REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR
ET DE LA RECHERCHE SCIENTIFIQUE

USTO-MB- Oran

Polycopié de cours

Algèbre I

Présenté par :
Dr. ANBER Ahmed

Ce cours est destiné aux étudiants 1ère ANNEE M.I
Mathématiques & Informatique

Année Universitaire 2020 -2021

Table des matières

Avant-propos

Ce polycopié est destiné aux étudiants inscrit en première année système LMD, mathématiques et informatique.

Le contenu de ce polycopié, correspond au programme officiel de la matière Algèbre I enseigné en première année.

Le manuscrit contient cinq chapitres :
- Notions de logique
- Ensembles et applications
- Relations binaires sur un ensemble
- Structures algèbriques
- Anneaux de polynomes

Chapitre 1

Notions de Logique

1.1 Table de vérité

1.1.1 Proposition

Définition 1.1.1 *On appelle proposition (assertion) toute affirmation (énoncé) ayant un sens, et à laquelle on peut clairement attribuer la valeur « vrai » ou « faux ».*
Par exemple, « $1 \geq 3$ » est une proposition fausse, et « 17 est un nombre premier » est une proposition vraie.
Nous noterons par la suite $P, Q, R, ...$ des propositions.

1.1.2 Négation

Définition 1.1.2 *La négation de la proposition P, noté **nonP** ou $\overline{P}$, est la proposition qui affirme qu'elle est vraie si P est fausse, et fausse si P est vraie.*
Par exemple, la négation de la proposition P : « $1 \geq 3$ » est nonP : « $1 < 3$ ».

1.1.3 Table de vérité

Définition 1.1.3 *En notant **1**(ou **V**) la valeur « vrai » et **0** (ou **F**) la valeur « faux », on peut résumer l'état d'une proposition **P** par une table de vérité comme suit :*

P	non P
1	0
0	1

ou

P	non P
V	F
F	V

Tab 1 : Table de vérité de **P** et **non P.**

1.2 Equivalence

Soient P et Q deux propositions.

On dit que P et Q sont équivalentes si elles ont les mêmes valeurs de vérité. On note "$P \Leftrightarrow Q$" qui se lit " P équivalent à Q"

la table de vérité de l'équivalence logique "$P \Leftrightarrow Q$" est

P	**Q**	$P \Leftrightarrow Q$
1	1	1
1	0	0
0	1	0
0	0	1

Tab 2 : Table de vérité de (**P** $\Leftrightarrow$ **Q**)

Propriété 1.1

Soit P une proposition, alors la négation de la négation de la proposition P est équivalente à P.

$$\left(\overline{\overline{P}}\right) \Leftrightarrow (P)$$

1.3 Les connecteurs "ET" , "OU"

1.3.1 La Conjonction «∧»

Soient P et Q deux propositions.

La proposition "P et Q" notée par "$P \wedge Q$" est vraie si P et Q sont toutes les deux vraies et est fausse sinon.

On peut résumer l'état de proposition "$P \wedge Q$" par la table de vérité suivante :

P	**Q**	$P \wedge Q$
1	1	1
1	0	0
0	1	0
0	0	0

ou

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

Tab 3 : Table de vérité de **P** $\wedge$ **Q**

Propriété 1.2

Soit P une proposition, alors «$P \wedge \overline{P}$» est une proposition fausse.

Preuve il suffit de remarque que la table de vérités de $P \wedge \overline{P}$

P	$\overline{P}$	$P \wedge \overline{P}$
1	0	0
0	1	0

Tab 4 : Table de vérité de $P \wedge \overline{P}$

1.3.2 La disjonction «$\vee$»

Soient P et Q deux propositions.

La proposition "P ou Q" notée par "$P \vee Q$" est vraie si au moins l'une des deux propositions est vraie et est fausse sinon.

On peut résumer l'état de proposition "$P \vee Q$" par la table de vérité suivante :

P	**Q**	$P \vee Q$
1	1	1
1	0	1
0	1	1
0	0	0

ou

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

Tab 5 : Table de vérité de $\mathbf{P} \vee \mathbf{Q}$

Propriété 1.3

Soit P une proposition, alors «$P \vee \overline{P}$» est une proposition vraie.

Preuve il suffit de remarque que la table de vérités de $P \vee \overline{P}$

P	$\overline{P}$	$P \vee \overline{P}$
1	0	1
0	1	1

Tab 6 : Table de vérité de $P \vee \overline{P}$

Théorème 1.3.1 *(Règles de Morgan)*

Soient P et Q deux propositions, alors :

1. $\overline{P \wedge Q} \Leftrightarrow \overline{P} \vee \overline{Q}$.
2. $\overline{P \vee Q} \Leftrightarrow \overline{P} \wedge \overline{Q}$.

Preuve On établit la preuve de ces règles en donnant les valeurs de vérités des propositions logiques correspondantes.

P	Q	$\overline{P}$	$\overline{Q}$	$P \wedge Q$	$P \vee Q$	$\overline{P \wedge Q}$	$\overline{P \vee Q}$	$\overline{P} \vee \overline{Q}$	$\overline{P} \wedge \overline{Q}$
1	1	0	0	1	1	0	0	0	0
1	0	0	1	0	1	1	0	1	0
0	1	1	0	0	1	1	0	1	0
0	0	1	1	0	0	1	1	1	1

On voit que les propositions $\overline{P \wedge Q}$ et $\overline{P} \vee \overline{Q}$ ont les mêmes valeurs de vérité, donc elles sont équivalentes. De même pour $\overline{P \vee Q}$ et $\overline{P} \wedge \overline{Q}$.

Théorème 1.3.2 *Soient P , Q et R deux propositions, alors :*

1. $P \wedge Q \Leftrightarrow Q \wedge P$ et $P \vee Q \Leftrightarrow Q \vee P$.
2. $(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$ et $(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$.
3. $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$ et $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$.

(On dit que le «OU» et le «ET» sont commutatifs, associatifs et distributifs l'un sur l'autre).

Preuve

Démontrons par exemple la deuxième équivalence de 3 à l'aide d'une table de vérité (vous démontrerez le reste de manière analogue).

P	Q	R	$Q \wedge R$	$P \vee (Q \wedge R)$	$P \vee Q$	$P \vee R$	$(P \vee Q) \wedge (P \vee R)$
1	1	1	1	1	1	1	1
1	1	0	0	1	1	1	1
1	0	1	0	1	1	1	1
1	0	0	0	1	1	1	1
0	1	1	1	1	1	1	1
0	1	0	0	0	1	0	0
0	0	1	0	0	0	1	0
0	0	0	0	0	0	0	0

On lit effectivement les mêmes valeurs de vérité dans les quatrième et huitième colonnes.

1.4 Implication

Définition 1.4.1 *La proposition "$P \Rightarrow Q$ " est la proposition "nonP ou Q" qui se lit " P implique Q". Sa table de vérités est donnée par*

P	**Q**	$P \Rightarrow Q$
1	1	1
1	0	0
0	1	1
0	0	1

Tab 7 : Table de vérité de $\mathbf{P \Rightarrow Q}$

Contraposée et réciproque

Soient P et Q deux propositions.

– La contraposée de l'implication «$P \Rightarrow Q$» est l'implication « $NonQ \Rightarrow NonP$».

– La réciproque de l'implication «$P \Rightarrow Q$» est l'implication « $Q \Rightarrow P$».

Propriété 1.4

Une implication et sa contraposée sont équivalentes.

$$(P \Rightarrow Q) \Leftrightarrow (\text{Non}Q \Rightarrow \text{Non}P)$$

Preuve On peut utiliser deux manière différentes.

1. En utilisant les valeurs de vérité des implications «$P \Rightarrow Q$» et «Non$Q$ ⇒Non$P$», on obtient :

P	Q	Non$P$	Non$Q$	$P \Rightarrow Q$	Non$Q$ ⇒Non$P$
1	1	0	0	1	1
1	0	0	1	0	0
0	1	1	0	1	1
0	0	1	1	1	1

Tab 8 : Table de vérité de $P \Rightarrow Q$ et $NonQ \Rightarrow NonP$

On voit que les propositions «$P \Rightarrow Q$» et «Non$Q$ ⇒Non$P$» ont les mêmes valeurs de vérité, donc elles sont équivalentes.

2. En utilisant la définition de l'implication, on obtient :

$$(\text{Non}\,Q \Rightarrow \text{Non}\,P) \Leftrightarrow (\text{Non}\,(\text{Non}\,Q) \vee \text{Non}\,P)$$

$$\Leftrightarrow (Q \vee \text{Non}\,P)$$

$$\Leftrightarrow (P \Rightarrow Q)$$

Propriété 1.5

Soient P , Q et R deux propositions, alors :

$$((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)$$

Preuve Démontrons à l'aide d'une table de vérité.

P	Q	R	$\overbrace{P \Rightarrow Q}^{P_1}$	$\overbrace{Q \Rightarrow R}^{P_2}$	$\overbrace{P \Rightarrow R}^{P_3}$	$\overbrace{P_1 \wedge P_2}^{P_4}$	$P_4 \Rightarrow P_3$
1	1	1	1	1	1	1	1
1	1	0	1	0	0	0	1
1	0	1	0	1	1	0	1
1	0	0	0	1	0	0	1
0	1	1	1	1	1	1	1
0	1	0	1	0	1	0	1
0	0	1	1	1	1	1	1
0	0	0	1	1	1	1	1

Propriété 1.6

Soient P et Q deux propositions, alors :

La proposition "$P \Rightarrow Q$ et $Q \Rightarrow P$" est la proposition notée par "$P \Leftrightarrow Q$"

Preuve

En utilisant la table de vérités suivante :

P	Q	$\overbrace{P \Rightarrow Q}^{P_1}$	$\overbrace{Q \Rightarrow P}^{P_2}$	$P_1 \wedge P_2$	$P \Leftrightarrow Q$
1	1	1	1	1	1
1	0	0	1	0	0
0	1	1	0	0	0
0	0	1	1	1	1

On voit que les propositions «$(P \Rightarrow Q) \wedge (Q \Rightarrow P)$» et «$P \Leftrightarrow Q$» ont les mêmes valeurs de vérité, donc elles sont équivalentes.

1.5 CNS, SSI, Il faut et il suffit

Les expression «Condition nécessaire et suffisante (**C.N.S**)», «Si et seulement si (**SSI**)», «il faut et il suffit» signifient toutes « l'équivalance ».

$\Rightarrow$	$\Leftarrow$
Condition nécessaire Il faut Seulement si	Condition suffisante Il suffit Si

Considérons par exemple l'implication vraie :

$$(x+1)^2 = 4 \Leftarrow x+1 = 2.$$

Pour que $(x+1)^2$ soit égal à 4, il suffit que $x+1$ soit égal à 2, ou encore $(x+1)^2$ vaut 4 si $x+1$ vaut 2. Mais, pour que $(x+1)^2$ soit égal à 4, il n'est pas nécessaire, il n'est pas obligatoire que $x+1$ soit égal 2 (car $x+1$ peut aussi être égal à -2) ou encore l'égalité $(x+1)^2 = 4$ ne se produit pas seulement si $x+1$ vaut 2 (l'implication $(x+1)^2 = 4 \Rightarrow x+1 = 2$ est fausse).

1.6 Quantificateurs

On définit les deux symboles $\forall$ et $\exists$, appelés quantificateurs, de la manière suivante :

1.6.1 Quantificateur universel ($\forall$) : «Pour tout»

Une proposition P peut dépendre d'un paramètre x, par exemple «$x^2 + 2x \geq 0$», la proposition $P(x)$ est vraie ou fausse selon la valeur de x.

La proposition « $\forall x \in E \quad P(x)$ » est vraie lorsque les propositions $P(x)$ sont vraies pour tous les éléments x de l'ensemble E.

On lit : «Pour tout (Quelque soit) x appartenant à E, $P(x)$ »

Exemple 1.1

– « $\forall x \in \mathbb{R}, \ x^2 + 2x \geq 0$ » est une proposition fausse.

– « $\forall n \in \mathbb{N}, \ \frac{n(n+1)}{2} \in \mathbb{N}$ » est une proposition vraie.

1.6.2 Quantificateur existentiel : «Il existe»

La proposition « $\exists x \in E \;\; P(x)$ » est vraie lorsque l'on peut trouverau moins un x de E pour lequel $P(x)$ est vraie.

On lit : «Il existe x appartenant à E tel que $P(x)$ »

Exemple 1.2

– « $\exists x \in \mathbb{R}, \;\; x^2 + 2x \geq 0$ » est une proposition vraie.

– « $\exists z \in \mathbb{N}, \;\; z^2 + 2 \neq 0$ » est une proposition fausse.

Remarque 1.1

La proposition : «Il existe un et un seul élément x de E tel que la proposition $P(x)$ est vraie» s'écrit en abrégé «$\exists! x \in E,\, P(x)$».

1.6.3 La négation des quantificateurs

La négation de « $\forall x \in E \;\; P(x)$ » est « $\exists x \in E \;\; nonP(x)$ » et La négation de « $\exists x \in E$ $P(x)$ » est « $\forall x \in E \;\; nonP(x)$ ».

Exemple 1.3

– La négation de « $\forall x \in \mathbb{R}, \;\; x^2 + 2x \geq 0$ » est « $\exists x \in \mathbb{R}, \;\; x^2 + 2x < 0$ ».

– La négation de « $\exists z \in \mathbb{N}, \;\; z^2 + 2 \neq 0$ » est « $\forall z \in \mathbb{N}, \;\; z^2 + 2 = 0$».

Remarque 1.1

On peut distribuer $\forall$ sur «ET» et $\exists$ sur «OU» mais on ne peut pas distribuer $\forall$ sur «OU» et $\exists$ sur «ET».

1. $(\forall x \in E, P(x) \wedge Q(x)) \Leftrightarrow (\forall x \in E, P(x)) \wedge (\forall x \in E, Q(x))$.
2. $(\exists x \in E, P(x) \vee Q(x)) \Leftrightarrow (\exists x \in E, P(x)) \vee (\exists x \in E, Q(x))$.
3. $(\forall x \in E, P(x) \vee Q(x)) \Leftarrow (\forall x \in E, P(x)) \vee (\forall x \in E, Q(x))$.
4. $(\exists x \in E, P(x) \wedge Q(x)) \Rightarrow (\exists x \in E, P(x)) \wedge (\exists x \in E, Q(x))$.

On peut permuter des quantificateurs de même nature mais on ne peut pas permuter des quantificateurs de natures différentes.

1. $(\forall x \in E, \forall y \in E, P(x, y)) \Leftrightarrow (\forall y \in E, \forall x \in E, P(x, y))$.
2. $(\exists x \in E, \exists y \in E, P(x, y)) \Leftrightarrow (\exists y \in E, \exists x \in E, P(x, y))$.

1.7 Types de raisonnements

1.7.1 Raisonnement direct

Pour montrer que la proposition «$P \Rightarrow Q$» est vraie, on suppose que la proposition P est vraie et on montre qu'alors Q est vraie.

Exemple 1.4

Soit $n \in \mathbb{N}$, montrer que «si n est impair alors n^2 est impair».

Supposons que n est impair, alors il existe un entier naturel k tel que $n = 2k + 1$, Calculons alors n^2.

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2\left(2k^2 + 2k\right) + 1$$

Donc, il existe un entier naturel $p = 2k^2 + 2k$ tel que $n^2 = 2p + 1$,ce qui montre que n^2 est impair.

1.7.2 Disjonction de cas

Si l'on souhaite vérifier une proposition $P(x)$ pour tous les x dans un ensemble E , on montre la proposition pour les x dans une partie A de E , puis pour les x n'appartenant pas à A. C'est la méthode de disjonction ou du cas par cas.

Exemple 1.5 :

Montrer que pour tout $n \in \mathbb{N}$, $n(n+1)$ est divisible par 2.

Soit $n \in \mathbb{N}$, on peut distinguer deux cas

Premier cas : n est pair, $n = 2k$ avec $k \in \mathbb{N}$.

On a :

$$n(n+1) = 2k(2k+1) = 2k_1, \qquad avec\ k_1 = k(2k+1) \in \mathbb{N}.$$

d'où $n(n+1)$ est pair.

Deuxième cas : n est impair, $n = 2k + 1$ avec $k \in \mathbb{N}$.

On a :

$$n(n+1) = (2k+1)(2k+2) = 2k_2, \qquad avec\ k_2 = (k+1)(2k+1) \in \mathbb{N}.$$

d'où $n(n+1)$ est pair.

On déduit que pour tout $n \in \mathbb{N}$, $n(n+1)$ est divisible par 2.

Exemple 1.6

Montrer que «Pour tout $x \in \mathbb{R}, |x-1| \leq x^2 - x + 1$».

Soit $x \in \mathbb{R}$,

Premier cas : $x \geq 1$

$$x^2 - x + 1 - |x-1| = x^2 - x + 1 - (x-1)$$

$$= x^2 - 2x + 2$$

$$= (x+1)^2 + 1 \geq 0$$

et donc, $|x-1| \leq x^2 - x + 1$.

Deuxième cas : $x < 1$

$$x^2 - x + 1 - |x-1| = x^2 - x + 1 - (-x+1)$$

$$= x^2 \geq 0$$

et donc, $|x-1| \leq x^2 - x + 1$.

Conclusion : Dans tous les cas $|x-1| \leq x^2 - x + 1$.

1.7.3 Absurde

Le raisonnement par l'absurde pour montrer «$P \Rightarrow Q$ » repose sur le principe suivant : on suppose à la fois que P est vraie et que Q est fausse et on cherche une contradiction.

Exemple 1.7 :

Soient $x, y \in \mathbb{R}_+$, Montrer que : *si* $\frac{x}{y+1} = \frac{y}{x+1}$ *alors* $x = y$.

Supposons que $\frac{x}{y+1} = \frac{y}{x+1}$ et $x \neq y$ et on cherche une contraduction.

On a :

$$\frac{x}{y+1} = \frac{y}{x+1} \Rightarrow x(x+1) = y(y+1)$$

$$\Rightarrow x^2 + x - y^2 - y = 0$$

$$\Rightarrow (x-y)(x+y) + (x-y) = 0$$

$$\Rightarrow (x-y)(x+y+1) = 0$$

$$\Rightarrow x + y + 1 = 0, \ car \ \ x - y \neq 0$$

$$\Rightarrow x + y = -1$$

Qui est impossible, car la somme de deux nombres positifs ne peut être négative.(On obtient une contradiction).

Alors, d'aprés le principe de raisonnement par absurde, on déduit que *si* $\frac{x}{y+1} = \frac{y}{x+1}$ *alors* $x = y$.

Exemple 1.8 :

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

Supposons que est rationnel. Alors

$$\sqrt{2} = \frac{p}{q}$$

avec $p \in \mathbb{Z}, q \in \mathbb{Z}^*$ et p et q sont premiers entre eux ($p \gcd(p, q) = 1$).

On a :

$$\sqrt{2} = \frac{p}{q} \Rightarrow 2 = \frac{p^2}{q^2} \Rightarrow p^2 = 2q^2.$$

Commme $p^2 = 2q^2$ alors p^2 est pair, alors p est pair.

Comme p est pair, alors $\exists p_0 \in \mathbb{Z}$ tel que $p = 2p_0$.

Donc

$$p^2 = 2q^2 \Rightarrow (2p_0)^2 = 2q^2 \Rightarrow q^2 = 2p_0^2.$$

Commme $q^2 = 2p_0^2$ alors q^2 est pair, alors q est pair.

Comme q est pair, alors $\exists q_0 \in \mathbb{Z}^*$ tel que $q = 2q_0$.

Ce qui donne une contradiction, car $p \gcd(p, q) = 1$.

D'aprés le principe de raisonnement par absurde, on déduit que $\sqrt{2}$ est irrationnel.

1.7.4 Contraposée

Le raisonnement par contraposition est basé sur l'équivalence suivante :

$$(P \Rightarrow Q) \Leftrightarrow \left(\overline{Q} \Rightarrow \overline{P}\right)$$

Donc, pour mantrer que $P \Rightarrow Q$, on montre que si $\overline{Q}$ est vraie alors $\overline{P}$ est vraie.

Exemple 1.9

Soit $n \in \mathbb{N}$, montrer que «si n^2 est pair alors n est pair».

On sait que «si n^2 est pair alors n est pair» équivalente à «si n est impair alors n^2 est impair».

Et comme la proposition «si n est impair alors n^2 est impair» est vraie (Voir l'exemple 1.4), alors d'aprés le principe de raisonnement par contraposée, on déduit que «si n^2 est pair alors n est pair».

Exemple 1.10 :

Soit $a, b \in \mathbb{R}$. Montrer que

$$(a \neq 3 \ et \ b \neq 3) \Rightarrow (ab - 3a - 3b + 9 \neq 0)$$

Par contraposée, on démontre que

$$ab - 3a - 3b + 9 = 0 \Rightarrow (a = 3 \ ou \ b = 3)$$

On suppose que $ab-3a-3b+9=0$, donc

$$ab-3a-3b+9=0 \Rightarrow a(b-3)-3(b-3)=0$$

$$\Rightarrow (b-3)(a-3)=0$$

$$\Rightarrow (a=3 \quad ou \quad b=3)$$

Alors, d'aprés le principe de raisonnement par contaposée, on déduit que

$$(a\neq 3 \ et \ b\neq 3) \Rightarrow (ab-3a-3b+9\neq 0).$$

1.7.5 Contre exemple

Pour montrer qu'une proposition du type «$\forall x\in E \ \ P(x)$» est vraie, il faut montrer que pour chaque x de E, $P(x)$ est vraie. Par contre pour montrer que cette proposition est fausse il suffit de trouver $x\in E$ tel que $P(x)$ soit fausse. Trouver un tel x c'est trouver un contre-exemple à la proposition «$\forall x\in E \ \ P(x)$».

Exemple 1.11

Montrer que la proposition «$\forall x\in\mathbb{C}, \ \ x^2+1\neq 0$» est fausse.

Un contre exemple pour $x=i$ ou $x=-i$, on trouve $x^2+1=0$, ce qui montre que la proposition est fausse.

1.7.6 Récurrence

Leprincipe de récurrence permet de montrer qu'une proposition $P(n)$, dépendante de n, est vraie pour tout $n\geq n_0$ avec $n, n_0\in\mathbb{N}$.

La démonstration par récurrence se déroule en 3 étapes :

- *Etape 1-**Initialisation** : On prouve que $P(n_0)$ est vraie*
- *Etape 2-**Héridété :** On montre que $P(n)\Rightarrow P(n+1)$, on suppose que $P(n)$ vraie, et on démontre alors que la proposition $P(n+1)$ est vraie.*

- *Etape 3-**Conclusion :** On rappelle que, par le principe de récurrence, $P(n)$ est vraie pour tout entier naturel $n\geq n_0$.*

Exemple 1.12

Montrer que : $\forall n \in \mathbb{N}^*, \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$

Dans ce cas, on a : $n_0 = 1$ et la proposition $P(n)$ définie par $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$.

Etape 1-Initialisation : On prouve que $P(n_0)$ est vraie

Pour $n = 1$, on a :
$\sum_{k=1}^{n} k^2 = 1^2 = 1$ et $\frac{n(n+1)(2n+1)}{6} = \frac{1(1+1)(2\times1+1)}{6} = 1.$
Donc, la proposition est vraie pour le rang n_0.

Etape 2-Héridété : On montre que $P(n) \Rightarrow P(n+1)$

Supposons que la proposition $P(n)$ est vraie c'est à dire $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$ et montrons que la proposition $P(n+1)$ est vraie c'est à dire $\sum_{k=1}^{n+1} k^2 = \frac{(n+1)(n+2)(2n+3)}{6}$.

On a :

$$\sum_{k=1}^{n+1} k^2 = \left(\sum_{k=1}^{n} k^2\right) + (n+1)^2$$

$$= \frac{n(n+1)(2n+1)}{6} + (n+1)^2$$

$$= \frac{n+1}{6}\left(n(2n+1) + 6(n+1)\right)$$

$$= \left(\frac{n+1}{6}\right)(2n^2 + 7n + 6)$$

$$= \frac{(n+1)(n+2)(2n+3)}{6}.$$

Ce qui montre que la proposition $P(n+1)$ est vraie.

Etape 3-Conclusion : D'aprés le principe de raisonnement par récurrence la proposition $P(n)$ est vraie pour tout entier naturel $n \geq 1$.

Exemple 1.13 :

Montrer que

$$\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4}$$

On décompose la démonstration en trois étapes :

(i) **Initialisation :** on prouve $P(n_0)$ avec $n_0 = 1$.

On a :

$$\sum_{k=1}^{n_0} k^3 = (1)^3 = 1$$

et

$$\frac{n_0^2(n_0+1)^2}{4} = \frac{(1)^2(1+1)^2}{4} = 1$$

Ce qui montre que $P(n_0)$ est vraie.

(ii) **Hérédité** :

On suppose que $P(n)$ vraie, c.à.d

$$\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4}$$

et on démontre alors que la proposition $P(n+1)$ est vraie, c.à.d

$$\sum_{k=1}^{n+1} k^3 = \frac{(n+1)^2(n+2)^2}{4}$$

On a

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

$$= \frac{n^2(n+1)^2}{4} + (n+1)^3$$

$$= (n+1)^2 \left(\frac{n^2}{4} + (n+1)\right)$$

$$= (n+1)^2 \left(\frac{n^2+4n+4}{4}\right)$$

$$= \frac{(n+1)^2(n+2)^2}{4}$$

d'où la proposition $P(n+1)$ est vraie

(iii) **Conclusion** : on rappelle que par le principe de récurrence $P(n)$ est vraie pour tout $n \geq n_0$, $n_0 \in \mathbb{N}$.

D'aprés le principe de raisonnement par récurrence la proposition $P(n)$ est vraie pour tout entier naturel non nul.

1.8 Exercices

Exercice 1

Soient f et g deux fonctions de $\mathbb{R}$ dans $\mathbb{R}$. Traduire en termes de quantificateurs les expressions suivantes puis donner leurs négations.

1. f est majorée.
2. f est bornée.
3. f est croissante.
4. f est strictement décroissante.
5. f ne s'annule jamais.
6. f est inférieur à g.

Solution

– P_1 :«f est majorée»

$$\exists M \in \mathbb{R}, \forall x \in \mathbb{R}; f(x) \leq M$$

Sa négation est :

$$\overline{P_1} : \text{«}\forall M \in \mathbb{R}, \exists x \in \mathbb{R}; f(x) > M\text{»}$$

– P_2 :«f est bornée»

$$\exists m, M \in \mathbb{R}, \forall x \in \mathbb{R}; m \leq f(x) \leq M$$

ou

$$\exists A \in \mathbb{R}^+, \forall x \in \mathbb{R}; |f(x)| \leq A$$

Sa négation est :

$$\overline{P_2} : \text{«}\forall m, M \in \mathbb{R}, \exists x \in \mathbb{R}; (f(x) > M) \text{ ou } (f(x) < m)\text{»}$$

– P_3 :«f est croissante»

$$\forall a, b \in \mathbb{R}, a \leq b \Rightarrow f(a) \leq f(b)$$

Sa négation est :

$$\overline{P_3} : \text{«}\exists a, b \in \mathbb{R}, (a \leq b) \wedge (f(a) > f(b))\text{»}$$

– P_4 :«f est strictement décroissante»

$$\forall a, b \in \mathbb{R}, a < b \Rightarrow f(a) > f(b)$$

Sa négation est :

$$\overline{P_4} : \text{«}\exists a, b \in \mathbb{R}, (a < b) \wedge (f(a) \leq f(b))\text{»}$$

– P_5 :«f ne s'annule jamais»

$$\forall x \in \mathbb{R}, f(x) \neq 0$$

Sa négation est :

$$\overline{P_5} : \text{«}\exists x \in \mathbb{R}, f(x) = 0\text{»}$$

– P_6 :«f est inférieur à g»

$$\forall x \in \mathbb{R}, f(x) \leq g(x)$$

Sa négation est : $\overline{P_6}$: «$\exists x \in \mathbb{R}, f(x) > g(x)$ »

Exercice 2 :

Dans chacun des cas suivants, dire si la proposition est vraie ou fausse puis la nier :

1. $(\forall x \in \mathbb{R}\ ), (2x \geq x)$.
2. $(\forall x \in \mathbb{R}), (x > 0 \Rightarrow 2x \geq x)$
3. $(\exists x \in \mathbb{N})$,$(5x + 11 = 3x + 14)$.
4. $(2 + 6 = 5\ ) \wedge (3 - 1 = 2)$.
5. $(2 + 6 = 5\ ) \vee (3 - 1 = 2)$.
6. $(2 + 6 = 5\ ) \Rightarrow (3 - 1 = 2)$.
7. $(\forall x \in \mathbb{C}\ ), (x^2 + 1 \neq 0)$.

