mathbb{Z}$. $\mathbb{Z}/\mathcal{R} = \mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{p-1}\}$ $(\mathbb{Z}/p\mathbb{Z}, +)$ est un groupe abélien. Cas particulier de $\mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$.*

$\overset{\curvearrowright}{+}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

2. *$\mathcal{A}_n$, l'ensemble des permutations paires est un sous-groupe invariant de $\mathcal{S}_n$. En effet,*

$$\begin{array}{rccl} \varepsilon & : & \mathcal{S}_n & \longrightarrow & \{-1;1\} \\ & & \sigma & \longmapsto & \varepsilon(\sigma) = (-1)^{i(\sigma)} \end{array}$$

$Ker(\varepsilon) = \{\sigma \in \mathcal{S}_n : \varepsilon(\sigma) = 1\} = \mathcal{A}_n$. $(\mathcal{S}_n/\mathcal{A}_n, \circ)$ est un groupe appelé groupe-quotient de $\mathcal{S}_n$ par $\mathcal{A}_n$, avec $\mathcal{S}_n/\mathcal{A}_n = \{\bar{\sigma}/\sigma \in \mathcal{S}_n\}$. Si σ est une permutation paire, et σ' une permutation impaire, on a : $\mathcal{S}_n/\mathcal{A}_n = \{\bar{\sigma}, \bar{\sigma}'\}$, $o(\mathcal{S}_n/\mathcal{A}_n) = 2$ et $o(\mathcal{A}_n) = \frac{o(\mathcal{S}_n)}{2} = \frac{n!}{2}$. D'où l'ordre de l'ensemble des permutations paires est $\frac{n!}{2} = Card(\mathcal{A}_n)$.

Définition 3.2.10 *Soit $(G, \cdot)$ un groupe.*

1. *On dit que G est monogène s'il existe $a \in G$ tel que $G =< a >= \{a^k : k \in \mathbb{Z}\}$.*
2. *On dit que G est cyclique si G est monogène et fini.*

Exemple 3.2.9 *$\mathbb{Z}$ est monogène et $\mathbb{Z}/p\mathbb{Z}$ est un groupe cyclique.*

3.2.6 Groupes symétriques : $\mathcal{S}_n$

3.2.6.1 Préliminaires Soit E un ensemble quelconque non vide et $Card(E) = n$.

Définition 3.2.11 *Une bijection de E sur E est dite une permutation de E.*

Remarque 3.2.9 *$\mathcal{S}(E)$ est l'ensemble des permutations de E, $Card(\mathcal{S}(E)) = n!$.*

Proposition 3.2.7 *$(\mathcal{S}(E), \circ)$ est un groupe appelé le groupe des permutations de E.*

Remarque 3.2.10 *1. $(\mathcal{S}(E), \circ)$ n'est pas en général commutatif.*

2. Si $E = \{1, 2, 3, ..., n\}$, alors on note $\mathcal{S}(E) = \mathcal{S}_n$. Voir l'exemple nř ? au début de la section.

3.2.6.2 Support

Définition 3.2.12 *On appelle support de σ l'ensemble des $k \in \{1, 2, 3, ..., n\} : \sigma(k) \neq k$, on le note $supp(\sigma)$.*

Exemple 3.2.10 *On considère $(\mathcal{S}_3, \circ)$. On pose $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $supp(\sigma_2) = \{1, 3\}$.*

Proposition 3.2.8 *Soient $\sigma, \sigma' \in \mathcal{S}_n$. Si $supp(\sigma) \cap supp(\sigma') = \emptyset$, alors σ et σ' commutent entre eux.*

Exemple 3.2.11 *On pose $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 5 & 6 \end{pmatrix}$ et $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 5 & 6 & 4 \end{pmatrix}$. $Supp(\sigma_1) = \{1, 2, 3\}$ et $supp(\sigma_2) = \{4, 5, 6\}$. Les deux supports sont disjoints, donc les deux permutations commutent.*

3.2.6.3 Cycles

Soit $\sigma \in \mathcal{S}_n$.

Définition 3.2.13 *Une permutation σ est un cycle de longueur $r\,(1 \leq r \leq n)$ s'il existe $a_1, a_2, ..., a_r \in \{1, 2, 3, ..., n\} : \sigma(a_1) = a_2, \sigma(a_2) = a_3, ..., \sigma(a_{r-1}) = a_r$, $\sigma(a_r) = a_1$ et $\forall k \in \{1, 2, 3, ..., n\} - \{a_1, a_2, ..., a_r\}$, on a $\sigma(k) = k$. On note alors le cycle $\sigma = (a_1, a_2, ..., a_r)$.*

Exemple 3.2.12 *Avec l'exemple précédent, on a $\sigma_1 = (1, 2, 3)$ et $\sigma_2 = (4, 5, 6)$. Donc σ_1 et σ_2 sont de longueur 3.*

Remarque 3.2.11 *Soit $\sigma = (a_1, a_2, ..., a_r)$ un cycle.*

1. $supp(\sigma) = \{a_1, a_2, ..., a_r\}$.

2. $o(\sigma) = o(a_1, a_2, ..., a_r) = r$.

3. $\sigma^r = I_d$.

Définition 3.2.14 *Une transposition est un cycle de longueur 2.*

Remarque 3.2.12 *Si σ est une transposition, alors il existe $\alpha_1, \alpha_2 \in \{1, 2, 3, ..., n\}$ tels que $\sigma = (\alpha_1, \alpha_2)$.*

Exemple 3.2.13 *Dans le groupe $(\mathcal{S}_3, \circ)$, $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1, 3)$ est une transposition de longueur 2 .*

3.2.6.4 Décomposition d'une permutation

Théorème 3.2.3 *Soit $\sigma \in \mathcal{S}_n$ et $\sigma \neq I_d$. Alors, σ s'écrit sous la forme de produits de cycles disjoints $\sigma = \sigma_1 \circ \sigma_2 \circ \sigma_3 \circ ... \circ \sigma_r$, où les $\sigma_i, i \in \{1, 2, ..., r\}$ sont des cycles de longueur i.*

Exemple 3.2.14

1. $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 6 & 2 & 1 \end{pmatrix} = (1, 3, 4, 6) \circ (2, 5)$.

2. $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 6 & 9 & 7 & 2 & 5 & 8 & 1 & 3 \end{pmatrix} = (1, 4, 7, 8) \circ (2, 6, 5) \circ (3, 9)$.

Théorème 3.2.4 *Soit $\sigma \in \mathcal{S}_n\, (\sigma \neq Id)$. Alors, σ se décompose en un produit de transpositions non permutables en général. $\sigma = \sigma_1 \circ \sigma_2 \circ ... \circ \sigma_s$, où σ_i sont des cycles, pour $(1 \leq i \leq s)$.*

Soit $\sigma_j = (a_{j1}, a_{j2}, ..., a_{jk})$ un cycle. Alors on a $\sigma_j = (a_{j1}, a_{j2}) \circ (a_{j2} \circ a_{j3}) \circ ... \circ (a_{j\,k-1}, a_{jk})$.

Exemple 3.2.15

$$\begin{aligned} \sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 6 & 2 & 1 \end{pmatrix} \\ &= (1, 3, 4, 6) \circ (2, 5) \\ &= (1, 3) \circ (3, 4) \circ (2, 5) \end{aligned}$$

Définition 3.2.15 *Soit $\sigma = \sigma_1 \circ \sigma_2 \circ ... \circ \sigma_s \in \mathcal{S}_n$. On appelle ordre de σ le ppcm des ordes des cycles σ_1, σ_2,..., σ_s. On a ainsi $o(\sigma) = ppcm\big(o(\sigma_1), ..., o(\sigma_s)\big)$*

Définition 3.2.16 *Soit $\sigma \in \mathcal{S}_n$ et $(i, j) \in \mathbb{N}$. On dit que σ réalise une inversion entre i et j si pour $i \leq j$ on a : $\sigma(i) \geq \sigma(j)$. On note $i(\sigma)$ le nombre d'inversion de σ .*

Exemple 3.2.16 *On pose* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 6 & 9 & 7 & 2 & 5 & 8 & 1 & 3 \end{pmatrix} = \underbrace{(1,4,7,8)}_{\sigma_1} \circ \underbrace{(2,6,5)}_{\sigma_2} \circ \underbrace{(3,9)}_{\sigma_3}$.