Solution :

Dans chacun des cas suivants, dire si la proposition est vraie ou fausse puis la nier :

1. La proposition $P_1 : (\forall x \in \mathbb{R}\ ), (2x \geq x)$ est fausse, car il existe $x \in \mathbb{R}$ tel que $2x < x$ (on peut prendre par exemple $x \in]-\infty, 0[$).

Sa négation est

$$\overline{P_1} : (\exists x \in \mathbb{R}), (2x < x)$$

2. La proposition $P_2 :(\forall x \in \mathbb{R}), (x > 0 \Rightarrow 2x \geq x)$ est vraie, car pour tout $x \in \mathbb{R}$, on a $x \leq 0$ ou $2x \geq x$.

Sa négation est

$$\overline{P_2} : (\exists x \in \mathbb{R}), (x > 0 \wedge 2x < x)$$

3. La proposition $P_3 :(\exists x \in \mathbb{N})\ ,(5x + 11 = 3x + 14)$ est fausse, car la solution de l'équation $5x + 11 = 3x + 14$ est $x = \frac{3}{2} \notin \mathbb{N}$.

Sa négation est

$$\overline{P_3} : (\forall x \in \mathbb{N}), (5x + 11 \neq 3x + 14)$$

4. La proposition $P_4 :(2 + 6 = 5\ ) \wedge (3 - 1 = 2)$ est fausse, car P_4 est une conjonction de deux proposition, V et F donne F.

Sa négation est

$$\overline{P_4} : (2 + 6 \neq 5) \vee (3 - 1 \neq 2)$$

5. La proposition P_5 :$(2+6=5\ ) \vee (3-1=2)$ est fausse, car P_4 est une disjonction de deux proposition, V ou F donne V.

Sa négation est

$$\overline{P_5} : (2+6 \neq 5) \wedge (3-1 \neq 2)$$

6. La proposition P_6 :$(2+6=5\ ) \Rightarrow (3-1=2)$ est vraie.

Sa négation est

$$\overline{P_6} : (2+6=5) \wedge (3-1 \neq 2)$$

7. La proposition P_7 :$(\forall x \in \mathbb{C}\ ),\ (x^2+1 \neq 0)$ est fausse, car il existe $x = \pm i \in \mathbb{C}$ tel que $x^2+1=0$.

Sa négation

$$\overline{P_7} : (\exists x \in \mathbb{C}), (x^2+1=0)$$

Exercice 3 :

Soient P_1, P_2, P_3 et P_4 trois propositions telles que :

$P_1 : \forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x \geq y$.

$P_2 : \forall x \in \mathbb{R}, x^2 - 4 \geq 0$.

$P_3 : \forall x \in \mathbb{R}, \forall y \in \mathbb{R}$ *si* $x \geq y$ *alors* $x^2 + y^2 \geq 0$.

$P_4 : \forall x \in \mathbb{R}, \forall y \in \mathbb{R}$, si $x \geq y$ alors $(x+y)^2 + 1 \geq 0$.

1. Les propositions P_1, P_2, P_3, P_4 sont-elles vraies ou fausses ?

2. Donner leurs négation.

Solution :

1. Les propositions P_1, P_2, P_3, P_4 sont-elles vraies ou fausses ?

- P_1 est une proposition vraie, car pour tout $x \in \mathbb{R}$, on peut prendre $y = x - 1$.

- P_2 est une proposition fausse, car pour $x = 0 \in \mathbb{R}, x^2 - 4 = -4 < 0$.

- P_3 est une proposition vraie, car pour tout $x, y \in \mathbb{R}$, on a

$$x \geq y \Rightarrow x^2 \geq y^2$$

$$\Rightarrow x^2 + y^2 \geq 2y^2$$

et comme $y^2 \geq 0$ alors $x^2 + y^2 \geq 0$.

- La proposition $P_4 : \forall x \in \mathbb{R}, \forall y \in \mathbb{R}$, si $x \geq y$ alors $(x+y)^2 + 1 \geq 0$ est vraie, car si $x \geq y$ alors $x + y \geq 2y$ et par suite $(x+y)^2 \geq 4y^2$ ce qui donne $(x+y)^2 + 1 \geq 4y^2 + 1$ et comme $4y^2 + 1 \geq 0$, alors $(x+y)^2 + 1 \geq 0$.

2. La négation.

- La négation de P_1 est

$$\overline{P_1} : \exists x \in \mathbb{R}, \forall y \in \mathbb{R}, x < y$$

- La négation de P_2 est

$$\overline{P_2} : \exists x \in \mathbb{R}, x^2 - 4 < 0$$

- La négation de P_3 est

$$\overline{P_3} : \exists x \in \mathbb{R}, \exists y \in \mathbb{R}, (x \geq y) \wedge (x^2 + y^2 < 0)$$

- La négation de P_4 est

$$\overline{P_4} : \exists x \in \mathbb{R}, \exists y \in \mathbb{R}, (x \geq y) \wedge ((x+y)^2 + 1 < 0)$$

Exercice 4

Ecrire les contraposées des implications suivantes et les démontrer. n est un entier naturel, x et y sont des nombres réels

1. $(x \neq y) \Rightarrow (x+1)(y-1) \neq (x-1)(y+1)$.
2. $(xy \neq 0) \Rightarrow x \neq 0$ et $y \neq 0$.
3. n premier$\Rightarrow n = 2$ ou n est impair

Solution Soient $n \in \mathbb{N}$ et $x, y \in \mathbb{R}$

On sait que la contraposée de l'implication $(P \Rightarrow Q)$ est $\left(\overline{Q} \Rightarrow \overline{P}\right)$ et de plus on a :

$$(P \Rightarrow Q) \Leftrightarrow \left(\overline{Q} \Rightarrow \overline{P}\right)$$

1. La contraposée de $(x \neq y) \Rightarrow (x+1)(y-1) \neq (x-1)(y+1)$ est

$$(x+1)(y-1) = (x-1)(y+1) \Rightarrow x = y$$

Supposons que $(x+1)(y-1) = (x-1)(y+1)$, alors

$$xy - x + y - 1 = xy + x - y - 1 \Rightarrow -x + y = x - y$$

$$\Rightarrow 2x = 2y$$

$$\Rightarrow x = y$$

2. La contraposée de $(xy \neq 0) \Rightarrow x \neq 0$ et $y \neq 0$ est

$$x = 0 \text{ ou } y = 0 \Rightarrow xy = 0$$

Supposons que $x = 0$ ou $y = 0$, alors $xy = 0$ (Triviale).

3. La contraposée de «n premier$\Rightarrow$ $n=2$ ou n est impair» est

$$(n \neq 2 \text{ et } n \text{ pair}) \Rightarrow (n \text{ non premier})$$

Supposons que $n \neq 2$ et n pair, alors 2 divise n, donc n n'est pas premier.

Exercice 5

Montrer en utilisant le principe de raisonnement par l'absurde que :

1. Pour tout réel $x \neq 3$ on a : $\frac{1+2x}{3-x} \neq -2$.
2. Si $x, y \geq 0$ tel que $\frac{x}{y+1} = \frac{y}{x+1}$,alors $x = y$.
3. Si a et b sont deux entiers relatifs tels que $a + b\sqrt{2} = 0$,alors $a = b = 0$.

Solution

1. Pour tout réel $x \neq 3$ on a : $\frac{1+2x}{3-x} \neq -2$

Soit $x \neq 3$, supposons que $\frac{1+2x}{3-x} = -2$ et on cherche une contradiction.

On a :

$$\frac{1+2x}{3-x} = -2 \Leftrightarrow 1 + 2x = -2(3 - x)$$

$$\Leftrightarrow 1 + 2x = -6 + 2x$$

$$\Leftrightarrow 1 = -6$$

qui est impossible.

Alors, D'aprés le principe de raisonnement par l'absurde, on a : Pour tout réel $x \neq 3$ on a : $\frac{1+2x}{3-x} \neq -2$.

2. Si $x, y \geq 0$ tel que $\frac{x}{y+1} = \frac{y}{x+1}$,alors $x = y$.

Soient $x, y \geq 0$.

Supposons que $\frac{x}{y+1} = \frac{y}{x+1}$ et $x \neq y$ et on cherche une contradiction.

On a :

$$\frac{x}{y+1} = \frac{y}{x+1} \Leftrightarrow x(x+1) = y(y+1)$$

$$\Leftrightarrow x^2 + x = y^2 + y$$

$$\Leftrightarrow x^2 - y^2 + x - y = 0$$

$$\Leftrightarrow (x-y)(x+y) + (x-y) = 0$$

$$\Leftrightarrow (x-y)(x+y+1) = 0$$

et comme $x \neq y$, alors $x - y \neq 0$. Donc

$$x + y + 1 = 0 \Leftrightarrow x + y = -1$$

C'est une contradiction, car la somme des deux nombres positifs ne peut être négative.

Conclusion : D'aprés le principe de raisonnement par l'absurde, «Si $x, y \geq 0$ tel que $\frac{x}{y+1} = \frac{y}{x+1}$,alors $x = y$».

3. Si a et b sont deux entiers relatifs tels que $a + b\sqrt{2} = 0$,alors $a = b = 0$.

Soient a, b deux relatifs.

Supposons que $a + b\sqrt{2} = 0$ et $(a, b) \neq (0, 0)$ et on cherche une contradiction.

Alors nécessairement $b \neq 0$ car si $b = 0$ alors on devrait aussi avoir $a = 0$, ce qui est contraire à l'hypothèse $(a, b) \neq (0, 0)$.

Mais alors, on a : :

$$a + b\sqrt{2} = 0 \Leftrightarrow \sqrt{2} = -\frac{a}{b} \in \mathbb{Q}$$

Ce qui est faux.

Conclusion : D'aprés le principe de raisonnement par l'absurde, «Si a et b sont deux entiers relatifs tels que $a + b\sqrt{2} = 0$,alors $a = b = 0$».

Exercice 6 :

Montrer en utilisant le principe de raisonnement par contraposée que :

soit $n \in \mathbb{N}$

$$n^2 - 1 \text{ n'est pas divisible par } 8 \Rightarrow n \text{ est pair}$$

Solution :

Soit $n \in \mathbb{N}$

$$n^2 - 1 \text{ n'est pas divisible par } 8 \Rightarrow n \text{ est pair}$$

Par contraposée, on démontre que

$$n \text{ est impair} \Rightarrow n^2 - 1 \text{ est divisible par } 8$$

Soit n est impair, alors $n = 2k + 1$ avec $k \in \mathbb{N}$.

Pour $k = 2p$ (le ca où k est pair), on a $n = 2k + 1 = 4p + 1$, par suite

$$\begin{aligned} n^2 - 1 = & \ (4p+1)^2 - 1 \\ & = (16p^2 + 8p + 1) - 1 \\ & = 8\left(2p^2 + p\right) \end{aligned}$$

ce qui montre que $n^2 - 1$ est divisible par 8.

Pour $k = 2p + 1$ (le ca où k est impair), on a $n = 2k + 1 = 4p + 3$, par suite

$$\begin{aligned} n^2 - 1 = & \ (4p+3)^2 - 1 \\ & = (16p^2 + 24p + 9) - 1 \\ & = 8\left(2p^2 + 3p + 1\right) \end{aligned}$$

ce qui montre que $n^2 - 1$ est divisible par 8.

D'aprés le principe de raisonnement par contaposée, on déduit que

$$n^2 - 1 \text{ n'est pas divisible par } 8 \ \Rightarrow \ n \text{ est pair}$$

Exercice 7 :

Montrer en utilisant le principe de raisonnement par récurrence que :

1. Pour tout entier naturel non nul,

$$\sum_{k=1}^{n} \frac{k}{2^k} = 2 - \frac{n+2}{2^n}$$

2. Pour tout entier naturel non nul,

$$\sum_{k=1}^{n} k.k! = (n+1)! - 1.$$

3. Pour tout entier naturel n, $n^3 - n$ est divisible par 6.

Solution :

Pour tout entier naturel non nul, on a :

1.

$$\sum_{k=1}^{n} \frac{k}{2^k} = 2 - \frac{n+2}{2^n}$$

(i) **Initialisation :** On prouve que $P(n_0)$ est vraie avec $n_0 = 1$.

On a :

$$\sum_{k=1}^{n_0} \frac{k}{2^k} = \frac{1}{2^1} = \frac{1}{2}$$

et

$$2 - \frac{n_0+2}{2^{n_0}} = 2 - \frac{1+2}{2^1} = \frac{1}{2}$$

Ce qui montre que $P(n_0)$ est vraie.

(ii) **Hérédité** : $P(n) \Rightarrow P(n+1)$?

On suppose que $P(n)$ vraie, c.à.d

$$\sum_{k=1}^{n} \frac{k}{2^k} = 2 - \frac{n+2}{2^n}$$

et on démontre alors que la proposition $P(n+1)$ est vraie, c.à.d

$$\sum_{k=1}^{n+1} \frac{k}{2^k} = 2 - \frac{n+3}{2^{n+1}}$$

On a

$$\sum_{k=1}^{n+1}\frac{k}{2^k} = \underbrace{\left(\frac{1}{2}\right)+\left(\frac{2}{4}\right)+...+\left(\frac{n}{2n}\right)}_{\sum_{k=1}^{n}\frac{k}{2^k}} + \left(\frac{n+1}{2^{n+1}}\right)$$

$$= 2 - \frac{n+2}{2^n} + \left(\frac{n+1}{2^{n+1}}\right)$$

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

$$= 2 - \frac{n+3}{2^{n+1}}$$

d'où la proposition $P(n+1)$ est vraie

(iii) **Conclusion** : D'aprés le principe de raisonnement par récurrence la proposition $P(n)$ est vraie pour tout entier naturel non nul.

2. $\forall n \in \mathbb{N}^*$,

$$\sum_{k=1}^{n} k.k! = (n+1)! - 1.$$

Dans ce cas, on a : $n_0 = 1$ et la proposition $P(n)$ définie par $\sum_{k=1}^{n} k.k! = (n+1)! - 1$.

Etape 1-Initialisation : On prouve que $P(n_0)$ est vraie

Pour $n = 1$, on a :

$\sum_{k=1}^{n} k.k! = 1.1! = 1$ et $(n+1)! - 1 = (1+1)! - 1 = 1.$

Donc, la proposition est vraie pour le rang n_0.

Etape 2-Héridété : On montre que $P(n) \Rightarrow P(n+1)$

Supposons que la proposition $P(n)$ est vraie c'est à dire $\sum_{k=1}^{n} k.k! = (n+1)! - 1$ et montrons que la proposition $P(n+1)$ est vraie c'est à dire $\sum_{k=1}^{n+1} k.k! = (n+2)! - 1$.

On a :

$$\sum_{k=1}^{n+1} k.k! = \left(\sum_{k=1}^{n} k.k!\right) + (n+1)(n+1)!$$

$$= (n+1)! - 1 + (n+1)(n+1)!$$

$$= ((n+1)!)(1 + (n+1)) - 1$$

$$= ((n+1)!)(n+2) - 1$$

$$= (n+2)! - 1.$$

Ce qui montre que la proposition $P(n+1)$ est vraie.

Etape 3-Conclusion : D'aprés le principe de raisonnement par récurrence la proposition $P(n)$ est vraie pour tout entier naturel $n \geq 1$.

3. Pour tout entier naturel n, $n^3 - n$ est divisible par 6.

Dans ce cas, on a : $n_0 = 0$ et la proposition $P(n)$ définie par $n^3 - n$ est divisible par 6.

Etape 1-Initialisation : On prouve que $P(n_0)$ est vraie

Pour $n = 1$, on a :

$n^3 - n = 0 = 6 \times 0$.

Donc, la proposition est vraie pour le rang n_0.

Etape 2-Héridété : On montre que $P(n) \Rightarrow P(n+1)$

Supposons que la proposition $P(n)$ est vraie c'est à dire $n^3 - n$ est divisible par 6 et montrons que la proposition $P(n+1)$ est vraie c'est à dire $(n+1)^3 - (n+1)$ est divisible par 6.

On a :

$$(n+1)^3 - (n+1) = n^3 + 3n + 3n^2 + 1 - n - 1$$

$$= (n^3 - n) + 3n + 3n^2$$

$$= (n^3 - n) + 3n(n+1)$$

On sait que $n(n+1)$ est pair, donc il existe un entier naturel k tel que $n(n+1) = 2k$.

Alors,

$$(n+1)^3 - (n+1) = 6p + 6k$$

Donc, il existe un entier naturel s tel que $(n+1)^3 - (n+1) = 6s$. D'où $(n+1)^3 - (n+1)$ est divisible par 6.

Ce qui montre que la proposition $P(n+1)$ est vraie.

Etape 3-Conclusion : D'aprés le principe de raisonnement par récurrence la proposition $P(n)$ est vraie pour tout entier naturel n.

Chapitre 2

Ensembles et Applications

2.1 Ensembles

2.1.1 Définitions et exemples

Définition 2.1 *Un ensemble est une collection d'objets, ces objets s'appellent les éléments de l'ensemble.*

- *Nous désignerons en général les ensembles par des lettres majuscules : E, F, A, B,etc. Les éléments d'un ensemble seront désignés en général par des lettres minuscules : a, b, x, y, etc.*
- *Si a est un élément d'un ensemble E, on écrit $a \in E$ et on lit «a appartient à E».*
- *Si a n'est pas un élément d'un ensemble E, on écrit $a \notin E$ et on lit «a n'appartient pas à E».*

Définition 2.2 *L'ensemble vide noté $\varnothing$, c'est l'ensemble qui ne contenant aucun élément.*

Exemble 2.1

- $\mathbb{N} = \{0, 1, 2, ...\}$ est l'ensemble des entiers naturels.
- $\mathbb{Z} = \{..., -1, 0, 1, ...\}$ est l'ensemble des entiers relatifs.
- $\mathbb{R}$ est l'ensemble des nombres réels.

Exemble 2.2

Soit

$$E = \{x \in \mathbb{N} / x \leq 8\}$$

E est un ensemble défini par

$$E = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$$

Le nombre d'éléments de E est fini, on l'appelle **cardinal de** E et on note $Card\,(E) = 9$.

2.1.2 Parties d'un ensemble et complémontaire

Définition 2.3 *On dit qu'un ensemble F est une partie d'un ensemble E ou que F est inclus dans E ou que F est un sous ensemble de E, si tout élément de F est un élément de E et on note $F \subset E$.*

$$(F \subset E) \Leftrightarrow (\forall a, a \in F \Rightarrow a \in E)$$

Définition 2.4 *On dit que l'ensemble E égal à l'ensemble F si on a : $(E \subset F)$ et $(F \subset E)$.*

$$(E = F) \Leftrightarrow ((E \subset F) \wedge (F \subset E))$$

– *L'ensemble des parties de E est noté par $P\,(E)$.*

$$A \in P\,(E) \Leftrightarrow A \subset E$$

– *Si E possède n élément, alors $P(E)$ possède 2^n.*

Exemple 2.3

Soit

$$E = \{a, b, c, d\}$$

On a $Card(E) = 4$ donc $Card(P(E)) = 2^4 = 16$.

$$P(E) = \left\{ \begin{array}{c} \varnothing, \{a\}, \{b\}, \{c\}, \{d\}, \{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \\ \\ \{c, d\}, \{a, b, c\}, \{a, b, d\}, \{a, c, d\}, \{b, c, d\}, \{a, b, c, d\}, \end{array} \right\}$$

Définition 2.5 *Soient E un ensemble et A une partie de E. On appelle complémentaire de A dans E, l'ensemble des éléments de E qui n'appartiennent pas à A et on note $C_E A$.*

$$C_E A = \{a \in E / a \notin A\}$$

Propriété 2.1

Soient A, B deux parties d'un ensemble E.

1. $C_E\,(C_E A) = A$, $C_E \varnothing = E$, $C_E E = \varnothing$.

2. *Si* $A \subset B$ *alors* $C_E B \subset C_E A$.

Preuve

Soient A, B deux parties d'un ensemble E telles que $A \subset B$, alors

$$A \subset B \Leftrightarrow \forall a, a \in A \Rightarrow a \in B$$

$$\Leftrightarrow \forall a, a \notin B \Rightarrow a \notin A$$

$$\Leftrightarrow \forall a, a \in C_E B \Rightarrow a \in C_E A$$

$$\Leftrightarrow C_E B \subset C_E A$$

2.1.3 Intersection et réunion

Définition 2.6 *On appelle intersection de deux ensembles* E *et* F*, et on note* $E \cap F$*, l'ensemble des éléments* x *tels que* $x \in E$ *et* $x \in F$.

$$E \cap F = \{x : x \in E \ \ et \ \ x \in F\}$$

Si $E \cap F = \varnothing$*, on dit que* E *et* F *sont disjoint.*

Définition 2.7 *On appelle réunion de deux ensembles* E *et* F*, et on note* $E \cup F$*, l'ensemble des éléments* x *tels que* $x \in E$ *ou* $x \in F$.

$$E \cup F = \{x : x \in E \ \ \text{ou} \ \ x \in F\}$$

Propriété 2.2

Soient A, B *et* C *trois ensembles.*

1. $A \cap B = B \cap A, \ \ A \cup B = B \cup A$.
2. $A \subset A \cup B, \ \ B \subset A \cup B$.
3. $A \cap B \subset A, \ \ A \cap B \subset B$.
4. $A \cap (B \cap C) = (A \cap B) \cap C, \ \ A \cup (B \cup C) = (A \cup B) \cup C$.
5. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \ \ A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Preuve Soient A, B et C trois ensembles.

1. Soit $x \in A \cap B$, on a :

$$x \in A \cap B \Leftrightarrow (x \in A) \wedge (x \in B)$$

$$\Leftrightarrow (x \in B) \wedge (x \in A)$$

$$\Leftrightarrow x \in B \cap A$$

d'où $A \cap B = B \cap A$.

Soit $x \in A \cup B$, on a :

$$x \in A \cup B \Leftrightarrow (x \in A) \vee (x \in B)$$

$$\Leftrightarrow (x \in B) \vee (x \in A)$$

$$\Leftrightarrow x \in B \cup A$$

d'où $A \cup B = B \cup A$.

2.3. Trivial.

4. Soit $x \in A \cap (B \cap C)$

$$x \in A \cap (B \cap C) \Leftrightarrow (x \in A) \wedge (x \in B \cap C)$$

$$\Leftrightarrow (x \in A) \wedge ((x \in B) \wedge (x \in C))$$

$$\Leftrightarrow (x \in A) \wedge (x \in B) \wedge (x \in C)$$

$$\Leftrightarrow ((x \in A) \wedge (x \in B)) \wedge (x \in C)$$

$$\Leftrightarrow (x \in A \cap B) \wedge (x \in C)$$

$$\Leftrightarrow x \in (A \cap B) \cap C$$

D'où $A \cap (B \cap C) = (A \cap B) \cap C$.

Pour la deuxième égalité, même raisonnement que la première égalité.

5. Soit $x \in A \cap (B \cup C)$

$$x \in A \cap (B \cup C) \Leftrightarrow (x \in A) \wedge (x \in B \cup C)$$

$$\Leftrightarrow (x \in A) \wedge ((x \in B) \vee (x \in C))$$

$$\Leftrightarrow ((x \in A) \vee (x \in B)) \wedge ((x \in A) \vee (x \in C))$$

$$\Leftrightarrow (x \in A \cup B) \wedge (x \in A \cup C)$$

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

D'où $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Pour la deuxième égalité, même raisonnement que la première égalité.

2.1.4 Différence et différence symétrique

Définition 2.8 *On appelle différence de deux ensembles E et F, et on note $E \setminus F$, l'ensemble des éléments x tels que $x \in E$ et $x \notin F$.*

$$E \setminus F = \{x : x \in E \ \ et \ \ x \notin F\}$$

Définition 2.9 *On appelle différence symétrique de deux ensembles E et F, et on note $E \Delta F$, l'ensemble difini par :*

$$E \Delta F = (E \setminus F) \cup (F \setminus E) = (E \cup F) \setminus (E \cap F)$$

Exemple 2.4

Soient A, B et C trois ensembles tels que

$$A = \{0, 1, 2, 3, 4, 5, 6, 7\}$$

$$B = \{0, 1, 4, 5, 6\}$$

$$C = \{0, 2, 3, 4, 5\}$$

- B et C sont des sous ensembles de A.
- $B \cap C = \{x : x \in B \ \text{ et } \ x \in C\} = \{0, 4, 5\}$
- $B \cup C = \{x : x \in B \ \text{ ou } \ x \in C\} = \{0, 1, 2, 3, 4, 5, 6\}$.
- $B \setminus C = \{x : x \in B \ \text{ et } \ x \notin C\} = \{1, 6\}$
- $C \setminus B = \{x : x \in C \ \text{ et } \ x \notin B\} = \{2, 3\}$.
- $B \Delta C = \{1, 2, 3, 6\}$.
- $C_A B = \{x \in A / x \notin B\} = \{2, 3, 7\}$
- $C_A C = \{x \in A / x \notin C\} = \{1, 6, 7\}$

Théorème 2.1 *Soient A, B deux parties d'un ensemble E. Alors on a les égalités suivantes :*

1. $C_E (A \cap B) = C_E A \cup C_E B$.
2. $C_E (A \cup B) = C_E A \cap C_E B$.

Preuve

1. Soit $x \in C_E(A \cap B)$. Alors $x \in E$ et $x \notin A \cap B$, donc $x \notin A$ ou $x \notin B$. Donc $x \in C_E A$ ou $x \in C_E B$. Donc $x \in C_E A \cup C_E B$, d'où l'inclusion

$$C_E(A \cap B) \subset C_E A \cup C_E B.$$

Réciproquement, Soit $x \in C_E A \cup C_E B$. Si $x \in C_E A$, alors $x \notin A$ donc$x \notin A \cap B$, et par suite $x \in C_E(A \cap B)$.

De même si $x \in C_E B$, alors $x \notin B$ donc$x \notin A \cap B$, et par suite $x \in C_E(A \cap B)$.

Dans les deux cas $x \in C_E(A \cap B)$, d'où l'inclusion

$$C_E A \cup C_E B \subset C_E(A \cap B).$$

La première égalité est donc démontrée.

2. Pour la deuxième égalité, en posant $A_1 = C_E A$, $B_1 = C_E B$ et en utilisant $C_E(C_E A) = A$.

2.1.5 Partition d'un ensemble

Définition 2.9 *On appelle partition d'un ensemble E, toute famille $G \subset P(E)$ telle que :*

a- *Les éléménts de G sont disjoints deux à deux, c'est à dire*

$$\forall A, B \in G, A \cap B = \varnothing$$

b- *G est un recouvrement de E.*

$$\bigcup_{A \in G} A = E$$

Exemple 2.5

Soit E un ensemble tel que :

$$E = \{0, 1, 2, 3, 4\}$$

1. La famille

$$G_1 = \{\{0, 1\}, \{2\}, \{3, 4\}\}$$

est une partition de E.

2. La famille

$$G_2 = \{\{0, 1\}, \{2\}, \{2, 3, 4\}\}$$

n'est pas une partition de E, car $\{2\} \cap \{2, 3, 4\} = \{2\} \neq \varnothing$.

2.1.6 Produit cartésien

Définition 2.10 *Soient E, F deux ensembles.*

On appelle produit cartésien de E et F, et on note $E \times F$, l'ensemble des couples (x, y) tels que $x \in E$ et $y \in F$.

$$E \times F = \{(x, y) / x \in E \text{ et } y \in F\}$$

Exemple 2.6

Soient E, F deux ensembles tels que :

$$E = \{1, 2, 3, 4\} \quad \text{et} \quad F = \{a, b, c\}$$

Alors,

$$E \times F = \left\{ \begin{array}{c} (1,a), (2,a), (3,a), (4,a), (1,b), (2,b), (3,b), (4,b), \\ \\ (1,c), (2,c), (3,c), (4,c) \end{array} \right\}$$

$$F \times E = \left\{ \begin{array}{c} (a,1), (b,1), (c,1), (a,2), (b,2), (c,2), (a,3), (b,3), \\ \\ (c,3), (a,4), (b,4), (c,4) \end{array} \right\}$$

Remarque 2.1 *$E \times F = F \times E$ si et seulement si $E = F$.*

2.2 Applications

Définition 2.11 O*n appelle application d'un ensemble E dans un ensemble F, toute correspondance f entre les éléments de E et ceux de F qui à tout élément $x \in E$ fait correspondre un unique élément $y \in F$ noté $f(x)$.*

$$f : E \to F$$

$$x \mapsto f(x)$$

- *-E : l'ensemble de départ.*
- *F : l'ensemble d'arrivée*
- *x : l'antécédent de y par f.*
- *$y = f(x)$: l'image de x par f.*

$$(f : E \to F \text{ est une application}) \Leftrightarrow (\forall x_1, x_2 \in E\,(x_1 = x_2 \Rightarrow f(x_1) = f(x_2)))$$

Exemple 2.7

1. $$f : \mathbb{R} \to \mathbb{R}$$
$$x \mapsto \frac{1}{1+x^2}$$
f est une application.

2. $$g : \mathbb{N} \to \mathbb{N}$$
$$x \mapsto \sqrt{x}$$
g n'est pas une application. (Par exemple l'élément $x = 3$ n'a pas une image par g).

3. L'application identité Id
$$Id : E \to E$$
$$x \mapsto Id\,(x) = x$$

2.2.1 Egalité deux applications

On dit que deux applications f, g sont égales si

1. *Elles ont un même ensemble de départ E et un même ensemble d'arrivée F.*
2. *Pour tout $x \in E, f(x) = g(x)$.*

On note $f = g$.

2.2.2 Compositions d'applications

Soient $f : E \to F$ et $g : F \to G$ deux applications. On note $g \circ f$ l'application de E dans G définie par :

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

Cette application est appelée composée des applications f et g.

2.2.3 Restriction et prolongement

Soient f une application de E dans F et $A \subset E \subset G$.

La restriction de f à A est définie par :

$$f_{/A} : A \to F$$

$$x \mapsto f_{/A}(x) = f(x)$$

On appelle prolongement de f à G, toute application $g : G \to F$ telle que pour tout $x \in G, g(x) = f(x)$.
On dit aussi que f est un prolongement de $f_{/A}$.

2.2.4 Injection, surjection et bijection

Soient E, F deux ensembles et f une application de E dans F.

Injection

On dit que f est une application injective si et seulement si

$$\forall x_1, x_2 \in E; \quad f(x_1) = f(x_2) \Rightarrow x_1 = x_2$$

ou

$$\forall x_1, x_2 \in E; \quad x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$$

Exemple 2.8

Soit $f : \mathbb{R}^+ \to \mathbb{R}$ une application définie par

$$\forall x \in \mathbb{R}^+, f(x) = x^2.$$

Soient $x_1, x_2 \in \mathbb{R}^+$

$$f(x_1) = f(x_2) \Rightarrow x_1^2 = x_2^2$$

$$\Rightarrow (x_1 + x_2)(x_1 - x_2) = 0$$

$$\Rightarrow x_1 = x_2.$$

Donc, f est une application injective.

Exemple 2.9

Soit $g : \mathbb{R} \to \mathbb{R}$ une application définie par

$$\forall x \in \mathbb{R}, g(x) = x^2 + x.$$

Soient $x_1, x_2 \in \mathbb{R}$

$$g(x_1) = g(x_2) \Rightarrow x_1^2 + x_1 = x_2^2 + x_2$$

$$\Rightarrow (x_1 - x_2)(x_1 + x_2) + (x_1 - x_2) = 0$$

$$\Rightarrow (x_1 - x_2)(1 + x_1 + x_2) = 0.$$

Donc, on peut trouver deux éléments différents ont même image. Par exemple pour $x_1 = 2$ et $x_2 = -3$,on a : $g(x_1) = g(x_2) = 6$.

Alors, g n'est pas une application injective.

Surjection

On dit que f est une application surjective si

$$\forall y \in F, \exists x \in E; \quad y = f(x)$$

Exemple 2.10

Soit $f : \mathbb{R} - \{2\} \to \mathbb{R} - \{3\}$ une application définie par

$$\forall x \in \mathbb{R} - \{2\}, f(x) = \frac{3x+1}{x-2}.$$

Soit $y \in \mathbb{R} - \{3\}$, on cherche un élément x de $\mathbb{R} - \{2\}$ s'il existe tel que $y = f(x)$.

On a :

$$y = f(x) \Rightarrow y = \frac{3x+1}{x-2}$$

$$\Rightarrow y(x - 2) = 3x + 1$$

$$\Rightarrow x = \frac{2y+1}{y-3}.$$

$x \in \mathbb{R} - \{2\}$?

Par l'absurde, supposons que $x = 2$ et on cherche une contradiction.

$$x = 2 \Leftrightarrow \frac{2y+1}{y-3} = 2$$

$$\Leftrightarrow 2y + 1 = 2(y - 3)$$

$$\Leftrightarrow 1 = -6.$$

Qui est impossible. Donc d'aprés le principe de raisonnement par l'absurde, on déduit que $x \neq 2$.

D'où f est une application surjective.

Exemple 2.11

Soit $g : \mathbb{R} \to \mathbb{R}$ une application définie par

$$\forall x \in \mathbb{R}, g(x) = x^2 + 3x.$$

Soit $y \in \mathbb{R}$, on cherche un élément x de $\mathbb{R}$ s'il existe tel que $y = g(x)$.

On a :

$$y = g(x) \Rightarrow y = x^2 + 3x$$

$$\Rightarrow x^2 + 3x - y = 0$$

Cette équation admet des solutions pour $y \in \left[-\frac{9}{4}, +\infty\right[$. Donc pour $y \notin \left]-\infty, -\frac{9}{4}\right[$, l'élément y n'a pas d'antécédent.

Alors, g n'est pas une application surjective.

Bijection

On dit que f est une application bijective si f est une application injective et surjective.

$$\forall y \in F, \exists! x \in E; \quad y = f(x)$$

Exemple 2.12

Soit $f : \mathbb{R} - \{2\} \to \mathbb{R} - \{3\}$ une application définie par

$$\forall x \in \mathbb{R} - \{2\}, f(x) = \frac{3x+1}{x-2}.$$

f est une application surjective (voir l'exemple 2.10).

Reste à montrer que f est une application injective.

Soient $x_1, x_2 \in \mathbb{R} - \{2\}$

$$f(x_1) = f(x_2) \Rightarrow \frac{3x_1+1}{x_1-2} = \frac{3x_2+1}{x_2-2}$$

$$\Rightarrow (3x_1 + 1)(x_2 - 2) - (x_1 - 2)(3x_2 + 1) = 0$$

$$\Rightarrow x_1 = x_2.$$

Donc, f est une application injective.

D'où f est une application bijective.

Théorème de la bijection :

Si f continue et strictement croissante (Resp : strictement décroissante) sur un intervalle $[a, b]$, alors f réalise une bijection de $[a, b]$ sur $[f(a), f(b)]$ (Resp : $[f(b), f(a)]$).

(Cela vaut aussi pour un intervalle ouvert).

2.2.5 L'application réciproque

Si $f : E \to F$ est une application bijective, alors il existe une unique application $g : F \to E$ telle que

$$g \circ f = Id_E \quad \text{et} \quad f \circ g = Id_F.$$

L'application g est appelée l'inverse ou la réciproque de f et on note :

$$g = f^{-1}$$

Exemple 2.13

Soit $f : \mathbb{R} - \{2\} \to \mathbb{R} - \{3\}$ une application définie par

$$\forall x \in \mathbb{R} - \{2\}, f(x) = \frac{3x+1}{x-2}.$$

f est une application bijective (voir l'exemple 2.12), alors elle est inversible et on a :

$$f^{-1} : \mathbb{R} - \{3\} \to \mathbb{R} - \{2\}$$

$$x \mapsto \frac{2x+1}{x-3}$$

Proposition 2.1 *Soient $f : E \to F$ et $g : F \to G$ deux applications, alors :*

1. $(f \text{ est injective}) \wedge (g \text{ est injective}) \Rightarrow (g \circ f \text{ est injective})$.
2. $(f \text{ est surjective}) \wedge (g \text{ est surjective}) \Rightarrow (g \circ f \text{ est surjective})$.
3. $(f \text{ est bijective}) \wedge (g \text{ est bijective}) \Rightarrow \left(g \circ f \text{ est bijective et } (g \circ f)^{-1} = f^{-1} \circ g^{-1}\right)$.

Preuve

1. Supposons que $(f$ est injective$) \wedge (g$ est injective$)$ et montrons que $g \circ f$ est injective.

Soient $a, b \in E$, on a :

$$(g \circ f)(a) = (g \circ f)(b) \Rightarrow g(f(a)) = g(f(b))$$

$$\Rightarrow f(a) = f(b) \quad (\text{car } g \text{ est injective})$$

$$\Rightarrow a = b \quad (\text{car } f \text{ est injective}),$$

ce qui montre que $g \circ f$ est une application injective.

2. Supposons que $(f$ est surjective$) \wedge (g$ est surjective$)$ et montrons que $g \circ f$ est surjective.

Soit $z \in G$, comme g est surjective, alors il existe $y \in F$ tel que $z = g(y)$.

Comme $y \in F$ et f est surjective, alors il existe $x \in E$ tel que $y = f(x)$, donc $z = g(y) = g(f(x))$.

On déduit que pour tout $z \in G$ il existe $x \in E$ tel que $z = g(f(x))$.

Ce qui montre que $g \circ f$ est une application surjective.

3. Supposons que (f est bijective) $\wedge$ (g est bijective) et montrons que

$\left(g \circ f \text{ est bijective et } (g \circ f)^{-1} = f^{-1} \circ g^{-1}\right)$.

De 1 et 2 on déduit que $g \circ f$ est une application bijective.

Soit $z \in G$, alors il existe $y \in F$ et $x \in E$ tel que $z = g(y), y = f(x)$ et $z = g(f(x))$.

Donc,

$$y = g^{-1}(z)$$

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

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

Alors,

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

D'où

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

Proposition 2.2 *Soient $f : E \to F$ et $g : F' \to G$ deux applications telles que $F' \subset F$, alors :*

1. ($g \circ f$ est injective) $\Rightarrow$ (f est injective).
2. ($g \circ f$ est surjective) $\Rightarrow$ (g est surjective).

Preuve

1. Supposons que ($g \circ f$ est injective) et montrons que (f est injective)

Soient $a, b \in E$, on a :

$$f(a) = f(b) \Rightarrow g(f(a)) = g(f(b)) \quad (\text{car } g \text{ est injective})$$

$$\Rightarrow (g \circ f)(a) = (g \circ f)(b)$$

$$\Rightarrow a = b \quad (\text{car } g \circ f \text{ est injective}),$$

ce qui montre que f est une application injective.

2. Supposons que ($g \circ f$ est surjective) et montrons que (g est surjective).

Soit $z \in G$, alors il existe $x \in E$ tel que $z = (g \circ f)(x) = g(f(x))$.

Donc, il existe $y = f(x) \in F$ tel que $z = g(f(x)) = g(y)$.

On déduit que pour tout $z \in G$ il existe $y \in F$ tel que $z = g(y)$.

Ce qui montre que g est une application surjective.

2.2.6 Image directe - Image réciproque

Soient E, F deux ensembles et f une application de E dans F.

Définition 2.12 *On appelle image directe d'un ensemble $A \subset E$, l'ensemble*

$$f(A) = \{f(x) \ / \ x \in A\}$$

Définition 2.13 *On appelle image réciproque d'un ensemble $B \subset F$, l'ensemble*

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

Proposition 2.3 *Soient $f : E \to F$ une application et $A, B \subset E$ et $M, N \subset F$. Alors :*

Proposition 2.2.1

1. $f(A \cup B) = f(A) \cup f(B)$.
2. $f(A \cap B) \subset f(A) \cap f(B)$.
3. $f^{-1}(M \cup N) = f^{-1}(M) \cup f^{-1}(N)$.
4. $f^{-1}(M \cap N) = f^{-1}(M) \cap f^{-1}(N)$.
5. $f^{-1}(C_F M) = C_E f^{-1}(M)$.

Preuve

1. Soit $y \in F$, alors

$$y \in f(A \cup B) \Leftrightarrow \exists x \in A \cup B, y = f(x)$$

$$\Leftrightarrow \exists x ((x \in A \vee x \in B) \wedge (y = f(x)))$$

$$\Leftrightarrow \exists x ((x \in A \wedge y = f(x)) \vee (x \in B \wedge y = f(x)))$$

$$\Leftrightarrow (\exists x, (x \in A \wedge y = f(x))) \vee (\exists x, (x \in B \wedge y = f(x)))$$

$$\Leftrightarrow (y \in f(A)) \vee (y \in f(B))$$

$$\Leftrightarrow y \in f(A) \cup f(B)$$

d'où $f(A \cup B) = f(A) \cup f(B)$.

2. Soit $y \in F$, alors

$$y \in f(A \cap B) \Leftrightarrow \exists x \in A \cap B, y = f(x)$$

$$\Leftrightarrow \exists x ((x \in A \wedge x \in B) \wedge (y = f(x)))$$

$$\Leftrightarrow \exists x ((x \in A \wedge y = f(x)) \wedge (x \in B \wedge y = f(x)))$$

$$\Rightarrow (\exists x, (x \in A \wedge y = f(x))) \wedge (\exists x, (x \in B \wedge y = f(x)))$$

$$\Rightarrow (y \in f(A)) \wedge (y \in f(B))$$

$$\Rightarrow y \in f(A) \cap f(B)$$

d'où $f(A \cap B) \subset f(A) \cap f(B)$.

3. Soit $x \in E$, alors

$$x \in f^{-1}(M \cup N) \Leftrightarrow f(x) \in M \cup N$$

$$\Leftrightarrow (f(x) \in M) \vee (f(x) \in N)$$

$$\Leftrightarrow (x \in f^{-1}(M)) \vee (x \in f^{-1}(N))$$

$$\Rightarrow x \in f^{-1}(M) \cup f^{-1}(N)$$

d'où $f^{-1}(M \cup N) = f^{-1}(M) \cup f^{-1}(N)$.

4. Soit $x \in E$, alors

$$x \in f^{-1}(M \cap N) \Leftrightarrow f(x) \in M \cap N$$

$$\Leftrightarrow (f(x) \in M) \wedge (f(x) \in N)$$

$$\Leftrightarrow (x \in f^{-1}(M)) \wedge (x \in f^{-1}(N))$$

$$\Rightarrow x \in f^{-1}(M) \cap f^{-1}(N)$$

d'où $f^{-1}(M \cap N) = f^{-1}(M) \cap f^{-1}(N)$.

5. Soit $x \in E$, alors

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

$$\Leftrightarrow (f(x) \in F) \wedge (f(x) \notin M)$$

$$\Leftrightarrow (x \in E) \wedge (x \notin f^{-1}(M))$$

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

d'où $f^{-1}(C_F M) = C_E f^{-1}(M)$.

2.3 Exercices

Exercice 1

Soit $E = \{\alpha, \beta, \gamma\}$ un ensemble. Peut-on écrire :

$$(a) - \alpha \in E \qquad (b) - \alpha \subset E \qquad (c) - \{\alpha\} \subset E$$

$$(d) - \varnothing \subset E \qquad (e) - \varnothing \in E \qquad (f) - \{\varnothing\} \subset E$$

Solution

On peut écrire $(a) - \alpha \in E \qquad (c) - \{\alpha\} \subset E \qquad (d) - \varnothing \subset E$.

$(a) - \alpha \in E$ vraie, car α est un élément de l'ensemble E.

$(b) - \alpha \subset E$ n'a pas de sens puisque α n'est pas un ensemble.

$(c) - \{\alpha\} \subset E$ vraie, car $\{\alpha\}$ est un sous ensemble de E.

$(d) - \varnothing \subset E$ vraie, l'ensemble vide est inclu dans tous les ensembles.

$(e) - \varnothing \in E$, l'ensemble vide n'est pas un élément de E.

$(f) - \{\varnothing\} \subset E$ faux.

Exercice 2

Soient $A = \{0, 1, 2, 3\}$ et $B = \{0, 2, 4, 6\}$. Décrire les ensembles $A \cap B$, $A \cup B$ et $A \times B$.

Solution

Décrire les ensembles $A \cap B$, $A \cup B$ et $A \times B$

1. $A \cap B$

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

$$= \{0, 2\}$$

2. $A \cup B$

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

$$= \{0, 1, 2, 3, 4, 6\}$$

3. $A \times B$

$$A \times B = \{(x, y) / x \in A \text{ et } y \in B\}$$

$$= \left\{ \begin{array}{l} (0,0), (0,2), (0,4), (0,6), (1,0), (1,2), (1,4), (1,6), \\ (2,0), (2,2), (2,4), (2,6), (3,0), (3,2), (3,4), (3,6), \end{array} \right\}$$

Exercice 3

Soient A, B et C trois parties d'un ensemble E.

Montrer que :

$$A \cap B = A \cap C \Leftrightarrow A \cap C_E^B = A \cap C_E^C$$

Solution

i- ($\Rightarrow$) On suppose que $A \cap B = A \cap C$

Soit $x \in A \cap C_E^B$,

On a :

$$x \notin B \Rightarrow x \notin A \cap B$$

$$\Rightarrow x \notin A \cap C$$

$$x \in A \text{ et } x \notin A \cap C \Rightarrow x \notin C$$

$$\Rightarrow x \in C_E^C,$$

donc

$$x \in A \cap C_E^C$$

On a prouvé l'inclusion

$$A \cap C_E^B \subset A \cap C_E^C$$

En échangeant B et C, on obtient l'inclusion contraire, donc par double inclusion

$$A \cap C_E^B = A \cap C_E^C$$

ii- ($\Leftarrow$) On suppose que $A \cap C_E^B = A \cap C_E^C$, en utilisant l'implication précédente avec C_E^B et C_E^C.

Soit $x \in A \cap B$,

On a :

$$x \notin C_E^B \Rightarrow x \notin A \cap C_E^B$$

$$\Rightarrow x \notin A \cap C_E^C$$

$$x \in A \text{ et } A \cap C_E^C \Rightarrow x \notin C_E^C$$

$$\Rightarrow x \in C,$$

donc

$$x \in A \cap C$$

On a prouvé l'inclusion

$$A \cap B \subset A \cap C$$

En échangeant C_E^B et C_E^C, on obtient l'inclusion contraire, donc par double inclusion

$$A \cap B = A \cap C$$

Alors, d'aprés (i) et (ii), on déduit que

$$A \cap B = A \cap C \Leftrightarrow A \cap C_E^B = A \cap C_E^C$$

Exercice 4

Soient A, B deux parties d'un ensemble E. On suppose que

$$A \cap B \neq \varnothing, A \cup B \neq E, A \nsubseteq B, B \nsubseteq A$$

On pose :

$$A_1 = A \cap B, A_2 = A \cap C_E^B, A_3 = B \cap C_E^A, A_4 = C_E^{A \cup B}.$$

Montrer que :

1. *A_1, A_2, A_3, A_4 sont non vides.*

2. *A_1, A_2, A_3, A_4 sont deux à deux disjoints.*

3. $A_1 \cup A_2 \cup A_3 \cup A_4 = E$.

Solution

1. *A_1, A_2, A_3, A_4 sont non vides. On a ;*

$$A_1 = A \cap B \neq \varnothing, \quad \textit{d'après l'énoncé.}$$

$$A_2 = A \cap C_E^B = A \setminus B \neq \varnothing, \qquad \textit{car} \;\; A \nsubseteq B.$$

$$A_3 = A \cap C_E^A = B \setminus A \neq \varnothing, \qquad \textit{car} \;\; B \nsubseteq A.$$

$$A_4 = C_E^{A \cup B} = E \setminus (A \cup B) \neq \varnothing, \qquad \textit{car} \;\; A \cup B \neq E.$$

2. *A_1, A_2, A_3, A_4 sont deux à deux disjoints.*

On démontre que

$$A_i \cap A_j = \varnothing \quad avec \quad i \neq j \quad et \quad i,j \in \{1,2,3,4\}$$

$$A_1 \cap A_2 = (A \cap B) \cap \left(A \cap C_E^B\right)$$

$$= A \cap B \cap A \cap C_E^B$$

$$= (A \cap A) \cap \left(B \cap C_E^B\right)$$

$$= A \cap \varnothing$$

$$= \varnothing$$

$$A_1 \cap A_3 = (A \cap B) \cap \left(B \cap C_E^A\right)$$

$$= A \cap B \cap B \cap C_E^A$$

$$= (B \cap B) \cap \left(A \cap C_E^A\right)$$

$$= B \cap \varnothing$$

$$= \varnothing$$

$$A_1 \cap A_4 = (A \cap B) \cap \left(C_E^{A \cup B}\right)$$

$$= (A \cap B) \cap \left(C_E^A \cap C_E^B\right)$$

$$= A \cap B \cap C_E^A \cap C_E^B$$

$$= \left(A \cap C_E^A\right) \cap \left(B \cap C_E^B\right)$$

$$= \varnothing \cap \varnothing$$

$$= \varnothing$$

$$A_2 \cap A_3 = \left(A \cap C_E^B\right) \cap \left(B \cap C_E^A\right)$$

$$= A \cap C_E^B \cap B \cap C_E^A$$

$$= \left(A \cap C_E^A\right) \cap \left(B \cap C_E^B\right)$$

$$= \varnothing \cap \varnothing$$

$$= \varnothing$$

$$A_2 \cap A_4 = \left(A \cap C_E^B\right) \cap \left(C_E^{A \cup B}\right)$$

$$= \left(A \cap C_E^B\right) \cap \left(C_E^A \cap C_E^B\right)$$

$$= A \cap C_E^B \cap C_E^A \cap C_E^B$$

$$= \left(A \cap C_E^A\right) \cap \left(C_E^B \cap C_E^B\right)$$

$$= \varnothing \cap C_E^B$$

$$= \varnothing$$

$$A_3 \cap A_4 = \left(B \cap C_E^A\right) \cap \left(C_E^{A \cup B}\right)$$

$$= \left(B \cap C_E^A\right) \cap \left(C_E^A \cap C_E^B\right)$$

$$= B \cap C_E^A \cap C_E^A \cap C_E^B$$

$$= \left(B \cap C_E^B\right) \cap \left(C_E^A \cap C_E^A\right)$$

$$= \varnothing \cap C_E^A$$

$$= \varnothing$$

3. $A_1 \cup A_2 \cup A_3 \cup A_4 = E$.

$$A_1 \cup A_2 \cup A_3 \cup A_4 = (A \cap B) \cup \left(A \cap C_E^B\right) \cup \left(B \cap C_E^A\right) \cup \left(C_E^{A \cup B}\right)$$

$$= (A \cap B) \cup \left(A \cap C_E^B\right) \cup \left(B \cap C_E^A\right) \cup \left(C_E^A \cap C_E^B\right)$$

$$= \left[(A \cap B) \cup \left(A \cap C_E^B\right)\right] \cup \left[\left(B \cap C_E^A\right) \cup \left(C_E^A \cap C_E^B\right)\right]$$

$$= \left[(A \cup A) \cap \left(A \cup C_E^B\right) \cap (B \cup A) \cap \left(B \cup C_E^B\right)\right] \cup \left[\left(B \cup C_E^A\right) \cap \left(B \cup C_E^B\right) \cap \left(C_E^A \cup C_E^A\right) \cap \left(C_E^A \cup C_E^B\right)\right]$$

$$= \left[A \cap \left(A \cup C_E^B\right) \cap (B \cup A) \cap E\right] \cup \left[\left(B \cup C_E^A\right) \cap E \cap C_E^A \cap \left(C_E^A \cup C_E^B\right)\right]$$

$$= \left[A \cap \left(\left(A \cup C_E^B\right) \cap (B \cup A)\right)\right] \cup \left[C_E^A \cap \left(\left(B \cup C_E^A\right) \cap \left(C_E^A \cup C_E^B\right)\right)\right]$$

$$= \left[A \cap \left(A \cup \left(B \cap C_E^B\right)\right)\right] \cup \left[C_E^A \cap \left(C_E^A \cup \left(B \cup C_E^B\right)\right)\right]$$

$$= [A \cap (A \cup \varnothing)] \cup \left[C_E^A \cap \left(C_E^A \cup E\right)\right]$$

$$= A \cup C_E^A$$

$$= E$$

Exercice 5

Soit $f : \mathbb{R} \to \mathbb{R}$ *une application définie par*

$$f(x) = \frac{2x}{1+x^2}.$$

1. f *est-elle injective ? surjective ?*

2. Montre que $f(\mathbb{R}) = [-1, 1]$.

3. Montrer que la restriction $g : [-1, 1] \to [-1, 1]$, $g(x) = f(x)$ *est une bijection.*

Solution

1. f **est-elle injective ?**

Soient $x_1, x_2 \in \mathbb{R}$

$$f(x_1) = f(x_2) \Rightarrow \frac{2x_1}{1+x_1^2} = \frac{2x_2}{1+x_2^2}$$

$$\Rightarrow 2x_1(1+x_2^2) - 2x_2(1+x_1^2) = 0$$

$$\Rightarrow (x_1 - x_2)(1 - x_1x_2) = 0.$$

Donc, on peut trouver deux éléments différents ont même image. Par exemple pour $x_1 = 2$ et $x_2 = \frac{1}{2}$,on a : $f(x_1) = f(x_2) = \frac{4}{5}$.

Alors, f n'est pas une application injective.

f **est-elle surjective ?**

Soit $y \in \mathbb{R}$, on cherche un élément x de $\mathbb{R}$ s'il existe tel que $y = f(x)$.

On a :

$$y = f(x) \Leftrightarrow y = \frac{2x}{1+x^2}$$

$$\Leftrightarrow yx^2 - 2x + y = 0$$

Cette équation admet des solutions pour $y \in [-1, 1]$. Donc pour $y \notin [-1, 1]$, l'élément y n'a pas d'antécédent.

Alors, f n'est pas une application surjective.

2. Montre que $f(\mathbb{R}) = [-1, 1]$.

L'équation $y = f(x)$ a des solutions réelles si et seulement si $\Delta = 4(1 - y^2) \geq 0$, donc il y a des solutions si et seulement si $y \in [-1, 1]$.

Ainsi,

$$f(\mathbb{R}) = [-1, 1]$$

3. Montrer que la restriction $g : [-1, 1] \to [-1, 1]$, $g(x) = f(x)$ **est une bijection.**

Soit $y \in [-1, 1]$, on cherche un élément unique $x \in \mathbb{R}$ tel que $y = g(x)$.

Si $y \in]-1,0[\cup]0,1[$, alors les solutions possibles sont

$$x = \frac{1-\sqrt{1-y^2}}{y}$$

ou

$$x = \frac{1+\sqrt{1-y^2}}{y}$$

La deuxième solution n'appartient pas à $[-1,1]$ (elle est strictement supérieure à 1 si $y > 0$, et strictement inférieure à -1 si $y < 0$).