$o(\sigma) = ppcm(o(\sigma_1), o(\sigma_2), o(\sigma_3)) = ppcm(4, 3, 2) = 12$.

Par ailleurs, $2012 = 12 \times 167 + 8$, *donc*

$$\begin{aligned} \sigma^{2012} &= \sigma^8 \\ &= (\sigma_1^4)^2 \circ (\sigma_2^3)^2 \circ \sigma_2^2 \circ (\sigma_3^2)^4 \\ &= \sigma_2^2 \\ &= (2,5,6) \end{aligned}$$

$i(\sigma) = 22$ *et* $\varepsilon(\sigma) = 1$ *: σ est une permutation paire.*

3.3 Anneaux -Corps

3.3.1 Définitions et exemples

Définition 3.3.1 *Soit A un ensemble muni de deux lois de composition internes notées $+$ et $\cdot$. On dit que A est un anneau si :*

1. *$(A, +)$ est un groupe abélien.*
2. *La loi notée $\cdot$ est associative.*
3. *La loi $\cdot$ est distributive par rapport à la loi $+$.*

Si de plus, la loi $\cdot$ est commutative, on dit que $(A, +, \cdot)$ est un anneau commutatif. Si de plus A admet un élément neutre pour la loi $\cdot$, notée 1_A, on dit que $(A, +, \cdot)$ est un anneau unitaire.

Exemple 3.3.1 $(\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$, $(\mathbb{C},+,\times)$, $(\mathbb{Z}/p\mathbb{Z},+,\times)$ *sont des anneaux commutatifs unitaires.*

Conséquences. (Quelques règles de calcul dans un anneau)
Soit $(A,+,\cdot)$ un anneau commutatif unitaire.

1. $\forall x \in A, x\cdot 0_A = 0_A\cdot x = 0_A$.
2. $\forall (x,y) \in A^2, x\cdot(-y) = (-x)\cdot y = -x\cdot y$.
3. $\forall x \in A, x^0 = 1_A$, et , $x^n = x\cdot x^{n-1}$.
4. $\forall (x,y) \in A, (x+y)^n = \sum_{k=0}^{n} C_n^k x^k\cdot y^{n-k}$

3.3.2 Eléments particuliers d'un anneau

Soit A un anneau unitaire.

1. **Elément inversible**
   Un élément $a \in A$ est inversible s'il existe $a' \in A$ tel que $a\cdot a' = a'\cdot a = 1_A$. Notons $a' = a^{-1}$ est appelé inverse de a.
2. **Elément nilpotent**
   Un élément a est dit nilpotent dans A s'il existe $n \in \mathbb{N}^*$ tel que $a^n = 0$.

   Exemple 3.3.2 *Soit* $\mathbb{Z}/8\mathbb{Z}$. $\overline{2}^3 = \overline{8} = \overline{0}$, *donc* $\overline{2}$ *et nilpotent d'indice 3 dans* $(\mathbb{Z}/8\mathbb{Z},+,\cdot)$.
3. **Diviseur de zéro**

   – Un élément $a \in A^*$ est dit diviseur de zéro à gauche s'il existe $b \in A^* : a\cdot b = 0$.
   – Un élément $a \in A^*$ est dit diviseur de zéro à droite s'il existe $b \in A^* : b\cdot a = 0$.

   Exemple 3.3.3 *Dans* $(\mathbb{Z}/6\mathbb{Z},+,\cdot)$, *on a* $\overline{2}\cdot\overline{3} = \overline{6} = \overline{0}$, *donc* $\overline{2}$ *et* $\overline{3}$ *sont des diviseurs de zéro.*

3.3.3 Anneaux intègres

Définition 3.3.2 *Un anneau A est dit intègre s'il n'a pas de diviseurs de zéro, i.e,* $\forall (x,y) \in A^2, (x\cdot y = 0 \Rightarrow x = 0$ *ou* $y = 0)$.

Exemple 3.3.4 *1.* $(\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$, $(\mathbb{C},+,\times)$, $(\mathbb{Z}/p\mathbb{Z},+,\times)$, *$p$ premier sont des anneaux intègres.*

2. L'anneau $(\mathbb{R}^2,+,\cdot)$ *avec :* $(x,y)+(x',y') = (x+x', y+y')$

$$(x,y)\cdot(x',y') = (xx', yy')$$

n'est pas intègre, puisque $(1,0)\cdot(0,6) = (0,0)$.

3. De même, $(\mathbb{Z}/6\mathbb{Z},+,\cdot)$ *n'est pas un anneau intègre.*

3.3.4 Sous-anneaux et idéaux

Définition 3.3.3 *Soit A un anneau. On appelle sous-anneau de A, toute partie B de A vérifiant les conditions suivantes :*

1. $(B,+)$ *est un est sous-groupe de* $(A,+)$,
2. $\forall (x,y) \in B^2, x\cdot y \in B$.

Si de plus $(A,+,\cdot)$ *est un anneau unitaire,* $1_A \in B$.

Exemple 3.3.5 $(\mathbb{Z},+,\times)$ *est un sous-anneau de* $(\mathbb{Q},+,\times)$.

Définition 3.3.4 *Soit* $(A,+,\cdot)$ *un anneau.*

1. *On appelle idéal à gauche de A, toute partie I de A vérifiant les conditions suivantes :*
   (a) $(I,+)$ *est un sous-groupe de* $(A,+)$.
   (b) $\forall a \in A, \forall x \in I, a\cdot x \in I$,
2. *On appelle idéal à droite de A, toute partie I de A vérifiant les conditions suivantes :*

(a) $(I,+)$ *est un sous-groupe de* $(A,+)$.

(b) $\forall a \in A, \forall x \in I, x\cdot a \in I$,

3. *Une partie I de A est dite idéal bilatère de A, si I est à la fois idéal à gauche et à droite de A, i.e, I est un idéal bilatère de A si*

(a) $(I,+)$ *est un sous-groupe de* $(A,+)$.

(b) $\forall a \in A, \forall x \in I, a\cdot x\cdot a \in I$,

Exemple 3.3.6 1. *Soit* $(A,+,\cdot)$ *un anneau.* $\{0_A\}$ *et A sont des idéaux de A.*

2. *Dans* $(\mathbb{Z},+,\times)$, *les idéaux de* $\mathbb{Z}$ *sont de la forme* $p\mathbb{Z}, p \in N^*$.

3.3.5 Homomorphismes d'anneaux

Définition 3.3.5 *Soient* $(A,+,\cdot)$ *et* $(A',+,\cdot)$ *deux anneaux. On appelle homomorphisme de A dans A', toute application* $f : A \longrightarrow A'$ *vérifiant les conditions suivantes :*

1. $f(x+y) = f(x) + f(y)$,
2. $f(x)\cdot f(y) = f(x\cdot y)$.

Si de plus A et A' sont des anneaux unitaires, alors $f(1_A) = 1_{A'}$.

Remarque 3.3.1 *Soit* $f : A' \longrightarrow A$ *un homomorphisme.*

1. *Si A = A', on dit que f est un endomorphisme de A.*
2. *Si f est bijectif, on dit que f est un isomorphisme.*
3. *On dit que f est un automorphisme si f est un endomorphisme bijectif de A.*

Définition 3.3.6 *Soit* $(A,+,\cdot$ *un anneau. Un idéal I de A est dit principal de A si I est engendré par un élément de l'anneau. On note* $I =< a >$.

Exemple 3.3.7 *Dans* $(\mathbb{Z},+,\times)$ *tous les idéaux sont principaux, car ils sont de la forme* $p\mathbb{Z} =< p >$.

Définition 3.3.7 *Soit* $(A,+,\cdot$ *un anneau commutatif. Un idéal bilatère P de A est dit premier si* $\forall a, b \in A, a\cdot b \in P \Rightarrow a \in P$ *ou* $b \in P$.

Exemple 3.3.8 *Dans* $(\mathbb{Z}, +, \times)$ *tous les idéaux sont premiers.*

Définition 3.3.8 *Soit* $(A, +, \cdot$ *un anneau. Un idéal bilatère* M *est dit maximal si* $M \neq A$ *et pour* J *idéal de* A*, si* $M \subset J$*, alors* $J = M$ *ou* $J = A$*.*

Exemple 3.3.9 *Dans* $(\mathbb{Z}, +, \times)$*,* $I = p\mathbb{Z}$ *est un idéal maximal de* $\mathbb{Z}$ *si et seulement si* p *est premier.*

3.3.6 Corps

Définition 3.3.9 *Soit* $\mathbb{K}$ *un ensemble muni de deux lois de composition internes* $+$ *et* $\cdot$*. On dit que* $(\mathbb{K}, +, \times)$ *est un corps si :*

1. $(\mathbb{K}, +, \times)$ *est un anneau unitaire ;*
2. *Tout élément non nul de* $\mathbb{K}$ *est inversible, i.e* $\forall x \in \mathbb{K}^*, \exists x' \in \mathbb{K}^*$ *tel que* $x \cdot x' = x' \cdot x = 1_{\mathbb{K}}$*.*

Si de plus, la loi $\cdot$ *est commutative, alors* $(\mathbb{K}, +, \times)$ *est un corps commutatif.*

Exemple 3.3.10

1. $(\mathbb{Q}, +, \times)$*,* $(\mathbb{R}, +, \times)$*,* $(\mathbb{C}, +, \times)$*,* $(\mathbb{Z}/p\mathbb{Z}, +, \times)$*,* p *premier sont des corps commutatifs.*
2. $(\mathbb{Z}, +, \times)$ *n'est pas un corps commutatif car 2 n'est pas un élément inversible.*
3. *De même,* $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ *est un corps commutatif.*

Définition 3.3.10 *Soit* $(\mathbb{K}, +, \times)$ *un corps, on appelle sous-corps de* $\mathbb{K}$*, toute partie* $\mathbb{K}'$ *de* $\mathbb{K}$ *vérifiant les conditions suivantes :*

1. $\mathbb{K}'$ *est un sous-anneau de* $\mathbb{K}$*.*
2. $\forall x \in \mathbb{K}' \backslash \{0\}, x^{-1} \in \mathbb{K}'$*.*

Exemple 3.3.11 $\mathbb{R}$ *est un sous-corps de* $\mathbb{C}$*.*

Chapitre 4

Polynômes et fractions rationnelles

Sommaire

4.1 Polynômes

4.1.1 Généralités

Soit $\mathbb{K}$ un corps commutatif.

Définition 4.1.1 *On appelle polynôme à une indéterminée X à coefficients dans $\mathbb{K}$, toute suite $(a_0, a_1, ..., a_{k+1}, ...) = (a_k)_{k\in\mathbb{N}}$ d'éléments de $\mathbb{K}$ nuls à partir d'un certain rang. On note : $P = (a_0, a_1, ..., a_{k+1}, ...)$, les éléments a_k sont appelés les coefficients du polynômes P.*

Note 4.1.1
1. *$\mathbb{K}[X]$ est l'ensemble des polynômes à coefficients dans $\mathbb{K}$, à une indéterminée X.*
2. *$\mathbb{R}[X]$ est l'ensemble des polynômes à coefficients dans $\mathbb{R}$, à une indéterminée X.*
3. *$\mathbb{C}[X]$ est l'ensemble des polynômes à coefficients dans $\mathbb{C}$, à une indéterminée X.*

Note 4.1.2 *Soit $P = (a_k)_{k\in\mathbb{N}}$ un polynôme de $\mathbb{K}[X]$. On dit que P est le polynôme nul si $a_k = 0, \forall k \in \mathbb{N}$.*

Définition 4.1.2 *Soit $P = (a_k)_{k\in\mathbb{N}}$ un polynôme non nul de $\mathbb{K}[X]$.*

1. *On appelle degré de P, le plus grand des entiers k tels que $a_k \neq 0$, et on note $d^\circ P = deg(P)$.*
$$P = (a_0, a_1, ..., a_n, 0, 0, ...) \Rightarrow deg(P) = n$$
2. *On appelle valuation de P, le plus petit des entiers k tels que $a_k \neq 0$ et on note $V(P) = Val(P)$.*

Exemple 4.1.1 *Soit $P = (0, 0, 0, -2, 8, 7, 10, 4, 5, 0, 0, ...)$ un polynôme. $deg(P) = 8$, $Val(P) = 3$.*

Remarque 4.1.1
1. *$Val(P) \leq deg(P), \forall P \in \mathbb{K}[X]$ et $P \neq 0$.*
2. *Si $P = 0, Val(P) = +\infty$ et $deg(P) = -\infty$.*
3. *Deux polynômes $P = (a_k)_{k\in\mathbb{N}}$ et $Q = (b_k)_{k\in\mathbb{N}}$ sont égaux si et seulement si $a_k = b_k,\ \forall k \in \mathbb{N}$.*

4.1.2 Structures de $\mathbb{K}[X]$

4.1.2.1 Addition Soient deux polynômes $P = (a_k)_{k\in\mathbb{N}}$ et $Q = (b_k)_{k\in\mathbb{N}}$.

$$\begin{aligned} P+Q &= (a_k+b_k)_{k\in\mathbb{N}} \\ &= (a_0+b_0, a_1+b_1, ..., a_k+b_k, ...) \end{aligned}$$

On montre que l'ensemble $\mathbb{K}[X]$, muni de l'addition est un groupe abélien.

Proposition 4.1.1 *$(\mathbb{K}[X], +)$ est un groupe abélien.*

Remarque 4.1.2 *Soient P et Q deux polynômes.*

1. $d^\circ(P+Q) \leq max\big(d^\circ(P), d^\circ(Q)\big)$.
2. $Val(P+Q) \geq min(Val(P), Val(Q))$.

4.1.2.2 Produit externe Soient $\alpha \in \mathbb{K}$ et $P = (a_k)_{k\in\mathbb{N}} \in \mathbb{K}[X]$, on a $\alpha\cdot P = (\alpha\cdot a_k)_{k\in\mathbb{N}}$.

Remarque 4.1.3 *Soient $(\alpha, \beta) \in \mathbb{K}^2, (P, Q) \in \mathbb{K}[X]^2$.*

1. $\alpha \cdot (P+Q) = \alpha \cdot P + \alpha \cdot Q$
2. $(\alpha+\beta)\cdot P = \alpha \cdot P + \beta \cdot P$
3. $\alpha(\beta \cdot P) = (\alpha\beta)\cdot P$
4. $1_{\mathbb{K}} \cdot P = P$
5. $deg(\alpha \cdot P) = \begin{cases} -\infty \ si \ \alpha = 0 \\ deg(P) \ si \ \alpha \neq 0 \end{cases}$
6. $Val(\alpha \cdot P) = \begin{cases} -\infty \ si \ \alpha = 0 \\ Val(P) \ si \ \alpha \neq 0 \end{cases}$

4.1.2.3 Produit de deux polynômes Soient deux polynômes $P = (a_k)_{k\in\mathbb{N}}$ et $Q = (b_k)_{k\in\mathbb{N}}$. On définit : $P \cdot Q = (c_n)_{n\in\mathbb{N}}$ où $c_n = \sum_{k=0}^{n} a_k b_{n-k}$.