D'autre part

$$x = \frac{1-\sqrt{1-y^2}}{y} = \frac{y}{1+\sqrt{1-y^2}} \in [-1,1]$$

En effet,

$$1 \leq 1 + \sqrt{1-y^2} \Rightarrow 0 \leq \frac{1}{1+\sqrt{1-y^2}} \leq 1$$

Donc,

$$-1 \leq -\frac{1}{1+\sqrt{1-y^2}} \leq y \leq \frac{1}{1+\sqrt{1-y^2}} \leq 1$$

Si $y = 1$, l'équation $g(x) = 1$ a pour unique solution $x = 1$.

Si $y = -1$, l'équation $g(x) = -1$ a pour unique solution $x = 1$.

Si $y = 0$, l'équation $g(x) = 0$ a pour unique solution $x = 0$.

Dans tous les cas, on a prouvé que pour tout $y \in [-1,1]$, l'équation $g(x) = y$ admet une unique solution avec $x \in [-1,1]$. Nous avons bien prouvé que g est une bijection.

Exercice 6

Soit $f : \mathbb{R} \to \mathbb{R}$ *une application définie par*

$$\forall x \in \mathbb{R}, f(x) = x^2 + 3x + 1.$$

et soit $A = [-2,1]$.

1. Déterminer l'image directe de A *par* f.

2. Déterminer l'image réciproque de A *par* f.

Solution

1. Déterminer l'image directe de A par f.

Par définition, on a

$$f(A) = \{f(x) / x \in A\}$$

On cherche toutes les valeurs prises par $f(x)$ lorsque x parcourt $[-2,1]$.

On a

$$f(x) = \left(x+\tfrac{3}{2}\right)^2 - \tfrac{5}{4}$$

donc

$$x \in A \Leftrightarrow -2 \leq x \leq 1$$

$$\Leftrightarrow -2+\tfrac{3}{2} \leq x+\tfrac{3}{2} \leq 1+\tfrac{3}{2}$$

$$\Leftrightarrow -\tfrac{1}{2} \leq x+\tfrac{3}{2} \leq \tfrac{5}{2}$$

$$\Leftrightarrow 0 \leq \left(x+\tfrac{3}{2}\right)^2 \leq \tfrac{25}{4}$$

$$\Leftrightarrow -\tfrac{5}{4} \leq \left(x+\tfrac{3}{2}\right)^2 - \tfrac{5}{4} \leq 5$$

Alors,

$$f(A) = \left[-\tfrac{5}{4}, 5\right]$$

2. Déterminer l'image réciproque de A par f.

Par définition, on a

$$f^{-1}(A) = \{x \in \mathbb{R} / f(x) \in A\}$$

donc,

$$f(x) \in A \Leftrightarrow -2 \leq f(x) \leq 1$$

$$\Leftrightarrow -2 \leq \left(x+\tfrac{3}{2}\right)^2 - \tfrac{5}{4} \leq 1$$

$$\Leftrightarrow -2+\tfrac{5}{4} \leq \left(x+\tfrac{3}{2}\right)^2 \leq 1+\tfrac{5}{4}$$

$$\Leftrightarrow -\tfrac{3}{4} \leq \left(x+\tfrac{3}{2}\right)^2 \leq \tfrac{9}{4}$$

$$\Leftrightarrow -\tfrac{3}{2} \leq x+\tfrac{3}{2} \leq \tfrac{3}{2}$$

$$\Leftrightarrow -3 \leq x \leq 0$$

Alors,

$$f^{-1}(A) = [-3, 0]$$

Chapitre 3

Relations binaires sur un ensemble

3.1 Définitions de base

Définition 3.1 *Soient E et F deux ensembles*

Une relation binaire de E vers F est une partie $\Re$ de $E \times F$. Si $(x, y) \in \Re$ alors on dit que x est en relation avec y et on le note $x\Re y$.

Dans le cas ou $E = F$ on dit que $\Re$ est définie sur E.

Exemple 3.1

– L'égalité «=» est une relation sur un ensemble E.

– L'inégalité «$\leq$» est une relation sur $\mathbb{N}$, $\mathbb{Z}$ ou $\mathbb{R}$.

– L'inclusion «$\subset$» est une relation sur $P(X)$, où X est un ensemble quelconque.

Remarque 3.1

On peut représenter une relation binaire par un graphe. Par exemple la relation «$\leq$» sur l'ensemble $E = \{0, 1, 2, 3, 4\}$

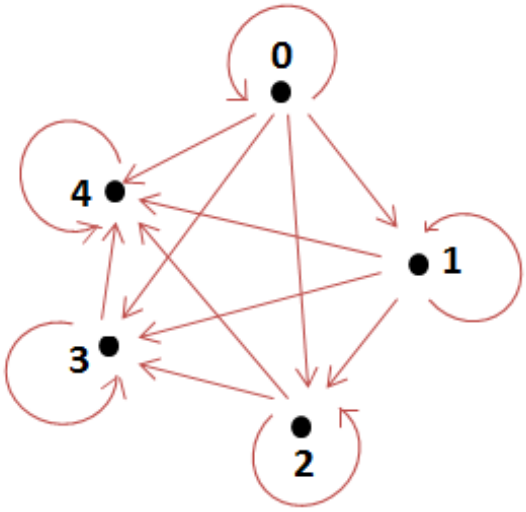


Fig 3.1 : Graphe de la relation « $\leq$ »
sur l'ensemble $E = \{0, 1, 2, 3, 4\}$

3.1.1 Relation réflexive

Définition 3.2 *Soit* $\Re$ *une relation binaire sur un ensemble* E.

$\Re$ *est réflexive si pour tout* $x \in E$, *on a :* $x\Re x$.

Exemple 3.2

– L'inégalité «$\leq$» sur $\mathbb{N}$, $\mathbb{Z}$ ou $\mathbb{R}$ est réflexive.

– L'inégalité «$<$» sur $\mathbb{N}$ n'est par réflexive. Car on peut trouver un entier naturel x qui n'est pas en relation avec lui même.

3.1.2 Symétrique

Définition 3.3 *Soit* $\Re$ *une relation binaire sur un ensemble* E.

$\Re$ *est symétrique si pour tout* $x, \in E$, *on a :*

$$x\Re y \Rightarrow y\Re x.$$

Exemple 3.3

– L'inégalité «$\leq$» sur $\mathbb{N}$, $\mathbb{Z}$ ou $\mathbb{R}$ est symétrique.

– L'inégalité «<» sur $\mathbb{N}$ n'est par symétrique. Car on peut trouver deux entiers naturels x, y tels que x est en relation avec y et y n'est pas en relation avec x.

3.1.3 Antisymétrique

Définition 3.4 *Soit $\Re$ une relation binaire sur un ensemble E.*

$\Re$ est antisymétrique si pour tout $x, y \in E$, on a :

$$(x\Re y \text{ et } y\Re x) \Rightarrow x = y.$$

Exemple 3.4

– L'inégalité «$\leq$» sur $\mathbb{N}$, $\mathbb{Z}$ ou $\mathbb{R}$ est antisymétrique.

3.1.4 Transitive

Définition 3.5 *Soit $\Re$ une relation binaire sur un ensemble E.*

$\Re$ est transitive si pour tout $x, y, z \in E$, on a :

$$(x\Re y \text{ et } y\Re z) \Rightarrow x\Re z.$$

Exemple 3.5

– L'inégalité «$\leq$» sur $\mathbb{N}$, $\mathbb{Z}$ ou $\mathbb{R}$ est tansitive.

– L'inégalité «<» sur $\mathbb{N}$ est tansitive.

3.2 Relation d'ordre

Définition 3.6 *Soit $\Re$ une relation binaire sur un ensemble E.*

On dit que $\Re$ est une relation d'ordre si $\Re$ est réflexive, antisymétrique ettransitive.

Exemple 3.6

– L'inégalité «$\leq$» sur $\mathbb{N}$, $\mathbb{Z}$ ou $\mathbb{R}$ est une relation d'ordre.

3.2.1 Ordre total et partiel

Définition 3.7 *Soit $\Re$ une relation d'ordre sur un ensemble E.*

1. *On dit que deux éléments x et y de E sont comparable ssi :*

$$x\Re y \quad ou \quad y\Re x.$$

2. *On dit que $\Re$ est une relation d'ordre total, si tous les éléments de E sont deux à deux comparables. Si non, on dit que la relation est une relation d'ordre partiel.*

Exemple 3.7

Soit E un ensemble et $X = \rho(E)$. On considère sur X la relation binaire suivante

$$\forall A, B \in X, \quad A \; T \; B \; \Leftrightarrow \; A \subset B.$$

Alors,

1- T est une relation d'ordre

– (i) T est réflexive, car pour tout ensemble $A \in X$, on a

$$A \subset A \Rightarrow A \; T \; A$$

– (ii) T est antisymétrique, car pour tous $A, B \in X$, on a

$$(A \; T \; B) \;\; et \;\; (B \; T \; A) \Rightarrow (A \;\subset\; B) \;\; et \;\; (B \;\subset\; A)$$

$$\Rightarrow A = B$$

– (iii) T est transitive, car pour tous $A, B, C \in X$, on a

$$(A \; T \; B) \;\; et \;\; (B \; T \; C) \Rightarrow (A \;\subset\; B) \;\; et \;\; (B \;\subset\; C)$$

$$\Rightarrow \forall x \;\; ((x \in A \Rightarrow x \in B) \;\; et \;\; (x \in B \Rightarrow x \in C))$$

$$\Rightarrow \forall x \;\; (x \in A \Rightarrow x \in C)$$

$$\Rightarrow B \;\subset\; C$$

$$\Rightarrow A \; T \; C$$

De (i), (ii) et (iii) on déduit que T est une relation d'ordre sur X.

2- L'ordre est - il total ?

– Si $E = \emptyset$, alors $X = \{\emptyset\}$ et on a : $\forall A, B \in X$, $A = B = \emptyset$, donc

$$\forall A, B \in X, \;\; A \subset B$$

ce qui montre que l'ordre est total.

– Si E est un signgleton, alors $E = \{a\}$ et $X = \{\emptyset, \{a\}\}$, pour tous $A, B \in X$ on a

$$A = \emptyset \ \vee \ A = \{a\}$$

$$et$$

$$B = \emptyset \ \vee \ B = \{a\},$$

donc

$$\forall A, B \in X, \ A \subset B \ ou \ B \subset A$$

ce qui montre que l'ordre est total.

– Si E contient au moins deux éléments distincts a et b, alors

$$\exists \ A = \{a\}, \ B = \{b\}, \ (A \ \not\subseteq \ B) \ et \ (B \ \not\subseteq \ A)$$

ce qui montre que l'ordre est partiel.

3.3 Relation d'équivalence

Définition 3.8 *Soit $\Re$ une relation binaire sur un ensemble E.*

On dit que $\Re$ est une relation d'équivalence sur E si $\Re$ est réflexive, symétriqueet transitive.

Exemple 3.8

Dans $\mathbb{R}$, on définit la relation binaire δ par :

$$\forall a, b \in \mathbb{R}, \quad a\delta b \Leftrightarrow \cos^2 a + \sin^2 b = 1$$

Montrer que δ est une relation d'équivalence.

Soient $a, b, c \in \mathbb{R}$, on a :

(i)

$$\cos^2 a + \sin^2 a = 1 \Rightarrow a\delta a$$

Alors, δ est réflexive.

(ii)

$$a\delta b \Rightarrow \cos^2 a + \sin^2 b = 1$$

$$\Rightarrow \left(1 - \sin^2 a\right) + (1 - \cos^2 b) = 1$$

$$\Rightarrow -\left(\sin^2 a + \cos^2 b\right) + 2 = 1$$

$$\Rightarrow \cos^2 b + \sin^2 a = 1$$

$$\Rightarrow b\delta a$$

Alors, δ est symétrique.

(iii)

$$(a\delta b \text{ et } b\delta c) \Rightarrow (\cos^2 a + \sin^2 b = 1 \text{ et } \cos^2 b + \sin^2 c = 1)$$

$$\Rightarrow (\cos^2 a + \sin^2 b + \cos^2 b + \sin^2 c = 2)$$

$$\Rightarrow (\cos^2 a + \sin^2 c = 1)$$

$$\Rightarrow a\delta c$$

Alors, δ est transitive.

De (i), (ii) et (iii) on déduit que δ est une relation d'équivalence.

3.3.1 Classe d'équivalence

– *Soit $\Re$ une relation d'équivalence sur un ensemble E. Soit $x \in E$, la classe d'équivalence de x est*

$$Cl(x) = \dot{\widehat{x}} = \{y \in E \ / \ y\Re x\}$$

– *$Cl(x)$ est donc un sous-ensemble de E.*

– *On appelle ensemble quotient de E par la relation d'équivalence $\Re$, l'ensemble des classes d'équivalence de tous les éléments de E . Cet ensemble est noté $E/\Re$.*

Exemple 3.9

Dans $\mathbb{R}$, on définit la relation binaire $\Re$ par :

$$\forall x, y \in \mathbb{R}, \quad x\Re y \Leftrightarrow x^3 - 3x = y^3 - 3y$$

Montrer que $\Re$ est une relation d'équivalence et déterminer la classe d'équivalence de $x \in \mathbb{R}$.

1. Montrer que $\Re$ est une relation d'équivalence

Soient $x, y, z \in \mathbb{R}$, on a :

(i)

$$x^3 - 3x = x^3 - 3x \Rightarrow x \Re x$$

Alors, $\Re$ est réflexive.

(ii)

$$x \Re y \Rightarrow x^3 - 3x = y^3 - 3y$$

$$\Rightarrow y^3 - 3y = x^3 - 3x$$

$$\Rightarrow y \Re x$$

Alors, $\Re$ est symétrique.

(iii)

$$(x \Re y \text{ et } y \Re z) \Rightarrow (x^3 - 3x = y^3 - 3y \text{ et } y^3 - 3y = z^3 - 3z)$$

$$\Rightarrow (x^3 - 3x = z^3 - 3z)$$

$$\Rightarrow x \Re z$$

Alors, $\Re$ est transitive.

De (i), (ii) et (iii) on déduit que $\Re$ est une relation d'équivalence.

2. Déterminer la classe d'équivalence de $x \in \mathbb{R}$

Soit $x \in \mathbb{R}$, on a :

$$Cl(x) = \{y \in E \ / \ y \Re x\}$$

$$= \{y \in E \ / \ y^3 - 3y = x^3 - 3x\}$$

$$y^3 - 3y = x^3 - 3x \Leftrightarrow (y^3 - x^3) - 3(y - x) = 0$$

$$\Leftrightarrow (y - x)(y^2 + xy + x^2 - 3) = 0$$

$$\Leftrightarrow \begin{cases} y - x = 0 \\ \\ y^2 + xy + x^2 - 3 = 0 \end{cases}$$

On résout la deuxième équation.

$$\Delta = x^2 - 4(x^2 - 3) = 3(4 - x^2)$$

Alors,

Si $x \in]-2, 2[$, l'équation admet deux solutions

$$y = \frac{-x - \sqrt{12 - 3x^2}}{2} \quad \text{ou} \quad y = \frac{-x + \sqrt{12 - 3x^2}}{2}$$

Si $x = -2$, l'équation admet une solution

$$y = 1$$

Si $x = 2$, l'équation admet une solution

$$y = -1$$

Si $x \in]-\infty, -2[\cup]2, +\infty[$, l'équation n'admet pas de solutions.

Donc,

$$Cl(x) = \begin{cases} \left\{x, \frac{-x-\sqrt{12-3x^2}}{2}, \frac{-x+\sqrt{12-3x^2}}{2}\right\} & \text{si } x \in]-2, 2[\\ \{x\} \quad \text{si } x \in]-\infty, -2[\cup]2, +\infty[\\ \{-2, 1\} \quad \text{si } x = -2 \\ \{-1, 2\} \quad \text{si } x = 2 \end{cases}$$

Proposition 3.1

Soit $\Re$ une relation d'équivalence sur un ensemble E. On a les propriétés suivantes :

1. $\forall x \in E$,
$$Cl(x) \neq \varnothing$$
2. $$Cl(x) = Cl(y) \Leftrightarrow x \Re y$$
3. $\forall x, y \in E$,
$$Cl(x) = Cl(y) \quad \text{ou} \quad Cl(x) \cap Cl(y) = \varnothing$$
4. *Soit F un ensemble de représentants de toutes les classes alors $\{Cl(x),\ x \in F\}$ constitue une partition de E.*

Démonstration :

1. Comme $\Re$ est une relation d'équivalence, alors $x \Re x$ ($\Re$ est réflexive).

d'où $x \in Cl(x)$,donc $Cl(x) \neq \varnothing$.

2.

($\Rightarrow$) Supposons que $Cl(x) = Cl(y)$.

Soit $z \in Cl(x)$, alors $z \in Cl(y)$ et donc $z \Re x$ et $z \Re y$, d'après la transitivitè, $x \Re y$.

($\Leftarrow$) Supposons que $x\Re y$.

On démontre que $Cl\,(x) \subset Cl\,(y)$.

Soit $z \in Cl\,(x)$, alors $z\Re x$ et comme $x\Re y$, alors d'après la transitivité, $z\Re y$ ce qui implique $z \in Cl\,(y)$.

D'où $Cl\,(x) \subset Cl\,(y)$.

De la même manière on démontre que $Cl\,(y) \subset Cl\,(x)$.

3. Soient $x, y \in E$. Supposons que $Cl\,(x) \cap Cl\,(y) \neq \varnothing$, alors il existe $z \in Cl\,(x) \cap Cl\,(y)$, donc $z\Re x$ et $z\Re y$.

Montrons que $Cl\,(x) = Cl\,(y)$.

Soit $t \in Cl\,(x)$, alors

$$((t\Re x) \wedge (z\Re x)) \wedge (z\Re y)\,.$$

Comme $\Re$ est symétrique et transitive, alors

$$(t\Re z) \wedge (z\Re y)\,,$$

et d'après la transitivité de $\Re$, on déduit que

$$t\Re y,$$

ce qui implique

$$t \in Cl\,(y)\,,$$

d'où

$$Cl\,(x) \subset Cl\,(y)\,.$$

De la même manière, on démontre que

$$Cl\,(y) \subset Cl\,(x)\,,$$

finalement, on trouve

$$Cl\,(x) = Cl\,(y)\,.$$

4. Est une conséquence directe de (1) et (3) : Il faut montrer que

(a) -

$$E = \bigcup_{\dot{a_i} \in E_{/\Re}} \dot{a_i}$$

(b) -

$$\dot{a_i} \cap \dot{a_j} = \varnothing, \quad i \neq j$$

(a) est une conséquence de (1) : Les classes d'équivalence de E sont toutes non vides (tout élément de E appartient à une classe d'équivalence).
(b) est une conséquence de (3) : Deux classes d'équivalences sont soit les mêmes, soit disjointes.

3.4 Les congruences

Définition 3.9 *Soit n un entier naturel non nul. On dit que deux entiers relatifs a et b sont congrus modulo n ou encore que a est congru à b modulo n si n divise $a - b$. On notera $a \equiv b$ mod n ou $a \equiv b[n]$.*

Exemple 3.10

– $2021 \equiv 21[20]$.

– $305 \equiv -15[5]$.

Proposition 3.2

La relation de congruence modulo n est une relation d'équivalence.

Preuve

Soient n un entier naturel non nul et $a, b, c \in \mathbb{Z}$. On a :

(i)

$$a - a = 0 = 0 \times n \Rightarrow a \equiv a[n]$$

Alors, la relation de congruence est réflexive.

(ii)

$$a \equiv b[n] \Rightarrow a - b = kn$$

$$\Rightarrow b - a = (-k)\, n$$

$$\Rightarrow b \equiv a[n]$$

Alors, la relation de congruence est symétrique.

(iii)

$$(a \equiv b[n] \text{ et } b \equiv c[n]) \Rightarrow (a - b = k_1 n \text{ et } b - c = k_2 n)$$

$$\Rightarrow (a - b + b - c = k_1 n + k_2 n)$$

$$\Rightarrow a - c = (k_1 + k_2)\, n$$

$$\Rightarrow a \equiv c[n]$$

Alors, la relation de congruence est transitive.

De (i), (ii) et (iii) on déduit que la relation de congruence est une relation d'équivalence.

Proposition 3.3

$a \equiv b[n]$ si et seulement si a et b ont le même reste dans la division euclidienne par n.

Preuve

Soient (q_1, r_1) et (q_2, r_2) les deux couples uniques d'entiers tels que

$$a = q_1 n + r_1 \quad \text{et} \quad b = q_2 n + r_2,$$

avec $0 \leq r_1, r_2 < n$.

Alors,

$$a - b = (q_1 - q_2)\, n + (r_1 - r_2)$$

$$a - b \in n\mathbb{Z} \Leftrightarrow r_1 - r_2 \in n\mathbb{Z}.$$

Or

$$-n < r_1 - r_2 < n \quad \text{et} \quad]-n, n[\cap n\mathbb{Z} = \{0\},$$

donc

$$r_1 = r_2.$$

Proposition 3.4

Soient n un entier naturel non nul et $a, b, c, d \in \mathbb{Z}$.

1. *Si $a \equiv b[n]$ et si $c \equiv d[n]$, alors*

$$a + c \equiv b + d[n], \qquad a - c \equiv b - d[n], \qquad a \times c \equiv b \times d[n], \qquad a^k \equiv b^k[n] \text{ avec } k \in \mathbb{N}^*$$

2. *Si $a \equiv b[n]$, alors pour tout $p \in \mathbb{Z}$*

$$a + p \equiv b + p[n], \qquad a - p \equiv b - p[n], \qquad a \times p \equiv b \times p[n]$$

Preuve

Soient n un entier naturel non nul et $a, b, c, d \in \mathbb{Z}$.

1. Si $a \equiv b[n]$ et si $c \equiv d[n]$, alors

   - $a - b$ est un multiple de n et $c - d$ est un multiple de n.

   On en déduit que : $(a - b) + (c - d)$ et $(a - b) - (c - d)$ sont des multiples de n.

   C'est-à-dire $(a + c) - (b + d)$ et $(a - c) - (b - d)$ sont des multiples de n.

   Donc $a + c \equiv b + d[n]$ et $a - c \equiv b - d[n]$.

   - Puisque $a - b$ est un multiple de n , $c(a - b)$ est un multiple de n.

   Puisque $c - d$ est un multiple de n , $b(c - d)$ est un multiple de n.

   On en déduit que $c(a - b) + b(c - d)$ est un multiple de n.

   C'est-à-dire $ca - cb + bc - bd$ est un multiple de n.

   On a alors $ac - bd$ est un multiple de n , c'est-à-dire $ac \equiv bd[p]$.

   - Considérons pour $k \in \mathbb{N}^*$ la proposition $P(k) : a^k \equiv b^k[n]$.

   Pour $k = 1$, on a $a^1 = a$ et $b^1 = b$ et on sait que $a \equiv b[n]$ donc $P(1)$ est vraie.

   Supposons que la proposition $P(k)$ est vraie pour un entier $k \geq 1$.

   On a $a^k \equiv b^k[n]$ et $a \equiv b[n]$. On en déduit que (d'après la propriété précédente) : $a^k \times a \equiv b^k \times b[n] \Leftrightarrow a^{k+1} \equiv b^{k+1}[n]$

   La proposition $P(k + 1)$ est donc vraie.

   On a donc démontré par récurrence que $P(k)$ est vraie pour tout entier $k \geq 1$.

   Donc $a^k \equiv b^k[n]$ pour tout $k \in \mathbb{N}^*$.

2. *Si* $a \equiv b[n]$*, alors pour tout* $p \in \mathbb{Z}$

   - Alors $a - b$ est un multiple de n ,

   On peut écrire $a - b = (a + p) - (b + p)$. Donc $(b + p) - (a + p)$ est un multiple de n.

   On en déduit que $a + p \equiv b + p[n]$ pour tout $p \in \mathbb{Z}$.

   - De même on peut écrire $a - b = (a - p) - (b - p)$. Donc $a - p \equiv b - p[n]$ pour tout $p \in \mathbb{Z}$.

   D'autre part, puisque $a - b$ est un multiple de n, pour tout $p \in \mathbb{Z}$, $p(a - b)$ est un multiple de n, c'est-à-dire que $ap - bp$ est un multiple de n donc $a \times p \equiv b \times p[n]$.

3.5 Ensemble $\mathbb{Z}/n\mathbb{Z}$

Pour tout entier $n \geq 2$, $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble quotient de $\mathbb{Z}$ par la relation de congruence modulo n.

On a :

$$\mathbb{Z}/n\mathbb{Z} = \left\{\dot{0}, \dot{1}, \dot{2}, ..., \widehat{\dot{n-1}}\right\}$$

où $\dot{x}$ est la classe de x c'est à dire l'ensemble des nombres dont la division euclidienne par n a pour reste x.

Exemple 3.11

– $\mathbb{Z}/2\mathbb{Z} = \left\{\dot{0}, \dot{1}\right\}$ *avec* $\dot{0} = \{$*nombre pairs*$\}$ *et* $\dot{1} = \{$*nombre impairs*$\}$.

– $\mathbb{Z}/5\mathbb{Z} = \left\{\dot{0}, \dot{1}, \dot{2}, \dot{3}, \dot{4}\right\}$.

Opérations

On va définir une opération somme notée $\dot{+}$ et une opération multiplication notée $\dot{\times}$ sur $\mathbb{Z}/n\mathbb{Z}$ de la façon suivante :

$$\dot{a} \ \dot{+} \ \dot{b} = \widehat{\dot{a+b}}$$

$$\dot{a} \ \dot{\times} \ \dot{b} = \widehat{\dot{a \times b}}$$

Exemple 3.12

Quelques calculs dans $\mathbb{Z}/9\mathbb{Z}$

–

$$\dot{5} \ \dot{+} \ \dot{6} \ = \ \widehat{\dot{11}} \ = \ \dot{2}\,, \quad \dot{3} \ \dot{\times} \ \dot{7} \ = \ \widehat{\dot{21}} \ = \ \dot{3}$$

–

$$\dot{3} \ \dot{+} \ \dot{6} \ = \ \widehat{\dot{9}} \ = \ \dot{0}\,,$$

on dit que $\dot{3}$ est l'opposé de $\dot{6}$ et que $\dot{6}$ est l'opposé de $\dot{3}$.

–

$$\dot{2} \ \dot{\times} \ \dot{5} \ = \ \widehat{\dot{10}} \ = \ \dot{1}\,,$$

on dit que $\dot{2}$ est l'inverse de $\dot{5}$ et que $\dot{5}$ est l'inverse de $\dot{2}$.

–

$$\dot{3} \ \dot{\times} \ \dot{6} \ = \ \widehat{\dot{9}} \ = \ \dot{0}$$

on dit que $\dot{3}$ et $\dot{6}$ sont des diviseurs de zéros.

Exemple 3.13

L'opération somme $\dot{+}$ *et l'opération multiplication* $\dot{\times}$ *sur* $\mathbb{Z}/5\mathbb{Z}$

$\dot{+}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{0}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{1}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{0}$
$\dot{2}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{0}$	$\dot{1}$
$\dot{3}$	$\dot{3}$	$\dot{4}$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{4}$	$\dot{4}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$

$\dot{\times}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{4}$	$\dot{1}$	$\dot{3}$
$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{1}$	$\dot{4}$	$\dot{2}$
$\dot{4}$	$\dot{0}$	$\dot{4}$	$\dot{3}$	$\dot{2}$	$\dot{1}$

3.6 Exercices

Exercice 1

Soit $\Re$ *la relation binaire dans* $E = \{0, 1, 2, 3, 4, 5\}$ *définie par* $x\Re y$ *si et seulement si* $x \times y$ *est pair.*

1. Déterminer $\Gamma_{\Re}$ *graphe de* $\Re$.

2. $\Re$ *est-elle réflexive ? est-elle symétrique ? antisymétrique ? transitive ?*

Solution

1. Déterminer $\Gamma_{\Re}$ graphe de $\Re$.

$$\Gamma_{\Re} = \{(x,y) \in E \times E \ / \ x \Re y\}$$

$$= \{(x,y) \in E \times E \ / \ x \times y \ \textit{est pair}\}$$

$$= \left\{ \begin{array}{c} (0,0)\,,(0,1)\,,(0,2)\,,(0,3)\,,(0,4)\,,(0,5)\,, \\ (1,0)\,,(1,2)\,,(1,4)\,,(2,0)\,,(2,1)\,,(2,2)\,, \\ (2,3)\,,(2,4)\,,(2,5)\,,(3,0)\,,(3,2)\,,(3,4)\,, \\ (4,0)\,,(4,1)\,,(4,2)\,,(4,3)\,,(4,4)\,,(4,5)\,, \\ (5,0)\,,(5,2)\,,(5,4) \end{array} \right\}$$

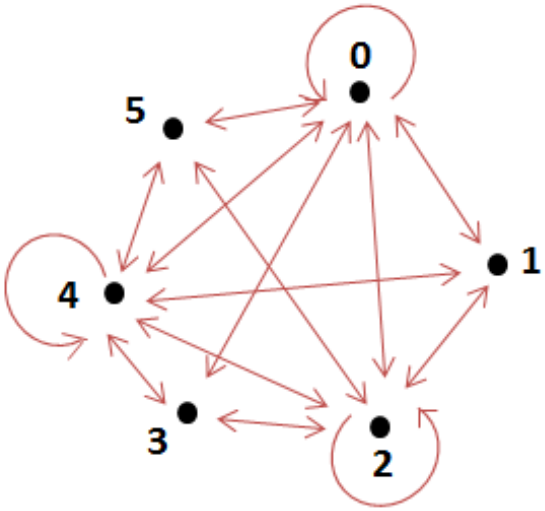


Fig 3.2 : Graphe de la relation «$\Re$»
sur l'ensemble $E = \{0,1,2,3,4,5\}$

2. $\Re$ est-elle réflexive ?

$\Re$ n'est pas réflexive, car il existe $x \in E$ tel que x n'est pas en relation avec lui même. (Par exemple $x = 1$, on a $1 \times 1 = 1$ est impair).

Est-elle symétrique ?

$\Re$ est symétrique, car pour tout $x, y \in E$ on a

$$x\Re y \Rightarrow x \times y \text{ est pair}$$

$$\Rightarrow y \times x \text{ est pair}$$

$$\Rightarrow y\Re x$$

Est-elle antisymétrique ?

$\Re$ n'est pas antisymétrique, car il existe $x, y \in E$ tel que x est en relation avec y et y est en relation avec x mais $x \neq y$. (Par exemple $x = 1$ et $y = 0$, on a $(1\Re 0) \wedge (0\Re 1) \wedge (x \neq y)$).

Est-elle transitive ?

$\Re$ n'est pas transitive, car il existe $x, y, z \in E$ tel que $x\Re y$ et $y\Re z$ mais x n'est pas en relation avec z. (Par exemple $x = 1, y = 2$ et $z = 3$, on a $(1\Re 2)\wedge(2\Re 3)\wedge(1$ n'est pas en relation avec $3)$).

Exercice 2

Dans $\mathbb{R}$, *on définit la relation binaire* $\Re$ *par :*

$$\forall x, y \in \mathbb{R}, \quad x\Re y \Leftrightarrow x^4 - y^4 = x^2 - y^2$$

Montrer que $\Re$ *est une relation d'équivalence et déterminer la classe d'équivalence de* $x \in \mathbb{R}$.

Solution

1. Montrer que $\Re$ est une relation d'équivalence

Soient $x, y, z \in \mathbb{R}$, on a :

(i)

$$x^4 - x^4 = x^2 - x^2 \Rightarrow x\Re x$$

Alors, $\Re$ est réflexive.

(ii)

$$x\Re y \Rightarrow x^4 - y^4 = x^2 - y^2$$

$$\Rightarrow y^4 - x^4 = y^2 - x^2$$

$$\Rightarrow y\Re x$$

Alors, $\Re$ est symétrique.

(iii)

$$(x\Re y \text{ et } y\Re z) \Rightarrow (x^4 - y^4 = x^2 - y^2 \text{ et } y^4 - z^4 = y^2 - z^2)$$

$$\Rightarrow x^4 - y^4 + y^4 - z^4 = x^2 - y^2 + y^2 - z^2$$

$$\Rightarrow x^4 - z^4 = x^2 - z^2$$

$$\Rightarrow x\Re z$$

Alors, $\Re$ est transitive.

De (i), (ii) et (iii) on déduit que $\Re$ est une relation d'équivalence.

2. Déterminer la classe d'équivalence de $x \in \mathbb{R}$

Soit $x \in \mathbb{R}$, on a :

$$Cl\,(x) = \{y \in E \ / \ y\Re x\}$$

$$= \{y \in \mathbb{R} \ / \ y^4 - x^4 = y^2 - x^2\}$$

$$y^4 - x^4 = y^2 - x^2 \Leftrightarrow (y^2 - x^2)(y^2 + x^2) - (y^2 - x^2) = 0$$

$$\Leftrightarrow (y^2 - x^2)(y^2 + x^2 - 1) = 0$$

$$\Leftrightarrow \begin{cases} y^2 - x^2 = 0 \\ \\ y^2 + x^2 - 1 = 0 \end{cases}$$

On résout la deuxième équation.

Si $x \in]-1, 1[$, l'équation admet deux solutions

$$y = \sqrt{1 - x^2} \ \text{ ou } \ y = -\sqrt{1 - x^2}$$

Si $x = \pm 1$, l'équation admet une solution

$$y = 0$$

Si $x \in]-\infty, -1[\cup]1, +\infty[$, l'équation n'admet pas de solutions.

Donc,

$$Cl\,(x) = \begin{cases} \left\{-x, x, \sqrt{1 - x^2}, -\sqrt{1 - x^2}\right\} & \text{si } \ x \in]-1, 1[\\ \\ \{-x, x\} & \text{si } \ x \in]-\infty, -2[\cup]2, +\infty[\\ \\ \{-1, 0, 1\} & \text{si } \ x \in \{-1, 1\} \end{cases}$$

Exercice 3

Dans $\mathbb{Z}$, on définit la relation binaire $\Re$ par :

$$\forall x, y \in \mathbb{Z}, \quad x \Re y \Leftrightarrow x - y \text{ est un multiple de } 5.$$

1. Montrer que $\Re$ est une relation d'équivalence.

2. Déterminer l'ensemble quotient $\mathbb{Z}_{/\Re}$.

3. Montrer que $\dot{\overline{84}} = \dot{\overline{14}}$ et $\dot{\overline{52}} \cap \dot{\overline{31}} = \varnothing$.

Solution

1. Montrer que $\Re$ est une relation d'équivalence.

Soient $x, y, z \in \mathbb{Z}$, on a :

(i)

$$x - x = 0 = 0 \times 5 \Rightarrow x - y \text{ est un multiple de } 5$$

$$\Rightarrow x \Re x$$

Alors, $\Re$ est réflexive.

(ii)

$$x \Re y \Rightarrow x - y \text{ est un multiple de } 5$$

$$\Rightarrow x - y = 5k, \text{ avec } k \in \mathbb{Z}$$

$$\Rightarrow y - x = -5k,$$

$$\Rightarrow \exists p = -k \in \mathbb{Z}, \ y - x = 5p$$

$$\Rightarrow y - x \text{ est un multiple de } 5$$

$$\Rightarrow y \Re x$$

Alors, $\Re$ est symétrique.

(iii)

$$(x\Re y \text{ et } y\Re z) \Rightarrow (x-y \textit{ est un multiple de } 5 \text{ et } y-z \textit{ est un multiple de } 5)$$

$$\Rightarrow \begin{cases} x-y=5k_1 \\ \\ y-z=5k_2 \end{cases}, \quad avec \;\; k_1,k_2 \in \mathbb{Z}$$

$$\Rightarrow x-y+y-z=5k_1+5k_2$$

$$\Rightarrow x-z=5\left(k_1+k_2\right)$$

$$\Rightarrow \exists k_3=k_1+k_2 \in \mathbb{Z},\; x-z=5k_3$$

$$\Rightarrow x-z \textit{ est un multiple de } 5$$

$$\Rightarrow x\Re z$$

Alors, $\Re$ est transitive.

De (i), (ii) et (iii) on déduit que $\Re$ est une relation d'équivalence.

2. Déterminer l'ensemble quotient $\mathbb{Z}_{/\Re}$.

On sait que $\mathbb{Z}_{/\Re}$ est l'ensemble des classes d'équivalence de tous les éléments de $\mathbb{Z}$.

Et comme $\Re$ c'est la relation de congruence, alors

$$\mathbb{Z}_{/\Re}=\mathbb{Z}/5\mathbb{Z}=\left\{\dot{\overline{0}},\dot{\overline{1}},\dot{\overline{2}},\dot{\overline{2}},\dot{\overline{4}}\right\}$$

3. Montrer que $\dot{\overline{84}}=\dot{\overline{14}}$ et $\dot{\overline{52}} \cap \dot{\overline{31}} = \varnothing$.

On sait que deux classes d'équivalences sont soit les mêmes, soit disjointes.

On a

$$84-14=70=14\times 5,$$

ce qui implique

$$84\Re 14,$$

alors,

$$\dot{\overline{84}} \;=\; \dot{\overline{14}}.$$

Et on a

$$52-31=21,$$

ce qui implique

$$52 \textit{ n'est pas en relation avec } 31,$$

alors,

$$\dot{\overline{84}} \cap \dot{\overline{14}} = \varnothing$$

Exercice 4

Dans $\mathbb{R}^2$, *on définit la relation binaire* $\Re$ *par :*

$$(a,b) \ \Re \ (c,d) \Leftrightarrow a \leq c \textit{ et } b \leq d.$$

1. Montrer que $\Re$ *est une relation d'ordre.*

2. L'ordre est il total ?

Solution

1. Montrer que $\Re$ est une relation d'ordre.

Soient $(a_1,b_1),(a_2,b_2),(a_3,b_3) \in \mathbb{R}^2$, on a :

(i)

$$a_1 \leq a_1 \textit{ et } b_1 \leq b_1 \Rightarrow (a_1,b_1) \ \Re \ (a_1,b_1)$$

Alors, $\Re$ est réflexive.

(ii)

$$\begin{cases} (a_1,b_1) \ \Re \ (a_2,b_2) \\ \qquad et \\ (a_2,b_2) \ \Re \ (a_1,b_1) \end{cases} \Rightarrow \begin{cases} (a_1 \leq a_2) \ \wedge \ (b_1 \leq b_2) \\ \qquad et \\ (a_2 \leq a_1) \ \wedge \ (b_2 \leq b_1) \end{cases}$$

$$\Rightarrow \begin{cases} (a_1 \leq a_2) \ \wedge \ (a_2 \leq a_1) \\ \qquad et \\ (b_1 \leq b_2) \ \wedge \ (b_2 \leq b_1) \end{cases}$$

$$\Rightarrow \begin{cases} a_1 = a_2 \\ \quad et \\ b_1 = b_2 \end{cases}$$

$$\Rightarrow (a_1,b_1) = (a_2,b_2)$$

Alors, $\Re$ est antisymétrique.

(iii)

$$\begin{cases} (a_1,b_1)\ \Re\ (a_2,b_2) \\ \qquad et \\ (a_2,b_2)\ \Re\ (a_3,b_3) \end{cases} \Rightarrow \begin{cases} (a_1 \leq a_2)\ \wedge\ (b_1 \leq b_2) \\ \qquad et \\ (a_2 \leq a_3)\ \wedge\ (b_2 \leq b_3) \end{cases}$$

$$\Rightarrow \begin{cases} (a_1 \leq a_2)\ \wedge (a_2 \leq a_3) \\ \qquad et \\ (b_1 \leq b_2)\ \wedge\ (b_2 \leq b_3) \end{cases}$$

$$\Rightarrow \begin{cases} (a_1 \leq a_2)\ \wedge (a_2 \leq a_3) \\ \qquad et \\ (b_1 \leq b_2)\ \wedge\ (b_2 \leq b_3) \end{cases}$$

$$\Rightarrow \begin{cases} a_1 \leq a_3 \\ \quad et \\ b_1 \leq b_3 \end{cases}$$

$$\Rightarrow (a_1,b_1)\ \Re\ (a_3,b_3)$$

Alors, $\Re$ est transitive.

De (i), (ii) et (iii) on déduit que $\Re$ est une relation d'ordre.

2. L'ordre est il total ?

Soient $(a_1,b_1) = (2,5), (a_2,b_2) = (7,3) \in \mathbb{R}^2$, on a :

$$(a_1,b_1)\ \textit{n'est pas en relation avec}\ (a_2,b_2)$$

$$et$$

$$(a_2,b_2)\ \textit{n'est pas en relation avec}\ (a_1,b_1)$$

On déduit que l'ordre est partiel.

Exercice 5

Soit T la relation sur $\mathbb{R}_+^*$ définie par :

$$xTy \Leftrightarrow \exists n \in \mathbb{N},\ y = x^n.$$

1. Montrer que T est une relation d'ordre.

2. L'ordre est il total ?

Solution

1. Montrer que T est une relation d'ordre.

Soient $x, y, z \in \mathbb{R}_+^*$, on a :

(i)

$$x = x^1 \Rightarrow \exists n = 1 \in \mathbb{N},\ x = x^n \Rightarrow xTx$$

Alors, T est réflexive.

(ii)

$$\begin{cases} x\ T\ y \\ \quad et \\ y\ T\ x \end{cases} \Rightarrow \begin{cases} \exists n_1 \in \mathbb{N},\ y = x^{n_1} \\ \quad et \\ \exists n_2 \in \mathbb{N},\ x = y^{n_2} \end{cases}$$

$$\Rightarrow x = (x^{n_1})^{n_2} = x^{n_1 n_2}$$

$$\Rightarrow n_1 n_2 = 1$$

$$\Rightarrow n_1 = n_2 = 1$$

donc,

$$x = y$$

Alors, T est antisymétrique.

(iii)

$$\begin{cases} x\ T\ y \\ \quad et \\ y\ T\ z \end{cases} \Rightarrow \begin{cases} \exists n_1 \in \mathbb{N},\ y = x^{n_1} \\ \quad et \\ \exists n_2 \in \mathbb{N},\ z = y^{n_2} \end{cases}$$

$$\Rightarrow z = y^{n_2} = (x^{n_1})^{n_2} = x^{n_1 n_2}$$

$$\Rightarrow \exists n_3 = n_1 n_2 \in \mathbb{N},\ z = x^{n_3}$$

$$\Rightarrow x\ T\ z$$

Alors, T est transitive.

De (i), (ii) et (iii) on déduit que T est une relation d'ordre.

2. L'ordre est il total ?

Soient $x = 5, y = 3 \in \mathbb{R}_+^*$, on a :

$$x \textit{ n'est pas en relation avec } y$$

$$\textit{et}$$

$$y \textit{ n'est pas en relation avec } x$$

On déduit que l'ordre est partiel.

Chapitre 4

Structures Algébriques

4.1 Loi de composition interne

Définition 4.1 *Soit E un ensemble.*

On appelle loi de composition interne (L.C.I) sur E, toute application de $E \times E$ dans E.

Exemple 4.1

- *Les lois de composition définies par l'addition et la multiplication sur les ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ sont des lois internes.*
- *Soit E un ensemble quelconque. Soient $X, Y \in P(E)$, la loi de composition $(X, Y) \to X \cup Y$ est une loi interne sur $P(E)$.*

4.1.1 Partie stable

Définition 4.2 *Soit $*$ une loi de composition interne dans un ensemble E.*

On dit que la loi $*$ est stable par rapport l'ensemble $F \subset E$ si

$$\forall x, y \in F, \quad x * y \in F.$$

4.1.2 Propriétés d'une loi de composition interne

Soient $*$ et Δ deux lois de composition interne dans un ensemble E.

1. *La loi $*$ est dite associative si et seulement si :*

$$\forall x, y, z \in E, \quad (x * y) * z = x * (y * z)$$

2. *La loi $*$ est dite commutative si et seulement si :*

$$\forall x, y \in E, \quad x * y = y * x$$

3. *La loi $*$ admet sur E un élément neutre (noté e), si et seulement si :*

$$\exists e \in E, \forall x \in E, \quad x * e = e * x = x$$

L'élément neutre, lorsqu'il existe, est unique. En effet, supposons que e' est un autre élément neutre pour la loi $*$, alors $e' = e' * e = e * e' = e$.

4. *L'élément $x \in E$ admet un élément symétrique, noté, x' si la loi $*$ admet un élément neutre e et si*

$$x * x' = x' * x = e$$

Le symétrique x' de $x \in E$ est unique pour la loi $*$. En effet, soit x'' un deuxième élément symétrique de x. En utilisant l'associativité de la loi $*$, on obtient

$$x' = e * x' = (x'' * x) * x' = x'' * (x * x') = x'' * e = x''.$$

5. *$*$ est distributive par rapport à Δ, si et seulement si :*

$$\forall x, y, z \in E, \quad \begin{cases} x * (y \Delta z) = (x * y) \, \Delta \, (x * z) \\ \\ (y \Delta z) * x = (y * x) \, \Delta \, (z * x) \end{cases}$$

6. *On dit que l'élément a est régulier si*

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

Proposition 4.1

Soit $\bigstar$ une loi de composition interne dans un ensemble E, associative et admettant un élément neutre e, alors

– *si a et b sont deux éléments inversibles (symétrisables), alors $(a \bigstar b)$ est inversible et on a :*

$$(a \bigstar b)^{-1} = b^{-1} \bigstar a^{-1}$$

– *Tout élément symétrisable dans* $(E, \bigstar)$ *est régulier.*

Preuve

1. Soient $a, b \in E$ deux éléments inversibles, alors

$$(a\bigstar b)\bigstar(b^{-1}\bigstar a^{-1}) = a\bigstar(b\bigstar b^{-1})\bigstar a^{-1}$$

$$= a\bigstar e\bigstar a^{-1}$$

$$= a\bigstar a^{-1}$$

$$= e$$

De la même manière on montre que

$$(b^{-1}\bigstar a^{-1})\bigstar(a\bigstar b) = e$$

d'où on déduit que $(a\bigstar b)$ est inversible et que

$$(a\bigstar b)^{-1} = b^{-1}\bigstar a^{-1}$$

2. Soit $x \in E$ un élément symétrisable dans E, alors x^{-1} existe et pour tous a et b dans E, on a :

$$a\bigstar x = b\bigstar x \Rightarrow (a\bigstar x)\bigstar x^{-1} = (b\bigstar x)\bigstar x^{-1}$$

$$\Rightarrow a\bigstar(x\bigstar x^{-1}) = b\bigstar(x\bigstar x^{-1})$$

$$\Rightarrow a\bigstar e = b\bigstar e$$

$$\Rightarrow a = b$$

Ce qui montre que x est régulier à droite de $\bigstar$.

De la même manière on montre que x est régulier à gauche de $\bigstar$.

4.2 Groupes

Définition 4.3 *Soit G un ensemble muni d'une loi $*$. On dit que $(G, *)$ est un groupe si et seulement si*

– $*$ *est interne dans G.*

– $*$ *est associative.*

– $*$ *admet un élément neutre dans G.*

– *Tout élément de G admet un symétrique pour la loi $*$.*

Et si de plus $*$ est commutative, on dit que G est un groupe abélien (ou commutatif).

Exemple 4.2

Soit $E =]-1, 1[$. On définit sur E la loi $*$ par

$$\forall a, b \in E,\ a * b = \tfrac{a+b}{1+ab}$$

Montrer que $(E, *)$ est un groupe abélien.

1. Montrer que $*$ est interne, c'est à dire

$$\forall a, b \in E,\ a * b \in E.$$

Soient $a, b \in E$, on a :

$$a, b \in E \Rightarrow |ab| < 1$$

$$\Rightarrow 1 + ab > 0$$

Donc,

$$a * b \in E \Leftrightarrow -1 < \tfrac{a+b}{1+ab} < 1$$

$$\Leftrightarrow \left|\tfrac{a+b}{1+ab}\right| < 1$$

$$\Leftrightarrow |a + b| < |1 + ab| = 1 + ab$$

$$\Leftrightarrow |a + b| - 1 - ab < 0$$

Premier cas : si $a + b \leq 0$, alors

$$|a + b| - 1 - ab = -a - b - 1 - ab$$

$$= -a\,(1 + b) - (1 + b)$$

$$= -\,(1 + a)\,(1 + b) < 0$$

Deuxième cas : si $a + b \geq 0$, alors

$$|a + b| - 1 - ab = a + b - 1 - ab$$

$$= a\,(1 - b) - (1 - b)$$

$$= -\,(1 - a)\,(1 - b) < 0$$

Dans les deux cas, on déduit que la loi $*$ est interne dans E.

2. La loi $*$ est commutative, c'est à dire

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

Soient $a, b \in E$, on a :

$$a * b = \frac{a+b}{1+ab} = \frac{b+a}{1+ba} = b * a$$

donc, $*$ est commutative.

3. La loi $*$ est associative, c'est à dire

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

Soient $a, b, c \in E$, on a :

$$a * (b * c) = \ a * \frac{b+c}{1+bc}$$

$$= \frac{a+\frac{b+c}{1+bc}}{1+a\frac{b+c}{1+bc}}$$

$$= \left(\frac{a+abc+b+c}{1+bc}\right) \times \left(\frac{1+bc}{1+bc+ab+ac}\right)$$

$$= \frac{a+b+c+abc}{1+bc+ab+ac},$$

et

$$(a * b) * c = \frac{a+b}{1+ab} * c$$

$$= \frac{\frac{a+b}{1+ab}+c}{1+\frac{a+b}{1+ab}c}$$

$$= \left(\frac{a+b+c+abc}{1+ab}\right) \times \left(\frac{1+ab}{1+ab+ac+bc}\right)$$

$$= \frac{a+b+c+abc}{1+ab+ac+bc}.$$

4. La loi $*$ est admet un élément neutre, c'est à dire

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

Soit $a \in E$, on cherche un élément e dans E tel que $a * e = e * a = a$.

On a :

$$a * e = a \Leftrightarrow \frac{a+e}{1+ae} = a$$

$$\Leftrightarrow a + e = a + a^2 e$$

$$\Leftrightarrow e\,(1 - a^2) = 0$$

$$\Rightarrow e = 0, \qquad car\ \ |a| < 1.$$

Comme la loi $*$ est commutative, alors

$$0 * a = a * 0 = a,$$

donc, $*$ admet un élément neutre $e = 0$.

5. Chaque élément de E admet un symétrique dans E, c'est à dire

$$\forall a \in E,\ \exists a' \in E,\ a * a' = a' * a = e.$$

Soit $a \in E$, on cherche un élément a' dans E tel que $a * a' = a' * a = e$.

On a :

$$a * a' = e \Leftrightarrow \tfrac{a+a'}{1+aa'} = 0$$

$$\Leftrightarrow a + a' = 0,$$

$$\Leftrightarrow a' = -a \in E.$$

Comme la loi $*$ est commutative, alors

$$a' * a = a * a' = 0,$$

donc, chaque élément a de E admet un symétrique $a' = -a$ dans E.

Finalement, $(E, *)$ est un groupe abélien.

4.2.1 Sous-groupe

Définition 4.4

Soit $(E, *)$ un groupe, on appelle sous groupe de $(E, *)$ tout sous ensemble non vide F de E tel que la restriction de $*$ à F en fait un groupe.

Proposition 4.2 *Soient $(E, *)$ un groupe d'élément neutre e et F un sous ensemble de E. On dit que F est un sous groupe de E si et seulement si*

– (i)

$$e \in F$$

– (ii)

$$\forall x, y \in F,\quad x * y \in F$$

– (iii)

$$\forall x \in F,\quad x^{-1} \in F$$

Exemple 4.3

1. *Soit $(E,*)$ un groupe d'élément neutre e. Alors, $F_1 = \emptyset$ et $F_2 = E$ sont des sous groupes de E.*

2. *L'ensemble*

$$n\mathbb{Z} = \{nk \ / \ k \in \mathbb{Z}\}, \quad avec \ \ n \in \mathbb{N}$$

est un sous groupe de $(\mathbb{Z},+)$

Proposition 4.3

Soient $(E,*)$ un groupe et F un sous ensemble de E.

On dit que F est un sous groupe de E si et seulement si

– (i)

$$F \neq \emptyset$$

– (ii)

$$\forall x, y \in F, \quad x * y^{-1} \in F$$

Preuve

(i) ($\Rightarrow$) Soit F un sous groupe de $(E,*)$, alors

– $*$ a un élémnt neutre dans F, donc $F \neq \emptyset$.

– Soient $x, y \in F$, comme F muni de la restriction de $*$ est un groupe alors y^{-1} existe dans F et comme F est stable par rapport à $*$ on déduit que $x * y^{-1} \in F$.

(ii) ($\Leftarrow$) Soit F un sous ensemble de E tel que

$$\begin{cases} F \neq \emptyset \\ \\ \forall x, y \in F, \quad x * y^{-1} \in F \end{cases}$$

Montrons que F muni de la restriction de $*$ est un groupe.

(1) Comme $F \neq \emptyset$ alors il existe $a \in F$ et d'après la deuxième hypothèse

$$e = a * a^{-1} \in F,$$

ce qui montre que la restriction de $*$ admet un élément neutre e dans F.

(2) Soit $x \in F$, c omme $e \in F$ alors d'après la deuxième hypothèse on aura

$$x^{-1} = e * x^{-1} \in F,$$

ce qui montre que tout élément x de F est inversible dans F par rapport à la restriction de $*$ à F.

(3) La restriction de $*$ à F est une loi de composition interne, car pour tous x et y dans F, d'après (2) on a

$$y^{-1} \in F$$

et en utilisant la deuxième hypothèse on déduit que

$$x * y = x * (y^{-1})^{-1} \in F$$

(4) La restriction de $*$ à F est associative, car $*$ est associative dans E.

Proposition 4.4

Soient $(E, *)$ un groupe d'élément neutre e et F_1, F_2 deux sous groupes de E. Alors $F_1 \cap F_2$ est un sous groupe de E.

Preuve

Notons $F = F_1 \cap F_2$. On a :

(i) $F \neq \emptyset$, car $e \in F_1, F_2$.

(ii) Soient $x, y \in F$

$$x, y \in F \Rightarrow x, y \in F_1 \cap F_2$$

$$\Rightarrow (x, y \in F_1) \text{ et } (x, y \in F_2)$$

$$\Rightarrow (x * y \in F_1) \text{ et } (x * y \in F_2)$$

$$\Rightarrow (x * y \in F_1 \cap F_2)$$

$$\Rightarrow x * y \in F$$

(iii) Soient $x \in F$

$$x \in F \Rightarrow x \in F_1 \cap F_2$$

$$\Rightarrow (x \in F_1) \text{ et } (x \in F_2)$$

$$\Rightarrow (x^{-1} \in F_1) \text{ et } (x^{-1} \in F_2)$$

$$\Rightarrow (x^{-1} \in F_1 \cap F_2)$$

$$\Rightarrow x^{-1} \in F$$

De (i), (ii) et (iii) on déduit que $F_1 \cap F_2$ *est un sous groupe de* E.

Remarque *En général, la réunion de sous groupes n'est pas un sous groupe.*

Exemple 4.4

On considère le groupe $(\mathbb{Z},+)$. *On a* $(2\mathbb{Z},+)$ *et* $(3\mathbb{Z},+)$ *sont deux sous groupes de* $(\mathbb{Z},+)$ *mais* $(2\mathbb{Z}\cup 3\mathbb{Z},+)$ *n'est pas un sous groupe de* $(\mathbb{Z},+)$, car

$$2,3\in 2\mathbb{Z}\cup 3\mathbb{Z} \text{ et } 2+3\notin 2\mathbb{Z}\cup 3\mathbb{Z}$$

4.2.2 Groupe quotient

Soient $(E,*)$ *un groupe et* F *un sous groupe de* E. *On définit une relation binaire* $\Re$ *sur* E *par :*

$$\forall a,b\in E,\quad a\ \Re\ b\Leftrightarrow a*b^{-1}\in F.$$

$\Re$ *est une relation d'équivalence sur* E.