Théorème 4.1.1 *$(\mathbb{K}[X], +, \cdot)$ est un anneau commutatif et intègre.*

On a $0_{\mathbb{K}[X]} = (0, 0, 0, ..., 0, ...)$ et $1_{\mathbb{K}[X]} = (1, 0, 0, ..., 0, ...)$

Remarque 4.1.4 *Soient P et Q deux polynômes non nuls.*

1. $d^\circ(P \cdot Q) = d^\circ(P) + d^\circ(Q)$;
2. $Val(P \cdot Q) = Val(P) + Val(Q)$.

Proposition 4.1.2 *Soit $\mathbb{K}$ un corps commutatif. Alors le groupe des éléments inversibles de $\mathbb{K}[X]$ est l'ensemble des polynômes de degré zéro.*

Preuve. Soit $P \in \mathbb{K}[X]$. P est inversible s'il existe $Q \in \mathbb{K}[X]$ tels que $P \cdot Q = 1_{\mathbb{K}[X]}$. Ainsi, $deg(P \cdot Q) = deg(1_{\mathbb{K}[X]}) = 0$, donc $deg(P) + deg(Q) = 0$. D'où $deg(P) = deg(Q) = 0$. Par conséquent $P = (a_0, 0, 0, ..., 0)$, avec $a \in \mathbb{K}$ (P est un polynôme constant).

Définition 4.1.3 *On appelle indéterminée le polynôme X dont tous les coefficients sont nuls sauf le coefficient d'indice $1 \in \mathbb{N}$, qui est égal à $1_{\mathbb{K}} = 1$.*

$$X = (0, 1, 0, 0, ..., 0)$$

$$X^2 = (0, 1, 0, 0, ..., 0)(0, 1, 0, 0, ..., 0) = (0, 0, 1, 0, ..., 0)$$

$$X^3 = (0, 0, 0, \underbrace{1}_{4^{ime} position}, 0, ...,)$$

$$X^n = (0, 0, 0, ..., 0, \underbrace{1}_{(n+1)^{ime} position}, 0, ...)$$

$$a_n X^n = (0, 0, 0, ..., 0, \underbrace{a_n}_{(n+1)^{ime} position}, 0, ...)$$

$$\begin{aligned}
P &= (a_k)_{k\in\mathbb{N}} \in \mathbb{K}[X] \\
&= (a_0, a_1, a_2, ..., a_n, ...) \\
&= (a_0, 0, 0, ..., 0) + (0, a_1, 0, ..., 0) + ... + (0, 0, 0, ..., a_n, 0, ...) + ... \\
&= a_0(1, 0, 0, ..., 0) + a_1(0, 1, 0, ..., 0) + ... + a_n(0, 0, 0, ..., 1, 0, ...) + ... \\
&= a_0 \cdot 1_{\mathbb{K}[X]} + a_1 \cdot X + a_2 \cdot X_n + ... + a_n \cdot X^n + ... \\
&= \sum_{k\in\mathbb{N}} a_k x^k
\end{aligned}$$

Ainsi, si $deg(P) = n$, alors $P = (a_0, a_1, ..., a_n, 0, ...) = \sum_{k=0}^{n} a_k X^k$.

Remarque 4.1.5 *1. Si $deg(P) = n$, alors le coefficient non nul a_n est dit coefficient dominant de P.*

2. Si $a_n = 1$, alors P est dit polynôme unitaire ou normal.

4.1.3 Propriétés arithmétiques des polynômes

4.1.3.1 Division euclidienne

Définition 4.1.4 *Soient A et B deux polynôme de $\mathbb{K}[X]$. On dit que B divise A s'il existe un polynôme $Q \in \mathbb{K}[X]$ tel que $A = B \cdot Q$. Dans ce cas, A est dit multiple de B et Q s'appelle le quotient de la division de A par B.*

Théorème 4.1.2 *Soitent A et B deux polynômes tels que $B \neq 0$. Alors il exite un couple (Q, R) de $\mathbb{K}[X]$ unique tels que $A = B \cdot Q + R$ avec $deg(R) < deg(B)$. Q s'appelle le quotient de la division de A par B. R est le reste de la division de A par B.*

Preuve.

1. Unicité :
   Supposons que $A = B \cdot Q + R$ avec $deg(R) < deg(B)$ et $A = B' \cdot Q + R$, avec $deg(R) < deg(B)$. On a $B \cdot (Q - Q') = R' - R$, ainsi $deg(B(Q - Q')) = deg(R' - R)$. Comme $deg(R - R') < deg(B)$, alors on a $Q - Q' = 0$. Par conséquent, on a $R = R'$.
2. Existence : on raisonne par récurrence sur le degré de A.
   - Si $deg(A) = 0$ et $deg(B) > 0$, alors on pose $Q = 0$ et $R = A$.
     Si $deg(A) = 0$ et $deg(B) = 0$, on pose $Q = \frac{A}{B}$ et $R = 0$.
   - Supposons l'existence vraie jusqu'à $deg(A) \leq n - 1$.
     Soient $A = a_n X^n + ... + a_0$ un polynôme de degré n et $B = b_m X^m + ... + b_0$, avec $b_m \neq 0$.
     Si $n < m$, on pose $Q = 0$ et $R = A$.
     Si $n \geq m$, on écrit $A = B \cdot \frac{a_n}{b_m} X^{n-m} + A_1$ avec $deg(A_1) \leq n - 1$. On applique l'hypothèse de récurence à A_1 : il existe alors Q_1 et $R_1 \in \mathbb{K}[X]$ tels que $A_1 = BQ_1 + R_1$, avec $deg(R_1) < deg(B)$. Ainsi on a $A = B(\frac{a_n}{b_m} X^{n-m} + Q_1) + R_1$.
     Par conséquent $Q = \frac{a_n}{b_m} X^{n-m} + Q_1$ et $R = R_1$ conviennent.

Exemple 4.1.2 *Soit* $A = 2X^4 - X^3 - 2X^2 + 3X - 1$ *et* $B = X^2 - X + 1$. *On trouve* $Q = 2X^2 + X - 3$ *et* $R = -X + 2$. *D'où* $A = BQ + R$.

Remarque 4.1.6 *Division euclidienne suivant les puissances croissantes*
Soit $p \in \mathbb{N}, A, B$ *deux polynômes de* $\mathbb{K}[X]$ *telq que* $Val(B) = 0$, *alors il existe un unique couple* $(Q, R) \in \mathbb{K}[X]^2$ *tels que* $A = B \cdot Q + X^{p+1}R$. Q *le quotient,* R *le reste de la division, et* $deg(Q) \leq p$.

Exemple 4.1.3 *Soit,* $A = 1 + X$ *et* $B = 1 - X + X^2$.

$$\begin{array}{r|l} 1+X & 1-X+X^2 \\ \hline -(1-X+X^2) & 1+2X+X^2 \\ 2X-X^2 & \\ -(2X-2X^2-2X^3) & \\ X^2-2X^3 & \\ -(X^2-X^3+X^4) & \\ -X^3-X^4 = -X^3(1+X) & \end{array}$$

$$\overbrace{1+X}^{A} = \overbrace{(1-X+X^2)}^{B}\overbrace{(1-2X+X^2)}^{Q} + \overbrace{X^3(-1-X)}^{R}$$

4.1.3.2 Idéaux de $\mathbb{K}[X]$

Définition 4.1.5 *Un anneau* A *est principal si tout idéal de* A *est engendré par un élément.*

Exemple 4.1.4 $\mathbb{Z}$ *est un anneau principal. Ces idéaux sont de la forme* $I = p\mathbb{Z}$ $(p \geq 0)$.

Théorème 4.1.3 $\mathbb{K}[X]$ *est un anneau principal.*

Preuve. On a déjà vu que $\mathbb{K}[X]$ est un anneau intègre commutatif.
Il suffit de vérifier que tout idéal de $\mathbb{K}[X]$ peut être engendré par un élément. Soit I un idéal de $\mathbb{K}[X]$.