En effet, pour $a,b,c\in E$ *on a :*

(i) $\Re$ est réflexive, car

$$a*a^{-1}=e\in F\ ,\quad car\ F\ \ est\ un\ sous\ groupe\ de\ E,$$

donc, $a\ \Re\ a$.

(ii) $\Re$ est symétrique, car

$$a\ \Re\ b\Rightarrow a*b^{-1}\in F$$

$$\Rightarrow (a*b^{-1})^{-1}\in F$$

$$\Rightarrow b*a^{-1}\in F$$

$$\Rightarrow b\ \Re\ a$$

(iii) $\Re$ est transitive, car

$$(a\ \Re\ b)\ et\ (b\ \Re\ c)\ \Rightarrow (a*b^{-1}\in F)\ et\ (b*c^{-1}\in F)$$

$$\Rightarrow (a*b^{-1})*(b*c^{-1})\in F\ ,\ \ car\ F\ \ est\ un\ sous\ groupe\ de\ E$$

$$\Rightarrow a*(b^{-1}*b)*c^{-1}\in F\ ,\quad car\ \ *\ \ est\ associative,$$

$$\Rightarrow a*c^{-1}\in F$$

$$\Rightarrow a\ \Re\ c$$

On note E/F l'ensemble quotient $E/\Re$. On définit sur $E/F \times E/F$ l'opération $\oplus$ par :

$$\forall \left(\dot{a}, \dot{b}\right) \in E/F \times E/F,\ \dot{a} \oplus \dot{b} \ = \ \dot{\overline{a * b}}$$

Proposition 4.5

Si $(E, *)$ est un groupe abélien, alors $(E/F, \oplus)$ est un groupe abélien, appelé groupe quotient de E par F.

Preuve

(1) $\oplus$ est une loi de composition interne,

On montre que $*$ est une application de $E/F \times E/F$ dans E/F.

Soient $\dot{a}, \dot{b}, \dot{c}, \dot{d} \in E/F$, montrons que

$$\left(\dot{a}, \dot{b}\right) = \left(\dot{c}, \dot{d}\right) \Rightarrow \ \dot{a} \oplus \dot{b} \ = \ \dot{c} \oplus \dot{d}$$

Supposons que $\left(\dot{a},\dot{b}\right)=\left(\dot{c},\dot{d}\right)$, alors : $\forall x\in E$,

$$x\in\ \dot{a}\oplus\dot{b}\ \Leftrightarrow x\in\ \overline{\dot{a*b}}$$

$$\Leftrightarrow x\Re\left(a*b\right)$$

$$\Leftrightarrow x*\left(a*b\right)^{-1}\in F$$

$$\Leftrightarrow x*b^{-1}*a^{-1}\in F$$

$$\Rightarrow\left(x*b^{-1}*a^{-1}\right)*\left(a*c^{-1}\right)\in F,\ car\ F\ est\ un\ sous\ groupe$$

$$\Rightarrow\left(x*b^{-1}\right)*\left(a^{-1}*a\right)*c^{-1}\in F,\ car\ *\ est\ associative$$

$$\Rightarrow\left(x*b^{-1}\right)*c^{-1}\in F$$

$$\Rightarrow\left(\left(x*b^{-1}\right)*c^{-1}\right)*\left(b*d^{-1}\right)\in F,\ car\ F\ est\ un\ sous\ groupe$$

$$\Rightarrow x*\left(b^{-1}*b\right)*c^{-1}*d^{-1}\in F,\ car\ *\ est\ associative\ et\ commtative$$

$$\Rightarrow x*c^{-1}*d^{-1}\in F$$

$$\Rightarrow x*\left(d*c\right)^{-1}\in F$$

$$\Rightarrow x\Re\left(d*c\right)$$

$$\Rightarrow x\Re\left(c*d\right),\ car\ *\ est\ commtative$$

$$\Rightarrow x\in\ \overline{\dot{c*d}}$$

$$\Rightarrow x\in\ \dot{c}\oplus\dot{d}$$

donc

$$\dot{a}\oplus\dot{b}\ \subset\ \dot{c}\oplus\dot{d},$$

et de la même manière on montre que

$$\dot{c}\oplus\dot{d}\ \subset\ \dot{a}\oplus\dot{b},$$

par suite :

$$\dot{a}\oplus\dot{b}\ =\ \dot{c}\oplus\dot{d},$$

ce qui montre que la loi $\oplus$ est interne dans E/F.

(2) $\oplus$ est associative, car $\forall \dot{a}, \dot{b}, \dot{c} \in E/F$, on a

$$\begin{aligned}
\dot{a} \oplus \left(\dot{b} \oplus \dot{c}\right) &= \dot{a} \oplus \left(\overline{\dot{b} * \dot{c}}\right) \\
&= \overline{\dot{a} * (\dot{b} * \dot{c})} \\
&= \overline{(\dot{a} * \dot{b}) * \dot{c}} \quad , \textit{car } * \textit{ est associative} \\
&= \left(\overline{\dot{a} * \dot{b}}\right) \oplus \dot{c} \\
&= \left(\dot{a} \oplus \dot{b}\right) \oplus \dot{c}
\end{aligned}$$

(3) $\oplus$ admet un élément neutre,

Si e est l'élément neutre de $*$, alors $\dot{e}$ est l'élément neutre de $\oplus$, car $\forall \dot{a} \in E/F$, on a

$$\dot{a} \oplus \dot{e} = \overline{\dot{a} * \dot{e}} = \dot{a}$$

et

$$\dot{e} \oplus \dot{a} = \overline{\dot{e} * \dot{a}} = \dot{a}$$

(4) Tout élément est inversible,

Soit $\dot{a} \in E/F$, alors $(\dot{a})^{-1} = \overline{\dot{a^{-1}}}$

$$\dot{a} \oplus (\dot{a})^{-1} = \overline{\dot{a} * a^{-1}} = \dot{e}$$

et

$$(\dot{a})^{-1} \oplus \dot{a} = \overline{\dot{a^{-1}} * a} = \dot{e}$$

(5) $\oplus$ est commutative, car $\forall \dot{a}, \dot{b} \in E/F$, on a

$$\begin{aligned}
\dot{a} \oplus \dot{b} &= \overline{\dot{a} * \dot{b}} \\
&= \overline{\dot{b} * \dot{a}}, \quad \textit{car } * \textit{ est commutative} \\
&= \dot{b} \oplus \dot{a}
\end{aligned}$$

De (1), (2), (3), (4) et (5) on déduit que $(E/F, \oplus)$ est un groupe abélien.

Exemple 4.5

On sait que $n\mathbb{Z}$ est un sous groupe de $(\mathbb{Z},+)$ avec $n \in \mathbb{N}$. Donc $(\mathbb{Z}/_{n}\mathbb{Z},\oplus)$ est un groupe quotient.

4.2.3 Groupe des permutations

Définition 4.5 *Soit E un ensemble non vide .*

On appelle permutation de E , toute bijection $\sigma : E \to E$.

Définition 4.6 *Lorsque l'ensemble $E = \{1,2,3,...\}$, on note S_n le groupe des permutations de E.*

S_n est un groupe fini de cardinal $n!$ que l'on appellera le groupe symétrique d'ordre n.

Une permutation $\sigma \in S_n$ se note :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & . & . & . & n \\ \sigma(1) & \sigma(2) & \sigma(3) & . & . & . & \sigma(n) \end{pmatrix}$$

Exemple 4.6

Supposons que $E = \{1.2,3,4\}$, soient σ, μ deux permutation de S_4 telles que :

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

et

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

On a :

$$\sigma(1) = 3, \sigma(2) = 1, \sigma(3) = 2, \sigma(4) = 4,$$

$$\mu(1) = 4, \mu(2) = 1, \mu(3) = 3, \mu(4) = 2,$$

On peut calculer $\sigma \circ \mu$ comme suit :

$$\sigma \circ \mu = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \sigma \circ \mu(1) & \sigma \circ \mu(1) & \sigma \circ \mu(3) & \sigma \circ \mu(4) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ \sigma(\mu(1)) & \sigma(\mu(1)) & \sigma(\mu(3)) & \sigma(\mu(4)) \end{pmatrix}$$

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

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

Exemple 4.7 *Déterminer les permutations de l'ensemble* $E = \{1.2, 3\}$.

Dans ce cas, on a : $S_3 = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$ tel que :

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = Id_3, \qquad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \qquad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \qquad \sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$(S_3, \circ)$ est un groupe non commutatif.

4.2.4 Homomorphisme de groupes- isomorphisme de groupes

Soient $(E, *)$ *et* (G, Δ) *deux groupes, avec* e *et* h *leurs éléments neutres respectifs.*

Définition 4.7

Une application $f : E \to G$ *est appelée homomorphisme de groupes de* E *dans* G *si :*

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

– *Si* f *est bijective, on dit que* f *est un isomorphisme (de groupes) de* E *sur* G. *On dit alors que* E *est isomorphe à* G, *ou que* E *et* G *sont isomorphes.*

– *Si $E = G$, on dit que f est un endomorphisme de E, et si de plus f est bijective, on dit que f est un automorphisme (de groupe) de E.*

Exemple 4.8

Soient f et g deux applications telles que :

$$f : (\mathbb{R}, +) \to (\mathbb{R}^*, \times)$$

$$x \mapsto e^x$$

et

$$g : (\mathbb{R}^*, \times) \to (\mathbb{R}, +)$$

$$x \mapsto \ln |x|$$

Pour $x, y \in \mathbb{R}$ et $a, b \in \mathbb{R}^*$ on a

$$f(x+y) = e^{x+y}$$

$$= e^x \times e^y$$

$$= f(x) \times f(y)$$

et

$$g(a \times b) = \ln |a \times b|$$

$$= \ln |a| + \ln |b|$$

$$= g(a) + g(b)$$

Alors, f est un homomorphisme de groupes de $(\mathbb{R}, +)$ dans $(\mathbb{R}^*, \times)$ et g est un homomorphisme de groupes de $(\mathbb{R}^*, \times)$ dans $(\mathbb{R}, +)$.

Définition 4.7

Soit $f : E \to F$ un homomorphisme de groupes de $(E, *)$ dans (G, Δ).

– *On appelle **noyau** de f l'ensemble*

$$\ker f = f^{-1}(\{h\}) = \{x \in E \ / \ f(x) = h\}$$

– *On appelle **image** de f l'ensemble*

$$\mathrm{Im}\, f = f(E) = \{f(x) \ / \ x \in E\}$$

Proposition 4.6

Soit $f : E \to F$ un homomorphisme de groupes de $(E, *)$ dans (G, Δ). Alors

1.

$$f(e) = h$$

2. $\forall x \in E$,

$$(f(x))^{-1} = f(x^{-1})$$

Preuve

1. On a

$$f(e * e) = f(e) = h \ \Delta \ f(e)$$

et comme f est un homomorphisme on déduit que

$$f(e) \ \Delta \ f(e) = h \ \Delta \ f(e)$$

et comme tous les éléments du groupe (G, Δ) sont réguliers, on dé duit que

$$f(e) = h$$

2. Soit $x \in E$, on a

$$f(x) \ \Delta \ f(x^{-1}) = f(x * x^{-1})$$

$$= f(e)$$

$$= h$$

et

$$f(x^{-1}) \ \Delta \ f(x) \ = f(x^{-1} * x)$$

$$= f(e)$$

$$= h$$

On dé duit que

$$(f(x))^{-1} = f(x^{-1})$$

Proposition 4.7

Soit $f : E \to F$ un homomorphisme de groupes de $(E, *)$ dans (G, Δ). Alors

1. L'image d'un sous groupe de E est un sous groupe de F.

2. L'image réciproque d'un sous groupe de F est un sous groupe de E.

Preuve

1. Soit E' un sous groupe de E .

(i) On a $e \in E'$, car E' est un sous groupe de E, donc

$$f(e) \in f(E'),$$

par suite

$$f(E') \neq \emptyset.$$

(ii) Soient $a, b \in f(E')$, alors il existe $x, y \in E'$ tels que $a = f(x)$ et $b = f(y)$, donc

$$a \ \Delta \ b^{-1} = f(x) \ \Delta \ (f(y))^{-1} = f(x) \ \Delta \ f(y^{-1}) = f(x * y^{-1})$$

et comme E' est un sous groupe de E alors $x * y^{-1} \in E'$, par suite

$$a \ \Delta \ b^{-1} = f(x * y^{-1}) \in f(E'),$$

de (i) e t (ii) on déduit que $f(E')$ est un sous groupe de F.

2. Soit F' un sous groupe de F, alors

(i) $f(e) = h$ et comme F' un sous groupe de F, alors

$$h \in F',$$

donc $e \in f^{-1}(F')$.

(ii) Soient $x, y \in f^{-1}(F')$, alors

$$f(x), f(y) \in F',$$

et comme F' estun sous groupe de F, alors

$$f(x)\Delta(f(y))^{-1} \in F' \Leftrightarrow f(x)\Delta f(y^{-1}) \in F'$$

$$\Leftrightarrow f(x * y^{-1}) \in F',$$

ce qui montre que

$$x * y^{-1} \in f^{-1}(F').$$

De (i) et (ii) on déduit que $f^{-1}(F')$ est un sous groupe de E.

Proposition 4.8

Soit $f : E \to F$ un homomorphisme de groupes de $(E, *)$ dans (G, Δ). Alors

1. f est injective si et seulement si $\ker f = \{e\}$.

2. f est surjective si et seulement si $\operatorname{Im} f = F$.

Preuve

Soit $f : E \to F$ un homomorphisme de groupes.

1. ($\Rightarrow$) Supposons que f est injectif.

On a

$$e \in \ker f.$$

Montrons que $\ker f \subset \{e\}$.

Soit $x \in \ker f$, alors $f(x) = h$

$$f(x) = h \Leftrightarrow f(x) = f(e)$$

$$\Rightarrow x = e \text{ , } car \text{ } f \text{ } est \text{ } injectif$$

$$\Rightarrow x \in \{e\}$$

d'où $\ker f \subset \{e\}$.

($\Leftarrow$) Supposons que $\ker f = \{e\}$.

Soient $a, b \in E$,

$$f(a) = f(b) \Rightarrow f(a) \ \Delta \ (f(b))^{-1} = h$$

$$\Rightarrow f(a) \ \Delta \ f(b^{-1}) = h$$

$$\Rightarrow f(a * b^{-1}) \ = h$$

$$\Rightarrow a * b^{-1} \in \ker f$$

$$\Rightarrow a * b^{-1} = e \ \text{ , } car \ \ker f = \{e\}$$

$$\Rightarrow a = b,$$

ce qui montre que f est injectif.

2. La preuve est immédiate, sachant que

$$\operatorname{Im} f = f(E)$$

4.3 Anneaux

Définition 4.8

On appelle anneau, tout ensemble A muni de deux lois de composition internes $+$ et $\bullet$ telles que :

1. $(A, +)$ *est un groupe abélien (on notera 0_A l'élément neutre de $+$).*
2. $\bullet$ *est associative*
3. $\bullet$ *est distributive par rapport à $+$.*

Si de plus $\bullet$ est commutative, on dit que $(A, +, \bullet)$ est un anneau commutatif.
Si $\bullet$ admet un élément neutre, l'anneau est dit unitaire.
On note 0_A l'élément neutre de $+$ et *1_A l'élément neutre de $\bullet$.*
On note $-x$ le symétriqe de x par la loi $+$ (appelé opposé de x) et x^{-1} le symétriqe de x par la loi $\bullet$ (appelé inverse de x).

Exemple 4.9

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

4.3.1 Règles de calculs dans un anneau

Soit $(A, +, \bullet)$ un anneau, alors on a les règles de calculs suivantes :
Pour tous x, y et $z \in A$,

1. $0_A \bullet x = x \bullet 0_A = 0_A$.
2. $x \bullet (-y) = (-x) \bullet y = -(x \bullet y)$.
3. $x \bullet (y - z) = (x \bullet y) - (x \bullet z)$.
4. $(y - z) \bullet x = (y \bullet x) - (z \bullet x)$.

Preuve

1. Soit $x \in A$, alors

$$0_A \bullet x = (0_A + 0_A) \bullet x = (0_A \bullet x) + (0_A \bullet x)$$

car $\bullet$ est distributive par rapport à $+$

comme tous les éléments de A sont symétrisables, on déduit que

$$0_A \bullet x = 0_A.$$

De la même manière on montre que

$$x \bullet 0_A = 0_A.$$

2. Soient $x, y \in A$ et montrons que $x \bullet (-y)$ est le symétrique de $(x \bullet y)$. On a :

$$(x \bullet (-y)) + (x \bullet y) = x \bullet (-y + y) = x \bullet 0_A = 0_A$$

comme $+$ est commutative on déduit que

$$(x \bullet (-y)) = -(x \bullet y).$$

De la même manière on montre que

$$(-x) \bullet y = -(x \bullet y).$$

La preuve des propriétés **3** et **4** utilise essentiellement la distributivité de la loi $\bullet$ par rapport à $+$.

4.3.2 Anneaux intègres

Définition 4.9

Soit $(A, +, \bullet)$ un anneau commutatif.

- *On dit que $y \in A^* = A \setminus \{0_A\}$ divise $x \in A$, ou que y est un diviseur de x ou que x est divisible par y, si*

$$\exists z \in A^*,\ x = y \bullet z.$$

- *Si 0_A ne possède pas de diviseur dans A, on dit que $(A, +, \bullet)$ est un anneau intègre ou un anneau d'intégrité.*
- *$(A, +, \bullet)$ est un anneau intègre si*

$$\forall x, y \in A,\ (\ x \bullet y = 0_A \Rightarrow x = 0_A \text{ ou } y = 0_A)$$

- *Ou encore, par contraposition, si*

$$\forall x, y \in A,\ (\ x \neq 0_A \text{ et } y \neq 0_A \Rightarrow\ x \bullet y \neq 0_A)$$

4.3.3 Sous anneaux

Définition 4.10

On appelle sous anneau de $(A, +, \bullet)$, tout sous ensemble A' de A tel que muni des restrictions des lois $+$ et $\bullet$ est anneau.

Si A est un anneau unitaire et $1_A \in A'$, on dit que A' est sous anneau unitaire.

Proposition 4.9

Un sous ensemble A'de A est un sous anneau si et seulement si :

1. $A' \neq \emptyset$,
2. $\forall x, y \in A', (x - y) \in A'$
3. $\forall x, y \in A', (x \bullet y) \in A'$.

Exemple 4.10

$(\mathbb{Z}, +, \times)$ *est un sous anneau de* $(\mathbb{R}, +, \times)$.

4.3.4 Homomorphisme d'anneaux

Soient $(A, +, \bullet)$ et $(B, \oplus, \otimes)$ deux anneaux et $f : A- \rightarrow B$.

Définition 4.11 *On dit que f est un homomorphisme d'anneaux si :*

$$\forall x, y \in A,\ f(x + y) = f(x) \oplus f(y) \quad et \quad f(x \bullet y) = f(x) \otimes f(y)$$

– *Si $A = B$ on dit que f est un endomorphisme d'anneau de A.*

– *Si f est bijective, on dit que f est un isomorphisme d'anneaux*

– *Si f est bijective et $A = B$, on dit que f est un automorphisme d'anneaux.*

4.3.5 Idéaux

Soit $(A, +, \bullet)$ un anneau.

Définition 4.12 *On appelle idéal à droite (respectivement à gauche) de l'anneau A, tout ensemble $I \subset A$ tel que*

1. *I est un sous groupe de $(A, +)$,*
2. *$\forall x \in A$, $(\forall y \in I)$, $x \bullet y \in I$ (respectivement $y \bullet x \in I$).*

Si I est idéal à droite et à gauche de A, on dit que I est un idéal bilatère de A.

Si l'anneau A est commutatif, tout idéal de A est bilatère, et dans ce cas on parle seulement d'Idéal sans préciser s'il l'est à droite, à gauche ou bilatère.

Exemple 4.11

– *Soit $(A, +, \bullet)$ un anneau, alors $I = \{O_A\}$ est un idéal bilatère de A.*

– *Dans l'anneau commutatif $(Z, +, \times)$, $n\mathbb{Z}$ est un idéal.*

4.3.6 Anneaux quotients

Soient $(A, +, \bullet)$ un anneau commutatif et I un idéal de A. On considère le groupe quotient $(A/I, \oplus)$, et on définit l'application $\otimes$ de $A/I \times A/I$ dans A/I par

$$\forall \left(\dot{a}, \dot{b}\right) \in A/I \times A/I,\ \dot{a} \otimes \dot{b} \ = \ \dot{\overline{a \bullet b}}$$

$(A/I, \oplus, \otimes)$ est anneau commutatif. Si de plus A est un anneau unitaire, alors $(A/I, \oplus, \otimes)$ est un anneau unitaire et $\dot{\overline{1_A}}$ est son élément unité.

4.4 Corps

Définition 4.13

On dit qu'un anneau unitaire $(\mathbb{k}, +, \bullet)$ est un corps si tout élément non nul de $\mathbb{k}$ est inversible.

Si de plus $\bullet$ est commutative, on dit que $\mathbb{k}$ est un corps commutatif.

Proposition 4.10

Tout corps est un anneau intègre.

Exemple 4.12

– *$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des corps commutatifs pour les lois usuelles $+, \times$.*

– *$(\mathbb{Z}, +, \times)$ n'est pas un corps car les éléments de $\mathbb{Z}$ n'ont pas d'inverses pour la loi $\times$.*

4.4.1 Sous corps

Définition 4.14

On appelle sous corps, d'un corps $(\mathbb{k}, +, \bullet)$, tout sous ensemble $\mathbb{k}'$ de $\mathbb{k}$ tel que, muni des restrictions des lois $+$ et $\bullet$ est un corps.

Proposition 4.11

$\Bbbk' \subset \Bbbk$ est un sous corps de $(\Bbbk, +, \bullet)$ si et seulement si

1. $\Bbbk' \neq \emptyset$
2. $\forall a, b \in \Bbbk'$, $a - b$ et $a \bullet b^{-1} \in \Bbbk'$.

Exemple 4.13

– $\mathbb{Q}$ est un sous corps de $\mathbb{R}$ pour les lois usuelles.

– $\mathbb{R}$ est un sous corps de $\mathbb{C}$ pour les lois usuelles.

Proposition 4.12

$\mathbb{Z}/_n\mathbb{Z}$ est un corps si n est premier

4.5 Exercices

Exercice 1

On munit $\mathbb{R}^2$ de la loi $\bigstar$ définie par :

$$\forall\,(x,y)\,,(x',y') \in \mathbb{R}^2, \quad (x,y) \bigstar (x',y') = \left(x + x', ye^{x'} + y'e^{-x}\right)$$

1. Montrer que $(\mathbb{R}^2, \bigstar)$ est un groupe.

2. $(\mathbb{R}^2, \bigstar)$ est-il abélien ?

Solution

1. Montrer que $(\mathbb{R}^2, \bigstar)$ est un groupe :

(1). Montrer que $\bigstar$ est interne, c'est à dire

$$\forall\,(x,y)\,,(x',y') \in \mathbb{R}^2, (x,y) \bigstar (x',y') \in \mathbb{R}^2.$$

Soient $(x,y)\,,(x',y') \in \mathbb{R}^2$, on a :

$$x + x' \in \mathbb{R}$$

$$et$$

$$ye^{x'} + y'e^{-x} \in \mathbb{R}$$

Donc,

$$\left(x + x', ye^{x'} + y'e^{-x}\right) \in \mathbb{R}^2$$

On déduit que la loi $\bigstar$ est interne dans $\mathbb{R}^2$.

(2). La loi ★ est associative, c'est à dire

$$\forall\,(x,y)\,,(x',y')\,,\left(x^{''},y^{''}\right)\in\mathbb{R}^2,\ \ (x,y)\bigstar\left((x',y')\bigstar\left(x^{''},y^{''}\right)\right)=((x,y)\bigstar(x',y'))\bigstar\left(x^{''},y^{''}\right).$$

Soient $(x,y)\,,(x',y')\,,\left(x^{''},y^{''}\right)\in\mathbb{R}^2$, on a :

$$\begin{aligned}(x,y)\bigstar\left((x',y')\bigstar\left(x^{''},y^{''}\right)\right)&=(x,y)\bigstar\left(x'+x^{''},y'e^{x^{''}}+y^{''}e^{-x'}\right)\\&=\left(x+x'+x^{''},ye^{x'+x^{''}}+\left(y'e^{x^{''}}+y^{''}e^{-x'}\right)e^{-x}\right)\\&=\left(x+x'+x^{''},ye^{x'+x^{''}}+y'e^{-x+x^{''}}+y^{''}e^{-x-x'}\right),\end{aligned}$$

et

$$\begin{aligned}((x,y)\bigstar(x',y'))\bigstar\left(x^{''},y^{''}\right)&=\left(x+x',ye^{x'}+y'e^{-x}\right)\bigstar\left(x^{''},y^{''}\right)\\&=\left(x+x'+x^{''},\left(ye^{x'}+y'e^{-x}\right)e^{x^{''}}+y^{''}e^{-x-x'}\right)\\&=\left(x+x'+x^{''},ye^{x'+x^{''}}+y'e^{-x+x^{''}}+y^{''}e^{-x-x'}\right),\end{aligned}$$

et donc on a

$$(x,y)\bigstar\left((x',y')\bigstar\left(x^{''},y^{''}\right)\right)=((x,y)\bigstar(x',y'))\bigstar\left(x^{''},y^{''}\right).$$

(3). La loi ★ est admet un élément neutre, c'est à dire

$$\exists\,(e_1,e_2)\in\mathbb{R}^2,\forall\,(x,y)\in\mathbb{R}^2,\ \ (x,y)\bigstar(e_1,e_2)=(e_1,e_2)\bigstar(x,y)=(x,y)\,.$$

Soit $(x,y)\in\mathbb{R}^2$, on a

$$\begin{aligned}(x,y)\bigstar(e_1,e_2)=(x,y)&\Leftrightarrow(x+e_1,ye^{e_1}+e_2e^{-x})\\&\Leftrightarrow\begin{cases}x+e_1=x\\ye^{e_1}+e_2e^{-x}=y\end{cases}\\&\Leftrightarrow\begin{cases}e_1=0\\y+e_2e^{-x}=y\end{cases}\\&\Rightarrow\begin{cases}e_1=0\\e_2=0\end{cases}\end{aligned}$$

et

$$(e_1, e_2) \bigstar (x, y) = (x, y) \Leftrightarrow (e_1 + x, e_2 e^x + y e^{-e_1}) = (x, y)$$

$$\Leftrightarrow \begin{cases} e_1 + x = x \\ \\ e_2 e^x + y e^{-e_1} = y \end{cases}$$

$$\Leftrightarrow \begin{cases} e_1 = 0 \\ \\ e_2 e^x + y = y \end{cases}$$

$$\Rightarrow \begin{cases} e_1 = 0 \\ \\ e_2 = 0 \end{cases},$$

donc, $\bigstar$ admet un élément neutre $(0, 0)$.

(4). Chaque élément de $\mathbb{R}^2$ admet un symétrique dans $\mathbb{R}^2$, c'est à dire

$$\forall\, (x, y) \in \mathbb{R}^2,\ \exists\, (a, b) \in \mathbb{R}^2,\ \ (x, y) \bigstar (a, b) = (a, b) \bigstar (x, y) = (0, 0)\,.$$

Soit $(x, y) \in \mathbb{R}^2$, on cherche un élément (a, b) dans $\mathbb{R}^2$ tel que $(x, y) \bigstar (a, b) = (a, b) \bigstar (x, y) = (0, 0)$.