1. Si $I = \{0\}$, alors I est engendré par le polynôme nul.

2. Si $I \neq \{0\}$. Alors l'ensemble $M = \{n \in \mathbb{N}/\exists P(X) \in I : d^o(P) = n\}$ est une partie non vide de $\mathbb{N}$. Donc M admet un plus petit élément noté n_0. Soit P un polynôme non nul de I et $d^o(P) = n_0$. Tout multiple de P est un élément de I.
   Soit maintenant A un polynôme non nul de I tel que $d^o(A) \geq d^o(P)$. Ainsi on a $A = QP + R$ (Q et R étant respectivement le quotient et le reste de la division euclidienne de A par P). Comme $A \in I$, $P \in I$ alors $R = A - QP \in I$. Si $R \neq 0$, alors $\left.\begin{array}{l} d^o(R) < d^o(P) \\ R \in I \end{array}\right\}$ est une contradiction.
   D'où $R = 0$, par conséquent $A = PQ$. Par suite on a $I = \{h \in \mathbb{K}[X] : h = PQ\} =< P >$ idéal engendré par A.

4.1.3.3 Plus grand commun diviseur (PGCD) Soient $A_1, A_2, ..., A_n$ des polynômes de $\mathbb{K}[X]$ non nuls. Posons

$$I = \{P \in \mathbb{K}[X], \exists U_1, U_2, ..., U_n \in \mathbb{K}[X]^n, P = \sum_{i=1}^{n} U_i A_i\}$$

On a I est un idéal de $\mathbb{K}[X]$, et d'après le théorème précédent, $\exists D \in \mathbb{K}[X]$ tel que $I =< D >$ (idéal engendré par D), D un polynôme unitaire. On a $A_i \in I$, car $A_i = 0 \cdot A_1 + 0 \cdot A_2 + ... + 1 \cdot A_i + ... + 0 \cdot A_n$. Donc, $\forall i \in \{1, ..., n\}, A_i \in I, A_i = D \cdot U_i$, avec $U_i \in \mathbb{K}[X]$. Donc D est un diviseur commun des A_i. Vérifions que D est plus grand diviseur commun des $A_i \in \mathbb{K}[X], i \in \{1, ..., n\}$. Soit D' un autre diviseur commun des A_i. Soit $A_i = D' \cdot U_i'$, où $U_i' \in \mathbb{K}[X]$, comme $I =< D >$, donc $D \in I$, donc $D = \sum_{i=1}^{n} A_i \cdot U_i = \sum_{i=1}^{n} D' U_i' U_i$, soit $D = D' \cdot (\sum_{i=1}^{n} U_i' U_i)$, et donc, D est le plus grand diviseur commun des A_i.

Théorème 4.1.4 (De Bézout) *Soient $A_1, A_2, ..., A_n$ des polynômes non nuls de $\mathbb{K}[X]$. Alors $A_1, A_2, ..., A_n$ sont premiers entre eux si et seulement s'il existe $U_1, U_2, ..., U_n \in \mathbb{K}[X]$ tel que $1_{\mathbb{K}[X]} = U_1 A_1 + U_2 A_2 + \cdots + U_n A_n$.*

Corollaire 4.1.1 *(Théorème de Gauss)*
Soient A, B et C trois polynômes . Si A divise $B \cdot C$ et si $pgcd(A, B) = 1$, alors A divise C.

Preuve. $pgcd(A, B) = 1$, d'après Bézout, $\exists U, V \in \mathbb{K}[X]$, tel que $U \cdot A + V \cdot B = 1$.
A divise $B \cdot C \Rightarrow \exists W \neq 0, W \in \mathbb{K}[X]$, tel que $BC = W \cdot A$.
$A \cdot U + B \cdot V = 1 \Rightarrow C \cdot A \cdot U + C \cdot B \cdot V = C$. Donc, $A \cdot C \cdot U + A \cdot W \cdot V = C$, soit $A[C \cdot U + W \cdot V] = C$. Si nous posons $U" = C \cdot U + W \cdot V \in \mathbb{K}[X]$, $AU" = C$. D'où A divise C.

Exemple 4.1.5 *On pose* $A_1 = X(X+1), A_2 = X(X+2), A_3 = (X+1)(X+2)$.

$$pgcd(A_1, A_2) = X$$

$$pgcd(A_1, A_3) = X + 1$$

$$pgcd(A_2, A_3) = X + 2$$

$$pgcd(A_1, A_2, A_3) = 1$$

Remarque 4.1.7 *Soient* $A, B \in \mathbb{K}[X]$ *tel que* $A = Q \cdot B + R$, *alors* $pgcd(A, B) = pgcd(B, R)$.

Recherche du pgcd : algorithme d'Euclide

Soient A et B deux polynômes tels que $B \neq 0$.

$$A = Q_1 B + R_1, \ avec \ deg(R_1) < deg(B)$$

$$B = R_1 Q_2 + R_2, \ avec \ deg(R_2) < deg(R_1)$$

$$R_1 = R_2 Q_3 + R_3, \ \text{avec} \ deg(R_3) < deg(R_2)$$

$$\vdots \quad \vdots \quad \vdots$$

$$R_{k-2} = R_{k-1} Q_k + R_k, \ \text{avec} \ deg(R_k) < deg(R_{k-1})$$

$$R_{k-1} = R_k Q_{k+1}.$$

Le degré du reste diminue à chaque division. On arrête l'algorithme lorsque le reste est nul. Le pgcd(A, B) est le dernier reste non nul R_k (rendu unitaire).

Exemple 4.1.6 *Calculons le pgcd de* $A = X^4 - 1$ *et* $B = X^3 - 1$.
On applique l'algorithme d'euclide :

$$X^4 - 1 = (X^3 - 1)X + X - 1$$

$$X^3 - 1 = (X - 1)(X^2 + X + 1) + 0$$

Comme le pgcd est le dernier reste non nul rendu unitaire, alors
$pgcd(X^4 - 1, X^3 - 1) = X - 1$.

Remarque 4.1.8 *Le pgcd des polynômes* $A_1, A_2, ..., A_n$ *s'obtient en prenant dans leurs décompositions en produit de facteurs irréductibles, les facteurs unitaires communs à chacune des décompositions.*

4.1.3.4 Fonctions polynômes

Définition 4.1.6 *Soit* $P = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{K}[X]$. *On appelle fonction polynôme associé à* P *l'application* $\tilde{p}$ *définie de* $\mathbb{K}$ *dans* $\mathbb{K}$ *associant à tout élément* $x \in \mathbb{K}$, *l'élément* $\tilde{p}(x) = a_0 + a_1x + \cdots + a_nx^n$

$$\begin{array}{rccc} \tilde{p} & : & \mathbb{K} & \longrightarrow & \mathbb{K} \\ & & x & \longmapsto & a_0 + a_1x + \cdots + a_nx^n \end{array}$$

Exemple 4.1.7 *Soit* $P = 2 + 5X - 5X^2 + 8X^3 \in \mathbb{R}[X]$. $\tilde{P}(x) = 2 + 5x - 5x^2 + 8x^3$ *est la fonction polynôme associée à* P .

4.1.3.5 Polynôme dérivé Soit $P = \sum_{k=0}^{n} a_kX^k \in \mathbb{K}[X]$. On appelle polynôme dérivé, tout polynôme :

$$\tilde{P} = \sum_{k=1}^{n} ka_kX^{k-1} = \sum_{j=0}^{n+1}(j+1)a_{j+1}X^j$$

Théorème 4.1.5 *(Formule de Leibniz pour les polynômes)*
Soient $P, Q \in \mathbb{K}[X]$ *deux polynômes. On a*

$$(PQ)^n = \sum_{k=0}^{n} C_n^k P^{(n-k)}Q^{(k)}$$

Théorème 4.1.6 *(Formule de Taylor pour les polynômes)*
Soient $P \in \mathbb{K}[X]$ un polynôme de degré inférieur ou égal à n et $a \in \mathbb{K}$. Alors on a,

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k$$

4.1.3.6 Racine d'un polynôme Soit $a \in \mathbb{K}$ et $p \in \mathbb{K}[X]$.

Définition 4.1.7 *On dit que a est racine ou zéro de P si $P(a) = a$.*

Remarque 4.1.9 *Si a est une racine de P, alors X - a divise P.*

Définition 4.1.8 *Soit $a \in \mathbb{K}et\ P \in \mathbb{K}[x]$. On dit que a est une racine multiple d'ordre k de P si $(X-a)^k$ divise P et $(X-a)^{k+1}$ ne divise pas P.*

Remarque 4.1.10
1. *Si $k = 1$, on dit que a est une racine simple de P.*
2. *Si $k = 2$, on dit que a est une racine double de P.*

Exemple 4.1.8 *$P = (X-a)(X-b)^2(X-c)^3$ avec $a, b, c \in \mathbb{R}$. a est racine simple de P, b est racine double de P, c est racine triple de P.*

Définition 4.1.9 *Soit $P \in \mathbb{K}[X]$ un polynôme non constant. On dit que P est scindé s'il existe $\lambda_1, \lambda_2, ..., \lambda_n \in \mathbb{K}$, tels que $P = \alpha(X-\lambda_1)(X-\lambda_2)\cdots(X-\lambda_n)$, avec $\alpha \in \mathbb{K}$, appelé coefficient dominant de P. les $\lambda_i, i \in \{1, ..., n\}$ sont appelés racines de P.*

Exemple 4.1.9 *$P = X^2 + 1$ est scindé dans $\mathbb{C}[X]$ car $P = (X-i)(X+i)$, mais il n'est pass scindé dans $\mathbb{R}[X]$.*

Définition 4.1.10 *(Polynômes irréductibles) On dit qu'un polynôme P de $\mathbb{K}[X]$ est irréductible ou premier sur $\mathbb{K}$ s'il n'est pas constant et si ses seuls diviseurs dans $\mathbb{K}[X]$ sont des polynômes associés à P, et les éléments non nuls de $\mathbb{K}$.*

Exemple 4.1.10
1. *$P = X^2 - 2$ est un polynôme irréductible dans $\mathbb{Q}[X]$, (car $\sqrt{2} \in \mathbb{Q}$),*

2. $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$ *n'est pas irréductible dans* $\mathbb{R}[X]$.

3. $X^2 + 1$ *est irréductible dans* $\mathbb{R}[X]$, *mais n'est pas irréductible dans* $\mathbb{C}[X]$.

Remarque 4.1.11 *1. Les polynômes irréductibles dans* $\mathbb{C}$ *sont les polynômes de degré 1.*

2. Les polynômes irréductibles dans $\mathbb{R}$ *sont :*

(i) les polynômes de degré 1.

(ii) les polynômes de degré 2 dont le discriminant est négatif.

Théorème 4.1.7 (De D'Alembert) *Soit* P *un polynôme de* $\mathbb{C}[X]$ *de degré supérieur où égal à 1. Alors il existe* $a \in \mathbb{C}$, *tel que* $P(a) = 0$. *On dit que* $\mathbb{C}$ *est algébriquement clos.*

Définition 4.1.11 *Soit* $\alpha_1, ..., \alpha_p \in \mathbb{K}$. *On définit les polynômes symétriques élémentaires en les variables* $\alpha_1, ..., \alpha_p$ *par :*

$$\begin{aligned}
\sigma_1 &= \alpha_1 + ... + \alpha_p \ \ (\textit{somme des racines}) \\
\sigma_2 &= \sum_{i_1 < i_2} \alpha_{i_1}\alpha_{i_2} = \alpha_1\alpha_2 + \alpha_1\alpha_3 + ... + \alpha_1\alpha_p + \alpha_2\alpha_3 + ... + \alpha_2\alpha_p + ... + \alpha_{p-1}\alpha_p \\
&... \\
&... \\
&... \\
\sigma_p &= \alpha_1\alpha_2...\alpha_p \ \ (\textit{produit des racines})
\end{aligned}$$

Plus précisément, pour tout $k \in \{1, ..., p\}$, *on a* $\sigma_k = \sum_{i_1 < ... < i_k} \alpha_{i_1}...\alpha_{i_k}$

Théorème 4.1.8 *(Relation entre les coéficients et les racines d'un polynôme) Soit* $Q = a_0 + a_1X + ... + a_pX^p \in \mathbb{K}[X]$ *un polynômes scindé de degré* p. *Soient* $\alpha_1, ..., \alpha_p \in \mathbb{K}$ *les* p *racines de* Q. *On a*

$$\forall k \in \{1, ..., p\},\ \sigma_k = (-1)^k \frac{a_{p-k}}{a_p}$$

Exemple 4.1.11 *1. Pour $p = 2$, on a $P = a_0 + a_1X + a_2X^2$*
Ainsi $P = a_2(X - \alpha_1)(X - \alpha_2) = a_2(X^2 - (\alpha_1 + \alpha_2)X + \alpha_1\alpha_2$
On a alors $\sigma_1 = \alpha_1 + \alpha_2 = -\frac{a_1}{a_2}$ et $\sigma_2 = \alpha_1\alpha_2 = \frac{a_0}{a_2}$.

2. Pour $p = 3$, on a $P = a_0 + a_1X + a_2X^2 + a_3X^3$
Ainsi $P = a_3(X - \alpha_1)(X - \alpha_2)(X - \alpha_3) = a_3(X^3 - (\alpha_1 + \alpha_2 + \alpha_3)X^2 + (\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3)X - \alpha_1\alpha_2\alpha_3$
On a alors $\sigma_1 = \alpha_1 + \alpha_2 + \alpha_3 = -\frac{a_2}{a_3}$, $\sigma_2 = \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3 = \frac{a_1}{a_3}$ et $\sigma_3 = \alpha_1\alpha_2\alpha_3 = -\frac{a_0}{a_3}$.

4.2 Fractions rationnelles

Soit $\mathbb{K}$ un corps commutatif, $\mathbb{K} = \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$.

4.2.1 Corps des fractions rationnelles

On définit sur $\mathbb{K}[X] \times \mathbb{K}[X]^*$ la relation binaire suivante par :

$$(A, B)\mathcal{R}(A', B') \Longleftrightarrow A \cdot B' = A' \cdot B.$$

$\mathcal{R}$ est une relation d'équivalence sur $\mathbb{K}[X] \times \mathbb{K}[X]^*$.

$$\mathbb{K}[X] \times \mathbb{K}[X]^*/\mathcal{R} = \{\widehat{(A, B)} : (A, B) \in \mathbb{K}[X] \times \mathbb{K}[X]^*\}$$

$$\widehat{(A, B)} = \{(C, D) \in \mathbb{K}[X] \times \mathbb{K}[X]^* : (C, D)\mathcal{R}(A, B)\}$$

Définition 4.2.1 *On appelle fraction rationnelle F, toute classe d'équivalence modulo $\mathcal{R}$.*

Remarque 4.2.1 *On dit aussi fraction rationnelle à une indéterminée X à coefficients dans $\mathbb{K}$.*

Note 4.2.1 *Si $(A, B) \in F$, on écrit : $F = \frac{A}{B} = A \cdot B^{-1}$; (A, B) est un représentant de la classe $F = \widehat{(A, B)}$.*

Exemple 4.2.1 $\frac{X+1}{X^2-1} = \frac{X-1}{X^2-2X+1}$, $(X-1, \overset{\circ}{\widehat{X^2-2X+1}}) = \frac{X-1}{X^2-2X+1}$. *De même,* $(X+\overset{\circ}{\widehat{1, X^2}}-1) = \frac{X+1}{X^2-1}$.

Note 4.2.2 *On note* $\mathbb{K}(X)$ *l'ensemble des fractions rationnelles à une indéterminée* X *à coefficients dans* $\mathbb{K}$.

4.2.2 Opérations sur $\mathbb{K}(X)$

Soient $\frac{A}{B}$ et $\frac{C}{D}$ deux éléments de $\mathbb{K}(X)$.