On a :

$$(x, y) \bigstar (a, b) = (0, 0) \Leftrightarrow (x + a, y e^a + b e^{-x}) = (0, 0)$$

$$\Leftrightarrow \begin{cases} x + a = 0 \\ \\ y e^a + b e^{-x} = 0 \end{cases},$$

$$\Leftrightarrow \begin{cases} a = -x \\ \\ y e^{-x} + b e^{-x} = 0 \end{cases}.$$

$$\Leftrightarrow \begin{cases} a = -x \\ \\ b = -y \end{cases}$$

et

$$(a,b)\bigstar(x,y)=(0,0)\Leftrightarrow(a+x,be^{x}+ye^{-a})=(0,0)$$

$$\Leftrightarrow\begin{cases}a+x=0\\ \\ be^{x}+ye^{-a}=0\end{cases},$$

$$\Leftrightarrow\begin{cases}a=-x\\ \\ be^{x}+ye^{x}=0\end{cases}.$$

$$\Leftrightarrow\begin{cases}a=-x\\ \\ b=-y\end{cases},$$

donc, chaque élément $(x,y)\in\mathbb{R}^2$ admet un symétrique $(-x,-y)$ dans $\mathbb{R}^2$.

Finalement, $(\mathbb{R}^2,\bigstar)$ est un groupe.

2. $(\mathbb{R}^2,\bigstar)$ est-il abélien ?

C'est à dire la loi $\bigstar$ est-elle commutative ?

$$\forall\,(x,y),(x',y')\in\mathbb{R}^2,\ \ (x,y)\bigstar(x',y')=(x',y')\bigstar(x,y)\,.$$

On a

$$(x,y)\bigstar(x',y')=\left(x+x',ye^{x'}+y'e^{-x}\right)$$

et

$$(x',y')\bigstar(x,y)=\left(x'+x,y'e^{x}+ye^{-x'}\right)$$

Pour $(x,y)=(1,0)$ et $(x',y')=(0,1)$ on a :

$$(1,0)\bigstar(0,1)=(1,e^{-1})$$

$$(0,1)\bigstar(1,0)=(1,e)$$

D'où $(\mathbb{R}^2,\bigstar)$ n'est pas un groupe abélien.

Exercice 2

On considère les permutations suivantes

$$\sigma_1=\begin{pmatrix}1&2&3\\ \\ 1&3&2\end{pmatrix},\qquad\sigma_2=\begin{pmatrix}1&2&3\\ \\ 2&1&3\end{pmatrix}$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ & & \\ 2 & 3 & 1 \end{pmatrix}, \qquad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ & & \\ 3 & 1 & 2 \end{pmatrix}$$

1. Calculer $\sigma_1 \circ \sigma_2$, $\sigma_1 \circ \sigma_3$, $\sigma_2 \circ \sigma_3$, $\sigma_3 \circ \sigma_2$, $\sigma_4 \circ \sigma_4$.

2. $(S_3, \circ)$ *est - il groupe commutatif ?*

Solution

1. $\sigma_1 \circ \sigma_2$

$$\sigma_1 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ & & \\ \sigma_1 \circ \sigma_2(1) & \sigma_1 \circ \sigma_2(1) & \sigma_1 \circ \sigma_2(3) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ & & \\ \sigma_1(\sigma_2(1)) & \sigma_1(\sigma_2(1)) & \sigma_1(\sigma_2(3)) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ & & \\ \sigma_1(2) & \sigma_1(1) & \sigma_1(3) \end{pmatrix}$$

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

$$= \sigma_4$$

De la même manière, on trouve

$$\sigma_1 \circ \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ & & \\ 3 & 2 & 1 \end{pmatrix}, \qquad \sigma_2 \circ \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ & & \\ 1 & 3 & 2 \end{pmatrix} = \sigma_1$$

$$\sigma_3 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ & & \\ 3 & 2 & 1 \end{pmatrix}, \qquad \sigma_4 \circ \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ & & \\ 2 & 3 & 1 \end{pmatrix} = \sigma_3$$

2. $(S_3, \circ)$ n'est pas un groupe commutatif, car

$$\sigma_2 \circ \sigma_3 \neq \sigma_3 \circ \sigma_2$$

Exercice 3

Soient $(G, *)$ *un groupe et* H, K *deux sous-groupes de* G.

Démontrer que :

$H \cup K$ *est un sous-groupe de* G *si et seulement si* $H \subset K$ *ou* $K \subset H$.

Solution

($\Rightarrow$) En utilisant le raisonnement par l'absurde.

Supposons que $H \cup K$ est un sous-groupe de G et que ni $H \subset K$, ni $K \subset H$.

Soient $x \in H \setminus K$ et $y \in K \setminus H$.

Puisque $H \cup K$ est un groupe et que $x, y \in H \cup K$, on a $x * y \in H \cup K$.

Mais si $x * y \in H$, alors

$$x^{-1} * (x * y) = y \in H, \ \textit{car } H \textit{ est un sous groupe,}$$

ce qui est une contradiction.

On obtient de même une contradiction dans l'autre cas possible $x * y \in K$.

$$(x * y) * y^{-1} = x \in K, \ \textit{car } K \textit{ est un sous groupe.}$$

L'hypothèse de départ est donc fausse, alors d'après l'absurde on déduit que $H \subset K$ ou $K \subset H$.

($\Leftarrow$)Si $H \subset K$, alors $H \cup K = K$ qui est un sous-groupe de G.

De même, si $K \subset H$, $H \cup K = H$ qui est un sous-groupe de G.

Exercice 4

Soit

$$A = \left\{ \tfrac{m}{n}, \ m \in \mathbb{Z}, \ n \textit{ entier naturel impair} \right\}$$

Démontrer que $(A, +, \times)$ *est un anneau. Quels sont ses éléments inversibles ?*

Solution

1. Démontrons que A est un sous-anneau de $(\mathbb{Q}, +, \times)$.

Soient $x = \frac{m}{n}, y = \frac{p}{q} \in A$, on a :

$$x + (-y) = \tfrac{m}{n} - \tfrac{p}{q} = \tfrac{mq - pn}{nq}$$

$$et$$

$$xy = \tfrac{mp}{nq}$$

Comme nq, produit de deux nombres impairs, est impair, et que $A \neq \emptyset$ ($\text{car} 1_{\mathbb{Q}} = 1 \in A$), on déduit que A est un sous-anneau de $(\mathbb{Q}, +, \times)$.

2. Déterminons les inversibles de A.

Soit $x = \frac{m}{n} \in A$ inversible, et soit $y = \frac{p}{q} \in A$ tel que $xy = 1$.

$$xy = 1 \Leftrightarrow \frac{m}{n} = \frac{p}{q} \Leftrightarrow mq = np$$

En particulier, m est nécessairement impair.

Réciproquement, si $x = \frac{m}{n}$ avec m impair, alors $y = \frac{n}{m} \in A$ (si $m < 0$, il suffit d'écrire $y = \frac{-n}{-m}$) et $xy = 1$.

Donc, les inversibles de A sont les éléments $\frac{m}{n}$ avec $m \in \mathbb{Z}, n \in \mathbb{N}^*$ et m, n impairs.

Exercice 5

Soient $+$ et $\bullet$ deux lois de composition internes dans $\mathbb{R}^2$ définies par :

$$\forall (a,b),(c,d) \in \mathbb{R}^2, \quad (a,b) + (c,d) = (a+c, b+d)$$

$$\forall (a,b),(c,d) \in \mathbb{R}^2, \quad (a,b) \bullet (c,d) = (ac - bd, ad + cb)$$

Montrer que $(\mathbb{R}^2, +, \bullet)$ est un corps commutatif.

Solution

1. $(\mathbb{R}^2, +)$ est un groupe abélien

(a). $+$ est commutative

$$\forall (a,b),(c,d) \in \mathbb{R}^2, \quad (a,b) + (c,d) = (c,d) + (a,b)$$

Soient $(a,b),(c,d) \in \mathbb{R}^2$, on a

$$\begin{aligned}(a,b) + (c,d) &= (a+c, b+d) \\ &= (c+a, d+b) \\ &= (c,d) + (a,b)\end{aligned}$$

(b). $+$ est associaive,

$$\forall (a,b),(c,d),(e,f) \in \mathbb{R}^2, \quad (a,b) + ((c,d) + (e,f)) = ((a,b) + (c,d)) + (e,f)$$

Soient $(a,b),(c,d),(e,f) \in \mathbb{R}^2$, on a

$$\begin{aligned}(a,b) + ((c,d) + (e,f)) = &\ (a,b) + (c+e, d+f) \\ &= (a+c+e, b+d+f) \\ &= (a+c, b+d) + (e,f) \\ &= ((a,b) + (c,d)) + (e,f)\end{aligned}$$

(c). Elément neutre

$$\exists\,(e_1,e_2)\in\mathbb{R}^2,\forall\,(a,b)\in\mathbb{R}^2,\quad (a,b)+(e_1,e_2)=(e_1,e_2)+(a,b)=(a,b)$$

Soit $(a,b)\in\mathbb{R}^2$, on a

$$(a,b)+(e_1,e_2)=(a,b)\Leftrightarrow(a+e_1,b+e_2)=(a,b)$$

$$\Leftrightarrow\begin{cases}a+e_1=a\\ \\ b+e_2=b\end{cases}$$

$$\Leftrightarrow\begin{cases}e_1=0\\ \\ e_2=0\end{cases},$$

comme la loi + est commtative, alors

$$(e_1,e_2)+(a,b)=(a,b)+(e_1,e_2)=(a,b)\,,$$

d'où + possède un élément neutre $0_{\mathbb{R}^2}=(0,0)$.

(d). Elément symétrique

$$\forall\,(a,b)\in\mathbb{R}^2,\exists\,(a',b')\in\mathbb{R}^2,\quad (a,b)+(a',b')=(a',b')+(a,b)=(e_1,e_2)$$

Soit $(a,b)\in\mathbb{R}^2$,

$$(a,b)+(a',b')=(0,0)\Leftrightarrow(a+a',b+b')=(0,0)$$

$$\Leftrightarrow\begin{cases}a+a'=0\\ \\ b+b'=0\end{cases}$$

$$\Leftrightarrow\begin{cases}a'=-a\\ \\ b'=-b\end{cases}$$

comme la loi + est commtative, alors

$$(a',b')+(a,b)=(a,b)+(a',b')=(0,0)\,,$$

D'où tout élément $(a,b)\in\mathbb{R}^2$ est symétrisable et son symétrique est $(a',b')=(-a,-b)$.

2. • est associative,

$$\forall\,(a,b)\,,(c,d)\,,(e,f)\in\mathbb{R}^2,\quad (a,b)\bullet((c,d)\bullet(e,f))=((a,b)\bullet(c,d))\bullet(e,f)$$

Soient $(a,b),(c,d),(e,f) \in \mathbb{R}^2$, on a :

$$(a,b) \bullet ((c,d) \bullet (e,f)) = (a,b) \bullet (ce - df, cf + ed)$$

$$= (a(ce - df) - b(cf + ed), a(cf + ed) + (ce - df) b)$$

$$= (ace - adf - bcf - bed, acf + aed + ceb - dfb)$$

et

$$((a,b) \bullet (c,d)) \bullet (e,f) = (ac - bd, ad + cb) \bullet (e,f)$$

$$= ((ac - bd) e - (ad + cb) f, (ac - bd) f + e(ad + cb))$$

$$= (ace - bde - adf - cbf, acf - bdf + ade + cbe),$$

et donc on a

$$(a,b) \bullet ((c,d) \bullet (e,f)) = ((a,b) \bullet (c,d)) \bullet (e,f)$$

3. $\bullet$ est commtative,

$$\forall (a,b),(c,d) \in \mathbb{R}^2, \quad (a,b) \bullet (c,d) = (c,d) \bullet (a,b)$$

$$(a,b) \bullet (c,d) = (ac - bd, ad + cb)$$

$$= (ca - db, cb + ad)$$

$$= (c,d) \bullet (a,b)$$

4. $\bullet$ est distributive par rapport à $+$, $\forall (a,b),(c,d),(e,f) \in \mathbb{R}^2$,

$$(a,b) \bullet ((c,d) + (e,f)) = ((a,b) \bullet (c,d)) + ((a,b) \bullet (e,f))$$

et

$$((c,d) + (e,f)) \bullet (a,b) = ((c,d) \bullet (a,b)) + ((e,f) \bullet (a,b))$$

Soient $(a,b),(c,d),(e,f) \in \mathbb{R}^2$, on a

$$(a,b) \bullet ((c,d) + (e,f)) = (a,b) \bullet (c + e, d + f)$$

$$= (a(c + e) - b(d + f), a(d + f) + (c + e) b)$$

$$= (ac + ae - bd - bf, ad + af + cb + eb),$$

et

$$((a,b) \bullet (c,d)) + ((a,b) \bullet (e,f)) = (ac - bd, ad + cb) + (ae - bf, af + eb)$$

$$= (ac - bd + ae - bf, ad + cb + af + eb),$$

donc

$$(a,b)\bullet((c,d)+(e,f))=((a,b)\bullet(c,d))+((a,b)\bullet(e,f))$$

Comme la loi $\bullet$ est commtative, alors

$$\begin{aligned}((c,d)+(e,f))\bullet(a,b)&=(a,b)\bullet((c,d)+(e,f))\\&=((a,b)\bullet(c,d))+((a,b)\bullet(e,f))\\&=((c,d)\bullet(a,b))+((e,f)\bullet(a,b))\end{aligned}$$

d'où $\bullet$ est distributive par rapport à $+$.

5. Elément neutre par rapport à $\bullet$

$$\exists\,(a_1,a_2)\in\mathbb{R}^2,\forall\,(a,b)\in\mathbb{R}^2,\quad (a,b)\bullet(a_1,a_2)=(a_1,a_2)\bullet(a,b)=(a,b)$$

Soit $(a,b)\in\mathbb{R}^2$

$$(a,b)\bullet(a_1,a_2)=(a,b)\Leftrightarrow(aa_1-ba_2,aa_2+a_1b)=(a,b)$$

$$\Leftrightarrow\begin{cases}aa_1-ba_2=a\\ \\aa_2+a_1b=b\end{cases}$$

$$\Leftrightarrow\begin{cases}a_1=1\\ \\a_2=0\end{cases},$$

comme la loi $\bullet$ est commtative, alors

$$(a_1,a_2)+(a,b)=(a,b)+(a_1,a_2)=(a,b)\,,$$

d'où $\bullet$ possède un élément neutre $1_{\mathbb{R}^2}=(1,0)$

6. Elément symétrique par rapport à $\bullet$

$$\forall\,(a,b)\in\mathbb{R}^2-\{(0,0)\}\,,\exists\,(a',b')\in\mathbb{R}^2-\{(0,0)\}\,,\quad (a,b)\bullet(a',b')=(a',b')\bullet(a,b)=(1,0)$$

Soit $(a,b)\in\mathbb{R}^2-\{(0,0)\}$, on cherche un élément (a',b') dans $\mathbb{R}^2-\{(0,0)\}$ tel que

$$(a,b)\bullet(a',b')=(a',b')\bullet(a,b)=(1,0)$$

On a :

$$(a,b) \bullet (a',b') = (1,0) \Leftrightarrow (aa' - bb', ab' + a'b) = (1,0)$$

$$\Leftrightarrow \begin{cases} aa' - bb' = 1 \\ \\ ab' + a'b = 0 \end{cases}$$

$$\Leftrightarrow \begin{cases} a' = \frac{a}{a^2+b^2} \in \mathbb{R}^* \\ \\ b' = \frac{-b}{a^2+b^2} \in \mathbb{R}^* \end{cases},$$

comme la loi $\bullet$ est commtative, alors

$$(a',b') + (a,b) = (a,b) + (a',b') = (1,0)\,,$$

donc, chaque élément $(a,b) \in \mathbb{R}^2 - \{(0,0)\}$ admet un inverse $\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$ dans $\mathbb{R}^2 - \{(0,0)\}$.

Exercice 6

1. *Est-ce que* $\dot{\overline{23}}$ *est inversible dans* $\mathbb{Z}/_{121}\mathbb{Z}$ *? Si oui, quel est son inverse ?*
2. *Est-ce que* $\dot{\overline{25}}$ *est inversible dans* $\mathbb{Z}/_{90}\mathbb{Z}$ *? Si oui, quel est son inverse ?*

Solution

1. 23 et 121 sont premiers entre eux, et donc $\dot{\overline{23}}$ est inversible dans $\mathbb{Z}/_{121}\mathbb{Z}$.

Pour trouver son inverse, il faut résoudre l'équation de Bezout

$$23u + 121v = 1$$

Avec l'algorithme d'Euclide, on trouve que

$$121 = 23 \times 5 + 6$$

$$23 = 6 \times 3 + 5$$

$$6 = 5 \times 1 + 1$$

$$6 = 5 \times 1 + 1 \Leftrightarrow 6 - 5 \times 1 = 1$$

$$\Leftrightarrow 6 - (23 - 6 \times 3) = 1$$

$$\Leftrightarrow 6 \times (4) + 23 \times (-1) = 1$$

$$\Leftrightarrow (121 - 23 \times 5) \times (4) + 23 \times (-1) = 1$$

$$\Leftrightarrow 121 \times (4) + 23 \times (-21) = 1$$

Ainsi, l'inverse de $\dot{\overline{23}}$ dans $\mathbb{Z}/_{121}\mathbb{Z}$ est $\dot{\overline{-21}} = \dot{\overline{100}}$.

2. 5 divise à la fois 25 et 90. Ainsi, $\dot{\overline{25}}$ n'est pas inversible dans $\mathbb{Z}/_{90}\mathbb{Z}$.

Exercice 7

1. *Montrer que $\mathbb{Z}/_6\mathbb{Z}$ admet des diviseurs de zéro. $\mathbb{Z}/_6\mathbb{Z}$ est -il un corps ?*
2. *Montrer que $\mathbb{Z}/_5\mathbb{Z}$ est un corps.*

Solution

1. On sait que

$$\mathbb{Z}/_6\mathbb{Z} = \left\{\dot{\overline{0}}, \dot{\overline{1}}, \dot{\overline{2}}, \dot{\overline{3}}, \dot{\overline{4}}, \dot{\overline{5}}\right\}$$

On a :

$$\dot{\overline{2}} \times \dot{\overline{3}} = \dot{\overline{0}}$$

et

$$\dot{\overline{4}} \times \dot{\overline{3}} = \dot{\overline{0}}$$

Donc, $\mathbb{Z}/_6\mathbb{Z}$ admet des diviseurs de zéro.

Ce qui montre que $\mathbb{Z}/_6\mathbb{Z}$ n'est pas un corps.

2. $\mathbb{Z}/_5\mathbb{Z}$ est un corps, car 5 est premier.

Chapitre 5

Anneaux de Polynômes

5.1 Polynôme

Définition 5.1

Soit $\Bbbk = \mathbb{R}$ *ou* $\mathbb{C}$.

Un polynôme à coefficient dans $\Bbbk$ *est une expression de la forme*

$$P(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n$$

$$= \sum_{i=0}^{n} a_iX^i,$$

où $n \in \mathbb{N}$ *et les coefficients* $a_0, a_1, ..., a_n$ *sont des éléments de* $\Bbbk$. *Le symbole* X *est appelé l'indéterminée (on pose* $X^0 = 1$ *).*

– *L'ensemble des polynômes à coefficients dans* $\Bbbk$ est *noté* $\Bbbk[X]$.

$$\Bbbk[X] = \{\textit{polynômes à coefficients dans } \Bbbk\}$$

– *Les* a_i *sont appelés les coefficients du polynôme.*

– *Si tous les coefficients* a_i *sont nuls,* P *est appelé le polynôme nul, il est noté* 0.

– *Les polynômes comportant un seul terme non nul (du type* a_kX^k*) sont appelés monômes.*

– *Soit* $P(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n$, *un polynôme avec* $a_n \neq 0$. *On appelle terme dominant le monôme* a_nX^n. *Le coefficient* a_n *est appelé le coefficient dominant de* P.

– *Si le coefficient dominant est* 1, *on dit que* P *est un polynôme unitaire.*

Exemple 5.1

– $P(X) = 3 - 5X + X^2$ et $Q(X) = 7 + X^6$ sont deux polynômes.

– $R(X) = \frac{4+X^2}{1+X}$ n'est pas un polynôme.

5.1.1 Degré

Définition 5.2

– *Soit P un polynôme non nul, on appelle degré de P, le plus grand indice de ses coefficients non nuls, et on le note $degP$.*

Ainsi

$$degP = n \Leftrightarrow P(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n, \text{ avec } a_n \neq 0.$$

a_n s'appelle coefficient dominant de P. Par convention $\deg(0) = -\infty$.

– *Un polynôme de la forme $P = a_0$ avec $a_0 \in \mathbb{k}$ est appelé un polynôme constant. Si $a_0 \neq 0$, son degré est 0.*

– On note

$$\mathbb{k}_n[X] = \{P \in \mathbb{k}[X] \ / \ \deg(P) \leq n\}.$$

Exemple 5.2

– $P(X) = 1 - X + X^5$ est un polynôme de degré 5.

– $P(X) = 2 + X^{2n+1}$ est un polynôme de degré $2n+1$.

– $Q(X) = 3$ est un polynôme de degré 0.

Théorème 5.1

Soient $P, Q \in \mathbb{k}[X]$, on a :

–

$$\deg(P+Q) \leq \max(\deg(P), \deg(Q))$$

–

$$\deg(P \times Q) = \deg(P) + \deg(Q)$$

– *Soit λ une constante non nulle alors :*

$$\deg(\lambda P) = \deg(P)$$

Proposition 5.1

$\mathbb{k}[X]$ est intègre. $\forall P, Q \in \mathbb{k}[X]$

$$(P.Q = 0) \Rightarrow (P = 0 \text{ ou } Q = 0)$$

Preuve

Soient $P, Q \in \Bbbk[X]$, on a

$$(P.Q = 0) \Rightarrow \deg(P \times Q) = \deg(P) + \deg(Q) = -\infty$$

$$\Rightarrow \deg(P) = -\infty \text{ ou } \deg(Q) = -\infty$$

$$\Rightarrow (P = 0 \text{ ou } Q = 0)$$

5.2 Opérations sur les polynômes

5.2.1 Egalité

Soient $P, Q \in \Bbbk[X]$ tels que

$$P(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n$$

$$Q(X) = b_0 + b_1X + b_2X^2 + ... + b_nX^n$$

$$(P = Q) \Leftrightarrow (a_i = b_i \text{ pour tout } i)$$

et on dit que P et Q sont égaux.

5.2.2 Addition

Soient $P, Q \in \Bbbk[X]$ tels que

$$P(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n$$

$$Q(X) = b_0 + b_1X + b_2X^2 + ... + b_nX^n$$

On définit

$$(P + Q)(X) = (a_0 + b_0) + (a_1 + b_1)X + ... + (a_n + b_n)X^n$$

5.2.3 Multiplication

Soient $P, Q \in \Bbbk[X]$ tels que

$$P(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n$$

$$Q(X) = b_0 + b_1X + b_2X^2 + ... + b_nX^m$$

On définit

$$(P \times Q)(X) = c_0 + c_1X + ... + c_rX^r$$

avec $r = n + m$ et $c_k = \sum_{i+j=k} a_ib_j$ pour $k \in \{0, 1, ..., r\}$.

5.2.4 Multiplication par un scalaire

Soit $P \in \mathbb{k}[X]$ tel que

$$P(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n$$

Soit $\lambda \in \mathbb{k}$.

On définit

$$(\lambda P)(X) = \lambda a_0 + \lambda a_1X + ... + \lambda a_nX^n$$

Exemple 5.3

Soient $P, Q \in \mathbb{R}[X]$ tels que

$$P(X) = 2 + X - 3X^4$$

$$Q(X) = X + X^2$$

On a

$$(3P - 4Q)(X) = 6 - X - 4X^2 - 9X^4,$$

et

$$(P \times Q)(X) = c_0 + c_1X + c_2X^2 + c_3X^3 + c_4X^4 + c_5X^5 + c_6X^6,$$

avec $c_k = \sum_{i+j=k} a_ib_j$ pour $k \in \{0, 1, ..., 6\}$

$$c_0 = \sum_{i+j=0} a_ib_j = a_0b_0 = 0$$

$$c_1 = \sum_{i+j=1} a_ib_j = a_0b_1 + a_1b_0 = 2 \times 1 + 1 \times 0 = 2$$

$$c_2 = \sum_{i+j=2} a_ib_j = a_0b_2 + a_2b_0 + a_1b_1 = 3$$

$$c_3 = \sum_{i+j=3} a_ib_j = a_0b_3 + a_3b_0 + a_1b_2 + a_2b_1 = 1$$

$$c_4 = \sum_{i+j=4} a_ib_j = 0$$

$$c_5 = \sum_{i+j=5} a_ib_j = -3$$

$$c_6 = \sum_{i+j=6} a_ib_j = -3$$

donc,

$$(P \times Q)(X) = 2X + 3X^2 + X^3 - 3X^5 - 3X^6.$$

Proposition 5.2

Soient $P, Q, R \in \mathbb{k}[X]$, on a

–

$$P + Q = Q + P, \qquad P \times Q = Q \times P$$

–

$$P + (Q + R) = (P + Q) + R$$

$$P \times (Q \times R) = (P \times Q) \times R$$

–

$$0 + P = P + 0 = P$$

$$1 \times P = P \times 1 = P$$

–

$$P \times (Q + R) = (P \times Q) + (P \times R)$$

5.3 Arithmétique des polynômes

5.3.1 Divisibilité

Définition 5.3

Soient $A, B \in \mathbb{k}[X]$, on dit que B divise A (ou que A est multiple de B ou que A est divisible par B) s'il existe $Q \in \mathbb{k}[X]$ tel que $A = BQ$. On note alors $B \mid A$.

Exemple 5.4

Soient $A, B \in \mathbb{R}[X]$ tels que

$$A(X) = 2 + X + 2X^2 - X^5$$

$$B(X) = 1 + X^2$$

A est divisible par B, car il existe $Q \in \mathbb{k}_3[X]$ tel que $A = BQ$.

Le polynôme Q est défini par

$$Q(X) = 2 + X - X^3.$$

Proposition 5.3

Soient $A, B, C \in \mathbb{k}[X]$, on a

– *Si* $B \mid A$ *et* $A \mid B$*, alors il existe* $\lambda \in \mathbb{k}^*$ *tel que* $A = \lambda B$.

– *Si* $A \mid B$ *et* $B \mid C$*, alors* $A \mid C$.

– *Si* $C \mid A$ *et* $C \mid B$*, alors* $C \mid UA + VB$ *avec* $U, V \in \mathbb{k}[X]$.

5.3.2 Division euclidienne

Définition 5.4

– *Soient* $A, B \in \mathbb{k}[X]$*, avec* $B \neq 0$*, alors il existe un unique polynpôme* Q *et il existe un unique polynôme* R *tels que :*

$$A = QB + R \qquad et \qquad \deg R < \deg B$$

Q est appelé le quotient et R le reste et cette écriture est la ***division euclidienne*** *de A par B.*

– *La condition* $\deg R < \deg B$ *signifie* $R = 0$ *ou bien* $0 \leq \deg R < \deg B$.

– *Enfin* $R = 0$ *si et seulement si* $B \mid A$.

Exemple 5.5

Soient $A, B \in \mathbb{R}[X]$ tels que

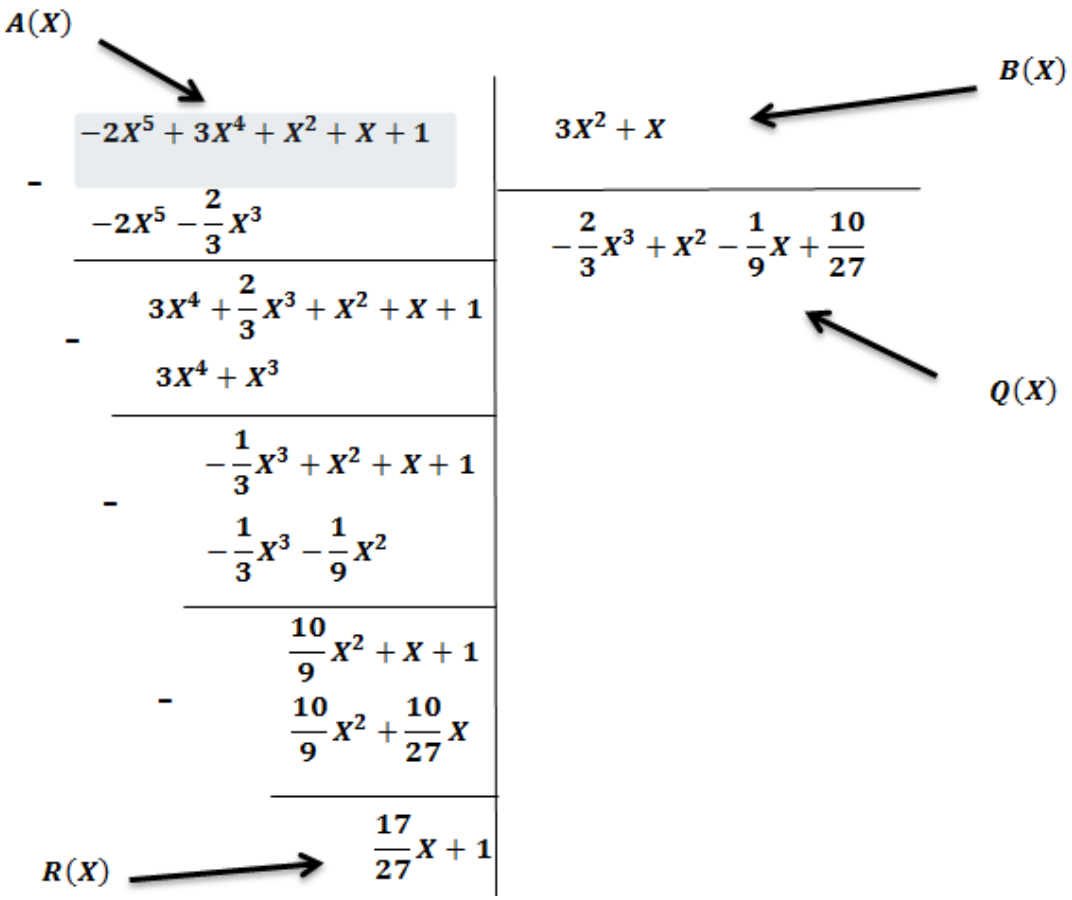
$$A(X) = 1 + X + X^2 + 3X^4 - 2X^5$$

$$B(X) = X + 3X^2$$

Alors on trouve

$$Q(X) = \tfrac{10}{27} - \tfrac{1}{9}X + X^2 - \tfrac{2}{3}X^3$$

$$R(X) = 1 + \tfrac{17}{27}X$$



5.3.3 Pgcd et ppcm de deux polynômes

Définition 5.5

Soient $A, B \in \mathbb{k}[X]$, avec $A \neq 0$ ou $B \neq 0$. Il existe un unique polynôme unitaire de plus grand degré qui divise à la fois A et B.

Cet unique polynôme est appelé le pgcd (plus grand commun diviseur) de A et B que l'on note $pgcd(A, B)$.

Algorithme d'Euclide.

Soient A et B des polynômes, $B \neq 0$.

On calcule les divisions euclidiennes successives,

$$A = BQ_1 + R_1, \qquad \deg R_1 < \deg B$$

$$B = R_1Q_2 + R_2, \qquad \deg R_2 < \deg R_1$$

$$R_1 = R_2Q_3 + R_3, \qquad \deg R_3 < \deg R_2$$

.

.

$$R_{k-2} = R_{k-1}Q_k + R_k, \qquad \deg R_k < \deg R_{k-1}$$

$$R_{k-1} = R_kQ_{k+1},$$

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

Exemple 5.6

Soient $A, B \in \mathbb{R}[X]$ tels que

$$A(X) = 2 + 3X + 4X^2 + 2X^3 - X^4$$

$$B(X) = X + X^2$$

On calcule les divisions euclidiennes successives,

$$A = B\left(1 + 3X - X^2\right) + (2 + 2X),$$

$$B = \left(\tfrac{1}{2}X\right)(2X + 2) + 0,$$

Le *pgcd* est le dernier reste non nul (rendu unitaire), donc

$$pgcd(A, B) = 1 + X$$

5.3.4 Polynômes premiers entre eux

Définition 5.6

Soient $A, B \in \Bbbk[X]$,

On dit que A *et* B *sont premiers entre eux si* $pgcd(A, B) = 1$.

Pour A, B *quelconques on peut se ramener à des polynômes premiers entre eux :*

si $pgcd(A, B) = D$, *alors* A *et* B *s'écrivent :* $A = DA'$, $B = DB'$ *avec* $pgcd(A', B') = 1$.

Exemple 5.7

Soient $A, B \in \mathbb{R}[X]$ tels que

$$A(X) = 1 + X^5$$

$$B(X) = 2 + 3X + X^2$$

On a

$$pgcd(A, B) = 1 + X,$$

donc

$$A(X) = (1 + X)(1 - X + X^2 - X^3 + X^4)$$

$$B(X) = (1 + X)(2 + X)$$

$$pgcd(1 - X + X^2 - X^3 + X^4, 2 + X) = 1$$

Théorème de Bézout

Soient $A, B \in \Bbbk[X]$, avec $A \neq 0$ ou $B \neq 0$. On note $D = pgcd(A, B)$.

Il existe deux polynômes $U, V \in \Bbbk[X]$ tels que

$$AU + BV = D$$

Proposition 5.4

Soient $A, B \in \Bbbk[X]$, A et B sont premiers entre eux s'il existe deux polynômes $U, V \in \Bbbk[X]$ tels que

$$AU + BV = 1$$

Définition 5.7

Soient $A, B \in \Bbbk[X]$, avec $A \neq 0$ et $B \neq 0$. Alors il existe un unique polynôme unitaire M de plus petit degré tel que $A \mid M$ et $B \mid M$.

Cet unique polynôme est appelé le ppcm (plus petit commun multiple) de A et B qu'on note $ppcm(A, B)$.

5.3.5 Décomposition en produit de facteurs irréductibles

Définition 5.8

Un polynôme A de $\Bbbk[X]$ est dit irréductible s'il est de degré supérieur ou égal à 1 et si ses seuls diviseurs sont les polynômes constants non nuls et les polynômes de la forme cA ($c \in \Bbbk^*$).

Un polynôme A est donc irréductible s'il a exactement deux diviseurs unitaires (ces deux diviseurssont alors 1 et $\frac{1}{d}A$ où d est le coefficient dominant).

Théorème 5.2

Tout polynôme non constant A s'écrit de manière unique sous la forme

$$A = cR_1^{\alpha_1}...R_k^{\alpha_k}$$

où $k \in \mathbb{N}^*$, $c \in \Bbbk^*$, R_1,...,R_k sont des polynômes unitaires irréductibles deux à deux distincts et $\forall i \in \{1, ..., k\}$ $\alpha_i \in \mathbb{N}^*$.

5.4 Racines d'un polynôme

5.4.1 Racines

Définition 5.9

Soit $P \in \Bbbk[X]$ tel que

$$P(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n$$

Soit $\alpha \in \Bbbk$.

On dit que α est une racine (ou un zéro) de P si

$$P(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + ... + a_n\alpha^n = 0$$

Exemple 5.7

Soient $A \in \mathbb{R}_3[X]$ tel que

$$A(X) = 3 - X + 2X^2 - 4X^3$$

Ona :

$$A(1) = 3 - (1) + 2(1)^2 - 4(1)^3 = 0$$

donc, $\alpha = 1$ est une racine de A.

Proposition 5.5

Soient $P(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n \in \Bbbk[X]$ et $\alpha \in \Bbbk$.

$$P(\alpha) = 0 \Leftrightarrow (X - \alpha) \text{ divise } P(X)$$

Démonstration

Soientt $P(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n \in \Bbbk[X]$ *et* $\alpha \in \Bbbk$.

La division euclidienne de $P(X)$ par $(X - \alpha)$ donne

$$P(X) = Q(X - \alpha) + R,$$

avec $\deg R < \deg(X - \alpha) = 1$.

Donc, $\deg R = 0$ ce qui donne R est une constante.

Alors,

$$P(\alpha) = 0 \Leftrightarrow R(\alpha) = 0 \Leftrightarrow R = 0,$$

donc, $(X - \alpha)$ *divise* $P(X)$.

5.4.2 Multiplicité des racines

Définition 5.10

Soient $P(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n \in \Bbbk[X]$ *et* $\alpha \in \Bbbk$.

On dit que α *est une racine de multiplicité* $k \in \mathbb{N}^*$ *(ou racine d'ordre* k*) de* P *si* $(X - \alpha)^k$ *divise* P *alors que* $(X - \alpha)^{k+1}$ *ne divise pas* P.

Lorsque $k = 1$ *on parle d'une racine simple, lorsque* $k = 2$ *d'une racine double, etc.*

Polynôme dérivé

On définit le polynôme dérivé de $P(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n \in \Bbbk[X]$ *comme suit*

$$P'(X) = a_1 + 2a_2X + ... + na_nX^{n-1}$$

On peut définir de la même façon les dérivées successive.

Proposition 5.6

Soient $P(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n \in \Bbbk[X]$ *et* $\alpha \in \Bbbk$.

On a l'équivalence entre

1. α *est une racine de multiplicité* $k \in \mathbb{N}^*$.
2. *Il existe* $Q(X) \in \Bbbk[X]$ *tel que*

$$P(X) = (X - \alpha)^k Q(X),$$

avec $Q(\alpha) \neq 0$.

3.
$$P(\alpha) = P'(\alpha) = ... = P^{(k-1)}(\alpha) = 0$$

$$et$$

$$P^{(k)}(\alpha) \neq 0$$

5.5 Exercices

Exercice 1

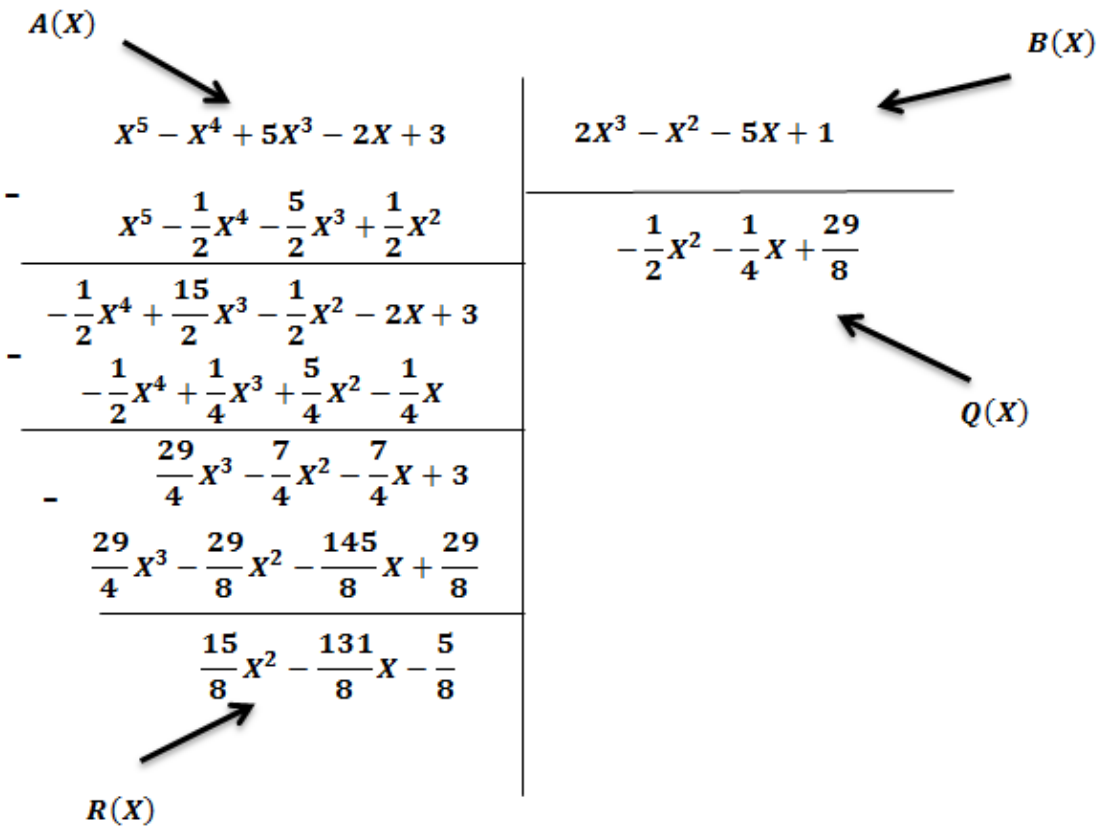
Dans les cas suivants, effectuer la division euclidienne de A par B :

1.
$$A(X) = X^5 - X^4 + 5X^3 - 2X + 3 \ et \quad B(X) = 2X^3 - X^2 - 5X + 1.$$

2.
$$A(X) = X^7 + 3X^5 - X^3 - 7X^2 + X \quad et \quad B(X) = X^4 + 4X^2 + 5X - 3.$$

Solution

1.
$$A(X) = X^5 - X^4 + 5X^3 - 2X + 3 \ et \quad B(X) = 2X^3 - X^2 - 5X + 1.$$



$$A(X) = B(X)\underbrace{\left(\frac{1}{2}X^2 - \frac{1}{4}X + \frac{29}{8}\right)}_{Q(X)} + \underbrace{\left(\frac{15}{8}X^2 + \frac{131}{8}X - \frac{5}{8}\right)}_{R(X)}$$

2.

$$A(X) = X^7 + 3X^5 - X^3 - 7X^2 + X \quad et \quad B(X) = X^4 + 4X^2 + 5X - 3.$$

De la même manière, on trouve

$$A(X) = B(X)\underbrace{\left(X^3 - X + 5\right)}_{Q(X)} + \underbrace{\left(6X^3 + 18X^2 + 23X - 15\right)}_{R(X)}$$

Exercice 2

Déterminer les pgcd des polynômes suivants :

1.

$$P(X) = X^6 - 7X^4 + 8X^3 - 7X + 7 \; et \; Q(X) = 3X^5 - 7X^3 + 3X^2 - 7.$$

2.

$$A(X) = X^5 + 4X^4 + X^3 - 5X^2 + 3X \; et \; B(X) = X^6 + 3X^5 + 3X^3 + 14X^2 + 15X.$$

Solution

1. $pgcd\,(P, Q)$

On calcule les divisions euclidiennes successives,

$$P = Q\underbrace{\left(\frac{1}{3}X\right)}_{Q_1} + \underbrace{\left(-\frac{14}{3}X^4 + 7X^3 - \frac{14}{3}X + 7\right)}_{R_1},$$

$$Q = R_1\underbrace{\left(-\frac{9}{14}X - \frac{27}{28}\right)}_{Q_2} + \underbrace{\left(-\frac{1}{4}X^3 - \frac{1}{4}\right)}_{R_2},$$

$$R_1 = R_2\underbrace{\left(\frac{56}{3}X - 28\right)}_{Q_3} + \underbrace{(0)}_{R_3}$$

Le *pgcd* est le dernier reste non nul (rendu unitaire), donc

$$pgcd(A, B) = 1 + X^3$$

2. $pgcd\,(A, B)$

On calcule les divisions euclidiennes successives,

$$B = A\underbrace{(X - 1)}_{Q_1} + \underbrace{\left(3X^4 + 9X^3 + 6X^2 + 18X\right)}_{R_1},$$

$$A = R_1\underbrace{\left(\frac{1}{3}X + \frac{1}{3}\right)}_{Q_2} + \underbrace{\left(-4X^3 - 13X^2 - 3X\right)}_{R_2},$$

$$R_1 = R_2\underbrace{\left(-\frac{3}{4}X + \frac{3}{16}\right)}_{Q_3} + \underbrace{\left(-\frac{99}{16}X^2 - \frac{297}{16}X\right)}_{R_3}$$

$$R_2 = R_3\underbrace{\left(\frac{64}{99}X + \frac{16}{99}\right)}_{Q_4} + \underbrace{(0)}_{R_4}$$

Le *pgcd* est le dernier reste non nul (rendu unitaire), donc

$$pgcd(A, B) = X^2 + 3X$$

Exercice 3

Montrer que les polynômes P et Q suivants sont premiers entre eux. Trouver U et $V \in \mathbb{k}[X]$ tel que $UP + VQ = 1$.

1. $$P(X) = 1 - 2X + X^3 + X^4 \quad et \quad Q(X) = 1 + X + X^2$$

2. $$P(X) = 1 + X^2 + X^3 \quad et \quad Q(X) = 1 + X + X^3$$

Solution

1. $pgcd(P, Q) = 1$?

On calcule les divisions euclidiennes successives,

$$P = Q\underbrace{\left(X^2 - 1\right)}_{Q_1} + \underbrace{(-X + 2)}_{R_1},$$

$$Q = R_1\underbrace{(-X - 3)}_{Q_2} + \underbrace{(-7)}_{R_2},$$

$$R_1 = R_2\underbrace{\left(\frac{1}{7}X - \frac{2}{7}\right)}_{Q_3} + \underbrace{(0)}_{R_3}$$

Le *pgcd* est le dernier reste non nul (rendu unitaire), donc

$$pgcd(P, Q) = 1$$

Trouver U et $V \in \mathbb{k}[X]$ tel que $UP + VQ = 1$

$$Q = R_1\underbrace{(-X - 3)}_{Q_2} + \underbrace{(-7)}_{R_2} \Leftrightarrow 7 = R_1\underbrace{(-X - 3)}_{Q_2} - Q$$

$$\Leftrightarrow 7 = \left(P - Q\underbrace{\left(X^2 - 1\right)}_{Q_1}\right)\underbrace{(-X - 3)}_{Q_2} - Q$$

$$\Leftrightarrow 7 = (-X - 3)P + (-(-X - 3)(X^2 - 1) - 1)Q$$

$$\Leftrightarrow \tfrac{1}{7}(-X - 3)P + \tfrac{1}{7}(-(-X - 3)(X^2 - 1) - 1)Q = 1$$

$$\Leftrightarrow \left(-\tfrac{1}{7}X - \tfrac{3}{7}\right)P + \left(\tfrac{1}{7}X^3 + \tfrac{3}{7}X^2 - \tfrac{1}{7}X - \tfrac{4}{7}\right)Q = 1$$

Donc,

$$U = -\tfrac{1}{7}X - \tfrac{3}{7}$$

$$V = \tfrac{1}{7}X^3 + \tfrac{3}{7}X^2 - \tfrac{1}{7}X - \tfrac{4}{7}$$

2. $pgcd\,(P,Q) = 1$?

On calcule les divisions euclidiennes successives,

$$P = Q\underbrace{(1)}_{Q_1} + \underbrace{\left(X^2 - X\right)}_{R_1},$$

$$Q = R_1\underbrace{(X+1)}_{Q_2} + \underbrace{(-2X-1)}_{R_2},$$

$$R_1 = R_2\underbrace{\left(-\frac{1}{2}X + \frac{3}{4}\right)}_{Q_3} + \underbrace{(-3)}_{R_3}$$

$$R_2 = R_3\underbrace{\left(\frac{2}{3}X + \frac{1}{3}\right)}_{Q_4} + \underbrace{(0)}_{R_4}$$

Le *pgcd* est le dernier reste non nul (rendu unitaire), donc

$$pgcd(P,Q) = 1$$

Trouver U et $V \in \mathbb{k}\,[X]$ tel que $UP + VQ = 1$

$$R_1 = R_2\underbrace{\left(-\frac{1}{2}X + \frac{3}{4}\right)}_{Q_3} + \underbrace{(-3)}_{R_3} \Leftrightarrow 3 = R_2\underbrace{\left(-\frac{1}{2}X + \frac{3}{4}\right)}_{Q_3} - R_1$$

$$\Leftrightarrow 3 = \left[Q - R_1\underbrace{(X+1)}_{Q_2}\right]\underbrace{\left(-\frac{1}{2}X + \frac{3}{4}\right)}_{Q_3} - R_1$$

$$\Leftrightarrow 3 = Q\left(-\tfrac{1}{2}X + \tfrac{3}{4}\right) - R_1\left((X+1)\left(-\tfrac{1}{2}X + \tfrac{3}{4}\right) - 1\right)$$

$$\Leftrightarrow 3 = Q\left(-\tfrac{1}{2}X + \tfrac{3}{4}\right) - (P-Q)\left((X+1)\left(-\tfrac{1}{2}X + \tfrac{3}{4}\right) - 1\right)$$

$$\Leftrightarrow -\tfrac{1}{3}\left((X+1)\left(-\tfrac{1}{2}X + \tfrac{3}{4}\right) - 1\right)P + \tfrac{1}{3}\left[\left(-\tfrac{1}{2}X + \tfrac{3}{4}\right) - \left((X+1)\left(-\tfrac{1}{2}X + \tfrac{3}{4}\right) - 1\right)\right]Q = 1$$

$$\Leftrightarrow \left(\tfrac{1}{6}X^2 + \tfrac{1}{12}X - \tfrac{1}{12}\right)P + \left(\tfrac{1}{6}X^2 - \tfrac{3}{12}X + \tfrac{1}{3}\right)Q = 1$$

Donc,

$$U = \frac{1}{6}X^2 + \frac{1}{12}X - \frac{1}{12}$$

$$V = \frac{1}{6}X^2 - \frac{3}{12}X + \frac{1}{3}$$

Exercice 4

Soit le polynôme

$$P(X) = 8 + 12X + 10X^2 + 5X^3 + X^4$$

1. *Montrer que* -2 *est une racine double du polynôme* P*.*
2. *Factoriser* P *dans* $\mathbb{R}[X]$*.*
3. *Déduire les racines de* P *dans* $\mathbb{C}$*.*

Solution

1. Montrer que -2 **est une racine double du polynôme** P**.**

On a :

$$P'(X) = 12 + 20X + 15X^2 + 4X^3$$

$$P(-2) = 8 + 12(-2) + 10(-2)^2 + 5(-2)^3 + (-2)^4$$

$$= 8 - 24 + 40 - 40 + 16$$

$$= 0$$

et

$$P'(-2) = 12 + 20(-2) + 15(-2)^2 + 4(-2)^3$$

$$= 12 - 20 + 60 - 32$$

$$= 20 \neq 0$$

Alors, $P(-2) = 0$ et $P'(-2) \neq 0$, ce qui montre que -2 est une racine double du polynôme P.

2. Factoriser P **dans** $\mathbb{R}[X]$**.**

On effectue la division euclidienne de $P(X)$ par $(X+2)^2$, on obtient

$$P(X) = (X+2)^2(X^2 + X + 2)$$

3. Déduire les racines de P **dans** $\mathbb{C}$

$$(P(X)=0) \Leftrightarrow \left((X+2)^2 (X^2+X+2) \right)$$

$$\Leftrightarrow \begin{cases} X+2=0 \\ \\ X^2+X+2=0 \end{cases}$$

On résout la deuxième équation. On a :

$$\Delta = (1)^2 - 4(1)(2) = -7,$$

donc l'équation admet deux racines complexes.

$$Z_1 = \frac{-1-i\sqrt{7}}{2}$$

$$Z_2 = \frac{-1+i\sqrt{7}}{2}$$

Alors, les racines de P dans C sont :

$$Z_0 = -2 \text{ (racine double)}, \qquad Z_1 = \frac{-1-i\sqrt{7}}{2} \text{ (racine simple)}, \qquad Z_2 = \frac{-1+i\sqrt{7}}{2} \text{ (racine simple)}$$

Exercice 5

Factoriser dans $\mathbb{C}[X]$ *puis dans* $\mathbb{R}[X]$ *les polynômes suivants :*

$$1+X^4$$

$$1-X^8$$

$$1-(X^2+3X-4)^2$$

Solution

1. On commence par chercher les racines complexes pour factoriser dans $\mathbb{C}[X]$, puis on regroupe les racines complexes conjuguées.

$$\begin{aligned} 1+X^4 &= \left(X-e^{\frac{\pi}{4}i}\right)\left(X-e^{\frac{3\pi}{4}i}\right)\left(X-e^{\frac{5\pi}{4}i}\right)\left(X-e^{\frac{7\pi}{4}i}\right) \\ &= \left[\left(X-e^{\frac{\pi}{4}i}\right)\left(X-e^{\frac{7\pi}{4}i}\right)\right]\left[\left(X-e^{\frac{5\pi}{4}i}\right)\left(X-e^{\frac{3\pi}{4}i}\right)\right] \\ &= \left[X^2-\left(e^{\frac{\pi}{4}i}+e^{\frac{7\pi}{4}i}\right)X+e^{\frac{\pi}{4}i}e^{\frac{7\pi}{4}i}\right]\left[X^2-\left(e^{\frac{5\pi}{4}i}+e^{\frac{3\pi}{4}i}\right)X+e^{\frac{5\pi}{4}i}e^{\frac{3\pi}{4}i}\right] \\ &= \left[X^2-\sqrt{2}X+1\right]\left[X^2+\sqrt{2}X+1\right] \end{aligned}$$

Les deux polynômes $X^2 - \sqrt{2}X + 1$ et $X^2 + \sqrt{2}X + 1$ n'ont pas de racines réelles, ils sont donc irréductibles dans $\mathbb{R}[X]$.

2.

$$\begin{aligned}
1 - X^8 &= (1 + X^4)(1 - X^4) \\
&= (1 + X^4)(1 - X^2)(1 + X^2) \\
&= (1 + X^4)(1 - X)(1 + X)(i + X)(X - i) \\
&= \left(X - e^{\frac{\pi}{4}i}\right)\left(X - e^{\frac{3\pi}{4}i}\right)\left(X - e^{\frac{5\pi}{4}i}\right)\left(X - e^{\frac{7\pi}{4}i}\right) \\
&(1 - X)(1 + X)(i + X)(X - i) \\
&= \left(X^2 - \sqrt{2}X + 1\right)\left(X^2 + \sqrt{2}X + 1\right)(1 + X^2)(1 - X)(1 + X)
\end{aligned}$$

3.

$$\begin{aligned}
1 - (X^2 + 3X - 4)^2 &= (1 - (X^2 + 3X - 4))(1 + (X^2 + 3X - 4)) \\
&= (-X^2 - 3X + 5)(X^2 + 3X - 3)
\end{aligned}$$

Factoriser de $-X^2 - 3X + 5$

$$\Delta = (-3)^2 - 4(-1)(5) = 29$$
$$X = \frac{-3+\sqrt{29}}{2}$$
$$ou$$
$$X = \frac{-3-\sqrt{29}}{2}$$

Donc,

$$-X^2 - 3X + 5 = -\left(X + \frac{3+\sqrt{29}}{2}\right)\left(X + \frac{3-\sqrt{29}}{2}\right)$$

Factoriser de $X^2 + 3X - 3$

$$\Delta = (3)^2 - 4(1)(-3) = 21$$
$$X = \frac{-3-\sqrt{21}}{2}$$
$$ou$$
$$X = \frac{-3+\sqrt{21}}{2}$$

Donc,

$$X^2 + 3X - 3 = \left(X + \frac{3+\sqrt{21}}{2}\right)\left(X - \frac{3-\sqrt{21}}{2}\right)$$

Alors,

$$1-\left(X^2+3X-4\right)^2=-\left(X+\tfrac{3+\sqrt{29}}{2}\right)\left(X+\tfrac{3-\sqrt{29}}{2}\right)\left(X+\tfrac{3+\sqrt{21}}{2}\right)\left(X-\tfrac{3-\sqrt{21}}{2}\right)$$

Bibliographie

[1] Cours de mathématiques Première année : exo7.

[2] Djebbar Samir, Cours Maths 1 Et Exercices Avec Solutions.

[3] M. Mechab : Cours d'algèbre-LMD Sciences et Techniques.