1. Addition $(+)$

$$\frac{A}{B} + \frac{C}{D} = \frac{AD+BC}{BD}$$

2. Multiplication $(\times)$

$$\frac{A}{B} \times \frac{C}{D} = \frac{AC}{BD}$$

Proposition 4.2.1 *1.* $(\mathbb{K}(X), +)$ *est un groupe abélien.*

2. $(\mathbb{K}(X), +, \times)$ *est un corps commutatif appelé corps des fractions rationnelles à une indéterminée* X*, et à coefficients dans* $\mathbb{K}$*, avec* $0_{\mathbb{K}(X)} = \frac{0}{B}$ *où* $B \neq 0$*,* $1_{\mathbb{K}(X)} = \frac{B}{B}$ *où* $B \neq 0$.

Définition 4.2.2 *On dit qu'une fraction rationnelle* $F = \frac{A}{B}$ *est irréductible si* $pgcd(A, B) = 1$.

Définition 4.2.3 *On appelle fonction rationnelle associée à la fraction rationnelle* $F = \frac{A}{B}$*, toute application :*

$$\begin{array}{rccc} \tilde{F} & : & \mathbb{K} & \longrightarrow & \mathbb{K} \\ & & x & \longmapsto & \tilde{F} = \frac{\tilde{A}(x)}{\tilde{B}(x)} \end{array}$$

où $\tilde{A}$ *est la fonction polynôme associée à* A*.* $\tilde{B}$ *la fonction polynôme associée à* B.

Définition 4.2.4 *1. On appelle pôle de la fraction rationnelle $F = \frac{A}{B}$, tout élément $\alpha \in \mathbb{K}$, tel que $B(\alpha) = 0$.*

2. On appelle pôle d'ordre k de $F = \frac{A}{B}$, toute racine d'ordre k de B.

3. L'ensemble $D_F = \mathbb{K} - \{\alpha \in \mathbb{K} : B(\alpha) = 0\}$ s'appelle le domaine de définition de la fraction rationnelle $F = \frac{A}{B}$.

4.2.3 Décomposition en éléments simples

4.2.3.1 Préliminaires

Théorème 4.2.1 *Soit F un élément de $\mathbb{K}(X)$. Alors, il existe un unique polynôme E tel que $F = E + R$ où R est une fraction rationnelle du dégré strictement négatif (i.e si $R = \frac{A}{B}$, on a : $deg(A) < deg(B)$).*

Définition 4.2.5 *Soit $F = \frac{A}{B} \in \mathbb{K}(X)$, $deg(F) = deg(A) - deg(B)$.*

Exemple 4.2.2 $F = \frac{X^3+X+2}{X^2+1} = X + \frac{2}{X^2+1}$.

Remarque 4.2.2 *Si $F = E + R$, E est dite partie entière (ou partie polynômiale) de F.*

Théorème 4.2.2 *Soit $F = \frac{P}{Q_1 \cdot Q_2 \cdots Q_n}$ une fraction rationnelle où les polynômes $Q_1, Q_2, ..., Q_n$ sont premiers entre eux et $deg(P) < deg(Q_1 \cdot Q_2 \cdots Q_n)$. Alors il existe une famille et une seule $(P_i)_{1 \leq i \leq n}$ de polynômes tels que*

$$\frac{P}{Q_1 \cdot Q_2 \cdots Q_n} = \sum_{i=1}^{n} \frac{P_i}{Q_i} \text{ et } deg(P_i) < deg(Q_i)$$

Exemple 4.2.3 $F = \frac{X^2+2}{(X-1)(X+1)(X^2+X+1)} = \frac{P_1}{X-1} + \frac{P_2}{X+1} + \frac{P_3}{X^2+X+1}$.

Définition 4.2.6 *On appelle élément simple de $\mathbb{K}(X)$, toute fraction rationnelle de la forme $\frac{A}{B^\alpha}$, où B est un polynôme irréductible de $\mathbb{K}[X]$ et α un entier supérieur ou égal à 1, avec $deg(A) < deg(B)$.*

Exemple 4.2.4 *1. Soit* $F_1 = \frac{a}{(X-b)^\alpha} \in \mathbb{R}(X), \alpha \in \mathbb{N}^*, (a,b) \in \mathbb{R}^2$. F_1 *est un élément simple de première espèce.*

2. $F_2 = \frac{aX+b}{(X^2+pX+q)^\beta} \in \mathbb{R}(X)$, *avec* $p^2 - 4q < 0$ *est un élément simple de seconde espace.*

3. Dans $\mathbb{C}(X)$, *les éléments simples sont de la forme* $\frac{a}{(X-b)^\gamma} \in \mathbb{C}(X), \alpha \in \mathbb{N}^*, (a,b) \in \mathbb{C}^2$.

Théorème 4.2.3 *Soit* $F = \frac{P}{Q^n} \in \mathbb{K}(X)$, $(n \in \mathbb{N}^*)$, *une fraction rationnelle telle que* $deg(P) < deg(Q^n)$, *alors il existe une famille et une seule de polynômes* $P_1, P_2, ..., P_n$ *telle que* $F = \sum_{i=1}^{n} \frac{P_i}{Q^i}$, *avec* $deg(P_i) < deg(Q_i)$ $(1 \leq i \leq n)$.

Exemple 4.2.5 $F = \frac{X^3+1}{(X-2)^4} = \frac{a_1}{(X-2)} + \frac{a_2}{(X-2)^2} + \frac{a_3}{(X-2)^3} + \frac{a_4}{(X-2)^4}$. *Il ne reste qu'à identifier les coefficients* a_1, a_2, a_3 *et* a_4.

Théorème 4.2.4 *Soit F un élément de* $\mathbb{K}(X)$ *écrit sous la forme* $F = \frac{P}{Q}$, *avec Q un polynôme de degré au moins égal à 1, et soit* $Q = \gamma \cdot A^\alpha \cdot B^\beta \cdots L^\lambda$ *la décomposition de Q en facteurs irréductibles. Alors, il existe une famille unique* $A_1, ..., A_\alpha, B_1, ..., B_\beta, L_1, ..., L_\lambda$, *telle que :*

$$\begin{aligned} F &= \frac{P}{Q} = \frac{P}{\gamma \cdot A^\alpha \cdot B^\beta \cdots L^\lambda} \\ &= E + \Big[\frac{A_1}{A} + \frac{A_2}{A^2} + \cdots + \frac{A_\alpha}{A^\alpha}\Big] \\ &\quad + \Big[\frac{B_1}{B} + \frac{B_2}{B^2} + \cdots + \frac{B_\beta}{B^\beta}\Big] \\ &\quad + \cdots + \Big[\frac{L_1}{L} + \frac{L_2}{L^2} + \cdots + \frac{L_\lambda}{L^\lambda}\Big] \end{aligned}$$

avec $deg(A_i) < deg(A)$ $(1 \leq i \leq \alpha)$; $deg(B_i) < deg(B)$ $(1 \leq i \leq \beta)$; $deg(L_i) < deg(L)$ $(1 \leq i \leq \lambda)$.

4.2.3.2 Décomposition en éléments simples dans $\mathbb{C}(X)$

Théorème 4.2.5 *Soit F un élément de* $\mathbb{C}(X)$ *écrit sous la forme* $F = \frac{P}{Q}, deg(Q) \geq 1$. $Q = \lambda(X-a_1)^{\alpha_1}(X-a_2)^{\alpha_2} \cdots (X-a_n)^{\alpha_n}$, *alors il existe un unique polynôme E tel*

que :

$$\begin{aligned} F &= \frac{P}{\lambda(X-a_1)^{\alpha_1}(X-a_2)^{\alpha_2}\cdots(X-a_n)^{\alpha_n}} \\ &= E+\sum_{i=1}^{n}\sum_{j=1}^{\alpha_i}\frac{b_{ij}}{(X-a_i)^j} \end{aligned}$$

avec $b_{ij}\in\mathbb{C}, \forall i=1,...,n; \forall j=1,...,\alpha_i$.

Exemple 4.2.6 $F=\frac{X^5}{(X-1)^2(X^2+1)}\in\mathbb{C}(X)$. *La division euclidienne donne :* $X^5=(X+2)((X-1)^2(X^2+1)+2X^3-2X^2+3X-2$, *donc* $F=X+2+F'$, *avec* $F'=\frac{2X^3-2X^2+3X-2}{(X-1)^2(X^2+1)}$. *D'après le théorème, il existe* $(a_1,a_2,a_3,a_4)\in\mathbb{C}^4$, *tels que*

$$F'=\frac{a_1}{X-1}+\frac{a_2}{(X-1)^2}+\frac{a_3}{(X-i)}+\frac{a_4}{(X+i)}$$

Déterminons les coefficients de la décomposition.

1. *On multiplie les deux membres par* $(X-1)^2$, *et ensuite on fait tendre* X *vers 1. On a : donc* $\frac{2X^3-2X^2+3X-2}{(X-i)(X+i)}=a_1(X-1)+a_2+(X-1)^2(\frac{a_3}{(X-i)}+\frac{a_4}{(X+i)})$, *ce qui donne* $a_2=\frac{1}{2}$.
2. *On multiplie par* $(X-i)$, *et on fait tendre* X *vers* i. *On a :* $a_3=\frac{i}{4}$.
3. *De même on multiplie par* $X+i$, *et on fait tendre* X *vers* $-i$, *on a :* $a_4=-\frac{i}{4}$.
4. *Il ne reste que* a_1, *qui donne quand on fait tendre* X *vers 0,* $a_1=2$.

Ainsi $F=\frac{X^5}{(X-1)^2(X^2+1)}=X+2+\frac{2}{X-1}+\frac{\frac{1}{2}}{(X-1)^2}+\frac{\frac{i}{4}}{(X-i)}+\frac{\frac{-i}{4}}{(X+i)}$

4.2.3.3 Décomposition d'une fraction rationnelle dans $\mathbb{R}(X)$

Soit $F=\frac{P}{Q}\in\mathbb{R}(X)$, avec :

$$Q=\lambda(X-a_1)^{\alpha_1}(X-a_2)^{\alpha_2}\cdots(X-a_n)^{\alpha_n}(X^2+\beta_1X+\delta_1)^{\gamma_1}(X^2+\beta_2X+\delta_2)^{\gamma_2}\cdots(X^2+\beta_mX+\delta_m)^{\gamma_m}$$

avec $\beta_j-4\delta_j<0, \forall j=1,...,m$.

Théorème 4.2.6 *Soit $F = \frac{P}{Q} \in \mathbb{R}(X)$, avec $deg(Q) \geq 1$. Alors il existe un unique polynôme E et des familles de réels $A_{ij}, \left(\begin{smallmatrix} 1 \leq i \leq n \\ 1 \leq j \leq \alpha_i \end{smallmatrix} \right)$ et $B_{kl}, \left(\begin{smallmatrix} 1 \leq k \leq m \\ 1 \leq l \leq \gamma_k \end{smallmatrix} \right)$ et $C_{kl}, \left(\begin{smallmatrix} 1 \leq k \leq m \\ 1 \leq l \leq \gamma_k \end{smallmatrix} \right)$, tels que :*

$$F = E + \sum_{i=1}^{n} [\sum_{j=1}^{\alpha_i} \frac{A_{ij}}{(X - a_i)^j}] + \sum_{k=1}^{n} [\sum_{l=1}^{\gamma_k} \frac{B_{kl}X + C_{kl}}{(X^2 + \beta_k X + \delta_k)^l}]$$

Exemple 4.2.7 *Soit $F = \frac{X^5}{(X-1)^2(X^2+1)} \in \mathbb{R}(X)$.*

$F = X + 2 + F'$, avec $F' = \frac{2X^3-2X^2+3X-2}{(X-1)^2(X^2+1)}$. D'après le théorème précédent, il existe $(a_1, a_2, b_1, b_2) \in \mathbb{R}^4$, tels que

$$F' = \frac{a_1}{X-1} + \frac{a_2}{(X-1)^2} + \frac{b_1 X + b_2}{(X^2+1)}$$

Déterminons les coefficients de la décomposition de F'.

1. *On multiplie les deux membres par $(X-1)^2$, et on fait tendre X vers 1. On trouve $a_2 = \frac{1}{2}$.*
2. *On multiplie par $(X - i)$ et on fait tendre X vers i. On a $b_1 i + b_2 = -\frac{1}{2}$, par identification, on obtient $b_1 = 0$ et $b_2 = -\frac{1}{2}$.*
3. *On multiplie par X et on fait tendre vers 0. On obtient : $a_2 = -2$.*

$$F = X + 2 - \frac{2}{X-1} + \frac{1}{2(X-1)^2} - \frac{1}{2(X^2+1)}$$

4.3 Exercices

Exercice 1. Effectuer les divisions euclidiennes de :

1. $3X^5 + 4X^2 + 1$ par $X^2 + 2X + 3$
2. $3X^5 + 2X^4 - X^2 + 1$ par $X^3 + X + 2$
3. $X^4 - X^3 + X - 2$ par $X^2 - 2X + 4$

Exercice 2. Trouver un polynôme P de degré < 3 tel que $P(1) = -2$, $P(-2) = 3$ et $P(0) = -1$

Exercice 3. Déterminer le PGCD des polynômes suivants :

1. $A = X^4 - 1$ et $B = X^3 - 1$
2. $A = X^5 + 3X^4 + 2X^3 - X^2 - 3X - 2$ et $B = X^4 + 2X^3 + X + 2$
3. $A = X^4 + X^3 - 3X^2 - 4X - 1$ et $B = X^3 + X^2 - X - 1$
4. $A = X^4 + X^3 - 2X + 1$ et $B = X^3 + X + 1$
5. $A = X^5 + 5X^4 + 9X^3 + 7X^2 + 5X + 3$ et $B = X^4 + 2X^3 + 2X^2 + X + 1$

Exercice 4.

1. Soient $A = X^5 + X^4 + 2X^3 + X^2 + X + 2$ et $B = X^4 + 2X^3 + X^2 - 4$.
   (a) Trouver le PGCD D des polynômes A et B.
   (b) Trouver des polynômes U et V tels que $D = AU + BV$
2. Soient $A = X^5 + 3X^4 + 2X^3 - X^2 - 3X - 2$ et $B = X^4 + 2X^3 + 2X^2 + 7X + 6$.
   (a) Trouver le PGCD D des polynômes A et B.
   (b) Trouver des polynômes U et V tels que $D = AU + BV$

Exercice 5. Décomposer en éléments simples sur $\mathbb{R}$

1. $\frac{X^4-8X^2+9X-7}{(X-2)^2(X+3)}$
2. $\frac{X^5-3X^4-X^3-9X^2-2X+1}{(X-2)^2(X+2)^2}$
3. $\frac{X^5+X^4+1}{X(X-1)^4}$
4. $\frac{X^2+1}{X^4-1}$
5. $\frac{X+2}{(X-1)(X^2+1)}$

6. $\frac{X^5-2X^3+4X^2-8X+11}{X^3-3X+2}$

Exercice 6. Décomposer en éléments simples sur $\mathbb{C}$

1. $\frac{1}{X^2+1}$
2. $\frac{X^4+1}{X^3-1}$
3. $\frac{X}{(X^2+1)(X^2+4)}$

Bibliographie

[1] **Annick Auzimour et Frédérique Petit**, Algèbre 1 Vuibert Supérieur Paris 1998.

[2] **Roger Godement**, Cours d'algèbre Hermann, Paris 1966.

[3] **J. Lelong Ferrand et J.M. Arnaudiees**, Algèbre 1, Dunod Université Bordas Paris 1978.

[4] **Jean Marie Monier**, Algèbre 1, Dunod, Paris 2000.

[5] **M. Queysanne**, Algèbre, Armand Colin, Pars 1964.

[6] **J. Rivaud**, Exercices d'algèbre, Tome 1, Librairie Vuibert, Paris 1973.